N° d'ordre : 10 / 2005 – M / MT.

MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET DE LA RECHERCHE SCIENTIFIQUE

Université des Sciences et de la Technologie
Houari Boumediene

جامعة هواري بومدين
للعلوم والتكنولوجيا
U S T H B

Faculté de Mathématiques

**Mémoire présenté pour l'obtention du diplôme de Magister**

En **: MATHEMATIQUES**

Spécialité : **Algèbre et Théorie des Nombres**

Par M$^{elle}$ : **Soumia RAHMOUNI**

**Sujet :**

# Isogénies de courbes elliptiques

Soutenu publiquement le : 21 / Mai / 2005, devant le jury composé de :

| | | |
|---|---|---|
| **Mr K. BETINA,** | *Professeur à USTHB.* | ***Président*** |
| **Mr M. ZITOUNI,** | *Professeur à USTHB.* | ***Directeur de thèse*** |
| **Mr A. KESSI,** | *Professeur à USTHB.* | ***Examinateur*** |
| **Mr M. S HACHAICHI,** | *Maître de conférences à USTHB.* | ***Examinateur*** |
| **Mr B. BEN SEBAA,** | *Chargé de cours à USTHB.* | ***Examinateur*** |

# Remerciements

***Je voudrais exprimer ma gratitude à monsieur Mohamed ZITOUNI, professeur à L'USTHB, le directeur de la thèse pour la proposition de ce sujet, son aide durant la réalisation de cette thèse. Qu'il trouve ici l'expression de mon plus profond respect.***

***Je tiens également à remercier monsieur Kamel BETINA, professeur à L'USTHB, d'avoir accepter de présider le jury.***

***Je remercie également messieurs A. KESSI, professeur à L'USTHB, M. S HACHAICHI, maître de conférences à L'USTHB, B. BEN SEBAA, chargé de cours à L'USTHB, pour avoir bien voulu participer au jury.***

***Je tiens aussi à remercier tous ceux qui m'ont aidé pour la réalisation de cette thèse.***

# Sommaire

# Introduction

Les isogénies de courbes elliptiques ont été étudiées par plusieurs auteurs comme Velu [21], Mazur [12], Shimura [19], Cassels [3], Serre [17], etc.

Nous nous intéressons ici aux formules des isogénies de courbes elliptiques ;
Nous nous sommes inspirés de Velu [22] pour l'algorithme de construction d'une courbe elliptique p - isogène à une courbe elliptique.

Dans le chapitre 1, nous indiquons quelques points de la théorie arithmétique des courbes elliptiques.

Dans le chapitre 2, nous décrivons quelques propriétés géométriques des courbes elliptiques.

Dans le chapitre 3, nous construisons le groupe abélien sur l'ensemble E (K) des points rationnels.
Selon Mordell - Weil, ce groupe est de type fini.
Nous établissons les formules des coordonnées du symétrique avec la règle géométrique de 3 points colinéaires de la courbe elliptique et le point à l'infini $O_E = (\infty, \infty)$
comme élément neutre.
Nous étudions aussi dans ce chapitre la théorie des isogénies.

# *CHAPITRE I*
# *ARITHMETIQUE DES COURBES ELLIPTIQUES.*

**1 - Structures algébriques d'une courbe elliptique :**

Une courbe algébrique, dans le plan affine $\mathbb{A}^2(K)$ est déterminée par un polynôme $f(X, Y) \in K[X, Y]$.

Une courbe algébrique est donc l'ensemble des zéros d'un polynôme $f(X, Y)$ à coefficients dans un corps K, global, local ou fini :

Les polynômes de degré un définissent des droites :

$$f(X, Y) = d_1 X + d_2 Y + d_3 = 0 \qquad (1)$$

Les polynômes de degré 2 définissent des cercles de centre $(d_1, d_2)$ et rayon R :

$$f(X, Y) = (X - d_1)^2 + (X - d_2)^2 - R^2 = 0 \qquad (1 - 1)$$

et des coniques :

$$f(X, Y) = d_1 X^2 + d_2 XY + d_3 Y^2 + d_4 X + d_5 Y + d_6 = 0 \qquad (1 - 2)$$

Les polynômes de degré 3 définissent des cubiques.

$$f(X, Y) = d_1 X^3 + d_2 X^2 Y + d_3 XY^2 + d_4 Y^3 + d_5 X^2 + d_6 XY + d_7 Y^2 + d_8 X + d_9 Y + d_{10} = 0 \quad (1\text{-}3)$$

Les courbes algébriques contiennent des points simples et des points multiples.

Une courbe sans point multiple est lisse ; une courbe avec un point multiple est singulière.

Donc l'ensemble des cubiques, d'équations (1-3), est classifiée en 2 classes, par les points singuliers :

La classe des cubiques singulières et la classe des cubiques non singulières.

***Définition 1 :***

*Une courbe elliptique est une cubique plane E, non singulière, irréductible projective, d'équation de Weierstrass :*

$$E: \; y^2 z + a_1 xyz + a_3 yz^2 = x^3 + a_2 x^2 z + a_4 xz^2 + a_6 z^3 \in \mathbb{P}^2(K) \qquad (2)$$

***Définition 2***

*L'équation* (2) *est* ***l'équation de Weierstrass*** *de la courbe elliptique E dans le plan projectif* $\mathbb{P}^2(K)$.

Dans le plan affine $\mathbb{A}^2$, l'équation de Weierstrass de E est :

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

Les 5 coefficients $a_i$ sont des éléments d'un corps commutatif K, global ou local ou fini.
Les 2 variables *x* et *y* sont des racines de l'équation algébrique (2 - 1). Donc *x* et *y* sont des éléments d'une clôture algébrique du corps K.

La nature du corps K influe sur les propriétés de la courbe elliptique E.

Lorsque le corps K est un corps de nombres algébriques, il s'applique à la courbe elliptique E la Théorie des Nombres (Entiers Algébriques, Discriminants, Classes D'idéaux, Valuations, Equations Diophantiennes, Nombres Premiers, Fonctions Arithmétiques, comme la Fonction Zêta, Analyse p- Adique, Groupe de Galois, Ramification).

Lorsque le corps K est le corps des nombres complexes, il s'applique à la courbe elliptique E l'Analyse Complexe, (Réseaux, Tores, Isomorphismes Analytiques Complexes, Groupes de Lie, Formes Automorphes, Formes Modulaires) et la Géométrie Algébrique (Variétés Algébriques, Diviseurs, Théorème de Riemmann- Roch, Homologie, Cohomologie, Schémas, Courbes Algébriques Projectives).

Lorsque le corps K est un corps fini, il s'applique à la courbe elliptique E la Théorie des Corps Finis.

Lorsque le corps K est un corps de fonctions, il s'applique à la courbe elliptique E la Théorie des Corps de Fonctions.

Lorsque le corps K est un corps local, il s'applique à la courbe elliptique E la Théorie des Corps Locaux.

Une courbe elliptique a une structure de variété abélienne de dimension un.
Elle a une structure de schéma non singulier de dimension un.

**2 - Transformations de l'équation de Weierstrass :**

L'équation (2 - 1) peut être transformée au moyen de substitutions.
Lorsque la caractéristique du corps K est différente de 2, nous éliminons les monômes *xy* et *y* de l'équation (2 - 1) par le changement de variables linéaire :

$$(x, y) \to (x, \frac{y - a_1 x - a_3}{2}) \; ; \qquad (3)$$

Nous obtenons l'équation de Weierstrass :

$$E_1 : y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6 ; \qquad (3 - 1)$$

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

$$\begin{cases} b_2 = 4a_2 + a_1^2; \\ b_4 = a_1 a_3 + 2a_4; . \\ b_6 = a_3^2 + 4a_6; \end{cases} \qquad (3 - 2)$$

Les coefficients $b_{2i}$ sont des invariants de la courbe elliptique $E_1$.

Dans un corps de caractéristique $p \neq 2,3$, nous éliminons le monôme $x^2$ et le coefficient 4 de l'équation (3 -1) par le changement de variables linéaire :

$$(x, y) \to \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right); \qquad (4)$$

Nous obtenons l'équation de Weierstrass :

$$E_2 : y^2 = x^3 - 27c_4 x - 54c_6; \qquad (4 - 1)$$

Les coefficients $c_{2i}$ sont des polynômes « homogènes de degré $2i$ »

dans l'anneau $\mathbb{Z}[b_2, b_4, b_6]$ :

$$\begin{cases} c_4 = b_2^2 - 24b_4; \\ c_6 = -b_2^3 + 36b_2 b_4 - 216b_6; \end{cases} \qquad (4 - 2)$$

Les coefficients $c_{2i}$ sont des invariants de la courbe elliptique $E_2$.

**3 - Invariants d'une courbe elliptique :**

Une courbe elliptique E possède d'autres invariants, dont le discriminant $\Delta(E)$, l'invariant modulaire j(E), l'invariant différentiel $\omega(E)$, le rang $r(E)$, le conducteur $N(E)$, etc.

**a) Discriminant d'une courbe elliptique :**

***Définition 3 :***

*Le discriminant d'une courbe elliptique E est le polynôme homogène, de degré* 12*, dans l'anneau* $\mathbb{Z}[b_2, b_4, b_6, b_8]$ *égal à :*

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

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

*Le coefficient* $b_8$ *est déterminé par la relation :*

$$4b_8 = b_2 b_6 - b_4^2 \ ;$$

*$4b_8$ est un polynôme homogène, de degré 8, de l'anneau* $\mathbb{Z}[b_2, b_4, b_6]$ ;

La cubique d'équation de Weierstrass

$$\mathrm{E} : y^2 = x^3 + Ax + B \qquad (5)$$

a un discriminant égal à

$$\Delta(\mathrm{E}) = -16(4A^3 + 27B^2) \qquad (5 - 1)$$

Le discriminant de la courbe elliptique $\mathrm{E}_2$ est égal à :

$$\Delta(\mathrm{E}) = 8 \times 54^3 (c_4^3 - c_6^2) \qquad (5 - 2)$$

**Exemple :**

Le discriminant de la courbe d'équation de Weierstrass :

$$E_1 : y^2 - 7xy + 4y = x^3 - 5x^2 + 8x - 14$$

Les coefficients $b_2 = 29, \quad b_4 = -12, \ b_6 = -40, \quad b_8 = -326$ et le discriminant

$$\Delta(\mathrm{E}_1) = 370070 = 2 \times 5 \times 37007.$$

**b) Invariant modulaire d'une courbe elliptique :**

***Définition 4 :***

*L'invariant modulaire d'une courbe elliptique E est l'élément* j(E) *du corps K :*

$$\textit{égal à} \quad \mathrm{j}(\mathrm{E}) = \frac{c_4^3}{\Delta(E)} \qquad (6)$$

**Exemples :**

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

$$E_2 : y^2 + 6xy - 12y = x^3 - 10x^2 + 5x - 25$$

Nous obtenons avec le calcul $b_2 = -4, \quad b_4 = -62, \quad b_6 = 44, \quad b_8 = -105$,

Le discriminant $\Delta(\mathrm{E}_2) = 2^9 \times 5 \times 769$ et le coefficient $c_4 = 2^5 \times 47$ (6 - 1)

(6), (6 -1) impliquent $\mathrm{j}(\mathrm{E}_2) = \dfrac{2^6 \times 103823}{5 \times 769}$ (6 - 2)

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

$$E_3 : y^2 = x^3 + 4x + 3$$

Nous obtenons avec le calcul $b_2 = 0, \quad b_4 = 8, \quad b_6 = 12, \quad b_8 = -16$ et $c_4 = -2^6 \times 3$ (6 - 3)

La relation (5 - 1) implique $\Delta(\mathrm{E}_3) = -2^4 \times 499$ (6 - 4)

(6), (6 - 3) et (6 - 4) impliquent $\mathrm{j}(\mathrm{E}_3) = \dfrac{2^{14} \times 3^3}{499}$ (6 - 5)

**c) Invariant différentiel d'une courbe elliptique** :

***Définition 5 :***

*L'invariant différentiel d'une courbe elliptique est l'élément différentiel :*

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

*lié à la forme différentielle :*

$$dF = F'_x\,dx + F'_y\,dy,$$

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

$F'_y$ *est la dérivée partielle de F par rapport à y et*

$F'_x$ *est la dérivée partielle de F par rapport à x.*

**Exemple :**

1) l'invariant différentiel $\omega(E_1)$ de la cubique d'équation de Weierstrass :

$$E_1 : y^2 - 7xy + 4y = x^3 - 5x^2 + 8x - 14$$

$$\omega(E_1) = \frac{-dy}{F'_x} \qquad (7)$$

où $F(x, y) = y^2 - 7xy + 4y - x^3 + 5x^2 - 8x + 14$ (7 - 1)

$$F'_x = -7y - 3x^2 + 10x - 8 \qquad (7 - 2)$$

$$F'_y = 2y - 7x + 4 \qquad (7 - 3)$$

(7), (7 - 2) impliquent l'invariant différentiel $\omega(E_1) = \frac{-dy}{-7y - 3x^2 + 10x - 8}$ (7 - 4)

2) l'invariant différentiel $\omega(E_2)$ de la cubique d'équation de Weierstrass :

$$E_2 : y^2 + 6xy - 12y = x^3 - 10x^2 + 5x - 25$$

$$\omega(E_2) = \frac{dx}{G'_y} \qquad (8)$$

où $G(x, y) = y^2 + 6xy - 12y - x^3 + 10x^2 - 5x + 25$ (8 - 1)

$$G'x = 6y - 3x^2 + 20x - 5 \qquad (8 - 2)$$

$$G'y = 2y + 6x - 12 \qquad (8 - 3)$$

(8), (8 - 3) impliquent l'invariant différentiel : $\omega(E_2) = \frac{dx}{2y + 6x - 12}$ (8 - 4)

La présentation des autres invariants sera faite ultérieurement.

**4 - Points singuliers d'une courbe algébrique :**

Dans la théorie des points simples et des points multiples d'une courbe algébrique plane C c'est l'équation F($x$, $y$) = 0 de la courbe qui détermine la nature d'un point de C.

***Définition 6 :***

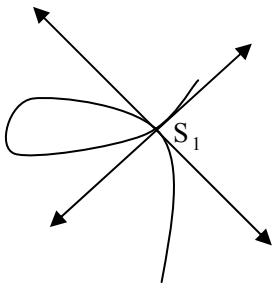
*Un point P = ($x$, $y$) d'une courbe algébrique plane C est singulier lorsqu'il satisfait les équations :*

$$F(P) = F'_x(P) = F'_y(P) = 0.$$

Il en résulte qu'un point singulier d'une courbe algébrique C est un point multiple de cette courbe.

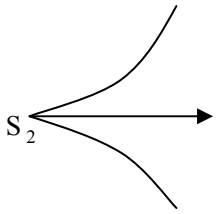
Donc pour une cubique, il n'y a qu'un seul point singulier, éventuellement.

1) Un nœud est un point singulier où la cubique admet 2 tangentes distinctes.
2) Un point de rebroussement est un point singulier où la cubique admet 2 tangentes confondues.




$S_1$ est un nœud.
(2 tangentes distinctes).

Figure -1 -




$S_2$ est un point de rebroussement.
(2 tangentes confondues).

Les courbes algébriques planes admettent un invariant géométrique, qui est le genre de la courbe.

***Définition 7 :***

*Soit une courbe algébrique C, d'équation projective f($x$, $y$, $z$) = 0, de degré n, admettant d points singuliers.*

*Le genre de cette courbe est l'entier non négatif ;*

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

Ainsi, une droite a une équation projéctive de degré $n$ = 1, donc son genre est égal à g = 0.

Les cercles et les coniques ont des équations projectives de degré $n = 2$, donc leur genre est égal à g = 0.

Les cubiques planes singulières ont une équation projective de degré $n = 3$ et un point singulier, leur genre est égal à g = 0.

Les courbes elliptiques sont des cubiques non singulières, elles ont une équation projective de degré 3, donc leur genre est égal à g = $\frac{(3-1)(3-2)}{2}$ -0 = 1.

**5 - Classification des cubiques planes suivant leurs discriminants :**

Le discriminant $\Delta(E)$ d'une courbe elliptique E d'équation $y^2 = f(x)$ est lié au dicriminant dis ($f$) de ce polynôme par la théorie du résultant.

Pour la théorie du résultant, nous avons consulté les ouvrages *Algebra de Lang et Introduction à l'Algèbre de Kostrikine.*

Nous exposons quelques points de la théorie :

***Définition 8 :***

*Soit deux polynômes f et g d'un anneau K*[$x$] *de la forme :*

$$f(x) = r_0 x^n + r_1 x^{n-1} + \ldots\ldots\ldots + r_n \quad \textit{de degré n.}$$

*et*

$$g(x) = s_0 x^m + s_1 x^{m-1} + \ldots\ldots\ldots + s_m \quad \textit{de degré m.}$$

*Le résultant des deux polynômes f et g est le déterminant d'ordre n + m, formé de m lignes de coefficients* $(r_0, r_1, \ldots\ldots, r_n)$ *et de n lignes de coefficients* $(s_0, s_1, \ldots\ldots s_m)$.

$$Res(f, g) = \begin{vmatrix} r_0 & r_1 & \ldots & \ldots & r_{n-1} & r_n & 0 & \ldots & \ldots & \ldots & \ldots & 0 \\ 0 & r_0 & r_1 & \ldots & \ldots & r_{n-1} & r_n & 0 & \ldots & \ldots & \ldots & 0 \\ 0 & 0 & r_0 & r_1 & \ldots & \ldots & r_{n-1} & r_n & 0 & \ldots & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & \ldots & \ldots & 0 & r_0 & r_1 & \ldots & \ldots & r_{n-1} & r_n & 0 \\ 0 & 0 & \ldots & \ldots & \ldots & 0 & r_0 & r_1 & \ldots & \ldots & r_{n-1} & r_n \\ s_0 & s_1 & \ldots & \ldots & \ldots & \ldots & s_{m-1} & s_m & 0 & \ldots & \ldots & 0 \\ 0 & s_0 & s_1 & \ldots & \ldots & \ldots & \ldots & s_{m-1} & s_m & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & s_0 & s_1 & \ldots & \ldots & \ldots & \ldots & s_{m-1} & s_m & 0 \\ 0 & \ldots & \ldots & 0 & s_0 & s_1 & \ldots & \ldots & \ldots & \ldots & s_{m-1} & s_m \end{vmatrix}$$

($m$ lignes ; $n$ lignes)

Le résultant Res (*f, g*) est un polynôme en les zéros de *f* et *g*.

***Proposition 1 :***

*Soit* 2 *polynômes :*

$$f(x) = r_0(x-u_1)(x-u_2).....(x-u_n) \quad (9)$$

$$g(x) = s_0(x-v_1)(x-v_2).....(x-v_m). \quad (9 - 1)$$

*Alors leur résultant est égal à* :

$$Res\ (f, g) = r_0^m s_0^n \prod_{i=1}^{n}\prod_{j=1}^{m}(u_i - v_j) \quad (9 - 2)$$

**Preuve :** (S.Lang Algebra)

□.

***Corollaire :***

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

$$Res\ (f, f') = r_0^{n-1}\prod_{i=1}^{n} f'(u_i) \quad (9 - 3)$$

□.

Le discriminant d'un polynôme *f*(*x*) est une fonction de ses racines.

Avec les racines de *f*(*x*), nous pouvons construire la différente et le discriminant de *f*

***Définition 9 :***

*Le discriminant d'un polynôme de degré n*

$f(x) = r_0(x-u_1)(x-u_2).....(x-u_n)$ *est égal à :*

$$dis\ (f) = r_0^{2n-2}\prod_{1\le i<j\le n}(u_i - u_j)^2 \quad (10)$$

Il en résulte que le discriminant est nul si et seulement si *f* admet une racine multiple.

Ce discriminant est lié au résultant de *f.*

***Proposition 2 :***

*Soit un polynôme* $f(x) = r_0(x-u_1)(x-u_2).....(x-u_n)$ *de degré n, son discriminant dis (f) et son résultant Res (f,* $f'$*) ;*

$$Alors\ Res\ (f, f') = (-1)^{\frac{n(n-1)}{2}} r_0\ dis\ (f) \quad (11)$$

□.

***Définition 10 :***

*Soit un polynôme f(x)* $= x^n + d_1 x^{n-1} + \ldots\ldots\ldots + d_n \in k\,[x]$ *sur un corps k.*

$$= (x-\lambda_1)\ldots\ldots\ldots(x-\lambda_n).$$

1) *La différente de f est égale à :*

$$D\,(f) = \prod_{1\le i<j\le n}(\lambda_i - \lambda_j)\,.$$

2) *Le discriminant du polynôme f est égal à :*

$$dis\,(f) = D(f)^2 = \prod_{1\le i<j\le n}(\lambda_i - \lambda_j)^2\,.$$

**Applications :**

Polynôme de degré 2, $f(x) = ax^2 + bx + c$

Le discriminant dis $(f) = b^2 - 4ac$ , Res $(f, f') = -ab^2 + 4a^2c$

Polynôme de degré 3, $f(x) = a_0x^3 + a_1x^2 + a_2x + a_3$

Avec la formule de Lang dans Algebra

$$\text{dis}\,(f) = a_1^2a_2^2 - 4a_0a_2^3 - 4a_1^3a_3 - 27a_0^2a_3^2 + 18a_0a_1a_2a_3$$

Application au polynôme $f(x) = 4x^3 + b_2x^2 + 2b_4x + b_6$ .

Alors dis $(f)$ est égal à

$4b_2^2b_4^2 - 16\times 8b_4^3 - 4b_2^3b_6 - 27\times 16b_6^2 + 8\times 18b_2b_4b_6 = 16(9b_2b_4b_6 - 8b_4^3 - b_2^2b_8 - 27b_6^2)$ .

Il en résulte dis $(f) = 16\,\Delta(\text{E})$.

Application au polynôme $f(x) = x^3 + Ax + B$

Soit l'équation de Weierstrass :

$$\text{E} : y^2 = x^3 + Ax + B \qquad (1)$$

Le changement de variables $(x, y) \to \left(x, \dfrac{y - a_1x - a_3}{2}\right)$ transforme (1) en :

$$\text{E}' : 4x^3 + 4Ax + 4B = 4x^3 + b_2x^2 + 2b_4x + b_6$$

Il en résulte dis $(f) = 16\,\Delta(\text{E})$

Nous avons démontré la :

***Proposition 3 :***

*Soit une courbe elliptique E d'équation de Weierstrass :*

$$E :\ y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 = f(x)\,,\ Alors\ \ dis\,(f) = 16\,\Delta(E)$$

L'invariant discriminant Δ(E) permet de classifier les cubiques.

***Proposition 4 :***

*Soit une cubique plane E d'équation de Weierstrass :*

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

*de dicriminant* Δ(E) *Alors :*

1) *Le point à l'infini* $O_E = (\infty, \infty)$ *n'est pas singulier sur la courbe E.*

2) *La cubique E est une courbe elliptique si et seulement si son discriminant n'est pas nul.*

**Preuve de $O_E$ est un point non singulier de la courbe E :**

Soit une cubique plane E d'équation de Weierstrass, dans le plan projectif $\mathbb{P}^2$.

$$E : f(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0 \qquad (1)$$

La dérivée partielle $\frac{df}{dZ} = Y^2 + a_1XY + 2a_3YZ - a_2X^2 - 2a_4XZ - 3a_6Z^2$ (1 - 1)

Dans le plan projectif $\mathbb{P}^2$, le point à l'infini est représenté par $O_E = (0, 1, 0)$

La valeur $f(0, 1, 0) = 0$ implique que $O_E$ est un point de E (1 - 2)

La valeur $\frac{df}{dZ}(0, 1, 0) = 1 \neq 0$ implique que le point $O_E$ n'est pas singulier sur la courbe E.

□.

**Preuve de « E est une courbe elliptique » implique « Δ(E) ≠ 0 ».**

Nous prenons l'équation de Weierstrass de E :

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 = h(x) \qquad (2)$$

L'hypothèse « courbe elliptique » implique que « le polynôme $h(x)$ admet trois racines distinctes »

$h(x) = 4(x-e_1)(x-e_2)(x-e_3) \in K[x, y]$ avec $e_i \neq e_j$ (2 - 1)

La définition des racines simples et multiples d'un polynôme $h(x)$ et la relation (2 -1) impliquent que les racines de la dérivée $h'(x)$ ne sont pas racines de $h(x)$ (2 - 2)

(2 - 2) implique le résultant $\text{Res}(h, h') \neq 0$ (2 - 3)

(2 - 3) et la proposition 2 impliquent la valeur $\text{dis}(h) \neq 0$ (2 - 4)

Par définition, les discriminants dis ($h$) et Δ(E) de la cubique E sont liés par la relation :

$\text{dis}(h) = 16\,\Delta(E)$ (2 - 5)

(2 - 4) et (2 - 5) impliquent $\Delta(E) \neq 0$.

□.

**Preuve de « Δ(E) ≠ 0 » implique « E est une courbe elliptique ».**

Nous gardons l'équation de (2)

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

L'hypothèse Δ(E) ≠ 0 et la relation (2 - 5) impliquent dis $(h) \neq 0$ (3 - 1)

La relation (3-1) et la proposition 2 impliquent la valeur du résultant Res $(h, h') \neq 0$ (3 - 2)

Le corollaire de la proposition 1 implique les polynômes $h(x)$ et $h'(x)$ n'ont pas de zéro commun.

Donc le polynôme $h(x)$ admet trois racines simples.

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

□.

Le signe du discriminant Δ(E) caractérise deux types de courbes elliptiques :

***Proposition 5 :***

*Soit une courbe elliptique E dans le plan affine* $\mathbb{A}^2(\mathbb{R})$ *de discriminant* Δ(E).

1) *la relation* Δ(E) > 0 *implique que la cubique E est une courbe elliptique qui coupe l'axe Ox en trois points distincts.*
2) *La relation* Δ(E) < 0 *implique que la cubique E est une courbe elliptique qui coupe l'axe Ox en un seul point.*

**Preuve :**

**Preuve de «Δ(E) > 0 »implique « la courbe elliptique E coupe l'axe O*x* en trois points distincts ».**

Soit une courbe elliptique E d'équation de Weierstrass :

$$E : y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6 = g(x) \in \mathbb{R}[x] \quad (1)$$

La relation dis $(g(x)) = 16\Delta(E)$ et l'hypothèse Δ(E) > 0 impliquent dis $(g(x)) > 0$ (1 - 1)

(1) et (1 -1) impliquent que le polynôme $g(x)$ admet 3 racines simples $e_1, e_2, e_3$

Il en résulte trois points d'intersection $P_i = (e_i, 0)$ de la courbe E avec l'axe O*x*.

□.

**Preuve de "Δ(E) < 0" implique "la courbe elliptique E coupe l'axe O*x* en un seul point".**

Un polynôme cubique admet 3 racines $e_i$, simples ou multiples :

$$E : y^2 = 4(x - e_1)(x - e_2)(x - e_3) = g(x) \in \mathbb{R}[x] \quad (1)$$

La relation dis $(g(x)) = 16\Delta(E)$ et l'hypothèse Δ(E) < 0 impliquent dis $(g(x)) < 0$

Par définition dis (g) est lié aux racines $e_i$ de g par :

$$dis(g) = 4^4 (e_1 - e_2)^2 (e_2 - e_3)^2 (e_3 - e_1)^2 \in \mathbb{R} \qquad (1 - 1)$$

La relation (1 - 1) implique un carré négatif.

Cela n'est possible que pour $e_1 = e$ réel, $e_2 = r + it$ et $e_3 = r - it$ complexes conjuguées.

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

$$= -4t^2 \left[ (e - r)^2 + t^2 \right]^2 < 0 .$$

Il en résulte un seul point d'intersection $P_1 = (e_1, 0)$ de la courbe E avec l'axe O*x*.

□.

**Exemples :**

1) Soit une cubique $E_1$ d'équation de Weierstrass:

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

Nous obtenons avec Le calcul les invariants $b_{2i}$

$b_2 = -8$, $b_4 = -2$, $b_6 = 4$, $b_8 = -9$ et le discriminant $\Delta(E_1) = 784 = 2^4 \times 7^2 > 0$ (1 - 1)

Il en résulte que la cubique $E_1$ est une courbe elliptique qui coupe l'axe O*x* en 3 points.

Logiciel Maple donne les abscisses $x_1$, $x_2$ et $x_3$ de ces points :

$$x_1 \approx -0{,}68, \quad x_2 \approx 0{,}47, \quad x_3 \approx 3{,}21 \qquad (1 - 2)$$

**Quelques points sur la courbe $E_1$ :**

| $x$ | -1 | $x_1$ | $\frac{-1}{2}$ | 0 | $x_2$ | $\frac{1}{2}$ | 1 | $\frac{5}{2}$ | 3 | $x_3$ | $\frac{7}{2}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y$ | Pas de $y$ réel | 0 | $\frac{-1-\sqrt{\frac{7}{2}}}{2}$ et $\frac{-1+\sqrt{\frac{7}{2}}}{2}$ | 1 et -1 | 0 | $\frac{1-\sqrt{\frac{1}{2}}}{2}$ et $\frac{1+\sqrt{\frac{1}{2}}}{2}$ | Pas de $y$ réel | $\frac{5-\sqrt{\frac{13}{2}}}{2}$ et $\frac{5+\sqrt{\frac{13}{2}}}{2}$ | $3-\sqrt{7}$ et $3+\sqrt{7}$ | 0 | $\frac{7-\sqrt{\frac{127}{2}}}{2}$ et $\frac{7+\sqrt{\frac{127}{2}}}{2}$ |

**La courbe elliptique $E_1$ coupe l'axe O*x* en 3 points $(x_1,0),(x_2,0)$ et $(x_3,0)$ qui sont simples.**

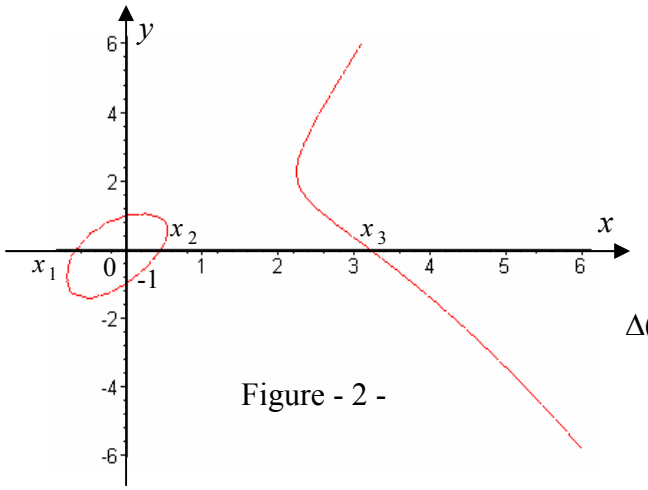



Figure - 2 -

$\Delta(E_1) > 0$

2) Soit une cubique $E_2$ d'équation de Weierstrass :

$$E_2 : y^2 + xy + 3y = x^3 + 5. \qquad (2)$$

Nous obtenons avec le calcul les invariants $b_{2i}$

$b_2 = 1,\ \ b_4 = 3,\ \ b_6 = 29, b_8 = 5$ et le discriminant $\Delta(E_2) =$ -22145 $= -5 \times 4429 < 0$ (2 - 1)

Il en résulte que la cubique $E_2$ est une courbe elliptique qui coupe l'axe O*x* en un seul point d'abscisse $x_4 = (-5)^{\frac{1}{3}}$ (2 - 2)

**Points particuliers de la courbe $E_2$ :**

| $x$ | -2 | $x_4$ | $\frac{-3}{2}$ | -1 | 0 | 1 | 2 |
|---|---|---|---|---|---|---|---|
| $y$ | Pas de racines $y$ réelles. | 0 | $\frac{-3-\sqrt{35}}{4}$ et $\frac{-3+\sqrt{35}}{4}$ | $-1-\sqrt{5}$ et $-1+\sqrt{5}$ | $\frac{-3-\sqrt{29}}{2}$ et $\frac{-3+\sqrt{29}}{2}$ | $-2-\sqrt{10}$ et $-2+\sqrt{10}$ | $\frac{-5-\sqrt{77}}{2}$ et $\frac{-5+\sqrt{77}}{2}$ |

**La courbe elliptique $E_2$ coupe l'axe O*x* en 1 seul point $(x_4,0)$ qui est simple.**

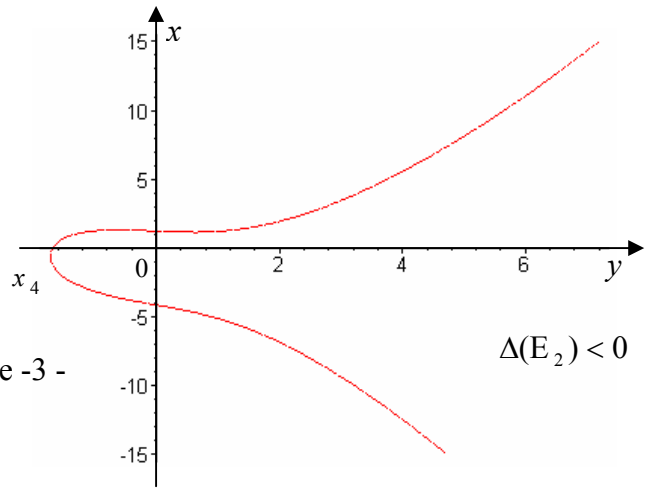



Figure -3 - $\Delta(E_2) < 0$

Nous nous intéressons aux cubiques singulières :

***Proposition 6 :***

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

1) *La cubique E admet un nœud 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* $\Delta(E) = 0$ *et* $c_4(E) = 0$

**Preuve de « la cubique E admet un nœud » implique « $\Delta(E) = 0$ et $c_4(E) \neq 0$ » :**

Nous prenons une cubique E d'équation de Weierstrass :

$$E : y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6 = h(x) \qquad (1)$$

L'hypothèse « E est singulière » implique que son discriminant est nul $\Delta(E) = 0$.

Par hypothèse la courbe admet un noeud.

Par définition d'un nœud, la courbe admet deux tangentes distinctes au nœud.

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

$$y' = \frac{6x^2 + b_2 x + b_4}{y} = \frac{f(x)}{y}; \qquad (2)$$

L'hypothèse de deux tangentes distinctes au nœud implique :

deux valeurs distinctes de $y'$ et deux racines distinctes du numérateur $f(x)$ (3)

Le discriminant du polynôme $f(x)$ de degré 2, a pour valeur : (4)

$$\text{dis}\,(f(x)) = b_2^2 - 24b_4 = c_4(E); \qquad (5)$$

Les relations (3) et (5) impliquent $c_4(E) \neq 0$ ;

□.

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

L'hypothèse « E est singulière » implique que son discriminant est nul $\Delta(E) = 0$.

Par hypothèse la courbe admet un point de rebroussement.

Par définition d'un point de rebroussement, la courbe admet deux tangentes confondues.

La pente de la tangente est la dérivée de $y$ :

$$y' = \frac{6x^2 + b_2 x + b_4}{y} = \frac{f(x)}{y}; \tag{6}$$

L'hypothèse « l'existence de deux tangentes confondues » implique une racine double du polynôme $f(x)$ (7)

Donc le discriminant dis ($f(x)$) est nul.

$$\text{dis } (f(x)) = b_2^2 - 24b_4 = c_4(\text{E}) = 0 \tag{8}$$

**Exemples :**

Nous construisons un exemple de chaque type de ces cubiques planes.

**1) Cubique plane non singulière de discriminant positif :**

Soit la cubique $\text{E}_1$ d'équation de Weierstrass :

$$\text{E}_1 : y^2 - 15y = x^3 - 30x - 5x^2 - 14 \tag{1}$$

Nous obtenons avec le calcul les invariants $b_{2i}$ et $\Delta(\text{E}_1)$ :

$$b_2 = -20, \quad b_4 = -60, \quad b_6 = 169, \quad b_8 = -1745 \text{ et } \Delta(\text{E}_1) = 3480053 > 0 \tag{2}$$

$\Delta(\text{E}_1) > 0$ implique que la cubique $\text{E}_1$ est une courbe elliptique qui coupe l'axe O$x$ en trois points :

Logiciel Maple donne les abscisses $x_1$, $x_2$ et $x_3$ de ces points :

$$x_1 \approx -3{,}11, \quad x_2 \approx -0{,}54 \text{ et } x_3 \approx 8{,}66 \tag{3}$$

**Quelques points de la courbe $E_1$:**

| $x$ | -5 | -4 | $x_1$ | -1 | -2 | $x_2$ | 0 | 1 | 8 | $x_3$ | $\frac{21}{2}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y$ | Pas de $y$ | $\frac{15-\sqrt{73}}{2}$ et $\frac{15+\sqrt{73}}{2}$ | 0 | $\frac{15-\sqrt{265}}{2}$ et $\frac{15+\sqrt{265}}{2}$ | $\frac{15-3\sqrt{33}}{2}$ et $\frac{15+3\sqrt{33}}{2}$ | 0 | 1 et 14 | $\frac{15-\sqrt{33}}{2}$ et $\frac{15+\sqrt{33}}{2}$ | Pas de $y$ | 0 | $\frac{15-\sqrt{\frac{2669}{2}}}{2}$ et $\frac{15+\sqrt{\frac{2669}{2}}}{2}$ |

**La courbe elliptique $E_1$ coupe l'axe O$x$ en 3 points $(x_1,0),(x_2,0)$ et $(x_3,0)$ qui sont simples.**

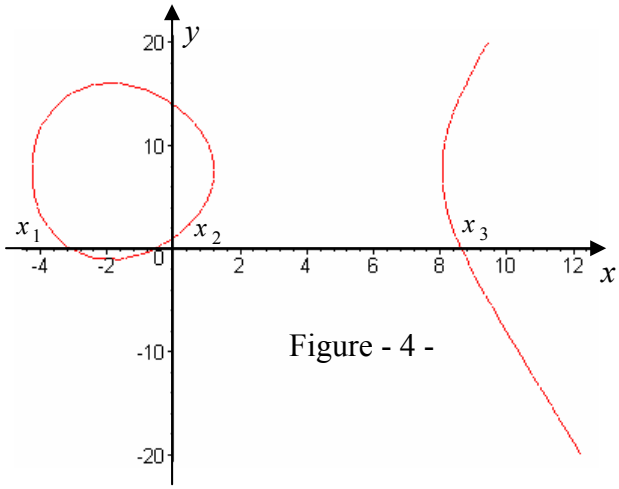



Figure - 4 -

**2) Cubique plane non singulière de discriminant négatif :**

Nous considérons la cubique $E_2$ d'équation de Weierstrass :

$$E_2: y^2+12y = x^3+5x^2+9x+14 \qquad (1)$$

Nous obtenons les invariants $b_{2i}$ et $\Delta(E_2)$ par le calcul :

$$b_2=20,\quad b_4=18,\quad b_6=200,\quad b_8=919 \text{ et } \Delta(E_2) = -846256 = -2^4\times 52891 < 0 \qquad (2)$$

Donc la cubique $E_2$ est une courbe elliptique qui coupe l'axe O$x$ en un seul point $x_4$.

Logiciel Maple donne l'abscisse $x_4$ de ce point :

$$x_4 \approx -3{,}52 \qquad (3)$$

**Quelques points de la courbe $E_2$:**

| $x$ | -4 | $x_4$ | -2 | -1 | $\frac{-1}{2}$ | 0 | -10 |
|---|---|---|---|---|---|---|---|
| $y$ | -6-$\sqrt{30}$ et -6+$\sqrt{30}$ | 0 | -6-2$\sqrt{11}$ et -6+2$\sqrt{11}$ | -6+3$\sqrt{5}$ et -6-3$\sqrt{5}$ | -6-$\sqrt{\frac{373}{8}}$ et -6+$\sqrt{\frac{373}{8}}$ | -6-$\sqrt{50}$ et -6+$\sqrt{50}$ | Pas de $y$ |

**La courbe elliptique $E_2$ coupe l'axe O*x* en 1 seul point $(x_4,0)$ qui est simple.**

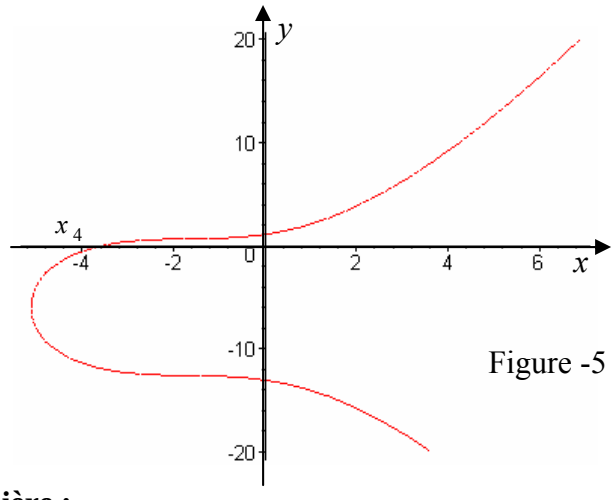



Figure -5 -

**3) Cubique plane singulière :**

Une cubique plane singulière n'est pas une courbe elliptique

**Cubique plane qui possède un nœud :**

Soit la cubique plane $E_3$ d'équation de Weierstrass :

$$E_3 : y^2 = x^3 - 12x + 16 \qquad (1)$$

Nous obtenons les invariants de $E_3$ par le calcul :

$b_2 = 0,\quad b_4 = -24,\ b_6 = 64,\ b_8 = -144,\quad c_4(E_3) = 576 = 2^6 \times 3^2$ et $\Delta(E_3) = 0$ (2)

$\Delta(E_3) = 0$ implique que la cubique plane $E_3$ est singulière

Cette cubique $E_3$ a un point singulier.

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

Les coordonnées de ce nœud sont les solutions du système de 3 équations algébriques :

$$\begin{cases} f(x,y) = y^2 - x^3 + 12x - 16 = 0; \\ \dfrac{df}{dx}(x,y) = -3x^2 + 12 = 0\,; \\ \dfrac{df}{dy}(x,y) = 2y = 0\,; \end{cases} \qquad (3)$$

Nous obtenons la solution (2,0) ;

Pour construire la courbe $E_3$, nous décomposons le $2^{éme}$ membre avec le :

**Théorème :**

*Soit une équation diophantienne :*

$$f(x) = x^n + d_1 x^{n-1} + \ldots\ldots\ldots + d_n = 0$$

*Toute solution de $f(x)$ est un diviseur du coefficient constant* $d_n$

□.

Ici $d_n = 16$, le test des diviseurs de 16 implique $f(2) = 0 = f(-4)$

Donc $f(x)$ admet 2 racines : $x_1 = -4$ et $x_2 = 2$.

Il en résulte la factorisation $x^3 - 12x + 16 = (x-2)(x-2)(x+4)$.

$$y^2 = x^3 - 12x + 16 = (x-2)^2(x+4) \qquad (4)$$

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

**Tableau de valeurs des coordonnées de quelques points :**

| $x$ | -4 | -3 | -2 | -1 | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|---|---|---|
| $y^2$ | 0 | 25 | 32 | 27 | 16 | 5 | 0 | 7 | 32 | 81 |
| $y$ | 0 | $\pm 5$ | $\pm 4\sqrt{2}$ | $\pm 3\sqrt{3}$ | $\pm 4$ | $\pm \sqrt{5}$ | 0 | $\pm \sqrt{7}$ | $\pm 4\sqrt{2}$ | $\pm 9$ |

**La cubique $E_3$ coupe l'axe O*x* en 1 seul point simple (-4, 0) et un point double (2, 0).**

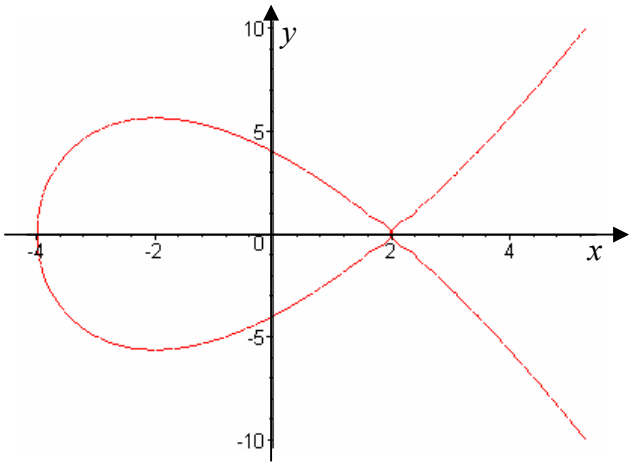



Figure - 6 -

**Cubique plane qui possède un point de rebroussement :**

Soit la cubique plane $E_4$ d'équation de Weierstrass :

$$E_4 : y^2 + 10y = x^3 - 25 \qquad (1)$$

Nous obtenons par le calcul les invariants de $E_4$ :

$$b_2 = 0,\quad b_4 = 0,\quad b_6 = 0,\quad b_8 = 0,\quad c_4(E_4) = 0 \text{ et } \Delta(E_4) = 0 \qquad (2)$$

$\Delta(E_4) = 0$ implique que la cubique plane $E_4$ n'est pas une courbe elliptique.

Cette cubique $E_4$ a un point singulier.

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

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

$$\begin{cases} f(x, y) = y^2 + 10y - x^3 + 25 = 0; \\ \dfrac{df}{dx}(x, y) = -3x^2; \\ \dfrac{df}{dy}(x, y) = 2y + 10; \end{cases} \qquad (3)$$

Nous obtenons la solution (0,-5) ;

**Tableau de valeurs des coordonnées de quelques points :**

| $x$ | -1 | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|---|
| $y$ | Pas de racines $y$ réelles. | -5 | -6 et- 4 | $-5-\sqrt{8}$ et $-5+\sqrt{8}$ | $-5-\sqrt{27}$ et $-5+\sqrt{27}$ | -13 et 3 |

**La cubique plane $E_4$ coupe l'axe O$y$ en 1 seul point d'abscisse $x$ = 0 et d'ordonnée $y$ = - 5.**

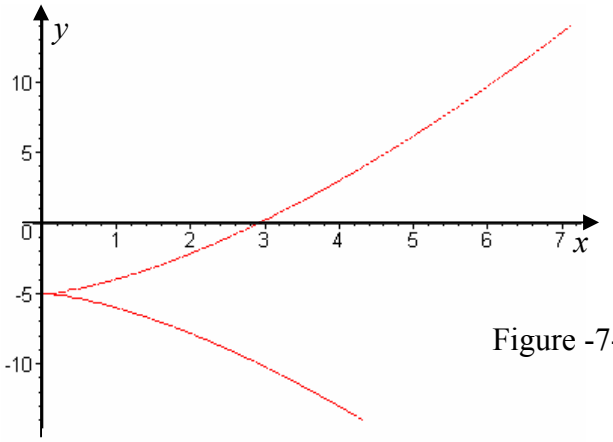



Figure -7-

Déterminons les courbes elliptiques d'équation de Weierstrass :

$$E : y^2 = x^3 + Ax + B \in K[x, y],\ 4A^3 + 27B^2 \neq 0$$ d'invariant modulaire j(E) fixé.

***Proposition 7 :***

*Soit une courbe elliptique E d'équation de Weierstrass* :

$$y^2 = x^3 + Ax + B \in K[x, y].$$

*Alors tout nombre n du corps K est l'invariant modulaire d'une courbe elliptique E.*

**Preuve :**

Soit une courbe elliptique E d'équation de Weierstrass :

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

Son invariant modulaire est égal à :

$$j(E) = \frac{4 \times 1728 A^3}{4A^3 + 27B^2},$$ pour un corps K de caractéristique différente de 2,3 (2)

Nous distinguons les trois cas :

$j(E) = 0$, $j(E) = 1728$ et $j(E) \neq 0,\ 1728$.

1) $j(E) = 0$ ; la formule (2) implique $A = 0$ et $B \neq 0$ (3)

Il en résulte l'équation de Weierstrass :

$$E_1 : y^2 = x^3 + B \quad \text{et} \quad \Delta(E_1) = -16(4A^3 + 27B^2) = -432 B^2 = -2^4 \times 3^3 B^2 \quad (4)$$

2) $j(E) = 1728$, la formule (2) implique $A \neq 0$ et $B = 0$ (5)

Il en résulte l'équation de Weierstrass :

$$E_2 : y^2 = x^3 + Ax \quad \text{et} \quad \Delta(E_2) = -64 A^3 = -2^6 A^3 \quad (6)$$

3) $j(E) = n \neq 0, 1728$ ; la formule (2) implique

$$108(4A)^3 = n(4A^3 + 27B^2) \quad (7)$$

En séparant $A^3$ et $B^2$ nous obtenons l'équation

$$4 A^3 (1728 - n) = 27 B^2 n \quad (8)$$

Cette équation algébrique est de degré 3 en A et de degré 2 en B ; le nombre $n \in$ K est un paramètre.

(8) se met sous la forme :

$$\frac{A^3 (1728 - n)}{27} = \frac{B^2 n}{4} \quad (9)$$

Nous en déduisons la solution :

$$A = \frac{3n}{1728 - n} \quad \text{et} \quad B = \frac{\pm 2n}{1728 - n} \quad (10)$$

Il en résulte les équations de Weierstrass :

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

et le discriminant $\Delta(\mathrm{E}) = -\frac{2985984n^2}{(1728-n)^3} = \frac{-2^{12}\times 3^6 n^2}{(1728-n)^3}$

□.

**Exemples :**

Courbe elliptique E d'invariant modulaire j(E) = *n* :

Pour $n = 1$, il y a 2 courbes elliptiques d'équations de Weierstrass :

$$\mathrm{E}_1 : \quad y^2 = x^3 + \frac{3}{1727}x + \frac{2}{1727} \quad \text{et} \quad \mathrm{j}(\mathrm{E}_1) = 1.$$

$$\mathrm{E}_2 : \quad y^2 = x^3 + \frac{3}{1727}x - \frac{2}{1727} \quad \text{et} \quad \mathrm{j}(\mathrm{E}_2) = 1.$$

Pour $n = 4$, il y a 2 courbes elliptiques d'équations de Weierstrass :

$$\mathrm{E}_3 : \quad y^2 = x^3 + \frac{3}{431}x + \frac{2}{431} \quad \text{et} \quad \mathrm{j}(\mathrm{E}_3) = 4.$$

$$\mathrm{E}_4 : \quad y^2 = x^3 + \frac{3}{431}x - \frac{2}{431} \quad \text{et} \quad \mathrm{j}(\mathrm{E}_4) = 4.$$

Pour $n = 6$, il y a 2 courbes elliptiques d'équations de Weierstrass :

$$\mathrm{E}_5 : \quad y^2 = x^3 + \frac{3}{287}x + \frac{2}{287} \quad \text{et} \quad \mathrm{j}(\mathrm{E}_5) = 6.$$

$$\mathrm{E}_6 : \quad y^2 = x^3 + \frac{3}{287}x - \frac{2}{287} \quad \text{et} \quad \mathrm{j}(\mathrm{E}_6) = 6.$$

# *CHAPITRE II*
# *LA GEOMETRIE DES COURBES ELLIPTIQUES.*

Une courbe elliptique possède une structure de variété abélienne de dimension 1. Dans ce chapitre nous exposons brièvement la théorie des espaces affines et projectifs.
Les notions d'espaces affines, d'espaces projectifs et de variétés abéliennes se trouvent dans des ouvrages de Géométrie Algébrique (*Hartshorne, Shafarevich, etc…*).

**1 - Espace algébrique affine :**

Les points rationnels ($x$, $y$) d'une cubique sont des zéros d'un polynôme.
Les zéros des polynômes forment des ensembles algébriques dans des espaces affines

***Définition 1 :***

*Le n- espace affine sur un corps algébriquement clos K est l'ensemble des n-uples d'éléments de K.*

$$\mathbf{A}^n(K) = \{(a_1,.....,a_n) = a, \quad a_i \in K \} \qquad (1)$$

*Un n - uple a est un point de l'espace affine, les éléments* $a_1 \ldots\ldots\ldots a_n$ *sont les coordonnées de ce point a.*

**2 - Ensemble algébrique dans un espace affine :**

La théorie algébrique des polynômes d'un anneau K [ $x_1,\ldots\ldots\ldots,x_n$ ] implique que tout polynôme $f$ admet des zéros dans un corps K algébriquement clos
Ces zéros forment un ensemble algébrique dans l'espace affine $\mathbf{A}^n$ (K).

***Définition 2 :***

*Un sous ensemble Y d'un espace affine* $\mathbf{A}^n$ *est un ensemble algébrique si et seulement si Y est l'ensemble des zéros d'un sous ensemble de polynômes de l'anneau K* [ $x_1,\ldots\ldots\ldots,x_n$ ] *des polynômes à n indéterminées.*

$$Y = \{a = (a_1,.....,a_n),\ f_1(a) = f_2(a) = ..... = f_j(a) = 0\,,\ f_i \in K\,[\,x_1,\ldots\ldots\ldots,x_n\,]\ \} \qquad (2)$$

Les opérations sur les ensembles algébriques sont précisées par la :

***Proposition 1 :***

1) *La réunion de deux ensembles algébriques dans un espace affine est un ensemble algébrique.*
2) *L'intersection d'une famille d'ensembles algébriques est un ensemble algébrique.*
3) *L'ensemble vide et l'espace affine* $\mathbf{A}^n$ *sont des ensembles algébriques.*

□.

Un espace affine $\mathbf{A}^n$ peut être muni d'une topologie.

***Définition 3 :***

*Dans la topologie de Zariski sur un espace affine les ensembles fermés sont les ensembles algébriques et les ensembles ouverts sont les complémentaires des fermés.*

**Exemples d'ensembles algébriques :**

1) Soit l'ensemble :

$V_1 = \{ x \in \mathbf{C},\ x^2 + 1 = 0 \}$; le polynôme de degré 2 admet 2 zéros $x = \pm i$, donc $V_1$ est un ensemble algébrique de 2 éléments dans l'espace affine $\mathbf{A}^1(\mathbf{C})$.

2) Soit l'ensemble :

$V_2 = \{P = (x, y) \in \mathbf{C}^2,\ x^2 - y^2 = 1\}$; le polynôme $x^2 - y^2 = 1$ admet une infinité de zéros

$$x = t, \quad y = \pm\sqrt{t^2 - 1}, \quad t \in \mathbf{C}$$

$V_2$ est un sous ensemble algébrique dans l'espace affine $\mathbf{A}^2(\mathbf{C})$, $\mathbf{C}$ = corps des nombres complexes.

***Définition 4 :***

*Une variété algébrique affine est un sous ensemble fermé irréductible dans un espace affine* $\mathbf{A}^n(K)$ *muni de la topologie de Zariski.*

**Exemple de variété affine :**

Soit l'espace affine $\mathbf{A}^3$ sur un corps algébriquement clos K :

L'ensemble :

$V_3 = \{(x, y, z) \in \mathbf{A}^3,\ y - x^2 = 0,\ z - x^3 = 0\}$ est formé des zéros :

$$x = t \in K, \quad y = t^2 \in K \quad \text{et} \quad z = t^3 \in K.$$

Donc $V_3$ est un ensemble algébrique, c'est une variété affine.

Toute variété affine possède des sous variétés et des variétés quasi affines :

***Définition 5 :***

1) *Une **sous variété affine** d'une variété affine X est une partie V de X qui a une structure de variété affine.*
2) *Une **variété quasi affine** dans une variété affine X est une partie ouverte V de X.*

Dans un anneau commutatif, il y a des sous anneaux et des idéaux. Les idéaux admettant un générateur sont principaux, ceux qui admettent 2 générateurs au moins, indépendants, sont ordinaires.

***Définition 6:***

*L'idéal d'une variété affine Y est l'ensemble des polynômes* $f \in K[x_1, \ldots\ldots, x_n]$ *qui s'annulent sur la variété Y.*

**3 - Variétés projectives :**

Nous considérons une relation binaire R sur l'espace affine $\mathbb{A}^{n+1} - \{(0,.....,0)\}$ :

« Deux points *a* et *b* de l'espace $\mathbb{A}^{n+1} - \{(0,.....,0)\}$ sont équivalents par la relation R »

$(a_0,.....,a_n)$ R $(b_0,.....,b_n)$ si et seulement si

$(a_0,.....,a_n) = \lambda\ (b_0,.....,b_n) = (\lambda b_0, \lambda b_1,..., \lambda b_n)$ pour un élément non nul $\lambda \in K$ .

Cette relation R satisfait les axiomes des relations d'équivalence dans l'espace $\mathbb{A}^{n+1} - \{(0,.....,0)\}$.

***Définition 7 :***

*L'espace projectif* $\mathbb{P}^n(K)$ *est l'ensemble quotient de l'espace affine* $\mathbb{A}^{n+1} - \{(0,.....,0)\}$ *par la relation d'équivalence R.*

Donc les éléments de l'espace projectif $\mathbb{P}^n(K)$ sont des classes d'équivalence.

Ces éléments sont représentés par des droites passant par l'origine.

**Exemple d'espace projectif :**

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

Le point à l'infini $O_E = (\infty, \infty)$ a pour coordonnées $O_E = (0, 1, 0) \in \mathbb{P}^2(\mathbb{R})$.

Cette classe est déterminée par la direction de l'axe O *y*.

Dans l'anneau $K[x_0, x_1,....., x_n]$ des polynômes associés à un espace projectif $\mathbb{P}^n(K)$, les polynômes sont homogènes.

Tout espace algébrique projectif $\mathbb{P}^n$ (K) peut être muni d'une structure de variété.

***Définition 8 :***

1) *Une variété projective de dimension n est une partie X de l'espace projectif* $\mathbb{P}^n$ (K), *qui est fermée et irréductible.*
2) *Une sous variété projective d'une variété projective X de dimension n est une partie V de X qui est irréductible et fermée.*
3) *Une variété quasi projective dans une variété projective X de dimension n est une partie V de X qui est ouverte.*

**Exemples :**

1) Soit l'espace projectif $\mathbb{P}^1(\mathbb{R})$ réel.

Il est formé des couples $(r_0, r_1)$, $r_0$, $r_1 \in \mathbb{R}$

Des polynômes homogènes de degré $a \geq 1$ : $f = r_0 x + r_1 y \in \mathbb{R}[x, y]$, $f = r_0 x^a + r_1 y^a$.

2) Soit l'espace projectif $\mathbb{P}^2(\mathbb{C})$ complexe.

Il est formé des triplets $(r_0, r_1, r_2)$, $r_0$, $r_1$ et $r_2 \in \mathbb{C}$

Des polynômes homogènes : $f = r_0 x + r_1 y + r_2 z \in \mathbb{C}[x, y, z]$,

$$g = r_0 x^4 + r_1 x^3 y + r_2 x^2 y^2 + r_3 y^4,$$

$$h = r_0 x^n + r_1 y^n + r_2 x^k y^{n-k}.$$

3) Soit l'espace projectif $\mathbb{P}^3(\mathbb{R})$ réel.

Il est formé des 4 - uples $(r_0, r_1, r_2, r_3)$, $r_0$, $r_1$, $r_2$ et $r_3 \in \mathbb{R}$

Des polynômes homogènes : $f = r_0 x + r_1 y + r_2 z + r_3 t \in \mathbb{R}[x, y, z, t]$,

$$g = r_0 x^2 yz + r_1 x^2 t^2 + r_2 xyzt,$$

$$h = r_0 x^n + r_1 x^{n-1} y + r_2 x^{n-2} y^2 + r_3 y^{n-1} x.$$

***Définition 9 :***

*La dimension d'un espace topologique X est le maximum des entiers n dans la chaîne ascendante* $Z_0 \subset Z_1 \subset ..... \subset Z_n$ *où les* $Z_i$ *sont des sous ensembles fermés irréductibles dans l'espace topologique X.*

**Exemples :**

Dimension $\mathbb{A}^1(K) = 1$, dimension $\mathbb{A}^2$ (K) = 2, dimension $\mathbb{A}^n$ (*K*) = *n.*

**4 - Variétés abéliennes :**

La notion de variété abélienne repose sur les fonctions régulières, les morphismes….
Nous examinons quelques notions sur les fonctions régulières.

***Définition 10 :***

*Soit une variété quasi affine Y dans un espace affine* $\mathbb{A}^n(K)$ *;*

*La fonction* $f: Y \to K$ *est régulière sur Y si et seulement si pour tout point P de Y il existe un voisinage ouvert U de Y qui contient le point P et des polynômes g, h dans l'anneau* $K[X_1, ....., X_n]$ *tels que* $f = g/h$ *sur U.*

Ces fonctions régulières possèdent des structures analytiques

***Proposition 2 :***

*Toute fonction régulière est continue.*

**Preuve :** Théorie des applications entre les espaces topologiques dans les ouvrages de topologie

□.

***Définition 11 :***

*Soit une variété quasi projective Y dans un espace projectif* $\mathbb{P}^n(K)$.

*La fonction* $f: Y \to K$ *est régulière sur Y si et seulement si pour tout point P de Y, il existe un voisinage ouvert U de Y contenant le point P, et des polynômes g, h homogènes de même degré dans l'anneau* $K[X_0, ....., X_n]$ *tels que* $f = g/h$ *sur U.*

Les morphismes de variétés sont des applications qui satisfont certaines conditions.

***Définition 12 :***

*Soient deux variétés X et Y affines ou quasi affines, projectives ou quasi projectives.*

*Un morphisme* $\varphi: X \to Y$ *est une application continue telle que pour tout ensemble ouvert U dans Y et pour toute fonction régulière* $f: U \to K$, *la fonction composée*

$f o \varphi: \varphi^{-1}(U) \to K$ *est régulière.*

***Proposition 3 :***

*La composée de deux morphismes de variétés est un morphisme de variétés*

**Preuve :**

Soit 2 morphismes $\varphi_1: X_1 \to X_2$ et $\varphi_2: X_2 \to X_3$ ; Alors la composée :

$\varphi_2 o \varphi_1: X_1 \to X_3$ est un morphisme.

□.

Nous construisons une variété abélienne à partir d'une variété de groupe.

***Définition 13 :***

*Une variété de groupe est une variété Y munie de deux morphismes f, g qui satisfont :*

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

La variété de groupe munie de cette loi de groupe abélien est une variété abélienne.

***Définition 14 :***

*Une variété abélienne est une variété de groupe munie d'une loi de groupe abélien.*

**Exemple :**

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

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

***Définition 15 :***

*Soit une variété Y d'un espace projectif $\mathbb{P}^n(K)$ ;*

*Le corps des fonctions de Y est l'ensemble K(Y) des fonctions régulières sur un ouvert U de la variété Y tel que deux fonctions régulières f et g sur les ouverts U, V de la variété Y satisfont :*

$$f(x) = g(x) \text{ pour tout point } x \in U \cap V.$$

**Exemple de corps des fonctions :**

Soit la variété V d'équation $f(x, y) = y^2 - 3y - x^3 + 4 = 0.$

Alors le corps des fonctions de cette variété est l'ensemble K (V) = K($x, y$) avec

$$f(x, y) = y^2 - 3y - x^3 + 4 = 0.$$

**5 - Diviseurs d'une variété et diviseurs d'une courbe :**

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

Nous exposons brièvement quelques propriétés des diviseurs d'une variété

Selon Hartshorne (*Algebraic Géometry*), toute courbe projective non singulière C de degré *d* dans le plan projectif $\mathbb{P}^2(K)$ est coupée par une ligne L de ce plan projectif en *d* points simples ou multiples.

***Définition 16 :***

*Un diviseur d'une courbe algébrique C est une somme formelle ;*

$D = \sum_{P_i \in C} n_i (P_i)$, *où les points* $P_i$ *sont les intersections de C par une droite L, et les* $n_i$ *sont les multiplicités des* $P_i$.

Lorsque la ligne L varie dans le plan projectif $\mathbb{P}^2(K)$ nous obtenons une famille de diviseurs de C.

Il y a plusieurs types de diviseurs :

1) Un diviseur D = (P) est premier.

2) Le diviseur nul : D = (0).

3) Un diviseur D = $\sum_{P_i \in C} n_i (P_i)$ est effectif si $n_i \geq 0$ pour tous les indices *i*.

4) D est principal s'il est égal au diviseur d'une fonction $f$ : $D = (f)$.

5) Le degré du diviseur D est l'entier rationnel deg D = $\sum n_i \in \mathbb{Z}$.

***Définition 17 :***

*L'ensemble des diviseurs d'une courbe algébrique C engendre un groupe libre qui est le groupe Div*(*C*) *des diviseurs de C.*

Une loi de groupe abélien est déterminée par l'addition de 2 diviseurs :

$$D = \sum_i n_i (P_i), \quad D' = \sum_i n_i' (P_i), \quad \text{alors } D + D' = \sum_i (n_i + n_i')(P_i).$$

***Proposition 4 :***

1) *L'ensemble* $Div(C)^0$ *des diviseurs de degré* 0 *forme un sous groupe du groupe Div*(*C*) *des diviseurs de la courbe C.*
2) *L'ensemble des diviseurs principaux de C, Prin*(*C*) *forme un sous groupe du groupe de diviseurs Div*(*C*).

**Preuve:** Shafarevich dans « Basic Algebraic Géometry »

□.

***Corollaire :***

*Les groupes quotients* $Div(C)/Div(C)^0$ *et* $Div(C)/\mathrm{Pr}in(C)$ *sont des groupes de classes de diviseurs.*

**Exemple 1 :**

Soit une fonction rationnelle :

$$f(x) = 3(x-1)^2 (x-2)(x+3)^4 (x-5)^{-5} (x+1)^{-3}.$$

Elle admet 3 zéros : $x_1 = 1$ d'ordre 2, $x_2 = 2$ d'ordre 1, $x_3 = -3$ d'ordre 4 et 2 pôles $x_4 = 5$ d'ordre 5 et $x_5 = -1$ d'ordre 3.

Alors le diviseur de $f$ égal à la somme formelle :

$$(f) = 2(P_1) + (P_2) + 4(P_3) - 5(P_4) - 3(P_5).$$

Le degré du diviseur $(f)$ est égal à deg $(f) = 2 + 1 + 4 - 5 - 3 = -1$

**Exemple 2 :**

Soit la courbe elliptique d'équation de Weierstrass :

$$\text{E} : \; y^2 - 20y = x^3 - 24x^2 + 95x + 40 \in \mathbb{Q}[x,y]$$

Nous considérons la droite L d'équation $x = 5$

Cette droite L coupe la courbe E en 2 points simples $\text{P}_1$ et $\text{P}_2$ et au point $\text{O}_E$ à l'infini

$x = 5$, implique les racines de l'équation $y^2 - 20y = 40$ en $y$, de racines simples

$$y = 10 \pm \sqrt{140} = 10 \pm 2\sqrt{35}.$$

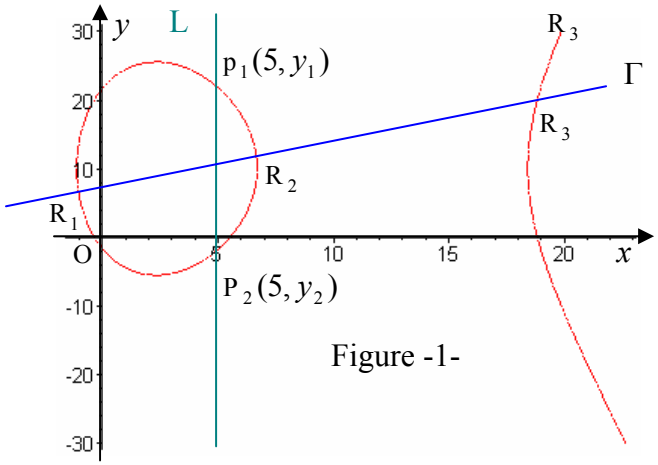



Figure -1-

La sécante L coupe E en 3 points $\text{P}_1$, $\text{P}_2$ et $\text{O}_E$.

Il en résulte que le diviseur associé à l'intersection E $\cap$ L est la somme formelle :

$$\text{D} = 1.(P_1) + 1.(P_2) + 3(O_E).$$

Soit une sécante $\Gamma$ qui coupe la courbe elliptique E en 3 points distincts $\text{R}_1$, $\text{R}_2$ et $\text{R}_3$.

Le diviseur de l'intersection $\Gamma \cap$ E est $\text{D} = (R_1) + (R_2) + (R_3)$

Ce diviseur D est linéairement équivalent au diviseur $D' = 3(O_E)$.

# *CHAPITRE III*
# *GROUPE DE MORDELL - WEIL D'UNE COURBE ELLIPTIQUE.*

Une loi de groupe sur une courbe elliptique peut être déterminée par la théorie des diviseurs sur une variété abélienne.

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

## 1 - Structure de groupe abélien sur l'ensemble E (K) des points K - rationnels d'une courbe elliptique E :

Soit une courbe elliptique E d'équation de Weierstrass :

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

Pour obtenir une structure de groupe abélien, nous considérons :

1) l'ensemble E(K) des points K- rationnels de la courbe elliptique E.
2) le point à l'infini $\mathrm{O}_E$ qui joue le rôle d'élément neutre ;

$\mathrm{O}_E = (\infty, \infty)$ dans le plan affine, et (0, 1, 0) dans le plan projectif $\mathbb{P}^2$ (K).

Ce point est unique. Il est déterminé par la direction de l'axe O*y* dans le plan projectif $\mathbb{P}^2$ ($\mathbb{R}$).

3) une loi de composition interne :

$$\mathrm{g} : \mathrm{E(K)} \times \mathrm{E(K)} \to \mathrm{E(K)}$$

$$\text{de valeur } \mathrm{g}(\mathrm{P}_1, \mathrm{P}_2) = \mathrm{P}_1 + \mathrm{P}_2 \qquad (1 - 1)$$

« Trois points $\mathrm{P}_i$ colinéaires de la courbe E ont une somme nulle ».

$$\mathrm{P}_1 + \mathrm{P}_2 + \mathrm{P}_3 = \mathrm{O}_E . \qquad (1 - 2)$$

La somme $\mathrm{M} = \mathrm{P}_1 + \mathrm{P}_2$ est obtenue par une construction géométrique : M est le symétrique par rapport à l'axe O*x* du troisième point d'intersection $\mathrm{P}_3$ de E par la sécante $\mathrm{P}_1\mathrm{P}_2$

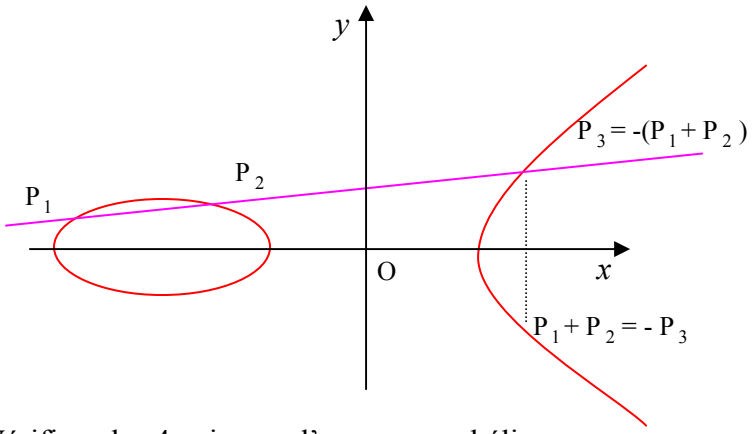



Figure -1-

Vérifions les 4 axiomes d'un groupe abélien.

Axiome de l'élément neutre $O_E$ :

P + $O_E$ est sur la parallèle à O$y$ passant par P.

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

Axiome du symétrique P' de P :

P + P' = $O_E$ implique que la sécante PP' est parallèle à O$y$ et P' = - P

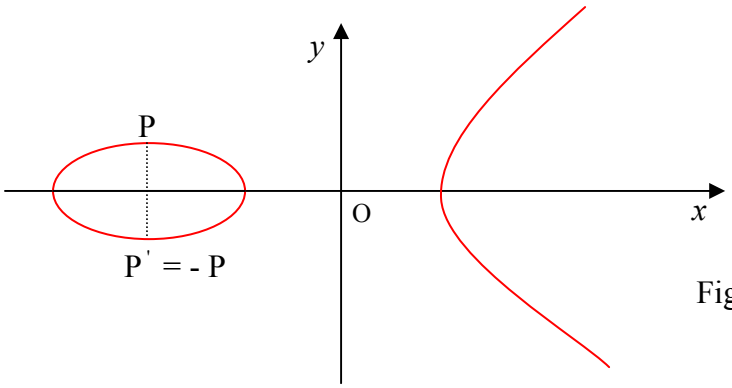



Figure - 2 -

Axiome de commutativité :

Les 2 sécantes $P_1P_2$ et $P_2P_1$ coïncident : donc $P_1 + P_2 = P_2 + P_1$.

Axiome d'associativité :

Il est vérifié par le calcul des sommes $(P_1 + P_2) + P_3$ et $P_1 + (P_2 + P_3)$ pour 3 points $P_i$ de E (K).

Ces calculs sont très longs comme le montre l'exemple d'une courbe elliptique E d'équation de Weierstrass :

$$E : y^2 = x^3 + ax + b, \qquad 4a^3 + 27b^2 \neq 0.$$

Pour calculer les sommes $F_1 + F_2$ de deux points $F_1 \neq F_2$ de la courbe elliptique, nous utilisons les formules :

$$F_1 + F_2 = G = (x_G, y_G) \quad \text{pour } F_i = (x_i, y_i)$$

Formules des coordonnées :

$$x_G = \lambda^2 - x_1 - x_2; \quad y_G = -\lambda^3 + (2x_1 + x_2)\lambda - y_1 \quad \text{pente } \lambda = \frac{(y_1 - y_2)}{(x_1 - x_2)}$$

Nous obtenons pour $P_1 + P_2 = M = (x_M, y_M)$

$$x_M = \lambda^2 - x_1 - x_2; \quad y_M = -\lambda^3 + (2x_1 + x_2)\lambda - y_1 \quad \text{pente } \lambda = \frac{(y_1 - y_2)}{(x_1 - x_2)} \qquad (1)$$

Pour la somme $M + P_3 = N = (x_N, y_N)$ nous obtenons :

$$x_N = \gamma^2 - x_M - x_3; \quad y_N = -\gamma^3 + (2x_M + x_3)\gamma - y_M \quad \text{pente } \gamma = \frac{(y_M - y_3)}{(x_M - x_3)} \qquad (2)$$

Pour la somme $P_2 + P_3 = S = (x_S, y_S)$ nous obtenons :

$$x_S = \alpha^2 - x_2 - x_3; \quad y_S = -\alpha^3 + (2x_2 + x_3)\alpha - y_2; \quad \text{pente } \alpha = \frac{(y_2 - y_3)}{(x_2 - x_3)} \qquad (3)$$

Pour la somme $P_1 + S = T = (x_T, y_T)$ nous obtenons :

$$x_T = \beta^2 - x_1 - x_S; \quad y_T = -\beta^3 + (2x_1 + x_S) - y_1; \qquad (4)$$

Un calcul fastidieux implique $M + P_3 = P_1 + S$ (5)

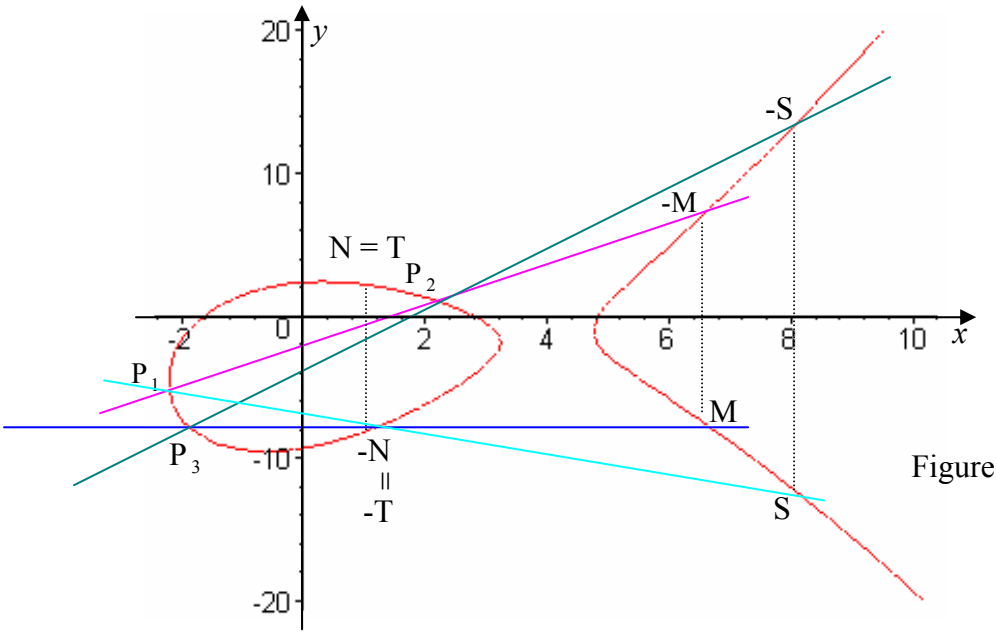



Figure -3 -

Nous avons démontré la :

***Proposition 1 :***

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

***Définition 1 :***

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

Calculons les coordonnées du symétrique – P d'un point P ∈ E (K) et les coordonnées de la somme $P_1 + P_2$ de 2 points :

Calcul du symétrique - P d'un point P = $(x_P, y_P)$.

Nous considérons la parallèle à l'axe O*y* passant par P.

Cette sécante a pour équation $x = x_P$.

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

$$y^2 + a_1 x_P y + a_3 y = x_P^3 + a_2 x_P^2 + a_4 x_P + a_6 \qquad (1 - 3)$$

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

$$y\,(\text{-P}) + y_P = -a_1 x_P - a_3$$

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

$$\text{- P} = (x_P, -(y_P + a_1 x_P + a_3)) \qquad (2)$$

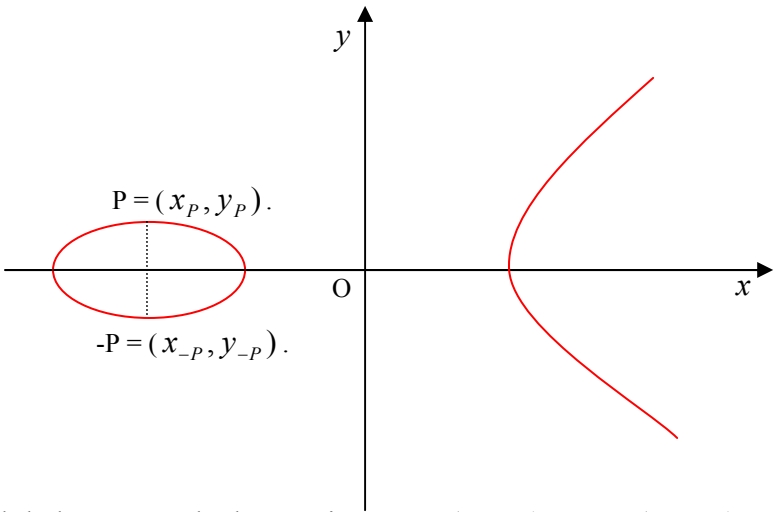



Figure - 4 -

Calcul de la somme de deux points $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ avec $P_1 \neq \pm P_2$.

La règle géométrique de trois points colinéaires implique la relation :

$$P_1 + P_2 + P_3 = O_E.$$

Cette relation implique la somme :

$$P_1 + P_2 = - P_3$$

L'équation de la sécante $P_1\ P_2$ est :

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

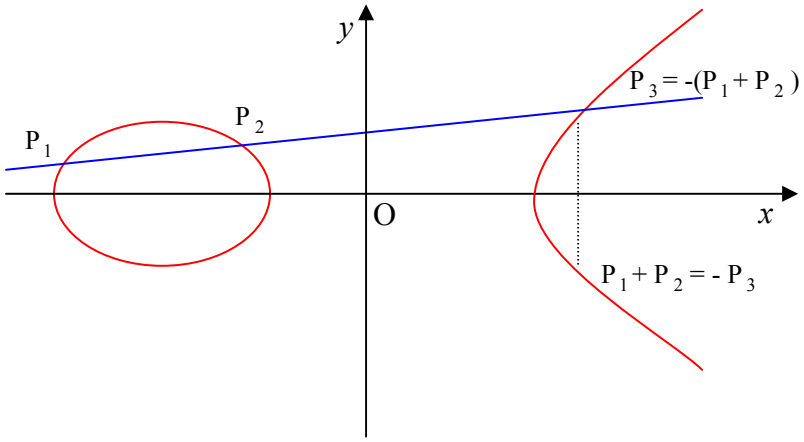



Figure - 5 -

La sécante $P_1\ P_2$ coupe la courbe elliptique E en trois points simples $P_1$, $P_2$ et $P_3$ d'abscisses $x_1, x_2$ et $x_3$.

Ces trois abscisses sont les racines de l'équation algébrique en $x$ de degré 3

$$(\lambda x + \alpha)^2 + a_1 x(\lambda x + \alpha) + a_3(\lambda x + \alpha) = x^3 + a_2 x^2 + a_4 x + a_6. \qquad (2 - 1)$$

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

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

(2 - 2) implique $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$

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

Avec les formules du symétrique du point $P_3$, nous obtenons le point $-P_3 = P_1 + P_2 = M$

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

avec la pente $\lambda = \frac{y_1 - y_2}{x_1 - x_2}$. $\qquad (2 - 3)$

**2 - Points de s-torion d'une courbe elliptique :**

Le groupe E (K) de Mordell - Weil possède des sous groupes cycliques et des sous groupes abéliens.

***Définition 2 :***

1) *Un point de s - torsion du groupe de Mordell - Weil* $E$ (K) *est un point d'ordre fini s.*
2) *L'ensemble* $T(E)$ *des points d'ordre fini de* $E$ (K) *est le groupe de torsion de la courbe elliptique E.*

$$T(E) = \{ P \in E(K); sP = O_E, s \in \mathbb{Z}\}.$$

*Ce groupe est la réunion de tous les sous groupes de s - torsion ;*

$$T(E) = \bigcup_{s \geq 0} E(K)[s].$$

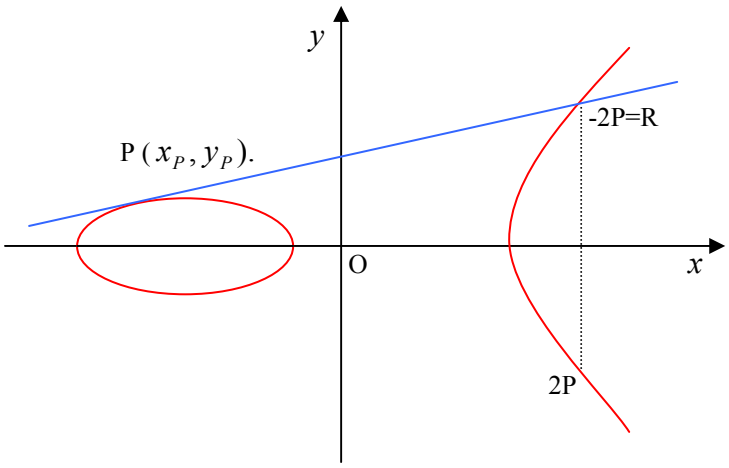
Les coordonnées d'un point 2P sont obtenues avec l'équation de la tangente à la courbe E au point P.

L'équation de la tangente à la courbe au point P est :

$y = y'(x - x_P) + y_P$ avec une pente de la tangente égale à la dérivée

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

Figure - 6 -




Cette tangente coupe la courbe E au point double P = ( $x_P$ , $y_P$ ) et au point simple R = ( $x_R$ , $y_R$ )

Ces abscisses sont les racines de l'équation algébrique en $x$ de degré 3

$$[y'_P(x - x_P) + y_P]^2 + [y'_P(x - x_P) + y_P][a_1x + a_3] = x^3 + a_2x^2 + a_4x + a_6 \qquad (3 - 1)$$

La fonction symétrique somme des racines implique :

$$2x_P + x_R = -a_2 + (y'_P)^2 + a_1y'_P \qquad (3 - 2)$$

Il en résulte l'abscisse :

$$x_R = (y'_P)^2 + a_1 y'_P - a_2 - 2x_P \qquad (3 - 3)$$

et l'ordonnée :

$$y_R = y'_P(x_R - x_P) + y_P$$

$$y_R = (y'_P)^3 + a_1(y'_P)^2 - (a_2 + 3x_P)y'_P + y_P$$

Le point 2P = - R est le symétrique du point R.

$$\begin{cases} x_{2P} = y'_P + a_1 y'_P - a_2 - 2x_P \ ; \\ y_{2P} = -(y'_P)^3 - 2a_1(y'_P)^2 + (a_2 - a_1^2 + 3x_P)y'_P + a_1 a_2 - a_3 + 2a_1 x_P - y_P \ ; \end{cases} \qquad (3 - 4)$$

où $\quad y'_P = \dfrac{3x_P^2 + 2a_2 x_P + a_4 - a_1 y_P}{2y_P + a_1 x_P + a_3}$

Les coordonnées d'un point $m$P, pour $m > 2$ peuvent être obtenues avec une récurrence sur l'entier $m > 2$.

*Cassels*, dans "*Diophantine equation with Special Reference to Elliptic Curves*" a indiqué les coordonnées des points $m$P pour une équation particulière de E :

***Proposition 2 :***

*Soit une courbe elliptique E sur le corps Q des nombres rationnels d'équation de Weierstrass :*

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

*Pour tout entier m > 2 les coordonnées des points mP sont indiquées par les formules :*

$$mP = \left( \frac{\phi_m}{\psi_m^2}, \frac{\omega_m}{\psi_m^3} \right) \qquad (4)$$

*Les polynômes* $\psi_m$ *satisfont les relations de récurrence* :

$$\begin{cases} 2y\psi_{2m} = \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \ \ pour \ m \geq 3 \ ; \\ \psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad pour \ m \geq 2. \end{cases}$$

*Les polynômes* $\phi_m$ *et* $\omega_m$ *satisfont les relations :*

$$\begin{cases} \phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}. \\ 4y\,\omega_m = \psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2. \ \ avec \ les \ valeurs \ particulières \end{cases} \qquad (4 - 1)$$

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

$$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3).$$

**Preuve :**

Pour $m = -1$, $-P = (x_P, -y_P)$ ; il en résulte $\psi_{-1} = -1$.

Pour $m = 0$, $0P = (\infty, \infty)$ ; il en résulte $\psi_0 = 0$.

Pour $m = 1$, $1P = (x, y)$ ; il en résulte $\psi_1 = 1$.

Pour $m = 2$, $2P = \left( \frac{\phi_2}{(2y)^2}, \frac{\omega_2}{(2y)^3} \right)$ ; il en résulte $\psi_2 = 2y$.

Pour $m = 3$, nous obtenons avec les calculs le polynôme :

$$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2;$$

Pour $m = 4$, $4P = 2(2P) = \left( \frac{\phi_4}{\psi_4^2}, \frac{\omega_4}{\psi_4^3} \right)$ ; nous obtenons le polynôme :

$$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) ;$$

Pour les autres polynômes nous disposons du raisonnement par récurrence.
Selon *Cassels, lemma* (7 - 2)*,* sur le corps des nombres complexes ces relations sont les formules familières qui découlent de la théorie de la fonction $P_L(z)$ de Weierstrass décrites par *Fricke* et *Weber.*

□.

***Proposition 3 :*** (Théorème de Mazur).

*Soit T*(*E*) *le sous groupe de torsion de groupe de Mordell - Weil d'une courbe elliptique E sur le corps des nombres rationnels Q ; alors T*(*E*) *est isomorphe à l'un des* 15 *groupes abéliens finis :*

1) $\mathbb{Z}/m\mathbb{Z}$ *pour* $1 \leq m \leq 10$ *et* $m = 12$.

2) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ pour $N = 2, 4, 6, 8$.

C'est une conjecture de Ogg, qui a été prouvée par Mazur dans [12].

Le sous groupe de *s*- torsion d'une courbe elliptique E est l'ensemble E (K) [*s*] des points d'ordre *s*.

**3 - Hauteurs et descente infinie :**

Selon « *Elliptic Curves. Diophantine Analysis »* (1978) par *S.Lang, « Mordell* a prouvé en 1922 une conjecture de Poincaré selon laquelle le groupe des points rationnels d'une courbe elliptique est de type fini ». Cette preuve se trouve dans [14]. En 1929 / 1930, *Weil* a étendu ce théorème aux variétés abéliennes.

Cette preuve est séparée en 2 parties : une partie pour montrer que le groupe quotient $E(K)/mE(K)$ est fini pour un certain entier *m*, valeur choisie *m* = 2 ; une partie " Descente Infinie " qui utilise des fonctions hauteurs sur les groupes abéliens.

Nous décrivons les hauteurs sur les groupes abéliens.

***Définition 3:***

*Soit un groupe abélien A ; une hauteur sur A est une fonction* $h : A \to [0,\infty[ \subset \mathbb{R}$, *à valeurs réelles positives ou nulles qui satisfait les 3 axiomes :*

(*h1*) *Pour tout point* $P_0 \in A$, *il existe une constante* $c_0$ *telle que :*

$$h(P+P_0) \le 2h(P) + c_0, \quad P \in A.$$

(*h2*) *Il existe une constante* $c_1$ *et un entier* $m \ge 2$ *tels que :*

$$h(mP) \ge m^2 h(P) - c_1.$$

(*h3*) *Il y a seulement un nombre fini de points* $P \in A$ *de hauteur bornée.*

Cette hauteur intervient dans la preuve du groupe de Mordell - Weil du type fini :

***Proposition 4 :***

*Soit un groupe abélien A muni de la hauteur h précédente.*

*Alors si le groupe quotient* $A/mA$ *est fini, le groupe A est de type fini.*

**Preuve :**

Soit un groupe quotient $A/mA$ fini pour un entier $m \ge 2$

Considérons des représentants $R_i$, $1 \le i < r$ des classes $A/mA$ (1)

Prenons un point $P_0 \in A$ sous la forme de combinaison linéaire :

$$P_0 = mP_1 + R_{i_1} \; ; \quad 1 \le i_1 \le r \tag{2}$$

Construisons une suite de points $P_2, P_3, ....., P_N$, par récurrence :

$$P_1 = mP_2 + R_{i_2} \; ; \quad 1 \le i_2 \le r \tag{3}$$

$$P_2 = mP_3 + R_{i_3} \; ; \quad 1 \le i_3 \le r \tag{4}$$

$$\vdots$$

$$P_j = mP_{j+1} + R_{i_{j+1}} \; ; \quad 1 \le i_{j+1} \le r \tag{5}$$

$$\vdots$$

$$P_N = mP_{N+1} + R_{i_{N+1}} \; ; \quad 1 \le i_{N+1} \le r \tag{6}$$

La relation (5) implique :

$$mP_{j+1} = P_j - R_{i_{j+1}} \tag{7}$$

L'axiome (*h2*) transforme le premier membre de l'égalité (7) :

$$h(mP_{j+1}) \geq m^2 h(P_{j+1}) - c_1 \tag{8}$$

et l'axiome (*h1*) transforme le deuxième membre de cette égalité :

$$h(P_j - R_{i_{j+1}}) \leq 2h(P_j) + c_0 \tag{9}$$

(7), (8) et (9) impliquent les inégalités :

$$m^2 h(P_{j+1}) - c_1 \leq h(mP_{j+1}) \leq 2h(P_j) + c_0 \tag{10}$$

En posant $c_0 + c_1 = c_2$, nous obtenons l'inégalité :

$$h(P_{j+1}) \leq \frac{2}{m^2} h(P_j) + \frac{c_2}{m^2} \tag{11}$$

Avec les relations de récurrence pour j = 1,……, N, nous obtenons l'inégalité :

$$h(P_{N+1}) \leq \frac{2^N}{m^{2N}} h(P_1) + c_2 \sum_{k=1}^{N} \frac{2}{m^{2k}} \tag{12}$$

L'hypothèse $m \geq 2$ et (12) impliquent que les points $P_j$ sont de hauteur bornée.

Par l'axiome (*h3*), il n'y a qu'un ensemble fini de tels points $P_1,.....,P_n$

Il en résulte que ces points $\{P_1,.....,P_n\}$ engendrent le groupe quotient $A/mA$.

Tout point $P \in A$ est donc une combinaison linéaire :

$$P = s_1 R_1 + ..... + s_r R_r + t_1 P_1 + ..... + t_n P_n, \quad s_i, t_j \in \mathbb{Z}$$

Le groupe abélien A est de type fini.

□.

C'est le théorème de Descente Infinie.

Cette descente infinie a été inventée par Fermat pour étudier des problèmes arithmétiques tels que celui de montrer que le nombre $\sqrt{2}$ n'est pas rationnel.

Le théorème de Descente Infinie s'applique au groupe abélien E (K) d'une courbe elliptique E.

***Proposition 5 :***

*Le groupe E (K) de Mordell - Weil d'une courbe elliptique est de type fini.*

**Preuve :** Mordell, [14]

□.

La structure de ce groupe est précisée par le :

***Corollaire :***

*Le groupe E (K) de Mordell - Weil est isomorphe au produit de 2 groupes abélien* **;**

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

*T*(*E*) = *groupe de torsion de E,* $\mathbb{Z}^r$ = *r copies du groupe abélien* $\mathbb{Z}$, *r entier* $\geq 0$.

**Preuve :** Mordell, [14] et Weil

□.

***Définition 4 :***

*L'entier r = r*(*E*) $\geq 0$ *de ce corollaire est le rang de la courbe elliptique E.*

Il y a d'autres valeurs possibles d'une hauteur qui satisfont les 3 axiomes
Cette notion est étendue à d'autres groupes et peut prendre des valeurs complexes. Il y a une hauteur de Weil, une hauteur logarithmique, une hauteur de Néron - Tate
des hauteurs locales, etc.

L'ensemble E (K) de Mordell - Weil d'une courbe elliptique a une structure de groupe abélien de type fini et d'élément neutre le point à l'infini ; alors par la théorie des groupes, il y a des homomorphismes de groupes construits sur les groupes E (K).

**4 - Homomorphismes de courbes elliptiques :**

Nous examinons les isomorphismes et les isogénies seulement.

***Définition 5 :***

*Un isomorphisme de* 2 *courbes elliptiques est un isomorphisme f : E* $(K) \to E'(K)$ *de leurs groupes de Mordell - Weil.*

Donc il satisfait les formules d'isomorphisme de groupes abéliens :

$$f(P_1 + P_2) = f(P_1) + f(P_2), \qquad f(O_E) = O_{E'};$$

$$f^{-1}(O_{E'}) = \{O_E\}, \quad f \text{ est bijective.}$$

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

***Proposition 6 :***

*Soit une courbe elliptique E et son groupe de Mordell - Weil E* (*K*),
*Alors le changement de variables :*

$$x = u^2 X + r, \quad y = u^3 Y + s u^2 X + t, \quad u \neq 0, \quad r, s, t \in K. \qquad (5)$$

*transforme l'équation de Weierstrass :*

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

*en l'équation de Weierstrass d'une courbe elliptique E' isomorphe à E ;*

$$E' : Y^2 + a_1' XY + a_3' Y = X^3 + a_2' X^2 + a_4' X + a_6 .$$

**Preuve :**

Avec le calcul, nous vérifions les formules d'isomorphismes de groupes abéliens

□.

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

***Corollaire :***

*Le changement de variables indiqué dans la proposition* 6 *implique les relations entre les invariants des 2 courbes elliptiques isomorphes* :

1) *relations entre* $a_i$ *et* $a_i'$ :

$$\begin{cases} ua_1' = a_1 + 2s \ ; \\ u^2 a_2' = a_2 - sa_1 + 3r - s^2 \ ; \\ u^3 a_3' = a_3 + ra_1 + 2t \ ; \\ u^4 a_4' = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st \ ; \\ u^6 a_6' = a_6 + ra_4 + r^2 a_2 + r^3 - ta_3 - t^2 - rta_1 \ ; \end{cases} \qquad (5 - 1)$$

2) *relations entre* $b_{2i}$ *et* $b_{2i}'$ :

$$\begin{cases} u^2 b_2' = b_2 + 12r \ ; \\ u^4 b_4' = b_4 + rb_2 + 6r^2 \ ; \\ u^6 b_6' = b_6 + 2rb_4 + r^2 b_2 + 4r^3 \ ; \\ u^8 b_8' = b_8 + 3rb_6 + 3r^2 b_4 + r^3 b_2 + 3r^4 \ ; \end{cases} \qquad (5 - 2)$$

3) *relation entre* $c_{2i}$ *et* $c_{2i}'$ :

$$\begin{cases} u^4 c_4' = c_4 \ ; \\ u^6 c_6' = c_6 \ ; \end{cases} \qquad (5 - 3)$$

4) *relation entre les discriminants* :

$$u^{12} \Delta(E') = \Delta(E). \qquad (5 - 4)$$

5) *relation entre les invariants modulaires* :

$$j(E) = j(E'). \qquad (5 - 5)$$

6) *relation entre les invariants différentiels* :

$$u^{-1}\omega(E') = \omega(E). \qquad (5 - 6)$$

Preuve avec le calcul

□.

La partie 5 du corollaire implique que l'invariant modulaire j(E) classifie les courbes elliptiques isomorphes.

***Proposition 7 :***

*Deux courbes elliptiques E et $E'$ sont isomorphes si et seulement si leurs invariants modulaires sont égaux : $j(E) = j(E')$.*

□.

**Exemple de courbes elliptiques isomorphes :**

Soit une courbe elliptique $\mathrm{E}_1$ d'équation de Weierstrass :

$$\mathrm{E}_1 : y^2 + 3xy + 17y = x^3 + 2x^2 + 20x + 3 .$$

Courbe elliptique isomorphe $\mathrm{E}_2$ avec les valeurs $u = 2,\ r = 0,\ s = 0,\ t = 0$ et les formules (5 - 1)

$$\mathrm{E}_2 : y^2 + \frac{3}{2}xy + \frac{17}{8}y = x^3 + \frac{1}{2}x^2 + \frac{5}{4}x + \frac{3}{64}.$$

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

$$b_2' = \frac{b_2}{4},\quad b_4' = \frac{b_4}{16},\quad b_6' = \frac{b_6}{64},\quad b_8' = \frac{b_8}{256},\quad \Delta(\mathrm{E}_2) = \frac{\Delta(E_1)}{4096} = \frac{\Delta(E_1)}{2^{12}}.$$

**Tableau de valeurs des coordonnées de quelques points sur la courbe $\mathbf{E}_1$ :**

| $x$ | -10 | -1 | 0 | 5 | 7 |
|---|---|---|---|---|---|
| $y$ | Pas de racines $y$ réelles | $-7 - \sqrt{33}$ et $-7 + \sqrt{33}$ | $\frac{-17 - \sqrt{301}}{2}$ et $\frac{-17 + \sqrt{301}}{2}$ | $-16 - \sqrt{2\times 3\times 89}$ et $-16 + \sqrt{2\times 3\times 89}$ | $-19 - 3\sqrt{105}$ et $-19 + 3\sqrt{105}$ |

La courbe elliptique $\mathrm{E}_1$ coupe l'axe O$x$ en un seul point d'abscisse $x_1$ :

Logiciel Maple donne l'abscisse $x_1 \approx -0{,}28$.

**Tableau de valeurs des coordonnées de quelques points sur la courbe $E_2$ :**

| $x$ | -10 | -1 | 0 | 5 | 7 |
|---|---|---|---|---|---|
| $y$ | Pas de racines $y$ réelles | Pas de racines $y$ réelles | $\frac{-17}{16}+\frac{1}{16}\sqrt{301}$ et $\frac{-17}{16}-\frac{1}{16}\sqrt{301}$ | $\frac{-77}{16}+\frac{3}{16}\sqrt{4749}$ et $\frac{-77}{16}-\frac{3}{16}\sqrt{4749}$ | $\frac{-101}{16}+\frac{3}{16}\sqrt{11837}$ et $\frac{-101}{16}-\frac{3}{16}\sqrt{11837}$ |

La courbe elliptique $E_2$ coupe l'axe O$x$ en un seul point d'abscisse $x_2$ :

Logiciel Maple donne l'abscisse $x_2 \approx -0{,}08$.

**La courbe elliptique $E_1$ :**

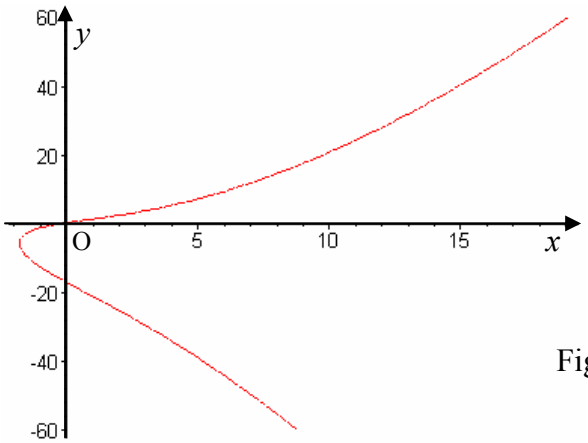



Figure - 7 -

**La courbe elliptique $E_2$ :**

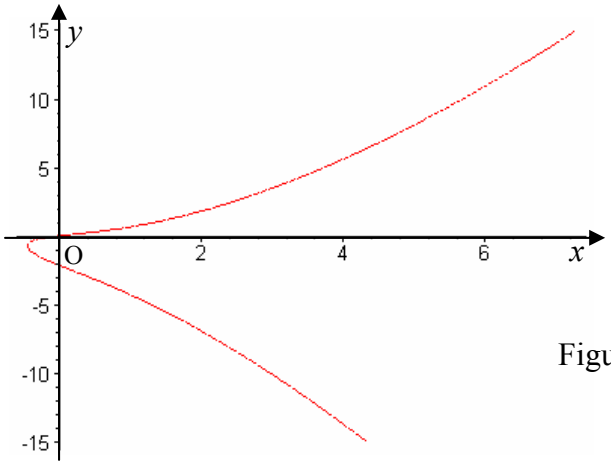



Figure - 8 -

La propriété de l'invariant modulaire j(E) définit une relation d'équivalence dans l'ensemble des courbes elliptiques.

Il en résulte que les courbes elliptiques se repartissent en classes d'équivalence de courbes elliptiques isomorphes.

cl $(E')$ = $\{E', E'_1, E'_2, \ldots\ldots, E'_n\}$, d'invariants modulaires égaux :

$$j(E') = j(E'_1) = j(E'_2) = \ldots\ldots = j(E'_n).$$

**5 - Isogénies de courbes elliptiques :**

Pour étudier les isogénies de courbes elliptiques, nous utilisons des ouvrages de Cassels [3] et de Shimura [19].

Signalons que le terme d'isogénie est utilisé pour les Variétés Abéliennes et pour les Tores Complexes.

***Définition 6:***

*Une isogénie de courbes elliptiques est un homomorphisme de leurs groupes de Mordell - Weil.*

$\psi : E_1(K) \to E_2(K)$ *qui satisfait les conditions :*

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

Cette définition est empruntée à *Shimura* [19].

Les courbes elliptiques $E_1$ et $E_2$ sont isogènes.

**Exemple :**

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

$u_m$: E (K) $\to$ E (K) ; de valeur $u_m$ (P) = *m*P.

Le symbole *m*P signifie :

*m*P = P+……+P, *m* fois P si $m > 0$.

*m*P = (-*m*) (-P), si $m < 0$.

$0P = O_E = (\infty, \infty)$, si $m = 0$.

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

***Définition 7 :***

1) *Le degré d'une isogénie* $\psi : E_1(K) \to E_2(K)$ *est l'ordre de son noyau.*

$$deg\,\psi = card\left\{\psi^{-1}(O_{E_2})\right\}.$$

2) *L'isogénie duale de l'isogénie* $\psi$ *de degré d est l'isogénie* $\hat{\psi} : E_2(K) \to E_1(K)$ *qui satisfait les relations de composition des applications :*

$\hat{\psi} o \psi :$ $E_1(K) \to E_1(K)$ *est la multiplication par d sur la courbe* $E_1$.

$\psi \; o \hat{\psi} : E_2(K) \to E_2(K)$ *est la multiplication par d sur la courbe* $E_2$.

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

***Proposition 8 :***

*Soit la multiplication* $u_m : E(\mathrm{K}) \to E(\mathrm{K})$ *par un entier rationnel m. Alors*

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

**Preuve :** [4]

□.

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

***Proposition 9:***

*Soit une courbe elliptique* $E_1$ *sur un corps K, et un sous groupe fini F du groupe de Mordell - Weil* $E_1(K)$.

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

□.

Les isogénies de courbes elliptiques sur le corps des nombres rationnels *Q*, qui sont de degré premier N sont en nombre fini d'après Mazur [12].

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

Par exemple, l'ensemble des multiplications par $m \in \mathbb{Z}$ a une structure d'anneau.

***Proposition 10 :***

*L'ensemble M(E) des multiplications par un entier rationnel sur une courbe elliptique E est un anneau isomorphe à l'anneau* $\mathbb{Z}$.

**Preuve :**

Considérons l'application $f: \mathbb{Z} \to M(E)$, de valeur $f(n)$ = multiplication par l'entier $n$ :

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

Soient 2 entiers rationnels $n,\ n' \in \mathbb{Z}$.

Calculons les valeurs $f(n+n')$, $f(0)$ et $f(nn')$ pour déterminer la structure de l'ensemble M(E).

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

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

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

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

$f(0) = 0$, $0P = O_E$ = élément neutre du groupe E(K) (4)

Les 3 relations (1), (2) et (3) impliquent que $f$ est un isomorphisme de l'anneau $\mathbb{Z}$ sur l'ensemble M(E).

Un isomorphisme conserve la structure algébrique ;

Cela implique que l'ensemble

M(E) = {multiplications par $\mathbb{Z}$ sur la courbe elliptique} est un anneau isomorphe à $\mathbb{Z}$

□.

**6 - Endomorphismes End(E) de courbes elliptiques :**

Les endomorphismes du groupe E (K) forment un anneau avec une addition déterminée par la valeur : $(f, g) \to f + g$ ; $(f+g)(P) = f(P) + g(P)$.

et une multiplication déterminée par la valeur :

$(fg)(P) = f(g(P)) \neq g(f(P))$ donc l'anneau End(E) n'est pas commutatif.

L'endomorphisme nul $\lambda_0$ est déterminé par les relations :

$$\lambda_0(P) = O_E \quad \text{et} \quad f + \lambda_0 = \lambda_0 + f = f$$

La description complète de cet anneau End(E) se trouve dans [4].

La nature de l'anneau End(E) dépend de la caractéristique du corps de base de la courbe elliptique

***Corollaire :***

*L'anneau End(E) des endomorphismes d'une courbe elliptique E sur un corps K, est isomorphe à l'anneau* $\mathbb{Z}$*, ou à un ordre d'un corps quadratique imaginaire lorsque K est de caractéristique* 0*, ou à un ordre de l'algèbre des quaternions sur le corps Q des rationnels, lorsque K est de caractéristique p > 0.*

**Preuve :** Dans [4]

□.

***Définition 8 :***

1) *Une algèbre des quaternions est une algèbre A sur le corps Q des nombres rationnels de la forme :*

$A = Q + Q\alpha + Q\beta + Q\alpha\beta, \quad \alpha, \beta$ *satisfont* $\alpha^2, \beta^2 \in Q \quad \alpha^2 < 0, \quad \beta^2 < 0 \qquad \beta\alpha = -\alpha\beta.$

2) *Un ordre d'un corps quadratique imaginaire K est l'anneau* $\mathbb{Z} + f\,A\,(K)$ *où f est le conducteur de l'ordre* $O_f$ *et A (K) est l'anneau des entiers de K.*

Cette description de l'anneau End(E) permet d'introduire la notion de Multiplication Complexe sur une courbe elliptique.

L'anneau End(E) classifie les courbes elliptiques en 2 classes : la classe des courbes elliptiques qui ont une Multiplication Complexe et la classe des courbes elliptiques qui n'ont pas de Multiplication Complexe.

***Définition 9 :***

*Une courbe elliptique E possède une Multiplication Complexe par un corps quadratique imaginaire* $K = Q\left(\sqrt{-d}\right)$*, lorsque son anneau des endomorphismes End(E) est isomorphe à un ordre de ce corps quadratique imaginaire, ou à un ordre de l'algèbre des quaternions.*

**Exemple :**

Courbe elliptique ayant une Multiplication Complexe par un ordre du corps quadratique imaginaire $Q(i)$.

Soit la courbe elliptique E, d'équation de Weierstrass :

$$E : y^2 = x^3 + 17 \in Q[x, y] \text{ de discriminant } \Delta(E) = -2^4 \times 3^3 \times 17^2 \neq 0$$

Soit un endomorphisme $f : E(Q) \to E(Q)$ de valeur $f(x, y) = (-x, iy)$,

$i$ = nombre complexe = $\sqrt{-1}$ ;

Il en résulte que l'anneau End(E) est isomorphe à un ordre du corps quadratique imaginaire K = $Q(i)$.

Il existe plusieurs méthodes pour déterminer les formules d'une isogénie et l'équation de Weierstrass de la courbe elliptique isogène.
Nous utilisons la technique de Velu [22].

**7 - Algorithme de Velu de construction d'équation de Weierstrass de courbes elliptiques isogènes :**

1) Soit une courbe elliptique E d'équation de Weierstrass :

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

2) Choix d'un sous groupe fini F du groupe E (K)

3) Prendre $F_2 = \{P \in F, d'ordre 2\}$

4) Partition de $F - F_2 - \{O_E\} = R \cup -R;$ donc $R \cap -R = \Phi$ et $-R = \{-P; P \in R\}$

5) Prendre la partie $S = F_2 \cup R$

6) Calculer les dérivées partielles $g'_x$ et $g'_y$

7) L'application $\lambda : E \to E/F = E',\quad (x,y) \to (X,Y)$ d'équations :

$$\begin{cases} X = x + \sum_{P \in S}\left[\dfrac{t_P}{x - x_P} + \dfrac{u_P}{(x - x_P)^2}\right], \\ Y = y - \sum_{P \in S}\left[u_P \dfrac{2y + a_1x + a_3}{(x - x_P)^3} + t_P \dfrac{a_1(x - x_P) + y - y_P}{(x - x_P)^2} + \dfrac{a_1u_P - g_P^x g_P^y}{(x - x_P)^2}\right] \end{cases}$$

est une isogénie de courbes elliptiques.

8) Calculer les nombres :

$g'_x(P);\quad g'_y(P);\quad t_P = g'_x(P)$ si $P \in F_2;\quad t_P = 6x_P^2 + b_2x_P + b_4$ si $P \notin F_2$

$u_P = 4x_P^3 + b_2x_P^2 + 2b_4x_P + b_6;\ b_2 = 4a_2 + a_1^2;\ b_4 = a_1a_3 + 2a_4$ et $b_6 = a_3^2 + 4a_6.$

$$t = \sum_{P \in S} t_P;\quad \omega = \sum_{P \in S}(u_P + x_Pt_P).$$

9) L'équation de Weierstrass de la courbe isogène $E' = E/F$ est

$$E' = E/F : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + (a_4 - 5t)X + a_6 - b_2t - 7\omega$$

**Application de l'algorithme à la courbe elliptique $E_1$ d'équation de Weierstrass :**

$$E_1 : y^2 = x^3 + 5 \tag{1}$$

Le calcul implique les invariants $\Delta(E_1) = -10800 = -2^4 \times 3^3 \times 5^2$ et $j(E_1) = 0$ (2)

Le groupe $E_1(K)$ a un sous groupe F d'ordre 3, formé des points :

$$F = \{P = (0,\sqrt{5}), 2P = (0,-\sqrt{5}), 3P = O_E = (\infty,\infty)\} \tag{3}$$

En utilisant la méthode de Velu, nous obtenons les ensembles :

$$F_2 = \Phi, \quad R = \{P\} = S \tag{4}$$

Avec le calcul nous obtenons les coordonnées du point (X, Y) :

$$(x,y) \rightarrow \left( X = x + \frac{20}{x^2}, Y = y - \frac{40y}{x^3} \right) \tag{5}$$

Par le calcul nous obtenons les nombres de l'étape (8)

$$t = 0, \quad \omega = 20 \tag{6}$$

Nous en déduisons l'équation de Weierstrass de la courbe elliptique isogène $E_2$ :

$$E_2 = E_1/F : Y^2 = X^3 - 135. \tag{7}$$

Le calcul implique les invariants :

$$\Delta(E_2) = -7873200 = -2^4 \times 3^9 \times 5^2 \text{ et } j(E_2) = 0 \tag{8}$$

La proposition 7 et la relation $j(E_1) = j(E_2) = 0$ impliquent que les courbes isogènes $E_1$ et $E_2$ sont isomorphes.

**Application de l'algorithme à l'exemple traité par Velu :**

Soit la courbe elliptique d'équation de Weierstrass :

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

Le calcul implique les invariants :

$$\Delta(E) = -1664 = -2^7 \times 13 \text{ et } j(E) = \frac{(3 \times 43)^3}{-2^7 \times 13} \tag{2}$$

Le groupe E ($Q$) a un sous groupe cyclique F d'ordre 7 formé des points :

P = (1,0), 2P = (-1,-2), 3P = (3,-6), 4P = (3,2), 5P = (-1,2), 6P = (1,-2) et $7P = O_E$

La relation $7P = O_E$ implique P = - 6P, 2P = - 5P, 3P = - 4P

Il en résulte les 3 parties :

$$F_2 = \Phi, \qquad R = \{P, 2P, 3P\} \quad \text{et} \quad S = \{P, 2P, 3P\} \tag{3}$$

Avec le calcul nous obtenons les nombres $t = 42, \quad \omega = 198$ (4)

Il en résulte l'équation de Weierstrass de la courbe elliptique isogène :

$$E' = E/F : \; Y^2 + XY + Y = X^3 - X^2 - 213X - 1257. \tag{5}$$

Le calcul implique les invariants de la courbe isogène E' :

$$\Delta(E') = -125497034 = -2 \times 62748517 \text{ et } j(E') = \frac{(3 \times 3403)^3}{-2 \times 62748517} \tag{6}$$

**Application de l'algorithme à la courbe elliptique E d'équation de Weierstrass :**

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

Le calcul implique les invariants $\Delta(E) = -11$ et $j(E) = \frac{-2^{12}}{11}$ (2)

Le groupe E ($Q$) a un sous groupe cyclique F d'ordre 5 formé des points :

$$P = (0,0), \; 2P = (1,-1), \; 3P = (1,0), \; 4P = (0,-1), \; 5P = (\infty, \infty).$$

La relation $5P = (\infty, \infty)$ implique $P = -4P$, $2P = -3P$.

Il en résulte les 3 parties du groupe E ($Q$) :

$$F_2 = \Phi, \quad R = \{P, 2P\} \quad \text{et} \quad S = \{P, 2P\} \tag{3}$$

Avec le calcul nous obtenons les nombres $t = 2, \quad \omega = 4$ (4)

et la courbe elliptique isogène E' d'équation de Weierstrass :

$$E' = E/F : \; y^2 + y = x^3 - x^2 - 10x - 20 \tag{5}$$

Le calcul implique les invariants :

$$\Delta(E') = -11^5 \text{ et } j(E') = \frac{-2^{12} \times 31^3}{11^5} \tag{6}$$

Citons des équations classiques d'isogénies que l'on trouve dans [20] ;

Soient deux courbes elliptiques sur un corps K de caractéristique $\neq 2$ ;

$$E_1 : y^2 = x^3 + ax^2 + bx \tag{1}$$

$$E_2 : Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X, \quad b \neq 0 \quad \text{et } a^2 - 4b \neq 0 \tag{2}$$

Alors les 2 applications $f$, $g$

$$f : E_1 \to E_2 \quad (x, y) \to \left( \frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right) \tag{3}$$

et

$$g : E_2 \to E_1 \quad (X,Y) \to \left( \frac{Y^2}{4X^2}, \frac{Y(a^2 - 4b - X^2)}{8X^2} \right) \tag{4}$$

sont des isogénies.

Les changements de variables sont des fonctions rationnelles. Les 2 applications ont des composées qui satisfont :

La composée $f \circ g : E_2 \to E_2$ est la multiplication par 2 sur $E_2(Q)$

c'est une isogénie de degré 4 (5)

La composée $g \circ f : E_1 \to E_1$ est la multiplication par 2 sur $E_1(Q)$

c'est une isogénie de degré 4 (6)

Les relations (5) et (6) impliquent que *g* est l'isogénie duale de l'isogénie *f*.

Le calcul implique les invariants de la courbe elliptique $E_1$ :

$$\Delta(E_1) = 16b^2(a^2 - 4b), \quad c_4(E_1) = 16(a^2 - 3b) \quad \text{et } j(E_1) = \frac{16^2(a^2 - 3b)^3}{b^2(a^2 - 4b)} \tag{7}$$

Les invariants de la courbe elliptique $E_2$ sont égaux à :

$$\Delta(E_2) = 64 \times 4b(a^2 - 4b)^2, \quad c_4(E_2) = 16a^2 + 192b \quad \text{et } j(E_2) = \frac{(16a^2 + 192b)^3}{64 \times 4b(a^2 - 4b)^2} \tag{8}$$

**Application pour *a* = 5, *b* = - 8**

$E_1 : y^2 = x^3 + 5x^2 - 8x$ (1)

$E_2 : Y^2 = X^3 - 10X^2 + 57X$ (2)

Les isogénies de degré 2 sont les 2 morphismes :

$$f : E_1 \to E_2 \quad (x,y) \to \left( \frac{y^2}{x^2}, \frac{y(-8 - x^2)}{x^2} \right) \tag{3}$$

$$g : E_2 \to E_1 \quad (X,Y) \to \left( \frac{Y^2}{4X^2}, \frac{Y(57 - X^2)}{8X^2} \right) \tag{4}$$

Le calcul implique les invariants de la courbe elliptique $E_1$ :

$$\Delta(E_1) = 2^{10} \times 57, \quad c_4(E_1) = 2^4 \times 7^2 \quad \text{et } j(E_1) = \frac{2^2 \times 7^6}{57} \tag{5}$$

Les invariants de la courbe elliptique $E_2$ sont égaux à :

$$\Delta(E_2) = 2^{11} \times 3^2 \times 361, \quad c_4(E_2) = -2^4 \times 71 \text{ et } j(E_2) = \frac{-2 \times (71)^3}{3^2 \times 361} \tag{6}$$

En conclusion, je me propose de chercher d'autres formules d'isogénies dans des travaux de recherches ultérieures. Pour cela je considérerai la structure analytique complexe d'une courbe elliptique associée à un tore complexe ℂ/L. Une autre voie consiste à prendre la structure de variété abélienne de dimension un.

# Bibliographie


**[1] E.Artin:** *Algebraic Numbers and Algebraic Functions.*Gottingen,Germany (1959).

**[2] A.O.L.Atkin et J.Lehner:** *Hecke Operators on* $\Gamma_0(m)$ . Math. Ann, **185**,134 – 160(1970).

**[3] J.W.S.Cassels:** *Diophantine Equation with Special Reference to Elliptic Curves.* J.London.Math. Soc **41**,193 – 291(1966).

**[4] M.Deuring:** *Die Typer der Muultiplikatorenringe Ellipticscher Funktionen Korper.* Abb.Math.Hambourg **14**, 197 – 272,(1941).

**[5] R.Hartshorne :** *Algebraic Geometry.* Springer Verlag(1977).

**[6] Hasse:** *Number Theory.* Springer – Verlag Berlin Heidelberg.New – York (1980).

**[7] Kostrikine:** *Introduction à l'algèbre*. Editions MIR – MOSCOU (1986).

**[8] D.Kubert :***Universal bounds on the Torsion of Elliptic Curves.* Proc.London Math.Soc.(3) **33**, 193 – 237(1976).

**[9] S.Lang :** *Elliptic Curves*:*Diophantine Analysis.* Springer -Verlag (1978).

**[10] G.Ligozat :** *Courbes Modulaires de genre* 1. mémoire **43**, Bull.Soc.Math.France. 1 – 80 (1975).

**[11] B.Mazur :** *Modular Curves and the Eisenstein ideal.* Publ.Math.I.H.E.S.**47** (1977).

**[12] B.Mazur:** *Rational Isogenies of prime degree.* Inventiones Math.**44**, 129 – 162(1978).

**[13] B.Mazur:** *Rational Points on Modular Curves.* Lectures Notes in Math, **601**, Berlin – Heidelberg – New York:Springer1977.

**[14] L.J.Mordell :** *Diophantine Equations.* Academic Press (1969).

**[15] A.P.OGG,J.Reine Angew.***Abelian Curves of small Conducator.* Math,**226**, 204 – 215 (1967).

**[16] J.P.Serre et B.Mazur:***Points Rationnels des Courbes Modulaires* $X_0(N)$ . Springer(1976).

**[17] J.P.Serre :** *Propriétés Galoisiennes des Points d'ordre fini des Courbes Elliptiques.* Inventiones Math.**15**, 259 – 331(1972).

**[18] I.R.Shafarevich :***Basic Algebraic Geometry.* Springer – Verlag (1977).

**[19] G.Shimura:** *Introduction to theArithmetic Theory of Automorphic Functions.* Publ.Math.Soc.Japan **11**, (1971).

**[20] J.H.Silverman :** *The Arithmetic of Elliptic Curves***.** Graduate Texts in Math.**106** Springer -Verlag (1986).

**[21] J.Velu :** *Courbes Elliptiques sur Q ayant bonne réduction en dehors de* $\{11\}$. CR Acad. Sci.Paris Sér **273**, 73 - 75(1971).

**[22] J.Velu :** *Isogénies entre Courbes Elliptiques.* CR Acad.Sci.Paris Sér **273**, 238 – 241(1971).

**[23] A.Weil :** *Courbes Algébriques et Variétés Abeliennes***.88**, Hermann (1972).

**[24] A.Weil :** *Sur un théorème de Mordell ;* Bulletin Scientifique Mathématique **54**, 182 – 191(1930).

**[25] E.Weiss:** *Algebraic Numbers Theory.* Mc Graw Hill Book Company,Inc, New – York (1968).