N° d'Ordre :23/2008 – M/MT

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université des Sciences et de la Technologie
Houari Boumediene
Faculté des Mathématiques

جامعة هواري بومدين
للعلوم والتكنولوجيا
U S T H B

Mémoire

Présenté pour l'obtention du diplôme de MAGISTER
En : Mathématique
Spécialité : Algèbre et Théorie des Nombres

Par :
M^{me} : LAID Fadhila

Sujet

Points de Heegner et Famille de courbes elliptiques

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

Soutenu publiquement le 16/04/2008 devant le jury
Composé de :

Mr M. AIDER, Professeur, USTHB	**Président**
Mr M. ZITOUNI, Professeur, USTHB	**Directeur de Thèse**
Mr M.O. HERNANE, Maitre de Conférence, USTHB	**Examinateur**
Melle L. ALOUACHE, Chargée de Cours, U.M.B.B	**Examinateur**

TABLE DES MATIERES

DEDICACES

- **A mon père et à ma mère**
- **A mon mari et mes enfants**
et aux autres parents et alliés

REMERCIEMENTS

C’est avec une très grande joie que j’exprime ici ma gratitude à toutes les personnes qui ont contribué de façon directe ou indirecte à l’élaboration de ma thèse.
Tout d’abord, je remercie mon directeur de thèse, le Professeur ZITOUNI Mohamed. Il m’a laissé une grande liberté dans mes activités de recherche. Je suis sensible à ses nombreux conseils et commentaires au cours de la préparation et de la rédaction de ma thèse.
J’ai été enchantée de la présence de Mr HERNANE parmi les membres du jury, je l’en remercie chaleureusement.
Je remercie aussi Melle Leila ALOUACHE d’avoir accepté d’être parmi les membres du jury.
Je remercie aussi le Professeur Meziane AIDER et je suis flattée qu’il soit président du jury de ma thèse.
Je remercie mon compagnon de tous les jours, mon mari qui m’a encouragé de façon permanente.

Introduction

L'étude des Courbes Elliptiques nécessite des connaissances en Théorie des Nombres, en Géométrie Algébrique, en Analyse Complexe.
Il existe de nombreux ouvrages traitant les Courbes Elliptiques : J.W.CASSELS : " Diophantine Equations with Special Reference to Elliptic Curves " [4] , Goro SHIMURA : " Introduction to the Arithmetic Theory of Automorphic Functions " [25], Joseph H..SILVERMAN: " The Arithmetic of Elliptic Curves " [26], Neal KOBLITZ :" Introduction to Elliptic Curves and Modular Formes" [15], HUSEMOLLER: "Elliptic Curves [12], A.W.KNAPP: "Elliptic Curves " [14].

Dans le chapitre I, j'ai étudié quelques aspects de la géométrie des Courbes Elliptiques. Dans l'ensemble des courbes algébriques planes il y a des cubiques particulières : les cubiques de Weierstrass :

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

Des invariants sont obtenus avec des changements convenables des variables.
J'ai obtenu une classification des ces cubiques à l'aide des 2 invariants Δ (E) et c_4 (E). J'ai appliqué ces résultats à la famille des Cubiques de Weierstrass E (t) .

Dans le chapitre II, j'ai étudié la structure algébrique de l'ensemble E (K) des points K–rationnels d'une cubique E de Weierstrass. C'est un groupe additif abélien de type fini de loi basée sur la règle géométrique des " 3 points colinéaires ". Ce groupe E(K) est le groupe de Mordell_Weil de E. J'ai décrit les isomorphismes et les isogénies, spécifiques aux Courbes Elliptiques.

Dans le chapitre III, j'ai étudié les notions de groupe modulaire, sous groupe modulaire de congruence, fonctions et formes Modulaires en utilisant les résultats de l'analyse complexe. En suivant Heegner et Birch, j'ai exposé la construction des points de Heegner avec une courbe modulaire X_0 (N), le corps quadratique imaginaire $\mathbb{Q}(\sqrt{-N})$ et une équation modulaire $\Delta(\omega) = A\,\omega^2 + B\,\omega + C$ de discriminant Δ (E) < 0.
Ces points de Heegner ont été l'objet de nombreux travaux que nous examinerons ultérieurement.

Chapitre I : Géométrie des Courbes Elliptiques

Les notions utilisées se trouvent dans des ouvrages de Géométrie Algébrique « Algebraic Geometry » de R.Hartshorne ;,[11], « BASIC Algebraic Geometry » de I.R. Shafarevich, [24], « Algebraic Geometry : First Course » de Harris (G.T.M 133), « Sur les courbes algébriques et les variétés qui s'en déduisent » de A.Weil ….

Nous décrivons successivement et brièvement les espaces affines et les variétés affines, les espaces projectifs et les variétés projectives, les variétés de groupe et les variétés abéliennes

1 Espace affine; Espace projectif

1.1 Espace affine $\mathbb{A}^n$ (K) sur un corps K

Définition1 :
Un n-espace affine sur un corps commutatif K est l'ensemble des n-uplets a_i de K

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

Le système a est un point de l'espace affine. Cet espace est de dimension n ; pour n = 2 cet espace est un plan.

A cet espace affine on associe l'anneau K [$X_1 \ldots X_n$] des polynômes à n indéterminées sur le corps K.

A toute famille { $f_1 , f_2 , \ldots f_d$} de polynômes de cet anneau on associe l 'ensemble Z ($f_1 , \ldots f_d$) des zéros de ces polynômes dans une clôture algébrique K_{alg} de K.

Définition2 :
Un sous ensemble X de l'espace affine $\mathbb{A}^n$ (K) est algébrique si ses points sont les zéros d'une famille de polynômes $f_i \in K [X_1 ; \ldots\ldots X_n]$

$$X = Z(f_1 , \ldots f_d) = \{ a \in \mathbb{A}^n (K) ; f_i (a) = 0 \quad i = 1,2 ,\ldots d \}$$

Les ensembles algébriques permettent de définir une topologie particulière sur le n-espace affine.

Définition3 :
La topologie de Zariski sur un n-espace affine $\mathbb{A}^n$ (K) est définie avec les ensembles algébriques comme sous ensembles fermés et leurs complémentaires comme des ouverts.

L'ensemble vide et le n-espace affine sont ouverts et fermés à la fois ; ce sont les seules parties à posséder cette propriété.
Le n-espace affine $\mathbb{A}^n$ (K) devient un espace topologique avec la topologie de Zariski .

Définition 4 :
Une partie Y de l'espace topologique $\mathbb{A}^n$ (K) est irréductible si Y n'est pas la réunion de deux sous ensembles fermés non vides disjoints.

1.2 – Variétés algébriques affines

Définition 5 :
1) Une variété algébrique affine est un sous espace irréductible et fermé d'un espace affine $\mathbb{A}^n$ (K) muni de la topologie de Zariski.
2) Une variété quasi affine est un sous ensemble ouvert d'une variété affine.

Dans la suite toutes les variétés algébriques seront désignées par le terme « variété ».

Exemple : le n-espace affine $\mathbb{A}^n$ *(K)* , muni de la topologie de Zariski est fermé et irréductible ; c'est donc une variété affine.

1.3 – Variétés projectives, variétés abéliennes

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).

Considérons dans une variété affine $\mathbb{A}^{n+1}$ *(K)* la relation binaire *Rel* définie par ;

$(a_1 , a_2 , \ldots\ldots a_{n+1})$ *Rel* $(b_1 , b_2 , \ldots\ldots b_{n+1})$ si seulement si
$b_1 = \lambda a_1 , \ldots\ldots.., \quad b_{n+1} = \lambda a_{n+1}$ pour un élément λ non nul du corps K

Cette relation Rel satisfait les 3 axiomes d'une relation d'équivalence; réflexibilité, symétrie et transitivité.

1.4 Espace projectif $\mathbb{P}^n$ (K).

Définition 6 :
Le n-espace projectif $\mathbb{P}^n$ (K). est le quotient de l'espace affine $\mathbb{A}^{n+1}$ (K) privé du point 0 = (0,.. , 0) par la relation d'équivalence Rel
$\mathbb{P}^n$ *(K) = { $\mathbb{A}^n$ (K) - {0}} / Rel*

Donc les éléments de l'espace projectif $\mathbb{P}^n$ (K) sont des classes modulo la relation Rel .

Exemple :
L'espace projectif $\mathbb{P}^2(\mathbb{R}) = \mathbb{A}^3 - \{0\} = \{ cl(0,1,0), cl(0,1,1), \ldots , cl(x,y,z) \}$

La topologie de Zariski s'applique aux espaces projectifs.

Définition 7:
1) *Une variété projective est un sous ensemble algébrique irréductible de l'espace projectif $\mathbb{P}^n$ (K) muni de la topologie de Zariski*
2) *Une variété quasi projective est un sous ensemble ouvert d'une variété projective*
3) *Un hyperplan d'un espace projectif $\mathbb{P}^n$ (K) est l'ensemble des zéros d'un polynôme homogène linéaire à n+1 –indéterminées.*

Exemple
Le polynôme homogène de degré 3

$$f(X,Y,Z) = Y^2 Z + 2XYZ + 3YZ^2 - X^3 + 4X^2Z - 5X Z^2 + 6 Z^3 \in \mathbb{P}^2(\mathbb{R})$$

Les zéros (a, b, c) de ce polynôme forment une variété projective de dimension 1

Ce polynôme admet le zéro (0,1,0) = O_E ; ce zéro est représenté par le point à l'infini de la cubique ; il est déterminé par la direction de l'axe Oy.

Il y a une autre relation entre les espaces $\mathbb{A}^n(K)$ et $\mathbb{P}^n(K)$.

Pour n =2, nous établissons les formules de passage de l'espace affine $\mathbb{A}^2(\mathbb{R})$ à l'espace projectif $\mathbb{P}^2(\mathbb{R})$.

Soit un polynôme f(x,y) de degré d ⩾ 1dans l'espace affine $\mathbb{A}^2(\mathbb{R})$.
Pour obtenir l'image de f (x,y) dans l'espace projectif $\mathbb{P}^2(\mathbb{R})$ nous faisons 2 opérations.
Le changement x =X/Z , y=Y/Z transforme f(x,y) en $f(\frac{X}{Z}, \frac{Y}{Z})$; (1)
nous multiplions ce polynôme par Z^d ; nous obtenons un polynôme homogène

$$Z^d f(\frac{X}{Z}, \frac{Y}{Z}) = g(X, Y, Z)$$

Exemple :
$f(x,y) = x^4 - 3x^2y^3 + 5x - y^2 + 2$: polynôme affine de degré 5 ;
Appliquons les 2 opérations

$$Z^5 ((\frac{X}{Z})^4 + 3\frac{X^2 Y^3}{Z^5} + 5\frac{X}{Z} - \frac{Y^2}{Z^2} + 2) = X^4Z - 3X^2 Y^3 + 5 X Z^4 - Y^2Z^3 + 2 Z^5 = g(X, Y, Z) .$$

C'est un polynôme homogène de degré 5

Pour transformer un polynôme h(x,y,z) homogène de degré d du plan projectif $\mathbb{P}^2(\mathbb{R})$ en polynôme affine nous utilisons le changement

$$x = X ; y = Y ; z = 1$$

Alors h (x,y,z) = h (X,Y,1) = u (X , Y)

Exemple
$h(x,y,z) = x^2 y^3 z^2 + 5 x^3 y^4 + 6 x y^5 z + x^3 y^2 z^2 - x y z^5 + 4 z^7$, polynôme homogène de degré 7 de $\mathbb{P}^2$.

Le changement x =X , y = Y , z = 1 le transforme en polynôme affine :
$h(X,Y, 1) = X^2Y^3 + 5 X^3Y^4 + 6 X Y^5 + X^3 Y^2 - X Y + 4$, polynôme affine de degré 7 du plan affine de $\mathbb{A}^2$.

Considérons 2 nouveaux types de variétés algébriques : les variétés de groupes et les variétés abéliennes.

Définition 8 :
Une variété de groupe est une variété X munie d'un morphisme

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

qui satisfait deux conditions :

1) *l'ensemble des points de X est muni d'une structure de groupe.*
2) *l'application inverse* $a \longrightarrow a^{-1}$ *est un morphisme de variété.*

Exemple
Le groupe additif formé par la variété X = $\mathbb{A}^n$ (K) munie du morphisme u (a,b) = a + b est une variété de groupe .
Une variété de groupe devient une variété abélienne avec quelques conditions supplémentaires.

Définition 9 :
Une variété abélienne est une variété de groupe projective et irréductible.

Il y a des variétés abéliennes construites avec le théorème de Chevalley :
"tout groupe algébrique G possède un sous groupe normal N affine tel que le groupe quotient G/N soit une variété abélienne " [11]
Il en résulte que toute variété abélienne est commutative.

Selon Shafarevich [24] les seuls exemples de variétés abéliennes que l'on a trouvé sont les Courbes Elliptiques.

2 - Cubiques de Weierstrass

Une cubique plane X a une équation algébrique de la forme

$$f(x, y) = d_1y^3 + d_2 x^3 + d_3y^2x + d_4yx^2 + d_5y^2 + d_6x^2 + d_7xy + d_8y + d_9x + d_{10} \in \mathbb{R}[x, y] \qquad (1)$$

$f(x,y) = 0,$

Les 10 coefficients d_1 , d_2 ,…., d_{10} sont des éléments du corps $\mathbb{R}$ des nombres réels avec deux des $d_i \neq 0$ au moins pour i=1,...,4.

Les variables x , y sont des éléments d'une clôture algébrique du corps $\mathbb{R}$; ce sont les coordonnées affines d'un point P du plan affine de dimension 2.

L'équation (1) ne change pas lorsqu'on remplace le corps $\mathbb{R}$ par un corps commutatif K.

Dans l'ensemble de ces polynômes il y a les polynômes de la forme

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

où K est un corps global, local ou fini.
x et y sont des éléments d'une clôture algébrique du corps K

Définition 10 :
1) Une cubique de Weierstrass *est une cubique plane irréductible d'équation (2)* **.**
2) Une cubique de Weierstrass non singulière est une Courbe Elliptique.

3 - Transformations de l'équation de Weierstrass

Dans l'équation (2) éliminons les monômes en xy et en y par le changement de variable linéaire :

$$(x , y) \longrightarrow (X , \frac{1}{2}(Y - a_1 X - a_3)) \text{ , pour carac } (K) \neq 2 \qquad (3)$$

Nous obtenons l'équation de Weierstrass :

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

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

$$b_2 = 4 a_2 + a_1^2 , \quad b_4 = 2 a_4 + a_1 a_3 \text{ et } b_6 = 4 a_6 + a_3^2 \qquad (5)$$

Dans l'équation (4) éliminons les monômes en x^2 et le coefficient 4 par le changement de variable linéaire

$$(X , Y) \longmapsto (\frac{x - 3 b_2}{36} , \frac{y}{108}) \text{ pour carac } (K) \neq 2, 3 \qquad (6)$$

Nous obtenons l'équation de Weierstrass :

$$E_2 : y^2 = x^3 - 27c_4 x - 54c_6 \in K [x , y] \qquad (7)$$

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

$$c_4 = b_2^2 - 24b_4, \text{ et } c_6 = - b_2^3 + 36 b_2 b_4 - 216 b_6 . \qquad (8)$$

Il existe d'autres modèles d'équations de Weierstrass

La cubique de Weierstrass

$E_3 : y^2 = x^3 + A x + B \in \mathbb{Z} (x, y)$, où $a_1 = a_2 = a_3 = 0$; $a_4 = A$ et $a_6 = B$

La cubique de Legendre :

$E_4 : y^2 = x (x -1)(x-t) \in K [x , y]$ pour $t \neq 1, 0$ où $a_1 = a_3 = a_6 = 0$; $a_2 = - (1+t)$ et $a_4 = t$

La cubique de Deuring

$E_5 : y^2 + t xy + y = x^3$ sur un corps de caractéristique $\neq 3$; $t^3 \neq 27$, où $a_1 = t$, $a_3 = 1$ et $a_2 = a_4 = a_6 = 0$

La cubique de Kubert

$E_6 = y^2 + (1 - s) xy - t y = x^3 - t x^2 \in K[x, y]$ où $a_1 = (1 - s)$; $a_2 = -t = a_3$, $a_4 = a_6 = 0$

La cubique de Tate

$E_7 : y^2 + xy = x^3 - ax - b \in \mathbb{C}[x, y]$

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

pour $n \geqslant 1$

$q = \exp(2\Pi iz)$; $z \in \mathbb{C}$ $z = x + iy$; $y > 0$

Une cubique de Weierstrass E possède plusieurs invariants : le discriminant Δ (E), l'invariant modulaire j(E), l'invariant différentiel ω (E), le conducteur N(E) , la série L -de Dirichlet – Hasse, les coefficients b_2, b_4 , b_6 , c_4 et, c_6 ,le régulateur R(E) etc.… Ces invariants servent à la classification des cubiques de Weierstrass ; ce sont des objets mathématiques qui varient.

4 - Invariants d'une cubique de Weierstrass

Soit une cubique de Weierstrass :

$E : y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \in K[x, y]$.
K = corps global , local ou fini

Définition 11
1) Le discriminant d'une cubique de Weierstrass *E est le polynôme " homogène de degré 12 " de l'anneau* $\mathbb{Z}[b_2, b_4, b_6, b_8]$ *égal à*

$\Delta(E) = 9 b_2 b_4 b_6 - 27 b_6^2 - 8 b_4^3 - b_2^2 b_8 \; ; \; 4 b_8 = b_2 b_6 - b_4^2$ *pour carac (K)* $\neq 2, 3$ (9)

2) L'invariant modulaire d'une cubique de Weierstrass est un élément du corps K égal à :

$j(E) = c_4^3 / \Delta(E)$) (10)

Il existe un invariant lié à la forme différentielle df (x , y) .

Définition 12
*L'invariant différentiel d'une cubique de We*ierstrass *:*

$f(x,y) = y^2 + a_1 x y + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6$ (11)

est égal à l'élément différentiel

$$\omega(E) = \frac{dx}{2y + a_1 x + a_3} = \frac{dy}{3x^2 + 2a_2 x + a_4 - a_1 y} \quad (12)$$

Cet invariant provient de la différentielle de la fonction polynôme $df = f_x' \, dx + f_y' \, dy$

Application à la famille E (t) de Cubique de Weierstrass

$E(t) : y^2 + t xy + t y = x^3 + 2t x \in \mathbb{Q}[x, y]$
$a_1 = a_3 = t$, $a_2 = a_6 = 0$; $a_4 = 2t$

Calcul des invariants $b_2 = t^2$, $b_4 = t^2 + 4t$, $b_6 = t^2$, $b_8 = -2t^3 - 4t^2$
Le discriminant $\Delta(E) = t^3(2t^4 + 5t^3 - 60t^2 - 411t - 512)$
L'invariant $c_4 = t^4 - 24t^2 - 96t$
L'invariant $c_6 = -t^6 + 36t^4 + 144t^3 - 216t^2$

L'invariant modulaire $j(E) = \dfrac{(t^3 - 24t^2 - 96)^3}{2t^4 + 5t^3 - 60t^2 - 357t - 512}$

L'invariant différentiel $\omega(E) = \dfrac{dx}{2y + tx + t} = \dfrac{dy}{3x^2 + 2t - ty}$

5- Discriminant d'un polynôme et résultant de deux polynômes

Tout polynôme f(x) de degré n admet des fonctions symétriques de ses racines

Définition 13 : *d'après [5]*
Le discriminant d'un polynôme de degré $n \geqslant 1$

$$f(x) = d_0 x^n + d_1 x^{n-1} + \ldots\ldots\ldots\ldots + d_n \in \mathbb{R}[x] \qquad (13)$$
$$= d_0 \Pi(x - e_i) \quad , \quad 1 \leqslant i \leqslant n \ ,$$

est une fonction symétrique de ses racines $e_1, e_2, \ldots\ldots e_n$

$$dis(f) = d_0^{2n-2} \Pi (e_i - e_j)^2 \ .$$
$$1 \leqslant i < j \leqslant n$$

Il existe une relation entre les discriminants d'un polynôme f(x) et d'une Courbe Elliptique $E : y^2 = f(x)$.

Proposition 1
Soit une Courbe Elliptique E d'équation de Weierstrass

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

et les discriminants dis (f) de f et $\Delta(E)$ *de E.*

1) *lorsque* $f(x) = 4x^3 + b_2 x^2 + 2 b_4 x + b_6$ *alors*
   $dis(f) = 16 \Delta(E)$;
2) *lorsque* $f(x) = x^3 + Ax + B$ *; alors*
   $\Delta(E) = 16\, dis(f)$;

Preuve

1) Soit une Courbe Elliptique E d'équation de Weierstrass
   $E : y^2 = f(x) = d_0 x^3 + d_1 x^2 + d_2 x + d_3 \in \mathbb{R}[x, y]$

   D'après Lang, [8-1] , le discriminant de ce polynôme est égal à
   $dis(f) = 18 d_0 d_1 d_2 d_3 + d_1^2 d_2^2 - 4 d_1^3 d_3 - 27 d_0^2 d_3^2 - 4 d_0 d_2^3$

   Le discriminant de la Courbe Elliptique E
   $E : y^2 = 4x^3 + b_2 x^2 + 2 b_4 x + b_6 \in \mathbb{R}[x, y]$
   est égal à
   $\Delta(E) = 9 b_2 b_4 b_6 - 8 b_4^3 - 27 b_6^2 - b_2^2 b_8$ avec $4 b_8 = b_2 b_6 - b_4^2$

Pour $d_0 = 4$, $d_1 = b_2$, $d_2 = 2\, b_2$ et $d_3 = b_6$, nous obtenons
$\text{dis}\, f(x) = 16\ \Delta(E)$.

2) Soit une Courbe Elliptique E d'équation de Weierstrass
$E : y^2 = x^3 + Ax + B = f(x) \in \mathbb{R}[x]$, avec $4A^3 + 27B^2 \neq 0$

D'après Lang , [18], le discriminant de f(x) est égal à
$\text{disf} = -4A^3 - 27B^2$

Le discriminant de la Courbe Elliptique E est égal à :
$\Delta(E) = -16(4A^3 + 27B^2)$;
Il en résulte la relation
$\Delta(E) = 16\ \text{dis}(f)$

□

Il existe une autre méthode de calcul de dis (f) dans [5]

$$\text{dis}(f) = \begin{vmatrix} s_0 & s_1 & s_2 & . & . & . & s_{n-1} \\ s_1 & s_2 & s_3 & . & . & . & s_n \\ s_2 & s_3 & s_4 & . & . & . & s_{n+1} \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ s_{n-1} & s_n & . & . & . & . & s_{2n-2} \end{vmatrix}$$

$f(x) = x^n + d_1 x^{n-1} + d_2 x^{n-2} + \ldots + d_n = \Pi (x - \theta_i)$, $1 \leqslant i \leqslant n$;
où les nombres s_t sont les fonctions symétriques des racines θ_t

$s_t = \sum \theta_t$, $s_0 = n$, $s_1 = -d_1$, $s_2 = d_1^2 - 2\, d_2$, …. ;
$1 \leqslant t \leqslant n$
$s_t = -t\, d_t - d_1\, d_{t-1} - \ldots - d_1$ et $s_t = 0$ pour $t > n$.

Soit 2 polynômes f et g $\in K[x]$.
Les zéros des 2 polynômes f(x) et g(x) sont liés par leur résultant Res (f , g)

Définition 14
Le résultant de 2 polynômes de l'anneau K [x] :
$f(x) = d_0 x^n + d_1 x^{n-1} + \ldots + d_n$ de degré $n \geqslant 1$
$g(x) = r_0 x^s + r_1 x^{s-1} + \ldots + r_s$ de degré $s \geqslant 1$ est le déterminant d'ordre $n + s$

formé de s lignes (d_0 , d_1 ….. , d_n) et n lignes (r_0 …. r_s), la diagonale principale est formée de s termes d_0 et n termes r_s ; les autres termes sont remplacés par des 0 .

$$Res\ (f,g) = \begin{pmatrix} d_0 & d_1 & d_n & 0 & . & . & 0 \\ 0 & d_0 & d_1 & d_n & 0 & . & 0 \\ 0 & . & d_0 & . & . & . & 0 \\ r_0 & r_1 & . & r_s & . & . & 0 \\ 0 & r_0 & r_1 & . & r_s & . & d_n. \\ . & . & . & . & . & . & . \\ 0 & . & . & r_0 & r_1 & . & r_s \end{pmatrix} \begin{matrix} \} \\ \} \\ \} \\ \} \\ \} \\ \} \\ \} \end{matrix} \begin{matrix} s\ lignes \\ \\ \\ \\ n\ lignes \\ \\ \end{matrix}$$

Exemple

Soit 2 polynômes

$f(x) = x^4 + x^3 - 2x^2 + 1$ et $g(x) = x^3 - x^2 + 4x - 1$;

Leur résultant est égal au déterminant d'ordre 7

$$Res\ (f, g) = \begin{bmatrix} 1 & 1 & -2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & -2 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & -2 & 0 & 1 \\ 1 & -2 & 4 & -1 & 0 & 0 & 0 \\ 0 & 1 & -2 & 4 & -1 & 0 & 0 \\ 0 & 0 & 1 & -2 & 4 & -1 & 0 \\ 0 & 0 & 0 & 1 & -2 & 4 & -1 \end{bmatrix}$$

Après calcul, je trouve Res (f, g) = 317

Proposition 2

Le résultant de deux polynômes f(x) et g(x) est une fonction polynomiale homogène des racines $\theta_1, \theta_2, \ldots\ldots\ldots\theta_n$ de f(x) et $\alpha_1, \alpha_2, \ldots\ldots\ldots\alpha_s$ de g (x)

1) $Res(f,g) = d_0^s\, r_0^n \prod_{1 \leqslant i,j \leqslant n} (\theta_i - \alpha_j) = d_0^s \prod_{i=1\ldots n} g(\theta_i)$

$$= (-1)^{ns}\, r_0^n \prod_{j=1,\ldots,s} f(\alpha_j)$$

Il en résulte la relation $Res\ (f,g) = (-1)^{ns}\, Res\ (g, f)$

2) Res (f , g) = 0 si et seulement si f et g ont une racine commune.

Preuve : Serge LANG [18 -1]

□

Corollaire

Le résultant du polynôme produit f(x) g(x) et d'un polynôme h(x) satisfait la relation

$$Res\,(fg, h) = Res\,(f, h)\,Res\,(g, h).$$

□

Dans le cas particulier d'un polynôme f(x) et sa dérivée f'(x), le résultant de ces deux polynômes est déterminé par la

Proposition 3

Soit un polynôme $f(x) = d_0x^n + d_1 x^{n-1} + \ldots + d_n$ *de degré n et sa dérivée f'(x),*

$$f'(x) = nd_0 x^{n-1} + (n-1)d_1x^{n-2} + \ldots + d_{n-1} \text{ pour } n > 1 .$$

Le résultant des polynômes f(x) et f' (x) est égal à

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

Il est lié au discriminant dis (f) de f par la relation

$$Res\,(f, f') = (-1)^{n(n-1)/2} d_0\, dis(f) .$$

Preuve

Soit $f(x) = d_0 x^n + d_1 x^{n-1} + \ldots + d_n$ un polynôme de degré n et sa dérivée f'(x) de degré n -1 .

$f'(x) = nd_0 x^{n-1} + (n-1)d_1 x^{n-2} + \ldots . + d_{n-1}$ de degré n -1 .

Alors d'après la définition du résultant de deux polynômes f (x) et g(x), le résultant de f (x) et de sa dérivée f'(x) est égal à :

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

□

Exemple

f (x) = $x^3 + x^2 + x + 1$; f'(x) = $3x^2 + 2x + 1$; alors le résultant est le déterminant d'ordre 5 égal à

$$Res\,(f, f') = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 3 & 2 & 1 & 0 & 0 \\ 0 & 3 & 2 & 1 & 0 \\ 0 & 0 & 3 & 2 & 1 \end{bmatrix} = -16$$

La relation entre Res (f, f') et dis (f) implique la valeur dis (f) = -16

6 - Classification des cubiques de Weierstrass avec leur discriminant Δ(E) et c_4 (E)

Soit une cubique E de Weierstrass : $E : y^2 = f(x) \in K[x, y]$.

Grâce aux propositions 1,2 et 3 nous pouvons déterminer les cubiques singulières, les cubiques non singulières et le signe des discriminants de f et de la cubique E.

Lorsque Res (f , f') =0 le polynôme f(x) admet une racine double ou triple ; donc la cubique est singulière.

Lorsque Res (f, f') $\neq 0$ le polynôme f(x) admet 3 racines simples ; il en résulte que la cubique est une Courbe Elliptique.

Proposition 4

Soit une cubique de Weierstrass d'équation

$y^2 = f(x) = x^3 + a_2 x^2 + a_4 x + a_6 \in K [x , y]$

de discriminant $\Delta(E)$; alors :

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

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

Soit une cubique E d'équation $y^2 = f(x) = x^3 + a_2 x^2 + a_4 x + a_6$ et de discriminant $\Delta (E) = 0$
Les propositions 1 et 3 impliquent Res (f,f') =0 ; il en résulte que le polynôme f admet une racine double ou triple, donc la cubique E est singulière ; ce n'est pas une Courbe Elliptique .

□

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

Soit E une cubique singulière, donc elle admet un point singulier. Cela implique que le polynôme f(x) admet une racine double ; $f(x) = (x – e)^2 (x – d)$ ou triple ;. $f (x) = = (x – e)^3$
La relation $\Delta(E) = 16$ dis (f) implique que $\Delta (E) = 0$.
□

Preuve de" $\Delta (E) \neq 0$ " implique" E est une Courbe Elliptique "

Soit une cubique E d'équation de Weierstrass :

$$E : y^2 = f (x) \qquad (1)$$

Alors la relation entre le discriminant de f et le discriminant $\Delta (E)$ implique dis (f) $\neq 0$. (2)
La relation entre Res (f, f') , dis (f) et (2) impliquent Res (f, f') $\neq 0$.
Par la proposition 2, le polynôme f (x) et sa dérivée f' (x) n'ont pas de racines communes ;
Il en résulte que le polynôme n'admet que des racines simples. .Donc la cubique E est une Courbe Elliptique .
□

Lorsque la cubique E est singulière elle admet un point singulier S ; ce point est soit un nœud (2 tangentes distinctes en S) , soit un point de rebroussement (2 tangentes confondues en S) .

La nature du point singulier est déterminée par l'invariant $c_4(E)$.

Proposition 5

Soit une cubique de Weierstrass *E d'équation $y^2 = f(x) \in K [x , y]$, de discriminant $\Delta (E)$ et d'invariant $c_4 (E)$*

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

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

Par la proposition 4 l'hypothèse " $\Delta (E) = 0$ " implique que la cubique est singulière ;

Soit S ce point singulier

Prenons un polynôme $f(x) = x^3 - 27c_4 x - 54 c_6 = y^2 \in K [x , y]$

.

En ce point S, la cubique E admet deux tangentes distinctes ou confondues. Les pentes de ces tangentes sont égales à la dérivée y' de y

$$y' = \frac{3 (x^2 - 9 c_4)}{2 x} = \frac{3 g (x)}{2 y}$$

g(x) est un polynôme de degré 2, son discriminant est égal à $dis(g) = 36c_4$
L'hypothèse " $c_4 (E) \neq 0$" implique que E admet en S deux tangentes distinctes ;
Il en résulte que le point S est un nœud .

□

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

Soit E une cubique de Weierstrass qui admet un nœud ; donc E est singulière. Par la proposition 4, son discriminant est égal à $\Delta (E) = 0$
L'hypothèse " E admet un noeud " implique que la courbe admet 2 tangentes distinctes en ce noeud.

Les pentes de ces tangentes sont égales à la dérivée y' de y. L'hypothèse de 2 pentes implique que le polynôme g(x) admet deux racines distinctes ; donc son discriminant $dis (g) \neq 0$.

$dis (g) = 36c_4 (E) \neq 0$

□

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

Soit E une cubique de Weierstrass :$y^2 = x^3 - 27c_4 x - 54 c_6$ qui admet un point de rebroussement ; donc E est singulière
Par la proposition 4, sont discriminant est égal à $\Delta (E) = 0$
L'hypothèse " E admet un point de rebroussement " implique que la cubique E admet 2 tangentes confondues au point singulier.

$y^2 = x^3 - 27c_4 x - 54 c_4$ implique $y' = \frac{3x^2 - 27 c_4}{2 x} = \frac{3 g (x)}{2 y}$; $g (x) = x^2 - 9c_4$

Au point singulier S de E le polynôme g (x) admet une racine double, cela implique le discriminant $dis (g) = 36 c_4 = 0$, soit $c_4 = 0$.

Preuve de " $\Delta (E) = c_4 (E) = 0$ " implique " le point S est un point de rebroussement "

L'hypothèse $\Delta (E) = 0$ implique que la cubique d'équation $y^2 = 4 x^3 + b_2 x^2 + 2b_4 x + b_6$ admet un point singulier
L'hypothèse $\Delta (E) = 0$ et la relation $dis (f) = 16 \Delta(E)$ impliquent que f (x) admet une racine double ou triple.

La dérivée f' de f est égale à $f'(x) = 12\ x^2 + 2b_2x + 2b_4$, son discriminant $dis\ (f') = b_2^2 - 24\ b_4 = c_4(E) = 0$; donc deux tangentes confondues. Il en résulte que E admet 1 point de rebroussement.

□

Examinons la forme d'une Courbe Elliptique E suivant le signe de son discriminant Δ(E)

Proposition 6

Soit une Courbe Elliptique E d'équation de Weierstrass.

$E : \quad y^2 = x^3 + a_2x^2 + a_4x + a_6 = f(x) \in \mathbb{R}[x]$, de discriminant $\Delta(E)$; alors :

1) *E coupe l'axe Ox en 3 points simples si et seulement si $\Delta(E) > 0$*
2) *E coupe l'axe Ox en 1 seul point simple si et seulement si $\Delta(E) < 0$*

Preuve de " E coupe Ox en 3 points simples " implique " $\Delta(E) > 0$"

Soit une Courbe Elliptique E qui coupe l'axe Ox en 3 points simples

$$P_i = (e_i, 0), \quad i = 1,2,3 \qquad (1)$$

L'équation de Weierstrass de E se met sous la forme

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3) = f(x) \in \mathbb{R}[x] \qquad (2)$$

Par la théorie des multiplicités des racines d'un polynôme, f(x) et sa dérivée f'(x) n'ont pas de racine commune (3)

Il en résulte que le résultant $Res(f,f') \neq 0$.

Par définition du discriminant d'un polynôme $f(x) = \Pi_i (x - e_i)$, le discriminant de f est égal à

$$dis(f) = \Pi_{i \neq j} (e_i - e_j)^2 \qquad (4)$$

Par hypothèse les 3 racines sont des nombres réels, cela implique que les carrés $(e_i - e_j)^2$ sont positifs et $dis(f) > 0$ (5)

Les relations entre Res (f,f'), dis (f) et Δ (E) impliquent que $\Delta(E) > 0$ (6)

□

Preuve de " $\Delta(E) > 0$ " implique " E coupe l'axe Ox en 3 points distincts"

Par la proposition 4, une Courbe Elliptique a un discriminant $\Delta(E) \neq 0$ (1)

Son équation de Weierstrass se met sous la forme

$$E : \quad y^2 = (x - e_1)(x - e_2)(x - e_3) \in \mathbb{R}[x] \qquad (2)$$

Par définition le discriminant de f est égal à

$$dis(f) = (e_1 - e_2)^2 (e_2 - e_3)^2 (e_3 - e_1)^2 \in \mathbb{R} \qquad (3)$$

La relation $dis(f) = 16\Delta(E)$ et l'hypothèse $\Delta(E) > 0$ impliquent l'inégalité $dis(f) > 0$ (4)

(3) et (4) impliquent que les 3 carrés sont des nombres réels ; il en résulte que les 3 racines e_i sont réelles.

Les 3 points $P_i = (e_i, 0)$ sont les 3 points d'intersection de la courbe E par l'axe réel Ox.

□

Preuve de " E coupe Ox en 1 point simple" implique " $\Delta(E) < 0$ "

L'équation de Weierstrass d'une telle Courbe Elliptique est de la forme

$$E : y^2 = (x - e)(x^2 + rx + s) = f(x) \text{ avec } r^2 - 4s < 0 \quad , f(x) \in \mathbb{R}[x] \qquad (5)$$

Elle admet une racine réelle $e_1 = e$ et 2 racines complexes

$$e_j = -\frac{1}{2}(r \pm i \sqrt{4s - r^2}) ; \; j = 2,3 \quad \text{et} \quad 4s - r^2 > 0 \qquad (6)$$

La formule 3 du discriminant d'un polynôme f implique la valeur

$$\text{dis}(f) = -4 (4s - r^2) [(e - \frac{1}{2} r) + (4s - r^2)^2]^2 < 0 \qquad (7)$$

La relation entre Res (f, f') ,les discriminants dis (f) de f et Δ (E) de E impliquent

$$\Delta (E) < 0 \qquad (8)$$

□

Preuve de " Δ (E) < 0 " implique " E coupe l'axe Ox en 1 seul point "
Soit les 3 racines e réelle , e_2 et e_3 complexes, ci-dessus
L'hypothèse " Δ (E) < 0 " implique dis f = $(e - e_2)^2 (e - e_3)^2 (e_2 - e_3)^2 < 0$
Par la théorie des racines d'un polynôme , f(x) admet une racine réelle e et 2 racines complexes conjuguées $e_2 = s + it$, $e_3 = s - it$

□

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

Corollaire
Les cubiques de Weierstrass *sont classifiées en 4 classes selon leur discriminant Δ (E) et leur invariant $c_4(E)$*
La classe (Cl_1) des cubiques de Weierstrass *singulières qui ont un nœud lorsque $\Delta(E) = 0$ et $c_4(E) \neq 0$*
La classe (Cl_2) des cubiques de Weierstrass *singulières qui ont un point de rebroussement lorsque $\Delta(E) = c_4(E) = 0$*
La classe (Cl_3) des Courbes Elliptiques qui coupent l'axe réel Ox en 1 seul point simple lorsque $\Delta (E) < 0$
La classe (Cl_4) des Courbes Elliptiques qui coupent l'axe réel Ox en 3 points simples lorsque $\Delta (E) > 0$

□

1) Application à la famille E (t)

$$E (-1) : y^2 - x y - y = x^3 - 2 x \in \mathbb{Q} [x , y]$$

Calcul des invariants

$a_1 = -1$, $a_2 = 0$, $a_3 = -1$, $a_4 = -2$, $a_6 = 0$

$b_2 = 1$, $b_4 = -3$, $b_6 = 1$, $b_8 = \frac{(- b_2 b_6 - b_4^2)}{4} = \frac{(1 - 9)}{4} = -2$, $c_4 = +73$,

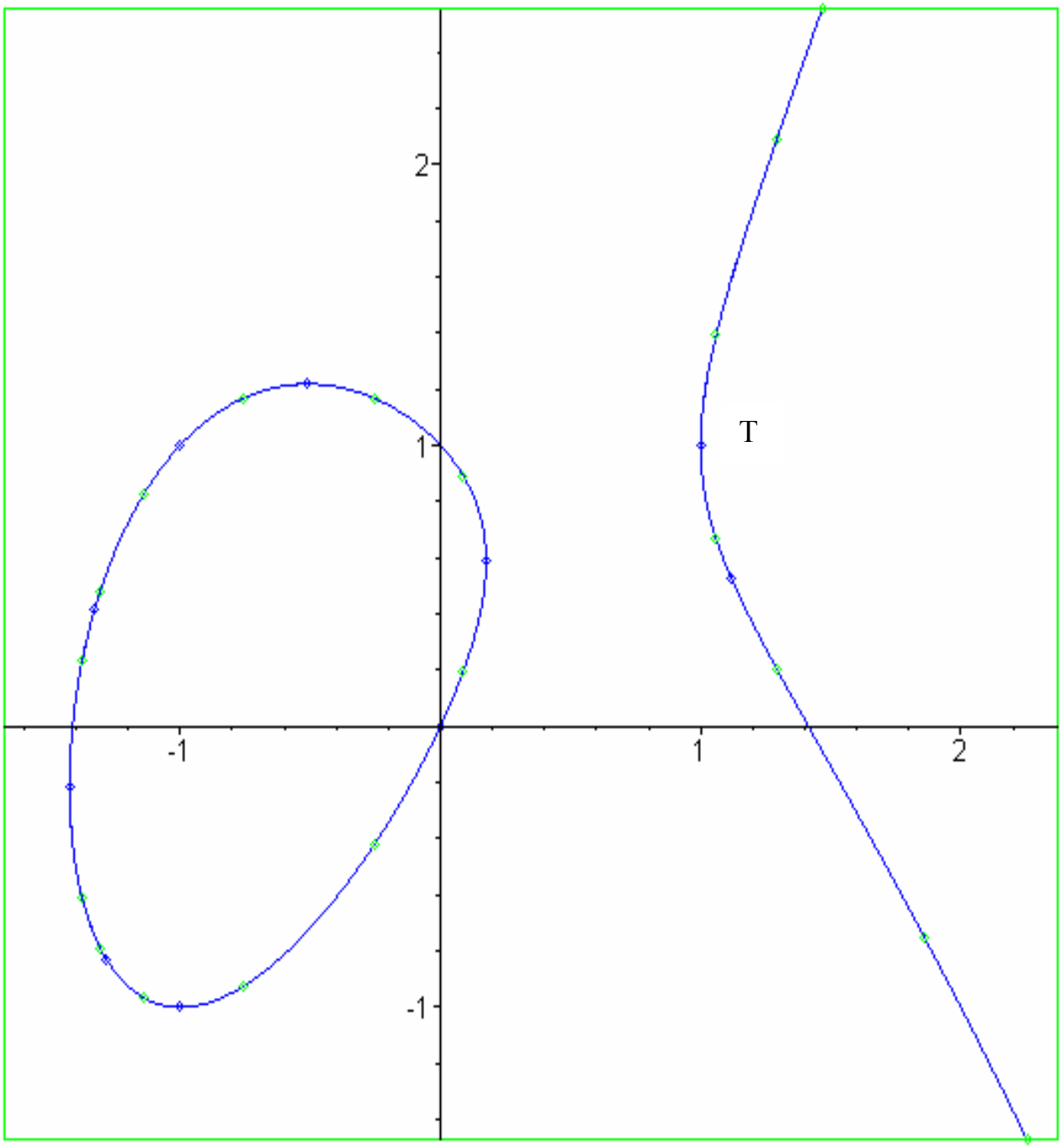
$\Delta (E (-1)) = 218$

D'après la classification des cubiques de Weierstrass, $\Delta(E) > 0$ implique que E est une Courbe Elliptique qui coupe l'axe Ox en 3 points simples.

Tableau des coordonnées de quelques points de la courbe E

x	-2	-1	0	$\frac{1}{2}$	1	2	3
y	pas de y réel	y = ± 1	y = 0 , y = 1	pas de y réel	y = 1 double	y = -1 , y = 4	$y= 2 \pm 2\sqrt{6}$

Je trace la Courbe Elliptique E (-1) avec le Maple 8



Le point T = (1, 1) est un point double ; la pente de la tangente à la courbe E en T est égale à y' (1,1) ; la dérivée y' est égale à :
$y' = (3 x^2 – 2 + y) / (2y – x – 1)$; il en résulte la pente $y'(1 , 1) = 2/0 = \infty$; donc la tangente à E en T est parallèle à l'axe Oy.

Intersection avec l'axe Ox : $y = 0$; $x^3 - 2x = 0$
$x(x^2 - 2) = 0$; 3 racines $x_1 = 0$, $x_2 = \sqrt{2}$, $x_3 = -\sqrt{2}$

2) Cubique $E(\frac{1}{2})$

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

Calcul des invariants

$a_1 = a_3 = \frac{1}{2}$, $a_2 = a_6 = 0$, $a_4 = 1$

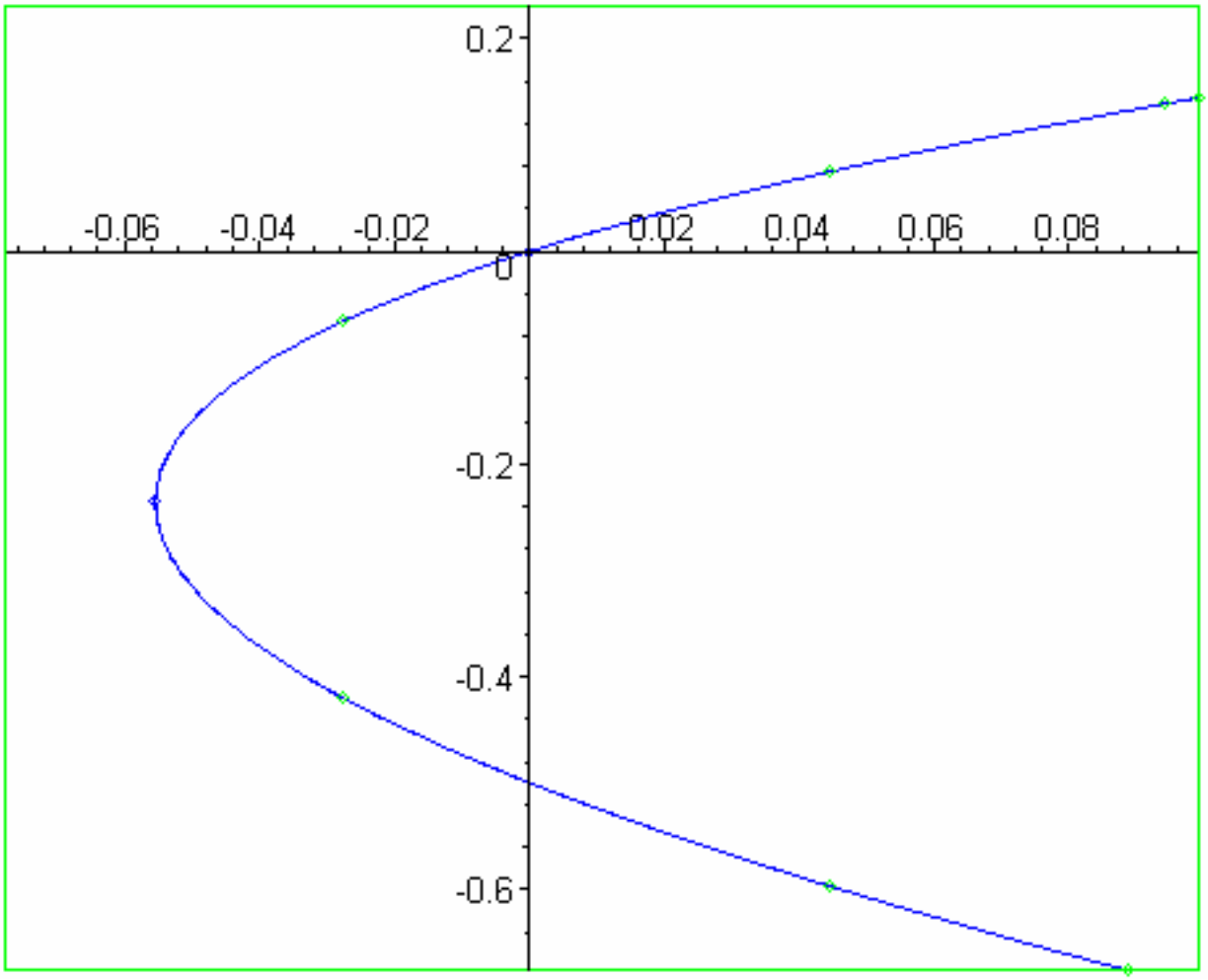
$b_2 = \frac{1}{4}$ $b_4 = \frac{5}{4}$, $b_6 = \frac{1}{4}$, $b_8 = -\frac{3}{8}$ et $\Delta (E) = -\frac{2129}{2.4^3}$

$\Delta(E) < 0$ implique que la courbe $E(\frac{1}{2})$ est une Courbe Elliptique qui coupe l'axe Ox en un seul point simple
Coordonnées de ce point : $y = 0$; $x^3 + x = 0$; $x (x^2 + 1) = 0$, ce polynôme admet une racine réelle simple $x_1 = 0$ et 2 racines complexes conjuguées $x_2 = i$, $x_3 = -i$

Tableau des coordonnées de quelques points de la courbe $E(\frac{1}{2})$

x	-2	-1	0	+1	+2
y	pas de y réel	Pas de y réel	y = 0, y = $-\frac{1}{2}$	- 2 et 1	- 4 et $\frac{5}{2}$

Je trace la courbe $E(\frac{1}{2})$: $y^2 + \frac{1}{2}xy + \frac{1}{2}y = x^3 + x$ avec le Maple 8



3) Soit la cubique de Weierstrass E (0) de la famille E(t) :

$y^2 = x^3$;

Calcul des invariants

$a_1 = a_3 = a_2 = a_6 = 0$, $a_4 = a_6 = 0$
$b_2 = b_4 = b_6 = b_8 = 0$, $\Delta (E) = 0$ et $c_4 = b_2^2 - 24\, b = 0$

Le discriminant $\Delta (E)$ et l'invariant $c_4 (E)$ sont nuls. Cela implique que la courbe E(0) présente un point de rebroussement S .

Les coordonnées de ce point singulier S sont les zéros du système d'équations linéaires algébriques

$$\begin{cases} \dfrac{dF}{dx} (x , y) = 0 ; \; F(S) = 0 \\ \dfrac{dF}{dy} (x, y) = 0 \end{cases}$$

$F (x, y) = y^2 - x^3$ implique les dérivées partielles

et
$$\begin{cases} \dfrac{dF}{dx} (x , y) = - 3 x^2 \\ \dfrac{dF}{dy} (x, y) = 2 y \end{cases}$$

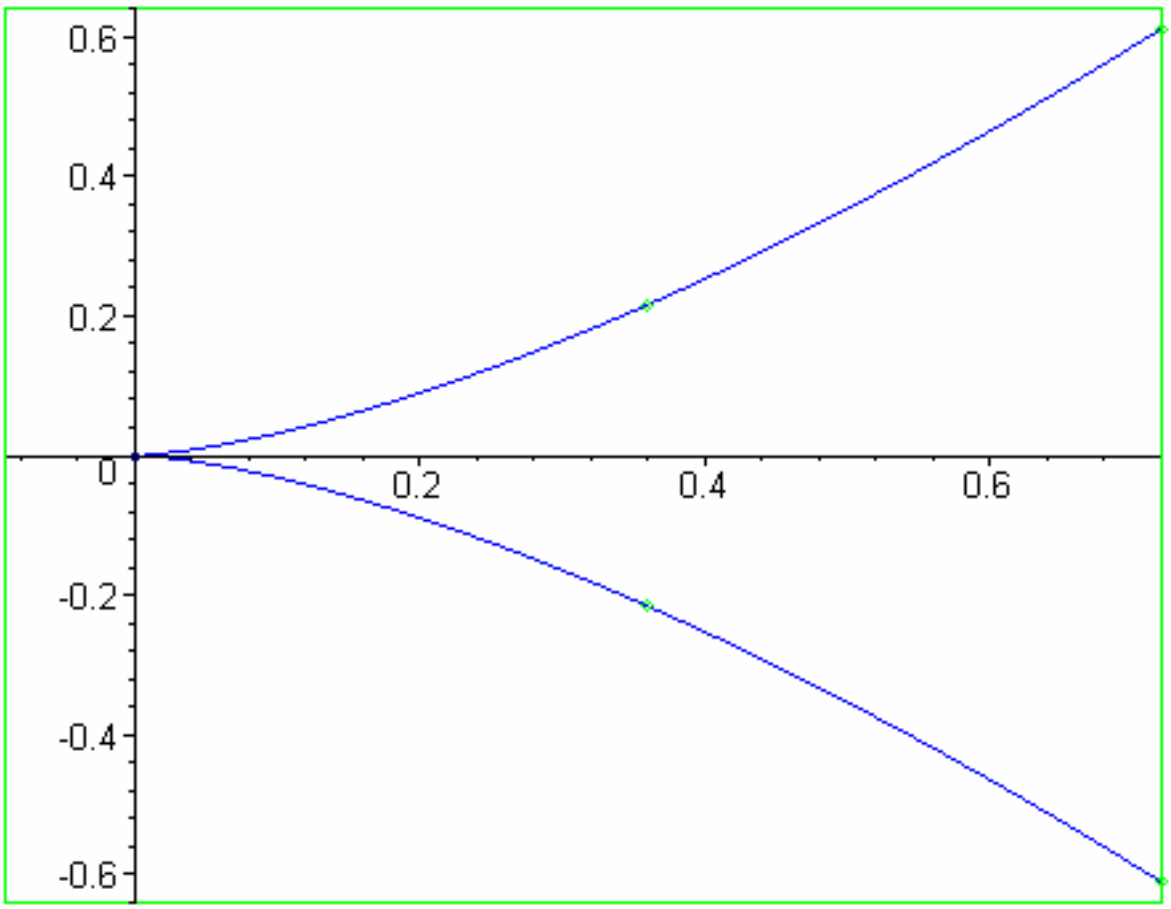
Ce système admet une solution unique : x = y = 0 .
Il en résulte que le point S = (0 , 0) est le point de rebroussement de la cubique E(0).

Tableau des coordonnées de quelques points de la cubique de E(0).

x	-2	-1	0	+1	+2	+ 3
y	pas de y réel	Pas de y réel	0	+ 1 et - 1	$+ 2\sqrt{2}$ $- 2\sqrt{2}$	$+\sqrt{3}$ $-\sqrt{3}$

La cubique de Weierstrass E (0) admet l'axe Ox comme axe de symétrie

Je trace la courbe E (0) avec le Maple 8



Chapitre 2 Groupe de Mordell–Weil de Courbes Elliptiques

C'est sans doute dans les travaux de Weierstrass et de Poincaré qu'est apparue la structure algébrique de l'ensemble des points d'une cubique plane et la construction de la somme de 2 points.

1 - Structure de groupe abélien additif E (K)

Soit une Courbe Elliptique E d'équation de Weierstrass.

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

Les 5 coefficients a_i sont des éléments d'un corps commutatif K, global, local ou fini, les 2 indéterminées x et y sont des éléments d'une clôture algébrique du corps K..

Considérons l'ensemble des points K-rationnels de la courbe E.

$$E(K) = \{ P = (x, y) \in E, x = f_1 / f_2 \ , y = f_3 / f_4, \text{ fractions rationnelles en } x , y , a_i \} \qquad (2)$$

Pour obtenir une structure algébrique de groupe abélien additif sur cet ensemble E(K) nous utilisons la :

Proposition 1

Soit l'ensemble E(K) des points K-rationnels d'une Courbe Elliptique E sur un corps commutatif K.

Alors l'application

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

est une loi de groupe abélien additif d'élément neutre , le point à l'infini O_{Et} , basé sur la règle géométrique de 3 points colinéaires de la courbe

$$P + Q + R = O_E = (\infty , \infty) \text{ dans le plan affine } \mathbb{A}^2(K)$$

$O_E = (0,1, 0)$ *dans le plan projectif* $\mathbb{P}^2(K)$ *; ce point est déterminé par la direction de l'axe Oy*

Le point P + Q = M est le symétrique du point R par rapport à l'axe Ox

Preuve :

1) Avec la règle géométrique de 3 points colinéaires, pour tout point P

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

L'axiome de l'élément neutre est vérifié

2) Sur une sécante PQ parallèle à l'axe Oy, la règle géométrique implique la relation

$$P + Q + O_E = O_E \quad .$$

Il en résulte -P = Q, l'axiome du symétrique est vérifié

3) Les sécantes PQ et QP coïncident, il en résulte

$$P + Q + R = Q + P + R = O_E$$

L'axiome de commutativité est vérifié

4) Pour l'associativité il faut calculer les points

$$P + Q = M,\ M + R = M' ,\ Q+R = T ,\ P + T = T'$$

Avec les formules des coordonnées obtenues au paragraphe suivant , nous obtenons l'égalité

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

qui assure l'axiome d'associativité.

□

Définition 1:
Le groupe abélien E(K) des points K rationnels d'une Courbe Elliptique E est le groupe de Mordell-Weil de la Courbe Elliptique E

Déterminons les coordonnées du symétrique d'un point, de la somme de 2 points d'une Courbe Elliptique et des points mP pour $m \geqslant 2$ et $P \neq O_E$.

2 - Coordonnées des points – P, $P_1 + P_2$, 2P et mP

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

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

1) Le symétrique d'un point $P = (x_P , y_P)$ de la courbe E est le point $-P = (x_p , -a_1 x_p - a_3 - y_p)$
2) La somme $P_1 + P_2 = M$ de 2 points $P_1 = (x_1 , y_1) \neq \pm P_2 = (x_2 , y_2)$ est le point

$$M = \begin{cases} x_M = \lambda^2 + a_1 \lambda - a_2 - x_1 - x_2 ; \lambda = \dfrac{y_2 - y_1}{x_2 - x_1} ; \\ y_M = -\lambda^3 - 2 a_1 \lambda^2 + (a_2 - a_1^2 + 2 x_1 + 2 x_2) + a_1 a_2 - a_3 + a_1 (x_1 + x_2) - y_1 \end{cases} ;$$

3) Le point P + P = 2P est le point de coordonnées :

$$x_{2p} = y'^2_p + a_1 y'_p - a_2 - 2 x_p \quad ; \qquad y' = \frac{3x^2 + 2 a_2 x + a_4 - a_1 y}{2y + a_1 x + a_3} ;$$

$$y_{2p} = -y_p'^3 - 2 a_1 y'^2_p + y'_p (a_2 - a_1^2 + 3x_p) + a_1 a_2 - a_3 + 2 a_1 x_p - y_p \quad ;$$

Preuve de 1
Le symétrique d'un point $P = (x_P , y_P)$ de la courbe E est l'intersection de E par la parallèle à l'axe Oy passant par P

Avec la géométrie analytique du plan Oxy j'obtiens les coordonnées du point d'intersection –P.
L'équation de la parallèle à l'axe Oy passant par P est $x = x_P$ (1)

L'équation cubique de Weierstrass de E devient une équation quadratique en y, cette équation admet donc 2 racines $y_1 = y_P$ et $y_2 = y(-P)$

La somme de ces 2 racines est égale à $y_1 + y_2 = -(a_1 x_P + a_3)$ (2)

Il en résulte la racine $y_2 = -(a_1 x_P + a_3 + y_P)$

$$-P = \begin{cases} x_{-P} = x_P \quad ; \\ y_{-P} = -(y_P + a_1 x_P + - a_P) ; \qquad (\text{ voir figure 1 }) \end{cases} \qquad (3)$$

Preuve de 2)
Soient 2 points $P_1 = (x_1 , y_1) \neq \pm P_2 = (x_2 , y_2)$ de la courbe E .
La sécante P_1P_2 , non parallèle à l'axe Oy coupe la courbe E en un 3^{em} point $P_3 = (x_3 , y_3)$
Pour la construction de la proposition 1, la somme $P_1 + P_2$ est le symétrique du point P_3
L'équation de la sécante P_1P_2 est égale à ,

$$y = \lambda(x - x_1) + y_1 \quad \text{pour} \qquad \lambda = \frac{y_1 - y_2}{x_1 - x_2} . \tag{4}$$

L'équation de Weierstrass de E devient une équation en y de degré 2 :

$$(\lambda(x - x_1) + y_1)^2 + (\lambda (x - x_1) + y_1) (a_1 x + a_3) = x^3 + a_2 x^2 + a_4 x + a_6 \tag{5}$$

La fonction symétrique élémentaire « somme des racines « d'une équation algébrique implique la relation

$$x_1 + x_2 + x_3 = \lambda^2 + \lambda a_1 - a_2 \tag{6}$$

Il en résulte les coordonnées du point $P_3 = (x_3 , y_3)$

$$x_3 = \lambda^2 + \lambda a_1 - x_1 - x_2 - a_2$$
$$y_3 = \lambda(x_3 - x_1) + y_1 = \lambda^3 + a_1 \lambda^2 - \lambda (a_2 + 2 x_1 + 2 x_2) + y_1 ;$$

La formule (3) précédente du symétrique d'un point P de E implique le symétrique de P_3

$$P_1 + P_2 = - P_3 = M = (x_M , y_M)$$

$$x_M = x_3 = \lambda^2 + a_1 \lambda - a_2 - x_1 - x_2 ;$$
$$y_M = -(y_3 + a_1x_3 + a_3) ;$$
$$= -\lambda^3 - a_1 \lambda^2 + \lambda (a_2 - a_1^2 + 2 x_1 + 2 x_2) + a_1a_2 - a_3 + a_1 (x_1 + x_2) - y_1 ;$$

(voir figure 2)

Preuve de 3)
La tangente à la courbe E au point $P = (x_P , y_P)$ a pour équation

$$y = y_P' (x - x_P) + y_P \text{ avec } y' = \frac{3 x^2 + 2 a_2 x + a_4 - a_1 y}{2y + a_1x + a_3} ; \tag{9}$$

Cette tangente coupe E au point double P et en un point simple T

Avec (9) , l'équation devient :

$$[y'_p (x - x_p) + y_p]^2 + [y'_p (x - x_p) + y_p] (a_4x + a_3) = x^3 + a_2 x^2 + a_4 x + a_6 . \tag{10}$$

C'est une équation cubique en x qui admet une racine double x_P et une racine simple x_T .

La fonction symétrique élémentaire « somme des racines » implique la relation

$$2 x_p + x_T = + y'^2_p + a_1 y'_p - a_2 \tag{11}$$

Il en résulte l'abscisse de T

$$x_T = y'^2_p + a_1 y'_p - a_2 - 2 x_p ; \tag{12}$$

et l'ordonnée

$$y_T = y'_p (x_T - x_p) + y_p$$
$$= y'_P + a_1 y'^2_p - y'_P (a_2 + 3 x_p) + y_P . \tag{13}$$

Le point 2P est le symétrique du point T

$$2P = -T = (x_T \ , \ y_T - a_1 x_T - a_3) \ ; \qquad (14)$$

Avec (12) , (13) et (14) j'obtiens les coordonnées du point 2P :

$$\begin{cases} x_{2P} = y'^2_P + a_1 y'_P - a_2 - 2 x_P \text{ avec } y' = \dfrac{3x^2 + 2a_2 x + a_4 - a_1 y}{2y + a_1 x + a_3} \ ; \\ y_{2P} = - y_P'^3 - 2 a_1 y'^2_P + y'_P (a_2 - a_1^2 + 3x_P) + a_1 a_2 - a_3 + 2 a_1 x_P - y_P \ . \end{cases}$$

(voir figure 3)

□

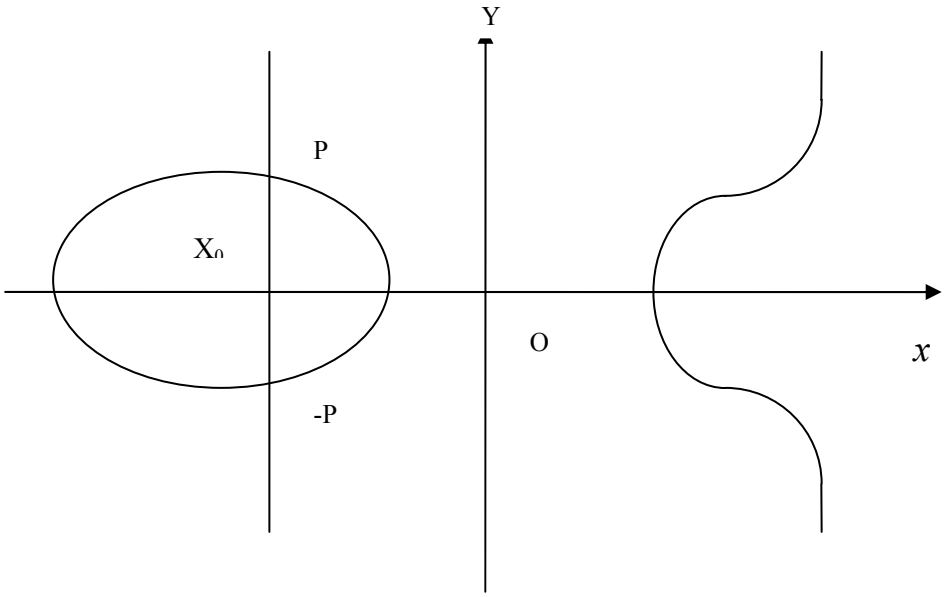


Figure 1

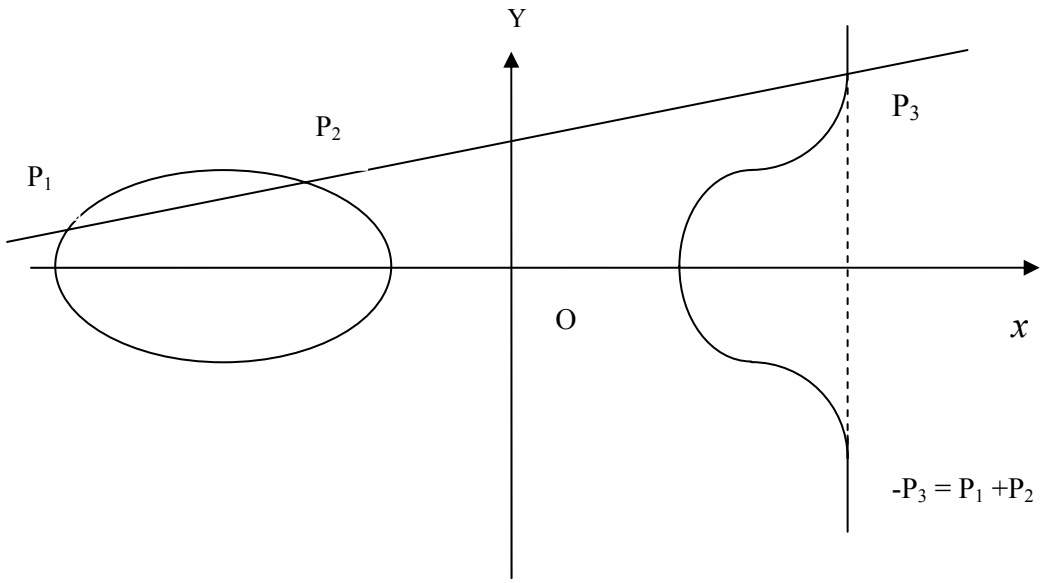


Figure 2

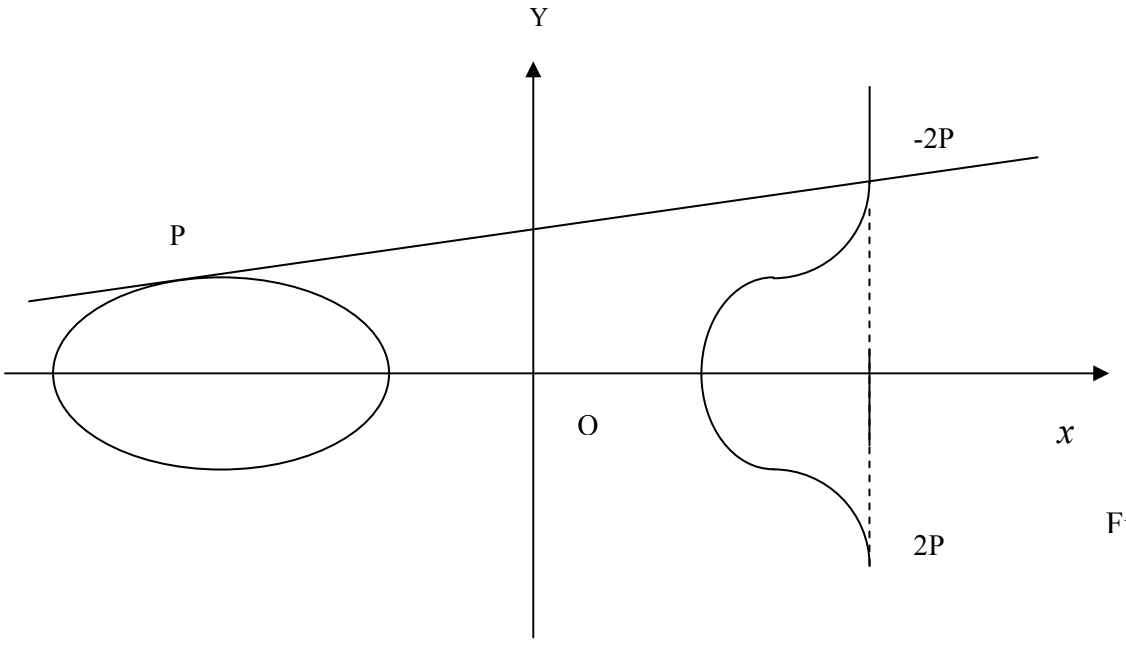


Figure 3

Les formules des coordonnées de la somme $P_1 + P_2$ et de 2P permettent de calculer les coordonnées des points 3P = 2P + P, 4P = 2(2P) = 3P + P, 5P = 4P + P , 6P = 2 (3 P) , etc ….

Ces coordonnées sont fonctions des 5 coefficients $a_1 , \dots , a_6$.

Pour obtenir des formules plus simples , il faut prendre des valeurs $a_i = 0$. C'est ce qu'on trouve dans [Cassels] pour les points d'ordre fini de Courbes Elliptiques.

Définition 2 :
Pour tout entier rationnel $m \in \mathbb{Z}$ un point P d'ordre m d'une Courbe Elliptique E est un point P du groupe de Mordell-Weil E(K) qui satisfait la relation $mP = O_E$

$mP = P + ...P$; m fois P si $m > 0$

$mP = (-m)(-P)$; (-m) fois (-P) si $m < 0$

et $0P = O_E$ si $m = 0$

C'est la notion de torsion de l'algèbre générale d'un groupe .

Proposition 3
Pour tout entier rationnel m, l'ensemble E(K) [m] des points P d'ordre m d'une Courbe Elliptique E est un sous groupe du groupe E(K) de Mordell- Weil de E .

Preuve
Soient 2 points P et Q d'ordre m de E :

$mP = mQ = 0_E$

Il en résulte la relation

$mP - mQ = m(P - Q) = O_E$.

Donc le point P – Q est d'ordre m ; il appartient à l'ensemble E(K)[m], cet ensemble est un sous groupe du groupe de Mordell- Weil (Théorème relatif aux sous groupes d'un groupe)

Définition 3
a) L'ensemble E(K)[m] est le sous groupe de m –torsion de la courbe E pour tout entier m
b) Le groupe de torsion de E est l'ensemble T (E) des points P de E d'ordre fini.

$T(E) = \{ P \in E(K) , mP = O_E , m \text{ fini} \}$.

Les points d'ordre infini forment un système générateur de E - T (E)

Le groupe de torsion T(E) est une partie finie du groupe de Mordell-Weil E(K),(conjecture). Sa structure algébrique a été déterminée dans certains cas.

Proposition 4
Le groupe de torsion T (E) ($\mathbb{Q}$) d'une Courbe Elliptique est un groupe abélien additif fini isomorphe à l'un des 15 groupes additifs abéliens finis..

$\mathbb{Z} / m\mathbb{Z}$ pour m =1, ... ;10 et m =12

$\mathbb{Z} / 2\mathbb{Z} + \mathbb{Z} / 2d\mathbb{Z}$ pour d = 1 , 2, 3, 4

Preuve
C'est un théorème conjecturé par OGG et démontré par Mazur [21]

□

D'autres résultats indiquent des informations sur certains points de torsion de Courbes Elliptiques .

Proposition 5
Soit une Courbe Elliptique E d'équation de Weierstrass

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

Alors pour tout point P =(x, y) $\in$ E ($\mathbb{Q}$) d'ordre m $\neq$ 0, les coordonnées x et y sont des rationnels ; si m > 2 alors y^2 divise $4\,A^3 + 27\,B^2$.

Preuve
T.Nagell (solution de quelques problèmes dans la théorie des cubiques planes du 1er genre , Wid Akad Oslo 1 (1935) et E.Lutz (sur l'équation $y^2 - Ax - B$ dans les corps p-adiques , Jour Reine Ang, Math.177 (1937) 237 -247) .

□

Les coordonnées des points de m-torsion d'une Courbe Elliptique E ont été déterminées dans [4] .

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

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

Alors, pour tout entier m, les coordonnées du point mP sont égales à

$$mP = (x_m , y_m)) = \left(\frac{\theta_m (x , y)}{\psi_m^{\,2} (x , y)} \ , \ \frac{\omega_m (x , y)}{\psi_m^{\,3} (x , y)} \right) .$$

θ_m , ω_m , ψ_m sont des polynômes de l'anneau $\mathbb{Z}$ [x,y ,A, B] avec les relations :

$$\psi_{-1} = -1\ ,\ \psi_0 = 0\ ;\ \psi_1 = 1\ ,\ \psi_2 = 2y\ ,\ \psi_3 = 3x + 6\,A\,x^2 + 12\,B\,x - A^2\ ;$$
$$\psi_4 = 4\,y\,(x^6 + 5\,A\,x^4 + 20\,B\,x^3 - 5\,A^2\,x^2 - 4\,A\,b\,x - A^3 - 8\,B^2)\ ;$$
$$\psi_{2m} = 2\,\psi_m\,(\psi_{2m+1}\,\psi_{m-1} - \psi^2_{m-2}\,\psi^2_{m+1})\ ;$$
$$\psi_{2m+1} = \psi_{m+2}\,\psi^3_m - \psi_{m-1}\,\psi^3_{m+1} \quad \text{pour } m \geqslant 2\ ;$$
$$\theta_m = x\,\psi^2_m - \psi_{m-1}\,\psi_{m+1}\ ;$$
$$4y\,\omega_m = \psi_{m+2}\,\psi^2_{m-1} - \psi_{m-2}\,\psi^2_{m+1}\ ;$$

Preuve :
La formule – P = (x , – y) implique :

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

La relation OP = (∞ , ∞) = $\left(\frac{x}{0}, \frac{y}{0}\right)$ implique $\psi_0 = 0$.

La relation 1 P = (x , y) = $\left(\frac{x}{1^2}, \frac{y}{1^3}\right)$ implique $\psi_1 = 1$.

Pour m $\geqslant$ 2 nous utilisons un raisonnement par récurrence sur m .

Lorsque K = $\mathbb{C}$ = Corps des nombres complexes, ce sont les formules de la fonction P (z, L) de Weierstrass qui sont utilisées [(Lemme 7 -2 [2]) [4]].

Application à la famille de cubiques de Weierstrass :

$$E(t) : y^2 + t\,xy + t\,y = x^3 + 2\,tx \in \mathbb{Q}[x, y]$$

Calcul des invariants

$a_1 = a_3 = t$, $a_2 = a_6 = 0$, $a_4 = 2t$, $b_2 = t^2$, $b_4 = t^2 + 4t$, $b_6 = t^2$, $b_8 = -2t^3 - 4t^2$

$\Delta(E) = t^3 (5t^3 + 2t^4 - 60t^2 - 357t - 512)$

$c_4 = t^4 - 24t^2 - 96t$; $c_6 = -t^6 + 36t^4 + 144t^3 - 216t^2$

Coordonnées du symétrique de $P = (x , y)$

$-P = (x , -y - tx - t)$

Coordonnées de la somme $M = P_1 + P_2$, $P_i = (x_i , y_i)$, $P_1 \neq P_2$

$x_M = \lambda^2 + t\lambda - x_1 - x_2$; avec $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$

$y_M = -\lambda^3 - 2t\lambda^2 + (2x_1 + x_2 - t^2)\lambda - t + t(x_1 + x_2) - y_2$

Coordonnées du point $2P = (x_{2P} , y_{2P})$

$x_{2P} = y'^2_P + t\,y'_P - 2x_P$ avec $y' = \dfrac{3x^2 + 2x - ty}{2y + tx}$

$y_{2P} = -y'^3 - 2t\,y'^2 + (3x - t^2)y'_P - t + 2t\,x_P - y_P$

Exemple : Cubique E(-2) de la famille E (t) :

$$E(-2) : y^2 - 2(x + 1)y = x^3 - 4x ;$$

$a_1 = a_3 = -2$, $a_2 = a_6 = 0$, $a_4 = -4$, $b_2 = 4$, $b_4 = -4$, $b_6 = 4$, $b_8 = 0$

$c_4 = 112$, $c_6 = -1504$, $\Delta(E) = +5552$

$\Delta(E) > 0$ implique que E (-2) est une Courbe Elliptique qui coupe l'axe Ox en 3 points simples.

Ces 3 points sont $T_1 = (0, 0)$; $T_2 = (2 , 0)$ et $T_3 (-2 , 0)$.

Quelques points de cette courbe

Intersection avec l'axe Oy . $x = 0$, $y = 0$ et 2

x	- 3	-1	0	1	2	0 , 2 et -2
y	Pas de y réel	$\pm\sqrt{3}$	0 et 2	1 et 3	0 et 6	0

$P_1 = (0 ,0)$, $P_2 = (0, 2)$, $P_3 = (2, 0)$, $P_4 = (2, 6)$

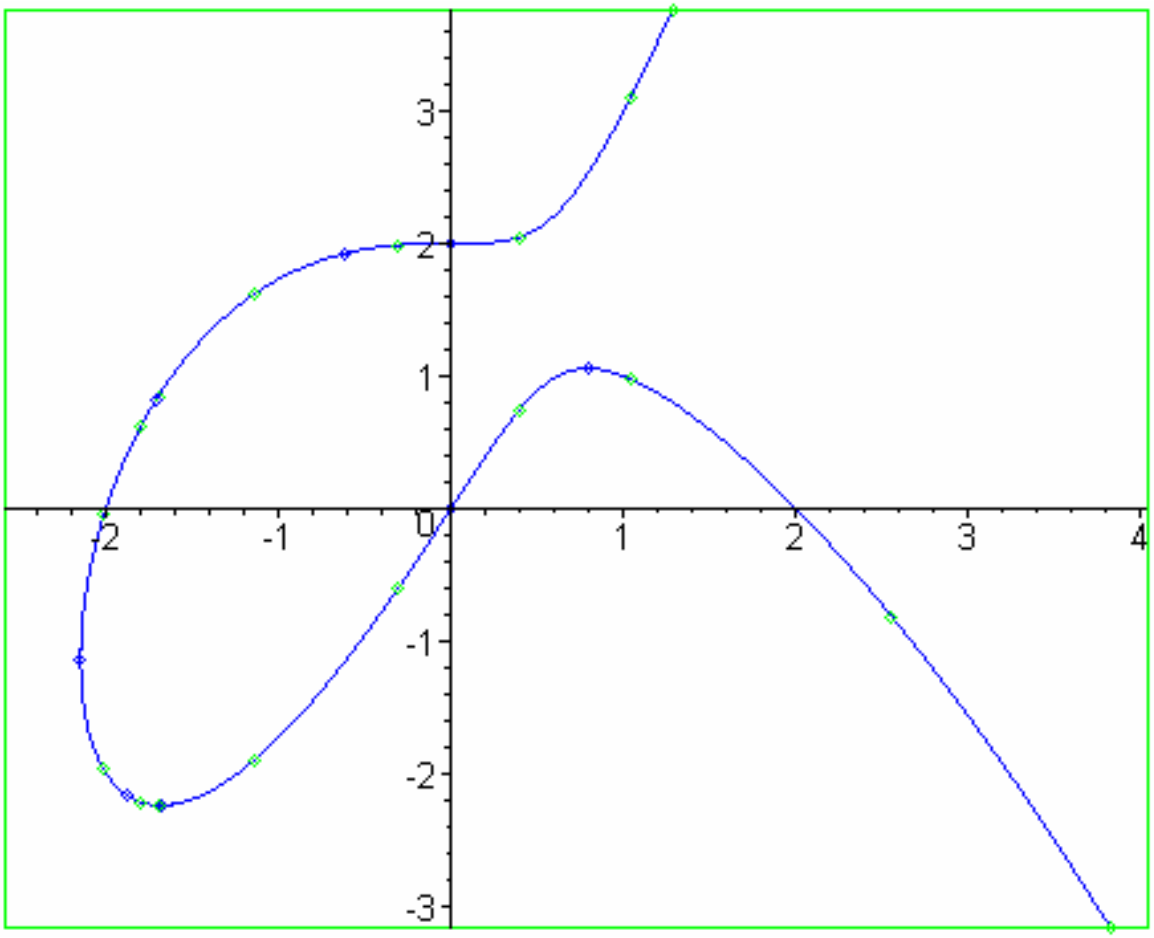
Calculons les coordonnées des points

$2P_1 = (0 , +2)$, $2P_2 = (0, 0)$, $2P_3 = (\frac{4}{9} , \frac{22}{27})$, $2P_4 = (\frac{4}{9} , \frac{79}{27})$

$-P_1 = (0, -2)$, $-P_2 = (0, - 4)$; $-P_3 = (2, 2)$; $-P_4 (2 , - 4)$

$P_1 + P_2 = (\infty , \infty)$, $P_2 + P_3 = (1, 3)$ $P_1 + P_4 = (1 , 1)$.

Je trace la courbe E (-2) avec le Maple 8



La position des 3 points simples de la courbe dépend de la propriété du discriminant $D = B^2 - 4\,AC$ de l'équation quadratique

$$y^2 + Ax + B = 0, \text{ ici } A = -2\,(x + 1).$$
$$B = -x^3 + 4\,x\,.$$

Nous obtenons $D = x^3 + x^2 - 2\,x + 1 = u\,(x)$.

Il en résulte que la courbe est définie dans le domaine $x > \alpha$ pour $-3 < \alpha < -2$.

3 -Isomorphisme de Courbes Elliptiques

Le groupe E (K) de Mordell-Weil d'une Courbe Elliptique admet les propriétés d'homomorphismes de groupes : homomorphismes, isomorphismes, endomorphismes, automorphismes.

Il y a des homomorphismes spécifiques : isogénies, twists, espaces homogènes.
Commençons par les isomorphismes

Proposition 7
Soit une Courbe Elliptique E d'équation de Weierstrass
$E : y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \in K [x , y]$
Le changement de variables
$$x = u^2X + r \quad ; \quad y = u^3Y + su^2X + t \quad avec \quad u \neq 0 , r, s, t \in K$$
est un isomorphisme du groupe E(K) dans l'image E'(K)
$E' : Y^2 + a'_1 XY + a'_3 Y = X^3 + a'_2 X^2 + a'_4 X + a'_6 \in K [X, Y]$

Preuve
Soit l'homorphisme de groupe
$$\lambda \quad E(K) \longmapsto E' (K)$$
de valeur $\lambda (x , y) = (u^2X + r , u^3Y + su^2X + t)$

La transformée de la courbe E est la courbe E' d'équation de Weierstrass
$E' : Y^2 + a'_1 XY + a'_3 Y = X^3 + a'_2 X^2 + a'_4 X + a'_6 \in K[X, Y]$

La relation $\lambda (P_1 + P_2) = \lambda (P_1) + \lambda(P_2)$ est vérifiée avec le calcul

La relation $\lambda (O_E) = O_{E'}$ est vérifiée avec le calcul

Le changement de variables $(x, y) \longmapsto (X , Y)$ implique les valeurs
$$X = \frac{x - r}{u^2} \quad \text{et} \quad Y = \frac{y - su^2 X - t}{u^3}$$

L'hypothèse $u \neq 0$ implique une solution unique X , Y . Donc λ est bijectif

□

Cet isomorphe E (K) $\longmapsto$ E' (K) implique des relations entre les invariants des 2 courbes isomorphes E et E'

Corollaire
Soit les hypothèses de la proposition précédente. Alors les coefficients a_i et b_i satisfont les relations :

$$\begin{aligned} ua'_1 &= a_1 + 2s \ ; \\ u^2a'_2 &= a_2 - sa_1 + 3r - s^2 \\ u^3a'_3 &= a_3 + ra_1 + 2t \\ u^4a'_4 &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st \\ u^6a'_6 &= a_6 + ra_4 + r^2a_2 - t a_3 - rt a_1 + r^3 - t^2 \end{aligned} \qquad \textit{(Isom 1)}$$

Les coefficients b_{2i} et c_{2i} satisfont les relations

$$
\begin{aligned}
u^2 b'_2 &= b_2 + 12\, r \\
u^4 b'_4 &= b_4 + r\, b_2 + 6\, r^2 \\
u^6 b'_6 &= b_6 + 2r\, b_4 + r^2 b_2 + 4\, r^3 \\
u^8 b'_8 &= b_8 + 3\, r\, b^6 + 3\, r^2 b_4 + r^3 b_2 + 3r^4 \\
u^4 c'_4 &= c_4 \quad \text{et } u^6 c'_6 = c_6
\end{aligned}
\qquad \textit{(Isom 2)}
$$

Les invariants ″discriminant ″et ″invariant modulaire″ satisfont les relations

$$u^{12}\, \Delta(E') = \Delta(E) \quad \text{et } j(E) = j(E') \qquad \text{(Isom 3)}$$

Preuve

Nous remplaçons dans l'équation de Weierstrass de E la variable x par $u^2X + r$ et la variable y par $u^3Y + su^2X + t$, nous obtenons ainsi les relations (Isom 1) , (Isom 2) et (Isom 3)

□

Dans la relation (Isom 3) nous constatons que l'invariant modulaire j (E) = j(E') est le même pour 2 Courbes Elliptiques isomorphes ; donc j (E) permet de classifier l'ensemble des Courbes Elliptiques en classes.
Cette théorie se trouve dans [26]

Proposition 8

Deux Courbes Elliptiques E/K et E'/K sont isomorphes si seulement si leurs invariants modulaires sont égaux j(E) = j(E')

Preuve de « E et E' isomorphes » implique » j (E) = j (E') »
Soient 2 Courbes Elliptiques E/K et E'/K isomorphes : Alors le corollaire ci-dessus implique l'égalité

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

Preuve de « j (E) = j (E') » implique « E isomorphe à E' »
Soient 2 Courbes Elliptiques E et E' dont les invariants modulaires sont égaux :

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

Considérons les 3 cas $j(E) = 0$, $j(E) = 1728$, $j(E) \neq 0,1728$ pour car $k \neq 2, 3$

1)- Cas $j(E) = j(E') = 0$ (1)

J'utilise la formule $$j(E) = \frac{1728\ c_4^3}{c_4^3 - c_6^2} \qquad (2)$$

Je choisis les équations de Weierstrass

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

$E' : Y^2 = X^3 - 27\, c'_4\, X - 54\, c'_6$ (3)

L'hypothèse $j(E) = j(E') = 0$ et (2) impliquent

$$c_4 = c'_4 = 0 \text{ et } c_6 \neq 0 \ ; \ c'_6 \neq 0 \qquad (4)$$

Il en résulte l'équation $u^4 c'_6 = c_6$ par (isom 2) (5)

Cette équation admet 6 racines u dans un clôture algébrique de K

$$u = z^t \ (c_6 // c'_6) \ , z \ = \exp \frac{2i \ \Pi}{6} \ \text{et t mod 6} \qquad (6)$$

Il en résulte les 6 isomorphismes

$$x = u^2X + r \quad ; \quad y = u^3Y + su^2X + \ t \qquad (7)$$

2) Cas de j (E)= j (E') = 1728 (8)

Avec (2), (3) et (8) j'obtiens les valeurs

$$c_6 = \ c'_6 \ = 0 \quad \text{et} \quad c_4 \ , \ c'_4 \neq 0 \qquad (9)$$

Il en résulte l'équation

$$u^4 c'_4 = \ c_4 \ \text{par (isom 2)} \qquad (10)$$

Cette équation admet 4 racines dans une clôture algébrique de K

$$u = \ i^{\ t} \ (c_4 / c'_4) \ , i = \exp \left(\frac{2 \ \Pi \ i}{4}\right) \quad \text{et} \quad \text{t mod 4} \qquad (11)$$

Cela implique les 4 isomorphismes

$$x = u^2X + r \quad ; \quad y = u^3Y + su^2X + \ t \qquad (12)$$

3) Cas de j (E) = j (E') = $\gamma \neq 0, 1728$, carac K $\neq 2, 3$ (13)

(2) implique les égalités

$$\frac{1728 \ c^3_4}{c^3_4 - c^2_6} = \frac{1728 \ c'^3_4}{c'^3_4 - c'^2_6} = \gamma \in K \qquad (14)$$

Avec les conditions $c_4 \neq 0$, $c'_4 \neq 0$, $c_6 \neq 0$, $c'_6 \neq 0$ (15)

(14) implique l'équation

$$c^3_4 (\gamma - 1728) = \gamma \ c^2_6 \qquad (16)$$

Cette équation admet la solution

$$c_4 = \frac{\gamma}{\gamma - 1728} = c_6 \qquad (17)$$

l'équation de Weierstrass de E est

$$y^2 = x^3 - \frac{27 \ \gamma}{\gamma - 1728} \ x - \frac{54 \ \gamma}{\gamma - 1728} \in K [x , y] \qquad (18)$$

Les formules (Isom 2) impliquent les relations

$$u^4 \ c'_4 = c_4 \quad \text{et} \quad u^6 \ c'_6 = c_6 \qquad (19)$$

(19) admet la solution

$$u = (c_4 // c'_4)^{1/4} = (c_6 / c'_6)^{1/6} \qquad (20)$$

Il en résulte l'isomorphisme

$$E(K) \longmapsto E'(K) \ , x = u^2 X \quad , \quad y = u^3 Y \tag{21}$$

4) Cas de carac K = 3

Cela implique $1728 = 0$ et $j(E) = 0$;

Calcul des invariants de l'équation de Weierstrass

$$E : y^2 = x^3 + a_2 x^2 + a_6 \in K[x, y] \tag{22}$$

J'obtiens avec $a_1 = a_3 = a_4 = 0$ les valeurs

$$b_2 = a_2 \ , b_4 = 0 \ , b_6 = a_6 \ , c_4 = a_2^2 \ , b_8 = a_2 a_6 \ \text{ et } \ \Delta(E) = -a_3^2 a_6 \tag{23}$$

Les relations (Isom 1) et (22) impliquent les 2 équations

$$u^2 a'_2 = a_2 \quad \text{et} \quad u^6 . a'_6 = a_6 \tag{24}$$

Ces 2 équations admettent la solution

$$u = \left(\frac{a_2}{a'_2}\right)^{1/2} = \left(\frac{a_6}{a'_6}\right)^{1/6} \tag{25}$$

Il en résulte les isomorphismes

$$x = u^2 X \quad \text{et} \quad y = u^3 Y$$

et l'équation de Weierstrass

$$E' : Y^2 = X^3 + a'_2 X^2 + a'_6 \in K[X, Y] \tag{26}$$

5) Cas de caract K = 2

Cela implique $1728 = 0$ et $j(E) = 0$ (27)

Je choisis une Courbe Elliptique E d'équation de Weierstrass

$$E : y^2 + x y + y = x^3 \in K[x, y] \tag{28}$$

Calcul des invariants de E

$$a_2 = a_4 = a_6 = 0 \ , \ a_1 = a_3 = 1 \ , b_2 = 1 = b_4 = b_6 \ , \ b_8 = 1 \ ; c_4 = 1 \ ; \ \Delta(E) = 1 \tag{29}$$

Avec les formulas (Isom 1) j'obtiens les équations

$u^2 a'_1 = a_1$ et $u^3 a'_3 = a_3$ qui admettent les solutions $u = \pm 1$

Il en résulte 2 isomorphismes $E(K) \longmapsto E'(K)$ et la Courbe Elliptique isomorphe

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

□

Application à la famille E (t)

Cubique E(5) d'équation de Weierstrass

$$E(5) : y^2 + 5 x y + 5 y = x^3 + 10 x \in \mathbb{Q}[x, y]$$

Calcul des invariants
$a_2 = a_6 = 0$, $a_1 = a_3 = 5$, $a_4 = 10$; $b_2 = 25$, $b_4 = 45$, $b_6 = 25$, $b_8 = -350$; $c_4 = -455$;
$c_6 = 3895$, $\Delta(E) = -5^5 \times 5686$; $j(E) = + \frac{(91)^2}{5^2 \, x \, 5686}$

$\Delta(E) \neq 0$ implique que la cubique E (5) est une Courbe Elliptique.

Appliquons l'isomorphisme
$(x, y) \longmapsto (u^2 X + 1 , u^3 Y + u^2 X - 5)$ pour u = 2

Ici $s = 1$, $t = -5$, $r = 1$

Par (Isom1) j'obtiens
$a'_1 = \frac{7}{2}$, $a'_2 = -\frac{3}{4}$, $a'_3 = 0$, $a'_4 = \frac{19}{8}$;,$a'_6 = \frac{9}{16}$
Par (Isom2) j'obtiens
$b'_2 = \frac{37}{4}$, $b'_4 = \frac{19}{4}$, $b'_6 = \frac{9}{4}$, $c'_4 = -\frac{455}{16}$, $c'_6 = \frac{3895}{64}$

Il en résulte la Courbe Elliptique E' d'équation de Weierstrass

$$E' : Y^2 + \frac{7}{2} X Y = X^3 - \frac{3}{4} X^2 + \frac{19}{8} X + \frac{9}{16} \quad \in \mathbb{Q} [X , Y]$$

et ses invariants.

$$\Delta(E') = - \frac{5686 \, x \, 5^5}{2^{12}} \quad \text{et} \quad j(E') = j(E) = \frac{91^3}{9^2 \, x \, 686}$$

4 Endomorphismes d'une Courbe Elliptique

Les endomorphismes $E(K) \longmapsto E(K)$ d'une Courbe Elliptique E forment un anneau $End_K (E)$, isomorphe à l'anneau $\mathbb{Z}$ ou à un ordre contenant $\mathbb{Z}$
La description de cet anneau est précisée par la proposition (Corollary 9-4 p 102 [26])

Définition 4
Les Courbes Elliptiques dont l'anneau des endomorphismes $End_K (E)$ contient l'anneau $\mathbb{Z}$ sont des Courbes Elliptiques à Multiplication Complexe.

Dans le cas où la Courbe Elliptique E est à Multiplication Complexe, l'anneau des endomorphismes de E est isomorphe soit à l'anneau des entiers d'un corps quadratique imaginaire $\mathbb{Q}(\sqrt{-d})$, soit à un ordre $\mathbb{Z} + f\sqrt{-d}$ de cet anneau .

Définition 5
Un ordre d'un corps quadratique imaginaire K , est un sous anneau.

$O(f) = A(K) + f \mathbb{Z}$ de l'anneau A (K) des entiers de K ; f est le conducteur de l'ordre O (f)
.

Si K est un corps fini, toute Courbe Elliptique E définie sur K est à Multiplication Complexe.

Application à la famille E (t)

La Cubique E (1) de la famille E (t) :

E (1) : $y^2 + x\,y + y = x^3 + 2x \quad \in \mathbb{F}_7$.

Calcul des invariants de E(1)
$a_1 = a_3 = 1$, $a_2 = 0$, $a_4 = 2$, $a_6 = 0$, $b_2 = 1$, $b_4 = 5$, $b_6 = 1$, $b_8 = 1$, $c_6 = 5$, $c_4 = 0$, j (E) = 0 ,
Δ (E) = 2 $\neq 0$ dans $\mathbb{F}_7$.

E (1) est une Courbe Elliptique sur $\mathbb{F}_7$ à Multiplication Complexe .

5 Automorphisme d'une Courbe Elliptique

Les automorphismes d'une Courbe Elliptique E, forment un groupe Aut_K (E) , qui dépend de la caractéristique de K et de l'invariant modulaire j (E).

Proposition 9
Soit une Courbe Elliptique E sur un corps K et j (E) son invariant modulaire; alors le groupe Aut_K (E) de ses automorphismes est un groupe d'ordre un diviseur de 24.

1) *Aut_K (E) est d'ordre 2 si j (E) $\neq$ 0, 1728*
2) *Aut_K (E) est d'ordre 4 si j(E) = 1728 et K de caractéristique $\neq$ 2,3*
3) *Aut_K (E) est d'ordre 6 si j (E) = 0 et K de caractéristique $\neq$2, 3*
4) *Aut_K (E) est d'ordre 12 si j (E) = 0 = 1728 et K de caractéristique 3*
5) *Aut_K (E) est d'ordre 24 si j (E) = 0 = 1728 et K de caractéristique 2*

Preuve
Je choisis une Courbe Elliptique E d'équation de Weierstrass
E : $y^2 = x^3 + Ax + B \in K[x , y]$.
définie sur un corps K de caractéristique $\neq$ 2,3 avec $4A^3 + 27B^2 \neq 0$ (1)
L'invariant modulaire est égal à $j(E) = -\dfrac{1728.\,4A^3}{4A^3 + 27B^2}$
Prenons un automorphisme de la Courbe E de la forme
E (K) $\longmapsto$ E (K) ; (x , y) $\longmapsto$ (u^2 x , u^3 y) avec u$\neq$ 0 (2)

Les formules d'isomorphisme liant les coefficients a_i et b_i impliquent les égalités
$u^4 A = A$, et $u^6 B = B$ (3)

1) l'hypothèse j (E) $\neq$ 0, 1728 implique AB $\neq$0 .
(4)
(3) et (4) impliquent 2 solutions u = $\pm$ 1.
Il en résulte 2 automorphismes de E ; donc le groupe Aut (E) est d'ordre 2 .

2) Soit $j(E) = 1728$, alors $A \neq 0$ et $B = 0$. (5)
(3) et (5) impliquent l'équation $u^4 = 1$.
Il en résulte 4 automorphismes de E ; donc le groupe Aut (E) est d'ordre 4 .

3) Soit $j(E) = 0$, alors $A = 0$ et $B \neq 0$.
(6)
(3) et (6) impliquent l'équation $u^6 = 1$.
Il en résulte 6 automorphismes de E ; donc le groupe Aut (E) est d'ordre 6 .

4) Soit une Courbe Elliptique E d'équation de Weierstrass
$E : y^2 = x^3 + a_4 x + a_6 \in K[x, y]$ (7)
définie sur une corps K de caractéristique 3 et d'invariant modulaire $j(E) = 0$ avec $a_4 a_6 \neq 0 \bmod 3$.

L'équation (7) est préservée par l'automorphisme :

$$E(K) \longmapsto E(K), (x, y) \longmapsto (u^2 x + r, u^3 y). \quad (8)$$

Les formules d'isomorphisme (Isom 1) impliquent les 2 équations
$u^4 a_4 = a_4$ et $u^6 a_6 = a_6 + r a_4 + r^3$ (9)

Les automorphismes de E sont déterminés par les couples (u, r) tels que
$u^4 = 1$ et $a_6 (u^6 - 1) = r a_4 + r^3$ (10)

u engendre un groupe cyclique C_4 d'ordre 4 et r engendre un groupe cyclique C_3 d'ordre 3

Les automorphismes de E forment un groupe Aut(E) isomorphe au produit de groupes $C_3 \times C_4$; il est d'ordre 12.

5) Je choisis une Courbe Elliptique E d'équation de Weierstrass

$$E : y^2 + a_3 y = x^3 + a_4 x + a_6 \in K[x, y] \quad (11)$$

sur un corps K de caractéristique 2 et d'invariant modulaire $j(E) = 0$
avec $a_3, a_4, a_6 \neq 0 \bmod 2$.

L'équation (11) est préservée par l'automorphisme

$$E(K) \longmapsto E(K), (x, y) \longmapsto (u^2 x + s^2, u^3 y + u^2 s x + t), u, s, t \in K, u \neq 0 \quad (12)$$

Les formules (Isom1) d'isomorphisme impliquent

$$u^3 a'_3 = a_3 ;$$
$$u^4 a'_4 = a_4 + s a_3 + s^4 ;$$
$$u^6 a'_6 = a_6 + s^2 a_4 + t a_3 + s^6 + t^2 ; \quad (13)$$

Les automorphismes de la Courbe E sont déterminés par les triplets (u , s , t) tels que :

$$u^3 = 1, \; s^4 + s = 0 \quad \text{et} \quad t^2 + t + s^3 + s^2 = 0$$

Il y a 3 valeurs u qui forment un groupe cyclique C(3) d'ordre 3, 4 valeurs s qui forment un groupe cyclique C(4) d'ordre 4 et 2 valeurs t qui forment un groupe cyclique C(2) d'ordre 2

Le groupe produit C(4) C(2) , d'ordre 8 est isomorphe au groupe H (8) des quaternions

Nous en déduisons que le groupe Aut (E) est d'ordre 24 , isomorphe au groupe produit H (8) C (3)

Application à la famille E (t)

1) Soit la Cubique E(5) de la famille E (t) :

$E(5) : y^2 + 5xy + 5y = x^3 + 10x \in \mathbb{Q}[x, y]$;

Calcul des invariants

$c_4 = -455$; $\Delta(E) = -5686 \times 5^5$ et $j(E) = \frac{91^3}{5^2 \times 5686} \neq 0$ et $\neq 1728$.

Il en résulte le groupe Aut (E(5)) est d'ordre 2 .

Soit un corps K de caractéristique 13, .$K = \mathbb{Z}/13\mathbb{Z}$.

Les invariants de E (5) sont égaux à :

$$c_4 = 0 , \Delta(E) = +1 \text{ et } j(E) = \frac{7^2 \times 13^2}{5^2 \times 5686} = 0$$

IL en résulte que.

Aut (E (5)) est d'ordre 6 sur le corps fini $\mathbb{Z}/13\mathbb{Z}$

2) Soit la Cubique E (-2) de la famille E (t)

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

Calcul des invariants de E (- 2) :

$c_4 = 112$, $\Delta(E) = -419$, $j(E) = \frac{c_4^3}{\Delta(E)}$;

Sur un corps de caractéristique 2 , $c_4 = 0$ et $\Delta(E) \neq 0$.

Il en résulte que le groupe Aut (E (- 2)) est d'ordre 24 . Ce groupe est isomorphe au groupe produit H (8) C (4) .

6 Isogénies des Courbes Elliptiques

Dans l'ensemble des morphismes de Courbes Elliptiques, il existe des morphismes particuliers

E (K) $\longmapsto$ E' (K) classés dans la classe des isogenies de Courbe Elliptique

Définition 6 : *d'après [25]*

Soit 2 Courbes Elliptiques E et E' sur le même corps K, d'éléments neutres respectifs O_E et $O_{E'}$, de groupes de Mordell – Weil E(K) et E' (K)

Une isogénie de E sur E' est un homomorphisme $\lambda : E(K) \longmapsto E'(K)$ qui satisfait les conditions :

1) $\lambda (O_E) = O_{E'}$
2) $\lambda \neq 0$
3) *λ est surjectif*
4) *Le noyau de λ est un sous groupe fini du groupe E (K)*
5) $\lambda (P + R) = \lambda (P) + \lambda (R)$ *pour tous points P et R de E (K)*

Par la théorie des morphismes de variétés, les conditions (1) , (2) , (3) et (4) sont équivalentes.

Une telle isogénie est caractérisée par un invariant**.**

Définition 7

Le degré de l'isogénie λ est égal au degré du noyau de l'isogénie ; card ker λ = degré de λ

A toute isogénie non nulle de degré m : $\lambda : E_1 \longmapsto E_2$ on associe l'isogénie duale $\tilde{\lambda}$

$\tilde{\lambda} : E_2 \longmapsto E_1$

Les 2 composées satisfont les relations .

$\tilde{\lambda} \circ \lambda : E_1 \longmapsto E_1$ est la multiplication par m sur la courbe E_1

$\lambda \circ \tilde{\lambda} : E_2 \longmapsto E_2$ est la multiplication par m sur la courbe E_2

Proposition 10

Soit une Courbe Elliptique E et un sous groupe fini F de degré d de E. Alors il existe une seule isogénie

$\lambda : E \longmapsto E$ *de degré d.*

Preuve

Soit une Courbe Elliptique E, un sous groupe fini F de E et le point à l'infini O_E de E (K).
Alors il existe un homomorphisme non nul

$$\lambda : E(K) \longmapsto E(K)$$

qui satisfait : $\lambda (O_E) = O_E$, $\lambda (E(K)) \neq \{ O_E \}$ et ker λ = F .
C'est la définition d'une isogénie de Courbes Elliptiques.
□

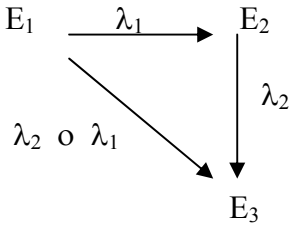
Proposition 11

Soient 3 Courbes Elliptiques E_1 / K, E_2 / K et E_3 / K et 2 isogénies de Courbes Elliptiques
$\lambda_1 : E_1 \longmapsto E_2$ *et* $\lambda_2 : E_2 \longmapsto E_3$;
alors la composée $\lambda_2 \, o \, \lambda_1 : E_1 \longmapsto E_3$ *est une isogénie de Courbes Elliptiques*

Preuve :
Soient 3 Courbes Elliptiques E_1 / K , E_2 / K , E_3 / K et 2 isogénies

$$\lambda_1 : E_1 \longmapsto E_2 \quad \text{et} \quad \lambda_2 : E_2 \longmapsto E_3$$
$$F \longmapsto \lambda_1 (F) \qquad G \longmapsto \lambda_2 (G)$$

D'après la théorie des groupes, la composée λ_2 o λ_1 des deux morphismes λ_1 et λ_2 est un morphisme de groupe



Soient les points à l'infini O_i , i = 1, 2 , 3 des 3 Courbes Elliptiques E_i .

Calculons les images des composées :

$$\lambda_2 \text{ o } \lambda_1 (O_1) = \lambda_2 (O_2) = O_3 .$$

Calculons les noyaux des isogénies .

$$\text{Ker } \lambda_1 = \{ P_1 / P_1 \in E_1 , \lambda_1 (P_1) = O_2 \}$$
$$= F_1 \subset E_1 .$$

$$\text{Ker } \lambda_2 = \{ P_2 / P_2 \in E_2 , \lambda_2 (P_2) = O_3 \}$$
$$= F_2 \subset E_2 ,$$

$$\text{Ker } (\lambda_2 \text{ o } \lambda_1) = \{ T \in E_1 / \ (\lambda_2 \text{ o } \lambda_1 (T) = O_3 \}$$
$$= F_3 \subset E_1$$

$\lambda_1 (E_2) = E_3$ pour λ_2 non nul, λ_2 est surjectif

Donc λ_2 o λ_1 non nul , λ_2 o $\lambda_1 (E_1) = E_3$ et λ_2 o λ_1 est surjectif,
il en résulte que λ_2 o λ_1 est une isogénie

□

Soit une Courbe Elliptique E d'équation de Weierstrass :

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_6 x + a_6 \in \mathbb{Q} [x , y] \qquad (1)$$

et le polynôme à 2 variables

$$g (x, y) = = x^3 + a_2 x^2 + a_6 x + a_6 - y^2 - a_1 xy - a_3 y \in \mathbb{Q} [x , y]. \qquad (2)$$

Pour déterminer l'équation de la Courbe Elliptique isogène, nous utilisons l'algorithme de VELU, CRAS, Paris, C.273 (26 Juillet 1971) p 238 -241.

Soit F [2] le sous groupe de F des points d'ordre 2 du groupe de Mordell- Weil E ($\mathbb{Q}$) :

$$F[2] = \{ P \in E(\mathbb{Q}) / 2P = O_E \} \quad (1)$$

Soit H une partie du groupe

$$F - O_E - F[2]$$

et – H l'ensemble des symétriques des points de H vérifiant les deux relations

$$H \cup (- H) = F - O_E - F [2] \quad \text{et} \quad H \cap (- H) = \varnothing ; \quad (2)$$

Posons $J = F [2] \cup H$. (3)

A tout point $P = (x, y) \in E(\mathbb{Q})$ associons les dérivées partielles

$$\begin{cases} g'_x (P) = = 3 x^3 + 2 a_2 x^2 + a_6 - a_1 y \ ; \\ g'_y (P) = - 2 y - a_1 x - a_3 ; \end{cases} \quad (4)$$

et les polynômes

$$h (P) = \begin{cases} g'_x (P) \quad \text{si } P \in F [2] ; \\ 2 g'_y (P) – a_1 g'_y (P) = 6 x^2 + b_2 x + b_4 \text{ si } P \notin F [2] . \end{cases} \quad (5)$$

avec $b_2 = 4 a_2 + a_1^2$, $b_4 = 2 a_4 + a_1 a_3$;

$$\text{Posons } i (P) = \left[g'_y (P) \right]^2 = 4 x^3 + b_2 x^2 + 2b_4 x + b_6 . \quad (6)$$

$$h (J) = \sum_{p \in J} h (P) \text{ et } i (J) = \sum_{p \in J} i (P) . \quad (7)$$

Alors l'isogénie f de noyau J a pour équation :

$$X = x + \sum_{P \in J} \left(\frac{h (P)}{x - x_P} + \frac{i (P)}{(x - x_P)^2} \right)$$

$$Y = y - \sum_{P \in J} \left(i (P) \frac{2y + a_1 x + a_3}{(x – x_P)^3} + h(P) \frac{a_1 (x – x_P) + y – y_P}{(x – x_P)^2} + \frac{a_1 i(P) – g'_x (P) – g'_y(P)}{(x – x_P)^2} \right)$$

Exemple de Velu :

Cubique de Weierstrass

$$E : y^2 + x\,y + y = x^3 - x^2 - 3\,x + 3 \in \mathbb{Q}[x, y] .$$

Calcul des invariants de E .

$b_2 = -3$; $b_4 = -5$; $b_6 = 13$; $b_8 = -16$; $\Delta(E) = 2561$.

$\Delta(E) > 0$ implique que cette cubique est une Courbe Elliptique .

Le groupe $E(\mathbb{Q})$ contient un sous groupe F d'ordre 7.
F = { R = (1, 0) ; 2R = (-1 , -2) ; 3R = (3 , -6) ; 4R = (3 , 2) ; 5R = (-1 , 2) ; 6R = (1, -2) et $7R = O_E$ } .

Après calcul des nombres de l'algorithme, on obtient l'équation de la Courbe Elliptique isogène E' à E dans l'isogénie

$\lambda : E \longmapsto E'$ de noyau F .

$E' = E/F : y^2 + x\,y + y = x^3 - x^2 - 213\,x - 1257$.

□

Théorème *[Velu]*
Soit E/K une Courbe Elliptique d'équation de Weierstrass .

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_6 x + a_6 \in \mathbb{Q}[x, y]$$

$$h(P) = \begin{cases} g'_x(P) \quad si\ P \in F\ [2]; \\ 2\,g'_y(P) - a_1 g'_y(P) = 6x^2 + b_2 x + b_4 \ si\ P \notin F\ [2] . \end{cases}$$

$$i(P) = \left[g'_y(P) \right]^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6 .$$

$$h(J) = \sum_{p \in J} h(P) \ et\ i(J) = \sum_{p \in J} i(P) .$$

Soit F un sous groupe fini du groupe E , alors la Courbe Elliptique E' isogène à E a pour équation

$$E' : y^2 + A_1 xy + A_3 y = x^3 + A_2 x^2 + A_4 x + A_6 \in \mathbb{Q}[x, y] \qquad (8)$$

avec $A_1 = a_1$, $A_2 = a_2$, $A_3 = a_3$, $A_4 = a_4 - 5\,h(J)$, $A_6 = a_6 - b_2 h(J) - 7\,i(J)$

□

Chapitre 3 Groupe Modulaire et Points de Heegner

1 Groupe Modulaire SL (2, $\mathbb{Z}$)

Pour décrire les points de Heegner d'une Courbe Elliptique, il faut connaître le groupe modulaire, les formes modulaires, les Courbes Modulaires X_0 (N) de niveau N.

Définition 1 :
Le groupe modulaire est le groupe spécial linéaire des 2 x 2 matrices à termes entiers rationnels et de déterminant égal à 1.

$$SL(2,\mathbb{Z}) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \; ; a, b, c, d \in \mathbb{Z} \; ; ad - bc = 1 \right\} \quad (1)$$

Le groupe modulaire est un sous groupe de groupes spéciaux linéaires sur les corps $\mathbb{Q}$, $\mathbb{Q}(\theta)$, $\mathbb{R}$, $\mathbb{C}$.

$$SL(2,\mathbb{Z}) \subset SL(2,\mathbb{Q}) \subset SL(2,K) \subset SL(2,\mathbb{R}) \subset SL(2,\mathbb{C}) \quad (2)$$

Ce groupe modulaire opère sur le demi plan supérieur de Poincaré :

$$\mathbb{H} = \{ x + iy \in \mathbb{C} \; ; y > 0 \} . \quad (3)$$

et sur le complété de ce demi plan

$$\mathbb{H}^* = \mathbb{H} \cup \{ \mathbb{Q} \} \cup \{ \infty \} . \quad (4)$$

Cette opération se fait avec la transformation de Mobius

$$Az = \frac{a z + b}{c z + d} \text{ pour } A = \begin{pmatrix} a & b \\ b & d \end{pmatrix} \text{ de (1) ;} \quad (5)$$

Le groupe modulaire contient des matrices particulières :

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \text{matrice unité , } S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ et } T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad (6)$$

Déterminons les actions de ces matrices sur le demi plan supérieur de Poincaré :

$$I_2 z = z , \quad Sz = -\frac{1}{z} \quad \text{et} \quad Tz = z + 1 \quad (7)$$

Définition 2

1) La transformation S est l'involution $W : Wz = -\frac{1}{z}$,

2) La transformation T est la translation $Tz = z + 1$.

La structure algébrique du groupe modulaire SL (2, $\mathbb{Z}$) dépend des matrices S et T

Proposition1

Le groupe modulaire SL(2, Z*) est un groupe multiplicatif , non abélien , infini ; engendré par les 2 matrices*

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ d'ordre 4 et } \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ d'ordre infini .}$$

Toute matrice A de SL (2 , $\mathbb{Z}$*) est un produit de la forme*

$$A = T^{n1} S^{n2} T^{n3} \ldots . T^{nk} , n_i \in \mathbb{N}$$

Cette représentation n'est pas unique.

Preuve

Calculons les puissances de S et T :

$S^2 = - I_2$, $S^3 = - S$ et $S^4 = I_2$.

$$T^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} ; \quad T^3 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \text{ et } T^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \text{ pour k = 4, 5, 6 ….}$$

Calculons les produits ST et TS :

$$ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} , \quad TS = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \text{ donc } ST \neq TS .$$

□

Exemple tiré de [1]

$$A = \begin{pmatrix} 4 & 9 \\ 11 & 25 \end{pmatrix} = ST^{-3} ST^{-4} ST^2$$

Pour obtenir une autre forme, il faut calculer des produits $ST^k S$, $T^k S T^k$, …..
Le groupe modulaire SL (2 , $\mathbb{Z}$) contient des sous groupes particuliers : les sous groupes modulaires de congruence.

Définition 3
Les sous groupes modulaires de congruence de niveau $N \geqslant 1$ sont de 3 types

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}),\quad c \equiv 0 \mod N \right\}; \qquad (1)$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z});\ c \equiv 0 \mod N \text{ et } a \equiv d \equiv 1 \mod N \right\}; \qquad (2)$$

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}),\ a \equiv d \equiv 1 \mod N \text{ et } b \equiv c \equiv 0 \mod N \right\}; \qquad (3)$$

Tout sous groupe Γ de SL (2, $\mathbb{Z}$) contenant $\Gamma(N)$ est un sous groupe de congruence, d'aprés [26]

Le groupe SL (2 , $\mathbb{Z}$) contient la matrice unité I_2 et son opposée $-I_2$; l'ensemble $\{ \pm I_2 \}$ est un groupe d'ordre 2

Définition 4
Le groupe quotient $SL(2, \mathbb{Z}) / \{ \pm I_2 \} = PSL(2, \mathbb{Z})$ est le groupe projectif spécial linéaire .

2 - Fonctions modulaires et formes modulaires

Elles sont construites avec les matrices $A \in SL(2, \mathbb{Z})$.

Définition 5
Soit un sous groupe de congruence Γ de niveau N du groupe modulaire SL (2, $\mathbb{Z}$) , le demi plan supérieur $\mathbb{H}$ de Poincaré et un entier $k \geqslant 1$:

1) *Une fonction modulaire de poids k pour le sous groupe Γ est une fonction méromorphe en chaque point parabolique de $\mathbb{H} / \Gamma$*
   $$f : \mathbb{H} \longrightarrow \mathbb{C}$$
   qui satisfait la relation
   $$f(Az) = (cz + d)^k f(z),$$
   pour toute matrice A de Γ .

2) *Une forme modulaire de poids k pour Γ est une fonction modulaire holomorphe sur $\mathbb{H}$ et sur les points paraboliques de l'espace $\mathbb{H}^*/\Gamma$.*

3) *Une forme parabolique est une forme modulaire qui s'annule en tout point parabolique de l'espace $\mathbb{H}^*/\Gamma$.*

Pour plus de détails , consulter [25] et [26]

Exemples

1) Une forme modulaire f admet un développement de Fourier en la variable

$$q = \exp 2\Pi iz$$

de la forme

$$f(z) = \sum_{n = n_0}^{\infty} c(n)\, q^n \quad , \text{ pour un certain entier } n_0 = n_0(f)$$

Lorsque $n_0 = 0$, la fonction f est une forme modulaire .
Lorsque $f(\infty) = 0$, f est une forme modulaire parabolique.

2) La fonction discriminant

$$\Delta(z) = (2\Pi)^{12} \sum_{n=1}^{\infty} \tau(n)\, q^n \quad ,$$

est une forme parabolique de poids 12

$\tau(n)$ est la fonction arithmétique Tau : $\tau(1) = 1$ et $\tau(n) \in \mathbb{Z}$;

détails dans [1].

3) Fonction Eta de Dedekind

$$\eta(z) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n)$$

4) La fonction $f(z) = \eta(z)^2\, \eta(11z)^2$ est une forme parabolique de poids 2 pour le sous groupe modulaire $\Gamma_0(11)$.

5) Séries d'Eisenstein , [1].

Ce sont les séries de la forme

$$G_{2k}(z) = \sum (m + nz)^{-2k} ,$$

Pour les entiers m et n premiers entre eux, $(m, n) \neq (0, 0)$ et $z \in \mathbb{H}$, $k \geq 2$.

Ces séries sont fonction de la fonction Zêta de Riemann, $\zeta(s)$ et de la somme $\sigma_k(n)$ des puissances k^e des diviseurs de n

$$G_{2k}(z) = 2\,\zeta(2k) + \frac{2(2\Pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)\,q^n ,$$

pour les entiers $k \geqslant 2$ et $q = \exp(2\Pi i z)$.

Les formes modulaires sont classifiées suivant leur poids par la :

Proposition 2

1) *Les seules formes modulaires de poids k = 0 sont les fonctions constantes ;*
2) *Pour k < 0, pour k impair et pour k = 2, la seule forme modulaire de poids k est la fonction nulle ;*
3) *Toute forme modulaire entière, non constante, a un poids pair k = 2k' ⩾ 4 ;*
4) *La seule forme modulaire parabolique k < 12 est la fonction nulle ;*

Preuve

Cela provient des définitions des formes modulaires.

Détails dans (Théorème 6 -2 – Apostol -1)

□

L'ensemble des formes modulaires de poids k est un espace vectoriel complexe M_k de dimension égale à :

dim M_k = [k/12] si $k \equiv 2 \bmod 12$, pour [k/12] = partie entière de l'entier rationnel k/12

= [k/12] + 1 si $k \not\equiv 2 \bmod 12$.

Ainsi , dim $M_k = 1$ si k = 4, 6, 8 , 10 et 14

L'ensemble M'_k des formes paraboliques modulaires est un sous espace vectoriel de l'espace M_k de dimension.

$$\text{Dim } M'_k = \dim M_{k-12}$$

Ainsi , dim $M'_k = 1$ pour k = 12 ; 16 ; 18 ; 20 ; 22 et 26 , d'après [1]

Hecke a déterminé des formes modulaires particulières et des opérateurs linéaires sur les espaces vectoriels M_k de formes.

Définition 6 *[Apostol]*
L'opérateur de Hecke T_n est la fonction

$$T_n : M_k \longrightarrow M_k$$

de valeur

$$(T_n f)(z) = n^{k-1} \sum_{d} d^{-k} \sum_{b=0}^{d-1} f\left(\frac{nz + bd}{d^2}\right)$$

pour tous les diviseurs $d > 1$ de n.
Pour les nombres premiers p cette formule devient

$$(T_p f)(z) = p^{k-1} f(pz) + \frac{1}{p} \sum_{b=0}^{p-1} f\left(\frac{z+p}{p}\right) ;$$

dans cette définition le poids k est un entier pair ;

Cet opérateur satisfait les relations, où $T_n = T(n)$:

1) $T(m)T(n) = T(n)T(m)$ pour tous entiers m et n ;
2) $T(m\,n) = T(m)\,T(n)$ si m et n sont premiers entre eux;
3) $T(p^{r+1}) = T(p^r)\,T(p) - p^{r-1}\,.\,T(p^{r-1})$ pour tout nombre premier p.

Cet opérateur de Hecke $T_n = T(n)$ est utilisé dans l'étude des formes modulaires.

3- Points de Heegner

Selon [2] , Birch a décrit quelques années auparavant un algorithme essentiellement dû à Heegner , pour construire des points rationnels non triviaux sur certaines Courbes Elliptiques.

Ces Courbes Elliptiques particulières sont associées aux Courbes Modulaires

$$\mathbb{H}^* / \Gamma_0(N) = X_0(N)$$

$\mathbb{H}^*$ représente le demi plan supérieur $\mathbb{H} = \{ x + iy \in \mathbb{C} , y > 0 \}$ de Poincaré complété par l'ensemble $\mathbb{Q} \cup \{ \infty \}$,

$\Gamma_0(N)$ est le sous groupe de congruence modulaire de niveau $N > 1$

$$\Gamma_0(N) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} ; a , b, c , d \in \mathbb{Z} \quad c \equiv 0 \mod N \text{ et } ad - bc = 1 \right\}$$

Le lien de la Courbe Modulaire $X_0(N)$ avec des Courbes Elliptiques se trouve dans la

Proposition 3

Il existe, pour tout entier $N \geq 1$, une courbe projective lisse $X_0(N)$ ($\mathbb{C}$) et un isomorphisme analytique complexe .

$$j_N : \mathbb{H}^* / \Gamma_0(N) \longmapsto X_0(N)(\mathbb{C})$$

qui satisfait les conditions :

à tout nombre complexe $z \in \mathbb{H}^* / \Gamma_0(N)$ il correspond le corps $K = \mathbb{Q}(j_N(z))$ et une classe d'équivalence de Courbes Elliptiques E qui possèdent un sous groupe cyclique E (N) d'ordre N pour le groupe E (K).

Preuve : ' Théorème 13 -1 (a) dans [26] :

□

Le groupe Γ_0 (N) opère sur le demi plan supérieur $\mathbb{H}$ de Poincaré par la formule :

$$A\,z = \frac{az+b}{cz+d} \quad .$$

Dans la théorie des Courbes Elliptiques, j est l'invariant modulaire et $j_N(z) = j(N z)$.

L'involution est la fonction W_N de valeur

$$W_N(z) = -\frac{1}{Nz} .$$

Les invariants j et j_N satisfont une équation modulaire

$$F_N(j, j_N) = 0 .$$

Le polynôme $F_N(u, v) \in \mathbb{Z}[u, v]$ est l'équation d'une courbe algébrique plane Z_0 (N), cette courbe est liée à X_0 (N) par l'application

$$\theta : X_0(N) \longmapsto Z_0(N) , \theta(z) = (j(z), j(N z))$$

Si ω est nombre complexe quadratique, il est racine d'une équation quadratique

$$A\,\omega^2 + B\,\omega + C = 0 \quad .$$

pour des entiers A, B et C premiers entre eux et un discriminant $B^2 - 4AC = \Delta(\omega) < 0$.

Définition 8

Un nombre complexe ω est un point de Heegner de $X_0(N)$ si $\Delta(\omega) = \Delta(N\omega)$.

A un point z de X_0 (N) il correspond 2 Courbes Elliptiques:

$E = \mathbb{C}^* / (\mathbb{Z} \oplus z\mathbb{Z})$ et $E' = \mathbb{C} / (\mathbb{Z} \oplus NZ)$; ces Courbes Elliptiques sont N-isogènes et possèdent la même Multiplication Complexe.

Si ω est point de Heegner de X_0 (N) il satisfait une équation ;

$$NA'\omega^2 + B\omega + C = 0$$

où les 3 entiers NA' , B et C sont premiers entre eux et les 3 entiers A', B et NC sont aussi premiers entre eux.

Le nombre $W_N(\omega) = -1 / N\omega$ est aussi un point de Heegner.
Un point de Heegner ω de X_0 (N) est lié au corps $\mathbb{Q}(\omega , j(\omega))$. Ce corps est le corps de classes de l'anneau

$$R(\omega) = \mathbb{Z}\left[\frac{(\Delta + \sqrt{\Delta})}{2}\right] \text{ pour } \Delta = \Delta(\omega) = B^2 - 4AC < 0.$$

Les h classes de l'anneau R (ω) sont représentées par les h conjugués ω_1 , …, ω_h. Alors les éléments $j(\omega_1)$, …..$j(\omega_h)$ forment un ensemble complet de conjugués sur le corps $\mathbb{Q}(\omega)$.

Les points de Heegner de la courbe Z_0 (N) sont :

$$\{ (j(I_k), j(\mathcal{N}^{\circ} I_k)) , k = 1 , …., h , \text{avec Norm } \mathcal{N}I_k = N \}$$

Où les I_k sont des idéaux de R (ω) correspondant au ω_κ k = 1,...,h

La courbe X_0 (N) permet une paramétrisation de Weil d'une Courbe Elliptique E par une application

$$\Psi : X_0(N) \longmapsto E$$

de valeur $i\infty \longmapsto O_E = (\infty , \infty)$

L'involution $W_N(z) = -\frac{1}{Nz}$ induit une action sur la Courbe Elliptique E ($\mathbb{C}$) .

Il en résulte les points de Heegner de la Courbe Elliptique E /$\mathbb{Q}$; ce sont les images $\Psi(\omega)$:

$$\Psi(z) = \Psi(0) + O_E - \Psi(W_N(z))$$

pour tout point z de X_0 (N) .

Il existe plusieurs travaux de recherche sur les points de heegner

1) Birch, B , et Stephens , N portant sur la construction de points de Heegner sur la courbe E : $y^2 = x^3 - 1728 e^3$ (1983) et sur le calcul des points de Heegner (1984).

2) B.H. GROSS : " Heegner Points on X_O (N) _ Formes Modulars " (1984)

3) N . D . Elkies : " Heegner Points Computation "

4) H . DARMON :" Points de Heegner sur une courbe Elliptique E ($\mathbb{Q}$) "

5), Benedict H.GROSS et Don ZAGIER :
a) “ Points de Heegner et dérivées de fonctions L “
b) “Heegner points and derivates of L – series”

6) J. NEKOVAR : ‘On the p-adic height of Heegner Cycles “

Conclusion ;

Dans ma thèse je n’ai étudié que quelques éléments de la théorie des Courbes Elliptiques, dans la suite je me propose de faire des recherches sur d’autres parties : espaces homogènes et groupes associés , groupes de torsion et groupes de cohomologie , théorie d’IWASAWA et combinatoire .

BIBLIOGRAPHIE

1- **Tom M.APOSTOL = Modular Functions and Dirichlet Series in Number Theory-Second Edition-Springer – New-York – Berlin- London – Paris Graduate Texts in Mathematics 41 (2000) AMS =1101**

2- **B.J.BIRCH = Heegner Points of Elliptic Curves – Symposia Mathématica, Vol 15 (1975) p441-445**

3- **B.J.BIRCH; N.STEPHENS = Computation of Heegner Points Modular Forms, Rankin Ed.Chichester (1984) p13-41**

4- **J.W.CASSELS = Diophantine Equations With Special Reference to Elliptic curves – Journal London Mathematical Society 41 (1966) p193-291**

5- **Harvey COHN = A Classical Invitation to Algebraic Numbers and Class Fields – Springer Verlag New York Berlin (1980)**

8- **J.E.CREMONA = Algorithms for Modular Elliptic Curves 2nd Edition; Cambridge University Press (1997) United Kingdon**

9- **Benedict H.GROSS = Heegner Points on Xo (N) – Modulars Forms, Rankin Ed Chichester (1984) p87-105**

10- **Benedict H.GROSS et Don ZAGIER = Points de Heegner et dérivées de function L – Comptes Rendus Académie des Sciences de Paris t.297, (19 Septembre 1983) p85-87**

11- **Robin HARTSHORNE = Algebraic Geometry – Springer 1977 – Corrigé en 1983 – Graduate Texts in Mathematics 52 –AMS =13-xx, 14 A10,14 A15, 14Fxx, 14Hxx, 14Jxx**

12- **D.HUSEMOLLER = Elliptic Curves, Springer – Graduate Texts in Mathematics 111 (1987)**

13- **Shokichi IYANAGA = The Theory Of Numbers – North – Holland Publishing Company – Amsterdam – Oxford, American Elsevier Publishing Company , Inc New-York (1977)**

14- **A.W.KNAPP = Elliptic Curves – Mathematical Notes 40, Princeton University Press (1992)**

15- **Neal KOBLITZ = (1) Introduction to Elliptic Curves and Modular Forms – 2nd Ed (2000) Graduate Texts in Mathematics 97 (2) A course in Number Theory and Cryptography 2nd - Graduate Texts in Mathematics 114 (1988)**

17- **Jean Pierre LAFON = Les formalismes fondamentaux de l'Algèbre Commutative – Hermann – Paris (1974)**

18- Serge LANG (1) = Algebra 2nd Ed Addison Wesley – New York (1984)
(2) Elliptic Curves Diophantine Analysis – Springer (1972)
(3) Elliptic Functions, 2nd Springer (1987)

21- Barry MAZUR = Rational Isogeny of Prime Degree; Inventiones Mathematicae 44(1978) p 129-162

22- Andrew OGG = Modular Forms and Dirichlet series – W.A Benjamin, Inc., New York, Amsterdam (1969)

23- Jean Pierre SERRE = Propriétés galoisiennes des points d'ordre fini des courbes Elliptiques – Inventiones Mathematicae 15 (1972) p 259-331

24- I.R.SHAFAREVICH = Basic Algebric Geometry, Springer, Verlag (1977)

25- Goro SHIMURA = Introduction to the Arithmetic Theory of Automorphic Functions – Princeton University Press (1971)

26- Joseph H.SILVERMAN = The Arithmetic of Elliptic Curves – Graduate Texts in Mathematics 106 (1986) Springer; AMS =1401, 14G99, 14H05, 14H251, 14K15

27- John TATE = The Arithmetic of Elliptic Curves – Inventiones Mathematicae 23 (1974) p 179-206

28- André WEIL = (1) Sur un théorème de Mordell – Bulletin Sciences Mathématique 5-6 Paris (1930) p487-495
(2) Dirichlet series and Automorphic forms – Lecture Notes in Mathematic 189, Springer Verlag (1971)
(3) Courbes Algébriques et Variétés Abéliennes, Herman, Paris (1974)

29 - Edwin WEISS = Algebraic Number Theory – Mc Graw – Hill; Book Company, Inc New – York ; London (1970)

30- M- ZITOUNI = Courbes Elliptiques; Géométrie- Arithmétique - Algorithmique (2007) OPU - Alger

31- Noam D.Elkies = Heegner point computation, pages 122-133 in Algorithmic Number Theory (Ithaca . NY, 1994 , L M Adleman and M.D Kuang eds Lecture Notes in Computation of Science Algorithmic Number Theory N° 877 (1994).

32- Colloque "Théorie d'Iwasawa 2006 –Limoges

1) **Ye TIAN (Montéal – Canada) = Heegner Points over Elliptic Curve E /ℚ .**
2) **Henri DARMON = Points de Heegner sur une Courbe Elliptique E (ℚ) pour la FTC – extension associée à 2 nombres premiers p et q**