

N° d'ordre : 32 / 2008 – M / MT.

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA
RECHERCHE SCIENTIFIQUE
UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE
HOUARI BOUMEDIENE
FACULTE DE MATHEMATIQUES



MEMOIRE

Présenté pour l'obtention du diplôme de MAGISTER

En : MATHEMATIQUES

Spécialité : Algèbre et Théorie des Nombres

par AZZOUNI Faïza

Sujet

Points d'ordre fini et isogénies de Courbes Elliptiques

Soutenue publiquement le : 25/06/2008, devant le jury composé de :

Mr AIDER Meziane	Professeur l'U.S.T.H.B	Président
Mr ZITOUNI Mohamed	Professeur l'U.S.T.H.B	Directeur de thèse
Mr HERNANE Mohand Ouamar	Maître de conférence l'U.S.T.H.B	Examineur
Mr BENSEBAA Boualem	Chargé de cours l'U.S.T.H.B	Invité

Dédicaces

Je tiens à dédier ce travail à :

Mes chers parents qui m'ont toujours soutenu.

Mes frères

Mes neveux et nièces

Remerciements

En premier lieu, je tiens à remercier ma famille surtout mon père et ma mère, qui m'ont soutenu, dans tous les sens de terme, pour que je concrétise ce travail. Mes remerciements s'adressent très vivement à mes frères, Saad, Mohamed, Yazid, Toufik, Kheireddine et ma belle sœur Fadila.

Ce travail de thèse a été effectué sous la direction du Professeur Mohamed ZITOUNI à qui je tiens à exprimer ici ma profonde reconnaissance pour m'avoir fait confiance, et pour m'avoir dirigé pendant ces années. Je tiens tout particulièrement à le remercier pour la richesse de ces idées et de ces conseils et pour m'avoir fait profiter de ses vastes connaissances, sa rigueur, sa créativité ainsi que ses qualités humaines qui m'ont énormément appris.

J'adresse mes sincères remerciements au professeur M. AIDER de m'avoir fait l'honneur de présider mon jury.

Je remercie Mr M. HERNANE, Mr B. BENSEBAA d'avoir fait partie de mon jury et l'intérêt qu'ils ont bien voulu porté à ce travail.

Enfin, mon plus vif remerciement va à mes amies Nassima, Aichouche, Warda et Louiza pour leur aide et leurs conseils.

Sommaire

Introduction.....	II
--------------------------	-----------

Chapitre I : Variétés abéliennes .

1. Introduction	1
2. Variétés affines	1
3. Variétés projectives	2
4. Variétés abéliennes	4
5. Courbes projectives	4
6. Diviseurs d'une courbe projective	5

Chapitre II : Géométrie des courbes elliptiques .

1. Courbes algébriques planes.....	8
2. Transformations de l'équation de Weierstrass	9
3. Invariants d'une cubique de Weierstrass	10
4. Discriminant d'un polynôme et résultant de 2 polynômes...	13
5. Classification des cubiques de Weierstrass par leur discriminant.....	16

Chapitre III : Groupe de Mordell-Weil d'une courbe elliptique .

1. Structure de groupe abélien.....	25
2. Calcul des coordonnées du symétrique d'un point et de la somme de 2 points	26
3. Points d'ordre fini et sous groupes de torsion d'une courbe elliptique.....	28
4. Application aux familles de courbes elliptiques à 2 paramètres $E(s,t)$	36

Chapitre IV : Morphismes de courbes elliptiques .

1. Isomorphismes de courbes elliptiques.....	38
2. Isogénies de courbes elliptiques	41
3. Méthode de Vélu	44

Bibliographie.....	54
---------------------------	-----------

Introduction

En 1998, A.Nitaj [8] a décrit des méthodes qui permettent de déterminer des Courbes Elliptiques ayant un rapport de Szpiro σ assez grand.

Il a construit des familles de Courbes Elliptiques $E(s,t)$ qui dépendent de 2 paramètres s et t pour lesquels le point $P_0=(0,0)$ est un point de torsion d'ordre $m = 2,3,4,5,6,7$ ou 8 .

Il a déterminé ensuite toutes les courbes isogènes de chaque Courbe Elliptique.

Nous nous intéressons dans cette thèse aux familles de Courbes Elliptiques d'équations de Weierstrass :

$$E_1(s,t) : y^2 = x(x^2 + 2(s+t)x + (s-t)^2) ;$$

$$E_2(s,t) : y^2 = x(x^2 + sx + t) ;$$

$$E_3(s,t) : y^2 = x(x-s)(x-t).$$

Le chapitre I est consacré à quelques notions de la Géométrie Algébrique :

Variétés Affines, Variétés Projectives, Variétés Abéliennes, Courbes Algébriques, Courbes Projectives, diviseurs d'une Courbe Projective..

Dans le chapitre II, nous présentons quelques résultats importants sur le discriminant d'un polynôme et le résultant de 2 polynômes. Nous indiquons des notions de base de la théorie des cubiques de Weierstrass. Nous terminons le chapitre par un exemple de chaque classe apparaissant dans la classification des cubiques de Weierstrass.

Dans le chapitre III, nous construisons le groupe de Mordell-Weil $E(K)$ d'une Courbe Elliptique sur un corps K . Nous en étudions les points et les sous groupes de torsion.

Le chapitre IV est consacré à l'étude des morphismes des Courbes Elliptiques. Nous utilisons des résultats de la théorie des isogénies des Courbes Elliptiques.

Nous décrivons l'algorithme de Vélu [13] pour déterminer l'équation d'une isogénie.

Nous terminons le chapitre en appliquant cet algorithme aux familles de Courbes Elliptiques dépendant de 2 paramètres s et t de Nitaj [8].

Chapitre I

Variétés Abéliennes

1. Introduction :

Selon plusieurs auteurs (Shimura, Tate, Hartshorne, Silverman, etc ...) :
une courbe elliptique a une structure de variété abélienne . Donc la théorie des courbes elliptiques utilise les notions qui sont du domaine de la Géométrie Algébrique .
Une variété algébrique, sur un corps commutatif K , peut être munie de plusieurs structures : affines, projectives, abéliennes, complètes, rationnelles, etc...

2. Variétés affines :

Ce sont des sous espaces particuliers des espaces affines .

Définition 1 : Un n -espace affine, sur un corps commutatif K , est l'ensemble des n -uples $(a_1, a_2, \dots, a_n) = a$ d'éléments de K :

$$A^n(K) = \{ (a_1, a_2, \dots, a_n) = a, \text{ avec } a_1, a_2, \dots, a_n \in K \} \quad (1)$$

Dans le vocabulaire géométrique, le n -uplet a est un point du n -espace affine A^n ,

les éléments $a_1, \dots, a_n \in K$ sont les coordonnées affines du point a .

Donc il y a des lignes et des surfaces sur cet espace .

Cet espace est de dimension n sur le corps K .

A ce n -espace affine nous associons l'anneau $K[x_1, \dots, x_n]$ des polynômes à n indéterminées $x_1, \dots, x_n$.

Tout polynôme $f(x) \in K[x]$ de degré n admet n zéros dans une clôture algébrique du corps K (théorème de d'Alembert-Gauss) .

Définition 2 : Un ensemble algébrique dans le n -espace affine $A^n(K)$ est l'ensemble des zéros d'une famille $T = \{f_1, \dots, f_t\}$ de polynômes $f_1, \dots, f_t \in K[x_1, \dots, x_n]$:

$$Z(T) = \{a \in A^n ; f_i(a) = 0 \text{ pour tout } f_i \in T\}$$

Exemple :

Dans le 2-espace affine $A^2(\mathbb{R})$, le polynôme $f(x,y) = 2x^2 - y^2 - 1$ est l'équation d'une hyperbole ; donc l'ensemble $Z(f) = \{(x,y) \in \mathbb{R}^2, f(x,y) = 0\}$ des zéros du polynôme f est un ensemble algébrique .

Un n -espace affine $A^n(K)$ peut être muni d'une topologie spéciale : la topologie de Zariski. Dans cette topologie les fermés sont les sous ensembles algébriques, les ouverts sont les complémentaires des ensembles algébriques. Cette topologie satisfait les axiomes d'une topologie usuelle.

Définition 3 :

- 1) Une variété algébrique affine est une partie fermée et irréductible d'un espace affine.
- 2) Une variété algébrique quasi affine est une partie ouverte d'une variété affine.

Dans la suite, toutes les variétés algébriques seront désignées par le nom de variétés.

3. Variétés projectives :

Dans un $(n+1)$ -espace affine $A^{n+1}(K)$ nous considérons la relation binaire $\mathcal{R}$:

$$a = (a_1, a_2, \dots, a_{n+1}) \mathcal{R} b = (b_1, b_2, \dots, b_{n+1})$$

si et seulement si a et b sont liés par les relations :

$$b_i = \lambda a_i, \text{ pour } i=1, 2, \dots, n+1 \text{ pour un élément } \lambda \text{ non nul du corps } K.$$

Cette relation binaire $\mathcal{R}$ satisfait les axiomes de réflexivité, de symétrie et de transitivité.

$\mathcal{R}$ est donc une relation d'équivalence sur le $(n+1)$ -espace affine $A^{n+1}(K)$.

Définition 4 : Un n -espace projectif est l'espace quotient

$$P^n(K) = A^{n+1}(K) \setminus \{0\} / \mathcal{R}$$

Muni de la topologie de Zariski , un n -espace projectif devient un espace topologique .

Définition 5 :

- 1) Une variété projective est une partie fermée et irréductible d'un espace projectif $P^n(K)$.
- 2) Une variété quasi projective est une partie ouverte d'une variété projective.

Il en résulte qu'un espace projectif est un ensemble de classes d'équivalences. Il n'y a pas de classe nulle par définition de la relation d'équivalence $\mathcal{R}$.

Exemple 1:

L'espace projectif $P^2(\mathbb{R})$ est l'ensemble des classes des points $P \in A^3(\mathbb{R}) - \{0\}$.

$$Cl(0,1,0) = \{(0,1,0), (0,2,0), \dots, (0,-1,0), \dots\}, \text{ classe du point } (0,1,0).$$

$$Cl(2,4,7) = \{(2,4,7), 2(2,4,7), -(2,4,7), 3(2,4,7), \dots\}, \text{ classe du point } (2,4,7).$$

$$Cl(0,0,1) = \{\lambda(0,0,1), \lambda \in \mathbb{R}, \lambda \neq 0\}, \text{ classe du point } (0,0,1).$$

$$Cl(a,b,c) = \{\lambda(a,b,c), \lambda \in \mathbb{R}, \lambda \neq 0\}, \text{ classe du point } (a,b,c).$$

Dans le plan cartésien Oxy , la classe $(0,1,0)$ représente la direction de l'axe Oy , le représentant $(0,1,0) = O_E$ est le point à l'infini.

Les coordonnées d'un point de l'espace projectif sont des coordonnées homogènes.

Les polynômes de l'espace projectif sont des polynômes homogènes.

Exemple 2:

$f(X,Y,Z) = X^4 - 2XYZ^2 + 5X^2Z^2 + 3Y^3Z$; c'est un polynôme homogène en X, Y, Z de degré 4 dans l'espace projectif $P^2(\mathbb{R})$.

Formules de passage du plan projectif $P^n(\mathbb{R})$ au plan affine $A^n(\mathbb{R})$:

Soit un point $P = (x_1, x_2, \dots, x_{n+1})$ du plan projectif $P^n(\mathbb{R})$.

Les coordonnées $x_1, x_2, \dots, x_{n+1}$ sont homogènes. En les divisant par l'une d'elles nous obtenons un point à n coordonnées.

Le passage du plan $P^n(\mathbb{R})$ au plan $A^n(\mathbb{R})$ s'obtient par l'application

$$(x_1, x_2, \dots, x_{n+1}) \rightarrow (x_1, \dots, x_n, 1)$$

Exemple 3:

Soit le polynôme $f(x,y,z,t) = 2x^6 - 3x^4y^2 + x^3yz^2 + 5y^2z^2t^2 + 6xyz t^3 + t^6$ de l'espace $P^3(\mathbb{R})$.

Le changement $(x, y, z, t) \rightarrow (x, y, z, 1)$ implique la valeur :

$$f(x, y, z, 1) = 2x^6 - 3x^4y^2 + x^3yz^2 + 5y^2z^2 + 6xyz + 1 = g(x, y, z).$$

C'est un polynôme affine dans l'espace $A^3(\mathbb{R})$.

Passage de l'espace affine $A^{n+1}(\mathbb{K})$ à l'espace projectif $P^n(\mathbb{K})$:

Il s'obtient avec 2 opérations :

Division par $x_{n+1} : A^{n+1}(K) \rightarrow K[x_1, \dots, x_{n+1}]$

$$(x_1, \dots, x_{n+1}) \rightarrow \left(\frac{x_1}{x_{n+1}}, \dots, \frac{x_{n+1}}{x_{n+1}} \right)$$

et l'opération de multiplication par x_{n+1}^d , $d = \text{degré du polynôme}$.

Exemple 4:

Soit un polynôme f d'équation dans l'espace affine $A^4(R)$:

$$f(x, y, z, t) = 2xyzt - y^2t^4 + 3z^3 - 4.$$

C'est un polynôme affine à 4 indéterminées, de degré 6.

Le polynôme f est transformé en un polynôme homogène $g(x, y, z, t)$ de degré 6 dans l'espace projectif $P^3(R)$:

$$g(x, y, z, t) = 2xyzt^3 - y^2t^4 + 3z^3t^3 - 4t^6.$$

4. Variétés abéliennes :

Une variété projective peut supporter une structure de groupe abélien.

Définition 6 :

Une variété abélienne est une variété projective A munie de 2 morphismes f et g :

$$f: A \times A \rightarrow A \text{ de valeur } f(a, b) = a + b, \text{ loi de groupe abélien}$$

$$\text{et } g: A \rightarrow A \text{ de valeur } g(a) = -a, \text{ symétrique pour cette loi.}$$

Exemple :

La variété projective A dans le plan $P^2(R)$, d'équation homogène et irréductible :

$$A: y^2z = x^3 + axz^2 + bz^3, \text{ est l'équation d'une cubique.}$$

Avec la loi de groupe $(P_1, P_2) \rightarrow P_1 + P_2$, cette cubique est une variété abélienne.

5. Courbes projectives :

Dans le plan projectif réel $P^2(R)$, une courbe projective est l'ensemble des zéros d'un polynôme homogène de degré $d \geq 1$,

$$C: f(X, Y, Z) = \sum_{d_i + d_j + d_k = d} c_{ijk} X^{d_i} Y^{d_j} Z^{d_k}$$

Les courbes C de degré 1 sont des droites.

Celles de degré 2 sont des coniques ou des cercles ou des produits de 2 droites.

Celles de degré 3 sont des cubiques ou des produits $C_1 C'_1 C''_1$ ou $C_1 C_2$,

C_i est une courbe irréductible de degré i .

Une courbe algébrique qui admet un point singulier est singulière.

Celle qui n'admet pas de point singulier est une courbe lisse.

Les courbes irréductibles peuvent être classifiées par un invariant ; le genre.

Définition 7 : le genre d'une courbe projective C , de degré d , qui admet s points singuliers, est l'entier non négatif :

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

Ainsi les droites, les cercles et les coniques sont des courbes algébriques de genre $g(C)=0$.

Les cubiques singulières C sont de genre $g(C)=0$.

Les cubiques non singulières C sont de genre $g(C)=1$.

Pour d'autres compléments sur ces courbes, consulter des ouvrages de Géométrie Algébrique :

" Algebraic Geometry " de R.Hartshorne ,...

6. Diviseurs d'une courbe projective :

La notion de diviseur des courbes algébriques est détaillée dans plusieurs ouvrages, par exemple dans [3] .

Considérons une courbe projective non singulière C , de degré d , dans le plan projectif $P^2(R)$ et une ligne variable L de ce plan .

Chaque ligne L coupe la courbe C en d points P_i distincts ou confondus, d'ordre de multiplicité n_i . A ces points P_i nous associons des diviseurs .

Définition 8 :

Un diviseur d'une courbe projective C non singulière est une somme finie formelle :

$$D = \sum_i n_i P_i , \text{ avec } n_i \in \mathbb{Z}, P_i \in C.$$

Lorsque la ligne L varie, nous obtenons une famille de diviseurs de la courbe C .

Définition 9 :

Un diviseur d'une fonction rationnelle f est une somme finie formelle :

$$(f) = \sum_i n_i P_i , \text{ avec } n_i > 0 \text{ pour les zéros } P_i \text{ de } f \text{ et } n_i < 0 \text{ pour les pôles de } f.$$

Exemple :

Soit $f(x) = 3(x-a_1)^2(x-a_2)^3(x-a_3)/(x-a_4)(x-a_5)^4 = y$;

Les zéros sont $P_1 = (a_1, 0)$, $P_2 = (a_2, 0)$ et $P_3 = (a_3, 0)$.

Les pôles sont $P_4 = (a_4, 0)$ et $P_5 = (a_5, 0)$.

Le diviseur de f est la somme formelle :

$$D(f) = 2P_1 + 3P_2 + P_3 - P_4 - 4P_5 .$$

Il y a plusieurs types de diviseurs.

Définition 10 :

- 1) un diviseur $D = \sum_{i=1}^N n_i P_i$ est effectif lorsque $n_i \geq 0$;
- 2) il est premier si $N=1$ et $n_1=1$; $D=(P)$
- 3) il est principal s'il est égal au diviseur (f) d'une fonction rationnelle f .
- 4) 2 diviseurs D et D' sont linéairement équivalents si leur différence $D - D'$ est un diviseur principal .
- 5) le degré d'un diviseur D est l'entier rationnel

$$\deg(D) = \sum_{i=1}^N n_i$$

Définition 11 :

Ces diviseurs sont des diviseurs de Weil .

Dans l'ensemble $\text{Div}(X)$ des diviseurs d'une courbe C , une structure de groupe abélien libre est déterminée par la loi :

$$(D, D') \rightarrow D + D' \text{ avec } D = \sum_i n_i P_i, D' = \sum_i n'_i P_i \text{ et } D + D' = \sum_i (n_i + n'_i) P_i$$

Le diviseur nul est égal à $D = \sum_i 0 P_i = (0)$.

Le diviseur $-D$ est égal à $-D = - \sum_i n_i P_i = \sum_i -n_i P_i$

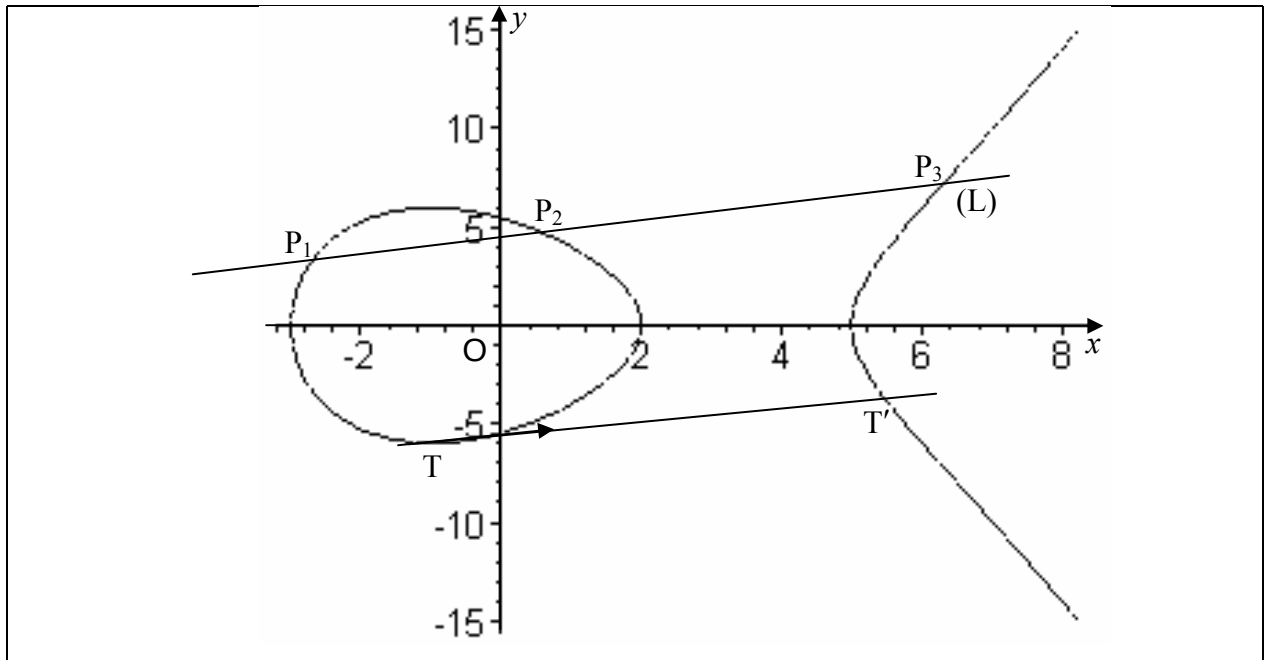
Le groupe $\text{Div}(X)$ admet plusieurs sous groupes comme le sous groupe $\text{Div}(X)^0$ des diviseurs de degré 0 , le sous groupe $\text{Prin}(X)$ des diviseurs principaux , etc.

Définition 12 :

Le groupe quotient $\text{Cl}(X) = \text{Div}(X) / \text{Prin}(X)$ est le groupe des classes de diviseurs de X .

Exemple :

Diviseurs d'une courbe elliptique E.



La courbe elliptique E possède un point à l'infini $O_E = (\infty, \infty)$ dans le plan affine,

$O_E = (0, 1, 0)$ dans le plan projectif P^2 .

Une ligne L coupe la courbe E en 3 points distincts P_1, P_2, P_3 .

Le diviseur de Weil associé à cette ligne L est égal à :

$$D = 1.P_1 + 1.P_2 + 1.P_3 = (P_1) + (P_2) + (P_3).$$

Une tangente en T coupe la courbe E en un point double T et un point simple T' .

Le diviseur associé est égal à :

$$D' = 2(T) + (T')$$

La loi de groupe des courbes elliptiques implique les relations :

$$P_1 + P_2 + P_3 = O_E \text{ et } 2T + T' = O_E,$$

Il en résulte les équivalences linéaires des diviseurs :

$(P_1) + (P_2) + (P_3) \approx 3(O_E)$ et $2(T) + (T') \approx 3(O_E)$, le diviseur de Weil du point à l'infini O_E est égal à :

$$D = 3(O_E)$$

Chapitre II

Géométrie des courbes elliptiques

1. Courbes algébriques planes :

Elles ont une équation $f(x,y)$ de degré $n \geq 1$ dans le plan affine $A^2(K)$, parmi ces courbes algébriques, il y a celles de degré 3 : les cubiques .

Les cubiques C ont une équation projective de la forme :

$$f(X,Y,Z)=d_1X^3+d_2X^2Y+d_3X^2Z+d_4XY^2+d_5XZ^2+d_6XYZ+d_7Y^3+d_8Z^3+d_9Y^2Z+d_{10}YZ^2=0 \quad (1)$$

Donc l'équation d'une cubique plane dépend de 10 coefficients .

Ce polynôme $f(X,Y,Z)$ peut être le produit de 3 polynômes de degré 1 , $f=f_1f_2f_3$; ou le produit d'un polynôme f_1 de degré 1 et f_2 de degré 2 . Dans les 2 cas, le polynôme f est réductible.

Un polynôme f qui n'est pas réductible est irréductible .

Dans l'ensemble des polynômes cubiques f irréductibles, il y a le sous ensemble des polynômes cubiques de Weierstrass.

Définition 1 :

Une équation de Weierstrass d'une cubique irréductible est un polynôme de la forme

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

Dans l'ensemble des cubiques d'équation de Weierstrass (2) il y a le sous ensemble des cubiques singulières et le sous ensemble des cubiques non singulières.

Définition 2 :

Une courbe elliptique est une cubique non singulière, irréductible, 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_1, a_2, a_3, a_4 et a_6 sont des éléments d'un corps commutatif K qui peut être global , local ou fini .

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

La nature du corps K a une influence sur la courbe elliptique.

2. Transformations de l'équation de Weierstrass :

Nous considérons des changements linéaires pour diminuer le nombre des monômes .

Les monômes xy et y sont éliminés par le changement linéaire :

$$x=X, y=\frac{1}{2}(Y-a_1X-a_3) \text{ pour } \text{car}(K) \neq 2 \quad (3)$$

Par le calcul nous obtenons l'équation de Weierstrass :

$$E_1: Y^2 = 4X^3 + b_2X^2 + 2b_4X + b_6, \text{ pour } \text{car}(K) \neq 2 \quad (3-1)$$

Les 3 coefficients b_{2i} sont des polynômes " homogènes de degré $2i$ " dans l'anneau

$Z[a_1, a_2, a_3, a_4, a_6]$:

$$b_2 = a_1^2 + 4a_2; b_4 = a_1a_3 + 2a_4; b_6 = a_3^2 + 4a_6 \quad (3-2)$$

Dans (3-1), le coefficient 4 et le monôme X^2 sont éliminés par le changement linéaire :

$$X = \frac{x - 3b_2}{36}, Y = \frac{y}{108}, \text{ pour } \text{car}(K) \neq 2, 3 \quad (3-3)$$

Par le calcul nous obtenons l'équation de Weierstrass :

$$E_2: y^2 = x^3 - 27c_4x - 54c_6 \in K[x, y] \quad (3-4)$$

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

$$c_4 = b_2^2 - 24b_4 \text{ et } c_6 = -b_2^3 + 36b_2b_4 - 216b_6; \quad (3-5)$$

Il existe d'autres modèles d'équations de Weierstrass :

Le modèle de Legendre :

$$E_3: y^2 = x(x-1)(x-t) \in K[x, y], \text{ avec } t \neq 0, 1; \quad (4)$$

Le modèle de Kubert :

$$E_4: y^2 + (1-s)xy - ty = x^3 - tx^2, \text{ à 2 paramètres } s, t \in K; \quad (5)$$

Le modèle de Deuring :

$$E_5: y^2 + txy + y = x^3 \in K[x, y] \text{ avec } t \neq 3 \quad (6)$$

Le modèle de Tate :

$$E_6: y^2 + xy = x^3 + ax + b \in \mathbb{C}[x, y] \quad (7)$$

où a et b sont des séries formelles de l'anneau $Z[[q]]$ pour

$$q = \exp(2\pi iz) \text{ et } z \in \mathbb{C} \text{ avec } \text{Im}(z) > 0 \quad (7-1)$$

$$a = -5 \sum_{n \geq 1} n^3 q^n / (1 - q^n) ; \quad (7-2)$$

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

Le modèle : $E_7 : y^2 = x^3 + Ax + B \in K[x, y]$, pour $4A^3 + 27B^2 \neq 0$; (8)

Nous nous intéressons à 3 familles de courbes elliptiques particulières $E(s, t)$ à 2 paramètres , d'équations :

$$E_1(s, t) : y^2 = x(x^2 + 2(s+t)x + (s-t)^2) ; \quad (9)$$

$$E_2(s, t) : y^2 = x(x^2 + sx + t) ; \quad (10)$$

$$E_3(s, t) : y^2 = x(x-s)(x-t) . \quad (11)$$

Ces exemples sont pris dans : [9].

Nous considérons les cubiques de Weierstrass singulières ou non .

3. Invariants d'une cubique de Weierstrass :

Les 5 coefficients b_2, b_4, b_6, c_4 et c_6 sont des invariants .

Il y en a d'autres comme : le discriminant , l'invariant modulaire , l'invariant différentiel , le rang , le régulateur , le conducteur , la série L de Dirichlet-Hasse , etc. .

Définition 3 :

Le discriminant d'une cubique de Weierstrass E est le polynôme "homogène de degré 12" :

$$\Delta(E) = 9b_2b_4b_6 - 27b_6^2 - 8b_4^3 - b_2^2b_8 \in \mathbb{Z}[b_2, b_4, b_6, b_8] ; \quad (1)$$

$$\text{pour } 4b_8 = b_2b_6 - b_4^2 ; \quad (1-1)$$

$$\text{Cette formule est valable pour un corps } K \text{ de } \text{car}(K) \neq 2, 3 \quad (1-2)$$

Définition 4 :

L'invariant modulaire d'une Cubique de Weierstrass E sur un corps K , de discriminant $\Delta(E)$, est l'élément :

$$j(E) = c_4^3 / \Delta(E) \in K \quad (2)$$

Sur le corps des nombres réels $\mathbb{R}$, cet invariant peut prendre les valeurs particulières :

$$j(E) = 0 \text{ et } j(E) = 1728 \quad (2-1)$$

L'invariant différentiel provient de la différentielle d'une fonction $F(x,y)$ de deux variables qui est différentiable :

$$dF = F'_x dx + F'_y dy \quad (3)$$

Cette relation permet de définir l'invariant différentiel.

Définition 5 :

L'invariant différentiel d'une cubique de Weierstrass :

$$E : F(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0 \quad (3-1)$$

est l'élément différentiel :

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

où les dénominateurs sont les dérivées partielles de $F(x,y)$.

Cet élément différentiel est intégrable sur le corps des nombres réels .

L'intégrale $\Omega = \int_{E(\mathbb{R})} dx/(2y + a_1x + a_3)$ est calculable par la technique usuelle.

Le nombre Ω constitue une période réelle ; il intervient dans la formule de la conjecture de Birch et Swinnerton-Dyer [12].

Exemples :

Calcul des trois invariants pour les modèles E_2 à E_7 précédents :

1) Courbe elliptique E d'équation de Weierstrass :

$$E : y^2 = x^3 - 27c_4x - 54c_6 ;$$

Nous obtenons les invariants :

$$\Delta(E) = (c_4^3 - c_6^2)/1728, \quad j(E) = \frac{1728c_4^3}{c_4^3 - c_6^2}, \quad \omega(E) = \frac{dx}{2y}.$$

2) Courbe elliptique E d'équation de Weierstrass :

$$E : y^2 = x(x-1)(x-t) ;$$

Nous obtenons les invariants :

$$\Delta(E) = 16t^2(t-1)^2, \quad j(E) = \frac{2^8(t^2 - t + 1)^3}{t^2(t-1)^2}, \quad \omega(E) = \frac{dx}{2y}.$$

3) Courbe elliptique à 2 paramètres E d'équation de Weierstrass :

$$E : y^2 + (1-s)xy - ty = x^3 - tx^2 ;$$

Nous obtenons les invariants :

$$\Delta(E) = 16t^5 - 27t^4 - (1-s)^3t^3 + (1-s)^4t^3 + 36(1-s)t^4 - 8(1-s)^2t^4 ;$$

$$j(E) = \frac{\left((1-s)^4 + 16t^2 - 8t(1-s)^2 + 24t(1-s) \right)^3}{\Delta(E)} ;$$

$$\omega(E) = \frac{dx}{2y + (1-s)x - t}$$

4) Courbe elliptique à 1 paramètre E d'équation de Weierstrass :

$$E : y^2 + txy + y = x^3 ;$$

Nous obtenons les invariants :

$$\Delta(E) = t^3 - 27 \text{ avec } t \neq 3, \quad j(E) = \frac{t^3(t^3 - 24)^3}{t^3 - 27}, \quad \omega(E) = \frac{dx}{2y + tx + 1}.$$

5) Courbe elliptique E d'équation de Weierstrass :

$$E : y^2 = x^3 + Ax + B$$

Nous obtenons les invariants :

$$\Delta(E) = -16(4A^3 + 27B^2), \quad j(E) = \frac{(48A)^3}{16(4A^3 + 27B^2)}, \quad \omega(E) = \frac{dx}{2y}.$$

6) Applications aux 3 courbes elliptiques E(s,t) :

Nous obtenons les invariants :

$$\Delta(E_1(s,t)) = 2^8 st(s-t)^4 \text{ et } j(E_1(s,t)) = \frac{2^4(s^2 + 14st + t^2)^3}{st(s-t)^4}$$

$$\Delta(E_1(s,t)) \neq 0 \text{ implique les conditions : } s \neq 0, \quad t \neq 0 \text{ et } s \neq t.$$

$$\Delta(E_2(s,t)) = 2^4 t^2 (s^2 - 4t) \text{ et } j(E_2(s,t)) = \frac{2^8 (s^2 - 3t)^3}{t^2 (s^2 - 4t)}$$

$$\Delta(E_2(s,t)) \neq 0 \text{ implique les conditions : } t \neq 0 \text{ et } s \neq \pm 2\sqrt{t}.$$

$$\Delta(E_3(s,t)) = 2^4 s^2 t^2 (s-t)^2 \text{ et } j(E_3(s,t)) = \frac{2^8 (s^2 - st + t^2)^3}{s^2 t^2 (s-t)^2}$$

$$\Delta(E_3(s,t)) \neq 0 \text{ implique les conditions : } s \neq 0, \quad t \neq 0 \text{ et } s \neq t.$$

4. Discriminant d'un polynôme et résultant de 2 polynômes :

Le discriminant $\Delta(E)$ d'une cubique de Weierstrass E est lié au discriminant $\text{dis}(f)$ du polynôme $f(x)$ de l'équation de Weierstrass de E : $y^2 = f(x)$.

C'est pourquoi nous faisons un bref exposé sur les théories des discriminants et des résultants.

Définition 6 :

le discriminant d'un polynôme de degré n :

$$f(x) = d_0 x^n + d_1 x^{n-1} + \dots + d_n = d_0 (x - e_1)(x - e_2) \dots (x - e_n)$$

est une fonction symétrique de ses racines $e_1, \dots, e_n$:

$$\text{dis}(f) = d_0^{2n-2} \prod_{1 \leq i < j \leq n} (e_i - e_j)^2 \quad (1)$$

Cette formule se trouve dans [4].

En appliquant cette formule au polynôme $f(x)$ de l'équation de Weierstrass :

$$E : y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6 = f(x)$$

Nous obtenons la valeur :

$$\text{dis}(f) = 16(9b_2 b_4 b_6 - 27b_6^2 - 8b_4^3 - b_2^2 b_8) \quad (1-1)$$

Cette relation (1-1) et la formule du discriminant $\Delta(E)$ impliquent la

Proposition 1 :

Soit une courbe elliptique E d'équation de Weierstrass :

$$E : y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6 = f(x)$$

Alors les discriminants $\text{dis}(f)$ du polynôme f et $\Delta(E)$ de la courbe E satisfont la relation :

$$\text{dis}(f) = 16 \Delta(E) .$$

Le discriminant est donc une fonction symétrique des coefficients du polynôme :

$$f(x) = (x - e_1) \dots (x - e_n) = x^n + d_1 x^{n-1} + \dots + d_n .$$

Selon la théorie, d'après Harvey Cohn, le discriminant se met sous la forme d'un déterminant d'ordre n , symétrique :

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

Les nombres s_m sont des fonctions symétriques : somme de puissances des racines de f .

$$s_m = e_1^m + e_2^m + \dots + e_n^m.$$

Avec le calcul ; nous obtenons :

$$s_0 = n, s_1 = -d_1, s_2 = d_1^2 - 2d_2, s_3 = 3d_1d_2 - d_1^3 - 3d_3, \text{ et les relations :}$$

$$s_m = -md_m - s_1d_{m-1} - \dots - s_{m-1}d_1, \text{ avec } d_m = 0 \text{ pour } m > n.$$

Exemple:

$$f(x) = x^5 - 2x^4 + 4x^3 - 5x^2 + 2x - 7.$$

Calcul des nombres s_m :

$$s_0 = 5, s_1 = 2, s_2 = -4, s_3 = -1, s_4 = 16, s_5 = 47, s_6 = 47, s_7 = -40, s_8 = -72.$$

$$\text{dis}(f) = \begin{vmatrix} 5 & 2 & -4 & -1 & 16 \\ 2 & -4 & -1 & 16 & 47 \\ -4 & -1 & 16 & 47 & 47 \\ -1 & 16 & 47 & 47 & -40 \\ 16 & 47 & 47 & -40 & -72 \end{vmatrix} = 3590369$$

Il existe un autre procédé de calcul de ce discriminant, il est basé sur la théorie du résultant de 2 polynômes.

Définition 7 : soient 2 polynômes d'un anneau $K[x]$:

$$f(x) = d_0x^n + d_1x^{n-1} + \dots + d_n = d_0(x-e_1)(x-e_2)\dots(x-e_n) \text{ de degré } n \text{ et}$$

$$g(x) = s_0x^t + s_1x^{t-1} + \dots + s_t = s_0(x-r_1)(x-r_2)\dots(x-r_t) \text{ de degré } t.$$

Alors le résultant des 2 polynômes f et g est le déterminant d'ordre $n+t$ formé de t lignes

$(d_0 \ d_1 \ \dots \ d_n)$ et n lignes $(s_0 \ s_1 \ \dots \ s_t)$:

$$\text{Res}(f,g) = \begin{vmatrix} d_0 & d_1 & . & . & . & d_n & 0 & . & 0 \\ 0 & d_0 & d_1 & . & . & . & d_n & . & . \\ . & . & . & . & . & . & . & . & 0 \\ 0 & . & 0 & d_0 & d_1 & . & . & . & d_n \\ s_0 & s_1 & . & . & s_t & 0 & . & . & 0 \\ 0 & s_0 & s_1 & . & . & s_t & . & . & . \\ . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & 0 \\ 0 & . & . & 0 & s_0 & s_1 & . & . & s_t \end{vmatrix} \left. \begin{array}{l} \text{ } \\ \text{ } \\ \text{ } \\ \text{ } \end{array} \right\} \begin{array}{l} t \text{ lignes} \\ n \text{ lignes} \end{array}$$

où les lignes sont complétées par des zéros.

Exemple :

Soient 2 polynômes f et g :

$$f(x) = x^3 - x^2 + 5x - 1 \text{ et } g(x) = 4x^2 - 3x + 7$$

Alors le résultant des 2 polynômes f et g est égal à :

$$\text{Res}(f, g) = \begin{vmatrix} 1 & -1 & 5 & -1 & 0 \\ 0 & 1 & -1 & 5 & -1 \\ 4 & -3 & 7 & 0 & 0 \\ 0 & 4 & -3 & 7 & 0 \\ 0 & 0 & 4 & -3 & 7 \end{vmatrix} = 988$$

Citons sans démonstration, quelques propriétés des résultants de 2 polynômes :

Proposition 2 :

Soient les deux polynômes $f(x)$ et $g(x)$ de la définition 7. Alors leur résultant $\text{Res}(f, g)$ satisfait les relations :

$$1) \text{Res}(f, g) = d_0^t s_0^n \prod_{\substack{1 \leq i \leq n \\ 1 \leq j \leq t}} (e_i - r_j) = d_0^t \prod_{1 \leq i \leq n} g(e_i) = (-1)^{nt} s_0^n \prod_{1 \leq j \leq t} f(r_j)$$

$$2) \text{Res}(f, g) = 0 \text{ si et seulement si } f \text{ et } g \text{ ont une racine commune } e_i = r_j.$$

Corollaire :

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

$$\text{Res}(fg, h) = \text{Res}(f, h) \text{Res}(g, h)$$

Le résultant $\text{Res}(f, f')$ d'un polynôme $f(x)$ et de sa dérivée $f'(x)$ est lié au discriminant $\text{dis}(f)$ du polynôme f .

Proposition 3 :

Soit un polynôme $f(x)$ d'un anneau $K[x]$, son résultant $\text{Res}(f, f')$ et son discriminant $\text{dis}(f)$. Alors :

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

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

Cas particulier du polynôme $(x^n - 1)/(x - 1) = x^{n-1} + x^{n-2} + \dots + x + 1$:

Proposition 4 :

Le discriminant du polynôme $f(x) = (x^n - 1)/(x - 1)$ est égal à :

$$\text{dis}(f(x)) = (-1)^{\frac{(n-1)(n-2)}{2}} \cdot n^{n-2}$$

Exemple :

Soit le polynôme $f(x) = (x^{10} - 1)/(x - 1)$

Nous obtenons le discriminant en appliquant cette proposition pour $n = 10$:

$$\text{dis}(f) = (-1)^{\frac{(10-1)(10-2)}{2}} \cdot 10^{(10-2)} = 10^8$$

5. Classification des cubiques de Weierstrass par leur discriminant :

Par définition , une courbe elliptique est une cubique non singulière . Les singularités d'une courbe A d'équation implicite $F(x,y)=0$ sont des points multiples de la courbe .

Les points singuliers d'une courbe plane sont solutions du système algébrique :

$$F(x,y)=0 ; F'_x=0 ; F'_y=0$$

Lorsque ce système admet une solution , alors la courbe est singulière . Lorsque le système n'admet pas de solution , la courbe est non singulière .

Les propriétés du résultant $\text{Res}(f, f')$ d'un polynôme $f(x)$ permettent de trouver une forme d'une cubique d'équation $y^2 = f(x)$ non singulière .

Proposition 5 :

Soit une cubique de Weierstrass E de discriminant $\Delta(E)$. Alors :

- 1) Le point à l'infini O_E est un point non singulier de E ;
- 2) La cubique E est une courbe elliptique si et seulement si $\Delta(E) \neq 0$.

Preuve de "le point à l'infini O_E est un point non singulier de E "

Soit une cubique E d'équation de Weierstrass

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

Dans le plan projectif P^2 , cette équation se met sous la forme :

$$F(X,Y,Z)=Y^2Z+a_1XYZ+a_3YZ^2-X^3-a_2X^2Z-a_4XZ^2-a_6Z^3=0 \quad (2)$$

Les 3 dérivées partielles de ce polynôme F sont égales à :

$$F'_X = a_1YZ - 3X^2 - 2a_2XZ - a_4Z^2; \quad (3)$$

$$F'_Y = 2YZ + a_1XZ + a_3Z^2; \quad (4)$$

$$F'_Z = Y^2 + a_1XY + 2a_3YZ - a_2X^2 - 2a_4XZ - 3a_6Z^2 \quad (5)$$

Au point à l'infini $O_E=(0,1,0)$ ces 4 polynômes prennent les valeurs :

$$F(O_E)=0, F'_X(O_E)=0, F'_Y(O_E)=0, F'_Z(O_E)=1. \quad (6)$$

La valeur $F(O_E)=0$ implique que le point à l'infini est sur la cubique E ;

La valeur $F'_Z(O_E) \neq 0$ implique que le point O_E n'est pas singulier .

Preuve de "E est une courbe elliptique " implique " $\Delta(E) \neq 0$ "

Soit une courbe elliptique E ; donc E n'a pas de point singulier . Prenons une équation de Weierstrass de la forme :

$$y^2=(x-e_1)(x-e_2)(x-e_3)=f(x) \text{ où les 3 racines } e_i \text{ de } f(x) \text{ sont simples .}$$

Par définition , le discriminant de ce polynôme est égal à :

$$\text{dis}(f)=(e_1-e_2)^2(e_2-e_3)^2(e_3-e_1)^2$$

L'hypothèse $e_i \neq e_j$ implique la valeur $\text{dis}(f) \neq 0$.

La relation $\text{dis}(f)=16\Delta(E)$ entre les discriminants de f et de E implique :

$$\Delta(E) \neq 0$$

Preuve de " $\Delta(E) \neq 0$ " implique "E est une courbe elliptique".

Soit une cubique E de Weierstrass :

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

Alors la relation entre le discriminant de f et le discriminant $\Delta(E)$ implique :

$$\text{dis}(f)=16\Delta(E) \neq 0 \quad (2)$$

La relation entre $\text{Res}(f, f')$ et $\text{dis}(f)$ et (2) impliquent :

$$\text{Res}(f, f') \neq 0 \quad (3)$$

Par une propriété des résultants , le polynôme $f(x)$ et sa dérivée $f'(x)$ n'ont pas de racine commune.

Il en résulte que le polynôme n'admet que des racines simples .

Donc la cubique de Weierstrass E est une courbe elliptique.

□

Une courbe algébrique singulière admet 2 types de points singuliers :

Un nœud est un point singulier à 2 tangentes distinctes.

Un point de rebroussement est un point singulier à 2 tangentes confondues.

Proposition 6 :

Soit une cubique de Weierstrass E de discriminant $\Delta(E)$ et d'invariant $c_4(E) = b_2^2 - 24b_4$.

Alors :

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

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

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

Soit une cubique de Weierstrass E qui admet un nœud , donc E est singulière .

Par la proposition 5 , elle admet un discriminant $\Delta(E)=0$

L'hypothèse "E admet un nœud" implique que la courbe admet 2 tangentes distinctes en ce nœud .

Les pentes de ces tangentes sont égales à la dérivée y' de y .

La dérivée y' est égale à :

$$y' = \frac{6x^2 + b_2x + b_4}{y} = \frac{h(x)}{y}$$

L'hypothèse de 2 pentes implique que le polynôme $h(x)$ admet 2 racines distinctes .

Donc son discriminant $\text{dis}(h(x))$ n'est pas nul :

$$\text{dis}(h(x)) = b_2^2 - 24b_4 = c_4(E) \neq 0 .$$

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

L'hypothèse $\Delta(E)=0$ implique que la cubique E d'équation de Weierstrass

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 \text{ admet un point singulier .}$$

Donc $f(x) = 4x^3 + b_2x^2 + 2b_4x + b_6$ possède une racine double ou triple ; cette racine est l'abscisse du point singulier de E .

$$\text{dis}(h(x)) = b_2^2 - 24b_4 = c_4(E)$$

L'hypothèse $c_4(E) \neq 0$ implique que $h(x)$ admet 2 racines simples .

Donc la cubique E admet 2 tangentes distinctes en son point singulier , donc le point singulier est un nœud .

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

L'hypothèse $\Delta(E) = 0$ implique que la cubique E d'équation :

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

admet un point singulier .

L'hypothèse $\Delta(E) = 0$ et la relation $\text{dis}(f(x)) = 16\Delta(E)$ impliquent que :

$f(x) = 4x^3 + b_2x^2 + 2b_4x + b_6$ admet une racine double ou triple .

La dérivée de $f(x)$ est égale à :

$$f'(x) = 12x^2 + 2b_2x + 2b_4$$

son discriminant est égal à :

$$\text{dis}(f'(x)) = b_2^2 - 24b_4 = c_4(E) = 0$$

Donc $f'(x)$ admet une racine double . Cela implique que E admet un point de rebroussement .

□

Examinons la forme d'une courbe elliptique E suivant le signe de son discriminant $\Delta(E)$.

Proposition 7 :

Soit une courbe elliptique E de discriminant $\Delta(E)$ et d'équation de Weierstrass :

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

1) La courbe elliptique E coupe l'axe Ox en 3 points distincts si et seulement si $\Delta(E) > 0$.

2) La courbe elliptique E coupe l'axe Ox en 1 seul point si et seulement si $\Delta(E) < 0$.

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

Par la proposition 5 , une courbe elliptique E a un discriminant non nul :

$$\Delta(E) \neq 0 \tag{1}$$

Son équation de Weierstrass se met sous la forme :

$$y^2 = (x - e_1)(x - e_2)(x - e_3) \in R[x, y] \tag{2}$$

Par définition le discriminant de f est égal à :

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

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

$$\text{dis}(f) > 0 \tag{4}$$

(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 Ox .

Preuve de : " $\Delta(E)<0$ " implique " E coupe l'axe Ox en 1 seul point " :

Les formules (2) et (3) sont encore valables .

L'hypothèse " $\Delta(E)<0$ " implique un discriminant :

$$\text{dis}(f)=(e_1-e_2)^2(e_2-e_3)^2(e_3-e_1)^2<0 .$$

Par la théorie des racines d'un polynôme , $f(x)$ admet une racine réelle , $e_1=r$ et 2 racines complexes conjuguées $e_2=s+it$ et $e_3=s-it$.

Seul le point $P_1=(r,0)$ est sur l'axe Ox .

□

Nous pouvons classifier les cubiques planes par leurs discriminants $\Delta(E)$ et leur invariant $c_4(E)$ à l'aide des propositions 5 , 6 et 7 .

Corollaire :

Les cubiques de Weierstrass E de discriminant $\Delta(E)$ et d'invariant $c_4(E)$, sont classifiées en 4 ensembles :

1) *l'ensemble des courbes elliptiques de discriminant $\Delta(E)>0$; elles coupent l'axe Ox en 3 points simples .*

2) *l'ensemble des courbes elliptiques de discriminant $\Delta(E)<0$; elles coupent l'axe Ox en un seul point .*

3) *l'ensemble des cubiques qui ont un nœud , alors $\Delta(E)=0$ et $c_4(E)\neq 0$.*

4) *l'ensemble des cubiques qui ont un point de rebroussement , alors $\Delta(E)=c_4(E)=0$.*

□

Illustrons cette classification par un exemple de cubique de chaque classe .

Les cubiques sont tracées par le maple 6.

Exemples :

1) Courbe elliptique de discriminant positif :

Soit la cubique E_1 d'équation de Weierstrass :

$$E_1 : y^2=x^3-23x+9 \in \mathbb{R}[x,y]$$

Calcul des invariants de la cubique :

$$a_1=a_2=a_3=0 , a_4=-23 , a_6=9 ;$$

$$b_2=0 , b_4=-46 , b_6=36 , b_8=-529 , \Delta(E)=743696 ;$$

$$c_4=1104 , c_6=-7776 .$$

Le discriminant positif implique que E_1 est une courbe elliptique qui coupe l'axe Ox en trois points $P_1=(e_1, 0)$, $P_2=(e_2, 0)$ et $P_3=(e_3, 0)$ simples.

Pour construire cette courbe elliptique, déterminons les coordonnées de quelques points particuliers :

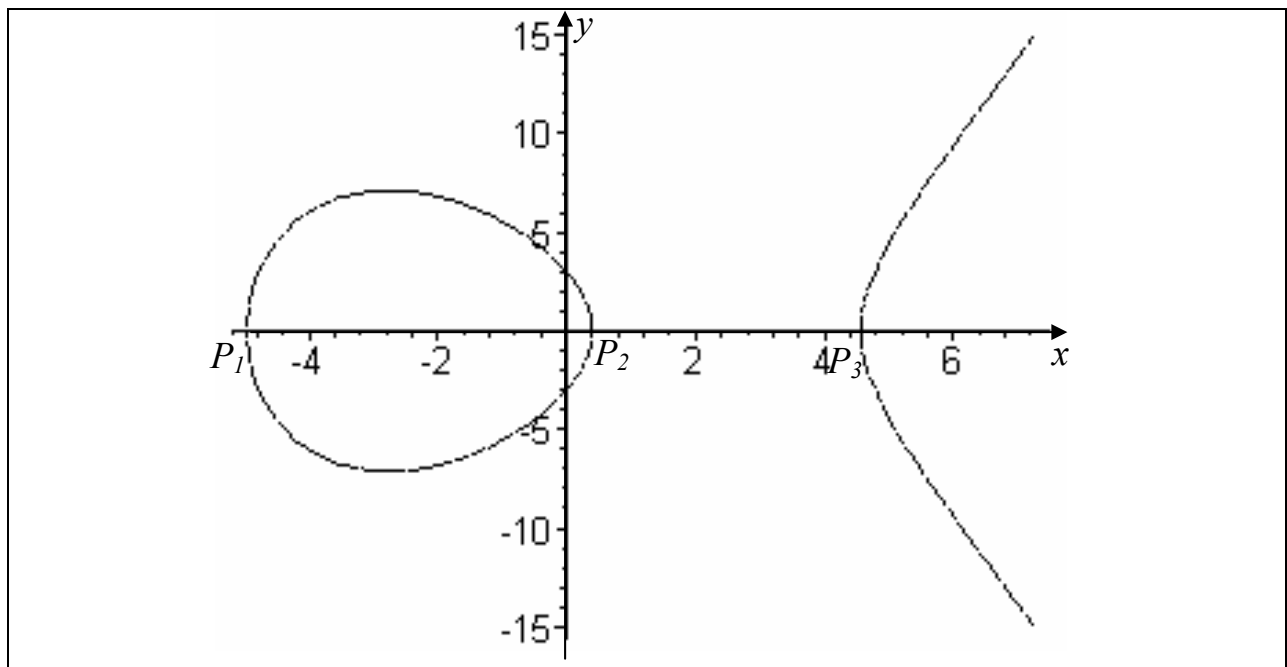
x	-5	-4	-3	-2	-1	0	1	2	3	4	5
$f(x)$	-1	37	51	47	31	9	-13	-29	-33	-19	19
y	Pas de réel	$\pm\sqrt{37}$	$\pm\sqrt{51}$	$\pm\sqrt{47}$	$\pm\sqrt{31}$	± 3	Pas de réel	Pas de réel	Pas de réel	Pas de réel	$\pm\sqrt{19}$

D'après ce tableau on peut encadrer les racines e_i de $f(x)$:

$$-5 \leq e_1 \leq -4, 0 \leq e_2 \leq 1, 4 \leq e_3 \leq 5.$$

Le calcul de ces racines s'obtient avec le logiciel Maple.

La courbe elliptique E_1 :



2) Courbe elliptique E_2 qui a un discriminant négatif :

Soit la cubique E_2 d'équation de Weierstrass :

$$E_2 : y^2 = x^3 + 8x^2 - 2x + 13 \in \mathbb{R}[x, y]$$

Calcul des invariants de la courbe E_2 :

$$a_1 = a_3 = 0, a_2 = 8, a_4 = -2, a_6 = 13;$$

$$b_2 = 32, b_4 = -4, b_6 = 52, b_8 = 412, \Delta(E) = -554288$$

$$c_4 = 1120, c_6 = -48608.$$

Le discriminant négatif implique que E_2 est une courbe elliptique qui coupe l'axe Ox en un seul point $P=(e, 0)$ avec e est l'unique racine réelle de l'équation

$$f(x)=x^3+8x^2-2x+13=0.$$

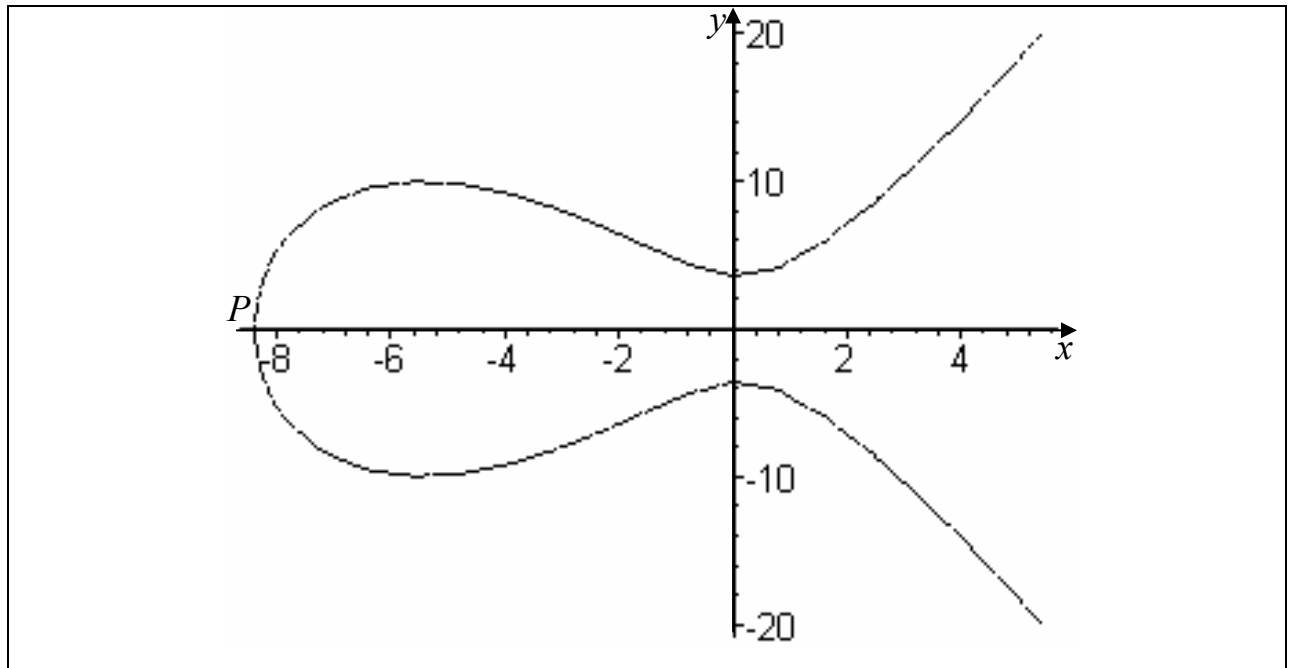
$$f(-9)= -50 \text{ et } f(-8)= 29$$

Cela implique que : $-9 \leq e \leq -8$.

Tableau de valeurs des coordonnées de quelques points de la courbe :

x	-2	-1	0	1	2
$f(x)$	41	22	13	20	49
y	$\pm\sqrt{41}$	$\pm\sqrt{22}$	$\pm\sqrt{13}$	$\pm 2\sqrt{5}$	± 7

La courbe elliptique E_2 :



3) Cubique de Weierstrass avec un nœud :

Soit la cubique E_3 d'équation de Weierstrass :

$$E_3 : y^2 + 2xy + 2y = x^3 - 3x^2 - x - 1 \in \mathbb{R}[x, y]$$

Calcul des invariants de la cubique E_3 :

$$a_1=2, a_2=-3, a_3=2, a_4=-1 \text{ et } a_6=-1.$$

$$b_2=-8, b_4=2, b_6=0, b_8=-1, \Delta(E)=0, c_4=16.$$

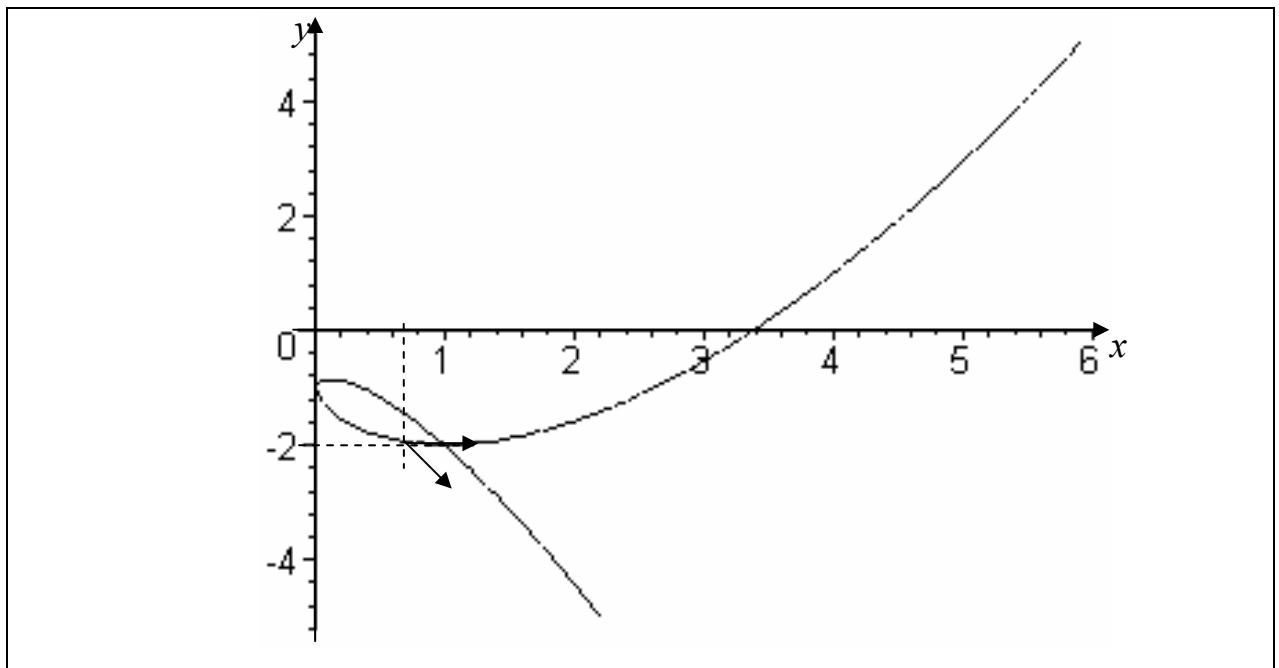
$\Delta(E)=0$ implique que la cubique a un point singulier.

$c_4(E) \neq 0$ implique que ce point singulier est un nœud de coordonnées (1,-2) .

Tableau de valeurs des coordonnées de quelques points de la cubique E :

x	-1	0	1	2
y	Pas de valeur réelle	-1 double	-2 double	$-3 \pm \sqrt{2}$

La cubique plane E_3 :



4) Cubique de Weierstrass E_4 avec un point de rebroussement :

Soit la cubique E_4 d'équation de Weierstrass :

$$E_4 : y^2 - 2y = x^3 - 1 \in \mathbb{R}[x, y]$$

Calcul des invariants de la cubique E_4 :

$$a_1=0, a_2=0, a_3=-2, a_4=0 \text{ et } a_6=-1.$$

$$b_2=0, b_4=0, b_6=0, \Delta(E)=0, c_4(E)=0.$$

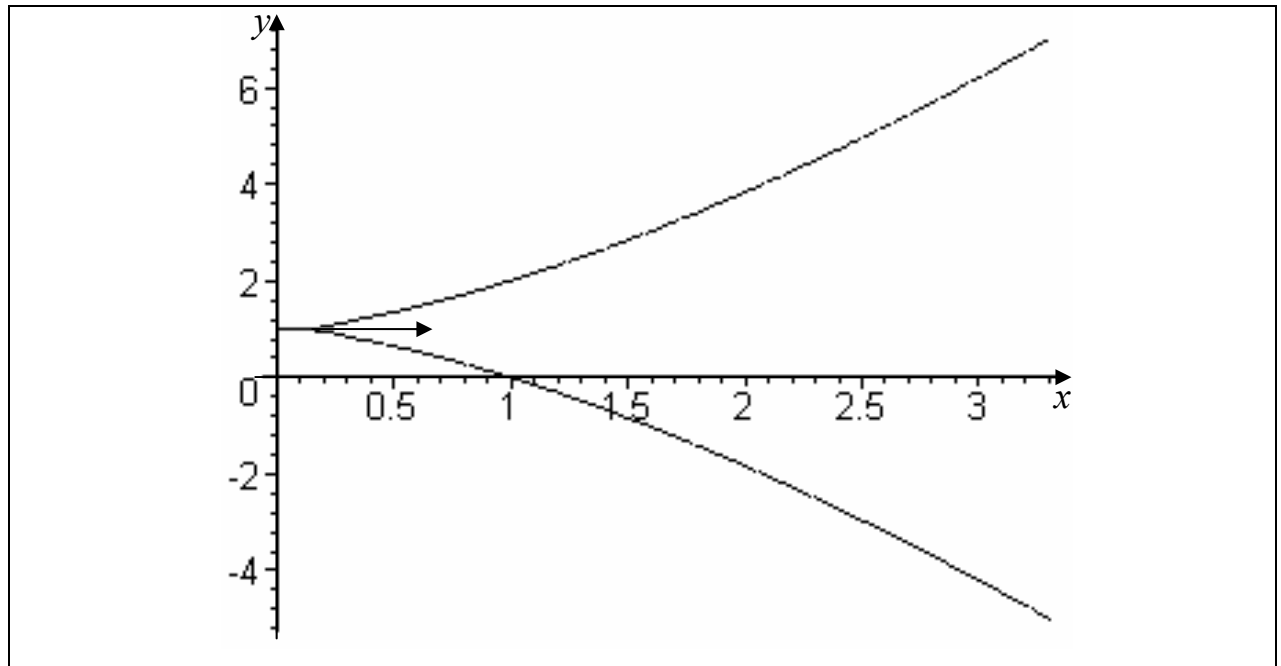
$\Delta(E)=0$ implique que la cubique a un point singulier .

Le coefficient $c_4(E)=0$ implique que ce point singulier est un point de rebroussement, de coordonnées (0,1) .

Tableau de valeurs des coordonnées de quelques points de la cubique E_4 :

x	0	1	2	3
y	racine 1 double	0 et 2	$1 \pm 2\sqrt{2}$	$1 \pm \sqrt{105}$

La cubique plane E_4 :



Chapitre III

GROUPE DE MORDELL-WEIL D'UNE COURBE ELLIPTIQUE

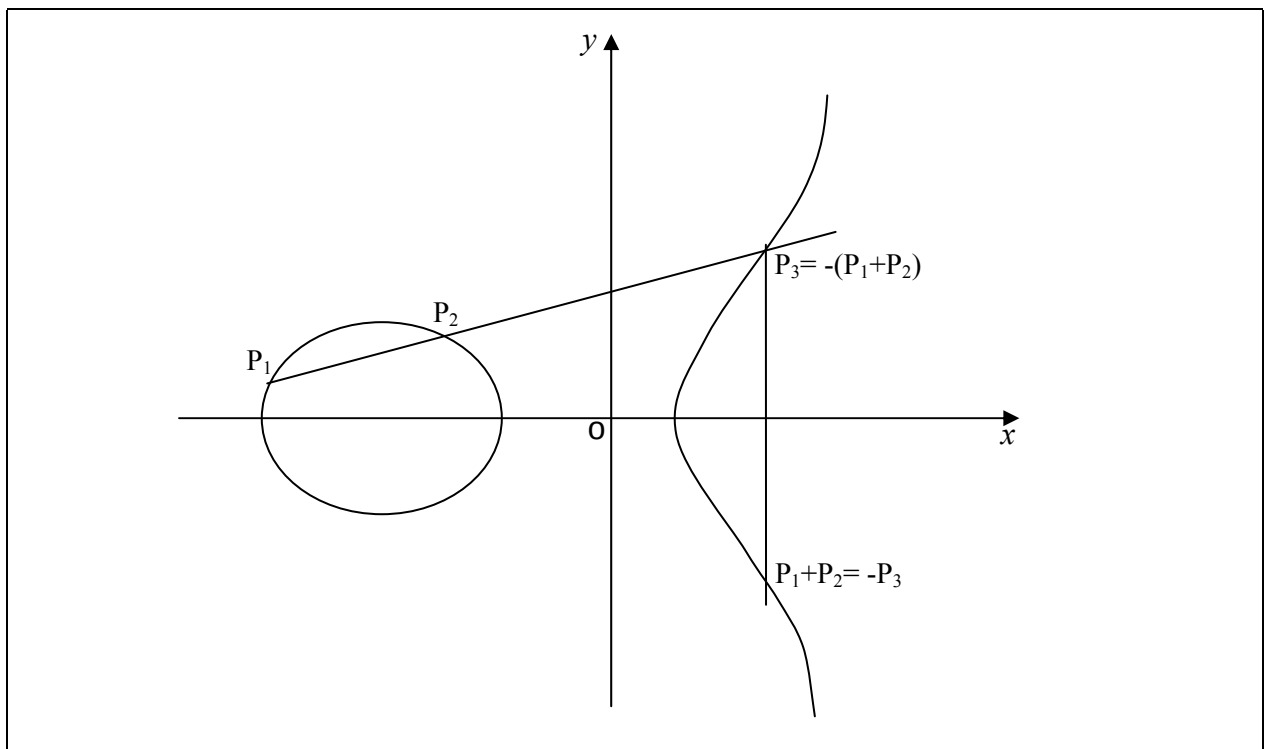
1. Structure de groupe abélien :

Pour munir l'ensemble $E(K)$ des points K -rationnels d'une courbe elliptique E d'une structure de groupe, nous prenons comme élément neutre le point O_E à l'infini et une loi de composition :

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

La somme $P_1 + P_2$ de deux points P_1 et P_2 est déterminée par la règle géométrique de trois points colinéaires P_1, P_2 et P_3 de la courbe :

$P_1 + P_2 + P_3 = O_E$; figure ci-dessous .



Vérifions les 4 axiomes d'un groupe abélien :

1) Axiome de l'élément neutre :

Soit un point $P \in E(K)$.

Alors la droite passant par les points P et O_E est parallèle à l'axe Oy ; elle satisfait la relation :

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

donc le point à l'infini est l'élément neutre de l'addition .

2) Axiome du symétrique :

Soit un point P de la courbe elliptique E . La parallèle à l'axe Oy passant par P coupe la courbe en un point P' qui satisfait la relation : $P + P' = O_E$;

Par définition du symétrique d'un élément , P' est donc le symétrique de P :

$$P' = -P .$$

3) Axiome d'associativité :

En comparant les 2 sommes $(P+Q)+R$ et $P+(Q+R)$ nous obtenons l'associativité .

4) La commutativité de la loi provient de la coïncidence des sécantes PQ et QP .

Nous avons démontré la :

Proposition 1 :

L'ensemble $E(K)$ des points K -rationnels d'une courbe elliptique E est un groupe abélien d'élément neutre le point à l'infini O_E et de loi basée sur la règle géométrique de 3 points colinéaires de E :

$$P_1 + P_2 + P_3 = O_E$$

Définition 1 :

Le groupe $E(K)$ est le groupe de Mordell-Weil de la courbe elliptique E .

2. Calcul des coordonnées du symétrique d'un point et de la somme de 2 points :

Soit un point $P = (x_P, y_P)$ sur le groupe $E(K)$, son symétrique $-P$ se trouve à l'intersection de la courbe par la parallèle à Oy passant par P .

Il en résulte que les points P et $-P$ ont même abscisse $x_P = x_{-P}$, leurs ordonnées satisfont l'équation de Weierstrass de E :

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

Cela implique :

$$y^2 + (a_1x + a_3)y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

C'est une équation du 2^{ème} degré en y ; donc la somme des 2 racines y_P et y_{-P} est égale au coefficient de y . Nous obtenons :

Coordonnées du symétrique $-P$ de $P=(x_P, y_P)$:

$$-P=(x_P, -y_P - a_1x_P - a_3) \quad (1)$$

Pour calculer la somme P_1+P_2 de 2 points $P_i=(x_i, y_i)$, nous appliquons la règle de 3 points colinéaires :

$$P_1+P_2+P_3=O_E$$

Il en résulte $P_1+P_2=-P_3$, pour les points $P_1 \neq \pm P_2$.

Donc la somme P_1+P_2 est le symétrique du point P_3 d'intersection de la sécante P_1P_2 avec E .

Equation de la sécante P_1P_2 :

$$y = \lambda(x - x_1) + y_1 \text{ avec la pente } \lambda = \frac{y_1 - y_2}{x_1 - x_2}$$

Les abscisses x_i des 3 points d'intersection avec la courbe sont les 3 solutions de l'équation cubique en x :

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

La somme des 3 racines est la fonction symétrique élémentaire : "Somme des racines" d'un polynôme $x^3 + A_1x^2 + A_2x + A_3 = 0$:

$$x_1 + x_2 + x_3 = -A_1.$$

Avec les calculs nous obtenons les coordonnées de la somme $P_1+P_2=-P_3=M$, pour $P_1 \neq \pm P_2$:

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

Regroupons ces résultats dans la

Proposition 2 :

Soit une courbe elliptique E d'équation de Weierstrass :

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

1) le symétrique $-P=(x(-P), y(-P))$ d'un point $P=(x_P, y_P)$ a pour coordonnées :

$$x(-P)=x_P \text{ et } y(-P) = -y_P - a_1x_P - a_3$$

2) la somme $P_1 + P_2 = M$ de 2 points $P_i = (x_i, y_i)$, $P_1 \neq \pm P_2$ a pour coordonnées :

$$x_M = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$

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

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2}$$

□

3. Points d'ordre fini et sous groupes de torsion d'une courbe elliptique :

Dans un groupe, il y a des points d'ordre fini, des points d'ordre infini, des sous groupes ...

Définition 2 :

Un point P d'ordre m du groupe de Mordell-Weil $E(K)$ est un point qui satisfait la relation :
 $mP = O_E$ et $kP \neq O_E$ pour $k < m$

C'est un point de m -torsion de la courbe elliptique.

Le symbole mP signifie :

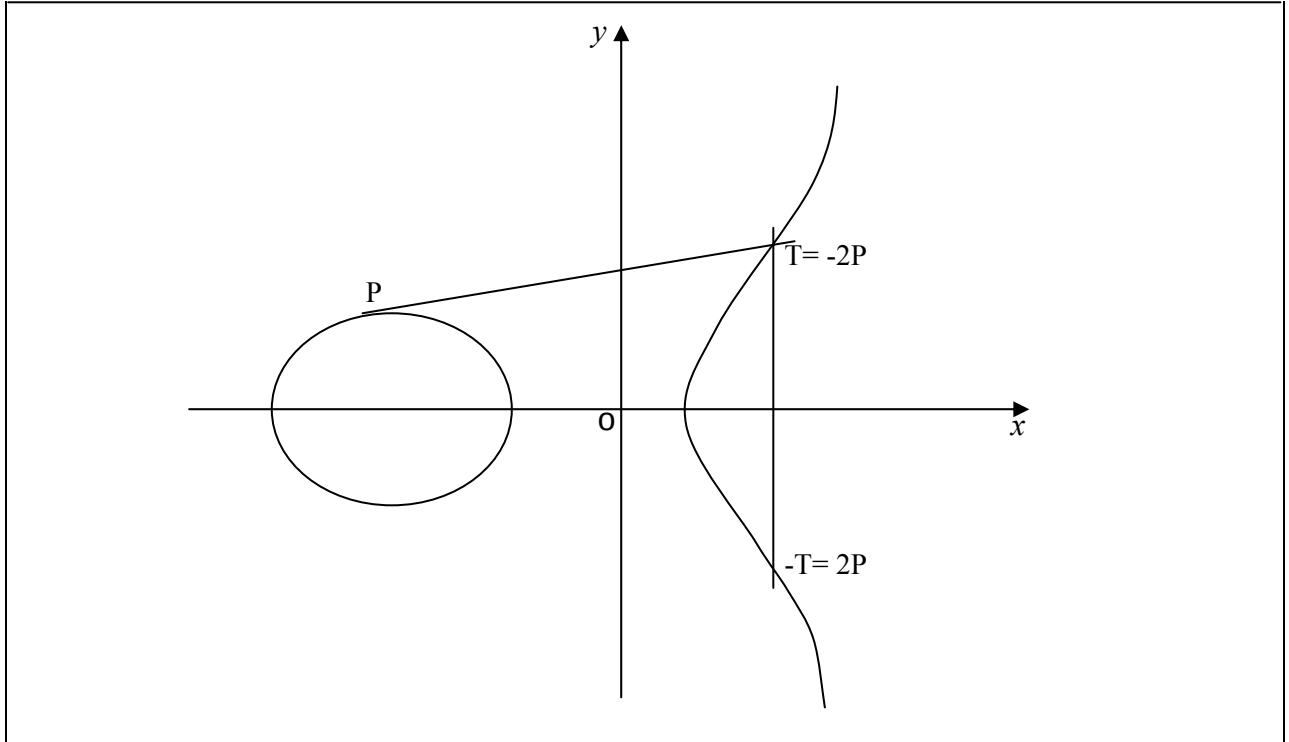
$$mP = \begin{cases} P + \dots + P, m \text{ fois} & \text{si } m > 0 \\ (-m)(-P) & \text{si } m < 0 \\ O_E & \text{si } m = 0 \end{cases}$$

Déterminons les coordonnées d'un point $2P = (x_{2P}, y_{2P})$ pour $P = (x_P, y_P)$:

Le point $2P$ est construit avec la tangente à la courbe E au point P ; cette tangente recoupe la courbe E en un point simple T .

Equation de la tangente en P :

$$y = y'(x - x_P) + y_P \text{ avec } y' = \frac{3x_P^2 + 2a_2x_P + a_4 - a_1y_P}{2y_P + a_1x_P + a_3}$$



Les abscisses du point double P et du point simple T sont calculées avec la fonction symétrique élémentaire "somme des racines" .

Avec le calcul nous obtenons les coordonnées :

$$\begin{cases} x_{2P} = y'^2 + a_1 y' - a_2 - 2x_P \\ y_{2P} = -y'^3 - 2a_1 y'^2 + (a_2 - a_1^2 + 3x_P) y' + a_1(a_2 + 2x_P) - y_P - a_3 \end{cases}$$

avec

$$y' = \frac{3x_P^2 + 2a_2x_P + a_4 - a_1y_P}{2y_P + a_1x_P + a_3}$$

Nous avons démontré la :

Proposition 3 :

Soit une courbe elliptique E , de groupe de Mordell-Weil $E(K)$, d'équation de Weierstrass :

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

Alors le point $2P$, pour $P = (x_P, y_P)$; a pour coordonnées :

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

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

$$y' = \frac{3x_P^2 + 2a_2x_P + a_4 - a_1y_P}{2y_P + a_1x_P + a_3}$$

□

Définition 3 :

Un sous groupe de m -torsion d'une courbe elliptique E est l'ensemble des points P d'ordre m :

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

Dans le cas particulier d'une courbe elliptique d'équation de Weierstrass :

$$y^2 = x^3 + ax + b \in \mathbb{Q}[x, y]$$

les coordonnées du point mP sont déterminées par les formules de récurrences de Cassels [1]:

Proposition 4 :

Soit une courbe elliptique E d'équation de Weierstrass :

$$y^2 = x^3 + ax + b \in \mathbb{Q}[x, y] \text{ et } 4a^3 + 27b^2 \neq 0$$

Alors les coordonnées du point mP pour $P = (x, y)$ sont de la forme :

$$mP = \left[\frac{\phi_m}{\psi_m^2}, \frac{\omega_m}{\psi_m^3} \right]$$

Les polynômes $\psi_m \in \mathbb{Z}[a, b, x, y]$ satisfont les formules de récurrence :

$$\psi_{-1} = -1, \psi_0 = 0, \psi_1 = 1, \psi_2 = 2y, \psi_3 = 3x^4 + 6ax^2 + 12bx - a^2,$$

$$\psi_4 = 4y(x^6 + 5ax^4 + 2bx^3 - 5a^2x^2 - abx - a^3 - 8b^2)$$

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

$$2y\psi_{2m} = \psi_m(\psi_{m+2} \psi_{m-1}^2 - \psi_{m-2} \psi_{m+1}^2) \text{ pour } m \geq 3.$$

Les polynômes ϕ_m et ω_m satisfont les relations:

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

$$4y\omega_m = \psi_{m+2} \psi_{m-1}^2 - \psi_{m-2} \psi_{m+1}^2$$

Preuve :

Pour $m = -1$, $-P = (x, -y)$; cela implique $\psi_{-1} = -1$.

Pour $m = 0$: $0P = O_E = (\infty, \infty) = \left[\frac{\phi_0}{\psi_0^2}, \frac{\omega_0}{\psi_0^3} \right]$. On trouve $\psi_0 = 0$.

Pour $m = 1$: $1.P = (x, y) = \left(\frac{x}{1^2}, \frac{y}{1^3} \right)$. On trouve $\psi_1 = 1$.

Pour $m=2$: les coordonnées du point $2P$ impliquent $\psi_2=2y$.

En utilisant une récurrence sur l'entier m , on obtient le résultat annoncé.

□

Exemple 1:

Soit E une courbe elliptique d'équation de Weierstrass :

$$E : y^2 = x^3 - 4x^2 - 11x + 30 \in \mathbb{Q}[x, y]$$

Calcul des invariants de E :

$$a_1=0, a_2=-4, a_3=0, a_4=-11, a_6=30$$

$$b_2=-16, b_4=-22, b_6=120, b_8=-601, c_4=784, c_6=-9152, \Delta(E)=230400=2^{10} \cdot 3^2 \cdot 5^2$$

Les points d'intersection de E avec l'axe Ox sont :

$$P_1=(-3,0), P_2=(2,0), P_3=(5,0).$$

Les points P_1, P_2 et P_3 sont d'ordre 2 par une propriété de la tangente à la courbe E en un point d'intersection de Ox par E .

Soit le point $Q=(1,4)$ de la courbe elliptique E .

En utilisant les formules usuelles nous obtenons les coordonnées des points $2Q, 3Q$:

$$2Q=(6,6), 3Q=\left(-\frac{71}{25}, -\frac{308}{125}\right).$$

Utilisons les formules de la proposition 2 pour calculer les coordonnées des points $5Q$ et $6Q$:

$$6Q=(x_6, y_6)=\left[\frac{\phi_6}{\psi_6^2}, \frac{\omega_6}{\psi_6^3}\right] \text{ avec } \phi_6=\psi_6^2-\psi_5\psi_7, \omega_6=\frac{\psi_5^2\psi_8-\psi_4\psi_7^2}{16},$$

$$\psi_6=\frac{\psi_3[\psi_2^2\psi_5-\psi_1\psi_4^2]}{\psi_2}.$$

Les calculs impliquent les coordonnées :

$$x_6=\frac{167686199863181611892736}{(-51673825280)^2}$$

$$y_6=\frac{-663491010924553813079837491687590000}{(-51673825280)^3}$$

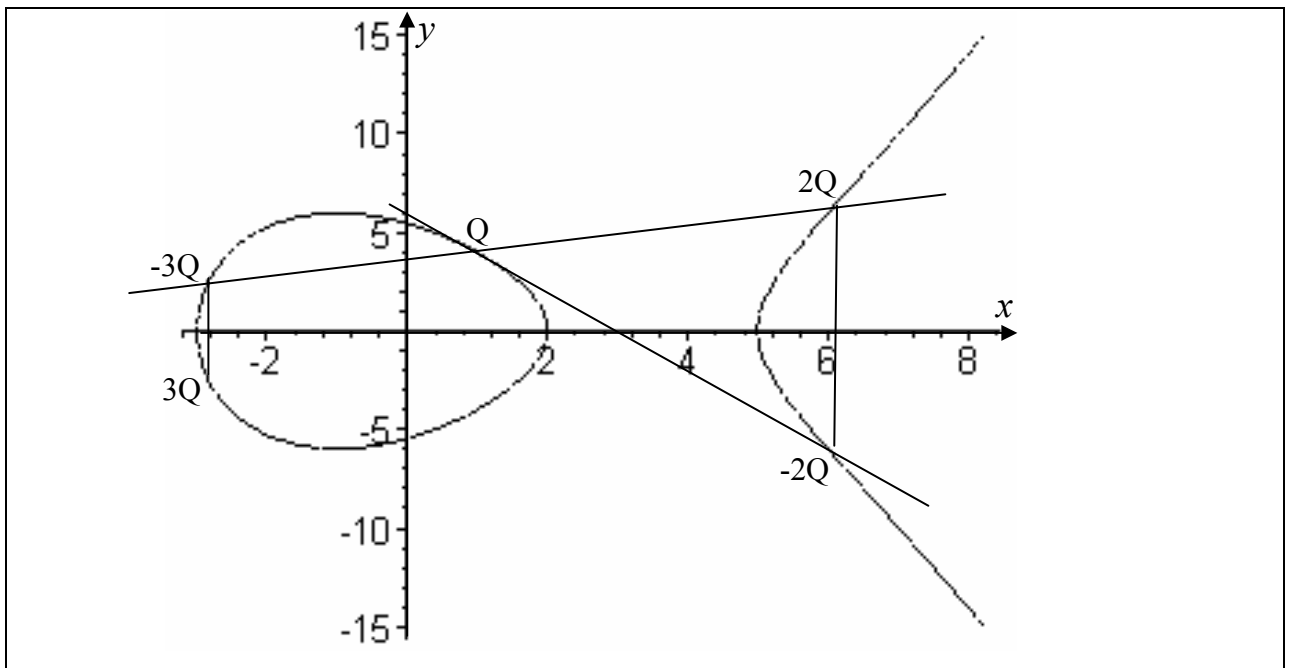
$$7Q = (x_7, y_7) = \left[\frac{\phi_7}{\psi_7^2}, \frac{\omega_7}{\psi_7^3} \right] \text{ avec } \phi_7 = \psi_7^2 - \psi_6\psi_8, \omega_7 = \frac{\psi_6^2\psi_9 - \psi_5\psi_8^2}{16}, \psi_7 = \psi_3^3\psi_5 - \psi_4^3\psi_2.$$

Les calculs impliquent les coordonnées :

$$x_7 = -\frac{573977351664}{2226553402896}$$

$$y_7 = \frac{98212629034018061599968}{17213680749818601740232}$$

La courbe elliptique E :



Définition 4 :

Le sous groupe de torsion du groupe de Mordell-Weil $E(K)$ est l'ensemble des points d'ordre fini de la courbe .

C'est la réunion infinie des sous groupes de m -torsion :

$$T(E) = \bigcup_{m \geq 1} E(K)[m]$$

La structure des groupes de torsion $T(E(K))$ a été déterminée dans les cas particuliers :

$K = \mathbb{Q}$ = corps des nombres rationnels, $K = \mathbb{Q}(\sqrt{d})$ = corps de nombres quadratique, ...

Proposition 5 :

Soit une courbe elliptique E sur le corps $\mathbb{Q}$ des nombres rationnels .

Alors le groupe de torsion $T(E(\mathbb{Q}))$ est isomorphe à l'un des 15 groupes abéliens :

$$\mathbb{Z}/m\mathbb{Z} \quad 1 \leq m \leq 10 \text{ ou } m = 12$$

$$\text{ou } \mathbb{Z}/2m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad 1 \leq m \leq 4$$

Preuve : (cf.[7])

Ce théorème a été conjecturé par A.Ogg et démontré par B.Mazur en 1976 [7].

Ce théorème implique que le sous groupe de torsion $T(E(\mathbb{Q}))$ est un groupe abélien d'ordre fini .
Mazur utilise un raisonnement par l'absurde pour démontrer que la courbe elliptique ne possède pas de point P d'ordre 11 et pas de points P d'ordre $m > 12$.

□

Les coordonnées d'un point de m -torsion satisfont la :

Proposition 6 :

Soit une courbe elliptique E sur le corps $\mathbb{Q}$ des nombres rationnels d'équation de Weierstrass :

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

Si le point $P = (x_P, y_P) \in E(\mathbb{Q})$ est d'ordre fini $m \geq 2$ et $2P \neq O_E$, ses coordonnées sont entières et y_P^2 divise $4A^3 + 27B^2$.

Preuve :

C'est le théorème de Nagell – Lutz :

(cf. [8])

□

Exemple 2:

Soit la courbe elliptique d'équation de Weierstrass :

$$E : y^2 = x^3 + 17x - 32 \in \mathbb{Q}[x, y] \quad (1)$$

$$4A^3 + 27B^2 = 47300 = 2^2 \cdot 5^2 \cdot 11 \cdot 43 \text{ et } \Delta(E) = -16(4A^3 + 27B^2) < 0 .$$

Les points de torsion du groupe $E(Q)$ sont les points $P=(x,y)$ tels que :

$$y^2 \text{ divise } 2^2 \cdot 5^2 \cdot 11 \cdot 43.$$

On détermine alors l'ensemble de tous les diviseurs carrés y_P^2 de $2^2 \cdot 5^2 \cdot 11 \cdot 43$.

Ce sont $y^2=1, 4, 25$ et 100 .

Tableau de valeurs des coordonnées de quelques points de la courbe :

x	0	1	2	4
y^2	-32	-14	10	100
y	Pas de y réel	Pas de y réel	$\pm \sqrt{10}$	± 10

$\Delta(E) = -16(4A^3 + 27B^2) = -47300 < 0$ implique que E est une courbe elliptique qui coupe l'axe Ox en un seul point, qui est simple.

Les abscisses associées sont les zéros des équations diophantiennes :

$$1) 1 = x^3 + 17x - 32$$

$$2) 4 = x^3 + 17x - 32$$

$$3) 25 = x^3 + 17x - 32$$

$$4) 100 = x^3 + 17x - 32$$

Pour $y=0$, l'équation cubique :

$$x^3 + 17x - 32 = 0$$

a 2 racines complexes conjuguées et une racine réelle comprise entre 1 et 2.

Pour $y=\pm 1$, l'équation cubique :

$$x^3 + 17x - 33 = 0$$

a 2 racines complexes conjuguées et une racine réelle comprise entre 1 et 2.

Pour $y=\pm 2$, l'équation cubique :

$$x^3 + 17x - 36 = 0$$

a 2 racines complexes conjuguées et une racine réelle comprise entre 1 et 2.

Pour $y=\pm 5$, l'équation cubique :

$$x^3 + 17x - 57 = 0$$

a 2 racines complexes conjuguées et une racine réelle comprise entre 2 et 3.

Pour $y=\pm 10$, l'équation cubique :

$$x^3 + 17x - 132 = 0$$

admet une racine $x=4$ et 2 racines complexes conjuguées.

Il en résulte les deux points $P_1=(4, -10)$ et $P_2=(4,10)$ symétriques par rapport à l'axe Ox .

Avec le calcul on obtient les coordonnées des points $2P_1, 3P_1$:

$$2P_1 = (4,10) = P_2, \quad 3P_1 = O_E \quad (2)$$

(2) implique que le sous groupe de torsion $T(E)$ est un groupe cyclique d'ordre 3 :

$$T(E) = \{O_E, P_1, P_2\}$$

Donc le sous groupe de torsion $T(E)$ est isomorphe au groupe cyclique $\mathbb{Z}/3\mathbb{Z}$.

Proposition 7 :

Le groupe de Mordell-Weil $E(K)$ des points K -rationnels d'une courbe elliptique E est de type fini .

C'est le théorème de Mordell-Weil .

Preuve : (cf. [12] , chap VIII).

□

La structure de ce groupe abélien est indiquée dans le :

Corollaire :

Le groupe de Mordell-Weil $E(K)$ d'une courbe elliptique E est isomorphe à un produit de groupes abéliens :

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

où $T(E)$ =groupe de torsion de E (groupe abélien fini)

$$r=r(E)=\text{entier} \geq 0.$$

$\mathbb{Z}^r = r$ copies du groupe additif abélien infini $\mathbb{Z}$.

Preuve : (cf. [12])

□

Définition 5 :

L'entier $r \geq 0$ de la relation d'isomorphisme $E(K) \cong T(E) \times \mathbb{Z}^r$ est le rang $r(E)$ d'une courbe elliptique E .

Application aux familles de courbes elliptiques à 2 paramètres $E(s,t)$:

1) Famille $E_1(s,t)$ d'équation de Weierstrass :

$$E_1(s,t) : y^2 = x(x^2 + 2(s+t)x + (s-t)^2) \in Q[x,y]$$

Le symétrique d'un point rationnel $P=(x_P, y_P)$ est le point :

$$-P=(x_P, -y_P)$$

La somme de 2 points $P_1=(x_1, y_1)$ et $P_2=(x_2, y_2)$ est le point :

$$P_1+P_2=(\lambda^2-2(s+t)-x_1-x_2, -\lambda^3+(2(s+t)+2x_1+x_2)\lambda-y_1)$$

$$\text{avec } \lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ pour } x_1 \neq x_2$$

Le point $2P = (y'^2 - 2(s+t) - 2x_P, -y'^3 + (2(s+t)+3x_P)y' - y_P)$

$$\text{avec } y' = \frac{3x_P^2 + 4(s+t)x_P + (s-t)^2}{2y_P}$$

2) Famille $E_2(s,t)$ d'équation de Weierstrass :

$$E_2(s,t) : y^2 = x(x^2 + sx + t) \in Q[x,y]$$

Le symétrique d'un point rationnel $P=(x_P, y_P)$ est le point :

$$-P=(x_P, -y_P)$$

La somme de 2 points $P_1=(x_1, y_1)$ et $P_2=(x_2, y_2)$ est le point :

$$P_1+P_2=(\lambda^2-s-x_1-x_2, -\lambda^3+(s+2x_1+x_2)\lambda-y_1)$$

$$\text{avec } \lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

Le point $2P = (y'^2 - s - 2x_P, -y'^3 + (s+3x_P)y' - y_P)$

$$\text{avec } y' = \frac{3x_P^2 + 2sx_P + t}{2y_P}$$

Le point $P_0=(0,0)$ est un point de 2-torsion de $E_2(s,t)$.

3) Famille $E_3(s,t)$ d'équation de Weierstrass :

$$E_3(s,t) : y^2 = x(x-s)(x-t) \in Q[x,y]$$

Le symétrique d'un point rationnel $P=(x_P, y_P)$ est le point :

$$-P=(x_P, -y_P)$$

La somme de 2 points $P_1=(x_1, y_1)$ et $P_2=(x_2, y_2)$ est le point :

$$P_1+P_2=(\lambda^2 + (s+t) - x_1 - x_2, -\lambda^3 + (-(s+t) + 2x_1 + x_2)\lambda - y_1)$$

avec $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$

Le point $2P = (y'^2 + (s+t) - 2x_P, -y'^3 + (-(s+t) + 3x_P)y' - y_P)$

avec $y' = \frac{3x_P^2 - 2(s+t)x_P + st}{2y_P}$

Les points P_0, P_1 et P_2 de cette courbe elliptique :

$P_0=(0,0)$, $P_1=(s,0)$ et $P_2=(t,0)$ satisfont :

$$2P_0=2P_1=2P_2=O_E$$

Donc ils sont d'ordre 2 .

Calcul des sommes $P_0 \pm P_1$, $P_0 \pm P_2$ et $P_1 \pm P_2$:

$2P_0=2P_1=2P_2=O_E$ implique $-P_0=P_0$, $-P_1=P_1$ et $-P_2=P_2$.

$$P_0 \pm P_1 = (t, 0) = P_2$$

$$P_0 \pm P_2 = (s, 0) = P_1$$

$$P_1 \pm P_2 = (0, 0) = P_0$$

Chapitre IV

MORPHISMES DE COURBES ELLIPTIQUES

Les morphismes de groupes s'appliquent aux groupes de Mordell-Weil $E(K)$ des courbes elliptiques : homomorphismes, endomorphismes, isomorphismes, isogénies, etc...

1. Isomorphismes de courbes elliptiques :

Proposition 1 :

Soit une courbe elliptique E d'équation de Weierstrass :

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

Alors l'homomorphisme de groupes de Mordell-Weil :

$$f : E(K) \rightarrow E'(K)$$

$$\text{de valeur } f(x,y) = (u^2X+r, u^3Y+su^2X+t), f(O_E) = O_{E'}$$

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

est un isomorphisme de courbes elliptiques :

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

Preuve :

Avec les formules de la somme de 2 points du groupe $E(K)$, nous obtenons la relation d'homomorphisme :

$$f(P_1+P_2) = f(P_1) + f(P_2) \text{ pour } P_i = (x_i, y_i)$$

Le changement de variables :

$$x = u^2X + r, y = u^3Y + su^2X + t$$

implique les coordonnées :

$$X = (x - r)/u^2, Y = (y - s(x - r) - t)/u^3$$

La condition $u \neq 0$ implique que la correspondance

$$x \rightarrow X, y \rightarrow Y$$

est bijective .

L'image $f(O_E)$ du point à l'infini de E est égale à $f(O_E) = O_{E'}$. $\square$

Les relations entre les invariants des 2 courbes elliptiques isomorphes E et E' sont obtenues par le calcul :

Relations entre les coefficients a_i et a'_i :

$$\begin{aligned}
 u a'_1 &= a_1 + 2s \\
 u^2 a'_2 &= a_2 - s a_1 + 3r - s^2 \\
 u^3 a'_3 &= a_3 + r a_1 + 2t \\
 u^4 a'_4 &= a_4 - s a_3 + 2r a_2 - (t + rs) a_1 + 3r^2 - 2st \\
 u^6 a'_6 &= a_6 + r a_4 - t a_3 + r^2 a_2 - r t a_1 + r^3 - t^2
 \end{aligned} \tag{1}$$

Relations entre les coefficients b_i et b'_i :

$$\begin{aligned}
 u^2 b'_2 &= b_2 + 12r \\
 u^4 b'_4 &= b_4 + r b_2 + 6r^2 \\
 u^6 b'_6 &= b_6 + 2r b_4 + r^2 b_2 + 4r^3 \\
 u^8 b'_8 &= b_8 + 3r b_6 + 3r^2 b_4 + r^3 b_2 + 3r^4
 \end{aligned} \tag{1-1}$$

Relations entre les coefficients c_i et c'_i :

$$\begin{aligned}
 u^4 c'_4 &= c_4 \\
 u^6 c'_6 &= c_6
 \end{aligned} \tag{1-2}$$

Relations entre les invariants :

Discriminants :

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

Invariants modulaires:

$$j(E') = j(E) \tag{1-3}$$

La relation $j(E') = j(E)$ permet de classifier les courbes elliptiques isomorphes .

Exemple :

Courbe elliptique E d'équation de Weierstrass :

$$E : y^2 + 3xy + 11y = x^3 - 5x^2 + 6x - 20 \in \mathbb{Q}[x, y]$$

Calcul de son discriminant $\Delta(E) = -882143$.

L'isomorphisme d'équation :

$$x=4X-3, \quad y=8Y-6X+9$$

transforme E en la courbe elliptique E' isomorphe à E :

$$E' : Y^2 + \frac{5}{2}Y = X^3 - \frac{47}{4}X^2 + \frac{33}{8}X - \frac{209}{64} \in \mathbb{Q}[x,y]$$

La relation $j(E) = j(E')$ permet de classifier les courbes elliptiques par leur invariant modulaire .

Proposition 2 :

2 courbes elliptiques E et E' sont isomorphes si et seulement si leurs invariants modulaires sont égaux .

Preuve de " E et E' isomorphes " implique " $j(E)=j(E')$ "

Soit 2 courbes elliptiques E et E' isomorphes .

Par la proposition 1 , cet isomorphisme a pour équation :

$$x=u^2X+r, \quad y=u^3Y+su^2X+t$$

La relation (1-3) implique $j(E)=j(E')$.

Preuve de " $j(E)=j(E')$ " implique " E et E' isomorphes "

Prenons 2 équations de Weierstrass :

$$E : y^2 = x^3 - 27c_4x - 54c_6 \in K[x,y] \quad (1)$$

$$E' : y^2 = x^3 - 27c'_4x - 54c'_6 \in K[x,y] \quad (1-1)$$

L'hypothèse $j(E)=j(E')$ implique l'égalité :

$$\frac{1728c_4^3}{c_4^3 - c_6^2} = \frac{1728c'_4^3}{c'_4^3 - c'_6{}^2}, \quad (2)$$

(2) implique $c_4^3 c'_6{}^2 = c'_4^3 c_6^2$ et 3 cas possibles :

1) Soit $c_4=0$ implique $j(E)=0$ et $c'_4=0$, $c_6 \neq 0$ et $c'_6 \neq 0$

On pose $u = \left(\frac{c_6}{c'_6} \right)^{1/6}$; 6 valeurs possibles de u .

alors les deux courbes elliptiques E et E' sont isomorphes par les isomorphismes :

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

2) Soit $c_6=0$, cela implique $j=1728$ et $c'_6=0$

$c_4 \neq 0$ et $c'_4 \neq 0$

On pose $u = \left(\frac{c_4}{c'_4} \right)^{1/4}$; 4 valeurs possibles de u .

3) Soit $c_4 \neq 0$ et $c_6 \neq 0$ alors $j \neq 0$, 1728

Cela implique $c'_4 \neq 0$ et $c'_6 \neq 0$

On pose $u = \left(\frac{c_6}{c'_6} \right)^{1/6} = \left(\frac{c_4}{c'_4} \right)^{1/4}$

On obtient l'isomorphisme entre E_1 et E_2 .

□

2. Isogénies de courbes elliptiques :

La notion d'isogénie de courbes elliptiques est d'un usage courant selon Shimura (cf. [11])

Définition 1 :

Une isogénie de 2 courbes elliptiques E et E' sur un corps K est un homomorphisme non nul de groupes abéliens :

$$\lambda : E(K) \rightarrow E'(K)$$

qui satisfait les conditions :

1) λ est surjectif .

2) le noyau de λ est d'ordre fini ;

3) $\lambda(P+Q) = \lambda(P) + \lambda(Q)$ pour tous points P et Q de la courbe E et $\lambda(O_E) = O_{E'}$

Chaque isogénie $\lambda : E(K) \rightarrow E'(K)$ possède 2 invariants :

Le degré $\deg(\lambda)$ et l'isogénie duale $\hat{\lambda}$ de λ .

Définition 2 :

1) le degré d'une isogénie λ est égal à l'ordre du noyau de λ .

2) l'isogénie duale d'une isogénie $\lambda : E(K) \rightarrow E'(K)$ de degré d est l'application

$$\hat{\lambda} : E'(K) \rightarrow E(K) \text{ qui satisfait les composées}$$

$$\hat{\lambda} \circ \lambda : E(K) \rightarrow E(K) \text{ est la multiplication par } d \text{ sur } E(K) .$$

$$\lambda \circ \hat{\lambda} : E'(K) \rightarrow E'(K) \text{ est la multiplication par } d \text{ sur } E'(K) .$$

$$\text{et } \deg(\hat{\lambda}) = \deg(\lambda) .$$

La multiplication par un entier rationnel $d \in \mathbb{Z}$ est l'endomorphisme $\lambda_d : E(K) \rightarrow E(K)$ de valeur

$$\lambda_d(P) = dP .$$

Proposition 3 :

Soit une courbe elliptique E sur un corps K , et un entier positif d .

Alors l'endomorphisme λ_d (multiplication par l'entier d) satisfait les propriétés :

- 1) $\deg \lambda_d = d^2$.
- 2) le noyau de l'endomorphisme λ_d est le sous groupe de d -torsion $E(K)[d]$.
- 3) si le corps K est de caractéristique 0 ou p premier avec l'entier d , alors :
ce sous groupe satisfait l'isomorphisme :

$$E(K)[d] \approx (Z/dZ) \times (Z/dZ)$$

Preuve :

- 1) (cf. [12] Théorème 6-2 , Chap III)
- 2) $\text{Ker}(\lambda_d) = \{ P \in E(K) \text{ tel que } \lambda_d(P) = O_E \} = \{ P \in E(K) \text{ tel que } dP = O_E \} = E(K)[d]$.
- 3) (cf. [12] corollaire 6-4 , Chap III)

□

L'ensemble $\text{End}_Z(E(K))$ des multiplications λ_d peut être muni d'une addition :

$$(\lambda_d + \lambda_{d'})(P) = \lambda_d(P) + \lambda_{d'}(P) = \lambda_{d+d'}(P)$$

La multiplication λ_0 par $d=0$ est l'élément neutre de cette addition :

$$(\lambda_d + \lambda_0)(P) = \lambda_d(P) + \lambda_0(P) = \lambda_d(P) + 0P = \lambda_d(P) + O_E = \lambda_d(P).$$

Il en résulte les formules $\lambda_d + \lambda_0 = \lambda_0 + \lambda_d = \lambda_d$.

$$\lambda_d \circ \lambda_{d'}(P) = \lambda_d(\lambda_{d'}(P)) = \lambda_d(d'P) = dd'P = \lambda_{dd'}(P)$$

Proposition 4 :

L'ensemble des multiplications $\lambda_d : E(K) \rightarrow E(K)$ par les entiers rationnels d est un anneau $\text{End}(E)$ isomorphe à l'anneau Z .

Preuve :

L'application $Z \rightarrow \text{End}(E)$ qui associe à tout entier d la multiplication λ_d est un isomorphisme d'anneaux.

□

Exemple : multiplication par $d = -1$

$$\lambda_{-1}(P) = -P$$

Avec la formule du symétrique de P , nous obtenons

$$\lambda_{-1}(x, y) = (x, -y - a_1x - a_3)$$

Lorsque l'anneau $\text{End}(E)$ des endomorphismes est isomorphe à un anneau contenant strictement $\mathbb{Z}$, il contient des isogénies $\theta : E(K) \rightarrow E(K)$ qui ne sont pas des multiplications λ_d .

Définition 3 :

Une courbe elliptique E a une multiplication complexe lorsque l'anneau $\text{End}(E)$ contient l'anneau $\mathbb{Z}$.

La structure de cet anneau $\text{End}(E)$ a été complètement déterminée par Deuring.

Proposition 5 :

Soit une courbe elliptique E , sur un corps K , et l'anneau $\text{End}(E)$ des endomorphismes de E . Alors cet anneau est de l'un des 3 types :

- 1) $\text{End}(E)$ peut être isomorphe à $\mathbb{Z}$ lorsque le corps K est de $\text{car}(K)=0$;
- 2) $\text{End}(E)$ peut être isomorphe à un ordre d'un corps quadratique imaginaire.
- 3) $\text{End}(E)$ peut être isomorphe à un ordre de l'algèbre des quaternions sur le corps $\mathbb{Q}$ lorsque $\text{car}(K)=p>0$.

Preuve : (cf. [2]).

□

Définition 4 :

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 , l'entier naturel f est le conducteur de cet ordre.

Définition 5 :

L'algèbre des quaternions sur le corps $\mathbb{Q}$ des rationnels est une algèbre H simple, centrale, de rang 4.

Elle est engendrée par 3 éléments i, j, k qui satisfont les conditions :

$$i^2 = j^2 = k^2 = -1 ; i j = k ; j k = i ; k i = j ; i j = -j i ; j k = -k j ; k i = -i k .$$

i^2 et j^2 sont des nombres rationnels négatifs.

Exemple : Multiplication Complexe par $\sqrt{-2}$.

Les formules de l'isogénie sont :

$$(x, y) \rightarrow (-x, y\sqrt{-2})$$

d'après Rajwade (cf. [10]).

Proposition 6 :

Soit une courbe elliptique E sur un corps K son groupe de Mordell-Weil $E(K)$ et soit un sous groupe A d'ordre fini de $E(K)$.

Alors il existe une unique courbe elliptique E' et une isogénie λ de noyau A telle que :

$$\lambda : E \rightarrow E' = E/A .$$

Preuve : (cf. [12]) .□

La détermination d'isogénies de courbes elliptiques qui utilise cette proposition a été entreprise par Vélu dans [13] :

C'est la méthode de Vélu que nous allons décrire .

Méthode de Vélu :

Cet algorithme de calcul comporte plusieurs étapes :

(1) Courbe elliptique E d'équation de Weierstrass :

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

(2) Sous groupe fini F du groupe de Mordell-Weil $E(Q)$.

(3) Isogénie de noyau le sous groupe F

$$f : E \rightarrow E/F = E'$$

de valeur $f(x, y) = (X, Y)$

(4) L'ensemble F_2 des points d'ordre 2 de $F - \{O_E\}$.

(5) Une partie R de $F - \{O_E\} - F_2$ telle que :

$$F - \{O_E\} - F_2 = R \cup (-R) \text{ et } R \cap (-R) = \emptyset .$$

(6) La partie $S = F_2 \cup R$.

(7) $G(x, y) = x^3 + a_2x^2 + a_4x + a_6 - y^2 - a_1xy - a_3y$.

(8) Pour $Q = (x_Q, y_Q) \in S$, les dérivées partielles :

$$G'_x(Q) = \frac{\partial G}{\partial x}(x_Q, y_Q) = 3x_Q^2 + 2a_2x_Q + a_4 - a_1y_Q ,$$

$$G'_y(Q) = \frac{\partial G}{\partial y}(x_Q, y_Q) = -2y_Q - a_1x_Q - a_3 .$$

(9) Les nombres :

$$u_Q = (G'_y)^2 = 4x_Q^3 + b_2^2x_Q + 2b_4x_Q + b_6$$

$$t_Q = \begin{cases} G'_x(Q) & \text{si } Q \in F_2 \\ 2G'_x(Q) - a_1G'_y(Q) = 6x_Q^2 + b_2x_Q + b_4 & \text{si } Q \in R \end{cases}$$

(10) Les nombres :

$$t = \sum_{Q \in S} t_Q \quad \text{et} \quad w = \sum_{Q \in S} (u_Q + x_Q t_Q)$$

Cet algorithme de calcul induit la :

Proposition 7 :

Soit une courbe elliptique E d'équation de Weierstrass :

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

Soit un sous groupe F fini du groupe $E(\mathbb{Q})$ et d'invariant $b_2(E)$.

Soit une isogénie $f : E \rightarrow E/F = E'$, d'équations $(x,y) \rightarrow (X,Y)$ et les nombres t, w de la formule (10) et les coordonnées X, Y :

$$X = x + \sum_{Q \in S} \left[\frac{t_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2} \right]$$

$$Y = y - \sum_{Q \in S} \left[u_Q \frac{2y + a_1x + a_3}{(x - x_Q)^3} + t_Q \frac{a_1(x - x_Q) + y - y_Q}{(x - x_Q)^2} + \frac{a_1u_Q - G'_x G'_y}{(x - x_Q)^2} \right]$$

Alors la courbe isogène E' a pour équation de Weierstrass :

$$E' : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + (a_4 - 5t)X + a_6 - b_2t - 7w.$$

Preuve : (cf. [13]).

□

Exemple 1 :

Soit une courbe elliptique d'équation de Weierstrass :

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

Les coefficients de E sont égaux à :

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

Les invariants de E :

$$b_2 = -4, b_4 = 0, b_6 = 1, b_8 = -1, \Delta(E) = -11.$$

Soit le sous groupe F d'ordre 5 du groupe $E(\mathbb{Q})$ engendré par le point de 5-torsion

$P = (0,0) \in E(\mathbb{Q})$:

$$F = \{ P, 2P, 3P, 4P, 5P = O_E \}$$

En appliquant les formules des coordonnées de la somme de 2 points et des coordonnées du point $2P$ nous obtenons les résultats :

$$2P = (1, -1), 3P = (1, 0), 4P = (0, -1).$$

Alors la partie S de la formule (6) de l'algorithme est l'ensemble :

$$S = \{ P, 2P \}$$

Calcul des nombres t et w de la formule (10) de l'algorithme :

$$x_P=0, y_P=0, t_P=0, u_P=1, G'_x(P)=0, G'_y(P)=-1$$

$$x_{2P}=1, y_{2P}=-1, t_{2P}=2, u_{2P}=1, G'_x(2P)=1, G'_y(2P)=1$$

$$t=2, w=4.$$

Les formules X et Y de la proposition 4 impliquent :

$$\begin{cases} X = x + \frac{1}{x^2} + \frac{2}{x-1} + \frac{1}{(x-1)^2} \\ Y = y - \frac{2y+1}{x^3} - \frac{2y+1}{(x-1)^3} - \frac{2y+1}{(x-1)^2} \end{cases}$$

Nous obtenons l'équation de Weierstrass de la courbe isogène :

$$E': Y^2 + Y = X^3 - X^2 - 10X - 20.$$

Exemple 2 :

Soit la famille de courbes elliptiques $E_3(s, t)$ à 2 paramètres d'équation de Weierstrass :

$$E_3(s, t) : y^2 = x(x-s)(x-t) \in Q[x, y]$$

Les coefficients de la courbe elliptique $E_3(s, t)$ sont égaux à :

$$a_1(s, t) = 0, a_2(s, t) = -(s+t), a_3(s, t) = 0, a_4(s, t) = st, a_6(s, t) = 0;$$

Les invariants de $E_3(s, t)$:

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

$$c_4(s, t) = 16(s^2 - st + t^2), c_6(s, t) = 2^5(2s^3 + 2t^3 - 3s^2t - 3st^2).$$

Calcul du discriminant :

$$\Delta(E_3(s, t)) = 2^4 s^2 t^2 (s-t)^2.$$

Les 3 points $P_0 = (0, 0)$, $P_1 = (s, 0)$ et $P_2 = (t, 0)$ satisfont :

$$2P_0 = 2P_1 = 2P_2 = O_{E_3}$$

Donc P_0, P_1, P_2 sont des points de 2-torsion de la courbe elliptique .

Soit le sous groupe F d'ordre 2 du groupe $E_3(Q(s,t))$ engendré par le point $P_0 = (0,0)$:

$$F = \{ P_0, 2P_0 = O_{E_3} \}$$

Calcul des nombres t et w de la formule (10) :

On remplace le nombre t de la formule (10) par v , pour ne pas le confondre avec le paramètre t .

L'ensemble F_2 des points d'ordre 2 de $F - \{ O_{E_3} \}$ est trivial :

$$F_2 = \{ P_0 \}$$

La partie R est vide car le sous groupe F ne contient pas de point d'ordre > 2 .

D'où la partie $S = F_2 = \{ P_0 \}$.

Le polynôme de 2 variables $G(x,y) = x(x-s)(x-t) - y^2$.

Les dérivées partielles de $G(x,y)$:

$$G'_x(x,y) = 3x^2 - 2(s+t)x + st ;$$

$$G'_y(x,y) = -2y .$$

Calcul des nombres v et w de la formule (10) de l'algorithme :

$$x_{P_0} = 0, y_{P_0} = 0, t_{P_0} = st, u_{P_0} = 0, G'_x(P_0) = st, G'_y(P_0) = 0$$

$$v = st, w = 0 .$$

Nous obtenons l'équation de la courbe isogène E' par l'isogénie de noyau F :

$$E' : Y^2 = X^3 - (s+t)X^2 - 4stX + 4st(s+t) \in Q[X,Y]$$

En posant $(X,Y) = (x+s+t, y)$, nous obtenons la courbe elliptique d'équation de Weierstrass :

$$E_I(s,t) : y^2 = x(x^2 + 2(s+t)x + (s-t)^2) \in Q[x,y]$$

Calcul du discriminant :

$$\Delta(E_I(s,t)) = 2^8 st(s-t)^4 .$$

L'isogénie est déterminée par les équations :

$$\begin{cases} X = x + \frac{st}{x} \\ Y = y - \frac{sty}{x^2} \end{cases}$$

C'est une isogénie du groupe $E_3(Q(s,t))$ dans le groupe $E_I(Q(s,t))$ de degré 2.

Soit le sous groupe F' d'ordre 2 du groupe $E_3(Q(s,t))$ engendré par le point $P_I = (s,0)$:

$$F' = \{ P_I, 2P_I = O_{E_3} \}$$

Calcul des nombres v et w de la formule (10) de l'algorithme :

L'ensemble F'_2 des points d'ordre 2 de $F' - \{O_{E_3}\}$ est :

$$F'_2 = \{P_1\}$$

La partie R est vide .

Donc la partie S = $F'_2 = \{P_1\}$.

$$x_{P_1} = s, y_{P_1} = 0, t_{P_1} = s(s-t), u_{P_1} = 0, G'_x(P_1) = s(s-t), G'_y(P_1) = 0$$

$$v = s(s-t), w = s^2(s-t) .$$

Nous obtenons l'équation de la courbe isogène $E_3(s,t)/F'$ par l'isogénie de noyau F' :

$$Y^2 = X^3 - (s+t)X^2 + (6st-5s^2)X - 3s^3 - 4st^2 + 7s^2t \in Q[X,Y]$$

En posant $(X,Y)=(x-s+t, y)$, on obtient la courbe elliptique d'équation de Weierstrass :

$$E_4(s,t) : y^2 = x(x^2 - 2(2s-t)x + t^2) \in Q[x,y]$$

Calcul du discriminant :

$$\Delta(E_4(s,t)) = 2^8 st^4 (s-t) .$$

L'isogénie est déterminée par les équations :

$$\begin{cases} X = x + \frac{s(s-t)}{x-s} \\ Y = y - \frac{s(s-t)y}{(x-s)^2} \end{cases}$$

C'est une isogénie du groupe $E_3(Q(s,t))$ dans le groupe $E_4(Q(s,t))$ de degré 2 .

Soit le sous groupe F'' d'ordre 2 du groupe $E_3(Q(s,t))$ engendré par le point $P_2 = (t,0)$:

$$F'' = \{P_2, 2P_2 = O_{E_3}\}$$

Calcul des nombres v et w de la formule (10) de l'algorithme :

L'ensemble F''_2 des points d'ordre 2 de $F'' - \{O_{E_3}\}$ est :

$$F''_2 = \{P_2\}$$

La partie R est vide .

Donc la partie S = $F''_2 = \{P_2\}$.

$$x_{P_2} = t, y_{P_2} = 0, t_{P_2} = -t(s-t), u_{P_2} = 0, G'_x(P_2) = -t(s-t), G'_y(P_2) = 0$$

$$v = -t(s-t), w = -t^2(s-t) .$$

Nous obtenons l'équation de la courbe isogène $E_3(s,t)/F''$ par l'isogénie de noyau F'' :

$$Y^2 = X^3 - (s+t)X^2 + (6st-5t^2)X - 3t^3 - 4s^2t + 7st^2 \in Q[X,Y]$$

En posant $(X,Y)=(x+s-t, y)$, on obtient la courbe elliptique d'équation de Weierstrass :

$$E_5(s,t) : y^2 = x(x^2 + 2(s-2t)x + s^2) \in Q[x,y]$$

Calcul du discriminant :

$$\Delta(E_5(s,t)) = -2^8 s^4 t(s-t).$$

L'isogénie est déterminée par les équations :

$$\begin{cases} X = x - \frac{t(s-t)}{x-t} \\ Y = y + \frac{t(s-t)y}{(x-t)^2} \end{cases}$$

C'est une isogénie du groupe $E_3(Q(s,t))$ dans le groupe $E_5(Q(s,t))$ de degré 2.

Soit l'exemple numérique pris dans [9] :

$$s = 2^{30}.5, t = -13.19^6 \text{ et } s-t = 3^{13}.11^2.31$$

Pour ces valeurs numériques, la courbe elliptique d'équation de Weierstrass :

$$E_3(2^{30}.5, -13.19^6) : y^2 = x(x-2^{30}.5)(x+13.19^6)$$

admet comme courbes isogènes :

$$1) E_1(2^{30}.5, -13.19^6) : y^2 = x(x^2 + 2(2^{30}.5 - 13.19^6)x + (3^{13}.11^2.31)^2)$$

de discriminant :

$$\Delta = -2^{38}.3^{52}.5.11^8.13.19^6.31^4$$

par l'isogénie de degré 2 et de noyau $F = \{ P_0=(0,0), 2P_0= O_{E_3} \}$, de valeur :

$(x,y) \rightarrow (X,Y)$ avec :

$$\begin{cases} X = x - \frac{2^{30}.5.13.19^6}{x} \\ Y = y + \frac{2^{30}.5.13.19^6 y}{x^2} \end{cases}$$

$$2) E_4(2^{30}.5, -13.19^6) : y^2 = x(x^2 - 2(2^{31}.5 + 13.19^6)x + 13^2.19^{12})$$

de discriminant :

$$\Delta = 2^{38}.3^{13}.5.11^2.13^4.19^{24}.31$$

par l'isogénie de degré 2 et de noyau $F' = \{ P_1=(2^{30}.5, 0), 2P_1= O_{E_3} \}$, de valeur :

$(x,y) \rightarrow (X,Y)$ avec :

$$\begin{cases} X = x + \frac{2^{30} \cdot 3^{13} \cdot 5 \cdot 11^2 \cdot 31}{x - 2^{30} \cdot 5} \\ Y = y - \frac{2^{30} \cdot 3^{13} \cdot 5 \cdot 11^2 \cdot 31y}{(x - 2^{30} \cdot 5)^2} \end{cases}$$

$$3) E_5(2^{30} \cdot 5, -13 \cdot 19^6) : y^2 = x(x^2 + 2(2^{30} \cdot 5 + 2 \cdot 13 \cdot 19^6)x + 2^{60} \cdot 5^2)$$

de discriminant :

$$\Delta = 2^{128} \cdot 3^{13} \cdot 5^4 \cdot 11^2 \cdot 13 \cdot 19^6 \cdot 31$$

par l'isogénie de degré 2 et de noyau $F'' = \{ P_2 = (-13 \cdot 19^6, 0), 2P_2 = O_{E_3} \}$, de valeur :

$(x, y) \rightarrow (X, Y)$ avec :

$$\begin{cases} X = x + \frac{3^{13} \cdot 11^2 \cdot 13 \cdot 19^6 \cdot 31}{x + 13 \cdot 19^6} \\ Y = y - \frac{3^{13} \cdot 11^2 \cdot 13 \cdot 19^6 \cdot 31y}{(x + 13 \cdot 19^6)^2} \end{cases}$$

Exemple 3 :

Soit la famille de courbes elliptiques $E_2(s, t)$ à 2 paramètres d'équation de Weierstrass :

$$E_2(s, t) : y^2 = x(x^2 + sx + t) \in Q[x, y]$$

On suppose que le polynôme $x^2 + sx + t$ est irréductible sur le corps Q des nombres rationnels .

Les coefficients de la courbe elliptique $E_2(s, t)$ sont égaux à :

$$a_1(s, t) = 0, a_2(s, t) = s, a_3(s, t) = 0, a_4(s, t) = t, a_6(s, t) = 0 ;$$

Les invariants :

$$b_2(s, t) = 4s, b_4(s, t) = 2t, b_6(s, t) = 0, b_8(s, t) = -t^2 .$$

Calcul du discriminant :

$$\Delta(E_2(s, t)) = 2^4 t^2 (s^2 - 4t) .$$

Le point $P_0 = (0, 0)$ est un point de 2-torsion de $E_2(Q(s, t))$.

Soit le sous groupe F d'ordre 2 du groupe $E_2(Q(s, t))$ engendré par le point $P_0 = (0, 0)$:

$$F = \{ P_0, 2P_0 = O_{E_2} \}$$

On détermine la courbe isogène $E_2(s, t)/F$ par l'isogénie de noyau le sous groupe F :

En appliquant les formules de Vélú , nous obtenons les résultats :

L'ensemble F_2 des points d'ordre 2 de $F - \{ O_{E_2} \}$ est trivial :

$$F_2 = \{ P_0 \}$$

La partie R est vide .

Donc la partie $S = F_2 = \{ P_0 \}$ est triviale .

Le polynôme de 2 variables $G(x,y) = x(x^2 + sx + t) - y^2$.

Les dérivées partielles de $G(x,y)$ sont égales à :

$$G'_x(x,y) = 3x^2 + 2sx + t ;$$

$$G'_y(x,y) = -2y .$$

Calcul des nombres v et w de la formule (10) de l'algorithme :

$$x_{P_0} = 0 , y_{P_0} = 0 , t_{P_0} = t , u_{P_0} = 0 , G'_x(P_0) = t , G'_y(P_0) = 0$$

$$v = t , w = 0 .$$

Nous obtenons l'équation de la courbe isogène $E_2(s,t)/F$ par l'isogénie de noyau F :

$$Y^2 = X^3 + sX^2 - 4tX - 4st \in Q[X,Y]$$

En effectuant le changement $(X,Y) = (x-s, y)$, on obtient la courbe elliptique d'équation de Weierstrass :

$$E_6(s,t) : y^2 = x(x^2 - 2sx + s^2 - 4t) \in Q[x,y]$$

Calcul du discriminant :

$$\Delta(E_6(s,t)) = 2^8 t(s^2 - 4t)^2 .$$

L'isogénie est déterminée par les équations :

$$\begin{cases} X = x + \frac{t}{x} \\ Y = y - \frac{ty}{x^2} \end{cases}$$

C'est une isogénie du groupe $E_2(Q(s,t))$ dans le groupe $E_6(Q(s,t))$ de degré 2 .

Nous choisissons les valeurs de Nitaj :

$$s = 40103941 , t = 2^{36} \cdot 7^2 \cdot 101$$

La courbe elliptique associée a pour équation de Weierstrass :

$$E_2(s, t) : y^2 = x(x^2 + 40103941x + 2^{36} \cdot 7^2 \cdot 101)$$

Elle admet comme courbe isogène la courbe elliptique :

$$E_6(s, t) : y^2 = x(x^2 - 2 \cdot 40103941x + 40103941^2 - 2^{38} \cdot 7^2 \cdot 101)$$

Son discriminant est égal à :

$$\Delta(E_6) = 2^{44} \cdot 7^2 \cdot 101 \cdot (40103941^2 - 2^{38} \cdot 7^2 \cdot 101)^2$$

par l'isogénie de degré 2 et de noyau $F = \{ O_{E_2}, P_0 = (0,0) \}$, de valeurs :

$(x,y) \rightarrow (X,Y)$ avec :

$$\begin{cases} X = x + \frac{2^{36} \cdot 7^2 \cdot 101}{x} \\ Y = y - \frac{2^{36} \cdot 7^2 \cdot 101 y}{x^2} \end{cases}$$

Conclusion :

Par définition, une isogénie de courbes elliptiques a un noyau non trivial ; un isomorphisme de courbes elliptiques a un noyau trivial, donc une isogénie n'est pas un isomorphisme.

Vérifions – le en calculant les discriminants et les invariants modulaires dans les exemples numériques précédents :

Exemple 1 :

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

$$E' : y^2 + y = x^3 - x^2 - 10x - 20$$

$$\Delta(E) = -11 \text{ et } j(E) = -\frac{16^3}{11}$$

$$\Delta(E') = -161051 \text{ et } j(E') = -\frac{464^3}{161051} \neq j(E).$$

Exemple 2 :

$$E_3(s,t) : y^2 = x(x-s)(x-t)$$

Pour les valeurs des paramètres s et t précédentes j'obtiens le discriminant et l'invariant modulaire :

$$\Delta(E_3) = 6,1693 \times 10^{57} \text{ et } j(E_3) = 22751.$$

Les courbes isogènes de E_3 sont :

$$1) E_1(s,t) : y^2 = x(x^2 + 2(s+t)x + (s-t)^2)$$

$$\Delta(E_1) = -1,0751 \times 10^{60} \text{ et } j(E_1) = 17,973 \neq j(E_3).$$

$$2) E_4(s,t) : y^2 = x(x^2 - 2(2s-t)x + t^2)$$

$$\Delta(E_4) = 1,1500 \times 10^{57} \text{ et } j(E_4) = 4,8390 \times 10^8 \neq j(E_3).$$

$$3) E_5(s,t) : y^2 = x(x^2 + 2(s-2t)x + s^2)$$

$$\Delta(E_5) = 7,7787 \times 10^{59} \text{ et } j(E_5) = 3508,7 \neq j(E_3).$$

Exemple 3 :

$$E_2(s,t) : y^2 = x(x^2 + sx + t)$$

$$\Delta(E_2) = 4,5887 \times 10^{44} \text{ et } j(E_2) = 1815,1.$$

La courbe isogène de E_2 est :

$$E_6(s,t) : y^2 = x(x^2 - 2sx + s^2 - 4t)$$

$$\Delta(E_6) = 5,3528 \times 10^{45} \text{ et } j(E_6) = 1,4092 \times 10^5 \neq j(E_2).$$

Perspectives:

En conclusion , cette étude des morphismes de courbes elliptiques $E(s,t)$ à 2 paramètres a permis d'obtenir des résultats intéressants . Elle sera complétée prochainement par l'étude d'autres aspects des courbes elliptiques : rang , twists , descentes , groupes de Châtelet-Weil $WC(E/Q)$, groupe de Selmer $S(E/Q)$, groupe de Shafarivich-Tate $III(E/Q)$, série de Hasse $L(E,s)$ de E ...

Bibliographie :

- [1] **J.W.S.Cassels** : "*Diophantine equations with special reference to elliptic curves*",
J. London Math . Soc. **41** (1966), 193-291)
- [2] **M.Deuring** : "*Die Typen der Multiplikatorenringe elliptischer Funktionenkörper* ",
Abh . Math . Sem . Hamburg **14** (1941),197-272 .
- [3] **R.Hartshorne** : "*Algebraic Geometry* ", *Graduate Texts in Mathematics* ,
Springer-Verlag , (1977) .
- [4] **Kostrikin** : "*Introduction à l'Algèbre* ",Mir-Moscou(2^e édition), (1984)
- [5] **S.Lang** : "*Elliptic Curves –Diophantine Analysis* ", Springer-Verlag , 1978 .
AMS : 10 B 45 , 10 F 99 , 14 G 25 , 14 H 25
- [6] **E.Lutz** : "*Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps p -adique* ",
J.Reine Angew . Math . **177** (1937) , 237-247 .
- [7] **B.Mazur** : "*Rationnel isogenies of prime degree* ",
Inventiones . Mathematicae . **44** (1978) . 129-162 .
- [8] **T.Nagell** : "*Solution de quelques problèmes dans la théorie arithmétique des
cubiques planes du premier genre* ", Wid . Akad . Skrifter Oslo **I** , (1935) , Nr . 1 .
- [9] **A. Nitaj** : "*Détermination de courbes elliptiques pour la conjecture de Szpiro* " ,
Acta Arith . LXXX . V4 (1998) , 351-376 .
- [10] **A.R.Rajwade** : "*Arithmetic on elliptic curves with Complex Multiplication by $\sqrt{-2}$* ",
Proc.Com . Phil . Soc **64** (1968) , 659-672 .
- [11] **G.Shimura** : "*Introduction to the Arithmetic Theory of Automorphic Functions*",
Princeton University . Press , (1971) .
- [12] **J.H.Silverman** : "*The Arithmetic of Elliptic Curves* ",*Graduate Texts in Mathematics*
Vol 106 , Springer- Verlag , Berlin , Heidelberg , NewYork ,Tokyo,(1986).
AMS : 14-01 , 11GXX , 14GXX , 14H52
- [13] **J. Vélu** : "*Isogénies entre courbes elliptiques* ",
Compte Rendus. Académie des Sciences , Paris , Série **273** ,(1971) , 238-241 .