N° d'ordre : 16/2010-M/MT

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université des Sciences et de la Technologie
Houari Boumediene

Faculté de Mathématiques

Thèse
Présenté pour l'obtention du diplôme de Magister en Mathématiques
Spécialité : Algèbre et Théorie des Nombres

Par

Mme: MOULOUDJ Fouzia

Quelques Propriétés Algébriques de la famille de Cubiques de Weierstrass à deux paramètres:

$$\boldsymbol{E(s,t)}: \boldsymbol{y^2 + 2sxy + 2ty = x^3 + stx^2 - stx - t^2} \in \boldsymbol{Q}[x,y]$$

Soutenu le: 11 / 03 / 2010, devant le jury composé de:

Mr AIDER Meziane	Professeur à l'U.S.T.H.B	Président
Mr ZITOUNI Mohamed	Professeur à l'U.S.T.H.B	Directeur de thèse
Mr HERNANE Mohaned Ouamar	Maître de conférences à l'U.S.T.H.B	Examinateur
Mr HACHAICHI Mohamed Salah	Maître de conférences à l'U.S.T.H.B	Examinateur

REMERCIEMENTS

Je tiens à exprimer mes vifs remerciements à monsieur, AIDER Meziene, professeur à l'U.S.T.H.B qui me fait l'honneur de présider mon jury. Je remercie vivement Monsieur HERNANE Mohaned Ouamar, maître de conférences à l'U.S.T.H.B et Monsieur HACHAICHI Mohamed Salah , maître de conférences à l'U.S.T.H.B d'avoir bien voulu participer à mon jury comme examinateurs.

Mes remerciements et ma gratitude à mon promoteur Monsieur ZITOUNI Mohamed, professeur à l'U.S.T.H.B qui a été à l'origine de ce sujet de thèse de Magistère et dont les conseils ont grandement contribué à l'élaboration de cette étude.

DEDICACES

Je dédie cette thèse de Magistère à ma mère, pour m'avoir élevée et m'avoir donné tous son amour et sa tendresse, à mes sœurs, à mes frères , et à mon mari pour leur aide et soutien.

Sommaire

INTRODUCTION

Il existe plusieurs ouvrages et publications consacrés aux Courbes Elliptiques.

L'ouvrage de référence est «The Arithmetic of Elliptic Curves » de Joseph H. SILVERMAN [13].

De nombreux Mathématiciens ont leurs noms associés aux Courbes Elliptiques, Citons : WEIERSTRASS (équations), MORDELL-WEIL (groupe), SILVERMAN, LANG, etc…

La théorie des Courbes Elliptiques est liée à la Théorie des Nombres, à l'Analyse Complexe, et à la Géométrie Algébrique. [SILVERMAN]

Dans cette thèse, nous nous sommes intéressés à l'étude de quelques propriétés algébriques de la famille $E(s,t)$ de cubiques de Weierstrass :

$$E(s,t): \quad y^2 + 2sxy + 2ty = x^3 + stx^2 - stx - t^2 \in \mathbb{Q}[x,y] \qquad (1)$$

Dans le chapitre 1, nous avons exposé brièvement les Variétés Algébriques Affines, la Topologie de Zariski, les Variétés Projectives, les Variétés Abéliennes. Au point de vue de la Géométrie Algébrique, la famille $E(s,t)$ est une Variété Abélienne de dimension 1.

Dans le chapitre 2, nous avons exposé des notions indispensables de la Théorie Arithmétique des Courbes Elliptiques : Equation de Weierstrass, quelques Invariants, points singuliers et Genre.

Dans le chapitre3, nous avons passé en revue la Théorie de Mordell-Weil relativement à la structure du groupe additif abélien de l'ensemble $E(K)$ des points rationnels grâce à la règle géométrique de trois points colinéaires et le point à l'infini comme élément neutre.

Ensuite, nous avons construit le symétrique d'un point, la somme de deux points et, enfin nous avons défini le sous groupe de torsion.

Dans le quatrième chapitre, nous avons choisi quelques points de la Théorie des Morphismes des Courbes Elliptiques tels que : Isomorphismes, Automorphismes, Endomorphismes.

A la fin de chaque chapitre, nous avons appliqué les résultats à la famille $E(s,t)$ de cubiques de Weierstrass.

CHAPITRE 1
VARIETES ALGEBRIQUES ABELIENNES

Les cubiques de Weierstrass qui font l'objet de ma thèse possèdent plusieurs structures algébriques :

Variétés Algébriques, Courbes Algébriques planes, schémas…

L'étude des Variétés Algébriques est basée sur la Géométrie Algébrique. Cette théorie est décrite par plusieurs auteurs : [2], [11]

Ces Variétés sont construites sur des espaces affines et sur des espaces projectifs.

1- Variétés Algébriques Affines :

Définition 1 :

Un n-espace affine, pour tout entier $n \geq 1$, est l'ensemble des n- uples d'éléments a_i d'un corps commutatif K :

$$\mathbb{A}^n(K) = \{a = (a_1, a_2, \dots, a_n), a_i \in K\}$$

En langage géométrique, a est un point de l'espace affine $\mathbb{A}^n(K)$ et $a_1, a_2, \dots, a_n$ sont les coordonnées de ce point.
On considère l'anneau $B = K[x_1, x_2, \dots, x_n]$ des polynômes *f* à n variables et l'application :
$\mathbb{A}^n(K) \to B$, $(a_1, a_2, \dots, a_n) = a \to f(a), f \in B$.Chaque polynôme f possède des zéros dans une clôture algébrique du corps *K*.

Soit $Z(f_1, f_2, \dots, f_q)$ l'ensemble des zéros d'une famille $\{f_1, f_2, \dots, f_q\}$ de polynômes de l'anneau *B*.

Définition 2 :

Un sous ensemble X de l'espace affine $\mathbb{A}^n(K)$ est algébrique s'il est égal à l'ensemble $Z(f_1, f_2, \dots, f_q)$ des zéros d'une famille de polynômes $\{f_1, f_2, \dots, f_q\}$ de l'anneau B :

$$X = Z(\{f_i\}, i = 1 \dots q) = \{a \in \mathbb{A}^n(K), f(a) = 0, i = 1 \dots q\}.$$

Ces ensembles algébriques *X* permettent d'introduire une topologie sur l'espace affine.

Définition 3 :

La topologie de Zariski sur l'espace affine $\mathbb{A}^n(K)$ est définie avec les ensembles algébriques comme parties fermées et leurs complémentaires comme parties ouvertes.

Cette topologie de Zariski satisfait les axiomes d'une topologie [7]:

T_1 : Toute intersection de fermés est fermée.

T_2 : Toute réunion finie de fermés est fermée.

T_3 : Toute intersection finie d'ouverts est ouverte.

T_4 : Toute réunion d'ouverts est ouverte.

En particulier, l'ensemble vide et l'espace affine sont des ensembles ouverts et fermés à la fois, d'après [2]:

Il en résulte qu'un espace affine $\mathbb{A}^n(K)$ devient un espace topologique avec la topologie de Zariski.

Exemples d'ensembles Algébriques :

1) soit l'ensemble : $V_1 = \{x \in \mathbb{C},\ x^2 + 1 = 0\}$. Le polynôme $x^2 + 1 = 0$ de degré 2 admet 2 zéros $x = \pm i$, donc V_1 est un ensemble algébrique de 2 éléments dans l'espace affine $\mathbb{A}^1(\mathbb{C})$,
$\mathbb{C}$ = corps des nombres complexes.

2) soit l'ensemble : $V_2 = \{P = (x, y) \in \mathbb{C}^2 / \ x^2 - y^2 = 1\}$, Le polynôme $x^2 - y^2 = 1$ admet une infinité de zéros ; $x = r, \quad y = \pm\sqrt{r^2 - 1}, \quad r \in \mathbb{C}$;
V_2 est un ensemble algébrique dans l'espace affine $\mathbb{A}^2(\mathbb{C})$.

Les parties d'un espace topologique X sont classifiées en deux classes :

La classe des sous ensembles irréductibles qui ne sont pas réunions de sous ensembles fermés non vides disjoints, et la classe des sous ensembles réductibles Y qui sont réunions de sous ensembles fermés disjoints.

Définition 4 :

Une Variété Algébrique affine est un sous- ensemble fermé irréductible dans un n-espace affine $\mathbb{A}^n(K)$ muni de la topologie de Zariski.

Exemples de Variété Affine :

Soit l'espace affine $\mathbb{A}^3(\mathbb{R})$ sur un corps algébriquement clos K ;

L'ensemble : $V_3 = \{(x, y, z) \in \mathbb{A}^3(\mathbb{R}),\ x^2 - y = 0,\ z - x^3 = 0\}$ est formé des zéros ;

$x = k \in K,\ y = k^2 \in K \quad et \ z = k^3 \in K$, donc V_3 est un ensemble algébrique, c'est une Variété Affine.

Toute Variété Affine possède des sous Variétés quasi Affines :

Définition 5 :

Une Variété quasi Affine est un sous- ensemble ouvert d'une Variété Affine pour la topologie induite [2, page 21 ; exercice 3.10].

Exemple :

L'ensemble X= $\{(k, k^2, k^3), k \in K\}$ est une Variété Algébrique affine dans l'espace $\mathbb{A}^3(K)$ de dimension 1. [2], Exercice 1.2

2- Variétés Projectives :

A partir d'une Variété Affine $\mathbb{A}^{n+1}(K)$ et d'une relation d'équivalence, on construit une Variété Projective $\mathbb{P}^n(K)$.

Dans l'ensemble des (n+1)-uples $(x_1, x_2, \dots, x_{n+1})$ d'éléments non tous nuls d'un corps *K*, on considère la relation *R* définie par : $(x_1, x_2, \dots, x_{n+1})$ *R* $(b_1, b_2, \dots, b_{n+1})$ si et seulement si :

$(x_1, x_2, \dots, x_{n+1}) = \lambda(b_1, b_2, \dots, b_{n+1}) = (\lambda b_1, \lambda b_2, \dots, \lambda b_{n+1})$ pour tout $\boldsymbol{\lambda} \in K^*$.

Alors cette relation *R* est une relation d'équivalence dans l'espace $\mathbb{A}^{n+1}(K) - \{0\}$.

Définition 6:

L'espace projectif $\mathbb{P}^n(K)$ est le quotient de l'espace affine $\mathbb{A}^{n+1}(K)$ privé du point 0 par cette relation R : $\mathbb{P}^n(K) = (\mathbb{A}^{n+1}(K)$ - (0, 0… 0))/ R;

L'espace projectif peut donc être représenté par l'ensemble des droites passant par l'origine.

Exemples d'espaces Projectifs :

1) Soit l'espace projectif $\mathbb{P}^2(IR) = (\mathbb{A}^3(IR) - \{0\})/R$;

Le point à l'infini $0_E = (\infty, \infty)$ a pour coordonnées $0_E = (0, 1, 0) \in \mathbb{P}^2(IR)$; Cette classe est déterminée par la direction de l'axe OY.

2) Soit la famille *E(s, t)* de cubiques de Weierstrass d'équation affine :
$E(s,t): y^2 + 2sxy + 2ty = x^3 + stx^2 - stx - t^2 \in \mathbb{Q}[x, y]$
Dans le plan projectif $\mathbb{P}^2(\mathbb{Q})$, cette équation devient :
$E(s,t): Y^2Z + 2sXYZ + 2tYZ^2 = X^3 + stX^2Z - stXZ^2 - t^2Z^3 \in \mathbb{P}^2(\mathbb{Q})$

L'anneau $A = K[x_1, x_2, \dots, x_n, x_{n+1}]$ des polynômes homogènes à *(n+1)* indéterminées admet une décomposition de la forme : A=$\bigoplus A_d$, $d \geq 0$.

A est une somme directe de groupes abéliens A_d formés de polynômes homogènes de degré *d* qui satisfont la condition : $A_d A_l \subset A_{d+l}$.

Définition 7 :

Un sous ensemble Y de l'espace projectif $\mathbb{P}^n(K)$ est algébrique s'il est l'ensemble Z(T) des zéros d'une famille T de polynômes homogènes de l'anneau A.

Ces notions permettent de définir des Variétés Projectives et des Variétés quasi Projectives.

Tout espace algébrique projectif $\mathbb{P}^n(K)$ peut être muni d'une structure de Variété Algébrique Projective:

Définition 8 :

1) Une Variété Projective de dimension n est une partie X de l'espace projectif $\mathbb{P}^n(K)$ qui est fermée et irréductible pour la topologie de Zariski [2] ;

2) Une sous-Variété Projective d'une Variété Projective X de dimension n est une partie V de X qui est irréductible et fermée pour la topologie induite [2 ; page 10].

3) Une Variété quasi-Projective dans une Variété Projective X de dimension n est une partie V de X qui est ouverte pour la topologie induite [2].

Exemples:

1) Soit l'espace projectif $\mathbb{P}^1(\mathbb{R})$ réel.
Il est formé des couples (r_1, r_2), d'éléments réels r_1 et r_2
Des polynômes homogènes de degré $a \geq 1$:

$$f = r_1 x + r_2 y \in \mathbb{R}[x, y],\ f = r_1 x^a + r_2 y^a .$$

2) Soit l'espace projectif $\mathbb{P}^2(\mathbb{C})$ complexe.
Il est formé des triplets (r_1, r_2, r_3), d'éléments complexe r_1, r_2 et r_3

Des polynômes homogènes :

$$f = r_1 x + r_2 y + r_3 z \in \mathbb{C}[x, y, z],\ \text{de degré 1}$$

$$g = r_1 x^4 + r_3 x^3 y + r_3 x^2 y^2 + r_2 y^4, \text{ de degré 4}$$

$$h = r_1 x^n + r_2 y^n + r_3 x^k y^{n-k}, \text{ de degré } n,\ k < n$$

3) Soit l'espace projectif $\mathbb{P}^3(\mathbb{R})$ réel.
Il est formé des triplets (r_1, r_2, r_3, r_4), à coordonnées réelles
Des polynômes homogènes :

$$f = r_1 x + r_2 y + r_3 z + r_4 t \in \mathbb{R}[x, y, z, t], \text{ de degré 1}$$

$$g = r_1 x^2 yz + r_2 x^2 t^2 + r_3 xyzt,\ \text{de degré 4}$$

$$h = r_1 x^n + r_2 x^{n-1} y + r_3 x^{n-2} y^2 + r_4 x y^{n-1}, \text{ de degré } n$$

3- Variétés Abéliennes :

La notion de Variété Abélienne repose sur les fonctions régulières, et des morphismes….
Les Variétés Abéliennes sont construites sur des groupes algébriques.

Définition 9[2, exercice3.21]:

Une Variété de Groupe est une Variété Y [2, Définition page 15] munie de deux morphismes f, g qui satisfont :

$$\begin{cases} \boldsymbol{f: Y \times Y \to Y \ \ de\ valeur\ (a,b) \mapsto f(a,b) = a+b} \\ \boldsymbol{g \quad : Y \to Y \ \ de\ valeur\ \ y \mapsto g(y) = y^{-1}} \end{cases}$$

La Variété de Groupe munie de cette loi de groupe abélien est une Variété Abélienne.

Définition 10:

Une Variété Abélienne est une Variété de Groupe munie d'une loi de groupe abélien.

Exemple :
L'ensemble $V = \{(x,y) \in \mathbb{A}^2, y^2 + x^2 = x\}$ dans l'espace affine $\mathbb{A}^2(\mathbb{R})$ est muni d'une structure de Variété Abélienne de dimension 1 avec la loi :

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2,\ \ y_1 + y_2)$$

CHAPITRE II
CUBIQUES DE WEIERSTRASS

1- Equation de Weierstrass :

Nous nous intéressons dans ce chapitre à des cubiques particulières.

Définition 1 :

Une Courbe Elliptique est une cubique plane irréductible, non singulière, d'équation de Weierstrass de la forme :

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

Cette équation détermine une cubique de Weierstrass.

Les cinq coefficients a_i sont des éléments d'un corps commutatif *K*, global, local ou fini.

Les variables *x* et *y* sont des zéros de l'équation algébrique (1) ; donc *x* et *y* sont des éléments d'une clôture algébrique K_{al} de *K*.

L'équation (1) de Weierstrass peut être transformée en d'autres équations par des changements de variables convenables :

Nous éliminons les monômes en *xy* et en *y* par le changement de variables linéaire :

$$(x,y) \to (X, \frac{1}{2}(Y - a_1X - a_3)) \qquad (2)$$

Nous obtenons pour un corps *K* de *carac(K)* $\neq$ *2*, l'équation de Weierstrass E_1 :

$$E_1 : Y^2 = 4X^3 + b_2X^2 + 2b_4X + b_6 \in K[x,y] \qquad (2\text{-}1)$$

Les trois coefficients $\boldsymbol{b_{2i}}$ sont des polynômes homogènes de degré *2i* dans l'anneau $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$;

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

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

$$(X,Y) \to \left(\frac{x - 3b_2}{36}, \quad \frac{y}{108} \right) \qquad (3)$$

Pour un corps *K* de *carac(K)* $\neq$ *2,3*, nous obtenons l'équation de Weierstrass E_2 :

$$E_2 : y^2 = x^3 - 27c_4x - 54c_6 \in K[x,y] \qquad (3\text{-}1)$$

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

$$c_4 = b_2^2 - 24b_4 \quad \text{et} \quad c_6 = 36b_2b_4 - b_2^3 - 216b_6 \text{ ;} \qquad (3\text{-}2)$$

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

1) L'équation de Weierstrass : $E_3: y^2 = x^3 + Ax + B \in K[x,y]$;
2) Le modèle de Legendre : $E_4: y^2 = x(x-1)(x-a)$, avec $a \neq 0$ et 1 ;
3) Le modèle de Deuring : $E_5: y^2 + axy + y = x^3$, avec $a^3 \neq 3$;
4) Le modèle de Tate : $E_6: y^2 + xy = x^3 + ax + b$;

Où a et b sont des séries de puissances formelles en $q = exp\ (2i\pi z)$;

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

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

2- *Invariants d'une cubique de Weierstrass :*

Les cubiques possèdent plusieurs invariants : un discriminant, un invariant modulaire, un invariant différentiel, un conducteur, un régulateur, une série de Dirichlet, etc…
Ces invariants sont associés aux cubiques et ils permettent de classifier l'ensemble des cubiques**.**

Définition 2 :

Le discriminant d'une cubique de Weierstrass d'équation :

$\boldsymbol{E}: \boldsymbol{y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \in K[x,y]}$ ***et de carac(K)*** $\neq$***2,3***

est le polynôme homogène de degré 12 de l'anneau $\mathbb{Z}[b_2, b_4, b_6, b_8]$***, égale à :***

$$\Delta(\boldsymbol{E}) = \boldsymbol{9b_2\,b_4b_6 - 8b_4^3 - 27\,b_6^2 - b_2^2b_8}$$

Le coefficient $\boldsymbol{b_8}$ ***est déterminé par la relation :*** $\boldsymbol{4b_8 = b_2b_6 - b_4^2}$ **,**
$\boldsymbol{4b_8}$ ***est un polynôme homogène de degré 8 de l'anneau*** $\mathbb{Z}[b_2, b_4, b_6,]$**.**

Exemples :

Calcul des discriminants des modèles précédents :

1) le modèle *:* $E_3: y^2 = x^3 - 27c_4\,x - 54c_6 \in K[x,y]$, avec *carac(K)* $\neq$*2,3*

Le discriminant est égal à : $\Delta(E_3) = \frac{1}{1728}\ (c_4^3 - c_6^2)$

2) le modèle de Legendre : $E_4: y^2 = x(x-1)(x-a)$, avec a $\neq$ 0 et 1.

Le discriminant est égal à : $\Delta(E_4) = 16\,a^2\,(1-a)^2$

3) la famille des cubiques de Weierstrass à deux paramètres :

$$E(s,t): y^2 + 2sxy + 2ty = x^3 + stx^2 - stx - t^2 \in \mathbb{Q}[x,y]$$

J'obtiens les coefficients : $b_2 = 4s\,(s+t)$; $b_4 = 2st$; $b_6 = 0$; $b_8 = -(st)^2$

$c_4 = 16s[s(s+t)^2 - 3t]$; $c_6 = 2^5s^2\,(s+t)[9t - 2s(s+t)^2]$

Et le discriminant : $\Delta(E(s,t)) = 16\ s^3\,t^2\,[s(s+t)^2 - 4t]$

Il existe d'autres méthodes de calcul du discriminant d'un polynôme *f(x)* : c'est la méthode du résultant de 2 polynômes, d'après [7], [8]:

3- Résultant de deux polynômes et classification des cubiques planes :

Le discriminant $\Delta(E)$ d'une Courbe Elliptique *E* d'équation de Weierstrass : $y^2 = f(x)$ est lié au discriminant *dis(f)* de ce polynôme par la théorie du résultant.

Le discriminant d'un polynôme $g(x) \in K[x]$ est un élément du corps *K* égale à la fonction symétrique des racines θ_i de *g(x)* ;

Pour : $g(x) = \prod_{1\leq i\leq n}(x-\theta_i)$: $dis(g) = \prod_{i\neq j}(\theta_i - \theta_j)^2$

et pour : $g(x) = d_0 \prod_{1\leq i\leq n}(x-\theta_i)$: $dis(g) = d_0^{2n-2}\prod_{i\neq j}(\theta_i - \theta_j)^2$

Le discriminant *dis(g)* est nul si et seulement si le polynôme *g* admet une racine multiple.

Exemples :

1) $g(x) = (x-2)(x-3)(x-5)$

Alors : $dis(g) = (2-3)^2(3-5)^2(5-2)^2 = 36$

2) $f(x) = 2(x-1)(x-4)(x-5)$

Alors : $dis(f) = (2)^{2(3)-2}(1-4)^2(4-5)^2(5-1)^2 = 2^8.3^2.$

Nous exposons quelques points de la théorie du résultant :

Définition 3 :

Soient deux polynômes f et g de l'anneau $\mathbb{R}[x]$:

$$\boldsymbol{f(x) = d_0x^n + d_1x^{n+1} + \cdots + d_n, \quad \text{de degré } n \geq 1}$$

$$\boldsymbol{g(x) = r_0x^m + r_1x^{m+1} + \cdots + r_m, \quad \text{de degré } m \geq 1}$$

Le résultant des deux polynômes f et g est le déterminant d'ordre n + m, formé de m lignes de coefficients $(d_0, d_1, \ldots, d_n)$ et de n lignes de coefficients $(r_0, r_1, \ldots, r_m)$;

$$Res(f,g) = \begin{vmatrix} \boldsymbol{d_0} & d_1 & \ldots & \ldots & d_n & 0 & \ldots & \ldots & \ldots & 0 \\ 0 & \boldsymbol{d_0} & d_1 & \ldots & \ldots & d_n & 0 & \ldots & \ldots & 0 \\ 0 & 0 & \boldsymbol{d_0} & d_1 & \ldots & \ldots & d_n & 0 & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & \ldots & \ldots & 0 & \boldsymbol{d_0} & d_1 & \ldots & \ldots & d_n \\ r_0 & r_1 & \ldots & \ldots & \ldots & \ldots & \boldsymbol{r_m} & 0 & \ldots & 0 \\ 0 & r_0 & r_1 & \ldots & \ldots & \ldots & \ldots & \boldsymbol{r_m} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & \ldots & 0 & r_0 & r_1 & \ldots & \ldots & \ldots & \boldsymbol{r_m} \end{vmatrix}$$

m lignes (les m premières lignes) ; *n lignes* (les n dernières lignes)

Les termes manquant sont remplacés par des zéros.

La diagonale principale est formée de m termes d_0 et n termes r_m

Indiquons quelques propriétés des résultants ;

Le discriminant *dis(f)* est lié au résultant $Res(f, f')$ de *f(x)* et sa dérivée $f'(x)$.

Proposition 1 :

Soit un polynôme $f(x) = d_0(x-\theta_1)\dots(x-\theta_n)$ ***de degré*** $n \geq 1$, ***sa dérivée*** $f'(x)$.
Le discriminant dis(f) et le résultant satisfont la relation :

$$Res(f,f') = (-1)^{\frac{n(n-1)}{2}} d_0 dis(f) = {d_0}^{n-1} \prod_{1\leq i\leq n} f'(\theta_i)$$

□

Preuve : [8] Lang, et [7] Kostrikin

Proposition 2:

Soient deux polynômes :

$$f(x) = d_0 \prod_{1\leq i\leq n}(x-\theta_i), \quad \text{de degré } n \geq 1$$
$$g(x) = r_0 \prod_{1\leq j\leq m}(x-\varphi_j), \quad \text{de degré } m \geq 1$$

Alors leurs résultant est égal à :

$$\begin{aligned} Res(f,g) &= d_0^m \prod_{1\leq i\leq n} g(\theta_i) \\ &= (-1)^{mn} r_0^n \prod_{1\leq j\leq m} f(\varphi_j) \\ &= d_0^m r_0^n \prod_{i,j} (\theta_i - \varphi_j) \end{aligned}$$

Preuve : [6] Lang, et [7] Kostrikin

□

Corollaire :

1) Le résultant $Res(f,g)$ ***est nul si et seulement si les deux polynômes f et g ont une racine commune.***
2) Le résultant d'un polynôme f(x) et de sa dérivée $f'(x)$. ***est égal à :***

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

Preuve : [8] Lang, et [7] Kostrikin

□

Examinons les relations entre les discriminants *dis(f)* d'un polynôme cubique $f(x) \in K[x]$ **et** $\Delta(E)$ **d'une cubique de Weierstrass** $E: y^2 = f(x)$:

Proposition 3 :

Soit une cubique de Weierstrass $E: y^2 = f(x)$, ***alors Les discriminants*** $\Delta(E)$ ***de E et dis(f) du polynôme*** f ***sont liés par la relation :***

1) $\Delta(E) = 16\ dis(f)$ ***lorsque*** $f(x) = x^3 + a_2 x^2 + a_4 x + a_6$;
2) $\Delta(E) = 16\ dis(f)$ ***lorsque*** $f(x) = x^3 + Ax + B \in \mathbb{R}[x]$;
3) $16\Delta(E) = dis(f)$ ***lorsque*** $(x) = 4x^3 + b_2 x^2 + 2b_4 x + b_6$.

1) Preuve de : "$\Delta(E) = 16\ dis(f)$ lorsque $f(x) = x^3 + a_2\,x^2 + a_4x + a_6$"

Le calcul de $\Delta(E)$ nécessite le calcul des invariants b_{2i} de la cubique de Weierstrass $E: y^2 = x^3 + a_2\,x^2 + a_4x + a_6$:

$b_2 = 4a_2$, $b_4 = 2a_4$, $b_6 = 4a_6$, $b_8 = 4a_2a_6 - a_4^2$

Le discriminant : $\Delta(E) = 9b_2\,b_4b_6 - 8b_4^3 - 27\,b_6^2 - b_2^2b_8$

Alors : $\Delta(E) = 16(18a_2\,a_4a_6 - 4a_4^3 - 27\,a_6^2 - a_2^3a_6 + a_2^2\,a_4^2$

D'après les règles de calcul des discriminants des polynômes $f(x) \in \mathbb{R}[x]$:

$dis(f) = 18a_2\,a_4a_6 - 4a_4^3 - 27\,a_6^2 - a_2^3a_6 + a_2^2\,a_4^2$

Alors : lorsque $f(x) = x^3 + a_2\,x^2 + a_4x + a_6$ nous obtenons $\Delta(E) = 16\ dis(f)$

2) Preuve de : "$\Delta(E) = 16\ dis(f)$ lorsque $f(x) = x^3 + Ax + B \in \mathbb{R}[x]$"

Les invariants b_{2i} de la cubique de Weierstrass $E: y^2 = x^3 + Ax + B$ égalent :

$b_2 = 0$, $b_4 = 2A$, $b_6 = 4B$, $b_8 = B$

Alors : le discriminant $\Delta(E) = -16\,(4A^3 + 27B^2)$, et $dis(f) = -(4A^3 + 27B^2)$

Cela implique $\Delta(E) = 16\ dis(f)$ lorsque $f(x) = x^3 + Ax + B \in \mathbb{R}[x]$

3) Preuve de : "$\Delta(E) = 16\ dis(f)$ lorsque $f(x) = 4\,x^3 + b_2\,x^2 + 2b_4x + b_6$"

On utilise la théorie des résultants pour calculer le $dis(f)$:

$dis(f) = 16(9b_2\,b_4b_6 - 8b_4^3 - 27\,b_6^2 - b_2^2b_8)$ implique $dis(f) = 16\Delta(E)$

□

Définition 4 :

L'invariant modulaire d'une cubique de Weierstrass d'équation :

$\boldsymbol{E: y^2 + a_1xy + a_3y = x^3 + a_2\,x^2 + a_4x + a_6 \in K[x,y]}$ ***, est l'élément j(E) du corps K, carac(K) ≠ 2,3, égale à :***

$$\boldsymbol{j(E) = c_4^3\,(E)/\Delta(E)}$$

Exemples :

Calcul de l'invariant modulaire des modèles précédents :

1) L'invariant modulaire du modèle : $E_3: y^2 = x^3 + A\,x + B$, est égal à :

$$j(E_3) = \frac{4(12A)^3}{4A^3 + 27B^2}$$

2) L'invariant modulaire du modèle de Legendre : $E_4: y^2 = x(x-1)(x-a)$,

Avec $a \neq 0\ et\ 1$, est égal à :

$$j(E_4) = \frac{2^8(a^2-a+1)}{a^2(a-1)^2}$$

3) L'invariant modulaire de la famille des cubiques de Weierstrass à deux paramètres :

$E(s,t): y^2 + 2sxy + 2ty = x^3 + stx^2 - stx - t^2 \in \mathbb{Q}[x,y]$, est égal à :

$$j(E(s,t)) = \frac{16^2s[s(s+t)^2 - 3t]^3}{t^2\,[s(s+t)^2 - 4t]}$$

Définition 5 :

L'invariant différentiel d'une cubique de Weierstrass d'équation :

$\boldsymbol{E: F(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0}$, ***est la forme différentielle :***

$$\boldsymbol{\omega(E) = \frac{dx}{F'_y} = \frac{-dy}{F'_x}} ;$$

où $\boldsymbol{F'_y}$ ***et*** $\boldsymbol{F'_x}$ ***désignent les dérivées partielles d'ordre 1 de*** $\boldsymbol{F(x,y)}$ ***;***

$\boldsymbol{F'_x = a_1y - 3x^2 - 2a_2x - a_4}$, $\boldsymbol{et}$ $\boldsymbol{F'_y = 2y + a_1x + a_3}$.

Exemples :

Calcul de l'invariant différentiel des modèles précédents :

1) L'invariant différentiel du modèle : E_3: $y^2 = x^3 + A\,x + B$, est égal à :

$$\omega(E_3) = \frac{dx}{2y} = \frac{dy}{3x^2 + A}$$

2) L'invariant différentiel du modèle de Legendre : E_4 : $y^2 = x(x-1)(x-a)$, avec $a \neq 0$ et 1, égale à :

$$\omega(E_4) = \frac{dx}{2y} = \frac{dy}{3x^2 - 2(a+1)x + a}$$

3) L'invariant différentiel de la famille des cubiques de Weierstrass à deux paramètres :

$E(s,t)$: $y^2 + 2sxy + 2ty = x^3 + stx^2 - stx - t^2 \in \mathbb{Q}[x,y]$, égale à :

$$\omega\big(E(s,t)\big) = \frac{dx}{2(y + sx + t)} = \frac{-dy}{2sy - 3x^2 - st(2x-1)}$$

4- Points singuliers d'une Courbe Algébrique plane :

Dans la théorie des courbes algébriques planes, ces courbes possèdent des points ordinaires et des points singuliers :

Proposition 4 :

Soit une cubique de Weierstrass d'équation :

$\boldsymbol{C: y^2 = x^3 + a_2x^2 + a_4x + a_6 \in K[x,y]}$, ***de discriminant*** $\boldsymbol{\Delta(C)}$

1) Le point $\boldsymbol{0_C = (0,1,0)}$ ***du plan projectif*** $\boldsymbol{\mathbb{P}^2(K)}$ ***est un point non singulier sur C ;***

2) La cubique C est singulière si et seulement si son discriminant est nul $\boldsymbol{\Delta(C) = 0}$.

1) Preuve de « Le point $0_C = (0,1,0)$ est non singulier sur C »

Le point (0, 1, 0) est un point du plan projectif $IP^2(K)$. L'équation de C dans ce plan est de la forme :

$F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$

Les coordonnées du point $0_C = (0,1,0)$ satisfont cette équation : $F(0_C) = 0$

Il en résulte que ce point à l'infini est sur la cubique C.

Comme la dérivée partielle $F'_Z(0,1,0) = 1 \neq 0$ alors le point $0_C = (0,1,0)$ n'est pas singulier sur la cubique *C*.

2) Preuve de « *C* est singulière » implique « $\Delta(C) = 0$ »
Soit une cubique *C* d'équation de Weierstrass : $y^2 = f(x)$
L'hypothèse « *C* est singulière » implique que le polynôme *f(x)* admet une racine multiple, donc *dis(f) =0.*
La relation *dis(f) =16*$\Delta(C)$ implique que $\Delta(C) = 0$

3) Preuve de « $(\Delta(C) = 0$ » implique « *C* est singulière »
Soit une cubique *C* et $\Delta(C) = 0$;
La théorie du résultant et la relation entre $\Delta(C)$ et *dis(f)* impliquent la valeur *dis(f) =0.*
Cela implique que le polynôme *f* admet une racine multiple, donc la cubique *C* est singulière.
□

Définition 6 :

Un point P = (x, y) d'une Courbe Algébrique C d'équation f(x, y) = 0 est singulier si ses coordonnées satisfont les équations : $\boldsymbol{f(P) = f'_x(P) = f'_y(P) = 0}$**.**

Le nombre de points singuliers permet de classifier les courbes algébriques irréductibles en deux classes :

1) Classe des courbes irréductibles singulières ;
2) Classe des courbes irréductibles non singulières ;

Une cubique irréductible singulière admet 2 types de point singulier :
Un nœud, où la cubique admet 2 tangentes distinctes. **(Figure 1)**
Un point de rebroussement, où la cubique admet 2 tangentes confondues. **(Figure 2)**

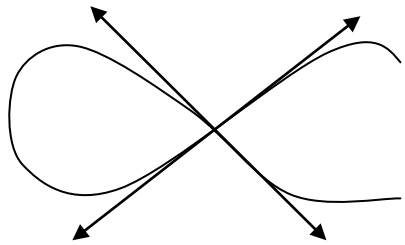


Figure 1 : un nœud

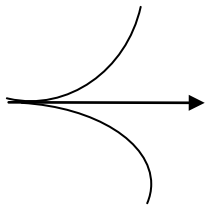


Figure 2 : un de rebroussement

Les courbes algébriques admettent un autre invariant : le genre, c'est un invariant arithmétique ;

Définition 7 :

Soit une courbe algébrique C d'équation f(x, y) =0 de degré n, qui possède m points singuliers, le genre de cette courbe est l'entier positif ou nul :

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

1) Une droite à une équation de degré *n = 1*, son genre est égal à 0 ;
2) Les cercles et les coniques ont des équations de degré *n = 2*, leur genre est égal à 0 ;
3) Les cubiques singulières ont une équation de degré *n = 3*, leur genre est égal à 0 ;
4) Les cubiques non singulières ont des équations de degré *n = 3*, leur genre est égal à 1.

5- *Courbes Elliptiques :*

Une Courbe Elliptique est, par définition une cubique de Weierstrass non singulière.
Son discriminant n'est pas nul. Le signe de ce discriminant influe sur l'allure de la Courbe Elliptique.

Proposition 5:

Soit une cubique de Weierstrass d'équation :

$E: y^2 = f(x) \in K[x, y]$, ***de discriminant*** $\Delta(E)$

La cubique E est une Courbe Elliptique si et seulement si son discriminant n'est pas nul :

$\Delta(E) \neq 0$.

1) Preuve de « $\Delta(E) \neq 0$ » implique « la cubique *E* est une Courbe Elliptique »
Soit une cubique *E* d'équation de Weierstrass : $E: y^2 = f(x)$, et de discriminant $\Delta(E)$
L'hypothèse « $\Delta(E) \neq 0$ » implique un résultant $Res(f, f') \neq 0$.
Alors le polynôme *f* admet 3 racines simples, donc la cubique *E* est une Courbe Elliptique.

2) Preuve de « la cubique *E* est une Courbe Elliptique » implique « $\Delta(E) \neq 0$ »
L'hypothèse « la cubique *E* est une Courbe Elliptique » implique que le polynôme *f(x)* admet 3 racines distinctes
Cela implique le résultant $Res(f, f') \neq 0$, alors : $dis(f) \neq 0$
La relation $dis(f) = 16\Delta(C)$ implique que $\Delta(E) \neq 0$.
□
Il y a 2 types de Courbes Elliptiques : le type des Courbes Elliptiques de discriminant $\Delta(E) > 0$, et le type des Courbes Elliptiques de discriminant $\Delta(E) < 0$.

Proposition 6 :

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

1) La courbe E coupe l'axe OX, ou une parallèle à l'axe OX en trois 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 $\Delta(E) < 0$ **.**

1) Preuve de « *E* coupe OX en 3 points » implique « $\Delta(E) > 0$ »
Soit une Courbe Elliptique *E*, alors son discriminant n'est pas nul : $\Delta(E) \neq 0$
L'hypothèse : la Courbe Elliptique *E* coupe l'axe OX en 3 points simples : $(e_i, 0)$, $i = 1,2,3$ implique que *E* admet une équation de Weierstrass de la forme:
$y^2 = (x - e_1)(x - e_2)(x - e_3) = f(x) \in IR[x]$

Par définition le discriminant d'un polynôme *f(x)* est égal à :
$dis(f) = \prod_{1 \leq i \leq j \leq 3} (e_i - e_j)^2$

Les 3 racines e_i sont des nombres réels,
Il en résulte que les carrés $(e_i - e_j)^2$ de différences de nombres réels sont positifs et $dis(f) > 0$
Donc la relation : $dis(f) = 16\,\Delta(E)$ implique que $\Delta(E) > 0$.

2) Preuve de « $\Delta(E) > 0$ » implique « E coupe OX en 3 points distincts »
Soit une Courbe Elliptique E d'équation de Weierstrass :
$E: Y^2 = 4X^3 + b_2 X^2 + 2 b_4 X + b_6 \in K[x, y]$ (1-2)

L'hypothèse « $\Delta(E) > 0$ » et la relation $dis(f) = 16\,\Delta(E)$ impliquent $dis(f) > 0$ (2-2)
(1-2) et (2-2) impliquent que le polynôme $f(x)$ admet 3 racines simples e_i , $i = 1,2,3$
Il en résulte 3 points d'intersection $(e_i\,, 0)$ de la courbe E avec l'axe OX.

3) Preuve de « E coupe OX en un seul point » implique « $\Delta(E) < 0$ »
Soit une Courbe Elliptique E qui coupe l'axe OX en un seul point (e, 0) simple, alors E a une équation de Weierstrass :
$y^2 = (x - e)\,(x^2 + rx + s) = f(x) \in \mathbb{R}\,[x]\,, r^2 - 4s < 0;\;\; g(x) = x^2 + rx + s$ (1-3)
Le polynôme du 3ème degré $f(x)$ admet 2 racines complexes conjuguées : $m \pm in$
Le discriminant de ce polynôme $f(x)$ est égal à :
$dis(f) = -4n^2((e - m)^2 + n^2)^2$; (2-3)
puisque les 3 nombres e, m et n sont réels, il en résulte la valeur :
$dis(f) < 0$ (3-3)
(3-3) et la relation $dis(f) = 16\,\Delta(E)$ impliquent le signe du discriminant : $\Delta(E) < 0$ (4-3)

4) Preuve de « $\Delta(E) < 0$ » implique « E coupe l'axe OX en un seul point simple »
Un polynôme cubique admet 3 racines e_i , $i = 1,2,3$ simples ou multiples
$E: y^2 = (x - e_1)\,(x - e_2)(x - e_3) = f(x) \in IR\,[x]$ (1-4)
La relation $dis(f) = 16\Delta(E)$ et l'hypothèse $\Delta(E) < 0$ impliquent $dis(f) < 0$ (2-4)
Le discriminant du polynôme $f(x)$ est égal à :
$dis(f) = -4^4(e_1 - e_2)^2(e_2 - e_3)^2(e_3 - e_1)^2$ (3-4)
(2-4) et (3-4) impliquent un carré négatif ;
Cela implique une racine e_1 réelle et les deux racines $e_2$et e_3 qui sont conjuguées complexes :
$m \pm in$
Alors : $dis(f) = -4n^2((e - m)^2 + n^2)^2$
Il en résulte un seul point d'intersection $(e_i, 0)$ de la courbe E avec l'axe OX, ce point est simple.
□

6-Classification des cubiques de Weierstrass :

Les propositions (4), (5) et (6) impliquent la classification des cubiques de Weierstrass

Proposition 7 ***: Soit l'ensemble des cubiques de Weierstrass:***
$\boldsymbol{E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \in K[x, y]}$ **.**

L'ensemble, des cubiques de discriminant $\Delta(E)$ et d'invariant $c_4(E)$ est classifié dans 4 classes :

1) ***Classe des cubiques singulières qui admettent un nœud, lorsque : $\Delta(E) = 0$ et $c_4(E) \neq 0$;***
2) ***Classe des cubiques singulières qui admettent un point de rebroussement lorsque : $\Delta(E) = 0$ et $c_4(E) = 0$;***
3) ***Classe des Courbes Elliptiques coupant l'axe OX en 3 points simples lorsque : $\Delta(E) > 0$;***
4) ***Classe des Courbes Elliptiques coupant l'axe OX en un seul point simple lorsque : $\Delta(E) < 0$.***

□

7- Application à la famille E(x, y) :

$$E(s,t): y^2 + 2sxy + 2ty = x^3 + stx^2 - stx - t^2 \in Q[x,y]$$

La famille $E(s,t)$ a des coefficients égaux à:

$a_1 = 2s, \quad a_2 = st, \quad a_3 = 2t, \quad a_4 = -st, \quad a_6 = -t^2$

En faisant les calculs, je trouve les résultats suivants:

$b_2 = 4s\,(s+t)$; $\quad b_4 = 2st$; $\quad b_6 = 0$; $b_8 = -(st)^2$

$c_4 = 16s[s(s+t)^2 - 3t]$; $\quad c_6 = 2^5 s^2(s+t)\,[9t - 2s(s+t)^2]$

Son discriminant : $\Delta(E(s,t)) = 16\ s^3\ t^2\ [s(s+t)^2 - 4t]$

Etude du signe du discriminant $\Delta(\boldsymbol{E(s,t)})$:

Je considère la fonction de second degré en t définie par : $h(t) = s(s+t)^2 - 4t$

Il en résulte la relation :

$$\Delta(E(s,t)) = 16\ s^3\ t^2\ h(t)$$

Le signe de $\Delta(E(s,t))$ est le produit des signes de s et celui de *h(t)*

$\Delta(E(s,t)) = 0$ implique : t = 0 ou s = 0 ou *h(t)* = 0

Etudions le signe de *h(t)* :

$h(t) = \mathrm{st}^2 + 2(\mathrm{s}^2 - 2)\mathrm{t} + \mathrm{s}^3$; avec $\mathrm{s}, \mathrm{t} \in \mathbb{Q}$ et $\mathrm{s} \neq 0$;

Le déterminant δ de la fonction *h(t)* égale:

$\delta = 4(1 - \mathrm{s}^2)$; *h(t)* = 0 implique *h(t)* admet 2 racines

$t_1 = \frac{1}{s}(2 - s^2 - 2\sqrt{1-s^2})$ et $t_2 = \frac{1}{s}(2 - s^2 + 2\sqrt{1-s^2})$;

Ces 2 racines sont réelles lorsque : $1 - s^2 > 0$ soit : $-1 < s < 1$

Le signe de δ est déterminé par :

1) Si $\mathrm{s} \in]-\infty,-1[\cup]1,+\infty[$ alors $\delta < 0$, cela implique $\begin{cases} \mathrm{s} < -1\ alors: h(\mathrm{t}) < 0 & (a); \\ \mathrm{s} > 1\ alors: \ h(t) > 0 & (b); \end{cases}$

2) Si $\mathrm{s} \in]-1,1[$ alors $\delta > 0$ cela implique que:

$$\begin{cases} \mathrm{s} \in]-1,0[\ , \text{ alors:} \begin{cases} h(t) > 0, t \in]\mathrm{t}_1, \mathrm{t}_2[& (c) \\ h(t) < 0, t \in]-\infty, \mathrm{t}_1[\cup]\mathrm{t}_2, +\infty[& (d) \end{cases} \\ \mathrm{s} \in]0,1[, \quad \text{alors:} \begin{cases} h(t) > 0, t \in]-\infty, \mathrm{t}_1[\cup]\mathrm{t}_2, +\infty[& (e) \\ h(t) < 0, t \in]\mathrm{t}_1, \mathrm{t}_2[& (f) \end{cases} \end{cases}$$

Alors je déduis le signe de discriminant $\Delta(E(s,t))$:

$\Delta(\boldsymbol{E(s,t)}) > 0$ si :

1) $\mathrm{s} \in]-\infty,-1[\cup]1,+\infty[$ et $\mathrm{t} \neq 0, \ \mathrm{t} \neq \mathrm{t}_1, \ \mathrm{t} \neq \mathrm{t}_2$
2) $\mathrm{s} \in]-1,0[$ et $\mathrm{t} \in]-\infty, \mathrm{t}_1[\cup]\mathrm{t}_2, +\infty[$
3) $\mathrm{s} \in]0,1[$ et $\mathrm{t} \in]-\infty, \mathrm{t}_1[\cup]\mathrm{t}_2, +\infty[$

Il y a 3 cas possibles

$\Delta(\boldsymbol{E}(\boldsymbol{s},\boldsymbol{t})) < 0$ si :

1) $s \in]-1,0[$ et $t \in]t_1, t_2[$
2) $s \in]0,1[$ et $t \in]t_1, t_2[$

Il y a 2 cas possibles.

$\Delta\big(\boldsymbol{E}(\boldsymbol{s},\boldsymbol{t})\big) = \boldsymbol{0}$ si:

1) $s = 0$
2) $t = 0$
3) $t = t_1 = \frac{1}{s}(2 - s^2 - 2\sqrt{1-s^2})$
4) $t = t_2 = \frac{1}{s}(2 - s^2 + 2\sqrt{1-s^2})$

Il y a 4 cas possibles.

1) Cubique singulière qui admet un nœud :

Pour $s = 1$ et $t = 0$, l'équation de Weierstrass :

$$E_1(1,0): y^2 + 2xy = x^3 \in \mathbb{Q}[x,y]$$

Avec le calcul j'obtiens : $\Delta(E_1) = 0$ et $c_4(E_1) = 2^2 \neq 0$

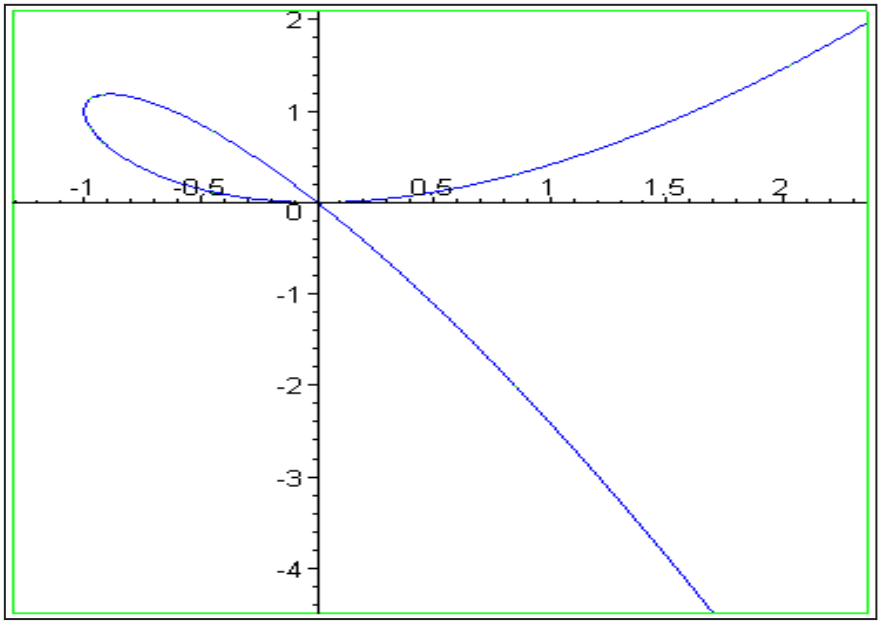
$\Delta(E_1) = 0$ implique que la cubique E_1 est singulière ;

$c_4(E_1) \neq 0$ implique que la cubique E_1 possède un nœud.

Tableau des coordonnées de quelques points de la cubique E_1

x	-1	0	1	2
y	1 racine double	0 1 racine	$-1 \pm \sqrt{2}$ 2 racines	$-2 \pm 2\sqrt{3}$ 2 racines

Le tableau implique que la cubique E_1 admet un nœud (0,0).



Courbe tracée avec logiciel « Maple »

2) Cubique singulière qui admet un point de rebroussement:

Pour $s = 0$ et $t = 2$, la cubique a pour équation :

$$E_2(0,2): y^2 + 4y = x^3 - 4 \in \mathbb{Q}[x, y]$$

Avec le calcul j'obtiens : $\Delta(E_2) = 0$ et $c_4(E_2) = 0$

$\Delta(E_2) = 0$ implique que la cubique E_2 est singulière ;

$c_4(E_2) = 0$ implique que la cubique E_2 possède un point de rebroussement.

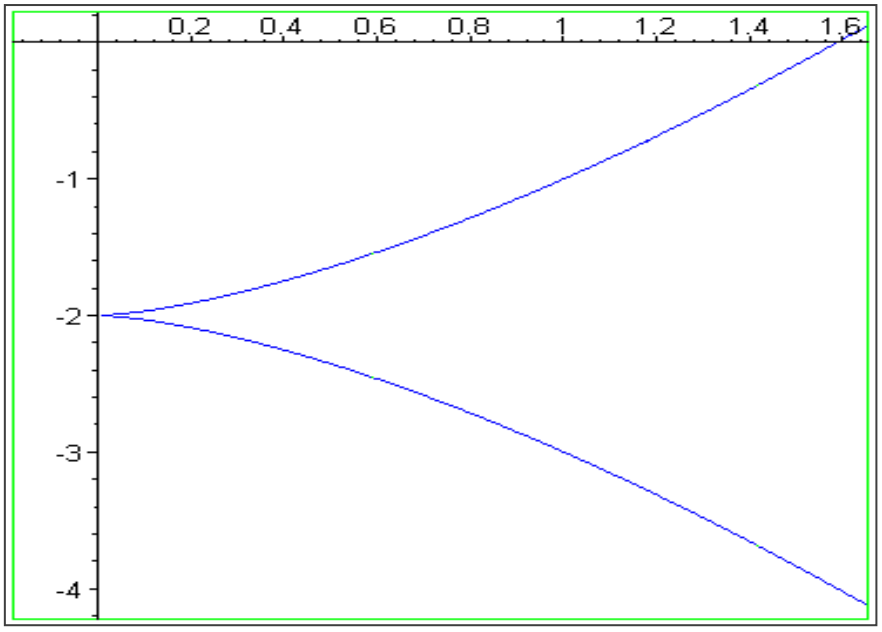
Tableau des coordonnées de quelques points de la cubique E_2

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

Le tableau implique :

La cubique E_2 coupe l'axe OX en un seul point ($\sqrt[3]{4}$,0) simple

La cubique E_2 admet un point de rebroussement (0, -2)



Courbe tracée avec logiciel « Maple »

3) Courbe Elliptique qui coupe l'axe OX en un seul point :

Pour $s = -\frac{1}{2}$ et $t = -2$, la cubique a pour équation :

$$E_3\left(-\frac{1}{2}, -2\right): y^2 - xy - 4y = x^3 + x^2 - x - 4 \in \mathbb{Q}[x, y]$$

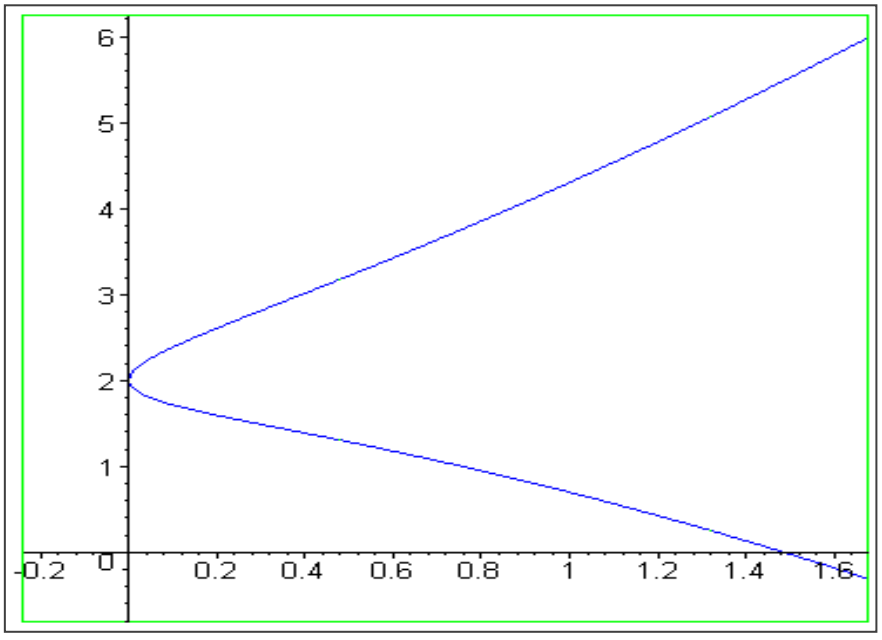
Avec le calcul j'obtiens : $\Delta(E_3) = -110$

$\Delta(E_3) < 0$ implique que la cubique E_3 est une Courbe Elliptique qui coupe l'axe OX en un seul point simple ;

Tableau des coordonnées de quelques points de la cubique E_3

x	-1	0	1. 4856	1
y	Pas de racines réelles	2 racine double	0 1 racine	$\frac{5 \pm \sqrt{13}}{2}$ 2 racines

Le tableau implique :
La Courbe Elliptique E_3 coupe l'axe OX en un seul point (1.4856, 0), elle est tangente à l'axe OY au point (0, 2).



Courbe tracée avec logiciel « Maple »

4) Courbe Elliptique qui coupe l'axe OX ou une parallèle à l'axe OX en 3 points simples :

Pour $s = -\frac{3}{2}$ et $t = 1$, la cubique de Weierstrass :

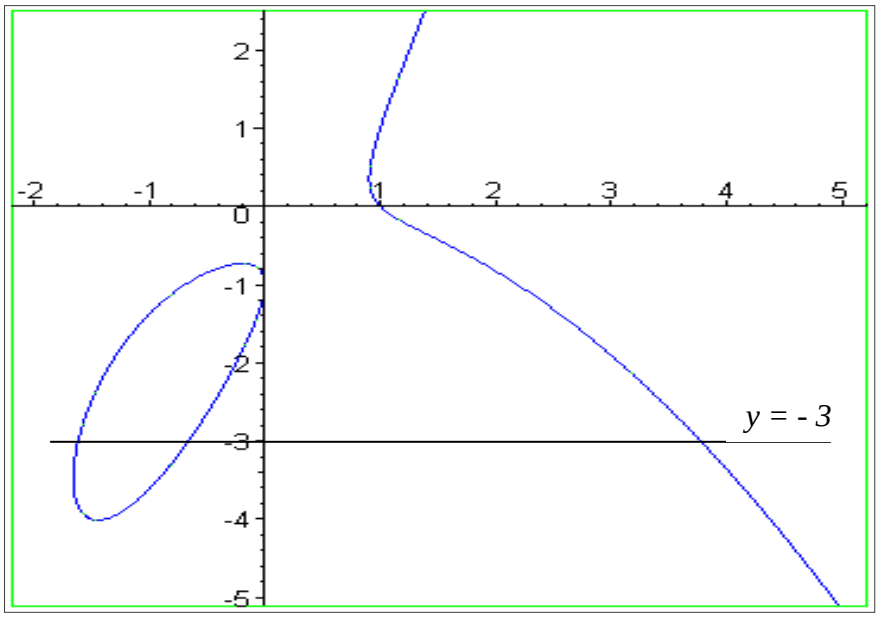
$$E_4\left(-\frac{3}{2}, 1\right): y^2 - 3xy + 2y = x^3 - \frac{3}{2}x^2 + \frac{3}{2}x - 1 \in \mathbb{Q}[x, y]$$

Avec le calcul j'obtiens : $\Delta(E_4) = {}^{3^6}/_{2^4} > 0$

Tableau des coordonnées de quelques points de la cubique E_4

x	0	1		-1	2
y	-1 Racine double	0	1	$\frac{-5 \pm \sqrt{5}}{2}$ 2 racines	$2 \pm 2\sqrt{2}$ 2 racines

La Courbe Elliptique E_4 coupe la parallèle à l'axe OX d'équation $y = -3$ en trois points simples **:** (-0.65784, -3), (-1. 6126, -3), (3. 7705, -3)



Courbe tracée avec logiciel « Maple»

CHAPITRE III

GROUPE DE MORDELL-WEIL DES COURBES ELLIPTIQUES

D'après [8]. Poincaré a conjecturé que l'ensemble *E(K)* des points *K*- rationnels d'une Courbe Elliptique *E* est un groupe abélien additif de type fini.
Sur une Courbe Elliptique *E*, d'équation de Weierstrass :

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

où *K* est un corps commutatif global, local ou fini.
L'élément neutre de ce groupe abélien *E(K)* est le point à l'infini 0_E.

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

Soit une Courbe Elliptique *E*, d'équation de Weierstrass :

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

Les 5 coefficients a_i sont des éléments d'un corps commutatif *K* ; les 2 variables *x* et *y* sont des éléments d'une clôture algébrique K_{al} de *K*.
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 0_E qui joue le rôle d'élément neutre ; $0_E = (\infty, \infty)$ dans le plan affine, et (0, 1, 0) dans le plan projectif $\mathbb{P}^2(K)$. Ce point est unique.
Il est déterminé par la direction de l'axe OY dans le plan $\mathbb{R}^2$.
3) Une loi de composition interne : $u: E(K) \times E(K) \to E(K)$ de valeur :

$$u(P_1, P_2) = P_1 + P_2$$

« Trois points colinéaires de la Courbe *E* ont une somme nulle » : $P_1 + P_2 + P_3 = 0_E$
Cette construction du point $P_1 + P_2$ est représentée dans la figure 1 :

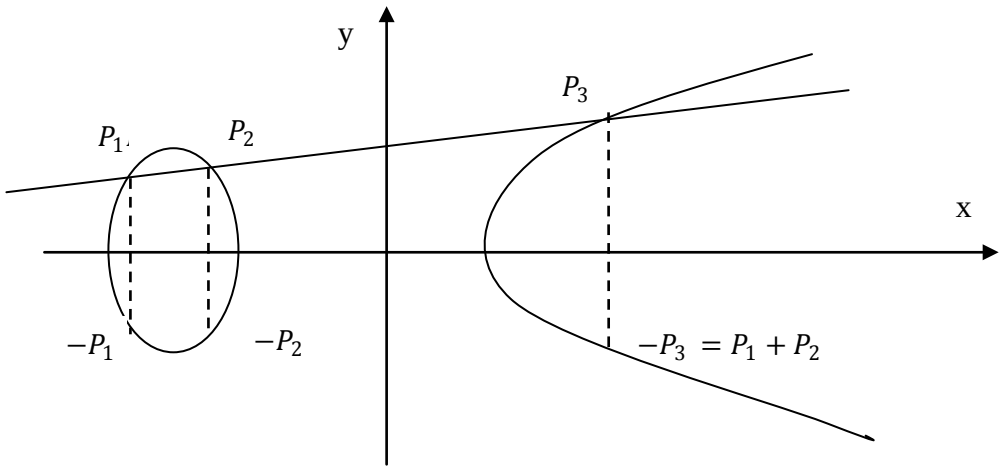


Figure 1

Vérification des 4 axiomes d'un groupe abélien additif: SIL [13]

Axiome de l'élément neutre 0_E [13]:

C'est le point 0_E à l'infini qui est l'élément neutre ; il est déterminé par la direction de l'axe OY.
Pour tout point *P* de *E(K)*, la sécante $P0_E$ est parallèle à l'axe OY.
La règle des 3 points colinéaires implique la relation:
$P + 0_E + 0_E = 0_E + 0_E + P = P$;
Donc : $P + 0_E = 0_E + P = P$;
L'axiome de l'élément neutre est vérifié.

Axiome du symétrique [13] :

Soit un point *P* sur le groupe *E(K)* ;

La parallèle à l'axe OY passant par le point P coupe la Courbe Elliptique *E* en trois points *P*, *S*, 0_E ; Il en résulte la relation : $P + S + 0_E = 0_E$
Nous en déduisions le symétrique : $S = -P$
Cette construction du symétrique d'un point *P* de la Courbe Elliptique *E* est représentée dans la figure 2 :

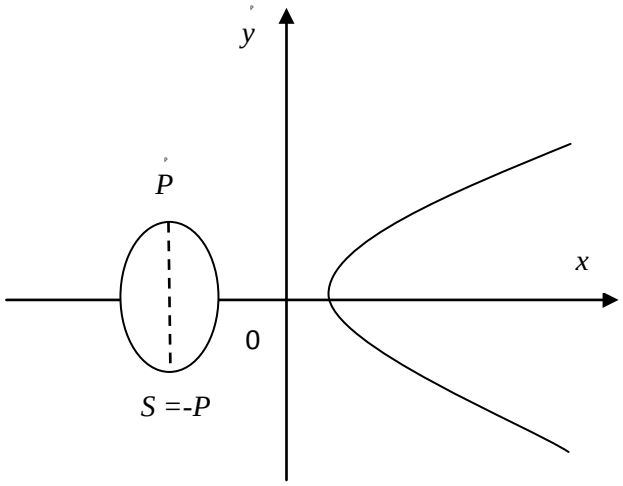


Figure 2

Axiome de commutativité [13]:

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

$$(P_1 + P_2) + P_3 = (P_2 + P_1) + P_3 = 0_E$$

Cela implique : $P_1 + P_2 = P_2 + P_1 = -P_3$.
L'axiome de commutativité est vérifié.

Axiome d'associativité [13] :

Soient 3 points *P, Q, R* colinéaires de la Courbe Elliptique *E* ;

Pour vérifier l'associativité de la loi, il faut comparer les points : *(P+ Q) + R et P+ (Q +R)*
Il faut donc calculer les coordonnées des sommes :
P+ Q = A, A +R = B, Q +R = C, P + C = D
Avec le calcul nous obtenons l'égalité *B= D*, l'axiome de l'associativité est ainsi vérifié :
(P+ Q) + R = P+ (Q +R).

□

Proposition 1 :

L'ensemble E(K) des points K- rationnels d'une cubique de Weierstrass, muni de l'application

$$u: E(K) \times E(K) \to E(K) \text{ de valeur : } u(P_1, P_2) = P_1 + P_2$$

est un groupe abélien additif d'élément neutre le point à l'infini $0_E = (\infty, \infty) = (0, 1, 0)$ ***, et de loi basée sur la règle géométrique de « 3 points colinéaires de la courbe E ont une somme nulle »:*** $P_1 + P_2 + P_3 = 0_E$;

□

Définition 1 :

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

Proposition 2 :

Le groupe de Mordell -Weil $E(K)$ ***d'une Courbe Elliptique E est de type fini, ce groupe est isomorphe au produit direct*** $E(K) \simeq T(E) \times \mathbb{Z}^r$ ***où*** $T(E)$ ***= le groupe de torsion de E,*** $\mathbb{Z}$ ***= groupe additif abélien et*** $r = r(E) \geq 0$.

Preuve : Lang [8].

Définition 2 :

L'entier $r = r(E) \geq 0$ ***est le rang de la Courbe Elliptique E.***
C'est le nombre de points qui engendrent la partie infini $E(K) - T(E)$

2- *Calcul des coordonnées du symétrique –P d'un point P de la somme* $P_1 + P_2$ *de 2 points* $P_1 \neq \pm P_2$ *, de la somme* $P + P = 2P$ *du groupe E(K)* [13]:

Soit la Courbe Elliptique *E* d'équation de Weierstrass:

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

Pour obtenir les coordonnées du symétrique d'un point, de la somme de 2 points et du point *2P* des Courbes Elliptiques, il faut utiliser la règle géométrique des 3 point colinéaires de la courbe et la théorie des intersections des courbes par des droites.

2-1) Calcul des coordonnées du symétrique –P d'un point P = (x, y) : (Figure 3)

Équation de la parallèle à OY passant par le point *P* : $x = x_P$
L'équation de Weierstrass de *E* devient une équation en *y* de degré 2 ;
La somme de ses 2 racines est égale à :

$$y + y_{(-P)} = -(a_1x + a_3) ;$$

Cela implique : $y_{(-P)} = -(y + a_1x + a_3)$
Nous en déduisons les coordonnées du symétrique *–P* de *P* :

P(x, y) et $-P(x, -y - a_1x - a_3)$;

Nous avons démontré la :

Proposition 3:

Le symétrique d'un point P = (x, y) d'une Courbe Elliptique E est le point –P de coordonnées

$x_{(-P)} = x_P$ ***et*** $y_{(-P)} = -(y + a_1x + a_3)$.

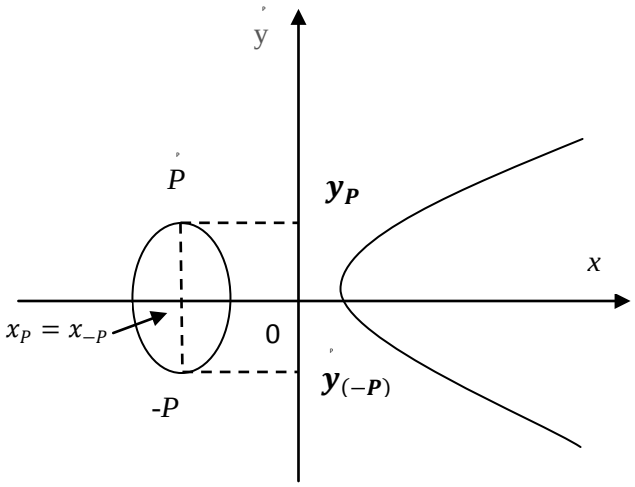


Figure 3

2-2) Calcul des coordonnées de la somme $P_1 + P_2$ de 2 points $P_i = (x_i, y_i) i = 1,2$ tels que

$P_1 \neq \pm P_2$: (Figure 4)

La sécante P_1P_2 a pour équation : $y = k\,(x - x_1) + y_1$ avec la pente $k = \frac{y_1 - y_2}{x_1 - x_2}$. (1)

Elle coupe la Courbe *E* en 3 points $P_1, P_2\ et\ P_3$. Ces 3 points satisfont la relation :

$P_1 + P_2 + P_3 = 0_E$

Remplaçons la valeur (1) dans l'équation de *E*, nous obtenons :

$[k\,(x - x_1) + y_1]^2 + (a_1x + a_3)[k\,(x - x_1) + y_1] = x^3 + a_2\,x^2 + a_4x + a_6$ (2)

L'équation de Weierstrass de *E* devient une équation en *x* de degré 3, elle admet 3 racines $x_1, x_2\ et\ x_3$

Avec la fonction symétrique élémentaire « somme des racines d'une équation algébrique» nous obtenons : $x_1 + x_2 + x_3 = -(a_2 - k^2 - a_1k)$ (3)

Cela implique l'abscisse x_3 du point P_3 :

$$x_3 = k^2 - a_2 + a_1k - x_1 - x_2 \quad (4)$$

Posons : $P_1 + P_2 = -P_3 = M =$ symétrique de P_3 (5)

D'après la proposition 3 : deux points symétriques ont même abscisse : $x_M = x_{P_3}$

L'ordonnée de M est égale à :

$$y_M = -y_3 - a_1x_3 - a_3 = -[k\,(x_3 - x_1) + y_1] - a_1x_3 - a_3$$

Nous obtenons ainsi les coordonnées de la somme : $P_1 + P_2 = M = (x_M, y_M)$ de 2 points

$x_M = k^2 + a_1k - a_2 - x_1 - x_2;$

$y_M = -k^3 - 2a_1k^2 + (a_2 - a_1^2 + 2x_1 + x_2)k + a_1a_2 - a_3 + a_1(x_1 + x_2) - y_1;$ (6)

Pour $k = \frac{y_1 - y_2}{x_1 - x_2}$.

Ces résultats sont rassemblés dans la ;

Proposition 4 :

Les coordonnées de la somme $M = P_1 + P_2$ de 2 points $P_1 \neq \pm P_2$ d'une Courbe Elliptique E sont égales à :

$$x_M = k^2 + a_1k - a_2 - x_1 - x_2;\ pour\ k = \frac{y_1 - y_2}{x_1 - x_2}$$

$$y_M = -k^3 - 2a_1k^2 + (a_2 - a_1^2 + 2x_1 + x_2)k + a_1a_2 - a_3 + a_1(x_1 + x_2) - y_1.$$

□

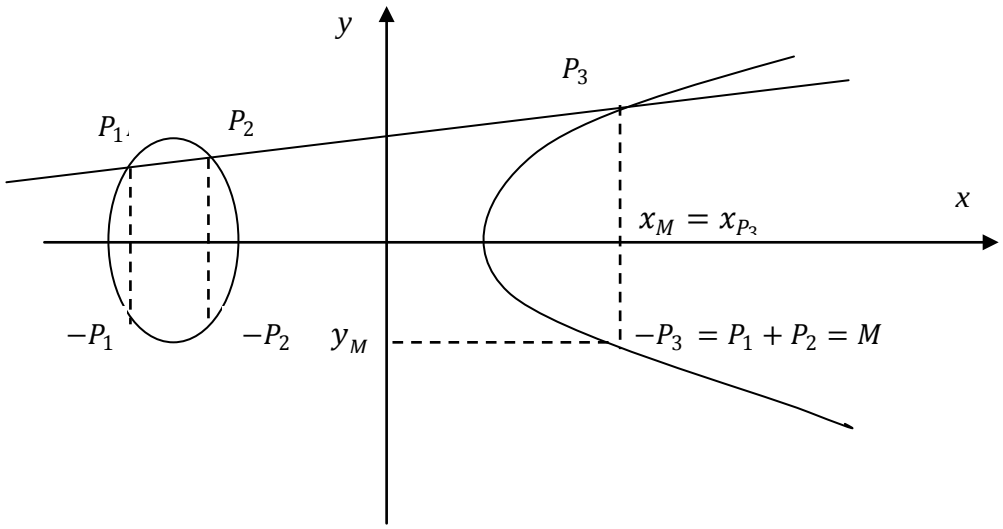


Figure 4

2-3) Calcul des coordonnées de la somme $P + P = 2P$: **(Figure 5)**

L'équation de la tangente à la courbe *E* au point *P* est égale à: $y = y_P'(x - x_P) + y_P$ (1)

La dérivée y' de y est égale à :

$$y' = \frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3} \quad (2)$$

La règle géométrique des 3 points colinéaires implique la relation:

$$P + P + T = 0_E \quad (3)$$

D'où la relation : $2P = -T$

Calcul des coordonnées du point *P* : dans (1) en remplaçant la valeur de y dans l'équation de *E*, nous obtenons l'équation cubique en x:

$$[y_P'(x - x_P) + y_P]^2 + (a_1x + a_3)[y_P'(x - x_P) + y_P] = x^3 + a_2x^2 + a_4x + a_6 \quad (4)$$

L'équation (4) est une équation en x de degré 3, elle admet 3 racines :

x_P racine double, x_T racine simple

La fonction symétrique élémentaire « somme des racines d'une équation algébrique» implique :

$$2x_P + x_T = -\frac{a_2 - y'^2_P - a_1y_P'}{1} \quad (6)$$

Nous en déduisons l'abscisse x_T :

$$x_T = y'^2_P + a_1y_p' - a_2 - 2x_P \quad (7)$$

Et l'ordonnée y_T:

$$y_T = y_P'(x_T - x_P) + y_P \quad (8)$$

Alors les coordonnées du point $2P = -T$ sont égales à :

$$x_{2P} = x_T \quad (9)$$

$$y_{2P} = -y_T - a_1 x_T - a_3$$

Avec le calcul nous obtenons les coordonnées:

$$x_{2P} = y'^2_P + a_1 y'_P - a_2 - 2x_P \qquad (10)$$
$$y_{2p} = -y'^3_P - 2a_1 y'^2_P + (a_2 + 3x_P - a_1^2) y'_P + a_1 a_2 - a_3 + 2a_1 x_P - y_P$$

Ces résultats sont rassemblés dans la :

Proposition 5:

Les coordonnées de la somme $P + P = 2P$ d'une Courbe Elliptique E sont égales à :

$$x_{2P} = y'^2_P + a_1 y'_P - a_2 - 2x_P, \text{ avec } y' = \frac{3x^2 + 2a_2 x + a_4 - a_1 y}{2y + a_1 x + a_3}$$

Polynôme quadratique en y'

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

Polynôme cubique en y'

□

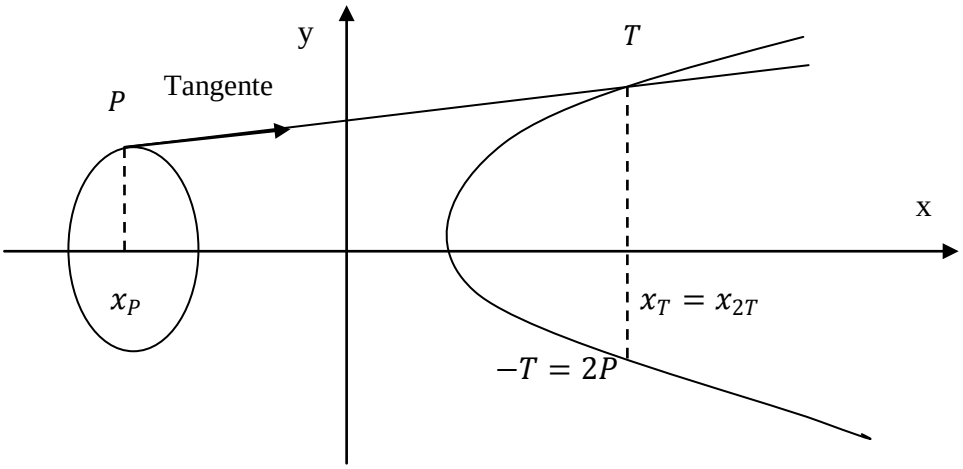


Figure 5

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

Soit une Courbe Elliptique E d'équation de Weierstrass :

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

Un point P du groupe de Mordel-Weil de la Courbe Elliptique E est un point d'ordre m si P appartient au groupe abélien $E(K)$ et $mP = 0_E$ avec $nP \neq 0_E$ pour $0 < n < m$.

Définition3 :

Soit m un entier rationnel et P un point d'ordre m du groupe de Mordelle-Weil $E(K)$ de la Courbe Elliptique E satisfaisant la relation $mP = 0_E$, alors le symbole mP représente les sommes :

$$\boldsymbol{mP} = \begin{cases} \boldsymbol{P + P + \cdots + P, m\ fois\ P, si\ m\ est\ positif} \\ \boldsymbol{(-P) + (-P) + \cdots + (-P), (-m)\ fois - P, si\ m\ est\ négatif} \\ \boldsymbol{0P = 0_E, si\ m = 0.} \end{cases}$$

Pour obtenir des formules utilisables Cassels a étudié les points *mP* sur une Courbe Elliptique particulière ;

Proposition 6 : (Lemme 7-2 de [1])

Soit une Courbe Elliptique E, d'équation de Weierstrass :

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

Les coordonnées des points mP, pour m ≥ 2 et pour tout point P de E, sont déterminées par les formules :

$$\boldsymbol{mP = \left[\frac{\phi_m(x,y)}{\psi_m^2(x,y)}, \frac{\omega_m(x,y)}{\psi_m^3(x,y)}\right]}$$

Où ϕ_m, ω_m et ψ_m sont des polynômes de l'anneau $\mathbb{Z}[x, y]$

Avec : $\boldsymbol{\psi_{-1} = -1,\ \ \psi_0 = 0,\ \ \psi_1 = 1,\ \ \psi_2 = 2y, \psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2}$

Et $\boldsymbol{\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - B^2 - A^3)}$

Les polynômes ψ_m satisfont les relations :

$$\psi_{2m} = 2\psi_m(\psi_{m+2}\psi_{m-1}^3 - \psi_{m-2}\psi_{m+1}^3)$$

$$\psi_{2m+1} = \psi_{m+2}\psi_{m-1}^3 - \psi_{m-1}\psi_{m+1}^3 \qquad \text{pour m} \geq 2$$

Les polynômes ϕ_m et ω_m satisfont les relations :

$$\phi_m = x\psi_m^2 - \psi_{m-1}\psi_{m+1}$$

$$4y\omega_m = \psi_{m-2}\psi_{m-1}^2 - \psi_{m+2}\psi_{m+1}^2 \qquad \text{pour m} \geq 3$$

Preuve :

Pour *m=-1*, le symétrique *–P* est égal à : $-(x, y) = (x, y) = (\frac{x}{(-1)^2}, \frac{y}{(-1)^3})$, alors $\psi_{-1} = -1$;

Pour *m= 0*, le symétrique *–P* est égal à : $0(x, y) = (\infty, \infty) = (\frac{x}{0}, \frac{y}{0})$, alors $\psi_0 = 0$;

Pour *m= 1*, le symétrique *–P* est égal à : $1(x, y) = (x, y) = (\frac{x}{1^2}, \frac{y}{1^3})$, alors $\psi_0 = 1$;

Pour *m= 2*, la formule $2P = (x_{2P}, y_{2P})$ est la fonction de $y' = \frac{3x^2+A}{2y}$ implique $\psi_1 = 2y$.

Cette proposition peut être démontrée par récurrence sur *m*.

□

Définition 4 :

Soit m un entier rationnel, l'ensemble $\boldsymbol{E(K)[m]}$ des points d'ordre m d'une Courbe Elliptique E, est le sous-groupe de m-torsion de E.

$$\boldsymbol{E(K)[m] = \{P \in E(K); mP = 0_E\}}$$

Définition 5 :

La réunion infinie des sous groupes de m-torsion de E est le groupe de torsion $\boldsymbol{T(E)}$ de la Courbe Elliptique E :

$\boldsymbol{T(E) = \cup_{m\in\mathbb{Z}} E(K)[m] = \{P \in E(K): mP = 0_m \text{ pour } m \in \mathbb{Z}\}}$ ***C'est l'ensemble des points de E d'ordre fini.***

4- *Application à la famille $E(s,t)$:*

Nous appliquons, ces résultats à la famille de Courbes Elliptiques $E(s,t)$ d'équation de Weierstrass :

$E(s,t)$: $\quad y^2 + 2sxy + 2ty = x^3 + stx^2 - stx - t^2 \in \mathbb{Q}[x,y]$ (1)

$st \neq 0$ *et* $t \neq t_i (i = 1,2)$ *où* $t_1 = \frac{1}{s}\left(2 - s^2 - 2\sqrt{1-s^2}\right)$, *et* $t_2 = \frac{1}{s}\left(2 - s^2 + 2\sqrt{1-s^2}\right)$;

Les 2 valeurs x, y sont des éléments d'une clôture algébrique $\mathbb{Q}_{al}$ du corps $\mathbb{Q}$.

1. *Le groupe de Mordell-Weil de la Courbe Elliptique $E(s,t)$:*

Soit $E(s,t)(\mathbb{Q})$ l'ensemble des points rationnels de la Courbe Elliptique de la famille $E(s,t)$.
Par la proposition 1, l'ensemble $E(s,t)(\mathbb{Q})$ admet une structure de groupe abélien additif, d'élément neutre le point 0_E, avec la règle géométrique :
« 3 points colinéaires de $E(s,t)$ ont une somme nulle : $P+R+S=0_E$ » et la loi de composition interne :
$f: E(s,t)(\mathbb{Q}) \times E(s,t)(\mathbb{Q}) \to E(s,t)(\mathbb{Q})$, avec $f(P,R) = P + R$.

Par définition 1, le groupe abélien $E(s,t)(\mathbb{Q})$ est le groupe de Mordell-Weil de la Courbe Elliptique $E(s,t)$.

2. *Calcul des coordonnées du symétrique – P d'un point P , de la somme $P_1 + P_2$ de 2 points $P_1 \neq \pm P_2$ Et de la somme $P + P = 2P$ du groupe $E(s,t)(\mathbb{Q})$:*

a) Calcul des coordonnées du symétrique $-P$ d'un point $P = (x_p, y_p) \in E(s,t)(\mathbb{Q})$.
Avec les formules de la proposition 3, on obtient les coordonnées du point
$-P = (x_{(-p)}, y_{(-p)})$
$x_{(-p)} = x_p$ et $y_{(-p)} = -y_p - 2sx_p - 2t$;

b) Calcul des coordonnées de la somme $M = P_1 + P_2$ de 2 points $P_i = (x_i, y_i) \in E(s,t)(\mathbb{Q})$ tels que $P_1 \neq \pm P_2$;
Avec la proposition 4, j'obtiens les coordonnées du point $M = (x_M, y_M)$
$x_M = k^2 + 2sk - st - x_1 - x_2$, polynôme de degré 2 en k.
$y_M = -k^3 - 4sk^2 + (st - 4s^2 + 2x_1 + x_2)k + 2s^2t - 2t + 2s(x_1 + x_2) - y_1$, polynôme de degré 3 en $k = \frac{y_1 - y_2}{x_1 - x_2}$

c) Calcul des coordonnées de la somme $2P = P + P$ pour tout $P = (x_p, y_p) \in E(s,t)(\mathbb{Q})$.
Par la proposition 4, nous obtenons les coordonnées du point $2P = (x_{2p}, y_{2p})$

$x_{2p} = y_p'^2 + 2sy_p' - st - 2x_p$, polynôme en y' de degré 2

$y_{2p} = -y_p'^3 - 4sy_p'^2 + (st - 4s^2 + 3x_p)y_p' + 2s^2t - 2t + 4sx_p - y_p$, polynôme en y' de degré 3:

$$y_p' = \frac{3x_p^2 + 2stx_p - st - 2sy_p}{2y_p + 2sx_p + 2t}$$

CHAPITRE IV

HOMOMORPHISMES DE COURBES ELLIPTIQUES

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

Les homomorphismes de Courbes Elliptiques se répartissent dans la classe des isomorphismes *{E(K) → E'(K)}*, la classe des automorphismes *{E(K) → E(K)}*.
E(K) et *E'(K)* sont les groupes de Mordell-Weil respectivement de *E* et *E'*.

Soient deux Courbes Elliptiques d'équations de Weierstrass :

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \in K[x,y]$$
$$E': y'^2 + a'_1x'y' + a'_3y' = x'^3 + a'_2x'^2 + a'_4x' + a'_6 \in K[x',y'] \quad (1)$$

Définition 1 :

Soit deux Courbes Elliptiques E et E' sur le même corps K, d'éléments neutres respectifs $\mathbf{0}_E$ ***et*** $\mathbf{0}_{E'}$ **.**
Un morphisme de Courbes Elliptiques est un homomorphisme de groupes abéliens additifs $f: E(K) \rightarrow E'(K)$.

1- Endomorphismes de Courbes Elliptiques :

Selon Deuring, l'anneau des endomorphismes *End(E)* 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.

Corollaire :

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 ordre de l'algèbre des quaternions.***
□

Définition 2 :

Soit une Courbe Elliptique E sur un corps K, d'élément neutre $\mathbf{0}_E$**.**
Un endomorphisme de Courbes Elliptiques est un endomorphisme de leurs groupes de Mordell- Weil.

2- *Isomorphismes de Courbes Elliptiques* :

Définition 3 :

Un isomorphisme de deux Courbes Elliptiques E et E′ est un homomorphisme de groupes de Mordell-Weil : $f: E(K) \rightarrow E'(K)$

Qui satisfait les formules d'isomorphisme de groupes :

$f(P+Q) = f(P) + f(Q)$;

$f(0_E) = 0_{E'}$ ***Pour les points à l'infini*** 0_E ***et*** $0_{E'}$ ***, et*** f ***bijective.***

Il y a un changement de variables particulier pour un tel isomorphisme.

Proposition1 :

Soit une Courbe Elliptique E sur un corps K et sa transformée E′ par le changement linéaire de variables : $x = u^2x' + r$; $y = u^3y' + s'u^2x' + t'$ (2)

Avec les éléments $u \neq 0$, r, s' ***et*** t' ***dans le corps K.***

Alors les Courbes Elliptiques E et E' sont isomorphes.

Preuve :

Soit une application : $\lambda : E(K) \rightarrow E'(K)$ de valeur $\lambda(x,y) = (u^2x' + r,\ u^3y' + s'u^2x' + t')$. Les calculs permettent de vérifier les relations d'isomorphisme de groupes :

$\lambda(P+R) = \lambda(P) + \lambda(R)$, $\lambda(0_E) = 0_{E'}$ et λ bijective.

□

Les relations entre les invariants de *E* et ceux de la Courbe isomorphe *E'* sont déterminées par le :

Corollaire :

Le changement de variables (2) indiqué dans la proposition 1 implique les relations entre les invariants des 2 Courbes Elliptiques E et E′ isomorphes :

1) Relation entre les coefficients a_i *et* a'_i :

$$\begin{cases} ua'_1 = a_1 + 2s' \\ u^2a'_2 = a_2 - s'a_1 + 3r - s'^2 \\ u^3a'_3 = a_3 + ra_1 + 2t' \\ u^4a'_4 = a_4 - s'a_3 + 2ra_2 - (t' + rs')a_1 + 3r^2 - 2s't' \\ u^6a'_6 = a_6 + ra_4 + r^2a_2 - t'a_3 - rt'a_1 - t'^2 + r^3 \end{cases} \quad (3)$$

2) Relation entre les invariants b_{2i} et b'_{2i} et entre c_{2i}et c'_{2i} :

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

Et : $u^4c'_4 = c_4$ *et* $u^6c'_6 = c_6$ (5)

3) Relation entre les invariants $\Delta(E)$ *et* $\Delta(E')$, $j(E)$ *et* $j(E')$:

$u^{12}\Delta(E') = \Delta(E)$ (6)

$j(E) = j(E')$ (7)

La relation (7) implique la:

Proposition 2 :

1) ***Deux Courbes Elliptiques E et E' sur un corps K, qui sont isomorphes admettent des invariants modulaires égaux*** $j(E) = j(E')$ **.**
2) ***Deux Courbes Elliptiques E et E' sur un corps K, qui admettent des invariants modulaires égaux*** $j(E) = j(E')$ ***sont isomorphes sur une clôture algébrique*** K_{alg} ***du corps K.***

Preuve de (1) :

Soit deux Courbes Elliptiques *E* et *E'* sur un corps *K* qui sont isomorphes.

Alors la $1^{ième}$ formule (5) précédente implique $j(E) = j(E')$.

Preuve de (2) :

Soit deux Courbes Elliptiques *E* et *E'* sur un corps *K* qui ont même invariant modulaire *j(E) = j (E')* et $carac(K) \neq 2,3$.

Considérons les 3 cas : $j(E) = 0$, $j(E) = 1728$ et $j(E) = A \neq 0$, 1728

1) Lorsque $j(E) = j(E') = 0$:

Je choisis des Courbes Elliptiques d'équation de Weierstrass :

$$E : y^2 = x^3 - 27c_4\,x^2 - 54c_6 \qquad (8)$$

$$E' : y^2 = x^3 - 27c'_4\,x^2 - 54c'_6$$

Alors la formule des invariants modulaires égale à:

$$j(E) = \frac{1728\,c_4^3}{(c_4^3 - c_6^2)} \quad \text{et} \quad j(E') = \frac{1728\,c_4'^3}{(c_4'^3 - c_6'^2)}$$

L'hypothèse $j(E) = j(E') = 0$ implique les relations :

$c_4 = c'_4 = 0$ et $c_6 \neq 0$, $c'_6 \neq 0$.

L'équation (8) devient : $E : y^2 = x^3 - 54c_6$

Les formules d'isomorphismes impliquent la relation : $u^6 c'_6 = c_6$

Il en résulte 6 valeurs $u = (c_6/c'_6)^{1/6}$ dans une clôture algébrique du corps *K*.

Cela implique les 6 isomorphismes $f : E(K) \rightarrow E'(K)$ de valeur : $f(x, y) = (u^2 x,\ u^3 y)$

2) Lorsque $j(E) = j(E') = 1728$:

Gardons les équations de Weierstrass des Courbes Elliptiques *E* et *E'*

L'hypothèse $j(E) = j(E') = 1728$ implique les relations :

$c_6 = c'_6 = 0$ et $c_4 \neq 0$, $c'_4 \neq 0$

L'équation (8) devient : $E : y^2 = x^3 - 27c_4\,x^2$

Les formules d'isomorphismes impliquent la relation: $u^4 c'_4 = c_4$

Cette équation admet 4 racines $u = (c_4/c'_4)^{1/4}$ dans une clôture algébrique de *K*.

Il en résulte 4 isomorphismes $f : E(K) \rightarrow E'(K)$ de valeur : $f(x, y) = (u^2 x,\ u^3 y)$

3) Lorsque $j(E) = j(E') = A \neq 0,1728$

Gardons les équations de Weierstrass des Courbes Elliptiques *E* et $'$.

La formule de l'invariant modulaire *j(E)* et L'hypothèse $j(E) = j(E') = A$ impliquent :

$$\frac{1728c_4^3}{c_4^3 - c_6^2} = \frac{1728c'^3_4}{c'^3_4 - c'^2_6} = A.$$

Alors on a la relation: $A\,c_6^2 = c_4^3(A - 1728)$

Par les formules d'isomorphismes, il existe un élément non nul *u* tel que :

$u^4 c'_4 = c_4 \quad et \quad u^6 c'_6 = c_6;$

nous déduisons les solutions : $u = (c_4/c'_4)^{1/4} = (c_6/c'_6)^{1/6}$.

Cela implique 24 isomorphismes : $f : E(K) \rightarrow E'(K)$ de valeur : $f(x, y) = (u^2 x,\ u^3 y)$;

□

Il en résulte une classification des Courbes Elliptiques en classes de courbes de même invariant modulaire.

1) Classe des Courbes Elliptiques d'invariant $j(E) = 0$
2) Classe des Courbes Elliptiques d'invariant $j(E) = 1728$
3) Classe des Courbes Elliptiques d'invariant $j(E) \neq 0,\ 1728$

Exemple de Courbes Elliptiques isomorphes :

Soit une Courbe Elliptique *E* d'équation de Weierstrass :

$E: y^2 + 2xy + y = x^3 + 3x^2 + 4x + 1 \in K[x, y], \qquad cara(K) \neq 2,3$

$\Delta(E) = -195.$

Une Courbe Elliptique isomorphe *E'* pour les valeurs :

$u = 2, \qquad r = 1, \qquad s' = 0, \qquad t' = 0:$

$$E' : y'^2 + x'y' + \frac{3}{8}y' = x'^3 + \frac{3}{2}x'^2 + \frac{13}{16}x' + \frac{9}{64}$$

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

$$b'_2 = 7; \qquad b'_4 = 2; \qquad b'_6 = \frac{45}{64}; \qquad b'_8 = \frac{59}{256};$$

$$\Delta(E') = \frac{-195}{4096} = 2^{-12}\,\Delta(E)$$

Tableau de valeurs des coordonnées de quelques points de la Courbe *E :*

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* coupe l'axe OX en un seul point d'abscisse x_1 obtenue avec le logiciel :

$x_1 \approx -0,31$.

Elle coupe l'axe OY en 2 points d'ordonnées : $-\frac{1}{2} + \frac{\sqrt{5}}{2}$ et $-\frac{1}{2} - \frac{\sqrt{5}}{2}$

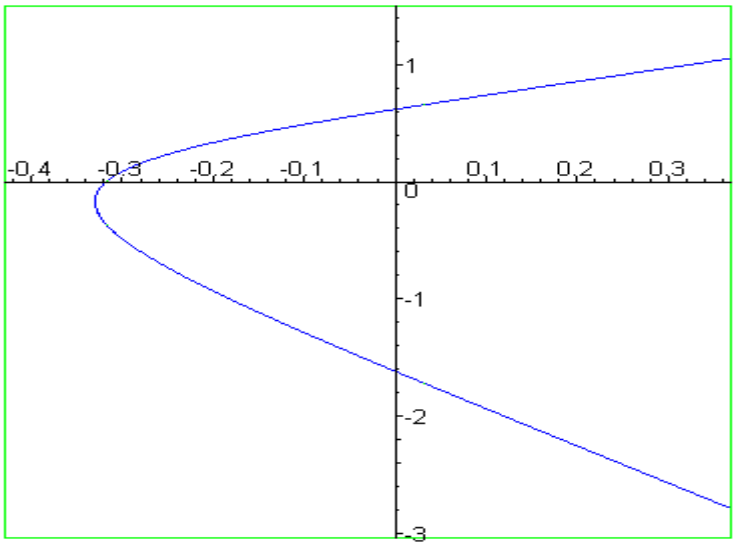
Tableau de valeurs des coordonnées de quelques points de la Courbe *E'* :

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'* coupe l'axe OX en un seul point d'abscisse x_2 obtenue avec le logiciel : $x_2 \approx -0{,}33$.

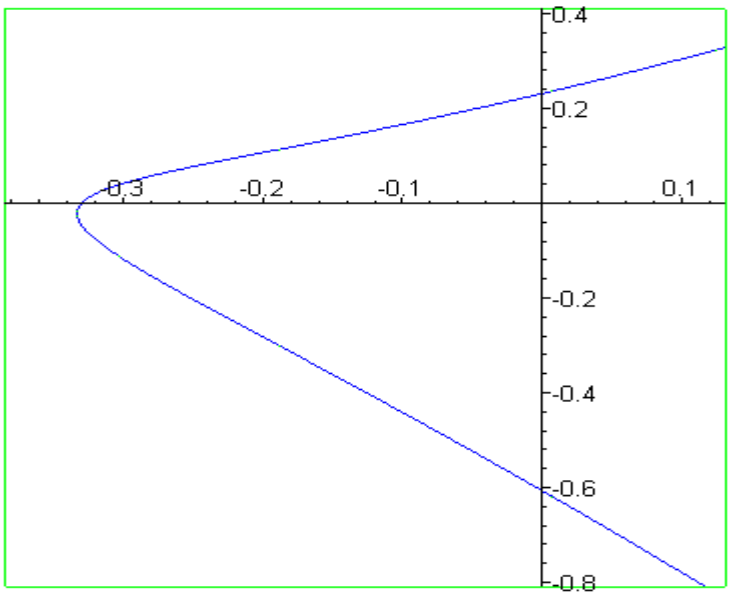
Elle coupe l'axe OY en 2 points d'ordonnées : $-\frac{3}{16} + \frac{3\sqrt{5}}{16}$ et $-\frac{3}{16} - \frac{3\sqrt{5}}{16}$

La Courbe Elliptique *E* :



Courbe tracée avec logiciel « Maple»

La Courbe Elliptique *E'* isomorphe à *E*:



Courbe tracée avec logiciel « Maple»

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'équivalence de Courbes Elliptiques isomorphes :
$cl(E') = \{E', E'_1, E'_2, \dots, E'_n\}$, d'invariants modulaires égaux :
$j(E) = j(E'_1) = j(E'_2) = \cdots = j(E'_n)$

3-Application à la famille E(s, t) :

Soit une Courbe Elliptique $E\left(\frac{1}{2}, 1\right)$ d'équation de Weierstrass :

$$E\left(\frac{1}{2}, 1\right): y^2 + xy + 2y = x^3 + \frac{1}{2}x^2 - \frac{1}{2}x - 1 \in \mathbb{Q}[x, y], \qquad cara(\mathbb{Q}) \neq 2,3$$

$$\Delta(E) = -\frac{7}{4}$$

Une Courbe Elliptique isomorphe *E'* pour les valeurs :

$$u = 2, \quad r = 1, \quad s' = 0, \quad t' = 0:$$

$$E'\left(\frac{1}{2}, 1\right): y'^2 + \frac{1}{2}x'y' + \frac{3}{8}y' = x'^3 + \frac{7}{8}x'^2 + \frac{7}{32}x'$$

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

$$b'_2 = \frac{15}{4}; \quad b'_4 = \frac{5}{4}; \quad b'_6 = \frac{9}{64}; \quad b'_8 = \frac{35}{1024};$$

$$\Delta(E') = \frac{-7}{2^{14}} = 2^{-12}\,\Delta(E)$$

Tableau de valeurs des coordonnées de quelques points de la Courbe *E* :

x	-1	0	1		2	4
y	$Pas\ de\ valeurs$	-1	-3	0	$-2 \pm 2\sqrt{3}$	$-3 \pm \sqrt{78}$

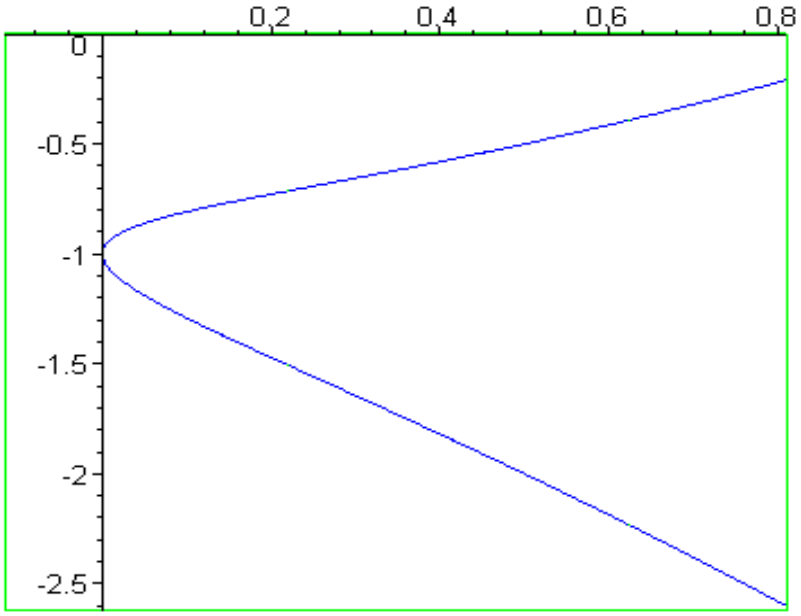
La Courbe Elliptique *E* coupe l'axe OX en un seul point (1, 0).
Elle coupe l'axe OY en un seul point (0, -1).

Tableau de valeurs des coordonnées de quelques points de la Courbe *E'* :

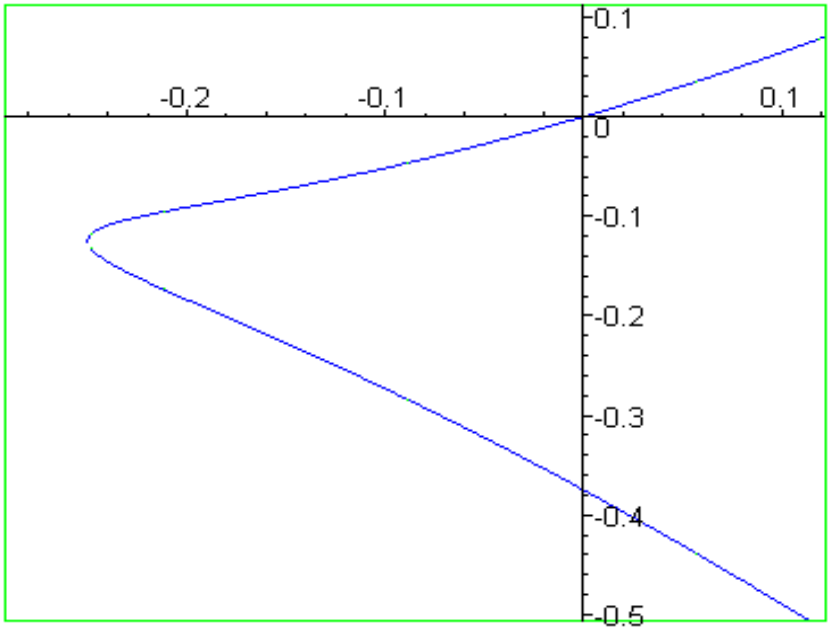
x'	-1	0		1	2	3
y'	$Pas\ de\ valeurs$	0	$-\frac{3}{8}$	$\frac{-7}{16} \pm \frac{3\sqrt{65}}{16}$	$-\frac{11}{16} \pm \frac{\sqrt{3177}}{16}$	$-\frac{15}{16} \pm \frac{\sqrt{9321}}{16}$

La courbe Elliptique *E'* passe par l'origine O (0, 0).
Elle coupe l'axe OY en un seul point $(0, -\frac{3}{8})$.

La Courbe Elliptique $E\left(\frac{1}{2},1\right)$:



La Courbe Elliptique $E'\left(\frac{1}{2},1\right)$ isomorphe à $E\left(\frac{1}{2},1\right)$:



4- Automorphismes d'une Courbe Elliptique :

Sur un corps *K*, les automorphismes d'une Courbe Elliptique *E* forment un groupe *Aut(E).*
Ce groupe dépend de la caractéristique de *K* et de l'invariant modulaire *j(E).*

Définition4 :

Un automorphisme d'une Courbe Elliptique E est un endomorphisme bijectif du groupe abélien E(K).

L'ordre du groupe des automorphismes d'une Courbe Elliptique est un diviseur de 24,

Proposition3 :

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*** $j(E) \neq 0,1728$ ***et carac(K)*** $\neq 2$ ***et*** 3
2) ***4 si*** $j(E) = 1728$ ***et carac(K)*** $\neq 2$ ***et*** 3
3) ***6 si*** $j(E) = 0$ ***et carac(K)*** $\neq 2$ ***et*** 3
4) ***12 si*** $j(E) = 0$ ***ou*** 1728 ***et carac(K)*** $= 3$
5) ***24 si*** $j(E) = 0$ ***ou*** 1728 ***et carac(K)*** $= 2$

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

Preuve de (1) :

Soit une Courbe Elliptique *E* d'équation de Weierstrass :
$E: y^2 = x^3 + a_4x + a_6 \in K[x,y]$,
avec $4a_4^3 + 27a_6^2 \neq 0$ et carac(K) $\neq 2$ et 3.
Et les deux invariants :

$$\Delta(E) = 4a_4^3 + 27a_6^2 \neq 0 \quad \text{et} \quad j(E) = \frac{4.1728a_4^3}{4a_4^3+27a_6^2} \tag{9}$$

Les hypothèses : $j(E) \neq 0,1728$ et $carac(K) \neq 2$ et 3 et la relation (9) impliquent les valeurs :

$$a_4 \neq 0 \quad \text{et} \quad a_6 \neq 0 \tag{10}$$

Les formules d'isomorphismes (2) impliquent l'automorphisme :
$h: E(K) \rightarrow E(K)$ de valeur: $h(x,y) = (u^2x, u^3y)$, pour *u* non nul de *K*
La Courbe Elliptique E' isomorphe à la Courbe Elliptique *E* par l'isomorphisme *h*, a pour équation :
$E': y^2 = x^3 + a'_4x + a'_6$
Avec les relations : $a_4 = u^4a'_4$ et $a_6 = u^6a'_6$.
La relation : $j(E) = j(E')$ implique :

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

les formules d'isomorphisme impliquent les équations :
$a_4 = u^4a_4$ et $a_6 = u^6a_6$, par les propriétés de l'automorphisme *h*
Ces deux équations impliquent : $u^4 = u^6 = 1$ alors $u^2 = 1$
Il en résulte les deux automorphismes :
(x, y) ⟶ *(x, y)* et *(x, y)* ⟶ *(x, - y).*
Alors le groupe *Aut(E)* est d'ordre 2.

Preuve de (2) :

Soit une Courbe Elliptique *E* d'équation de Weierstrass :

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

avec $4a_4^3 + 27a_6^2 \neq 0$ et $carac(K) \neq 2$ et 3.

Et les deux invariants :

$$\Delta(E) = 4a_4^3 + 27a_6^2 \neq 0 \quad \text{et} \quad j(E) = \frac{4.1728a_4^3}{4a_4^3+27a_6^2} \tag{11}$$

Les hypothèses : $j(E) = 1728$ et $carac(K) \neq 2$ et 3 et la formule (11) impliquent les valeurs :

$$a_6 = 0 \quad \text{et} \quad a_4 \neq 0 \tag{12}$$

La formule (12) et les relations $a_4 = u^4a'_4$ et $a_6 = u^6a'_6$ impliquent :

$u^4 = \frac{a_4}{a'_4} \neq 0$ et $a_6 = a'_6 = 0$.

Les formules d'isomorphismes (2) impliquent l'automorphisme :

$h: E(K) \rightarrow E(K)$ de valeur: $h(x,y) = (u^2x, u^3y)$, pour *u* non nul de *K*

La Courbe Elliptique E' isomorphe à la Courbe Elliptique *E* par l'isomorphisme *h*, a pour équation :

$E': y'^2 = x^3 + a'_4x$.

Les formules d'isomorphisme impliquent l équation :

$a_4 = u^4a_4$, par les propriétés de l'automorphisme *h*, qui implique: $u^4 = 1$. Cette équation admet quatre solutions $u = \pm 1, \pm i$

Il en résulte les quatre automorphismes :

(x, y) ⟶ *(x, y)* et *(x, y)* ⟶ *(x, - y)* et *(x, y)* ⟶ *(- x,- iy)* et *(x, y)* ⟶ *(- x, iy).*

Alors le groupe *Aut(E)* est d'ordre 4.

Preuve de (3) :

Soit une Courbe Elliptique *E* d'équation de Weierstrass :

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

avec $4a_4^3 + 27a_6^2 \neq 0$ et $carac(K) \neq 2$ et 3.

Et les deux invariants :

$$\Delta(E) = 4a_4^3 + 27a_6^2 \neq 0 \quad \text{et} \quad j(E) = \frac{4.1728a_4^3}{4a_4^3+27a_6^2} \tag{13}$$

Les hypothèses : $j(E) = 0$ et $carac(K) \neq 2$ et 3 et la formule (13) impliquent les valeurs :

$$a_4 = 0 \quad \text{et} \quad a_6 \neq 0 \tag{14}$$

La formule (14) et les relations $a_4 = u^4a'_4$ et $a_6 = u^6a'_6$ impliquent :

$a_4 = a'_4 = 0$ et $u^6 = \frac{a_6}{a'_6} \neq 0$

Les formules d'isomorphismes (2) impliquent l'automorphisme :

$h: E(K) \rightarrow E(K)$ de valeur : $h(x,y) = (u^2x, u^3y)$, pour *u* non nul de *K*

La Courbe Elliptique E' isomorphe a la Courbe Elliptique *E* par l'isomorphisme *h*, a pour équation :

$E': y^2 = x^3 + a'_6$

Les formules d'isomorphisme impliquent l équation :

$a_6 = u^6a_6$, par les propriétés de l'automorphisme *h*, qui implique: $u^6 = 1$. Cette équation admet six racines : $u = \pm 1, \pm j, \pm j^2$, ou $j = \exp(\frac{2i\pi}{3})$ et $j^3 = 1$

Il en résulte les six automorphismes :

(x, y) ⟶ *(x, y),* *(x, y)* ⟶ *(x, - y),* *(x, y)* ⟶ *(jx, y),* *(x, y)* ⟶ *(jx, -y),*

(x, y) ⟶ *(j^2x, y)* et *(x, y)* ⟶ *(j^2x,- y)*

Alors le groupe *Aut (E)* est d'ordre 6.

Preuve de (4) :

Les hypothèses : $j(E) = 0$ ou $j(E) = 1728$ et $carac(K) = 3$ impliquent l'équation de Weierstrass : $E: y^2 = x^3 + a_4x + a_6 \in K[x, y]$.

Considérons l'automorphisme du groupe abélien *E(K)* de la forme :

$h: E(K) \rightarrow E(K)$ de valeurs : $h(x, y) = (u^2x + r,\ u^3y)$

Les formules d'isomorphismes (2) impliquent les valeurs:

$u^4 = \frac{a_4}{a'_4}$ et $r^3 + ra_4 + a_6 - u^6a'_6 = 0$

L'automorphisme h implique les valeurs :

$a_4 = a'_4$ et $a_6 = a'_6$

Il en résulte le système :

$$\begin{cases} u^4 = 1 \\ r^3 + ra_4 + (1 - u^2)a_6 = 0 \end{cases} \quad (15)$$

Cela implique douze automorphismes de la Courbe *E*.

Les quatre valeurs : $u = \pm 1, \pm i$, et les trois valeurs de *r* sont les racines d'équation (15) :

$r = r_1, r_2, r_3$

Il en résulte les douze automorphismes :

$(x, y) \longrightarrow (x+r_1, y)$; $(x, y) \longrightarrow (x+r_2, y)$; $(x, y) \longrightarrow (x+r_3, y)$; $(x, y) \longrightarrow (x+r_1, -y)$;

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

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

Il en résulte : le groupe *Aut(E)* est d'ordre 12.

Preuve de (5) :

Les hypothèses : $carac(K) = 2$, et $j(E) = 0$ ou $j(E) = 1728$ impliquent l'équation de Weierstrass : $E: y^2 + a_3y = x^3 + a_4x + a_6 \in K[x, y]$,

Considérons l'automorphisme du groupe *E(K)* de la forme :

$h: E(K) \rightarrow E(K)$ de valeur : $h(x, y) = (u^2x + t'^2,\ u^3y + t'u^2x + s')$ (16)

et $E': y^2 + a'_3y = x^3 + a'_4x + a'_6$

Les relations entre a_i et a'_i impliquent les trois équations :

$$\begin{cases} u^3 = 1 = \frac{a_3}{a'_3} \\ t'^4 + a_3t' + (1 - u)a_4 = 0 \\ s'^2 + a_3s' + t'^6 + a_4t'^2 = 0 \end{cases} \quad (17)$$

Le nombre des automorphismes (16) est égal au nombre des triplet (u, t',s') solutions du système (17) qui admet 24 solutions : 3 valeurs u, 4 valeurs de t', 2 valeurs de s'

Il en résulte : le groupe *Aut(E)* est d'ordre 24.

□

5-Application à la famille E(s, t) :

Soit la Courbe Elliptique $E(s,t)$ d'équation de Weierstrass :

$$E(s,t): \quad y^2 + 2sxy + 2ty = x^3 + stx^2 - stx - t^2 \in \mathbb{Q}[x,y]$$

Avec :

$st \neq 0 \; et \; t \neq t_i (i = 1,2) \; où \; t_1 = \frac{1}{s}\left(2 - s^2 - 2\sqrt{1-s^2}\right), et \; t_2 = \frac{1}{s}\left(2 - s^2 + 2\sqrt{1-s^2}\right)$;

x, y sont des éléments d'une clôture algébrique $\mathbb{Q}_{al}$ de $\mathbb{Q}$.

a) **Calcul de la transformée $E'(s,t)$ de la Courbe Elliptique $E(s,t)$:**

Soit $E'(s,t)$ la transformée de la Courbe Elliptique $E(s,t)$ par le changement linéaire de variables :

$$\begin{cases} x = u^2 x' + r & (1) \\ y = u^3 y' + s' u^2 x' + t' & (2) \end{cases}$$ Avec, $u \neq 0$; r, s' et t' des éléments de $\mathbb{Q}$.

Par la proposition1, les Courbes Elliptiques $E(s,t) \; et \; E'(s,t)$ sont isomorphes, avec les calculs, nous obtenons l'équation:

$$\begin{aligned} E'(s,t) : \; & u^6 y'^2 + 2u^5(s'+s)x'y' + 2u^3(t' + rs + t)y' \\ & = u^6 x'^3 + u^4\left(3r + st - s'^2 - 2s's\right)x'^2 \\ & + u^2(3r^2 + 2rst - st - 2s't' - 2t's - 2s'rs - 2s't)x' \\ & + (r^3 + str^2 - rst - t^2 - t'^2 - 2t'rs - 2t't); \end{aligned}$$

pour les conditions :

$$st \neq 0 \text{ et } t \neq t_i (i = 1,2) \text{ où } t_1 = \frac{1}{s}\left(2 - s^2 - 2\sqrt{1-s^2}\right), \text{et } t_2 = \frac{1}{s}\left(2 - s^2 + 2\sqrt{1-s^2}\right)$$

b) **Relations entre les invariants de la Courbe Elliptique $E(s,t)$ et de sa transformée $E'(s,t)$.**

Le corollaire de la proposition1 implique les relations entre les invariants de $E(s,t) \; et \; ceux \; de \; E'(s,t)$:

b.1) Relations entre les coefficients $a_i \; et \; a_i'$:

$$ua_1' = 2s + 2s'$$
$$u^2 a_2' = st - 2s's + 3r - s'^2$$
$$u^3 a_3' = 2t + 2rs + 2t'$$
$$u^4 a_4' = -st - 2s't + 2rst - 2t's - 2s'rs + 3r^2 - 2s't'$$
$$u^6 a_6' = -t^2 - rst + r^2 st - 2t't - 2t'rs - t'^2 + r^3$$

b.2) Relations entre les invariants b_{2i} et b_{2i}' :

$$u^2 b_2' = 4s(s+t) + 12r$$
$$u^4 b_4' = 2st + 4rs(s+t) + 6r^2$$
$$u^6 b_6' = 4rst + 4r^2 s(s+t) + 4r^3$$
$$u^8 b_8' = -(st)^2 + 6r^2 st + 4r^3 st(s+t) + 3r^4$$

b.3) Relations entre les invariants $c_{2i} \; et \; c_{2i}'$:

$$u^4 c_4' = 16s[s(s+t)^2 - 3t]$$
$$u^6 c_6' = 2^5 s^2 (s+t)[9t - 2s(s+t)^2]$$

b.4) Relations entre les discriminants $\Delta(E(s,t))$ et $\Delta\left(E'(s,t)\right)$:

$$u^{12}\Delta\left(E'(s,t)\right) = 16s^3t^2[s(s+t)^2 - 4t]$$

b.5) Relations entre les invariants modulaires $j(E(s,t))$ et $j(E'(s,t))$:

$$j\left(E'(s,t)\right) = \frac{16^2[s(s+t)^2 - 3t]^3}{t^2\,[s(s+t)^2 - 4t]}$$

b.6) Relations entre les éléments neutres 0_E et $0_{E'}$ des deux courbes $E(s,t)$ et $E'(s,t)$

Les points neutres sont dans la même classe du plan projectif $\mathbb{P}^2$: $0_E = 0_{E'} = (0,1,0)$

c) Détermination de l'ordre du groupe $Aut\,(E(s,t))$ des automorphismes de $E(s,t)$

$j(E(s,t))$ étant l'invariant modulaire de la Courbe Elliptique $E(s,t)$.

Comme $carac(\mathbb{Q}) = 0 \neq 2,3$ et par application de la proposition 3, nous obtenons trois cas possibles pour l'ordre du groupe $Aut\,(E(s,t))$ des automorphismes de $E(s,t)$:

c.1) 1er Cas: $j(E(s,t)) \neq 0, et\ 1728$:

$j(E(s,t)) \neq 0$ Si et seulement si : $\begin{cases} t \neq \frac{3-2s^2+\sqrt{9-12s^2}}{2s} \\ t \neq \frac{3-2s^2-\sqrt{9-12s^2}}{2s} \end{cases}$ avec $s \in \left[-\frac{\sqrt{3}}{2}, \frac{\sqrt{3}}{2}\right] - \{0\}$

Et $j(E(s,t)) \neq 1728$ si et seulement si :

$4s[s^3(s+t)^6 - 9s^2(s+t)^4t + 27t^2s(s+t)^2 - 27t^3] - 27t^2s(s+t)^2 + 108t^3 \neq 0$

C'est un polynôme de dixième degré en s et de sixième degré en t.

Alors $Aut\,(E(s,t))$ est un groupe d'ordre 2.

c.2) 2ème Cas: : $j(E(s,t)) = 1728\ si, et\ seulement, si$:

$4s[s^3(s+t)^6 - 9s^2(s+t)^4t + 27t^2s(s+t)^2 - 27t^3] - 27t^2s(s+t)^2 + 108t^3 = 0$

C'est un polynôme de dixième degré en s et de sixième degré en t, alors $Aut\,(E(s,t))$ est un groupe d'ordre 4.

c.3) 3ème Cas: $j(E(s,t)) = 0$ si et seulement, si $\begin{cases} t = \frac{3-2s^2+\sqrt{9-12s^2}}{2s} \\ t = \frac{3-2s^2-\sqrt{9-12s^2}}{2s} \end{cases}$ avec

$s \in \left[-\frac{\sqrt{3}}{2}, \frac{\sqrt{3}}{2}\right] - \{0\}$, alors $Aut\,(E(s,t))$ est un groupe d'ordre 6.

Conclusion :

J'ai traité quelques aspects des Courbes Elliptiques et j'ai appliqué ces résultats à la famille $E(s,t)$. Je me propose d'étudier plus tard d'autres aspects de la théorie : isogénies de Courbes Elliptiques, hauteurs et rangs de Courbes Elliptiques, séries *L (E, s)* de Dirichlet -Hasse, groupes *WL(E/K)* de Châtelet -Weil, groupes $S_m(E/K)$ de Selmer, groupes *Ш(E/K)* de Chafarevich-Tate.

REFERENCES

1) **J.W.S CASSELS** : « Diophantine Equations with Special References to Elliptic Curves » Journal London Mathematical Society 41(1965-1966) 193-291.

2) **Robin HARTSHORNE** : « Algebraic Geometry », GTM 52-Springer (1983) Classification: 14 A10 -14Fxx- 14Hxx- 14Lxx.

3) **Helmut HASSE**: « Number Theory » -Springer (1980), Berlin.

4) **D. HUSEMOLLER**: « Elliptic Curves», Graduate tests in Mathematics n°111 Springer (1988).

5) **A.W KNAPP**: « Elliptic Curves», University Press n° 40 New York- USA- (1992).

6) **Neal KOBLITZ**: « Elliptic Curves», Introduction to Elliptic Curves and Modular Forms $2^{ème}$ Ed , Graduate tests in Mathematics n° 97- Springer Verlag (1984).

7) **KOSTRIKIN** : « Introduction à l'algèbre », Ed- Mir- Moscou, (1986).

8) **Serre LANG**: (1) « Algebra », 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.

9) **J.S. MILNE**: « Elliptic Curves – Curve Notes» University of Michigan (1996).

10) **Jean Pierre SERRE**: « Propriétés Galoisiennes des points d'ordre fini de Courbes Elliptiques» Inventiones Mathématicae n° 15 (1972) p 259-331.

11) **I-R SHAFAREVICH** : (1) « Basic Algebraic Geometry », Springer Verlag (1977)
(2) « Algebraic I », Moscou (1986), Springer Verlag (1987)
Classification: AMS = -12- xx, 20- xx.

12) **G. SHIMURA** : « Introduction to the Arithmetic Theory of Automorphic Function », Princeton University Press (1971).

13) **Joseph H- SILVERMAN**: « The Arithmetic of Elliptic Curves », GMT 106 - Springer (1986).
Classification: AMS = 1401, 14G 99, 14H 05, 14K 15.

14) **John TATE**: « The Arithmetic of Elliptic Curves », Inventiones Mathématicae N° 23 (1974) p 179-206.

15) **Mohamed ZITOUNI**: « Géométrie Arithmétique et Algorithmique des Courbes Elliptiques », OPU- 2007.