RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR

ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ MENTOURI-CONSTANTINE

FACULTÉ DES SCIENCES

DÉPARTEMENT DE MATHÉMATIQUE

N°D'ordre :……..

Série :……..

# MEMOIRE

Présenté pour obtenir le Diplôme de Magister

En : Mathématiques

THEME

# Courbes Elliptiques de Rang 1

Option :

Systèmes dynamiques et Topologie algébrique

Présenté par :

Mr. Amina Daoui

## Devant le jury :

Président : Rahmani Fouad Lazhar M.C :UMC

Rapporteur : Zitouni Mohamed Pr.. :USTHB

Examinateur : Benkafadar N.M Pr.. :UMC

Examinateur :Boughaba S M.C : UMC

Soutenue Le :22/04/2010

## *SOMMAIRE*

## INTRODUCTION :

Ma thèse concerne plusieurs domaines des Mathématiques : Géométrie Algébrique, Courbes algébriques planes , la Théorie algébriques des Nombres ,Cubiques de Weierstrass , Courbes Elliptiques .

Dans le chapitre I, je décris les structures et quelques propriètés des Variétés algébriques ,Variétés Affines , Variétés projectives , Variétés Abéliennes .

Ainsi , les Courbes Elliptiques sont à la fois des cubiques de Weierstrass non singulières et des Variétés abéliennes de dimension 1 .

Dans le chapitre II, j'étudie les courbes algébriques planes :j'étudie leurs points singuliers, genre. Je m'intéresse particulièrement aux cubiques de Weierstrass :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Je détermine quelques invariants de ces cubiques discriminants $\triangle(E)$ , invariants modulaires $j(E)$ .Les cubiques ayant $\triangle(E) = 0$ son singulières ; celles qui ont $\triangle(E) \neq 0$ ne son pas singulières ; ce sont des Courbes Elliptiques .

Dans le chapitre III, je me consacre aux Courbes Elliptiques : groupe additif abélien de Mordell-Weil E(K) et quelques aspects de la théorie : Je calcule les coordonnées des points $-P$, $P_1+P_2$ ,$2P$ ,sous groupes de m-torsion de E(K) ,réductions , isomorphismes , isogénies .

Dans le chapitre IV, je commence par la descente sur un corps , je décris les fonctions hauteurs sur des groupes abéliens , je les applique aux groupe de Mordell-Weil pour montrer que ces groupes sont additifs et de type fini . Ce type fini implique la notion de rang r(E) des Courbes Elliptiques . J'ai choisi quelques exemples de calculs de rang dans les références .

# CHAPITRE I :VARIÉTÉS ABÉLIENNES

Nous allons décrire les Variétés Algébriques qui sont du domaine de la Géométrie Algébrique , nous traiterons les Variétés Affines, les Variétés Projectives et les Variétés Abéliennes.

## 1.Variétés Affines :

Les Variétés Affines sont construites sur des espaces Affines avec la topologie de Zariski.

**Définition 1.** ***Un n- espace Affine sur un corps commutatif K est l'ensemble des n-uples d'éléments*** $a_i$ ***de K :***

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

Un élément $a \in \mathbb{A}^n(K)$ est un point $a = (a_1, .....a_n)$ de l'espace Affine , les $a_i$ sont les coordonnées de ce point .

A cet espace Affine on associe l'anneau $K[x_1, ....x_n] = B$ des polynômes à n variables par l'application :

$$f : a \to f(a_1, .....a_n) \ , f \in B$$

A toute famille $T = \{f_1, f_2, .....f_t\}$ de polynômes de l'anneau B, on associe l'ensemble $Z(f_1, f_2, .....f_t)$ des zéros de ces polynômes ;

$$Z(T) = \{a \in \mathbb{A}^n(K),\ f(a_1) = \cdots\cdots f(a_t) = 0\}$$

**Définition 2.** ***Un sous ensemble*** $X$ ***de l'espace Affine*** $\mathbb{A}^n(K)$ ***est algébrique si ses points sont des zéros d'une famille de polynômes*** $f_i$ ***a n variables :***

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

Cela implique qu'un sous ensemble X de l'espace Affine$A^n(K)$ est algébrique s'il existe un sous ensemble $T \subseteq B$ tel que $X = Z(T)$ .

**Proposition.** ***1.La réunion de deux ensembles algébriques est un ensemble algébrique.***

***L'intersection de deux ensembles algébriques est un ensemble algébrique.***

***L'ensemble vide et l'espace Affine sont des ensembles algébriques.***

*Démonstration* . Soit deux ensembles algébriques $X_1 = Z(f_i)$et $X_2 = Z(g_i)$ dans l'espace Affine$\mathbb{A}^n(K)$ ,alors leur réunion $X_1 \cup X_2 = Z(f_i, g_i)$ est l'ensemble des zéros des polynômes $f$ *et* $g$ ,cet ensemble est donc algébrique .

L'intersection de deux ensembles algébriques est l'ensemble des zéros communs des polynômes

L'ensemble vide est l'ensemble des zéros d'un polynôme constant : $\phi = Z(1)$

## CHAPITRE I :VARIÉTÉS ABÉLIENNES

L'espace Affine $\mathbb{A}^n(K)$ , est l'ensemble des zéros des polynômes identiquement nuls : $X = Z(0)$ □

Introduisons une topologie particulière sur les variétés

**Définition 3.** ***La topologie de Zariski sur l'espace Affine*** $\mathbb{A}^n(K)$ ***, est définie avec les ensembles algébriques comme des sous ensembles fermés , et leurs complémentaires comme des ouverts.***

C'est une topologie qui n'est pas de Haussdorf .

Cette topologie satisfait les 3 axiomes :

(1) L'intersection de deux ouverts est un ouvert.
(2) La réunion d'une famille fini d'ouverts est un ouvert .
(3) L'ensemble vide et l'espace Affine sont les seuls ensembles ouverts et fermés à la fois.

**Définition 4.** ***Un sous ensemble Y d'un espace topologique X est irréductible s'il n'est pas la réunion de deux sous ensembles fermés non vides disjoints.***

L'ensemble vide n'est pas considéré irréductible.[4]

**Définition 5.** ***Une Variété Affine est un sous ensemble irréductible fermé de l'espace Affine*** $\mathbb{A}^n(K)$ ***, pour la topologie de Zariski.***

Un sous ensemble ouvert d'une Variété Affine est une Variété quasi –Affine.

La réunion de deux Variétés Affines n'est pas une Variété Affine.

**Exemple.** Soit $f$ est un polynôme irréductible de degré n dans $K[x_1, ....x_t]$ on obtient une surface $Y = Z(T)$ si n= 3 et une hyper surface si n>3.

L'espace Affine $\mathbb{A}^n(K)$, étant fermé et irréductible est une Variété Affine .

**Définition 6.** ***Soit*** $Y \subseteq \mathbb{A}^n(K)$***, l'idéal de Y est l'ensemble :***

$$I(Y) = \{f \in K[x_1, ....x_n],\ f(a) = 0 \ pour\ tout\ a \in Y\}$$

**Proposition.** ***2.Soit un ensemble algébrique Y , Y est une Variété Affine si et seulement si son idéal I(Y) est premier***

Démonstration. Consulter « Algebraic Geometry » de Hartshorne .[4]

□

**2. Variétés Projectives :**

Soit K un corps algébriquement clos, construisons un autre type de Variétés :

**Définition 7.** ***Un n espace Projectif sur un corps K, est l'ensemble des classes d'équivalences de*** $(n+1)$ ***uples*** $(a_1, \ldots, a_{n+1})$ ***d'élément de K, non tous nuls par la relation d'équivalence*** $R$ ***:***

***si*** $a = (a_1, \ldots, a_{n+1})$ ***et*** $b = (b_1, \ldots, b_{n+1})$ ***alors :*** $a\,R\,b$ ***si et seulement si :***

$a = (a_1, \ldots, a_{n+1}) = \lambda b = (\lambda b_1, \ldots, \lambda b_{n+1})$ ***pour tout*** $\lambda \in K$ , $\lambda \neq 0\,, 1$ .

**Définition 8.** ***L'espace quotient de*** $\mathbb{A}^{n+1}(k) - \{(0, ...0)\}/R$ ***est l'espace Projectif*** $\mathbb{P}^n(k)$

$$\mathbb{P}^n(k) = \left\{\mathbb{A}^{n+1}(k) - \{(0, ...0)\}\right\} / \ R$$

***Un élément de*** $\mathbb{P}^n(k)$ ***est un point de l'espace Projectif .***

**Définition 9.** ***Un anneau gradué est une somme directe*** $A = \oplus A_d$ ***de sous anneaux qui satisfont la condition :***

$$A_d, A_1 \subset A_{d+1}$$

**Définition 10.** ***l'anneau*** $A = K[x_1, ...x_n]$ ***des polynômes homogènes à n indéterminées admet une décomposition de la forme*** $A = \oplus A_d, d \geq 0$ ***donc A est un anneau gradué .***

Considérons des polynômes homogènes $f_n$ de l'anneau $A$ et l'ensemble $Z(T)$ des zéros d'une famille T de polynômes $f_1 \ldots f_t$.

**Définition 11.** ***Un sous ensemble Y de*** $\mathbb{P}^n(k)$ ***est un ensemble algébrique s'il existe un ensemble T de polynômes homogènes de l'anneau*** $A = K[x_1, ...x_n]$ ***tel que le sous ensemble Y soit égal à l'ensemble des zéros des polynômes de la famille T .***

$$Y = Z(T) = \{a, f(a) = 0, pour\ tout\ f \in T\}$$

**Proposition.** ***3. Dans l'espace Projectif*** $\mathbb{P}^n(k)$ ***la topologie de Zariski associée a un espace affine*** $\mathbb{A}^{n+1}(K)$ ***est applicable à l'espace Projectif*** $\mathbb{P}^n(k)$ .

Démonstration. Avec les arguments de la définition.

□

## CHAPITRE I :VARIÉTÉS ABÉLIENNES

**Définition 12.** ***Une Variété Projective est un sous ensemble algébrique irréductible de l'espace Projectif*** $\mathbb{P}^n(k)$ ***muni de la topologie de ZARISKI.***

Une Variété quasi Projective est un sous ensemble ouvert d'une Variété Projective.

**Définition 13.** ***La dimension d'une Variété Projective ou quasi – Projective est la dimension de l'espace topologique associé.***

**Fonctions associé à une Variété algébrique :**

A tout anneau $A = K[x_1, ...x_n]$ de polynômes correspond le corps $K(x_1, x_2, ...x_n)$ des fonctions rationnelles $f = p_1/p_2$de deux polynômes de l'anneau A , $p_2 \neq 0$ .

Une courbe plane d'équation implicite $f(x, y) = 0$ est rationnelle s'il existe deux fonctions rationnelles $t \to \varphi(t), t \to \psi(t)$, non constantes , qui satisfont l'équation :

$$f(\varphi(t), \psi(t)) = 0.$$

**Définition 14.** ***Une fonction*** $f : V \to K$ ***d'une Variété quasi- Projective V est régulière en un point a de*** $V$ ***s'il existe un voisinage ouvert U de ce point a ,et deux polynômes*** $g et\ h \in K[x_1, ...x_n]$, **tel que** $h \neq 0$ **et** $f = \frac{g}{h}$ **sur l'ouvert U.**

Une fonction $f : V \to K$ est régulière sur V si elle est régulière en chacun des points de V.

**Définition 15.** ***L'anneau local d'un point a d'une Variété V est l'ensemble des fonctions régulières*** $f : V \to K$ ***qui satisfont :***

***Soit 2 sous ensembles ouvert*** $U_1 et\ U_2$ ***de V, contenant le point a ,deux fonctions régulières***

$$f : U_1 \to K \quad et \quad g : U_2 \to K$$

***Alors*** $f$ ***et*** $g$ ***sont équivalentes si*** $f = g$ ***sur l'intersection*** $U_1 \cap U_2$.

**3.Diviseurs d'une Variété :**

La théorie des diviseurs est un outil efficace pour l'étude des Variétés Algébriques et des courbes algébriques.

**Définition 16.Soit une Variété irréductible X et une collection de sous Variétés** $c_i\ de\ X$ **de codimention un ;un diviseur de X est une combinaison linéaire :**

$$D = l_1c_1 + l_2c_2 + ... + l_nc_n$$

**où les coefficients** $l_i$ **sont des entiers rationnels.**

puisque les opération sur les Variétés sont la réunion, l'intersection, alors le produit, des diviseurs n'est pas une Variété.

## CHAPITRE I :VARIÉTÉS ABÉLIENNES

**Proposition.** ***4. L'ensemble*** $Div(X)$ ***des diviseurs d'une Variété irréductible X est un groupe abélien.***

DÉMONSTRATION. La somme de deux diviseurs D et D' est égale au diviseur

$$D'' = D + D' :$$

$D = n_1 l_1 + n_2 l_2 + ... + n_d l_d$ e t $D' = n'_1 l_1 + n'_2 l_2 + ... + n'_d l_d$.

$D + D' = (n_1 + n'_{1)} l_1 + (n_2 + n'_2) l_2 + ... + (n_d + n'_d) l_d$

Le symétrique du diviseur D est le diviseur :

$$-D = -n_1 l_1 - n_2 l_2 - ... - n_d l_d$$

Le diviseur nul $0 = 0p_1 + 0p_2 + ... + 0p_d$est l'élément neutre de l'addition des diviseurs.

La commutativité de l'addition dans l'anneau des entiers $\mathbb{Z}$impliques que l'ensemble Div(X) des diviseurs d'une Variété irréductible X est abélien.

Il en résulte que l'ensemble $Div(X)$ des diviseurs d'une Variété irréductible X est

un groupe abélien.

□

### 4. Variétés abéliennes :

Elles sont construites avec des Variété de groupe :

**Définition 17.Une Variété de groupe est une Variété X muni d'un morphisme**

**U : $X_2 \to X$ qui satisfait les deux conditions :**

**1- l'ensemble des points de X est un groupe pour l'opérateur U .**

**2- l'application inverse**$U^{-1}$ **:** $X \to X_2$ **est un morphisme de cette Variété.**

**Définition 8.*Une Variété abélienne est une Variété de groupe Projective et irréductible. Il y a des Variétés abéliennes qui sont construites avec le théorème de Chevalley.***

**Theorem.** ***5. (CHEVALLEY)Tout groupe algébrique G contient un sous groupe normal N tel que le groupe quotient*** $G/N$ ***soit une Variété abélienne.***

Selon SHAFAREVICH, les seuls exemples connus de Variétés abéliennes sont les Courbes Elliptiques .

## CHAPITRE I :VARIÉTÉS ABÉLIENNES

**Définition 19.** ***La jacobienne d'une Variété abélienne X est l'ensemble de points fermés de X.***

**Theorem.** ***8. Soit un corps commutatif K de carac(K)*** $\neq 2, 3$ ***alors une Variété abélienne est birationnellement équivalente à une Courbe Elliptique sur K d'équation :***

$$Y^2 = X^3 + AX + B.$$

Démonstration. Cf [4] .

□

Examinons un type particulier de Variétés abéliennes

**Définition 20.** ***Une Variété abélienne simple est une Variété abélienne qui a 2 sous Variétés seulement elle même et la Variété*** $\{0\}$ ***réduite au point 0.***

# CHAPITRE II :COURBES ALGÉBRIQUES PLANES

Toute courbe algébrique plane est définie par une équation algébrique $f(x, y) = 0$ ; $f$ est un polynôme de l'anneau $K[x, y]$ des polynômes sur un corps commutatif K global , local ou fini .

## 1.Singularités d'une courbe plane algébrique :

Un point d'une courbe C est soit ordinaire soit singulier. La nature d'un point est précisée par la :

**Définition 1.** ***Soit une courbe algébrique C et un point*** $P = (x, y)$ ***de C, alors :***

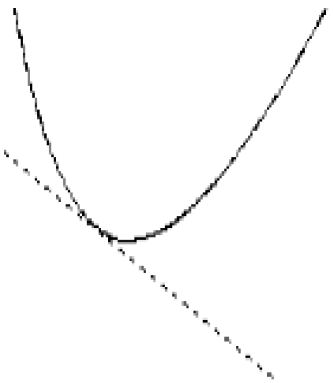
(1) ***P est ordinaire si C admet en ce point une tangente unique, et cette tangente ne traverse pas la courbe C au voisinage de P ;***

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

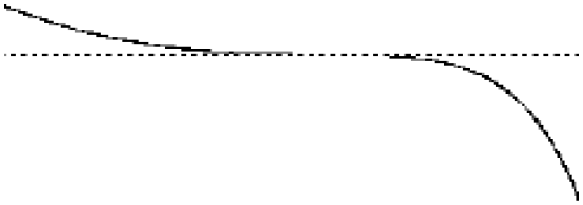
(3) ***P est un point singulier, nœud , si C admet en ce point 2 tangentes distinctes.***

(4) ***P est un point singulier, point de rebroussement, si C admet en ce point 2 tangentes confondues.***

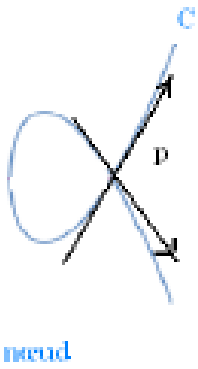
**Exemples :** ***1)Point ordinaire :***



***2)Point d'inflexion :***

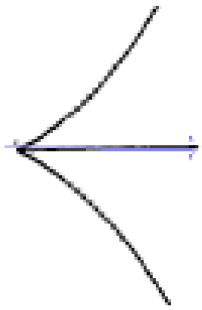


*3)Nœud :*




nœud

*4)Point de rebroussement :*



point de rebroussement

**Définition 2.**

***1.Une courbe algébrique plane C, d'équation*** $f(x,y)=0$ ***.admet un point singulier S si elle satisfait :***

$f(S)=0$ , $f'_x(S)=0$ ; $f'_y(S)=0$ ,... ;$\frac{\partial f^n(S)}{\partial x^n}\neq 0$ ***est la*** $1^{ère}$ ***dérivée partielle de f qui ne s'annule pas en S ;***$n\geq 2$.

***2.Le point singulier S est un point double pour*** $n=2$ ***, un point triple pour*** $n=3$ ***,etc .***

**Exemple** 1.Courbe algébrique C d'équation :

$$C:\ f(x,y)=y^3+3x^2-2xy\in\mathbb{R}[x,y]$$

Dérivées partielles de $f$ :

$$\text{d'ordre 1 : } f'_x = 6x - 2y \ , \ f'_y = 3y^2 - 2x \, ;$$

$$\text{d'ordre 2 : } f"_{x^2} = 6 \ , \ f"_{xy} = -2 \ , \ f"_{y^2} = 6y \, ;$$

Calculs : $f'_x(S) = f'_y(S) = 0$ implique $S = (0, 0)$

$f"_{x^2} = 6$ ,

Donc le point S est un point singulier double .

Le nombre de points singuliers d'une courbe algébrique plane permet d'introduire un invariant : le genre de C .

**Définition 3.*Le genre d'une courbe algébrique plane C est l'entier positif ou nul :***

$$g(C) = \frac{(n-1)(n-2)}{2} - s \geq 0 \qquad n \geq 1$$

***n = degré de la courbe , s = nombre de points singuliers .***

**Exemple** 1.précédent $C$ : $y^3 + 3x^2 - 2xy = 0$ ;

$n = 3$ , $s = 1$ et $g(C) = \frac{(3-1)(3-2)}{2} - 1 = 0$

Exemples de petites valeurs de $g$ :

(1) $g\,(C) = 0$ pour les droites, les cercles , les cubiques singulières ;les coniques (paraboles et hyperboles)
(2) $g\,(C) = 1$ pour les Courbes Elliptiques ;
(3) $g\,(C) = 2$ pour les quadratiques $(n = 4)$ avec $s = 2$
(4) $g\,(C) = 2$ pour les quintiques $(n = 5)$ avec $s = 4$

**2.Cubiques de Weierstrass** :

Les cubiques sont des courbes algébriques planes de degré 3 ;leur équation algébrique est de la forme :

$$C : (d_0x^3 + d_1x^2y + d_2xy^2 + d_3y^3) + (d_4x^2 + d_5xy + d_6y^2) + (d_7x + d_8y) + d_9 = 0$$

Nous avons groupés les polynômes homogènes degré 3,2,1,0 .

Dans l'ensemble de ces cubiques à 10 coefficients $d_0$,... , $d_9$ il y a des cubiques particulières avec 5 coefficients .

## CHAPITRE II :COURBES ALGÉBRIQUES PLANES

**Définition 4.**

(1) ***Une Cubique de Weierstrass est une Cubique plane d'équation particulière***

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

***K= corps commutatif global , local ou fini .***

(2) ***l'équation*** (1) ***est une équation de Weierstrass .***

Les particularités de l'équation de Weierstrass sont :

(1) Elle est unitaire en $y^2$ et $x^3$

(2) Pas de monômes en $y^3$

(3) 2 coefficients impaires $a_1$ et $a_3$ pour les monômes $xy$ et $y$

(4) 3 coefficients paires $a_2$ et $a_4$ et $a_6$ pour les monômes $x^2$ et $x$ et $x^0$

(5) pas de coefficient $a_5$ .x

Une cubique de Weierstrass a un genre $g(C) = 0$ ou 1; cet invariant implique la classification en deux classes :

1-Classe des cubiques de Weierstrass singulières :$g(C) = 0$ ;

2-Classe des Courbes Elliptiques cubiques non singulières : $g(C) = 1$ .

**Définition 5.** ***Une Courbe Elliptique est une cubique de Weierstrass, non singulière d'équation :***

$$C: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ldots (1)$$

Selon HARTSHORNE , SHIMURA , SILVERMAN ,...une Courbe Elliptique admet plusieurs structures algébriques :

1) Structure d'une Variété abélienne de dimension 1,

2) Structure de courbe Projective irréductible de genre 1,

3) Structure de schéma séparé, non singulier ,de dimension 1,

4) Structure de groupe additif abélien de type fini.

Les cubiques de Weierstrass possèdent des invariants

**3.Invariants des cubiques de Weierstrass :**

Il y en a plusieurs : les coefficients $b_{2i}$ ,et $c_{2i}$ , le discriminant $\triangle(E)$, l'invariant modulaire $j(E)$ , le régulateur $R(E)$ ,le conducteur $N(E)$, la série $L(E,s)$ de Dirichlet-Hasse ,le rang $r(E)$ ,etc ...

## CHAPITRE II :COURBES ALGÉBRIQUES PLANES

Les invariants sont liés à des changements de variables dans l'équation de Weierstrass

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

On élimine les monômes en $xy$ et en $y$ avec le changement de variables

$$x=X\quad et\quad y=\frac{1}{2}(Y-a_1X-a_3)\ ,\ cara\left(K\right)\neq 2,\ 3 \qquad (2)$$

(1) et (3) impliquent la cubique de Weierstrass :

$$E_1\ :\ Y^2=4X^3+a_3X^2-2b_4X+b_6\in K\left[x,y\right] \qquad (3)$$

Où : $b_2=a_1^2+4a_2,\ \ b_4=2a_4+a_1a_3,\ \ b_6=a_3^2+4a_6.$ (4)

Ce sont des polynômes " homogènes de degré $2i$ " de l'anneau $\mathbb{Z}[a_1,a_2,\ldots,a_6]$

On élimine le coefficient 4 de $X^3$ et le monôme $b_2X^2$ ,avec le changement de variables

$$X=\frac{x-3b_2}{36}\ ,\ Y=\frac{y}{108},\ cara\left(K\right)\neq 2,\ 3 \qquad (5)$$

On obtient la cubique de Weierstrass :

$$E_2\ :\ y^2=x^3-27c_4x-54c_6\in K\left[x,y\right] \qquad (6)$$

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

$$c_4=b_2^2-24b_4,\text{ et }c_6=-b_2^3+36b_2b_4-216b_6;\ (7)$$

D'autres transformations permettent d'obtenir d'autres équations de Weierstrass :-

$$E_2\ :\ y^2=x^3+Ax+B\in K\left[x,y\right] \qquad (8)$$

**Équation de Legendre :**

$$E_4\ :\ y^2=x(x-1)(x-a)\ ,a\neq 0,1 \qquad (9)$$

**Modèle de Deuring à 1 paramètre :**

$$E_5\ :\ y^2+txy+y=x^3\in K\left[x,y\right] \qquad (10)$$

**Modèle de Kubert à 2 paramètres $s$ et $t$ :**

$$E_6\ :\ y^2+(1-s)\,xy-ty=x^3+x\in K\left[x,y\right] \qquad (11)$$

## CHAPITRE II :COURBES ALGÉBRIQUES PLANES

**Définition 6.**

***1.le discriminant d'une cubique de Weierstrass E/K est le polynôme "homogène" de degré 12 de l'anneau*** $\mathbb{Z}[b_2, b_4, b_6, b_8]$

$$\triangle(E) = 9b_2b_4b_6 - b_2^2b_8 - 8b_4^3 - 27b_6^2 \in K \ ,$$

***avec*** $4b_8 = b_2b_6 - b_4^2$ ***et*** $, Carac(K) \neq 2, 3$

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

$$j(E) = \frac{c_4^3(E)}{\triangle(E)} \in K$$

***3.l'invariant différentiel d'une cubique de Weierstras E est l'élément différentiel :***

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

***avec*** $f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$

$$\textbf{\textit{et}}\ df = f'_x dx + f'_y dy = (a_1y - 3x^2 - 2a_2x - a_4)dx + (2y + a_1x + a_3)dy$$

Le discriminant $\triangle(E)$ est lié au discriminant d'un polynôme $f(x)$ de l'équation de Weierstrass $y^2 = f(x)$

Le discriminant d'un polynôme $f(x)$ peut être calculé avec la théorie du Résultant de 2 polynômes

**Discriminant de cubiques de Weierstrass :**

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

$$\triangle(E) = \frac{c_4^3 - c_6^2}{1728} \ , \left(1728 = 12^3\right) ;$$

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

$\triangle(E) = -16\left(4A^3 + 27B^2\right)$ et $j(E) = \frac{1728(4A)^3}{\Delta(E)}$ ;

## CHAPITRE II :COURBES ALGÉBRIQUES PLANES

Legendre : $y^2 = x(x-1)(x-a)$ , $a \neq 0, 1$ .

$\triangle(E) = 16a^2\,(a^2 - 2a + 1)$ ;

3) $E$ : $y^2 + 9xy + y = x^3 + 8x^2 - 5x + 25 \in \mathbb{R}[x, y]$

$b_2 = 113,\ \ b_4 = -1,\ b_6 = 101\ b_8 = 2853.$

$\triangle(E) = -36808093$ et $j(E) = -56881,872181$

5) $E$ : $y^2 + xy - 3y = x^3 - 7x^2 - 12x \in \mathbb{R}[x, y]$

$b_2 = -27,\ \ b_4 = -27,\ b_6 = 9$ , $b_8 = -243.$

$\triangle(E) = 391473 = 9^3 \times 537$ et $j(E) = 6669,603352$

**Calcul du discriminant avec la méthode du résultant de 2 polynômes :**

Cette méthode est décrite par Lang, Kostarikine ,etc

**4.Résultant de 2 polynômes de l'anneau $K[x]$ :**

**Définition 7.*Soit un polynôme*** $f(x) = x^n + a_1x^{n-1} + \ldots + a_n$, *de degré* $n > 1$. ***et sa factorisation*** $f(x) = \prod\limits_{1 \leq i \leq n} (x - \theta_i)$ ***;alors le discriminant de*** $f$ ***est égal à :***

$$disc(f) = \prod(\theta_i - \theta_j)^2 \ , \ 1 \leq i < j \leq n$$

C'est donc une forme quadratique .

L'une des méthodes de calcul de ce discriminant utilise la théorie du Résultant de 2 polynômes

Soit 2 polynômes de l'anneau $\mathbb{R}[x]$ :

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \ \ de \ \ degré \ n \geq 1 \ ;$$

$$g(x) = b_0x^m + b_1x^{m-1} + .. + b_{m-1}x + b_m \, de \ \ degré \ \ m \geq 1 \ ;$$

**Définition 8.*Le Résultant des 2 polynômes*** $f$ $et$ $g$ ***est le déterminant d'ordre*** $n + m$ ***:***

$$Res(f,g) = \begin{vmatrix} a_0 & a_1 & . & . & . & a_n & 0 & . & . & 0 \\ 0 & a_0 & a_1 & . & . & . & a_n & 0 & . & 0 \\ 0 & 0 & a_0 & & & & & & & 0 \\ . & . & . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & . & . & . & . & a_n \\ b_0 & b_1 & . & . & . & . & b_m & 0 & . & 0 \\ 0 & b_0 & . & . & . & . & . & b_m & 0 & 0 \\ . & . & . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & . & .b_0b_1. & . & . & b_m \end{vmatrix}$$

formé de m lignes $(a_0 \ldots\ldots a_n)$ et n lignes $(b_0 \ldots\ldots b_m)$ de diagonale principale formée de m termes $a_0$ et n termes $b_m$ et les termes manquants sont remplacés par des zéros.

**Exemple :** $f(x) = 2x^3 + 3x^2 + 4$ et $g(x) = 3x^4 - 5x^3 + 8x^2 - 6x - 3$ le Résultant $Res(f,g)$ est donc le déterminant d'une matrice carrée d'ordre $3 + 4 = 7$ :

de lignes $(a_0, a_1, a_2, a_3) = (2, 3, 0, 4)$ et $(b_0, b_1, b_2, b_3, b_4) = (3, -5, 8, -6, -3)$

$$Res(f,g) = \begin{vmatrix} 2 & 3 & 0 & 4 & 0 & 0 & 0 \\ 0 & 2 & 3 & 0 & 4 & 0 & 0 \\ 0 & 0 & 2 & 3 & 0 & 4 & 0 \\ 0 & 0 & 0 & 2 & 3 & 0 & 4 \\ 3 & -5 & 8 & -6 & -3 & 0 & 0 \\ 0 & 3 & -5 & 8 & -6 & -3 & 0 \\ 0 & 0 & 3 & -5 & 8 & -6 & -3 \end{vmatrix}$$

Le calcul de ce déterminant relève de l'algèbre linéaire :Applications linéaires ; formes multilinéaires alternées ; développement suivant une ligne ou une colonne ...

Les résultants $Res(f,g)$ possèdent plusieurs propriétés :

**Proposition 1.** $Res(f,g) = 0$ ***si et seulement si*** $f$ ***et*** $g$ ***possèdent un zéro commun .***

Démonstration. Cf : [11] et [10]

□

**Proposition*2.Soient 2 polynômes***

$$f(x) = a_0 (x - \theta_1)(x - \theta_2) \ldots\ldots (x - \theta_n) \quad , \theta_i \neq \theta_j,\ n > 1$$

$$g(x) = b_0 (x - \lambda_1)(x - \lambda_2) \ldots\ldots (x - \lambda_m) \quad , \lambda_i \neq \lambda_j,\ m > 1$$

et $\theta_i \neq \lambda_j$

***Alors leur résultant est égal à :***

$$Res(f,\ g) = a_0^m \prod_i g(\theta_i) = (-1)^{mn} b_0^n \prod_j f(\lambda_j) = a_o^m b_o^n \prod_{i,j} (\theta_i - \lambda_j)$$

Démonstration. Cf : [11] et [10]

□

**Définition 8.*Le discriminant d'un polynôme non unitaire*** $f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n$ ***est égal à :***

$$disc(f) = a_0^{2n-2} \prod_{1 \leq j < i \leq n} (\theta_i - \theta_j)$$

Le discriminant d'un polynôme $f(x)$ de degré $n > 1$ est lié au résultant $Res(f, f')$ de $f$ et de sa dérivée $f'$

**Proposition 3.** ***Soit un polynôme*** $f(x)$ ***de degré*** $n$ ***,et sa dérivée*** $f'(x)$ ***alors***

$$disc(f) = (-1)^{\frac{n(n-1)}{2}} \frac{1}{a_0} Res(f,\ f').$$

Démonstration. avec les proposition 1 et 2 et la définition de $disc(f)$ .

□

**Applications .**

1- soient 3 polynômes $f(x)$ , $g(x)$ et $h(x)$ ;alors

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

2- le résultant d'un produit de 2 polynômes $fg$ satisfait la formule :

$$disc(f) = disc(f) disc(g) Res(f,g)^2$$

3- discriminant des polynômes $f(x) = x^n + a$ :

$$dis(x^n + a) = (-1)^{\frac{n(n-1)}{2}} n^n a^{n-1}$$

4- discriminant des polynômes $f(x) = x^n + x^{n-1} - \ldots + x + 1$ on utilise la relation :

$$(x-1) f(x) = x^n - 1$$

Avec les propriétès des résultants $Res(fg,\ h)$ et $Res(f,\ g)$ nous trouvons le :

$$disc(f) = (-1)^T.n^{n-2}\, avec\, T = \frac{1}{2}(n-1)(n-2)$$

Les cubiques peuvent être classifiées avec leurs invariants :$\triangle(C)$ , $j(C)$ , $Re(C)$ , $etc...$

**5.Classification des cubiques de Weierstrass :**

Une cubique de Weierstrass peut être singulière avec un nœud ou un point de rebroussement ou une Courbe Elliptique qui est cubique non singulière .Chaque cubique contient un point particulier :le point à l'infini

**Proposition 4.** ***Sur les cubiques de Weierstrass C le point à l'infini*** $O_C = (\infty, \infty)$ ***est un point non singulier sur C .***

Démonstration. Soit une cubique de Weierstrass d'équation

$$C : f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 \in \mathbb{R}[x,y] \qquad (1)$$

Dans le plan Projectif $\mathbb{P}^2(\mathbb{R})$,(1) devient :

$$C : F(x,y,z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_6Z^3 \in \mathbb{P}^2(\mathbb{R}) \qquad (2)$$

le point l'infini $O_C = (\infty, \infty) = (0,1,0)$ (3)

Dérivées partielles :$F'_X = Y^2 + a_1YZ - 3X^2 - 2a_2XZ$ , $F'_Y = 2YZ + a_1XZ - a_3Z^2$

$F'_Z = Y^2 + a_1XY + 2a_3YZ - a_2X^2 - 2a_4XZ - a_6Z^2 \qquad (4)$

Les coordonnées du point $O_C$ satisfont cette équation : $f(O_C) = 0$

Il en résulte que ce point est sur la cubique C

La valeur $F'_Z(0,1,0) = 1 \neq 0$ implique que le point $O_C = (0,1,0) = (\infty, \infty)$ est un point simple de la cubique C .

□

**Proposition** ***5.Soit les cubiques de Weierstrass C de discriminant*** $\Delta(C)$ ***et coefficient usuel*** $c_4 = b_2^2 - 24b_4$ ***alors :***

***1) les cubique C est singulière si et seulement si*** $\Delta(C) = 0$

***2) les cubique C est singulière avec un nœud si*** $c_4 \neq 0$

***3) les cubique C est singulière avec un point de rebroussement si*** $c_4 = 0$

*Démonstration.* preuve de "la cubique est singulière " implique "$\Delta(C) = 0$"

Je choisis une cubique de Weierstrass d'équation :

$$C : y^2 = x^3 + Ax + B \in \mathbb{R}[x, y]$$

L'hypothèse "C singulière" implique que le système $f'_x = 0$ et $f'_y = 0$ admet une solution

Pour $f(x, y) = x^3 + Ax + B - y^2$ (2)

$f'_x = 3x^2 + A = 0$ et $f'_y = -2y = 0$ (3)

$f'_x = 0$ implique $A < 0$ , posons $A = 3t^2$ , $t \in \mathbb{R}$ (4)

(3) et (4) impliquent le point singulier : $S = (t, 0)$

La relation $f(S) = 0$ implique $B = 2t^2$ (5)

Il en résulte la valeur $\Delta(C) = -16(4A^3 + 27B^2) = 0$

2) Preuve de :" $\Delta(c) = 0$ " implique "C singulière"

Nous utilisons la formule du résultante

$Res(f, f') = 0$ si et seulement si $f$ a un zéro double .

Il en résulte que la cubique C est singulière.

3) Preuve :" C singulière avec un nœud " implique " $c_4 \neq 0$ "

Soit $S = (x_s, y_s)$ le nœud de la cubique $C$ ; (1)

alors $\Delta(C) = 0$ et la cubique C admet au point S 2 tangentes distinctes .

Je choisis l'équation :

$C : y^2 = x^3 + Ax + B$; alors $c_4(C) = -48A$ (2)

Les pentes de ses tangentes au nœud sont égales à la dérivée

$$y' = \frac{3x^2 + A}{2y}, \; avec \, A = -3t^2 \qquad (3)$$

Il en résulte les 2 tangentes $y'$ pour $x = \pm t$ et $c_4(C) = -48A = 3 \times 48t^2 \neq 0$ (4)

4) Preuve de " C singulière avec un point de rebroussement " implique " $c_4 = 0$ "

Je garde (2) et(3) .Au point S de rebroussement la cubique C admet 2 tangentes confondues.

Il en résulte une valeur $y'$ cela implique $A = 0$ dans (3) .

Alors $c_4(C) = -48A = 0$ . □

Caractérisons les Courbes Elliptiques qui sont des cubiques de Weierstrass non singulières

**Proposition.** ***6.Soit une Courbe Elliptique E de discriminant*** $\triangle(E)$***.Alors***

(1) ***E est une Courbe Elliptique si et seulement si*** $\triangle(E) \neq 0$ ***.***
(2) ***E est de type 1 :une branche fermée finie et une branche ouverte infinie si*** $\triangle(E) > 0$;
(3) ***E est de type 2 :une seule branche ouverte infini et si*** $\triangle(E) < 0$;

*Démonstration* .Preuve de 1) : Par définition ,une Courbe Elliptique est une cubique de Weierstrass non singulière .

Par la proposition 5 "une cubique C est singulière si et seulement si $\Delta(C) = 0$"

Il en résulte qu'une cubique C est non singulière si et seulement si $\Delta(C) \neq 0$

2) Preuve de "une Courbe Elliptique E est de type 1 "si $\triangle(E) > 0$;

Soit une Courbe Elliptique E formée de 2 branches

Alors elle est coupée par l'axe Ox ou par une parallèle à Ox en 3 points simples.son équation de Weierstrass est de la forme :

$$y^2 = (x - e_1)(x - e_2)(x - e_3) \in \mathbb{R}[x] \qquad (1)$$

où les 3 nombres $e_i$ sont les abscisses des 3 points simples

Le discriminant de E est de la forme

$$\triangle(E) = 16 \prod_{1 \leq i < j \leq 3} (e_i - e_j)^2 \qquad (2)$$

Les carrés des nombres réels sont positifs (3)

Cela implique $\triangle(E) > 0$.

3) Preuve de "une Courbe Elliptique E est de type 2 "si $\triangle(E) < 0$;

## CHAPITRE II :COURBES ALGÉBRIQUES PLANES

Par définition une Courbe Elliptique E est de type 2 si elle est formée d'une seule branche qui est infinie .Donc elle est a une équation de Weierstrass de la forme

$$E : y^2 = (x-e)\, g(x) = f(x) \in K[x,y], car(K) \neq 2,3$$

où $g(x) = x^2 + rx + 1$ admet 2 zéros complexes conjugués $c \pm id$ .

Avec le calcul j'obtiens le discriminant :

$$disc((x-e)\, g(x)) = -4d^2 \left((e-c)^2 + d^2\right)^2 < 0$$

Avec la formule $R(f, f')$ j'obtiens $\triangle(E) < 0$

Soit une Courbe Elliptique d'équation de Weierstrass :

$$y^2 = f(x)$$

$\triangle(E)$ le discriminant de E et $dis(f)$ le discriminant de $f$

**Proposition.** ***7.Soit des Courbes Elliptiques E d'équation de Weierstrass :***

$E : y^2 = f(x) \in K[x,y], carK \neq 2,3.$

***1) si*** $f(x) = x^3 + a_2x^2 + a_4x + a_6$ ***alors*** $\triangle(E) = 16dis(f)$

***2) si*** $f(x) = 4x^3 + b_2x^2 + 2b_4x + b_6$ ***alors*** $dis(f) = 16\triangle(E)$

DÉMONSTRATION. Cf : [11] et [10] , Résultants

□

Ressemblons ces Résultats dans la

**Proposition.** ***8.L'ensemble des cubiques de Weierstrass est réparti en 4 classes .avec le discriminant*** $\triangle(E)$ ***et l'invariant*** $c_4(E)$ ***:***

***1) Classe des cubiques singulières avec un nœud si*** $\triangle(E) = 0$ ***et*** $c_4(E) \neq 0$ ***;***

***2) Classe des cubiques singulières avec un point de rebroussement si*** $\triangle(E) = 0$ ***et*** $c_4(E) = 0$ ***;***

***3) Classe des Courbes Elliptiques de type 1 (2 branches) si*** $\triangle(E) > 0$ ***;***

***4) Classe des Courbes Elliptiques de type 2 (1 seule branche) si*** $\triangle(E) < 0$ ***;*** □

Donnons un exemple de chaque classe .

## CHAPITRE II :COURBES ALGÉBRIQUES PLANES

### 1.Cubique de Weierstrass singulière avec un nœud :

**Exemple 1 :** Cubique de Weierstrass singulière avec un nœud :

$$E : y^2 + 4xy - 6y = x^3 + 5x^2 + 12x - 9 \in \mathbb{R}[x, y]$$

Coefficients : $a_1 = 4$ ;$a_3 = -6$ ; $a_2 = 5$ ; $a_4 = 12$ ; $a_6 = -9$

invariants :

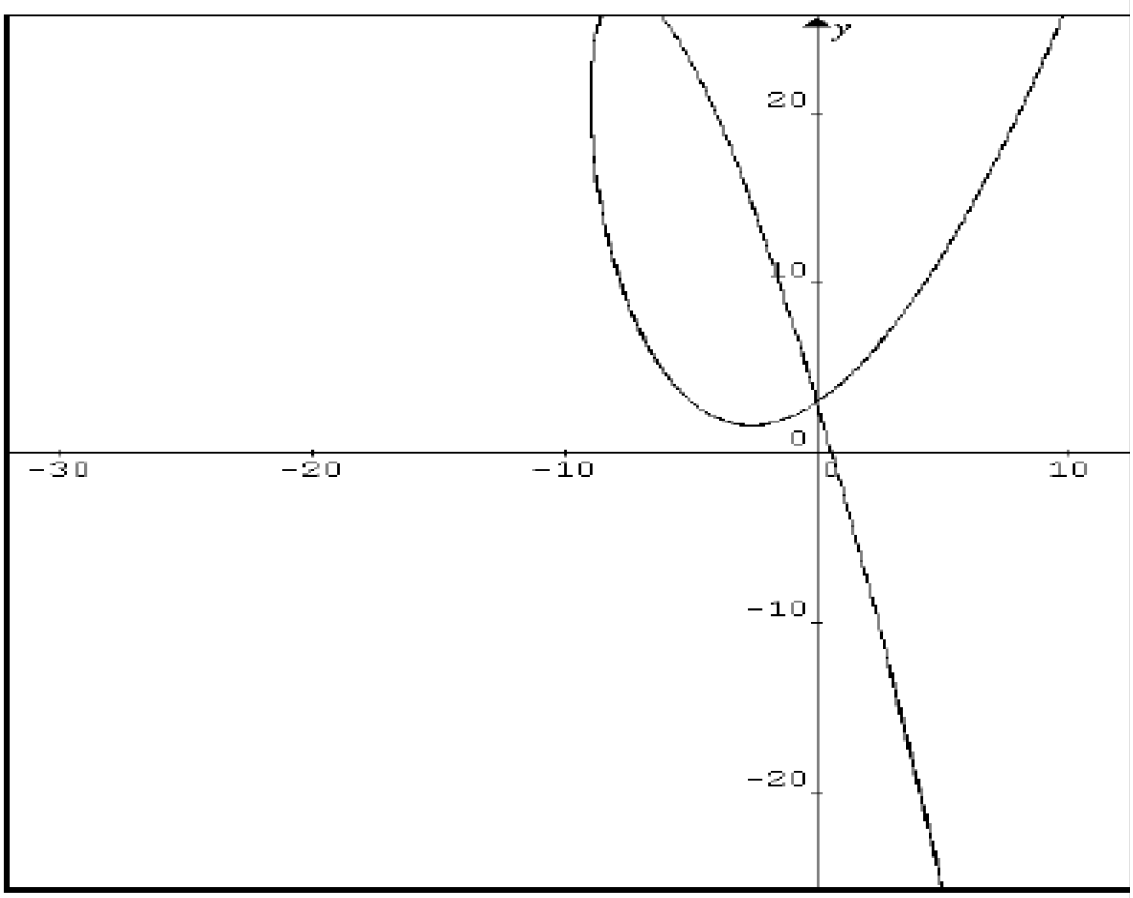
$b_2 = 36$ ; $b_4 = 0$ ; $b_6 = 0$ ; $b_8 = 0$

$\triangle(E) = 0$ :cela implique que la cubique est singulière .

$c_4(E) = b_2^2 - 24b_4 = 36^2 \neq 0$ ;

Donc la cubique est singulière avec un nœud.

Tracé de la cubique avec le logiciel Graphmatica :



## CHAPITRE II :COURBES ALGÉBRIQUES PLANES

2.**Une cubique avec un point de rebroussement :**

**Exemple 1 :** Cubique de Weierstrass singulière avec un point de rebroussement

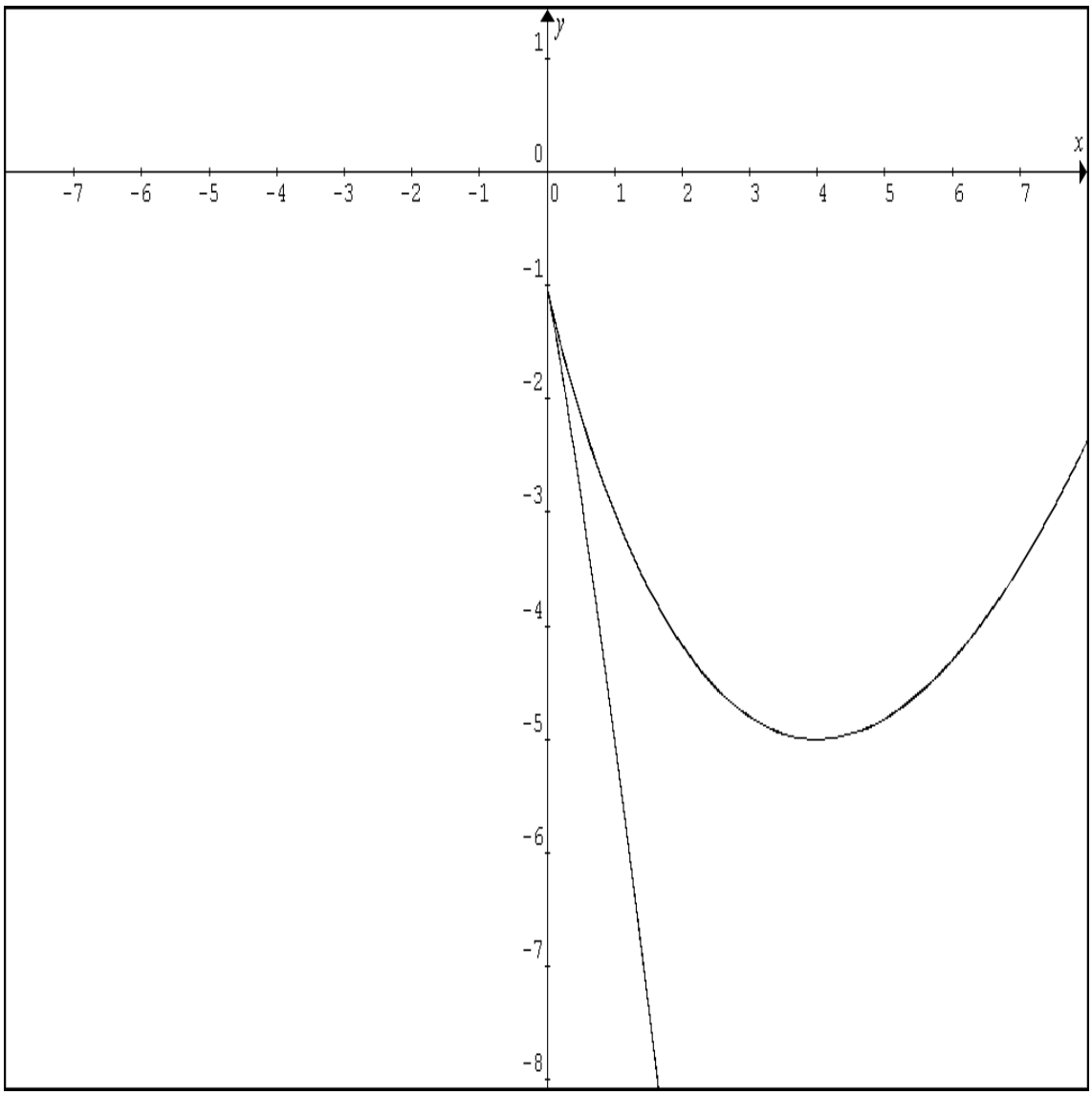
$$E : y^2 + 6xy + 2y = x^3 - 9x^2 - 6x - 1 \in \mathbb{R}[x, y] .$$

Coefficients : $a_1 = 6$ ;$a_3 = 2$ ; $a_2 = -9$ ; $a_4 = -6$ ; $a_6 = -1$ ;

invariants :$b_2 = 36 - 36 = 0$ ; $b_4 = 12 - 12 = 0$ ; $b_6 = 4 - 4 = 0$ ;

$\triangle(E) = 0$ , $c_4(E) = 0$ ;

Tracé de la cubique avec le logiciel Graphmatica :



**Exemple 3 :** Courbe Elliptique de type 1($\triangle(E) > 0$ )

$$E : y^2 = x^3 - x^2 - 2x + 40 \in \mathbb{R}[x, y] .$$

Coefficients : $a_1 = 0$ ;$a_3 = 0$ ; $a_2 = -1$ ; $a_4 = -2$ ; $a_6 = 40$ ;

invariants :$b_2 = -4$ ; $b_4 = -4$ ; $b_6 = 160$ ; $b_8 = -176$ ;

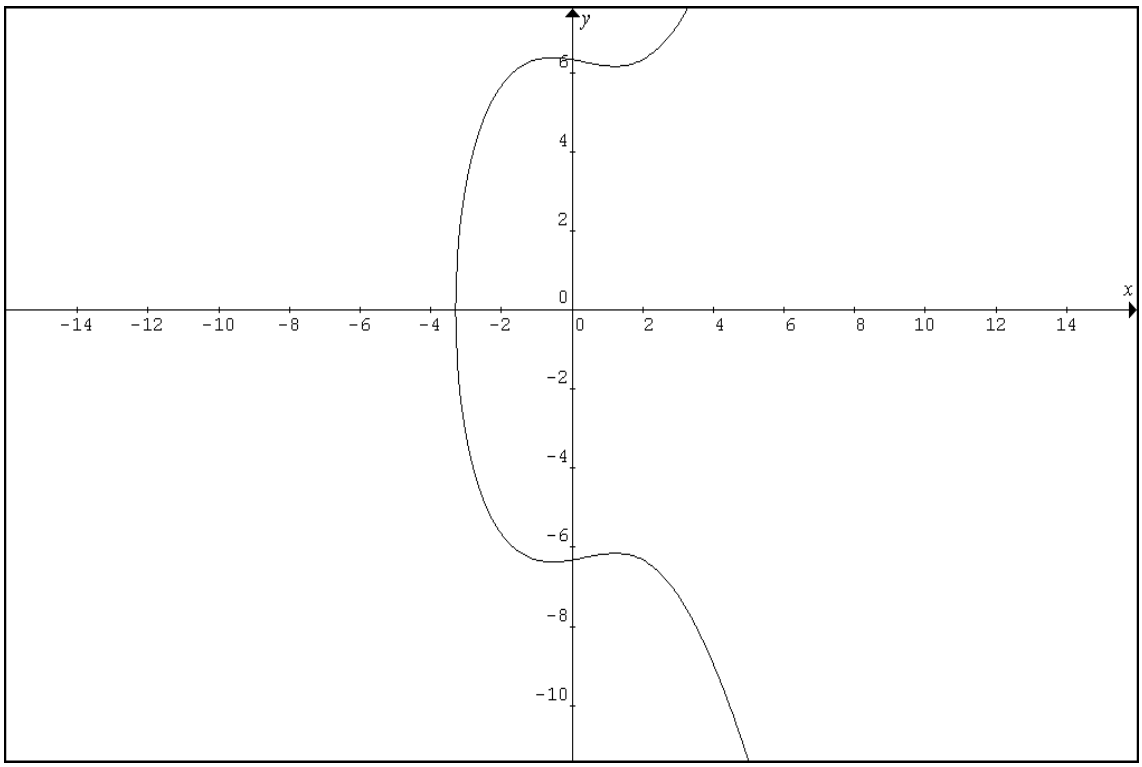
$\triangle(E) = 32 \times 689$ , $c_4(E) = 16 + 4 \times 24 = 112 = 16 \times 17$ ;

Point d'intersection avec Ox :

$y = 0$ , $x_1 = -5$ , $x_2 = 2$ , $x_3 = 4$ ;

$p_1(-5, 0)$ , $p_2(2, 0)$ , $p_3(4, 0)$ :3 points simples

Tracé de la cubique avec le logiciel Graphmatica :



**Exemple 4 :** Courbe Elliptique de type 2 ($\triangle(E) < 0$)

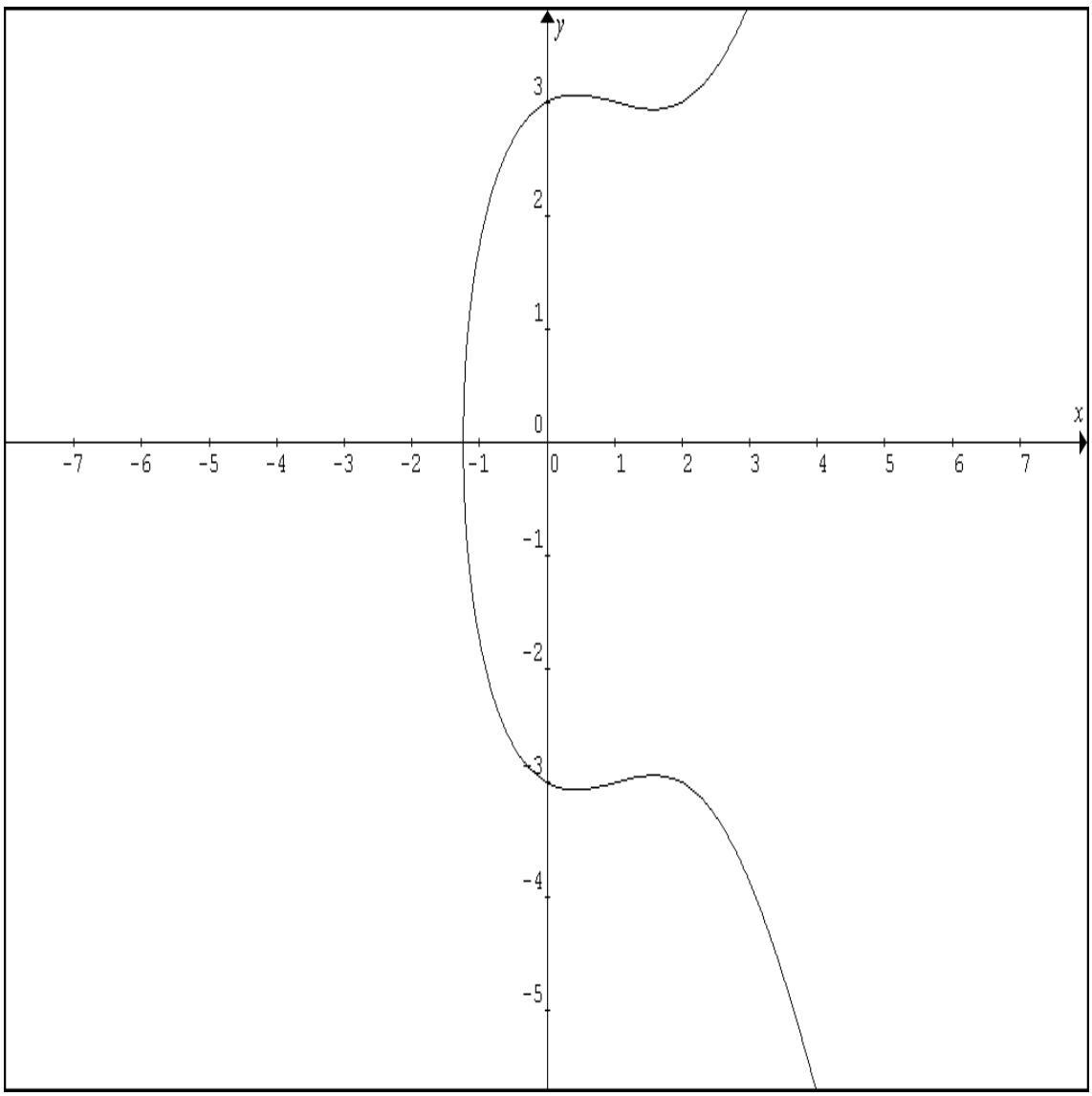
$$E : y^2 + 3x = x^3 - 3x^2 + 5x + 9 \in \mathbb{R}[x, y].$$

Coefficients : $a_1 = 0$ ;$a_3 = 3$ ; $a_2 = -3$ ; $a_4 = 5$ ; $a_6 = 9$ ;

invariants : $b_2 = -12$ ; $b_4 = 10$ ; $b_6 = 45$ ; $b_8 = -52$ ;

$\triangle(E) = 9(-12)\,10 \times 45 - 8 \times 10^3 - 27 \times 45^2 + 12^2 \times 52 = -32 \times 2657$ ;

Tracé de la cubique avec le logiciel Graphmatica :



## CHAPITRE III :GROUPE DE MORDELL-WEIL

Dans ce chapitre nous décrirons la structure de l'ensemble E(K) des points des cubiques de Weierstrass. En suite nous étudierons quelques propriétés de ces groupes E(K) .

### 1.Structure des groupes abéliens E(k) :

Soit la une cubique de Weierstrass :

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

Dans le plan Projectif $\mathbb{P}^2(\mathbb{R})$,(1) devient :

$$E' : F(x, y, z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_6Z^3 \in \mathbb{P}^2(K)[x, y, z] \quad (2)$$

Ce polynôme est homogène de degré 3.

**Définition 1.** ***a)un corps global est le corps*** $\mathbb{Q}$ ***des nombres rationnels ou un corps de nombres algébrique*** $K = \mathbb{Q}(\theta)$ ***, d'élément primitif*** $\theta =$ ***zéro du polynôme*** $f(x) \in \mathbb{Q}[x]$ ***,irréductible , de degré n , qui admet n zéro*** $\theta_1, \theta_2 ... \theta_n$ ***permutable par le groupe de Galois de K sur*** $\mathbb{Q}$ ***; K est de caractéristique nulle .***

***b) un corps local est un corps commutatif infini de caractéristique un nombre premier*** $p \geq 2$

***c) un corps fini est un corps commutatif*** $\mathbb{F}_q$ ***, à*** $q = p^n$ ***éléments et de caractéristique un nombre premier*** $p$ ***.***

**Exemples :**

1) $K = \mathbb{Q}(\sqrt{5})$ , $K = \mathbb{Q}(\sqrt{-14})$ , $K = \mathbb{Q}(\sqrt{6 + 2\sqrt{11}})$ , $K = \mathbb{Q}(\sqrt[3]{22})$ , sont des corps globaux .

2) $\mathbb{Q}_5 = 5^e$ corps p-adique , $\mathbb{Q}_{17} = 17^e$ corps p-adique , sont des corps locaux .

3) $\mathbb{F}_7 = \{1, 2, \ldots, 6, 7 = 0\}$ , $\mathbb{F}_{3^2} = \{1, 2, \ldots, 8, 9 = 0\}$ , sont des corps finis .

Considérons un corps global $K = \mathbb{Q}, \mathbb{R}, \mathbb{Q}(\theta)$ et une Courbes Elliptique E/K .

Soit l'ensemble $E(K)$ des points K- rationnels de E .

$E(K) = \{P = (x, y)\ satisfaisant\ l'équation\ (1)\ ;\ x\ et\ y\ quotions\ de\ 2\ polynômes\}$

Puisque l'équation de Weierstrass de E est de degré 3 ,il existe des sécantes qui la coupe en 3 points distencts $p_1$, $p_2$ , $p_3$ .

Alors ces 3 points colinéaires de la courbe satisfont la relation :

$$p_1 + p_2 + p_3 = 0_E \, , 0_E = (\infty, \infty) = (0, 1, 0) \, ; \qquad (3)$$

Le point $O_E$ est déterminé par la direction de l'axe $Oy$ dans le plan $Oxy$ .

**Proposition 1.** ***l'ensemble*** $E(K)$ ***des points K-rationnels d'une Courbe Elliptique E/K est un groupe abélien d'élément neutre le point*** $O_E = (\infty, \infty)$ ***, et de loi basée sur la règle géométrique de 3 points colinéaires de E :***

$$P_1 + P_2 + P_3 = O_E$$

Preuve de l'axiome de l'élément neutre :

Soit un point $P \neq O_E$ de E .

La parallèle à $Oy$ passante par P coup E en $O_E$ :

$P + O_E = O_E + P = P$ et $O_E + O_E = O_E$ .

L'axiome est vérifié .

Preuve de l'axiome du symétrique :

Soit un point P de la courbe E, alors la parallèle à l'axe $Oy$ passante par P recoupe la courbe E en R.

$$P + R + O_E = O_E$$

Il en résulte : $R = -P$

L'axiome du symétrique est vérifié.

Pour vérifier l'axiome d'associativité ,il n'y a pas de moyen géométrique .Il faut calculer les sommes $P + R = M$ ,$M + S$ , $R + S = U$ et $P + U$ puis comparer les résultats ces axiomes sont illustrés par la figure ci-dessous

$$E : y^2 = x^3 + 3x^2 - 10x - 24 \in \mathbb{R}\,[x, y]$$

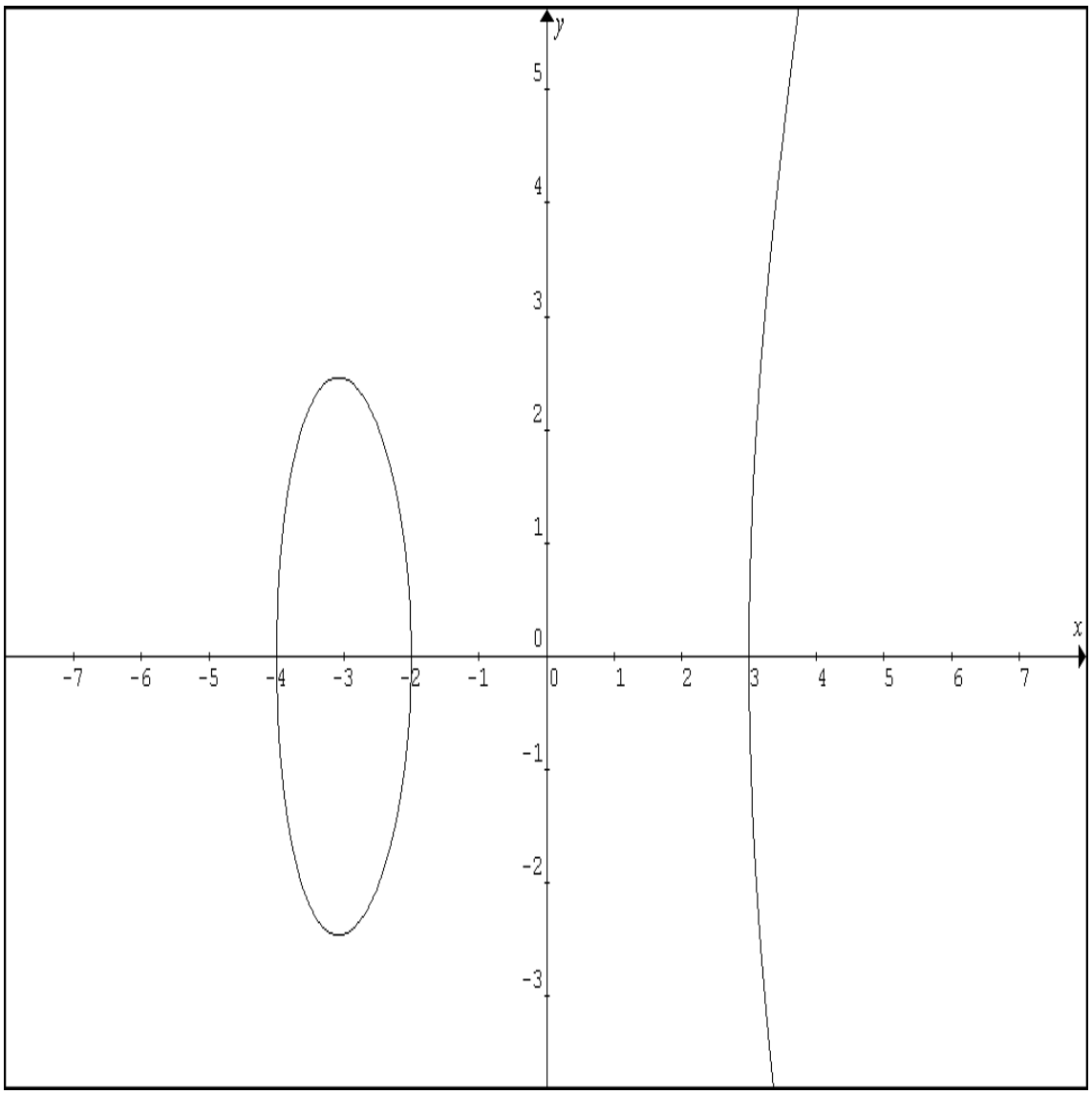
coefficients : $a_1 = a_3 = 0$ ; $a_2 = 3$ ; $a_4 = -10$ ; $a_6 = -24$

invariants : $b_2 = 12$ ; $b_4 = -20$ ; $b_6 = -96$ ; $b_8 = -4 \times 97$ ;

$$\triangle\,(E) = 64 \times 1225 > 0$$

E est une Courbe Elliptique à 2 branches.

## CHAPITRE III :GROUPE DE MORDELL-WEIL




**Définition 2.** ***Le groupe additif abélien*** $E(K)$ ***est le groupe de Mordell – Weil de la Courbe Elliptique E.***

**Théorème de Mordell-Weil :**

*Les groupes* $E(K)$ *de Mordell – Weil des Courbes Elliptiques sont additifs abéliens de type fini .*

Démonstration. cf [3] , [7]

□

## CHAPITRE III :GROUPE DE MORDELL-WEIL

André WEIL est un mathématicien américain d'origine française , Professeur à l'institut Princeton .

Mordell est un mathématicien anglais , Professeur à Cambridge .

**Corollaire.** ***Le groupe*** $E(K)$ ***de Mordell-Weil est isomorphe au produit directe de 2 groupes abéliens :***

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

$T(E)$ ***est le groupe de torsion de*** $E$ ***qui est fini ;***

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

Démonstration. cf [3]

□

Cette formule d'isomorphisme de groupe du corollaire est semblable à la formule du groupe des unités des corps de nombres algébriques .

**Théorème ( de Dirichlet)**

***Soit un corps de nombres algébriques L de degré*** $[L:] = n$ **,** $n = a + 2b$ **,*a conjugués réels*** $\sigma(L)$ ***de L et b paires de conjugués complexes*** $\sigma(L) \subset \mathbb{C}$ **. *Alors les unités de L forment un groupe*** $U(L)$ ***abélien ,multiplicatif de type fini , isomorphe à un produit direct de groupes abéliens :***

$$U(L) \simeq C(L) \times \mathbb{Z}^r$$

***o***ù $C(L)$ ***groupe des racines de l'unité contenues dans L***

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

**Définition 3.** ***Une unité d'un corps de nombres L est un élément*** $u$ ***de L de norme égale à*** $N_{L/Q}(u) = \pm 1$ **.**

Ansi pour tous les corps de nombres réels L $C(L) = \{1, -1\}$

pour tous les corps de nombres imaginaires ,il y a 2 cas :

$C(L) = \{1, -1, i, -i, i^2 = 1\}$ et $C(L) = \{1, -1, j, -j, j^2, -j^2, j^3 = 1\}$

**Définition 4.** ***Tout système de générateurs du groupe*** $U(L)$ ***est un système d'unité fondamentales de L :*** $u_1, ..., u_r$ **. *de sorte que toute unité u est un produit de la forme***

$$u = \pm u_1^{n_1} u_2^{n_2} ... u_r^{n_r} \text{ , avec } n_i \in \mathbb{N}$$

Il existe des algorithmes de calcul des unités des corps quadratiques $K = \mathbb{Q}\left(\sqrt{d}\right)$ .

## CHAPITRE III :GROUPE DE MORDELL-WEIL

**Définition 5.** ***L'entier naturel*** $r \geq 0$ ***du corollaire est le rang arithmétique de la Courbe Elliptique E ; c'est le nombre des générateurs*** $p_1, ..., p_r$ ***indépendants de la partie infinie*** $E(K)/T(E)$ ***de la Courbe E .***

Si les rangs des groupes $U(L)$ des unités des corps L peuvent être calculés avec une formule $r = a + b - t$ , il n'en est pas de même pour les Courbes Elliptiques .

Nous étudierons les méthodes de calculs dans le chapitre IV .

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

Nous utiliserons la règle géométrique de 3 points colinéaires de E et les formules de Viète [10] des fonctions symétriques élémentaires des zéros des polynômes

$$f(x) = a_0 x^n + a_1 x^{n-1} + .... + a_n \in \mathbb{R}[x, y]$$
$$f(x) = x_0 (x - \theta_1) ... (x - \theta_n)$$

En particulier la somme des zéros est égale à $\sum_{1 \leq i \leq n} \theta_i = -a_1/a_0$

**Proposition 3.** ***Soit une Courbe Elliptique E d'équation de Weierstrass :***

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

***Pour tout point*** $P = (x_p, y_p) \neq O_E$ ***de E , le symétrique de P est le point*** $-P$ ***de coordonnées :*** $x(-P) = x_p$ ***et*** $y(-P) = -(a_1 x_P + a_3 + y_p)$, (2)

Preuve .La parallèle à l'axe $Oy$ passante par le point P coupe E en 2 points P et $R = -P$ (3) ;

L'équation (1) est une équation en $y$ quadratique ; elle admet 2 zéros $y_p$ et $y(-P)$ (4)

Leur sommes est une fonction symétrique de Viète :

$$y_p + y(-P) = -a_1 x_p - a_3 \qquad (5)$$

l en résulte la valeur

$$y(-P) = -y_p - a_1 x_p - a_3 \qquad (6)$$

Donc les coordonnées du symétrique de tout point $P(x, y)$ sont égales à

$x(-P) = x_p$ ***et*** $y(-P) = -(a_1 x_P + a_3 + y_p)$, (7) $\square$.

## CHAPITRE III :GROUPE DE MORDELL-WEIL

I

**Proposition 4.** ***Soit une Courbe Elliptique E d'équation de Weierstrass (1) :***

***et 2 points*** $P_i = (x_i, y_i), P_1 \neq \pm P_2$ ***de E , Alors les coordonnées de la somme*** $P_1 + P_2 = M$ ***de ces 2 points sont égales à :***

$x(M) = t^2 + a_1 t - a_2 - x_1 - x_2$ ***pour*** $x_1 \neq x_2$ ***;***

$y(M) = -t^3 - 2a_1 t^2 + (a_2 - a_1^2 + 2x_1 + x_2)t + a_1 a_2 - a_3 + a_1(x_1 + x_2) - y_1$ ***avec*** $t = (y_1 - y_2) / (x_1 - x_2)$ ***;***

2) La somme de deux points $P_1 + P_2$

Soient 2 points $P_i = (x_i, y_i)$ de E , $x_1 \neq x_2$ et $P_1 \pm P_2$ ;(1)

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

$y = t(x - x_1) + y_1$ avec $t = \frac{y_1 - y_2}{x_1 - x_2}$ (2)

L'équation de E devient une équation cubique en $x$ :

$$x^3 + a_2 x^2 + (a_4 - a_1 y)\, x + a_6 - a_3 y = 0 \quad (3)$$

Donc cette équation admet 3 zéros $x_1$ , $x_2$ , $x_3$ (4)

Les formules de Viète impliquent : $x_1 + x_2 + x_3 = -P_3$ et les coordonnées du symétrique , nous obtenons les formules de la proposition .

**Proposition 4.** ***Pour tout point*** $P \neq O_E$ ***d'une Courbe Elliptique E , le point*** $2P$ ***a pour coordonnées :***

$x(2P) = y'^2 + a_1 y' - 2x$ ***;***

$y(2P) = -y'^3 - 2a_1 y'^2 + (a_2 - a1^2 + 3x)y' + a_1 a_2 - a_3 + 2a_1 x - y.$

***avec la dérivée*** $y' = \frac{(3x^2 + 2a_2 x + a_4 - a_1 y)}{(2y + a_1 x + a_3)}$

*Preuve*. Lorsque $P_1 = P_2$ , la sécante $p_1 p_2$ devient la tangente à la courbe au point $P$ (1) .

Cette tangente coupe E en un point T qui satisfait : $2P + T = O_E$ ; (2)

Il en résulte : $2P = -T$ ; (3)

avec l'équation de la tangente et les coordonnées du symétrique , nous obtenons les formules de la proposition .□

## CHAPITRE III :GROUPE DE MORDELL-WEIL

### 3.Sous groupe de m-torsion :

Selon la théorie des groupes il y a des éléments d'ordre fini .

**Définition 5 .**

***1) Un point d'une Courbe Elliptique E est d'ordre m si*** $mp = O_E$ **.**

***2)l'ensemble des points P de E d'ordre*** $m \geq 2$ ***est un sous groupe du groupe E(K) ; c'est un sous groupe de m-torsion :***

$$E[m] = \{p \in E; mp = O_E\}$$

***Le symbole*** $mp$ ***signifie :***

$mp = p + p + \ldots . + p$ , m fois p, si $m > 1$ ;

$mp = -p - p. \ldots . . - p$ , -m fois p , si $m < -1$ ;

$OP = O_E$ , si $m = 0$ .

Si $m = \infty$ , $mp$ est d'ordre infini ;ce n'est pas un point de torsion .

Il en résulte que les sous groupes de m-torsion sont finis .

**Définition 6.** ***Le groupe de torsion d'une Courbe Elliptique E est l'ensemble*** $T(E)$ ***des points*** $P$ ***de E d'ordre fini***

$$T(E) = \{p \in E(K), mp = O_E, m\, fini\}$$

Dans [15] nous trouvons quelques résultats .

**Théorème** ***(Lutz- nagell ) :***

***Soit une Courbe Elliptique*** $E/\mathbb{Q}$ ***d'équation de Weierstrass :***

$$E : y^2 = x^3 + Ax + B \in \mathbb{Q}[x, y], A, B \in \mathbb{Z}$$

***1) Si P est un point de torsion non nulle , alors*** $x(P)$ ***et*** $y(P) \in \mathbb{Z}$ ***;***

***2) Soit ;***$2P = O_E$ ***soit*** $y(P)^2$ ***divise*** $4A^3 + 27B^2$ $\square$

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

Alors $4A^3 + 27B^2 = 8 \times 27$

Les diviseurs $d^2$ de $8 \times 27$ sont $d^2 = 4, 9, 36 = y(P)^2$ ,cela implique les ordonnées possibles : $y = \pm 2, \pm 3, \pm 6$

L'équation diophantienne $4 = x^3 = 3x + 2 = 0$ n'admet pas de solution

Les autres équations diophantiennesd pour $d^2 = 9, 36$ n'admettent pas de solutions

## CHAPITRE III :GROUPE DE MORDELL-WEIL

**Théorème** ***(Masur ) :Soit une Courbe Elliptique*** $E/\mathbb{Q}$ ***.Alors ses sous groupes de torsion*** $T(E/\mathbb{Q})$ ***sont isomorphes à l'un des 15 groupes :***

$\mathbb{Z}/N\mathbb{Z}$ ***pour*** $1 \leqslant N \leqslant 10$ ***ou*** $N = 12$ ***;***

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ ***pour*** $1 \leqslant N \leqslant 4$ .

**Théorème** ***(Silverman ) :*** $T(E_p) \simeq \mathbb{Z}/2\mathbb{Z}$ ***pour tout nombre premier*** $p$ ***et les Courbes Elliptiques :*** $E : y^2 = x^3 + px$

*Preuve*. proposition 6-2 [15] □ .

Décrivons l'algorithme de J.W.S.CASSELS [3]

**Théorème** ***(Cassels ) :Soit une Courbe Elliptique*** $E/\mathbb{Q}$ ***d'équation de Weierstrass :***

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

***Alors les coordonnées des points*** $mp$ ***,*** $P \in E(\mathbb{Q})$ ***sont de la forme :***

$$x_m = \frac{\phi_m}{\psi_m^2}, y_m = \frac{\omega_m}{\psi_m^3}, m \in \mathbb{N}$$

***1)*** Les polynômes $\psi_m$ satisfont les relations :

$\psi_{-1} = -1, \psi_0 = 0, \psi_1 = 1, \psi_2 = 2y$ (1)

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

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

$\psi_{2m} = 2\psi_m(\psi_m\psi_{m-1} - \psi_{m+2}^2\psi_{m+1}^2$ *pour* $m \geq 2$ (4)

$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3$ *pour* $m \geq 1,$ (5)

***2)*** Les polynômes :

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

*Preuve.*

(1) par récurrence sur m ;

(2) théorie de la fonction $\wp(z)$ de Weierstrass ,selon Wiber et Fricke □ .

Nous obtenons les points $mp$ pour $m = -1, 0, 1$ et 2

$0P = 0_E = (\infty, \infty)$ ; cela implique $\psi_0 = 0$ ;

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

Pour $m = -1$ , $-P = (x, y) = \left(\frac{x}{1^2}, \frac{y}{1^3}\right)$ ; $\psi_1 = 1$

## CHAPITRE III :GROUPE DE MORDELL-WEIL

***Application :***

$$E : y^2 = x^3 + 5x - 2 \in \mathbb{Q}[x, y]$$
$$4A^3 + 27B^2 = 608 > 0$$

$E(\mathbb{Q})$ contient le point $P = (2; 4)$

$\psi_{-1} = -1, \psi_0 = 0, \psi_1 = 1, \psi_2 = 2y$

$\psi_3 = 3x^4 + 30x^2 - 24x - 25 = 95$

$\psi_4 = 4y(x^6 + 25x^4 - 40x^3 - 125x^2 + 40x - 157) = 9072$

$\psi_5 = \psi_4\psi_2^3 - \psi_1\psi_3^3 = 12y^4(x^6 + 25x^4 - 40x^3 - 125x^2 + 40x - 157) - (3x^4 + 30x^2 - 24x - 25)^3$
$\psi_5 = 3787489$

$\psi_6 = 1901165080$

$4y\omega_4 = \psi_6\psi_3^2 - \psi_2\psi_5^2 = 2812941921879$

$\phi_4 = x\psi_4^2 - \psi_3\psi_5 = 2(9072)^2 - 95 \times 3787489 = -195209087$

$4P = \left(\frac{\phi_4}{\psi_4^2}, \frac{\omega_4}{\psi_4^3}, \right) = \left(\frac{-195209087}{(9072)^2}, \frac{2812941921879}{16 \times (9072)^3}\right)$

**4.Réduction des Courbes Elliptiques :**

Lorsque les coefficients numériques $a_i$ des équations de Weierstrass ont un grand nombre de chiffres , on réduit par le moyen de la théorie des congruences modulo un nombre premier $p$ du corps $\mathbb{Q}$ des nombres rationnels

**Exemple.** $159 \equiv 1 \, mod \, 2$ **;** $159 \equiv 0 \, mod \, 3$ **;** $159 \equiv 4 \, mod \, 5$ **.**

**Définition 7.** ***Dans l'anneau $\mathbb{Z}$ des entiers rationnels , une congruence modulo un nombre naturel n entre 2 entiers naturels a et b est une relation de la forme .***

$$a \equiv b \, mod \, n \quad si \; a - b = kn \; pour \; k \in \mathbb{Z}$$

Les réductions qui nous intéressent sont les réductions modulo les nombres premiers .

La Courbe Elliptique E est transformée en la courbe réduite $E(p)$ modulo les nombres premiers $p$ .

**Exemple.**

que l'on applique sur les coefficients $a_i$. On obtient la courbe $\tilde{E}$

$$E : y^2 + 5234xy - 6855y = x^3 + 12411x^2 - 15072x + 7830 \in \mathbb{Q}[x, y]$$

## CHAPITRE III :GROUPE DE MORDELL-WEIL

Les courbes réduites $E(p)$ modulo p sont :

$$E(2) : y^2 + y = x^3 + x^2 \in \mathbb{F}_2[x, y]$$
$$E(3) : y^2 + 2xy = x^3 \in \mathbb{F}_3[x, y]$$
$$E(5) : y^2 + 4xy = x^3 + x^2 + 3x \in \mathbb{F}_5[x, y]$$
$$E(7) : y^2 + 5xy = x^3 + 6x^2 + 4 \in \mathbb{F}_7[x, y]$$
$$E(11) : y^2 + 9xy + 2y = x^3 + 3x^2 + 9x + 9 \in \mathbb{F}_{11}[x, y]$$

Le symbole $\mathbb{F}_P$ désigne les corps finis à $p$ éléments .

$\mathbb{F}_P = \{1, 2, ..., p-1, p = 0\}$ , $\mathbb{F}_2 = \{0, 1\}$ , $\mathbb{F}_3 = \{1, 2, 3\}$

La courbe réduite admet les invariants réduites $\triangle(E(p))$ et $c_4(E(p))$ .

Il y a donc 3 cas possibles pour les courbes réduites .

$E(p)$ est une Courbe Elliptique , ou une cubique singulière avec un noeud , ou une cubique singulière avec un point de rebroussement .

**Définition 8.** ***Soit un nombre naturel premier*** $p$ ***et une Courbe Elliptique*** $E/\mathbb{Q}$

***1) La réduction modulo*** $p$ ***est bonne si*** $E(p)$ ***est une Courbe Elliptique sur le corps*** $\mathbb{F}_P$ ***;***

***2)La réduction est multiplicative si*** $E(p)$ ***est une cubique avec un nœud ;***

***3) La réduction est additive si la courbe réduite*** $\tilde{E}$ ***a un point de rebroussement .***

**Définition 9.**

(1) ***Une bonne réduction modulo*** $p$ ***est une réduction stable ;***
(2) ***Une réduction multiplicative est une réduction semi -stable ;***
(3) ***Une réduction additive est une réduction instable .***

Lorsque le corps de base des Courbes Elliptiques E est un corps de nombres algébriques $K = \mathbb{Q}(\theta)$ , les nombres naturels premiers $p$ sont remplacés par les idéaux premiers du corps $K$ .

Chaque nombre premier $p \in \mathbb{N}$ , engendre dans l'anneau $A(K)$ des entiers algébriques du corps $K$ un idéal $pA(K)$ de type

1) ramifié si $pA(K) = p_K^n$ , $p_K =$ idéal premier de $K$ , $n \in \mathbb{N}$ .

2) décomposé si $pA(K) = P_1P_2...P_g$ =produit d'idéaux premiers $P_i$ conjugués , de norme commune $N_{K/\mathbb{Q}}(P_i) = p$ ,

3) inerte si $pA(K) = P =$ idéal premier de norme $N_{K/\mathbb{Q}}(P) = p^2$ ,

## CHAPITRE III :GROUPE DE MORDELL-WEIL

La réduction dans le corps $\mathbb{Q}$ s'obtient avec la théorie des valuations des corps [11] .

Il y a une valuation triviale , des valuations archémidiennes , des valuations non archémidiennes , des valuations p-adiques .

Nous ne traiterons pas dans ce chapitre des valuations qui déborde notre sujet sur les rangs des Courbes Elliptiques .

### 5.Homomorphismes des Courbes Elliptiques :

Un homomorphisme de Courbes Elliptiques $E/K$ et $E'/K$ est un homomorphisme de leurs groupes de Mordell Weil :

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

de valeur $f(P+R) = f(p) + f(R)$ et $f(O_E) = f(O_{E'})$ ,$O_E = O_{E'} = (\infty, \infty)$.

Il y a des isomorphismes ,des endomorphismes ,des automorphismes , des homomorphismes non bijectifs , des isogénies .

Commençons par les isomorphismes

**Proposition 6.** ***Soit une Courbe Elliptique*** $E/K$ ***son groupe de Mordell-Weil*** $E(K)$ ***.Alors ,l'application :***

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

***de valeur :*** $f(x,y) = (u^2x + r, u^3y + su^2x + t)$ ***, pour*** $u \neq 0$ , $r, s, t \in K, car(K) = 0$ .

***est un isomorphismes des Courbes Elliptiques*** $E$ ***et*** $E'$ .

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

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

La transformée de E par $f$ est une cubique $f(E) = E'$

$$E' : y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6 \in K[x,y] \quad (2)$$

La relation entre $E$ e***t*** $E'$ est déterminés par le calcul

La cubique E' a un point à l'infini $O_E = (\infty, \infty)$ (3)

Posons $X = u^2x + r$ , $Y = u^3y + su^2x + t$ (4)

L'hypothèse $u \neq 0$ implique

$x = (X - r)/u^2$ et $y = (Y - su^2x - t)/u^3$ (5)

Il en résulte que l'application réciproque $f^{-1}(x,y)$ existe ; donc $f$ est un isomorphisme de Courbes Elliptiques . □

Les relations entre les coefficients et les invariants de 2 Courbes Elliptiques E et E' s'obtiennent avec l'équation de E et les formules de la proposition .

**Corollaire.**

Soit les hypothèses de la proposition 6 :

Alors : ***Relation entre*** $a_i$ ***et*** $a'_i$

$ua'_1 = a_1 + 2s$ ; $u^2a'_2 = a_2 - sa_1 + 3r - s^2$ ;

$u^3a'_3 = a_3 + ra_1 + 2t$ ; $(Iso1)$

$u^4a'_4 = a_4 - sa_3 + 2ra_2 - (rs+t)a_1 + 3r^2 - 2st$ ;

$u^6a'_6 = a_6 + ra_4 - ta_3 + r^2a_2 - rta_1 - t^2 + r^3$

***Relation entre*** $b_{2i}$ ***et*** $b'_{2i}$ ***:***

$u^2b'_2 = b_2 + 12r$ ; $u^4b'_4 = b_4 + rb_2 + 6r^2$ ;

$u^6b'_6 = b_6 + 2rb_4 + r^2b_2 + 4r^3$ ; $(Iso2)$

$u^8b'_8 = b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4$ ;

***Relation entre*** $c_{2i}$ ***et*** $c'_{2i}$ ***:***

$u^4c'_4 = c_4$ et $u^6c'_6 = c_6$ $(Iso3)$

***Relation entre les discriminants :***

$$u^{12}\triangle(E') = \triangle(E) \quad (Iso4)$$

***Relation entre les invariants modulaires :***

$$j(E') = j(E) \qquad (Iso5)$$

□.

**Exemple.**

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

invariants : $b_2 = 1$ ; $b_4 = 0$ ; $b_6 = 52$ ; $b_8 = 13$ ; $c_4 = 1$

$\triangle(E) = -13 \times 433$ , $j(E) = -\frac{1}{13\times 433}$

Isomorphisme avec $u = 1/2$ , $r = 3$ , $s = -2$ , $t = 0$ .

Équation de la cubique $E'$ isomorphe à $E$ .

***Relation*** $(Iso1)$

$a'_1 = 2a_1 - 8 = 2 \times 3 - 8 = -2$ ;

$a'_2 = 4a_2 + 8a_1 + 20 = 4 \times (-2) + 8 \times 3 + 20 = 36$ ;

$a'_3 = 8a_3 + 24a_1 = 8(-4) + 24 \times 3 = 40$ ;

$a'_4 = 16(a_4 + 2a_3 + 6a_2 + 6a_1 + 27) = 16(6 + 2(-4) + 6(-2) + 6(3) + 27) = 496$ ;

$a'_6 = 64(a_6 + 3a_4 - r^2a_2 + r^3) = 64(9 + 3(6) - 9(-2) + 27) = 4608$ .

***Relation*** $(Iso2)$ ***:***

$b'_2 = 4(b_2 + 12r) = 148$ ;

$b'_4 = 16(b_4 + rb_2 + 6r^2) = 912$ ;

$b'_6 = 64(b_6 + 2rb_4 + r^2b_2 + 4r^3) = 10816$ ;

$b'_8 = 256(b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4) = 192256$ .

***Relation*** $(Iso3)$ ***:***

$c'_4 = 16c_4 = 16$

***Relation*** $(Iso4)$ ***:***

$\triangle(E') = 2^{12}\triangle(E) = 4096 \times (-13 \times 433) = 23056384$

Équation de la cubique $E'$ isomorphe a $E$ :

$$E : y^2 - 2xy + 40y = x^3 + 36x^2 + 496x + 4608$$

Examinons les endomorphismes des Courbes Elliptiques

**Proposition7.** ***les endomorphismes d'une Courbe Elliptique*** $E/K$ ***forment un anneau*** $End(E/K)$ ***isomorphe à l'anneau*** $\mathbb{Z}$ ***ou à un ordre de l'algèbre des quaternions .***

*Preuve* .dans [15] -Corollary 9-4

**Définition 10.** ***l'algèbre des quaternions est une l'algèbre engendré par 2 éléments*** $\alpha$ ***et*** $\beta$ ***satisfaisant les conditions :***

$$\alpha^2, \beta^2 \in \mathbb{Q}, \ \alpha^2 < 0, \ \beta^2 < 0, \ \beta\alpha = -\alpha\beta$$

***Tout quaternion A est de la forme :***

$$A = r_1 + r_2\alpha + r_3\beta + r_4\alpha\beta \in \mathbb{Q}[\alpha, \beta]$$

## CHAPITRE III :GROUPE DE MORDELL-WEIL

La description complète de l'anneau $End\,(E)$ a été déterminée par DEURING dans " Die Typen der Multiplikatorenringe elliptischer Funktionen korper- abh.Math.Sem. Hamburg14(1941) ,197-272.

Les automorphismes des Courbes Elliptiques forment des groupes $Aut\,(E)$ de structure spéciale .

**Proposition 8.** ***Soit une Courbe Elliptique*** $E/K$ ***. Alors son groupe*** $Aut\,(E)$ ***des automorphismes est un groupe fini d'ordre un diviseur de 24 égal à :***

2 ***si*** $j(E) \neq 0$, ***1728 ;***

4 ***si*** $j(E) = 1728$ ***et*** $carac(K) \neq 2, 3$ ***;***

6 ***si*** $j(E) = 0$ ***et*** $carac(K) \neq 2, 3$ ***;***

12 ***si*** $j(E) = 0 = 1728$ ***et*** $carac(K) = 3$ ***;***

24 ***si*** $j(E) = 0 = 1728$ ***et*** $carac(K) = 2$

Démonstration. Voire <The Arithmetic of elliptic curves> de Silverman.

□

Avec les groupes $Isom(E)$ et $Aut(E)$ nous obtenons des Twists de Courbes Elliptiques [15 ,x-pa 5]

**Définition 11.** ***un twist d'une Courbe Elliptique*** $E/K$ ***est une Courbe Elliptique*** $E_L$ ***définie sur*** $K$ ***et isomorphe sur une certaine extension galoisienne L de K .***

**Exemple.1**

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6 \in \mathbb{Q}\,[x, y] \qquad (1)$$

Soit une extension quadratique $L = \mathbb{Q}\left(\sqrt{d}\right)$ , $d$ sans facteur carré . Les automorphismes de L opèrent sur les corps $L$ et $L(E)$ (2) .

Prenons l'automorphisme d'équation $x = x'/d$ , $y = y'\sqrt{d}$ (3) .

Nous obtenons l'équation de la Courbe Elliptique twist de $E$ :

$$E : y^2 = x^3 + a_2dx^2 + a_4d^2x + a_6d^3 \in \mathbb{Q}\,[x, y] \qquad (4)\,.$$

Alors les discriminants satisfont : $\triangle\,(E\,(d)) = d^6\triangle\,(E) = \left(\sqrt{d}\right)^{12}\triangle\,(E)$ .

Il en résulte que la Courbe Elliptique E et son twist $E\,(d)$ sont isomorphes par :

$$x = u^2X\ ,\ y = u^3Y\ ,\ u = \sqrt{d}$$

**Exemple.2**

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 \in \mathbb{Q}[x, y]$$

Prenons l'extension $L = \mathbb{Q}\left(\sqrt{d}\right)$ pour twister $E$ :$x = X/4d$ , $y = Y/\sqrt{d}$ .

L'équation du twist de E est :

$$E(d) : Y^2 = X^3 + b_2dX^2 + 8b_4d^2X + 16b_6d^3 \in \mathbb{Q}[x, y] \qquad (4).$$

**6.Isogénies :**

**Définition 12.** ***Soit 2 Courbes Elliptiques*** $E/K$ ***et*** $E'/K$ ***de points à l'infini*** $O_E$ ***et*** $O_{E'}$ ***; une isogénie de*** $E$ ***sur*** $E'$ ***est un homomorphisme :***

$$\lambda : E(K) \to E'(K) , \lambda \neq 0$$

***qui satisfait les conditions :***

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

**Définition 13.**

(1) ***le noyau de*** $\lambda$ ***est l'image réciproque :***

$$\lambda^{-1}(E) = \{P \in E(K) : \lambda(P) = O_{E'}\}$$

(2) ***l'ordre de ce noyau est le degré de l'isogénie*** $\lambda$ ***.***

A chaque isogénie $\lambda$ est associée une isogénie duale :

**Définition 14.** ***l'isogénie duale d'une isogénie de degré*** $d$ ***:***

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

***est l'homomorphisme de groupes :*** $\hat{\lambda} : E'(K) \to E(K)$ ***qui satisfait les 2 composées .***

$\lambda\hat{\lambda}$ est la multiplication par $d$ sur le groupe $E'(K)$

$\hat{\lambda}\lambda$ est la multiplication par $d$ sur le groupe $E(K)$

**Proposition 8.** ***Soit 2 isogénies de Courbes Elliptiques*** $\lambda : E(K) \to E'(K)$ ***et*** $\psi : E'(K) \to E_1(K)$ ***; alors :***

***1)les isogénies duales satisfont :***

$$\psi\lambda : E(K) \to E_1(K) , \; et \; \widehat{(\psi\lambda)} = \widehat{\lambda}\widehat{\psi}$$

***2)*** $deg(\lambda) = deg\left(\widehat{\lambda}\right)$ , $deg(\psi) = deg\left(\widehat{\psi}\right)$ , $deg(\psi\lambda) = deg\psi deg\lambda$ ,

## CHAPITRE III :GROUPE DE MORDELL-WEIL

Un bon exemple d'isogénie est la multiplication par un entier naturel $m > 1$ .

**Proposition 9.** ***Soit un entier naturel*** $m$ ***premier à*** $carac(K)$ ***et une Courbe Elliptique*** $E/K$ ***, alors la multiplication*** $t_m : E(K) \rightarrow E(K)$ ***de valeur*** $t_m(P) = mP$ ***est une isogénie de Courbe Elliptique de degré*** $m^2$ ***.***

*Preuve* . avec la théorie des Courbes Elliptiques sur le corps $\mathbb{C}$ des nombres complexes .□

Signalons l'algorithme de Velu pour le calcul des isogénies (CRAS-Paris -26juillet 1971-238-241)

"Isogénies entre courbes Elliptiques :

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

est isogène à :

$$E' : y^2 + xy + y = x^3 - x^2 - 213x - 1257 \in \mathbb{Q}[x, y]$$

# CHAPITRE IV :RANG DES COURBES ELLIPTIQUES

## 1.Hauteurs et Descente infinie :

Pour démontrer que le groupe de Mordell-Weil $E(K)$ d'une Courbe Elliptique est de type fini ,les spécialistes ont utilisé une procédure de descente infinie et des fonctions particulières :les hauteurs sur un groupe abélien .

**Définition 1.** ***Une hauteur sur un groupe abélien*** $A$ ***est une fonction*** $h$ ***sur*** $A$ ***, à valeurs réelles positives :***

$$h : A \to \mathbb{R}_+$$

***qui satisfait les 3 axiomes :***

$(haut_1)$ ***à tout point*** $P_1$ ***de*** $A$ ***, on peut associer une constante*** $C_1 = C_1(P + P_1)$ ***qui satisfait l'inégalité :***

$$h(P + P_1) \leqslant 2h(P) + C_1 \text{ pour tout point } P \text{ de } A$$

$(haut_2)$ ***il existe un entier rationnel*** $m \geqslant 2$ ***et une constante*** $C_2$ ***tels que :***

$$h(mP) \geqslant m^2 h(P) - C_2 \text{ pour tout point } P \text{ de } A$$

$(haut_3)$ ***tout ensemble de points*** $P$ ***de*** $A$ ***de hauteurs bornées est fini .***

**Définition 2.** ***la descente infinie est un algorithme qui a été utilisé pour la première fois par Fermat pour résoudre certains problèmes d'arithmétique .***

**Exemple.**

Montrons que le nombre algébrique $\sqrt{7}$ n'est pas rationnel .

Supposons le contraire :

$\sqrt{7}$ est un nombre rationnel ; alors $\sqrt{7} = a/b$ , avec les 2 entiers naturels $a$ et $b$ premiers entre eux . (1)

En élevant au carré les 2 membres nous obtenons : $7b^2 = a^2$ (2)

Par un théorème de divisibilité de Gauss , si un entier naturel A divise un produit BC de 2 entiers naturels , et si A et premier à B , alors A divise C (3)

Dans (1) , $a$ divise $7b^2$ et $a$ premier à $b$ (4)

Donc 7 divise $a$ : $a = 7a_1$

(1) et (4) impliquent : $b^2 = 7a_1^2$ (5)

Il en résulte que 7 divise $b^2$ , donc 7 divise $b$ (6)

soit $b = 7b_1$ (7)

Nous obtenons ainsi :

une suite "infinie" d'entiers $a_1, a_2...., a_n, ...$ divisibles par 7 (8)

une suite "infinie" d'entiers $b_1, b_2...., b_n, ...$ divisibles par 7 (9)

(8) et (9) impliquent " $a$ et $b$ divisibles par 7 " contraire à (1)

Donc la supposition " $\sqrt{7}$ est un nombre rationnel " est absurde .

Cela prouve que $\sqrt{7}$ n'est pas rationnel .

**Proposition 1.** S*oit un groupe abélien A , et un entier naturel* $m \geqslant 2$ *tel que : le groupe quotient* $A/mA$ *soit fini .Alors le groupe A est de type fini* .

*Preuve* . Dans le groupe quotient $A/mA$ nous choisissons représentants :

$T_1, ....., T_S$.....(1)

Nous construisons une suite infinie récurrente de points

$P_1, ....., .....P_m, .....$deA par les formules si dessous :

Nous commençons par la relation :

$P = mP_I + T_{i,I}$

Nous poursuivons l'opération avec deux points $P_i$ et $P_{i+1}$

pour $i = 1, 2, ....$

$P_1 = mP_2 + T_{i,2}$

$P_2 = mP_3 + T_{i,3}$

.....

$P_j = mP_{j+1} + T_{i,j+1}$.....(2)

$P_{n-1} = mP_n + T_{i,n}$

où les points $T_{i,1}$,$T_{i,2}$ ,..... sont les représentants $T_1, ...T_S$.

Nous utilisons les axiomes d'une hauteur $h : A \to \mathbb{R}^+$

par l'axiome $(h_2)$des hauteurs , nous obtenons

avec (2) , l'inégalité :

$h(P_j) \leqslant \frac{1}{m^2} \{h(mP_j) + c_1\}$ .....(4)

dans la formule (2) de $P_{j-1}$ , nous calculons le point

$mP_j = P_{j-1} - T_{i,j}$.....(5)

La hauteur des deux membres implique la relation :

$h(mP_j) = h(P_{j-1} - T_{ij})$ .....(6)

(4) et (5) et (6) impliquent l'inégalité :

$h(P_j) \leqslant \frac{1}{m^2}(2h(P_{j-1}) + C_3$.....(8)

où $C_3$est un constante dépondant de $C_1$

les formules de récurrence (2) appliquées à (8) impliquent

l'inégalité :

$h(P_j) \leqslant (\frac{2}{m^2})^n h(P) + \left[\frac{1}{m^2} + \frac{2}{m^4} + \frac{4}{m^6} + ..... + \frac{2^{n-1}}{m^{2n}}\right] C_4$.....(9)

où$C_4$est un constante dépondant de $C_3$.

La somme du $2^{éme}$membre de (9) est le développement en série

de la fonction $\frac{1}{m^2-2} = \frac{1}{m^2} \cdot \frac{1}{1-\frac{2}{m^2}}$ il en résulte l'inégalité :

$h(P_n) \leqslant (\frac{2}{m^2})^n h(P) + \frac{C_4}{m^2-2}$.....(11)

L'hypothèse $m \geqslant 2$transforme (11) en l'inégalité

$h(P_n) \leqslant 2^{-n} h(P) + \frac{C_4}{2}$.....(12)

Pour n assez grand (12) devient :

$h(P_n) \leqslant 1 + \frac{C_4}{2}$.....(13)

donc par (13), la suite $P_{1,}, ....., P_n$ est de hauteur bornée ,par

l'axiome $(h_3)$ des hauteurs , cette suite de points est finie , nous

en déduisons que tout point $P$ du groupe abélien $A$ est une

combinaison $\mathbb{Z}-$linéaire finie de points de $A$ de la forme :

$P = n_1 T_1 + .....n_s T_s + \sum_d U_j N_j$

où les points $N_j$ sont de hauteur bornée par (13) .

donc le groupe abélien $A$ est de type fini $\square$ .

Appliquons ce résultat au groupe abélien additif $E(K)$ de Mordell- Weil des Courbes Elliptiques .

**Proposition 2.** ***Le groupe de Mordell –Weil*** $E(K)$ ***des Courbes Elliptiques est de type fini .***

## CHAPITRE IV :RANG DES COURBES ELLIPTIQUES

*Preuve* . Soit une Courbe Elliptique $E/K$ , son groupe $E(K)$ de Mordell- Weil .

Le groupe quotient $E(K)/2E(K)$ admet $r$ générateurs $P_1, ....., P_r$ d'ordre infini .

Le groupe de torsion $T(E)$ est fini ; il admet $s$ générateurs $T_1, ....., T_S$ qui son d'ordre fini .

La proposition 1 implique que tout point P de E est une $\mathbb{Z}-$combinaison linéaire des de ces générateurs :

$$P = m_1T_1 + .....m_sT_s + n_1P_1 + .....n_rP_r \qquad \square.$$

Nous constatons que la structure du groupe abélien $E(K)$ est de même type que celle du groupe $U(L)$ des unités des corps de nombres algébriques $L = \mathbb{Q}(\theta)$ .

**Théorème des unités de Dirichlet**

***Soit un corps de nombres algébriques L de degré*** $n = [L : \mathbb{Q}]$ **,** $n = a + 2b$ **,** $a$ ***conjugués réels*** $\sigma(L) \subset \mathbb{R}$ ***et*** $b$ ***paires de conjugués complexes*** $\sigma(L) \subset \mathbb{C}$ ***. Alors les unités de*** $L$ ***forment un groupe abélien*** $U(L)$ ***,multiplicatif ,de type fini .***

$U(L)$ ***isomorphe à*** $C(L) \times \mathbb{Z}^r$

***avec*** $C(L)$ ***:groupe des racines de l'unité contenues dans L .***

***et*** $r = a + b - 1$ $=$ ***rang du groupe des unités .***

Tout systèmes des générateurs e ce groupe $U(L)$ est un système d'unités fondamentales :$u_1, u_2, ..., u_r$ de L .

Toute unité $u$ de L est un produit de la forme :

$$u = \pm u_1^{n_1}u_2^{n_2}...u_r^{n_r} \ , n_i \in \mathbb{N}$$

Une unité de L est un élément $u$ de norme $N_{L/\mathbb{Q}}u = \pm 1$ .

Il en résulte que $-u, 1/u$ et $-1/u$ sont des unités de L .

Dans l'isomorphisme de groupes abéliens $E(K) \simeq T(E) \times \mathbb{Z}^r$ , $r = r(E)$ est le rang arithmétique des Courbes Elliptiques.

La détermination de $r(E)$ n'est pas simple comme celle du rang des unités $U(L)$ de L .

Pour $r(E)$ les spécialistes utilisent des hauteurs sur les Courbes Elliptiques , Il existe plusieurs types de hauteurs .

***1.Hauteur sur la corps*** $\mathbb{Q}$ ***des nombres rationnels :***

$$h_1 : \mathbb{Q} \to \mathbb{R}_+$$

de valeur : $h(\frac{a}{b}) = max\{|a|, |b|\}$ , $|a| = max\{a, -a\}$

## CHAPITRE IV :RANG DES COURBES ELLIPTIQUES

***1.Hauteur de Weil :***

$$h_w : E(K) \to \mathbb{R}$$

de valeurs :

$$h_w(p) = log\, max\left\{v\left(a\right), v\left(b\right)\right\}, x = a/b$$

$p = (x, y)$ , v= valuation du corps K

$$h_w(O_E) = 0$$

Cette hauteur de Weil est une fonction quasi quadratique .

Elle satisfait les relations : $f(-p) = f(p)$ et la loi du parallélogramme : $f(p+r) + f(p-r) = 2f(p) + 2f(r)$ .

***3.Hauteur de Neron -Tate :***

Elle est liée à la hauteur de Weil et à une fonction $f$ :

$$\tilde{h} : E(K) \to \mathbb{R}_+$$

de valeur $\tilde{h}(p) = \frac{1}{degf} \lim\limits_{n\to\infty} 4^{-n} h_w f(2^n p)$

où $f : K(E) \to \mathbb{R}$ , $f\left(-t\right) = f\left(t\right)$ .

***4.Hauteurs locales :***

La hauteur de Néron-Tate n'est pas pratique pour les calculs . Il lui est préféré les hauteurs locales .

Ce sont des hauteurs qui dépendent des valuations du corps K de base des Courbes Elliptiques en une valuation $v$ non archimédienne discrète .

hauteur locale :

$$\lambda_v : E\left(K_v\right) - O_E \to \mathbb{R}$$

$K_v$ =corps valué en v .

**Proposition 3.** ***Il existe une hauteur locale en une valuation v , unique , sur les Courbes Elliptiques*** $E/K$ ***, qui satisfait les 4 propriétés :***

***1) la hauteur locale*** $\lambda_v$ ***est continue pour la topologie v-adique de*** $E\left(K\right)$ ***et pour la topologie usuelle du corps*** $\mathbb{R}$ ***des nombres réels***

***2) Elle satisfait la relation***

$$\lambda_v\left(2P\right) = 4\lambda_v\left(P\right) + 2v\left(2y + a_1x + a_3\right) - v\left(\triangle\left(E\right)\right)/4$$

***pour tout point*** $P$ ***de*** $E\left(K\right)$ , $P = (x, y)$ , $2P \neq O_E$ ***;***

***3)*** $\lim\limits_{p\to O_E} \left(\lambda_v\left(p\right) + v\left(x\right)/2\right)$ ***existe ;***

***4)*** $\lambda_v$ ***satisfait la loi du parallélogramme :***

$$\lambda_v(P+R) + \lambda_v(P-R) = 2\lambda_v(P) + 2\lambda_v(R) + v\left(x_P - x_R\right) - v\left(\triangle\left(E\right)\right)/6$$

***pour tout point*** $P$ , $R$ , $P \pm R \neq O_E$ .

*Preuve* . [15] $\square$ .

Les hauteurs locales $\lambda_v$ sont liées à la hauteur de Néron-Tate .

**Proposition 3.** ***Soit une Courbe Elliptique*** $E/K$ , ***une valuation non archimedienne discrète du corps K et le groupe*** $E(K)$ ***de Mordell –Weil de E . Alors : la hauteur*** $\tilde{h}$ ***de Néron-Tate et la hauteur locale*** $\lambda_v$ ***sur le corps*** $K_v$ ***satisfont la relation :***

$$\tilde{h}(P) = \frac{1}{n} \sum_{v \in V(K)} n_v \lambda_v (P)$$

$V(K) =$***ensemble des*** $v$ , $P \neq O_E$ , $n_v = [K_v : \mathbb{Q}_v] =$ ***degré locale de K en v .***

*Preuve* . [15] , Appendix c-Theorem 18-2 $\square$.

**3-Conjecture de Birch et Swinerton-Dyer :**

Cette conjecture, introduit la notion de rang analytique des Courbes Elliptiques . Elle est liée à la série de Dirichlet-Hasse $L(E,s)$ des Courbes Elliptiques .

**Définition 3.** ***La série de Dirichlet-Hasse des Courbes Elliptiques*** $E/\mathbb{Q}$ ***est la fonction*** $L(E,s)$ ***de la variable complexe*** $s$ ***:***

$$L(E,s) = \prod_p \left(1 - t_p p^{-s}\right)^{-1} . \prod_q \left(1 - t_q q^{-s} + q^{1-2s}\right)^{-1}$$

***où*** $p =$***diviseurs premiers du discriminant*** $\triangle(E)$ .

$q =$***nombres premiers qui ne divise pas*** $\triangle(E)$ .

***nombres de points de la courbe réduite*** $E(p)$ ***modulo*** $p$ .

$t_p = 1 + p - A(p)$ .

**Proposition 4.** ***La série*** $L(E,s)$ ***associée aux Courbes Elliptiques*** $E/\mathbb{Q}$ ***admet un développement en série de Dirichlet de la forme :***

$$L(E,s) = \sum_{n \geq 1} c_n n^{-s} \; n = entier\ naturel$$

$c_p = t_p$ ***pour les nombres naturels*** $n = p$ ***premiers .***

***2) si*** $p$ ***divise*** $\triangle(E)$ ***alors E a mauvaise réduction en*** $p$ ;$t_p = 1$ ***ou*** $-1$ ***suivant que la cubique réduite*** $E(p)$ ***sur*** $\mathbb{F}_p$ ***a un noeud où la tangente à E est rationnelle ou quadratique et*** $t_p = 0$ ***si*** $E(p)$ ***admet un point de rebroussement .***

***3) le produit eulérien*** $L(E,s)$ ***converge dans le domaine*** $Re(s) > \frac{3}{2}$ **.**

*Preuve* . [15] $\square$ .

**Conjecture B-S-D :**

La série $L(E,s)$ de Dirichlet-Hasse des Courbes Elliptiques $E/\mathbb{Q}$ admet un zéro en $s=1$ d'ordre égal au rang $r$ de $E$ :

**Définition 4 .*Le rang*** $r$ ***de cette conjecture est le rang analytique*** $r_{ana}(E)$ ***des Courbes Elliptiques*** $E/\mathbb{Q}$ .

Énoncé de la conjecture :

$$\lim_{s\to 1} = \frac{L(E,s)}{(s-1)^r} = \Omega.card\,(Shaf\,(E/\mathbb{Q}))\,.R\,(E/\mathbb{Q})\,\frac{1}{card\,T\,(E)^2}\prod_p c_p.$$

où $\Omega = \int_{E(\mathbb{R})} \frac{dx}{2y+a_{1x}+a3}$

$Shaf\,(E/\mathbb{Q})$ =groupe de Shafarevich-Tate de $E/\mathbb{Q}$ ;

$R\,(E/\mathbb{Q})$ =régulateur de $E/\mathbb{Q}$ ;

$T(E)$ = groupe de torsion de E ;

**Définition 5.*Le régulateur d'une Courbe Elliptique*** $E/K$ ***est égal au déterminant***

$$R(E/K) = det(< R_i, R_j >), 1 \le i \le r,\ 1 \le j \le r$$

***pour la forme bilinéaire de Néron-Tate***

$$<,>: E\,(K) \times E\,(K) \to \mathbb{R}$$

***de valeur***

$$< P, R >= \tilde{h}(P+R) - \tilde{h}(P) - \tilde{h}(R)$$

$r =$ ***le rang*** $E\,(K)$ **,** $R(E/K) = 1$ ***si*** $r = 0$ **.**

Le groupe de Shafarevich-Tate est le sous groupe du groupe $WC\,(E/K)$ de Châtlet-Weil : $Shaf\,(E/K) = ker\left\{WC\,(E/K) \to \prod_{v\in Val(K)} WC\,(E/K_v)\right\}$ d'après [15] X-page4.

Cette conjecture de Birch et Swinnerton-Dyer a été vérifiée par Gross et Zagier dans "On the conjecter B-S-D for an Elliptic curve of rank 3" dans Math of Comput .vol . 44(1985) p.473-481.

## CHAPITRE IV :RANG DES COURBES ELLIPTIQUES

Il s'agit de la Courbe Elliptique $E/\mathbb{Q}$ d'équation de Weierstrass :

$$E : y^2 = 4x^3 - 28x + 25 \in \mathbb{Q}[x, y] \qquad (1)$$

Calcul des invariants :

$$\triangle(E) = N(E) = 5077 \qquad (2)$$

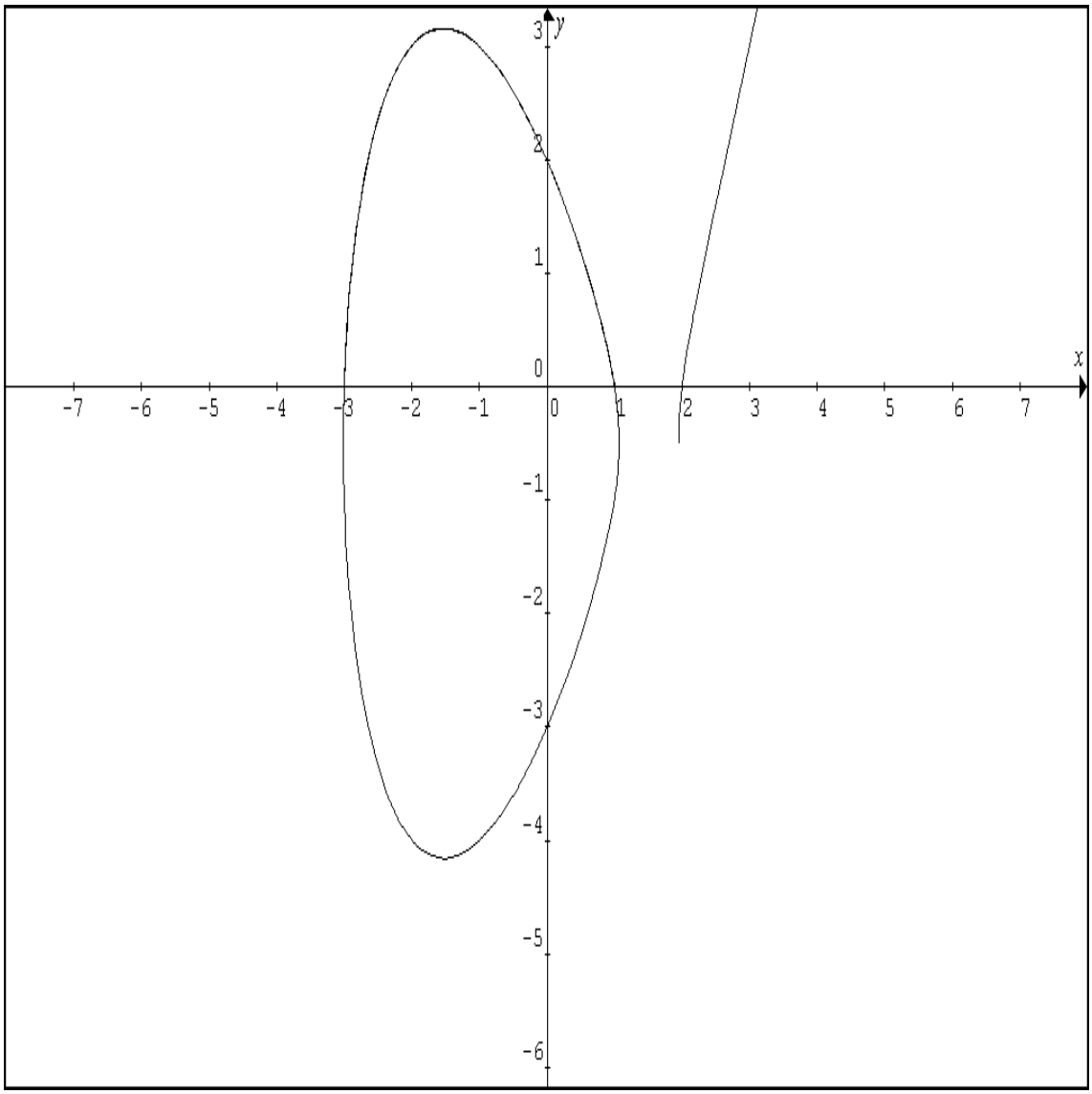
Changement de variables :

$$x = X; y = 2Y + 1 \qquad (3)$$

(1) devient :

$$E_1 : Y^2 + Y = X^3 - 7X + 6 \in \mathbb{Q}[X, Y] \qquad (4)$$

Calcul des points d'intersection de E et Ox : $p_1 = (-3, 0)$ ; $p_2 = (1, 0)$ ; $p_3 = (2, 0)$ ; $p_4 = (0, -2)$ ; $p_5 = (0, 3)$ (5)



## CHAPITRE IV :RANG DES COURBES ELLIPTIQUES

Points symétrique :

$-p_1 = (-3,-1)\,;\, -p_2 = (1,-1)\,;\, p_3 = (2,-1)$ (7) ;

Pour obtenir le rang $r\,(E)$ les 2 auteurs utilisent les réductions modulo $p$ :

$A\,(3)$ =7 points P sur $E(3) \in \mathbb{F}_3\,[x,y]$

$A\,(3)$ =10 points P sur $E(7) \in \mathbb{F}_7\,[x,y]$ (8)

Les 3 points $p_1$ , $p_2$ , $p_3$ engendrent le groupe $E(\mathbb{Q})$ (9)

Il en résulte $r(E) = 3$ (10)

Le rang analytique est calculé avec la série :

$$L\,(E,s) = (1+5077)^{-1} \prod_{p \nmid 5077} \left(1 - t_p p^{-s} + p^{1-2s}\right)^{-1}$$

A la limite :

$$\lim_{s \to 1} = \frac{L\,(E,s)}{(s-1)^3} = 1.731 \qquad (11)$$

Les auteurs en déduisent l'égalité :

$$r(E) = rang\, analytique = 3 \qquad (12)$$

**Courbes Elliptiques de Rang 1 :**

Plusieurs méthodes ont été utilisées :

1) Dans [2] ,Brumer et Kramer considèrent la suite exacte de groupes abéliens .

$$0 \to E(K)/2E(K) \to H^1\,(G; E\,(K_{alg}))$$

où $H^1$ est le $1^{er}$ groupe de cohomologie de groupe de Galois $G = G\,(K_{alg}/K)$ , $K_{alg} = clôture\, algébrique\, de\, K$ .

Le rang de E est calculé avec la formule .

$$r(E) = card\,(S\,(E)) - card\,(E\,(\mathbb{Q})\,[2]) - card\,(Shaf\,(E)\,[2])$$

où $S\,(E)$ = groupe de Selmer de E , $E\,(\mathbb{Q})\,[2]$=groupe de 2-torsion de E .

Avec la suite exacte de groupes :

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to S\,(E) \to Shaf\,(E) \to 0$$

Les 2 auteurs ont trouvé 3 Courbes Elliptiques :

$E_1 : y^2 + xy + y = x^3 - x^2 - 9x - 8$ de rang $r(E_1) = 0\,;$

$E_2 : y^2 + 9xy + y = x^3 - 7x^2$ de rang $r(E_2) = 1\,;$

$E_3 : y^2 + 15xy + y = x^3 - 7x^2$ de rang $r(E_3) = 0\,;$

## CHAPITRE IV :RANG DES COURBES ELLIPTIQUES

2) A.Bremmer et D.A .Buell ,dans Math of Comput .61-n° 203.(1993) ont étudié les Courbes Elliptiques :

$$E_p : y^2 = x\left(x^2 + p\right) \in \mathbb{Q}\left[x, y\right], p \; premier$$

Avec un algorithme , pour les $p < 20000$ , ils ont trouvé 3 nombres premiers intéressants : $p = 3917$ , 4157 et 4957 .

Pour $p = 3917$ , le générateur $p = (x, y)$ du groupe $E(\mathbb{Q})$ a des coordonnées rationnelles $x = \frac{a}{b}$ , $y = \frac{c}{d}$ , $a$ =entier naturel de 71 chiffres , $b$ =entier naturel de 70 chiffres , $c$ =entier naturel de 106 chiffres et $a$ =entier naturel de 164 chiffres ,

cet algorithme est exécuté avec un logiciel très performant

3)Silverman a étudié la Courbe Elliptique d'équation de Weierstrass :

$$E : x\left(x-2\right)\left(x-10\right) \in \mathbb{Q}\left[x, y\right]$$

Son discriminant est égal à : $\triangle(E) = 2^{14}.5^2$

Il en résulte que E a mauvaise réduction en $p = 2$ et $p = 5$ .

Au moyen d'une descente via une 2-isogénie , Silverman obtient le résultat :

$E(\mathbb{Q})$ est isomorphe au groupe somme directe :

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$$

Il en résulte : le rang de cette Courbe Elliptique est égal à : $r(E) = 1$

**Conclusion :**

Nous constatons que la détermination des rangs de Courbes Elliptiques est difficile parce qu'il n'y a pas de formules explicites comme dans le cas du rang des groupes U(L) des unité des corps de nombres algébriques .

Les méthodes que nous avons décrites utilisent un important bagage mathématique : torsion des groupes de Mordell-Weil , endomorphismes ,automorphisme , isogénie , corps finis , congruances , série L(E,s) de Dirichlet , valuations des corps , géométrie algébrique , cohomologie des groupes , Courbes algébriques planes ...

Après avoir soutenu mon magister , je compte poursuivre mes activités de recherche en vue d'un doctorat . Plusieurs directions m'intéressent : les groupes de Châtelet-Weil et ses sous groupes , les groupes de cohomologie et leurs applications , les Courbes Elliptiques à multiplication complexe et la cryptographie.

Cela exigera des conditions favorables , des contactes avec des spécialistes , des participations à des rencontres scientifiques et des colloques de la spécialité .

RÉFÉRENCES :

[1] B, BIRCH and H.P.F.SWINERTON-DYER : Notes on Elliptic Curves 1and2 -jour.Reine Angw .Math ,212 (1963) 7-25 and 218(1965)79-108

[2] Armand BRUMER and Kenneth KRAMER : The Rank of Elliptic Curves _Duke Mathematical Journal -Vol44n°4(dec1977)p715-743

[3] Cassels, J.W.S., Diophantine equations with special reference to elliptic curves, J. London Math. Soc. 41 (1966), 193–291.

[4] CREMONA,J,E :Algorithm for Modular Elliptic Curves 2éme Ed .Cambridge University Press (1998) London

[5] Robin HARTSHORNE, Algebraic Geometry,Graduate Texts in Mathematics n°52 Springer-Verlag, 1983.

[6] Dale HUSEM'OLLER Elliptic curves Geometry,Graduate Texts in Mathematics n°111 Springer-Verlag, 1987

[7] S.KIHARA :On infinite family of Elliptic Curves with rank$\geq$ 14 over $\mathbb{Q}$ -Proc Japan Acad-Ser .A.MathematicsScie n°73 (1997)p2-32

[8] ANTHONY .W. Knapp Elliptic Curves, n°40 in Mathematical Notes Princeton University Press -New Jersey.U.S.A(1992)

[9] N.KOBLITZ, Introduction to Elliptic Curves and Modular Forms,$2^{end}$ Ed Graduate Texts in Mathematics n° 97, (1984).

[10] D. S. KUBERT – « Universal bounds on the torsion of elliptic curves », Proc. London Math. Soc. (3) 33 (1976), no. 2, p. 193–237.

[11] Serge LANG Algebra ;revised third edition ;Graduate Texts in Mathematics n° 211,Springer.

[12] Serge LANG ;Elliptic Curves : Diophantine Analysis, Springer-Verlag, 1978.

[13] J.-F. MESTRE ;Rang de certaines familles de Courbes Elliptiques d'invarint donné-Comptes Rondus de l'Académie des Sciences Paris Mathématiques n° 327, (1998)p763-764.

[14] J.S. MILNE,Elliptic Curves-Course Notes University of Michigam-USA-(1996).

[15] D.E.PENNEY ;C. POMERANCE Asearch for Elliptic Curves with large rank Mathematical of computation 28(1974)p851-853.

[16] KARL RUBIN and ALICE SILVERBERG : Ranks of Elliptic Curves Bulletin (new series) of the American Mathematical Society Volume 39,( 2002) p455-474

[17] I-R-SHAFAREVICH :Basic Algebraic Geometry Springer-,( 1977)

[18] Goro SHIMURA :Introductin to the Arithmetic Theory of Automorphic Functions Princeton University Press U.S.A , (1976).

[19] J. H. SILVERMAN,The arithmetic of Elliptic Curves, Graduate Texts in Mathematicsn° 106, Springer- Verlag, New York,( 1986).

[20] André WEIL :courbes Algébrique et Variétés Abélinnes Hermann-Paris (1974).

[21] Mohamed- ZITOUNI :Courbes Elliptiques ;Arithmétique -Géometrie-Algorithmique-O.P.U-Alger-(2007).