N° d'ordre : / 2007 – 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

Thèse présentée pour l'obtention du diplôme de Magister

En : MATHEMATIQUES
Spécialité : **Algèbre et Théorie des Nombres**

Par M^me^ : AZIZI Hanane

LES COURBES ELLIPTIQUES SEMI STABLES SUR LE CORPS Q DES RATIONNELS

Soutenue publiquement le : .15 / 07/ 2007, devant le jury composé de :

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

SOMMAIRE

INTRODUCTION

CHAPITRE I VARIETES ALGEBRIQUES ABELIENNES

1. Espaces algébriques affines.....1
2. Topologie de Zariski 2
3. Variétés algébriques affines.....3
4. Variétés algébriques projectives.....4
5. Variétés algébriques abéliennes.....5
6. Diviseurs d'une variété algébrique et diviseurs d'une courbe.....6
7. Exemples…….....…….....8

CHAPITRE II ARITHMETIQUE DES COURBES ELLIPTIQUES

1. Courbes algébriques planes: degré, singularité, genre….....9
2. Cubiques de Weierstrass ……..……..…….....13
3. Invariants des cubiques de Weierstrass ….……14
4. Résultant de 2 polynômes. Discriminant d'un polynôme …..…….15
5. Classification des cubiques de Weierstrass avec $\Delta(E)$ et $c_4(E)$……..18
6. Exemples…..…….24

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

1- Construction du groupe abélien *E(K)*…….....28
2- Coordonnées des points $-P$, P_1+P_2 , $2P$, mP…….....29
3- Points d'ordre fini d'une courbe elliptique - Groupe de torsion.....36
4- Théorème de Mordell-Weil d'une Courbe Elliptique.....38
5- Rang d'une courbe elliptique.....42
6- Exemples.....43

CHAPITRE IV ISOMORPHISME - AUTOMORPHISME - ISOGENIE TWISTS

1- Isomorphismes de courbes elliptiques..…….....44
2- Automorphismes d'une courbe elliptique 50
3- Isogénies et endomorphismes de courbes elliptiques
algorithme de Velu 53
4- Twists de courbes elliptiques…….....58
5- Exemples.....……..…….…….... 60

CHAPITRE V REDUCTION DES COURBES ELLIPTIQUES

1- Valuations d'un corps.....61
2- Réduction d'une courbe elliptique.....66
3- Courbes semi –stables, exemples numériques.....68

REFERENCES.. 70

INTRODUCTION

Ma thèse porte sur les courbes elliptiques semi stables.

Les courbes elliptiques sont liées aux domaines des variétés Algébriques, au domaine de la théorie des nombres et aux domaines des courbes Algébriques planes.

Dans le Chapitre I, j'ai décrit quelques propriétés des variétés affines, des variétés projectives et des variétés abéliennes.

Une courbe elliptique a une structure de variété abélienne de dimension un ; ces variétés munies de la topologie de Zariski deviennent des espaces topologiques.

Dans le Chapitre II, j'ai étudie les courbes algébriques planes : degré singularité, genre. Les courbes algébriques sont liées aux courbes elliptiques sont les cubiques de Weierstrass. J'ai utilisé des changements linéaires de variables pour introduire plusieurs invariants de ces cubiques (c_4 , $\Delta(E), j(E), w(E), \ldots$) . J'ai utilisé la théorie du résultant de 2 polynôme f , $g \in IR[x]$ pour obtenir une relation entre les discriminants *Dis (f)* d'un polynôme et $\Delta(E)$ d'une cubique de Weierstrass .

Cela m'a permis de classifier ces cubiques de Weierstrass en 4 classes .

Dans le Chapitre III et IV j'ai déterminé une loi de groupe abélien sur l'ensemble *E(K)* des points *K*- rationnels de *E* .Avec la règle géométrique de 3 points colinéaire d'une courbe elliptique .

J'ai obtenu les formules des coordonnées des points $-P$, $P_1 + P_2$ et $2P$.

J'ai ensuite établi les propriétés de quelques homomorphismes de Courbes Elliptiques : Isomorphismes, Automorphismes, Endomorphismes, Isogénies, Twists.

Dans le chapitre V, j'ai décrit la théorie des Valuations d'un corps de nombres, les valuations *p*- adiques qui sont des valuations non archimédiennes fournissent des réductions des Courbes Elliptiques, réductions stables, réductions semi stables seulement .

J'ai illustré chaque chapitre de plusieurs figures et de plusieurs exemples.

CHAPITRE I : VARIETES ALGEBRIQUES ABELIENNES

Les Variétés Abéliennes sont du domaine de la Géométrie Algébrique. Parmi les ouvrages de Géométrie Algébrique, nous avons choisi ceux de **R.Hartshorne[3]** et de **I.R.Shafarevich [2]**.
Nous décrivons les espaces affines, les espaces projectifs, les variétés affines, les variétés projectives, les variétés abéliennes, et les diviseurs d'une variété et d'une courbe algébrique plane.

1- Espaces algébriques affines

Un tel espace est formé d'éléments d'un corps commutatif K algébriquement clos ou non.

Définition 1:

Un n-espace affine est l'ensemble des n-uples $a = (a_1,..., a_n)$ d'éléments a_i d'un corps K :

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

L'élément $a =(a_1,..., a_n)$ est un point de l'espace $IA^n(K)$ à n coordonnées $a_1,..., a_n$ dans le corps K .

A chaque espace affine $IA^n(K)$, nous associons l'anneau $K[X_1,...Xn]$ des polynômes f à n indéterminées $X_1,...X_n$.

$$f : IA^n(K) \rightarrow K \text{ de valeur } f(a) = f(a_1,..., a_n).$$

Dans tout espace affine il y a des ensembles particuliers.

Définition 2:

Un ensemble algébrique d'un n-espace affine $IA^n(K)$ est l'ensemble H des zéros d'une famille de polynômes $\{f_1 ,..., f_d\}$ de l'anneau $K[X_1,...X_n]$.

$$H = \{ a = (a_1,...,a_n) ; f_1(a) = f_2(a) =....= f_d(a) = 0 \} = H(f_1 ,. ..,f_d) \quad (2)$$

Exemple :

Soit l'ensemble :
$H= \{(x, y) \in \mathbb{C}^2; x^2-y^2 = 1\}$; le polynôme $x^2 - y^2=1$ admet une infinité de zéros

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

H est un sous ensemble algébrique dans l'espace affine $IA^2(\mathbb{C})$.

Les opérations sur les ensembles algébriques sont précisées par la.

Proposition 1:

1) ***La réunion et l'intersection de deux ensembles algébriques d'un n- espace affine IA^n (K) sont des ensembles algébriques.***
2) ***L'espace IA^n(K) et l' ensemble vide sont des ensembles algébriques.***

Preuve de 1) :
Soient deux ensembles $H_1=H(f_i)$ et $H_2=H(g_j)$ dans le n-espace affine $IA^n(K)$
Leur réunion $H_1 \cup H_2 = H(f_i, g_j)$ est l'ensemble des zéros des polynômes
f_i et g_i ; cet ensemble est donc algébrique.
Leur intersection $H_1 \cap H_2 = H(f_i, g_j)$ est l'ensemble des zéros communs des polynômes f_i et g_i .
Preuve de 2) :
Le polynôme $f = 1 + 0X_1 +...+ 0X_n$ n'admet pas de zéros. Il en résulte que l'ensemble vide est algébrique.
Le polynôme $f = 0X_1 +...+ 0X_n$ admet tous les éléments a du n-espace affine IA^n comme zéros, Il en résulte que le n-espace affine est algébrique.
□

Les sous ensembles algébriques du n- espace $IA^n(K)$ et leurs complémentaires jouent le rôle de fermés et d'ouverts d'une topologie .

2- Topologie de Zariski

Les ensembles algébriques permettent de déterminer une topologie spécifique.

Définition 3 :

La topologie de Zariski sur le n-espace affine $IA^n(K)$ est définie avec les ensembles algébriques comme sous ensembles fermés et leurs complémentaires comme des ouverts.
Donc l'espace affine peut être mun d'une structure d'espace topologique pour la topologie de Zariski.
Cette topologie n'est pas de Hausdorff. **[Hartshorne]**

La topologie de Zariski est associée à un espace topologique.

Définition 4 :

Dans un espace topologique X, un sous espace Y est irréductible s'il n'est pas la réunion de deux sous ensembles fermés non vides disjoints.
Il en résulte qu'un sous ensemble non irréductible est la réunion de composantes irréductibles.

Exemples :

1) Le sous ensemble $Y = H(x^4+x+1)$ de l'espace affine $IA^1(Q)$, sur le corps Q, est irréductible**.** Dans l'espace affine $IA^1(\mathbb{C})$, sur le corps $\mathbb{C}$, ce sous ensemble Y est réductible .
Il admet 4 composantes irréductibles correspondant à la factorisation du polynôme x^4+x+1.

2) L'espace affine $IA^1(K)$ est irréductible parce que ses sous-ensembles fermés sont finis .

3- Variétés algébriques affines

Une partie d'un espace affine devient une variété à certaines conditions.

Définitions 5 :

1) *une variété algébrique affine est un sous espace irréductible et fermépour la topologie de Zariski d'un espace affine* $IA^n(K)$.

2) *une variété algébrique quasi affine est un sous ensemble ouvert d'une variété affine.*

Exemples :

1) l'espace affine $IA^n(K)$ est une variété algébrique affine .

2) l'ensemble $X = \{ P = (x,y) ; y^2 = x^3 - 5x + 12 \}$ est une variété algébrique affine de l'espace $IA^2(\mathbb{C})$.

Dans un anneau commutatif, il y a des idéaux.

Définition 6 :

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

La dimension d'une variété algébrique affine est déterminée par la

Définition 7 :

Soit des chaînes croissantes de sous ensembles algébriques fermés d'un espace topologique $IA^n(K)$ *:*

$$H(T_0) \subset H(T_1) \subset \ldots \subset H(T_s) \qquad (H)$$

où les T_i *sont des familles de polynômes à n indéterminées et les* $H(T_i)$ *sont des familles irréductibles d'ensembles algébriques .*

Alors, la dimension d'une variété algébrique affine, ou quasi affine, X, est le maximum des indices s dans les chaînes (H) contenues dans X

Exemple :

$IA^n(K)$ est une variété *algébrique* affine de dimension n pour n = 1,2,3…

A chaque variété affine X nous associons le corps des fractions $K(X)$ de l'anneau $K[X]$. C'est le corps des fonctions rationnelles sur X.

Définition 8 :

Une fonction rationnelle $\varphi \in K(X)$ est régulière en un point $x \in X$ si elle se met sous la forme d'une fraction rationnelle :

$$\varphi = f/g \text{ où } f, g \in K[X] \text{ avec } g(x) \neq 0 .$$

4- Variétés algébriques projectives

Une variété projective $IP^n(K)$ est construite ă partir d'une variété algébrique affine $IA^{n+1}(K)$ et d'une relation d'équivalence .

Considérons la relation $\Re$ définie par :

$$x \Re y \quad si \quad et \quad seulement \quad si \quad \exists \lambda \neq 0 \quad tel \quad que \quad y = \lambda x \quad ;$$

$x = (x_1, x_2, \ldots, x_{n+1})$ et pour un élément non nul λ du corps K.

Alors cette relation $\Re$ satisfait les axiomes d'une relation d'équivalence.

Définition 9 :

L' espace projectif $IP^n(K)$ est le quotient de l'espace affine $IA^{n+1}(K)$ privé du point 0 par la relation $\Re$:

$IP^n(K) = IA^{n+1}(K) - (0,\ldots,0)) / \Re$.

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

Exemples :

1) l'espace projectif $IP^1(IR)$ est l'ensemble :

$IP^1(IR) = \{\lambda x , x = (x_1,x_2) ; x_i \in IR, \lambda \neq 0\} = \{$*classe des couples* $(x_1,x_2)\}$

Il existe un représentant canonique dans chaque classe.

2) l'espace projectif $IP^2(IR) = \{$*classe des triplets* $(x_1,x_2,x_3)\}$.

3) l'équation de Weierstrass d'une cubique C dans le plan projectif $IP^2(IR)$ est un polynôme homogène en x , y, z de degré 3:

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \in IP^2(IR)$$

Définition 10 :

Un sous ensemble X du n-espace projectif $IP^n(K)$ est algébrique, s'il existe un ensemble T de polynômes homogènes de l'anneau $K[X_1, \ldots, X_{n+1}]$ tel que :

$$Y = H(T) = \{ (x_0,x_1,\ldots,x_n) \in IP^n(K) ; P(x_0,x_1,\ldots,x_n) = 0 \text{ pour tout } P \in T \} .$$

Tout n-espace algébrique projectif $IP^n(K)$ peut être muni d'une structure de variété algébrique projective.

Définition 11 :

1) *Une variété algébrique projective est un sous ensemble algébrique irréductible d'un espace projectif* $IP^n(K)$ *muni de la topologie de Zariski .*

2) *Une variété algébrique quasi projective est un sous ensemble ouvert d'une variété algébrique projective.*

3) *La dimension d'une variété algébrique projective ou quasi - projective est égale à sa dimension en tant qu'espace topologique* pour la topologie de Zariski et telle que définie par la définition 7.

La notion d'idéal d'une variété algébrique affine se prolonge aux variétés projectives

Définition 12 :

l'idéal d'un sous ensemble Y de l'espace projectif $IP^n(K)$ *est engendré par l'ensemble des polynômes homogènes* $f \in K[X_1 \ldots, X_{n+1}]$ *qui s'annulent en tout point de Y*

$$I(Y) = \{ f \in K[X_1 \ldots, X_{n+1}] \; ; f(P) = 0 \text{ pour tout } P \in Y \subset \boldsymbol{IP^n}(\boldsymbol{K}) \}$$

5- Variétés algébriques abéliennes

Nous considérons des variétés algébriques munies d'une structure de groupe abélien.

Définition 13 : [Hartshorne]

Une variété de groupe est une variété algébrique Y munie d'une loi de groupe abélien :

$$\begin{aligned} \mu \; : \; Y \times Y &\longrightarrow Y \\ (a\,,\, b) &\longrightarrow a + b \quad . \end{aligned}$$

qui satisfait les 2 conditions :

1) *l'ensemble des points de Y est un groupe additif pour l'application* μ .

2) *l'application inverse* $\mu^{-1} : x \rightarrow x^{-1}$ *est un morphisme de variété Y.*

Exemples :

1) le groupe additif formé par la variété $Y = IA^1(K)$ et le morphisme $\mu(a\,,\, b) = a + b$ est une variété de groupe

2) une cubique plane X avec la loi de groupe abélien sur l'ensemble de ses points est une variété de groupe .

Une variété de groupe devient une variété algébrique abélienne par la :

Définition 14 :

Une variété algébrique abélienne est une variété de groupe munie d'une loi de groupe abélien ;elle est projective et irréductible.

Dans une variété algébrique abélienne il y a la notion de groupe abélien. Il en résulte que toute variété algébrique abélienne est commutative.

6- Diviseurs d'une variété algébrique et diviseurs d'une courbe

La notion de diviseur en Géométrie Algébrique permet de construire des diviseurs de plusieurs types pour l'étude des variétés algébriques, des courbes, des surfaces et des schémas algébriques.

Définition 15 : [Hartshorne]

Soit une variété algébrique irréductible X , et une famille de sous variétés C_i de X de codimension 1, alors un diviseur de X est une combinaison linéaire :

$$D = l_1(C_1) + l_2(C_2) + \ldots + l_n(C_n) \qquad (4)$$

à cœfficients l_i entiers rationnels.

Les opérations sur les variétés algébriques sont la réunion, l'intersection, le produit. Cela implique qu'un diviseur D n'est ni une variété algébrique, ni une sous variété . Il y a des diviseurs particuliers :

Définition 16 :

1) *lorsque tous les entiers l_i sont nuls,dans la formule (4), le diviseur D = 0 est nul.*

2) *lorsque tous les entiers l_i sont positifs, le diviseur D>0 est un diviseur positif.*

3) *lorsque $l_i = 1$ et tous les autres coefficients sont nuls, le diviseur $D = (C_i)$ est premier.*

L'ensemble des diviseurs d'une variété algébrique a une structure de groupe avec la :

Définition 17 :

L'ensemble Div(X) des diviseurs d'une variété algébrique X a une structure de groupe additif abélien pour la loi :

$$D' + D'' = (n'_1(C_1) + \ldots + n'_r(C_r)) + (n''_1(C_1) + \ldots + n''_r(C_r))$$
$$= n_1(C_1) + \ldots + n_r(C_r) \quad avec \quad n'_u + n''_u = n_u .$$

La structure de groupe est précisée par la

Proposition 2:

Dans l'ensemble des diviseurs Div(X) d'une variété* algébrique *X l'application :

$$Div(X) \times Div(X) \longrightarrow Div(X)$$
$$(D_1, D_2) \longrightarrow D_1 + D_2$$

est une loi de composition interne, cette loi est associative et commutative .
Elle admet comme élément neutre le diviseur D = 0 .

Chaque diviseur $D = \sum_{i=1}^{r} n_i(C_i)$ ***admet un symétrique*** $-D = \sum_{i=1}^{r} -n_i(C_i)$.

Donc l'ensemble Div(X) est un groupe additif abélien.

Preuve :
Soit l'ensemble *Div (X)* des diviseurs d'une variété algébrique X .
Considérons l'application :

$$f : Div(X) \times Div(X) \longrightarrow Div(X)$$

de valeur $f(D_1, D_2) = D_1 + D_2$.

La loi d'adition est une loi de composition interne pour 2 diviseurs :

$$D = \sum_{i=1}^{r} n_i(C_i) \text{ et } D' = \sum_{i=1}^{r} n_i'(C_i)$$

La somme est le diviseur $D + D' = \sum_{i=1}^{r} (n_i + n_i')(C_i)$.

Vérifions que cette application f satisfait les 4 axiomes d'un groupe additif abélien :

1)*Axiome de l'élément neutre :*

Pour $D = 0$, $\sum_{i=1}^{r} 0(C_i) = 0$, l'élément neutre de l'ensemble de diviseur est le diviseur $D = 0$.

2)*Axiome du symétrique :*

$D = \sum_{i=1}^{r} n_i(C_i)$, $-D = \sum_{i=1}^{r} (-n_i)(C_i)$ qui est le symétrique .

3)*Axiome de commutativité :*

$$D + D' = \sum_{i=1}^{r} n_i(C_i) + \sum_{i=1}^{r} n_i'(C_i) = \sum_{i=1}^{r} (n_i + n_i')(C_i) = \sum_{i=1}^{r} (n_i' + n_i)(C_i) = D' + D .$$

4)*Axiome d'associativité :*

il est vérifie par le calcul des diviseurs
$(D + D') + D''$ *et* $D + (D' + D'')$

□

La notion de diviseur d'une variété algébrique se prolonge aux fonctions rationnelles du corps *K (X)*

Définition 18 :

1)*Un diviseur* $D = (f)$ *d'une fonction* $f \in K(X)$ *est un diviseur principal*

$$(f) = \sum_{i=1}^{r} l_i(P_i) \qquad (5)$$

où les P_i *sont les zéros et les pôles de f et les entiers* l_i *sont des entiers rationnels égaux aux multiplicités des zéros et des pôles de la fonction f .*

2)*l'ensemble des diviseurs principaux de X, forme un sous groupe* $P(X)$ *du groupe des diviseurs* $Div(X)$.

Il en résulte que le groupe quotient $Div(X) / P(X)$ est un groupe abélien.

Définition 19 :

le groupe des classes de diviseurs d'une variété algébrique X est le groupe quotient :

$$Cl(X) = Div(X) / P(X) \qquad (6)$$

où $P(X)$ *désigne le sous groupe des diviseurs principaux de la variété algébrique .*

Les courbes algébriques planes admettent des diviseurs.

Définition 20 :

1) *Un diviseur d'une courbe C est une somme formelle :*

$$D = \sum_{P \in C} n_P.(P) \qquad (7)$$

où les entiers rationnels n_P *sont presque tous nuls .*

2) *Le groupe des diviseurs* $Div(C)$ *d'une courbe algébrique C est le groupe abélien libre, engendré par les points de C .*

Tout diviseur d'une courbe algébrique C possède un invariant qui est « le degré ».

Définition 21:

Le degré d'un diviseur D d'une courbe C est l'entier :

$$degD = \sum_{P \in C} n_p$$

Exemple :

Soit une courbe algébrique plane C d'équation affine :

$$f(x) = (x + a_1)^{-5}(x + a_2)^2 (x + a_3)^{-3} (x + a_4)^4 \qquad (8)$$

L'équation (8) implique les pôles ; $-a_1$ multiple d'ordre 5 , et $-a_3$ multiple d'ordre *3* et les zéros $-a_2$ multiple d'ordre 2 et $-a_4$ multiple d'ordre 4 .

Le diviseur de C est égal à :

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

où P_1, P_2, P_3, P_4 sont les points de la courbe C d'abscisses $-a_1, -a_2, -a_3, -a_4$ et les coefficients $-5, 2, -3, 4$ sont les ordres de multiplicité des zéros et des pôles de la courbe C .

La définition 23 implique la valeur du degré de C

deg C $= -5 + 2 - 3 + 4 = -2$. □

CHAPITRE II : ARITHMETIQUE DES COURBES ELLIPTIQUES

Les courbes elliptiques ont une structure de courbe algébrique plane sur un corps K commutatif que nous allons décrire

1- Courbes algébriques planes : degré, singularité, genre ;[1], [5], [7] , [17]

Définition 1 :

Une courbe algébrique plane est l'ensemble des points P = (x,y) qui satisfont un polynôme f(x,y)= 0 dans l'anneau K [x,y] .

Un polynôme $f(x,y) = \sum_{i,j\geq 0} d_{ij} x^i y^j$; a un degré égal au maximum *n* des sommes *i+j.*

C'est une somme de polynômes homogènes f_d de degré $n , n-1, \ldots, 0$.

$f(x,y) = f_n + f_{n-1} + \ldots + f_1 + f_0$.

Exemple : Figure 1

Pour n = 1 ;

$f(x,y)=d_1x + d_2y + d_3$ est l'équation d'une droite

Pour n = 2 ;

$f(x,y)=(x - a)^2 + (y - b)^2 - r^2$ est l'équation d'un cercle

$f(x,y)= y^2 - ax - b$ est l'équation d'une parabole

$f(x,y)=\frac{x^2}{a^2}+\frac{y^2}{b^2}-1=0$ est l'équation d'une ellipse pour $a \neq b \neq 0$ de centre (0,0)

$f(x,y)= \frac{x^2}{a^2}-\frac{y^2}{b^2}-1=0$ est l'équation d'une hyperbole pour $a \neq b \neq 0$.

Dans la géométrie dans l'espace euclidien IR^3 ,les intersections d'un cône par un plan sont des cercles, des ellipses ,des hyperboles ,des paraboles ,Les plans passant par le sommet du cône le coupent en 2 droites passant par le sommet ou le coupent au sommet seulement .

Pour n = 3 ;

$f(x,y) =(d_1x^3 + d_2x^2y + d_3xy^2 + d_4y^3)+(d_5x^2 + d_6xy + d_7y^2)+d_8x+d_9y+ d_{10}$

est l'équation d'une cubique plane.

Pour n = 4 ;

un polynôme de degré 4 est l'équation d'une quartique.

Pour n = 5 ;

un polynôme de degré 5 est l'équation d'une quintique.

Ces courbes sont irréductibles lorsque leur équation *f (x ,y)* est irréductible.

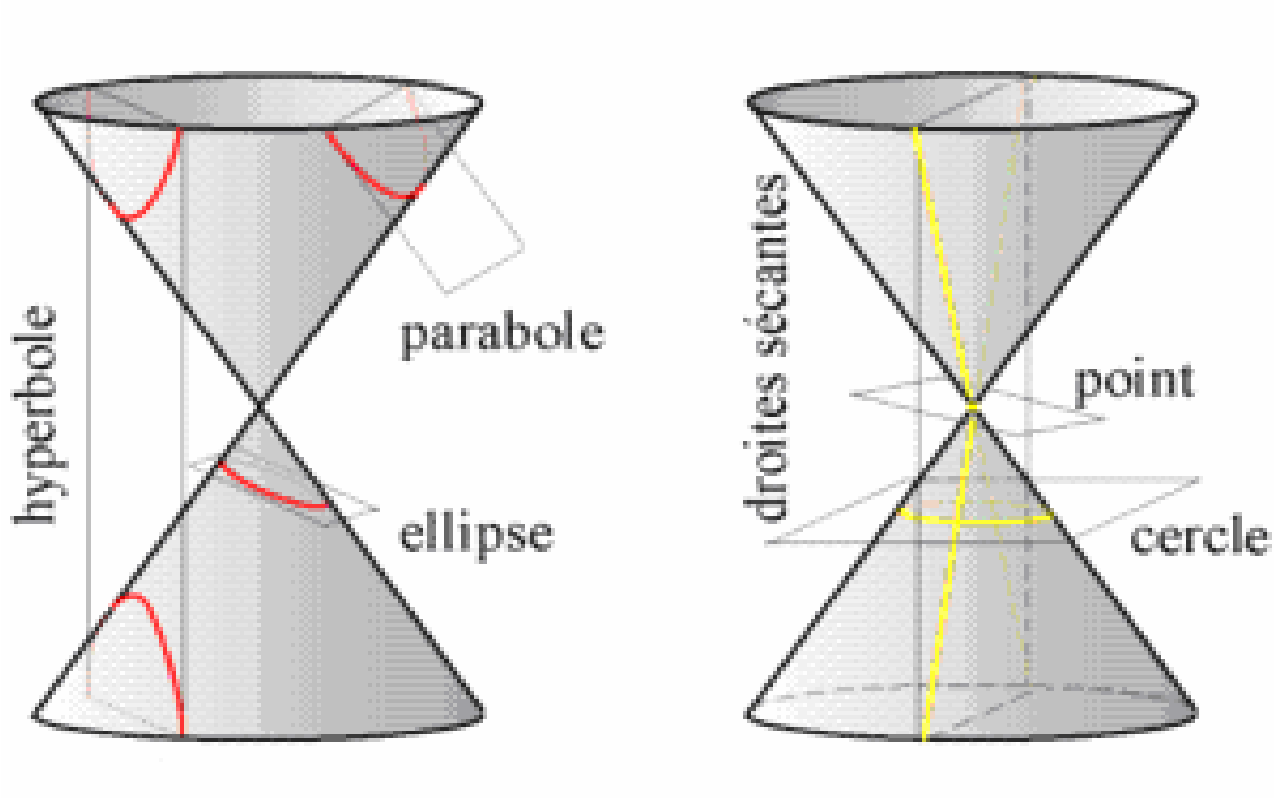

hyperbole
parabole
ellipse
droites sécantes
point
cercle

Figure 1

Une courbe algébrique C de degré n admet des points ordinaires et des points singuliers éventuels.

Définition 2 :

1) *Soit une courbe algébrique plane C d'équation :f(x,y) =0.*
Alors un point S = (x_s,y_s) de la courbe C est singulier si le système :

$$f(S) = f'_x(S) = f'_y(S) = 0$$

2) *Soit une courbe algébrique plane C d'équation :f(x,y) =0 de degré n. Un point S = (x_s,y_s) de C est singulier multiple d'ordre d si f(S) = 0 ; toutes les dérivées partielles de f d'ordre 1 à d sont nulles en S et une dérivée partielle d'ordre d+1 n'est pas nulle en S.*

Exemple :
Soit une courbe C d'équation $f(x,y) = x^4 - y^4$.
Les dérivées partielles sont égales à :

$$f'_x = 4x^3 \ , \ f''_{x^2} = 12x^2 \ , \ f^{(3)}_{x^3} = 24x \ , \ f^{(4)}_{x^4} = 24$$

$$f'_y = -4y^3 \ , \ f''_{y^2} = -12y^2 \ , \ f^{(3)}_{y^3} = -24y \ , \ f^{(4)}_{y^4} = -24$$

Les autres dérivées partielles sont nulles : $f''_{xy} = f''_{x^2y} = \ldots = 0$.

$$f(S) = f'_x(S) = \ldots = f^{(3)}_{x^3}(S) = f^{(3)}_{y^3}(S) = 0 \quad \text{et} \quad f^{(4)}_{x^4} = 24 \ .$$

Donc *S* est un point singulier multiple d'ordre *3* de la courbe *C*.

Le nombre s de points singuliers d'une courbe algébrique C de degré n permet de définir l'invariant genre de C.

Définition 3 :

Le genre d'une courbe algébrique C de degré n, qui possède s points singuliers est l'entier positif ou nul :

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

où s = nombre de points singuliers indépendant de l'ordre de multiplicité

Exemple 1:
Les droites les cercles, les coniques,les cubiques singulières ont un genre égal à zéro.
Les cubiques planes sont des courbes algébriques de degré n = 3 ; soit une cubique C qui possède un point singulier, ce point est d'ordre 2 ou 3. Alors *s* = 1 .son genre

$$g(C) = \frac{(3-1)(3-2)}{2} - 1 = 0$$

Pour une courbe elliptique *E, s=0 et g(E)* = 1.

Les quartiques planes sont des courbes algébriques de degré $n = 4$
Soit une quartique C , qui possède un point singulier, d'ordre 2,3 ou 4 .
Alors s = 1 et

$$g(C) = \frac{(4-1)(4-2)}{2} - 1 = 2$$

Soit une quartique C qui admet 2 points singuliers d'ordre 2, alors $s = 2$ et

$$g(C) = \frac{(4-1)(4-2)}{2} - 2 = 1$$

Pour une quartique E sans point singulier, $s = 0$ et $g(E) = 3$.
Les quintiques planes sont des courbes algébriques de degré n = 5,
soit une quintique C qui admet 1 point singulier d'ordre 2,3,4 ou 5, alors s = 1
son genre est égal à

$$g(C) = \frac{(5-1)(5-2)}{2} - 1 = 5$$

Une quintique ayant 2 points singuliers a un genre

$$g(C) = \frac{(5-1)(5-2)}{2} - 2 = 4$$

Les sextiques non singulières ont un genre g=(6-1)(6-2)/2=10
Donc les sextiques ayant un point singulier ont un genre g=9.

Exemple 2 :

1) Soit la courbe algébrique E_1 d'équation :
$E_1 : f(x,y) = y^2 = x^3 + x$;
Les dérivées partielles sont égales à :
$f'_x(x,y) = 3x^2 + 1$ et $f'_y(x,y) = 2y$; le système $f = f'_x = f'_y = 0$ n'a pas de solution.
Donc E_1 n'admet pas de point singulier, il en résulte $g(E_1) = 1$.

2) Soit la courbe algébrique E_2 d'équation :
$E_2 : f(x,y) = y^2 - x^3$.
Les dérivées partielles sont égales à :
$f'_x(x,y) = -3x^2$ et $f'_y(x,y) = 2y$; le système $f = f'_x = f'_y = 0$ admet donc $s = 1$ une solution (0,0), il en résulte un point singulier S= (0,0).
Le genre de E_2 est égal à $g(E_2) = 0$.

3) Soit la courbe algébrique E_3 d'équation :
$E_3 : f(x,y) = x^4 - 3x^2y^2 + 2x^3 + 4y^2 - 6xy$.
Ces dérivées partielles sont égales à :
$f'_x(x,y) = 4x^3 - 6xy^2 + 6x^2 - 6y$; $f'_y(x,y) = -6x^2y + 8y - 6x$
Le système d'équations $f(x,y) = f'_x = f'_y = 0$ admet au moins la solution $x = 0$, $y = 0$ .Cela implique 1 point singulier au moins , il en résulte $s \geq 1$ et le genre :

$$g(E_3) \leq \frac{(4-1)(4-2)}{2} - 1 = 2$$

Dans la suite nous nous intéresserons à des cubiques particulières.

2- Cubiques de Weierstrass :

Les cubiques de Weierstrass sont des courbes algébriques planes particulières.

Définition 4 :

1) *Une cubique de Weierstrass est une courbe algébrique plane C, irréductible d'équation spécifique de Weierstrass :*

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

Dans l'équation (1), les 5 coefficients $a_1, a_2, \ldots, a_6$ sont des éléments d'un corps commutatif K, les deux variables x et y sont des éléments d'une clôture algébrique K_{alg} du corps K, ce corps K est global, local ou fini.

2) *Une cubique de Weierstrass non singulière est une courbe elliptique .*

Pour l'étude des cubiques de Weierstrass, nous utilisons des changements de variables.

2-1 Changements de variables - Invariants :

L'élimination des monômes en *xy* et en *y* dans l'équation (1) s'obtient avec le changement linéaire de variables :

$x = X$ et $y = (Y - a_1X - a_3)/2$ pour carac$(K) \neq 2$ (2)

Avec le calcul nous obtenons l'équation de Weierstrass :

$E_1 : Y^2 = 4X^3 + b_2X^2 + 2b_4X + b_6 \in K[X,Y]$ (3)

Les coefficients b_{2i} sont des polynômes « homogènes de degré 2i » dans l'anneau $ZI[a_1, \ldots, a_6]$.

$b_2 = a_1^2 + 4a_2$; $b_4 = a_1a_3 + 2a_4$ *et* $b_6 = a_3^2 + 4a_6$ (4)

L'élimination, dans l'équation (3) , du coefficient 4 et du monôme en x² s'obtient avec le changement linéaire de variables :

$X = (x - 3b_2)/36$ *et* $Y = y/108$, pour *carac (K)* $\neq 2,3$. (5)

Nous obtenons avec le calcul, l'équation de Weierstrass :

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

Les coefficients c_{2i} sont des polynômes « homogènes de degré 2i » dans l'anneau $ZI[b_2, b_4, b_6]$.

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

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

La cubique de Weierstrass :

$E_3 : y^2 = x^3 + A\,x + B \quad \in K\,[x,y]$ (8-1)

Elle est utilisée en cryptographie et codage lorsque K est un corps fini à $q = p^n$ éléments.

La courbe elliptique de Tate :

$E_4 : y^2 + xy = x^3 + a_4 x + a_6 \in \mathbb{C}[x,y]$ (8-2)

Les coefficients a_4 et a_6 sont des séries infinies complexes :

$a_4 = -5\sum_{n\geq 1} n^3 q^n / (1-q^n)$ et $a_6 = -\frac{1}{12}\sum_{n\geq 1}(7n^5 + 5n^3) q^n / (1-q^n)$

où $q = exp(2i\,\pi\,z)$ et $z = x + i\,y\ ;\ y \rangle 0.$

La courbe elliptique de Deuring :

$E_5 : y^2 + Axy + y = x^3 \in K\,[x,y]$ *et* $A \neq 3$ (8-3)

La courbe elliptique de Legendre :

$E_6 : y^2 = x(x-1)(x-t) \in K\,[x,y]$ *avec* $t \neq 0,1$ (8-4)

Chaque cubique de Weierstrass est caractérisée par plusieurs invariants :
le discriminant $\Delta\ (E)$, l'invariant modulaire $j(E)$, l'invariant différentiel $\omega\,(E)$, le rang $r(E)$,
le conducteur N(E) , l'invariant de Hasse Hasse(E) , le régulateur $R(E)$, la série L de Dirichlet $L(E,s)$,etc ,…

3- Invariants des cubiques de Weierstrass : [1], [4], [6]

Avec les coefficients b_{2i}, nous obtenons le discriminant.

Définition 5 :

Le discriminant d'une cubique de Weierstrass E est le polynôme « homogène de degré 12 » de l'anneau ZI [b_2, b_4, b_6, b_8] égal à :

$$\Delta\ (E) = 9b_2b_4b_6 - 8b_4^3 - 27b_6^2 - b_2^2b_8 \in ZI\,[\,b_2, b_4, b_6, b_8\,] \quad (9)$$

$$où\ 4b_8 = b_2b_6 - b_4^2 \ et\ carac\ (K) \neq 2,3$$

Lorsque $E : y^2 = x^3 + Ax + B$, le discriminant est égal à :

$\Delta\ (E) = -16(4A^3 + 27B^2)$

La cubique de Weierstrass :

$E : y^2 = x^3 - 27c_4 x - 54\,c_6$, le discriminant est égal à :

$\Delta\,(E) = 2^6 \times 3^9 \left(c_4^3 - c_6^2\right)$.

Avec le coefficient c_4 et le discriminant, nous obtenons l'invariant modulaire.

Définitions 6 :

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

$j(E) = c_4^3 / \Delta(E)$ *; pour carac (K)* $\neq 2,3$

2) *l'invariant différentiel d'une cubique de Weierstrass d'équation :*

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

est égal à :

$\omega(E)=dx/(2y + a_1x + a_3)= -dy / (3x^2 + 2a_2x + a_4 - a_1y)$, *pour carac (K)* $\neq 2,3$.

Les dénominateurs sont les dérivées partielles d'ordre 1 dans la forme différentielle :

$df = f'_x dx + f'_y dy$; $f'_x = 3x^2 + 2a_2x + a_4 - a_1y$; $f'_y = 2y + a_1x + a_3$.

Calcul d'invariants de 3 cubiques :

(1) Cubique de Weierstrass : $E_1 : y^2 = x^3 + Ax + B \in IR[x,y]$

$b_2 = 0$; $b_4 = 2A$; $b_6 = 4B$; $b_8 = -A^2$; $c_4(E_1) = -48A$;

$\Delta(E_1) = -16(4A^3 + 27B^2)$ et $j(E_1) = \dfrac{1728 \times 4A^3}{4A^3 + 27B^2}$

(2) Cubique de Tate : $E_2 : y^2 + xy = x^3 + a_4x + a_6 \in K[x,y]$

$b_2 = 1$; $b_4 = 2a_4$; $b_6 = 4a_6$; $b_8 = a_6 - a_4^2$; $c_4(E_2) = 1 - 48a_4$;

$\Delta(E_2) = 72\, a_4\, a_6 - 64\, a_4^3 - 432a_6 + a_4^2 - a_6$; $j(E_2) = \dfrac{(1-48a_4)^3}{\Delta(E_2)}$.

(3) Cubique $E_3 : y^2 = x^3 - 27c_4x - 54\, c_6 \in IR[x,y]$

$b_2 = 0$; $b_4 = -2 \times 27c_4$; $b_6 = -4 \times 54c_6$; $b_8 = -27^2 \times c_4^2$; $c_4(E_3) = 48 \times 27c_4$.

$\Delta(E_3) = 64 \times 27^3 \left(c_4^3 - c_6^2\right)$; $j(E_3) = \dfrac{1728\, c_4^3}{c_4^3 - c_6^2}$

4- Résultant de 2 polynômes. Discriminant d'un polynôme

L'équation de Weierstrass d'une courbe elliptique E se met sous la forme $y^2 = f(x)$.Pour l'étude du polynôme $f(x)$, il est utile d'utiliser le résultant de 2 polynômes

La théorie des polynômes d'un anneau $K[t]$ donne une relation entre un polynôme $f(t) \in K[t]$ et sa dérivée par le moyen du résultant $Res(f, g)$ de deux polynômes $f(t)$ et $g(t)$:

$f(t) = a_0 t^n + a_1 t^{n-1} + a_2 t^{n-2} + \ldots + a_{n-1} t + a_n$, de degré $n \geq 1$

$g(t) = b_0 t^m + b_1 t^{m-1} + b_2 t^{m-2} + \ldots + b_{m-1} t + b_m$, de degré $m \geq 1$

Définitions 7 : (d'après « Algèbra » de S.Lang)

Le résultant des 2 polynômes f et g est le déterminant d'ordre n + m :

$$Res(f,g) = \begin{vmatrix} a_0 & a_1 & \dots & \dots & a_n & \dots & \dots & \dots & \dots \\ 0 & a_0 & \dots & \dots & a_{n-1} & a_n & \dots & \dots & \dots \\ 0 & \dots & \dots & a_0 & \dots & a_1 & \dots & \dots & a_n \\ b_0 & b_1 & \dots & \dots & b_m & \dots & \dots & \dots & \dots \\ 0 & b_0 & b_1 & \dots & \dots & b_m & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & b_0 & \dots & \dots & \dots & b_m \end{vmatrix}$$

m lignes

n lignes

Avec m lignes $(a_0,\dots, a_n)$ et n lignes $(b_0,\dots, b_m)$
Les termes manquants sont remplacés par des zéros.
La diagonale principale est formée de m termes a_0 et n termes b_m .

Les résultats suivants sont énoncés sans démonstration, ils se trouvent dans les ouvrages «Algebra »de **Lang [10]** et «Introduction à l'algèbre »de **Kostrikin [8]** .

Proposition 1 :

Soit un scalaire non nul $\lambda \in K$***, et deux polynômes f(x)de degré n et g(x)de degré m, d'un anneau K[X] . Alors leur résultant satisfait les propriétés :***

1) $Res(f,g) = (-1)^{mn} Res(g,f)$

2) $Res(\lambda f, g) = \lambda^m Res(f,g)$ ***et*** $Res(f, \lambda g) = \lambda^n Res(f,g)$.

□

La comparaison des zéros de 2 polynômes peut être effectuée par leur résultant.

Proposition 2 :

Soit 2 polynômes :

$f(t) = a_0 (t - \alpha_1)\dots (t - \alpha_n)$***, de degré*** $n \geq 1$

$g(t) = b_0 (t - \beta_1)\dots (t - \beta_m)$***, de degré*** $m \geq 1$***. Alors leur résultant est égal au produit :***

$$Res(f,g) = a_0^m b_0^n \prod_{1\leq i\leq n;\, 1\leq j\leq m} (\alpha_i - \beta_j) \qquad (10)$$

□

Le résultant des polynômes *f* et *g* s'exprime donc en fonction des zéros de

ces polynômes par la formule (10) qui implique la :

Proposition 3 :

Le résultant Res (f ,g) est nul si et seulement si ces 2 polynômes ont une racine commune $\alpha_i = \beta_j$ pour certains indices i et j .

Preuve :

Montrons que le résultant *Res (f , g)* = 0 implique $\alpha_i = \beta_j$.

la formule (10):*Res (f ,g)* $= a_0^m b_0^n \prod_{1\le i\le n;\,1\le j\le m} (\alpha_i - \beta_j) = 0$ implique α_i est une racine du polynôme *g (x)* et $\alpha_i = \beta_j$.

donc les deux polynômes f et g ont une racine commune .

□

Le résultant *Res (f , f′)* d'un polynôme f et de sa dérivée f' est lié à son discriminant

Dis (f) par la :

Proposition 4:

Soit un polynôme $f(x) = a_0(x-\alpha_1)...(x-\alpha_n)$ de degré n ,

et sa dérivée f'(x) et son discriminant Dis(f).

Alors :

1) Res (f , f′) = $a_0^{n-1}\prod_i f'(\alpha_i)$

2) Res (f , f′) = $a_0(-1)^{\frac{n(n-1)}{2}}$ Dis (f)

3) Res (f , f′) = $a_0^{2n-2}\prod_{i<j}(\alpha_i-\alpha_j)^2$

□

Exemples :

D'après Kostrikin

1) *Dis* $(X^n+a) = (-1)^{\frac{n}{2}(n-1)} n^n a^{n-1}$.

2) *Dis* $\left(\frac{X^n-1}{X-1}\right) = (-1)^{\frac{1}{2}(n-1)(n-2)} n^{n-2}$.

D'après « Algebra », LANG

1) Discriminant du polynôme cubique :

$f(x) = a x^3 + b x^2 + c x + d$

$Dis(f) = 18 a b c d + b^2c^2 - 4 a c^3 - 4 b^3 d - 27 a^2d^2$

2) Discriminant du polynôme cubique :

$f(x) = x^3 + A x + B$

Il est égal à :

$Dis(f) = -(4A^3 + 27 B^2)$

3) Soit *E* une cubique de Weierstrass d'équation :

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

Le discriminant du polynôme $f(x)$ est égal à :

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

4) Soit le polynôme :

$f(x) = 7x^3 - 4x^2 + 13x - 1$

Sa dérivée est égale à : $f'(x) = 21x^2 - 8x + 13$

Le résultant *Res (f, f'),* est égal au déterminant d'ordre 3+2 = 5:

$$Res(f, f') = \begin{vmatrix} 7 & -4 & 13 & -1 & 0 \\ 0 & 7 & -4 & 13 & -1 \\ 21 & -8 & 13 & 0 & 0 \\ 0 & 21 & -8 & 13 & 0 \\ 0 & 0 & 21 & -8 & 13 \end{vmatrix} = 376873$$

Proposition 4 :

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

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

Alors le discriminant Dis (f) du polynôme $f(x)$ et $\Delta(E)$ de E satisfont :

$Dis(f) = 16\,\Delta(E)$.

2) Soit une cubique de Weierstrass :

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

Alors le discriminant $\Delta(E)$ de E et $Dis(f)$ de f(x) satisfont la relation :

$\Delta(E) = 16\ Dis(f)$.

Preuve :

1) Pour une cubique de Weierstrass :

$E : y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6 = f(x) \in K[x]$.

Les discriminants sont égaux à :

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

$Dis(f) = 16(9b_2 b_4 b_6 - 8b_4^3 - 27b_6^2 - b_2^2 b_8)$

Cela implique la relation :

$Dis(f) = 16\,\Delta(E)$.

2) Soit une cubique de Weierstrass :

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

Le discriminant $\Delta(E) = -16(4A^3 + 27B^2)$.

La formule 13 de l'exemple 2) implique :

$\Delta(E) = 16\,Dis(f)$.□

5- Classification des cubiques de Weierstrass avec $\Delta(E)$ et c_4 :

Les cubiques sont classifiées, par leurs discriminants $\Delta(E)$ et leurs invariants $c_4(E)$. Les cubiques non singulières, qui sont des courbes elliptiques sont classifiées par le signe de $\Delta(E)$.

5-1 Cubiques singulières :

Considérons une cubique E de Weierstrass :

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

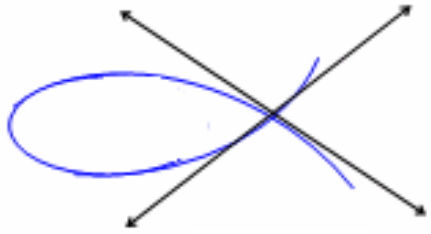
Le polynôme (1) admet des dérivées partielles f'_x et f'_y .

Lorsque le système $f'_x = f'_y = 0$ n'admet pas de solution, la courbe est non singulière, d'après la théorie des points singuliers d'une courbe plane .

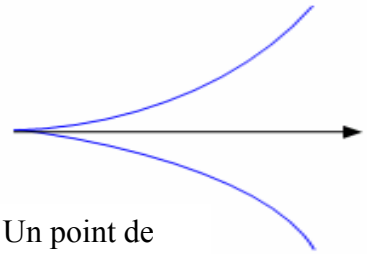
Lorsque ce système admet une solution S = (x, y) ,ce point S est un point singulier de E ;les points singuliers sont de 2 types :

Si E admet deux tangentes distinctes en S ,ce point est un nœud.

Si E admet deux tangentes confondues en S ; S est un point de rebroussement



Un noeud



Un point de rebroussement

Les cubiques singulières sont classifiées par le :

Théorème 1 :

Soit une cubique de Weierstrass E de discriminant $\Delta(E)$, et d'invariant $c_4(E)$, et son point à l'infini $O_E = (\infty,\infty) = (0, 1, 0)$.

1) Le point $O_E = (0, 1, 0)$ est un point non singulier sur E.

2) E est singulière si et seulement si $\Delta(E) = 0$.

3) E possède un nœud si et seulement si $\Delta(E) = 0$ et $c_4(E) \neq 0$.

4) E possède un point de rebroussement si et seulement si $\Delta(E) = 0$ et $c_4(E) = 0$.

Preuve de « O_E est sur E »

Dans le plan projectif IP^2, l'équation de la cubique E est de la forme

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

Les coordonnées du point O_E satisfont l'équation de E :

$$f(O_E) = f(0, 1, 0) = 0 \qquad (3)$$

Il en résulte que ce point à l'infini O_E est sur la courbe E

Preuve de « O_E est non singulier » :

La dérivée $\dfrac{\partial f}{\partial Z} = Y^2 + a_1XY + 2a_3YZ - a_2X^2 - 2a_4XZ - 3a_6Z^2$ prend, au point O_E

La valeur : $\frac{\partial f}{\partial Z}(0,1,0) = 1 \neq 0$

Cela implique que le point O_E n'est pas singulier sur E

□

Preuve de « la cubique E* est singulière *» implique « $\Delta(E) = 0$ » :

Soit l'équation de la forme :

$$E : y^2 = f(x) \quad (4)$$

L'hypothèse « E est singulière » implique que le polynôme $f(x)$ admet une racine multiple d'ordre 2 ou 3.

Par la théorie du résultant de deux polynômes

$$Res(f, f') = 0 \quad (5)$$

La relation entre $Res(f, f')$, discriminant $Dis(f)$ de f et (5) impliquent la valeur :

$$Dis(f) = 0 \quad (6)$$

La relation entre les discriminants de f et de la cubique E implique :

$$\Delta(E) = 0 \quad (7)$$

Preuve de «$\Delta(E) = 0$» implique «la cubique E* est singulière*» :

Soit une cubique E de discriminant $\Delta(E) = 0$

La relation entre les discriminants de E et de f implique :

$$Dis(f) = 0 \quad (8)$$

Par la théorie des points singuliers, cette relation implique que le polynôme f(x) admet une racine multiple d'ordre 2 ou 3 .

Il en résulte que la cubique E est singulière.

□

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

Soit une cubique de Weierstrass E d'équation $y^2 = f(x)$ (9)

L'hypothèse $\Delta(E) = 0$ implique que la cubique E est singulière donc l'équation $y^2 = f(x)$ admet une racine double ou triple .

Cette racine détermine un point singulier de la cubique E

Les pentes des tangentes en ce point sont égales à la dérivée y' de y :

$$y' = (6x^2 + b_2 x + b_4) / y = g(x) / y \quad (10)$$

L'hypothèse $c_4 \neq 0$ et la formule (7)impliquent le discriminant du polynôme $g(x)$:

$$Dis(g(x)) = b_2^2 - 24 b_4 = c_4(E) \neq 0$$

Cela implique que le polynôme $g(x)$ admet 2 racines simples

Donc E admet deux tangentes distinctes

Il en résulte que la cubique E admet un nœud.

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

D'après le théorème 1, la cubique E est singulière lorsque son discriminant est nul :

$$\Delta(E) = 0$$

Prenons la cubique de Weierstrass E d'équation :

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

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

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

$$y' = (6x^2 + b_2 x + b_4) / y = g(x) / y$$

L'hypothèse « 2 tangentes distinctes » implique que le polynôme $g(x)$ admet 2 racines distinctes.
Il en résulte que son discriminant $Dis(g(x))$ n'est pas nul
Avec le calcul j'obtiens la valeur :

$$Dis(g(x)) = b_2^2 - 24\, b_4 = c_4(E) \qquad (11)$$

Il en résulte la condition $c_4 \neq 0$
□

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

L'hypothèse *«* la cubique E admet un point de rebroussement *»* implique *«*la cubique E est singulière *»* cela implique que son discriminant $\Delta(E) = 0$
Prenons la cubique plane E d'équation de Weierstrass (9) précédente :

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

Soit S le point de rebroussement de la cubique E
Par définition d'un point de rebroussement d'une courbe algébrique, la cubique E admet 2 tangentes confondues en ce point S.
La pente de la tangente est déterminée par la formule (10)
L'hpothése de 2 tangentes confondues au point S implique une racine double du polynôme g(x) , cela implique la valeur du discriminant :

$$Dis(g(x)) = 0 \qquad (12)$$

les formules (11) et (12) impliquent la valeur $c_4(E) = 0$.
□

Le nombre de points d'intersection d'une courbe elliptique par l'axe réel Ox est déterminé par le signe de son discriminant .

Théorème 2 :

Soit une courbe elliptique E d'équation de Weierstrass :

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

et de discriminant $\Delta(E)$.Alors :

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

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

Soit une courbe elliptique d'équation de Weierstrass :

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

Alors son discriminant n'est pas nul :

$$\Delta(E) \neq 0. \qquad (2)$$

Soient les 3 points $(e_i, 0)$ avec i = 1, 2, 3 d'intersection de l'axe Ox par la courbe E.
L'équation de Weierstrass de E se met sous la forme :

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3) = f(x) \qquad (3)$$

Par définition du discriminant d'un polynôme, celui de *f(x)* est égal à :

$$Dis\,(f) = \prod_{1\le i\le j\le 3}(e_i - e_j)^2 \qquad (4)$$

L'hypothèse « 3 racines e_i réelles », implique que les carrés sont positifs

$$(e_i - e_j)^2 > 0 \qquad (5)$$

Il en résulte :

$$Dis\,(f) > 0$$

Le discriminant d'une courbe elliptique de Weierstrass

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

est lié au discriminant $Dis\,(f)$ par la relation :

$$\Delta(E) = 16\, Dis\,(f) \quad \text{ou} \quad Dis\,(f) = 16\,\Delta(E) \qquad (6)$$

Les relations (5) et (6) impliquent $\Delta(E) > 0$

□

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

Soit une courbe elliptique E qui coupe l'axe Ox en un seul point (e,0), simple . (7)

Donc E a une équation de la forme :

$$y^2 = (x-e)(x^2 + r\,x + s) = f(x) \in IR[x] \quad \text{avec} \quad r^2 - 4s < 0 \qquad (8)$$

La condition (8) implique 2 racines complexes conjuguées du polynôme $x^2 + r\,x + s$

$$x_i = -\tfrac{1}{2}\left(r \pm i\sqrt{4s - r^2}\right) \text{ avec } i = 1,2 \text{ et } 4s - r^2 > 0 \qquad (9)$$

Il en résulte que le discriminant du polynôme *f(x)* est égal à :

$$Dis\,(f) = [e - \tfrac{r}{2} + \tfrac{i}{2}\sqrt{4s - r^2}\,]^2\,[e - \tfrac{r}{2} - \tfrac{i}{2}\sqrt{4s - r^2}\,]^2\,[i\sqrt{4s - r^2}\,]^2$$

Avec le calcul j'obtiens la valeur :

$$Dis\,(f) = -(4s - r^2)\,[(e - \tfrac{r}{2})^2 + \tfrac{4s - r^2}{4}] < 0 \qquad (10)$$

Il en résulte le signe :

$$Dis\,(f) < 0 \qquad (11)$$

La relation entre les discriminants de E et de *f(x)* et (11) impliquent le signe:

$$\Delta(E) < 0 \qquad (12)$$

□

Ces théorèmes (1) et (2) permettent une classification des cubiques Weierstrass.

Corollaire :

Les cubiques de Weierstrass *E sont classifiées en 4 classes selon leur discriminant* $\Delta(E)$ *et leur invariant* $c_4(E)$.

1) Classe (W1) des cubiques de Weierstrass singulières qui ont un nœud :

$$\Delta(E) = 0 \quad et \quad c_4(E) \neq 0 .$$

2) Classe (W 2) des cubiques de Weierstrass singulières qui ont un point de rebroussement :

$$\Delta(E) = 0 \quad et \quad c_4(E) = 0 .$$

3) Classe (W 3) des courbes elliptiques qui coupent l'axe Ox en un seul point :

$$\Delta(E) < 0 .$$

4) Classe (W 4) des courbes elliptiques qui coupent l'axe Ox en 3 points simples

$$\Delta(E) > 0 .$$

□

Illustrons ce corollaire par un exemple de chaque classe

Exemple 1 : cubique E_1 qui admet un nœud.
Soit la cubique E_1 d'équation de Weierstrass

$$E_1 : y^2 = x^3 - 3x^2 + 4 \in IR[x,y]$$

Avec le calcul nous obtenons les invariants :

$$b_2 = -12 ; \quad b_4 = 0; \quad b_6 = 16; \quad b_8 = -48 ; \ \Delta(E_1) = 0.$$

$\Delta(E_1) = 0$ implique que la cubique est singulière.
L'invariant $c_4(E_1) = 144 \neq 0$ implique que ce point singulier est un noeud.
Les coordonnées de ce nœud sont les solutions du système d'équations algébriques :

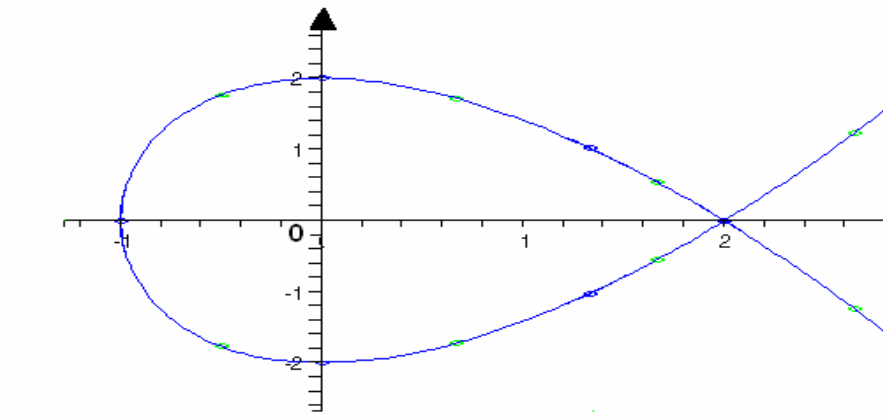
$$\begin{cases} f(x,y) = y^2 - x^3 + 3x^2 - 4 = 0 \\ f'_x(x,y) = -3x^2 + 6x = 0 \\ f'_y(x,y) = 2y = 0 \end{cases}$$

Nous obtenons la solution (2,0)
Donc le nœud de E_1 est le point (2,0)

Tableau des coordonnées de quelques points de la courbe E_1

x	-1	0	1	2	3
y^2	0	4	2	**0**	4
y	0	± 2	$\pm\sqrt{2}$	**0**	± 2

J'obtiens la courbe tracée avec le logiciel « MAPLE ».



Exemple 2 : cubique E_2 qui coupe l'axe Ox en 3 points :
Soit la cubique E_2 d'équation de Weierstrass :

$E_2 : y^2 = x^3 + 3x^2 - 9x - 5 = f(x) \in IR[x,y]$

Avec le calcul nous obtenons les invariants :

$b_2 = 12$; $b_4 = -18$; $b_6 = -20$; $b_8 = -141$; $c_4(E_2) = 576$ et $\Delta(E_2) = 2^5 \times 1701$

$\Delta(E_2)>0$ implique que cette cubique est une courbe elliptique qui coupe Ox en 3 points simples.

Pour construire cette courbe elliptique E_2, déterminons ses trois points d'intersection avec l'axe Ox .

Les solutions rationnelles de l'équation diophantienne :

$$y^2 = f(x) = x^3 + 3x^2 - 9x - 5. \qquad (13)$$

se calculent avec le :

Théorème 3 :

Soit une équation diophantienne :

$$f(x) = x^n + d_1x^{n-1} + \ldots + d_n = 0$$

Alors toute solution de cette équation est un diviseur du coefficient constant d_n .□

Dans l'équation (13) le terme constant est $d_3 = 5$;donc toute solution de (13) est un diviseur de 5.

Les diviseurs de 5 sont : $d = \pm 1, \pm 5$; les valeurs $f(d) \neq 0$ impliquent pas de solution entière

Avec le logiciel j'obtiens les 3 racines approchées :

$x_1 = -4.69$; $x_2 = 2,18$; $x_3 = -0.48$

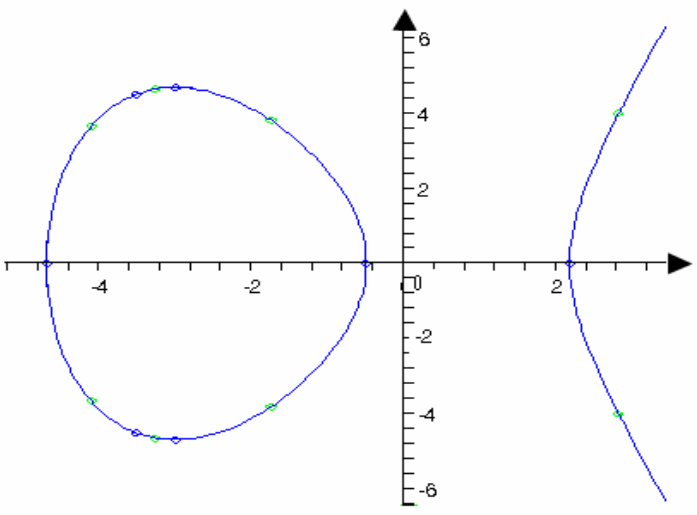
Donc la courbe E_2 coupe l'axe Ox en 3 points :

$P_1 = (-4.69,0)$; $P_2 = (2,18,0)$ et $P_3 = (-0,48,0)$.

Tableau des coordonnées de quelques points de la courbe E_2 :

x	-4.69127	-0.48887	0	1	2	2.18014	3
y^2	0	0	-5	-10	-13	0	22
y	0	0	Non	Non	Non	0	$\pm\sqrt{22}$

J'obtiens la courbe tracée avec le logiciel « MAPLE »



Exemple 3 : cubique E_3 qui coupe l'axe Ox en 1 seul point :

Soit la cubique E_3 d'équation de Weierstrass :

$E_3 : y^2 = x^3 - 2x^2 + 16 \in IR[x,y]$

Nous obtenons par le calcul les valeurs des invariants de E_3 :

$b_2 = -8$; $b_4 = 0$; $b_6 = 64$; $b_8 = -128$; $c_4(E_3) = 64$ et $\Delta(E_3) = -2^{12} \times 5^2$.

Le discriminant $\Delta(E_3) < 0$ implique que la cubique E_3 est une courbe elliptique qui coupe l'axe Ox en 1 seul point ,R.

Si ce point R a une abscisse x_R ,alors l'équation diophantienne :

$x^3 - 2x^2 + 16 = 0$

admet une solution x_R qui divise le terme constant 16.

Par le calcul nous obtenons la valeur $x_R = -2$.

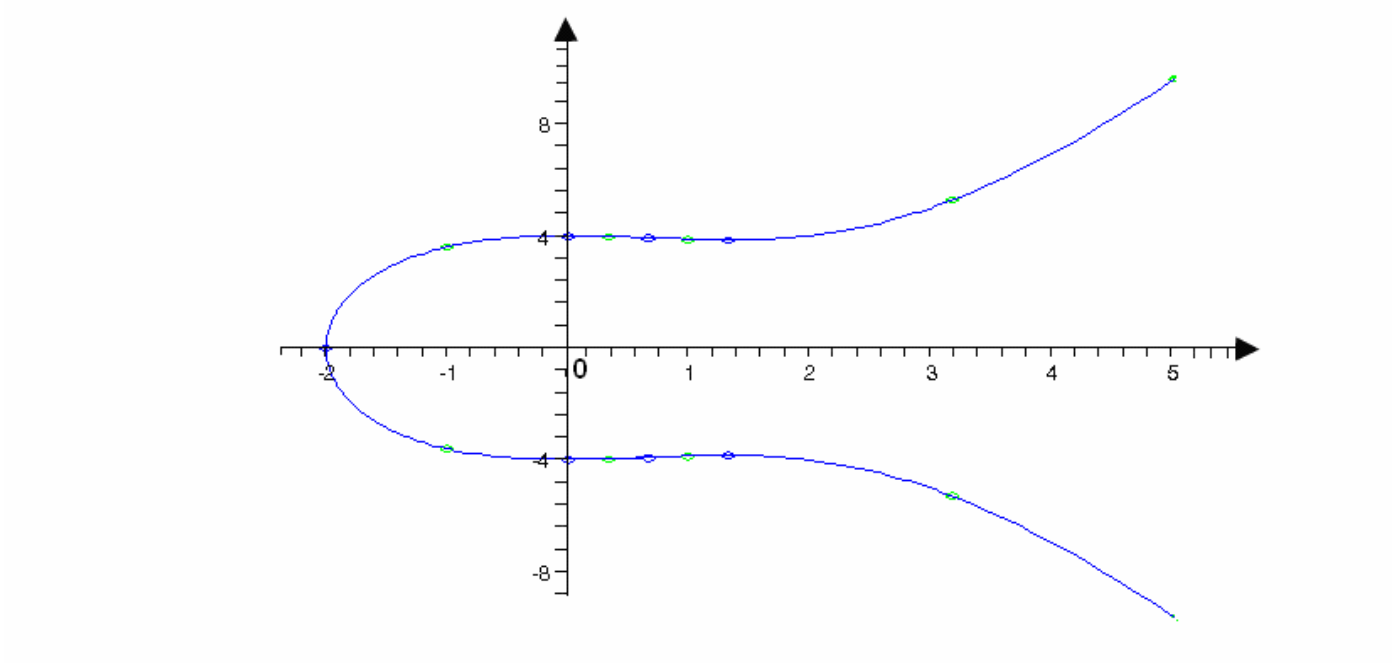
l'équation de E_3 se met sous la forme ;

$y^2 = (x+2)(x^2-4x+8)$.

Tableau de coordonnées de quelques points de E_3 :

x	-3	-2	-1	0	1	2	3	5
y^2	-29	0	13	16	15	16	25	91
y	Non	0	$\pm\sqrt{13}$	± 4	$\pm\sqrt{15}$	± 4	± 5	$\pm\sqrt{91}$

Courbe elliptique E_3 :



Exemple 4 : cubique E_4 qui admet un point de rebroussement :
Soit la cubique E_4 d'équation de Weierstrass :

$$E_4 : y^2 = x^3 - 6x^2 + 12x - 8 \in IR[x,y]$$

Nous obtenons par le calcul les valeurs des invariants de E_3 :

$b_2 = -24$; $b_4 = 24$; $b_6 = -32$; $b_8 = 48$; $c_4(E_4) = 0$ et $\Delta(E_4) = 0$.

Les valeurs $\Delta(E_4) = c_4(E_4) = 0$ impliquent que la cubique E_4 possède un point de rebroussement.

Les coordonnées de ce point sont les solutions du système :

$$\begin{cases} f(x,y) = y^2 - x^3 + 6x^2 - 12x + 8 = 0 \\ f'_x(x,y) = -3x^2 + 12x - 12 = 0 \\ f'_y(x,y) = 2y = 0 \end{cases}$$

Nous obtenons le système :

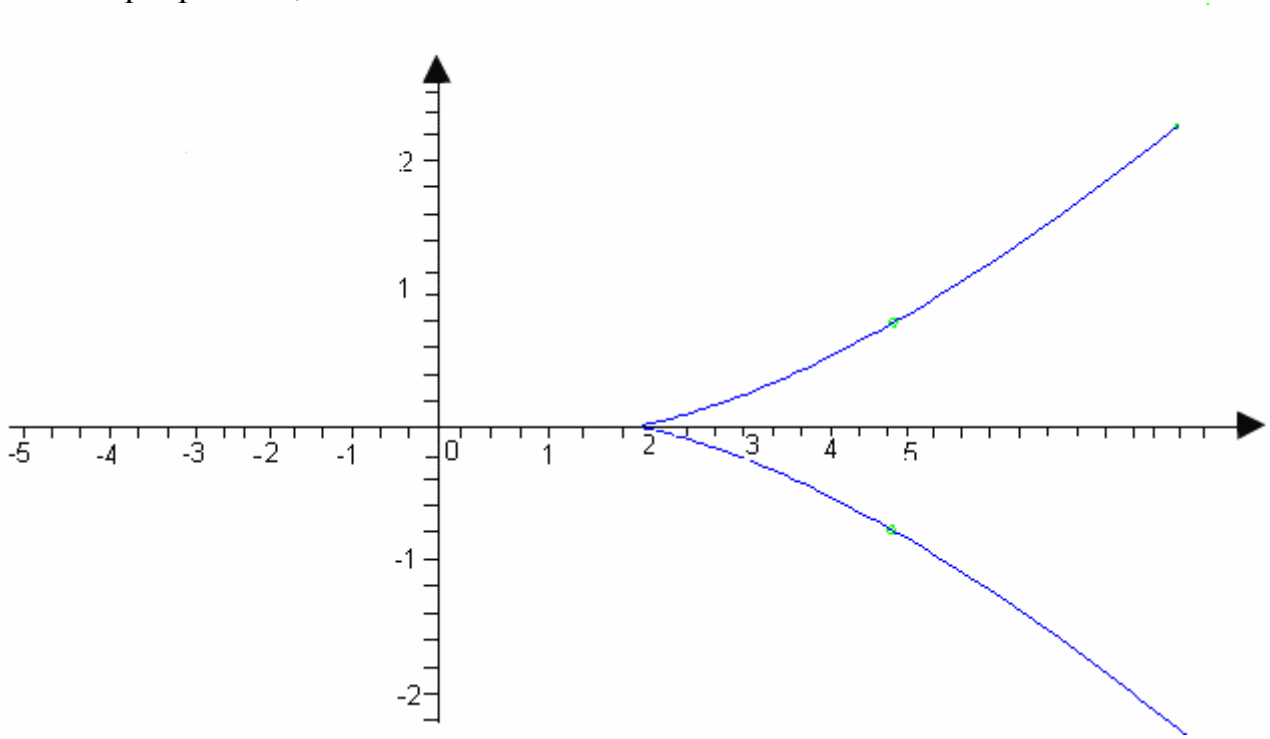
$$\begin{cases} x^3 - 6x^2 + 12x - 8 = 0 \\ x^2 - 4x + 4 = 0 = (x-2)^2 \end{cases}$$

Ce système admet la solution x = 2, y = 0
Donc le point de rebroussement est le point (2,0)

Tableau des coordonnées de quelques points de la courbe E_4

x	0	1	2	3	4	5	6
y^2	-8	-1	0	1	8	27	64
y	Non	Non	0	± 1	$\pm 2\sqrt{2}$	$\pm 3\sqrt{3}$	± 8

La cubique plane E_4



CHAPITRE III : GROUPE DE MORDELL-WEILL D'UNE COURBE ELLIPTIQUE

D'après Lang(Elliptic Curves Diophantine Analysis), Poincaré a conjecturé que l'ensemble $E(K)$ des points K-rationnels d'une Courbe Elliptique E est un groupe abélien de type fini. Plus tard en 1922 Mordell a prouvé cette conjecture.
Weil a étendu ce résultat aux variétés abéliennes(Sur un théorème de Mordell-Weil, Bull-Sci.Math-54(1930) p181-191).
Considérons l'ensemble $E(K)$ des points K rationnels d'une courbe elliptique E et le point à l'infini $O_E = (\infty,\infty)$ dans le plan affine $IA^2(K)$; $O_E = (0,1,0)$ dans le plan projectif $IP^2(K)$.

1- Construction du groupe abélien *E(K)* :

Soit une courbe elliptique E, sur un corps K , d'équation de Weierstrass :

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

Construisons un groupe abélien additif avec la :

Proposition 1 :

Soit une courbe elliptique E , et son point à l'infini $O_E = (\infty,\infty)$
Alors l'ensemble E(K) des points K rationnels de E, muni de l'application f :

$$f : E(K) \times E(K) \longrightarrow E(K)$$

de valeur : $f(P,Q) = P+Q$ **et** $f(O_E) = O_E$ **.**
où $P+Q = M$ ***est le symétrique ,par rapport à l'axe Ox du point d'intersection de la droite PQ et de la courbe E, est une loi de groupe abélien d'élément neutre le point*** $O_E = (\infty,\infty)$ ***avec la règle géométrique de 3 points*** **colinéaires P ,Q ,R de *E* :**

$$P + Q + R = O_E$$

□
Preuve :
Soit l'ensemble $E(K)$ des points K-rationnels de la courbe E.
Le point O_E unique par ses coordonnées projectives, est déterminé par la direction de l'axe Oy.
Considérons l'application :

$$f : E(K) \times E(K) \longrightarrow E(K)$$

de valeur $f(P,Q) = P + Q$.
Le point $P+Q$ est déterminé par la règle géométrique :
« Trois points colinéaires P, Q, R d'une courbe elliptique E ont une somme nulle » :

$$P + Q + R = O_E$$

Vérifions que cette application *f* satisfait les 4 axiomes d'un groupe abélien :

1) *Axiome de l'élément neutre* :

L'élément neutre du groupe est le point à l'infini O_E : ce point est déterminé par la direction de l'axe *Oy*.

La règle des 3 points colinéaires implique :

$$P+O_E + O_E = O_E + P = P \qquad (1)$$

pour tout point $P \in E$.

2) *Axiome du symétrique* :

Soit une sécante parallèle à l'axe O*y* qui coupe la courbe *E* en 3 points *P,Q,*et O_E

Il en résulte la relation :

$$P+Q+ O_E = O_E \qquad (2)$$

Nous en déduisons le symétrique :

$$P = -Q \quad ; \text{ pour tout point } P \in E \qquad (3)$$

3) *Axiome de commutativité* :

Il est vérifié par la coïncidence des sécantes *PQ* et *QP* qui implique l'égalité.

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

4) *Axiome d'associativité* :

Il est vérifié par le calcul des coordonnées des points

$(P + Q)+R$ *et* $P+(Q + R)$;

□

Définition 1 :

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

Déterminons les coordonnées du symétrique $-P$ d'un point *P et de la somme* P_1+P_2 de 2 points P_1 et P_2 .

2- Coordonnées des points $-P$, P_1+P_2 , $2P$, $m\,P$:

Soit une courbe elliptique d'équation de Weierstrass :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2 x^2 + a_4 x + a_6 \in K\,[x,y] \qquad (1)$$

2-1 Calcul des coordonnées du symétrique $-P$ d'un point P : (figure.1)

Soit un point $P = (x_p, y_p)$ du groupe *E(K)* et son symétrique

$$-P = (x,y) \quad ; \quad P + (-P) = O_E$$

Le point $-P$ est le 2$^{\text{éme}}$ point d'intersection de la courbe E par la parallèle à *Oy* passant par *P*.

L'équation de cette parallèle est $x = x_p$.

L'ordonnée de $-P$ est racine de l'équation (1); c'est une équation en y du $2^{éme}$ degré

$$y^2 + y\,(a_1x+a_3) = x_p^3 - a_2x_p^2 - a_4x_p - a_6 \quad . \qquad (2)$$

Elle admet 2 racines y_p et y ; leur somme est une fonction symétrique élémentaire des 2 racines égale à :

$y_p + y = -\,(a_1x_p + a_3)$ çela implique $y = -\,(y_p + a_1x_p + a_3)$

Nous en déduisons les coordonnées du symétrique $-P$ du point $P=(x_p\,,\,y_p)$:

$$-P = \quad (x_p\,,\,-y_p - a_1x_p - a_3) \qquad (3)$$

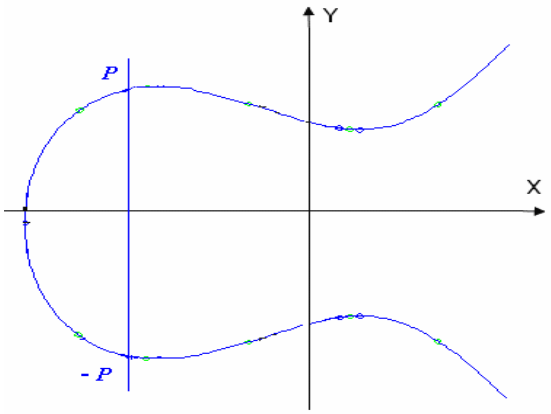


Figure.1

2-2 Calcul des coordonnées du point somme $P_1+P_2= M = (x_M,y_M)$: $P_i = (x_i\,y_i)$, pour $P_1 \neq \pm P_2$ (figure.2) :

La règle géométrique $P_1+P_2+P_3 = O_E$ implique :

$P_1+P_2= -P_3 + O_E = -P_3 = M$

Le point P_3 est l'intersection de E par la droite P_1P_2 :

L'équation de la sécante P_1P_2 est :

$$y = \lambda\,(x - x_1) + y_1 \quad \text{avec la pente} \quad \lambda = (y_1 - y_2) / (x_1 - x_2) \qquad (4)$$

Cette sécante P_1P_2 coupe la courbe en trois points simples P_1,P_2 et P_3 (figure.2)

Les abscisses de ces 3 points sont les zéros de l'équation cubique en x :

$$[\lambda\,(x - x_1)+y_1]^2 + (a_1x + a_3)\,[\lambda\,(x - x_1)+ y_1] = x^3 + a_2\,x^2 + a_4\,x + a_6$$

La fonction symétrique « somme des racines » vaut :

$$x_1+x_2+x_3 = \lambda^2 + a_1\lambda - a_2 \qquad (5)$$

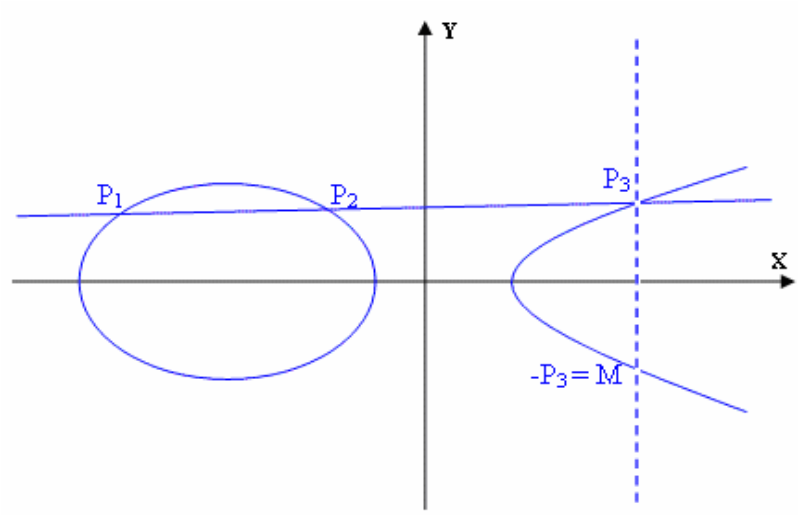
La formule (5) implique les coordonnées du point P_3 :

$P_3=(x_3 = \lambda^2+a_1\lambda-a_2-x_1-x_2,\ y_3=y_1+\lambda(x_3-x_1))$;

La relation géométrique $P_1+P_2+P_3 =O_E$ implique que le point $M = P_1+P_2$ est le symétrique du point P_3

Avec le calcul j'obtiens les coordonnées du point M :

$$\begin{cases} x_M = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \ ; \ avec \ \ \lambda = \dfrac{y_1 - y_2}{x_1 - x_2} \ \ et \ \ x_1 \neq x_2 \\ y_M = -\lambda^3 - 2a_1\lambda^2 + \lambda(a_1 + 2x_1 + x_2 - a_1^2) + a_1a_2 - a_3 - y_1 + a_1(x_1 + x_2) \end{cases}$$



□ **Figure.2**

Nous avons démontré la :

Proposition 2 :

Soit une courbe elliptique d'équation de Weierstrass :

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

1) le symétrique –P d'un point P = (x_p, y_p) de E a pour coordonnées

$$-P = (x,y) \ avec \ x = x_p \ ; y = -(y_p + a_1x_p + a_3)$$

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

$$\begin{cases} x_M = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \ ; \ avec \ \ \lambda = \dfrac{y_1 - y_2}{x_1 - x_2} \ \ et \ \ x_1 \neq x_2 \\ y_M = -\lambda^3 - 2a_1\lambda^2 + \lambda(a_1 + 2x_1 + x_2 - a_1^2) + a_1a_2 - a_3 - y_1 + a_1(x_1 + x_2) \end{cases}$$

□

2-3 Calcul des coordonnées du point *2P* :

Les coordonnées du point *2P* sont déterminées par la :

Proposition 3 :

Pour tout point P = (x_P , y_P) du groupe de Mordell-Weil E (K) d'une Courbe Elliptique E le point P+P= 2P a pour coordonnées :

$$2P = \begin{cases} x_{2P} = \lambda^2 + a_1\lambda - a_2 - 2x_P \text{ ; pour} \lambda = \dfrac{3x_p^{\,2} + 2a_2x_p + a_4 - a_1y_p}{2y_p + a_1x_p + a_3} \\ y_{2P} = -\lambda^3 - 2a_1\lambda^2 + \lambda\left(a_2 + 3x_P - a_1^2\right) + a_1a_2 - a_3 + 2a_1x_P - y_P \end{cases}$$

□

Preuve : (figure 3)

Soit un point $P = (x_P, y_P)$;

La tangente à la Courbe Elliptique E au point P a pour équation :

$y = \lambda\ (x - x_P) + y_P$,

où λ est la pente de la tangente à la Courbe Elliptique E au point $P = (x_P, y_P)$:

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

Cette tangente coupe la courbe E en un point double $P = (x_P , y_P)$ et un point simple

$M = (x_M, y_M)$

La règle de trois points colinéaires implique la relation :

$2P + \mathrm{M} = 0_E$ et $2P = -\mathrm{M}$; (6)

Les abscisses de ces trois points sont les racines de l'équation cubique en x :

$$[y_P + \lambda(x - x_P)]^2 + a_1x\,[\lambda(x - x_P) + y_P] = x^3 + a_2x^2 + a_4x + a_6 \text{ ;} \quad (7)$$

La fonction symétrique élémentaire des racines de l'équation (7) implique la relation :

$$2x_P + x_M = \lambda^2 + a_1\lambda - a_2 \text{ ;} \quad (8)$$

(8) implique l'abscisse du point M :

$$x_M = \lambda^2 + a_1\lambda - a_2 - 2x_P \text{ ;} \quad (9)$$

(6) (9) et la formule (3) du symétrique d'un point impliquent les coordonnées du point $2P$

$$2P = \begin{cases} x_{2p} = \lambda^2 + a_1\lambda - a_2 - 2x_P \text{ ;} \qquad \lambda = \dfrac{3x_P^2 + 2a_2x_P + a_4 - a_1y_P}{2y_P + a_1x_P + a_3} \\ y_{2p} = -\lambda^3 + 2a_1\lambda^2 + \lambda\,(a_2 - a_1^2 + 3x_P) + a_1a_2 - a_3 + 2a_1x_P - y_P \end{cases}$$

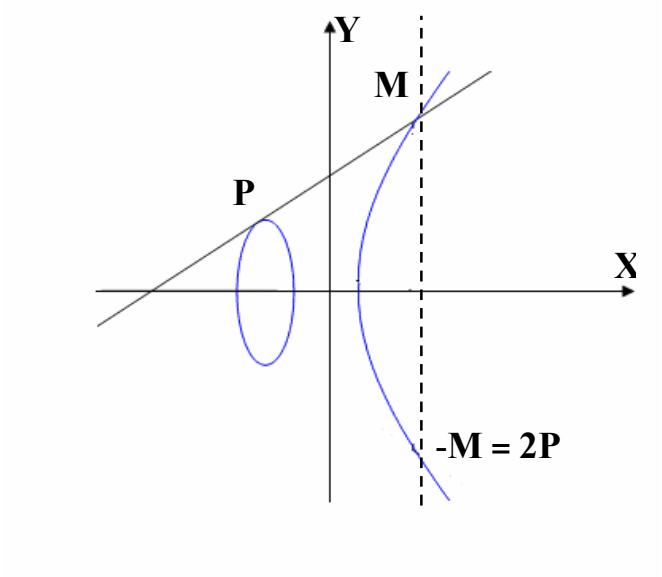


Figure.3

□

Exemple :(Figure.4)

Soit la Courbe Elliptique *E* d'équation de Weierstrass :
E : $y^2 - x\,y + 4\,y = x^3 - 2\,x^2 - x + 6$;

Le groupe de Mordell-Weil $E(\mathbb{Q})$ contient les deux points M = (1,-4) et R =(-2,-2)
Calcul des coordonnées des points M+ R, - M, 2 M .
Nous obtenons les résultats :

M+ R = $(\frac{37}{9},\frac{125}{27})$; - M = (1,1), 2 M = $(\frac{6}{25},\frac{96}{125})$

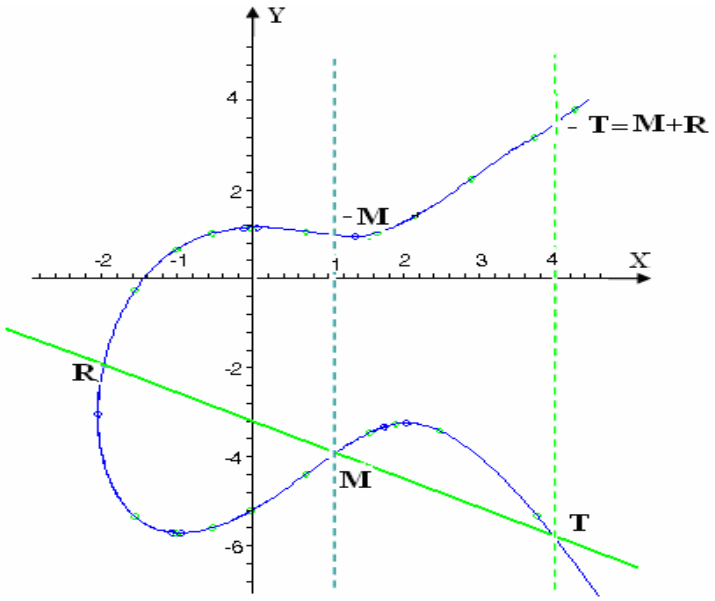


Figure.4

2-4 Calcul des coordonnées du point *mP* :

Pour tout entier rationnel *m*, et pour tout point *P* de la courbe *E*, le symbole *Mp* signifie :

$$\begin{cases} mP = P + P + \ldots + P, \ m \text{ fois } P \text{ lorsque } m>0 \ ; \\ mP = (-m)(-P) = (-P)+(-P)+\ldots+(-P), \ (-m) \text{ fois } -P \text{ lorsque } m<0 \\ \text{et } 0P = 0_E \ \text{ lorsque } m = 0. \end{cases} \qquad (10)$$

Les coordonnées d'un point *mP* sont des fractions rationnelles du corps $K(x,y,a_{1,\ldots,}a_6)$. Elles peuvent être obtenues par application des formules de la somme P_1+P_2 et du point *2P*.

Il existe des formules de récurrence que l'on trouve dans l'article de **« Cassels » [5]** : « Diophantine Equation with special reference to elliptic cruves.Jour.London Math.Soc41 (1966) 193-291.

Les formules des coordonnées de points *mP* sont déterminées par la :

Proposition 4 :

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

$$E : y^2 = x^3 + A\,x + B \ \text{ avec } 4A^3 + 27\,B^2 \neq 0 \ \text{ et } \ A, B \in IZ$$

Alors les coordonnées des points mP, pour tout point P de E sont égales à :

$$mP = \left(\frac{\phi_m(x,y)}{\psi_m^2(x,y)}, \frac{\omega_m(x,y)}{\psi_m^3(x,y)} \right) = (x_{mP}, y_{mP}) \ ;$$

Les numérateurs et les dénominateurs ϕ_m , ψ_m ***et*** ω_m ***sont des polynômes de l'anneau*** $ZI[A,B,x,y]$

Les polynômes ψ_m ***sont égaux à :***

$$\psi_0 = 0; \psi_{-1} = -1; \psi_1 = 1, \psi_2 = 2y$$
$$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2 ;$$
$$\psi_4 = 4y\left(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3\right);$$

Les polynômes ψ_m ***, pour*** $m \geq 2$ ***, sont déterminés par des relations de récurrence :***

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

Les polynômes ϕ_m ***et*** ω_m ***satisfont les relations :***

$$\begin{cases} \phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1} \\ 4y\omega = \psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2 \end{cases}$$

□

Preuve :

Pour $m = -1, -P$ est le symétrique du point P implique $-(x,y)=\left(\frac{x}{(-1)^2},\frac{y}{(-1)^3}\right)$; donc

ψ_{-1}= -1. Pour $m = 0$, $0P =(\infty,\infty) =\left(\frac{\phi_0}{\psi_0^2},\frac{\omega_0}{\psi_0^3}\right)$; cela implique $\psi_0 = 0, \phi_0 = \omega_0 = 1$.

Pour $m = 2$, la proposition 4 et la formule des coordonnées d'un point 2P sont déterminées

Par les 3 polynômes

$$\begin{cases}\psi_2 = 2y\\ \phi_2 = x^4 - 2Ax^2 - 8Bx + A^2\\ \omega_2 = x^6 - 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2\end{cases} \quad (1)$$

Les coordonnées du point $2P$ sont donc égales à :

$$\begin{cases}x_{2P} = \frac{\phi_2}{\psi_2^2} = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{(2y)^2}\\ y_{2P} = \frac{\omega_2}{\psi_2^3} = \frac{x^6 - 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2}{(2y)^3}\end{cases} \quad (2)$$

Pour $m = 3$, nous obtenons les polynômes :

$$\begin{cases}\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2\\ \phi_3 = x^9 - 12Ax^7 - 96Bx^6 + 30A^2x^5 - 24ABx^4 + 12(3A^3 + 4B^2)x^3 + 48A^2Bx^2 + 3A(A^3 + 32B^2)x + 8B(A^3 + 8B^2)\\ \omega_3 = y[\,(x^{12} + 22Ax^{10} + 220Bx^9 - 165A^2x^8 - 528ABx^7) - 4(23A^3 + 444B^2)x^6 + 264A^2Bx^5 - 5A(37A^3 + 576B^2)x^4\\ -80B(A^3 + 4B^2)x^3 - 6A^2(15A^3 + 104B^2)x^2 - 28AB(3A^3 + 32B^2)x - 96A^3B^2 - 512B^4 - 3A^6\,]\end{cases} \quad (3)$$

ψ_3 est un polynôme de l'anneau $IZ[x, A, B]$ de degré 4 en x .

ϕ_3 est un polynôme de l'anneau $IZ[x, A, B]$ de degré 9 en x

$\frac{\omega_3}{y}$ est un polynôme de l'anneau $IZ[x, A, B]$ de degré 12 en x .

La formule (3) implique les coordonnées des points 3P :

$$x_{3P} = \frac{\phi_3}{\psi_3^2}\,;\, y_{3P} = \frac{\omega_3}{\psi_3^3}$$

Un raisonnement par récurrence permet de démontrer cette proposition
C'est le lemme 7-2 de l'article « Diophantine Equation with special reference to elliptic cruves »

□

Exemple :

Pour appliquer les formules de Cassels il faut une courbe elliptique de la forme :

$$E : y^2 = x^3 + A\,x + B\ ; \qquad 4A^3 + 27\,B^2 \neq 0$$

Je choisis la courbe elliptique E pour $A = -5,\ B = -2$

$$E : y^2 = x^3 - 5x - 2 \in Q[x, y] \qquad (1)$$

Calcul des invariants de E :

$$b_2 = 0\ ,\ b_4 = -10\ ,\ b_6 = -8,\ b_8 = -25\ ,\ \Delta(E) = 2^7 \times 7^2 \neq 0$$

Je détermine les points de 2-torsion avec les formules de Cassels :

$$\begin{cases} x_{2P} = \dfrac{\phi_2}{\psi_2^2} = \dfrac{x^4 + 10x^2 + 16x + 25}{(2y)^2}; \\ y_{2P} = \dfrac{\omega_2}{\psi_2^3} = \dfrac{x^6 + 25x^4 - 40x^3 - 125x^2 - 40x + 93}{(2y)^3}; \end{cases} \qquad (2)$$

Par définition, un point P de 2-torsion satisfait la relation :

$$2P = O_E = (\infty, \infty)\ ; \qquad (3)$$

Les formules (2)et (3)impliquent l'ordonnée du point P :

$$y = 0 \qquad (4)$$

Les équations (1) et (4) impliquent trois solutions qui sont les abscisses de 3 points :

$P_1 = (2,0)$;

$P_2 = (1-\sqrt{2},0)$;

$P_3 = (1+\sqrt{2},0)$;

Par « ordre d'un point d'une courbe elliptique E », nous entendons l'ordre d'un point du groupe abélien $E(K)$ de Mordell-Weill de E .

3- Points d'ordre fini d'une courbe elliptique - Groupe de torsion :

Définition 2 :

Pour tout entier rationnel m, un point P de E(K) d'ordre m satisfait la relation :

$$mP = O_E\ .$$

Le groupe $E(K)$ de Mordell -Weill d'une courbe elliptique E ,qui est abélien, admet des sous groupe abéliens et des sous groupe cycliques .

Définition 3 :

1) *Un sous groupe de m -torsion d'une cubique E de Weierstrass est l'ensemble des points P d'ordre m :*

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

2) *La réunion infinie des sous groupes de torsion du groupe E(K) est le groupe de torsion de la courbe elliptique E :*

$$T(E) = \{P \in E(K); mP = 0, m \in ZI\} = \bigcup_{m \in ZI} E(K)[m].$$

Ce groupe de torsion *T(E)* est cyclique ou abélien, selon les invariants de la courbe elliptique.
La détermination du groupe de torsion *T(E)* a été obtenue pour les courbes elliptiques sur le corps Q des nombres rationnels.

La structure de ce groupe a été précisée par la :

Proposition 5 :

Soit une courbe elliptique E sur le corps Q des nombres rationnels. Alors, son groupe de torsion T(E)(Q) est isomorphe à l'un des 15 groupes abéliens :

$$ZI/mZI \quad pour \quad 1 \le m \le 10 \quad et \quad m = 12$$

$$ZI/2ZI \oplus ZI/2dZI \quad pour \quad 1 \le d \le 4$$

Preuve :
(Selon **Mazur [12-1]**)
Cette structure du groupe de torsion *T(E)(Q)* est apparue dans la recherche des nombres premiers N tels qu'il existe des courbes elliptiques qui admettent des N-isogénies Q- rationnelles
Ces nombres premiers sont égaux à :
N = 11, 17, 19, 37, 67, 163.
Les ordres des points des groupe de torsion*T(E)(Q)* ont été obtenues par **Kubert[10].**
Des propriétés de ces points sont utilisées pour la preuve.
□

Les coordonnées de points de torsion des Courbes Elliptiques *E*(*Q*)peuvent être calculées
avec la :

Proposition 7 :
Soit une Courbe Elliptique E d'équation de Weierstrass :
E : $y^2 = x^3 + Ax + B \in Q[x, y]$, A et B $\in$ IZ et $4A^3 + 27B^2 \neq 0$.
Soit un point P $\in$ E(Q)de torsion. Alors :
1) Les coordonnées x et y de P sont des entiers rationnels.
2) Lorsque $2P \neq O_E$, alors y^2 divise $4A^3 + 27B^2$.
Preuve :
Elle a été obtenue par (**Cassels [3]**).
□
Exemple :
Soit une courbe elliptique E d'équation de Weierstrass :
$E : y^2 = x^3 + 3x + 6 \in Q[x,y]$.
Alors $4A^3 + 27B^2 = 2^3 \times 3^3 \times 5$.
Les valeurs possibles de y^2 sont :
$y^2 = 4, 9, 36.$
Pour $y^2 = 4$, nous obtenons l'équation $x^3 + 3x + 2 = 0$, pas de solutions rationnelles.
Pour $y^2 = 9$, nous obtenons l'équation $x^3 + 3x - 3 = 0$, pas de solutions rationnelles.
Pour $y^2 = 36$, nous obtenons l'équation $x^3 + 3x - 30 = 0$, pas de solutions rationnelles.
Il en résulte que la courbe E ne possède pas de points de torsion à coordonnées x,y dans ZI.

4- Théorème de Mordell-Weil d'une Courbe Elliptique :
Selon Lang, la preuve de ce théorème comporte 2 parties ; l'une est consacrée à l'ordre fini du groupe quotient $E(K)/m\,E(K)$, l'autre partie concerne le type fini du groupe abélien $E(K)$.

Proposition 8 :
Soit le groupe de Mordell-Weil E(K)d'une Courbe Elliptique E
Alors le groupe quotient E(K) / mE(K) est fini pour un entier m $\geq$ 2 .
Preuve : selon **Lang [11-2]**
Soit une courbe elliptique d'équation de Weierstrass
$E : y^2 = (x - e)(x - e)(x - e) = h(x) \in K[x]$
Alors les trois points $P_i = (e_i, 0)$ sont d'ordre deux .
Considérons les trois homomorphismes de groupes :
$f_i : E(K) \rightarrow K^* / K^{*2}$, $i=1, 2, 3$
dont les noyaux satisfont l'inclusion :
$$\bigcap_{1 \leq i \leq 3} \ker f_i \subset 2E(K)$$
Prenons les valeurs :
$f_i(0_E) = 1, f_i(x, y) = (x - e_i) \bmod K^{*2}$ si $x \neq e_i$
$f_i(e_i , 0) = (e_i - e_j)(e_i - e_k) \bmod K^{*2}$ pour $i = 1,2,3$

Ces valeurs des homomorphismes f_i sont choisies pour que le groupe quotient $E(K)/2E(K)$ soit fini.

□

Pour montrer que le groupe $E(K)$ est de type fini, on utilise des fonctions « hauteurs » spéciales et la « descente infinie ».

Définition 4: (selon **Silverman [16-1]** p : 199)
Une hauteur sur un groupe abélien A est une fonction à valeurs réelles :

$$h : A \rightarrow IR$$

qui satisfait les 3 conditions :

(h_1) *Pour tout point P_1 de A on associe une constante $c_1(A,P_1) = c_1$ telle que :*

$$h(P + P_1) \leq 2\,h(P) + c_1 \text{, pour tout point P de A .}$$

(h2) *Il existe un entier $m \geq 2$ et une constante $c_2(A) = c_2$ tels que :*

$$h(mP) \geq m^2 h(P) - c_2 \text{, pour tout point P de A .}$$

(h3) *Pour toute constante c_3 ,l'ensemble des points P de hauteur bornée par c_3 est fini :*

$$\{ P \in A ; h(P) \leq c_3 \} \text{ est fini .}$$

Cette définition implique que l'on peut choisir les valeurs $h(P)$ pour obtenir plusieurs types de hauteurs sur une courbe elliptique.

Proposition 9:

Soit un groupe abélien A tel que le groupe quotient A/mA est fini pour un certain entier $m \geq 2$; alors le groupe abélien A est de type fini

Preuve :

Soit un groupe abélien A, et le groupe quotient A/mA fini.

Considérons un système de représentants des classes du groupe quotient A/mA :

$$R_1, R_2, \ldots, R_s \qquad (1)$$

Construisons une suite infinie de points $P_1, \ldots, P_n$ à partir d'un point P avec des combinaisons linéaires :

$$P = mP_1 + R_{i_1} \qquad 1 \leq i_1 \leq s$$

$$P_1 = mP_2 + R_{i_2} \qquad 1 \leq i_2 \leq s$$

$$\vdots$$

$$P_j = mP_{j+1} + R_{i_{j+1}} \qquad 1 \leq i_{j+1} \leq s$$

$$\vdots$$

$$\text{et } P_{n-1} = mP_n + R_{i_n} \text{ avec } 1 \leq i_1, \ldots, i_n \leq s \qquad (2)$$

La relation $P_{j-1}=mP_j+R_{i_j}$ implique la combinaison linéaire :

$$mP_j = P_{j-1} - R_{i_j} \qquad (3)$$

Appliquons au1^{er}membre de(3) l'axiome ***(h_2)*** et au 2 ^{ème}membre de (3) l'axiome ***(h_1)***. Nous obtenons l'inégalité :

$$h(P_j) \le \frac{2}{m^2}\,(h(P_{j-1}) + c') \qquad (4)$$

En additionnant membre à membre les inégalités (4) pour j = 1,…, n j'obtiens l'inégalité :

$$h(P_n) \le \left(\frac{2}{m^2}\right)^n h(P) + \left(\frac{1}{m^2} + \frac{2}{m^4} + \frac{2^{n-1}}{m^{2n}}\right)c' \qquad (5)$$

La série en $\frac{1}{m^2}$ du deuxième membre provient du développement limité de

$$\frac{1}{1-v} = 1 + v + v^2 + \ldots + v^N \text{ pour } \quad v^t = \frac{2^{t-1}}{m^{2t}} \qquad (6)$$

Les relations *(5)* et *(6)* impliquent les inégalités :

$$h(P_n) \le \left(\frac{1}{m^2}\right)^n h(P) + \frac{c'}{m^2 - 2} \le \frac{1}{2^n} h(P) + \frac{c'}{2} \text{ ; pour m} \ge 2 \qquad (7)$$

Donc l'ensemble $\{P_n, n \to \infty\}$ est un ensemble de points de hauteur bornée.
Par l'axiome **(h_3)**, cet ensemble est fini
Il en résulte que tout point P du groupe abélien A est une combinaison linéaire

$$P = n_1R_1 + \ldots + n_tR_t + n_{t+1}P_1 + \ldots + n_{t+r}P_u \; ; \; n_1, \ldots, n_{t+r} \in ZI \qquad (8)$$

Il en résulte que le groupe abélien A est de type fini.
□

L'algorithme des combinaisons linéaires constitue la descente infinie sur le groupe A.
Citons quelques types des hauteurs sur les courbes elliptiques : la hauteur logarithmique
(hauteur de Weill), la hauteur canonique(hauteur de Neron-Tate)et les hauteurs locales .

Exemples de hauteurs :
Comme toute fonction $f : A \to B$, la hauteur peut prendre plusieurs valeurs, il en résulte plusieurs types de hauteurs.

1) *Hauteur sur un espace projectif $IP^n(Q)$: avec l'ensemble M_Q des valuations du corps Q.*

$$h(P) = \prod_{v \in M_Q} \max v(a_N) \quad , P = (a_1, a_2, \ldots, a_{N+1})$$

2) *Hauteur sur le corps IQ des nombres rationnels ;* $h : IQ \to IR$

$h(x = a / b) = max\{|a|,|b|\}$ **;** $|x| = max\ \{x , -x\}$

3) *Hauteur sur le groupe E (IQ) d'une courbe elliptique E;* $h_f : E(IQ) \to IR$

$h_f(P) = log(max\{|a|,|b|\})$ **;**

$P= (x, y)$, $x = a/b$ et $h\ (0_E) = 0$

C'est la hauteur logarithmique (ou de Weil), elle satisfait la relation :

$h_f(P+Q) + h_f(P - Q) = 2h_f(P) + 2h_f(Q) + O(1)$;

où O(1)est une fonction bornée sur A

Pour tous points P et Q de E.

4) *Hauteur canonique (ou de Néron-Tate) sur une Courbe Elliptique E est la fonction*

$h\hat{}: E(K) \to IR$

de valeur $h\hat{}(P) = \lim_{N \to +\infty} 4^{-N} h_f(2^N.P)$

Cette hauteur canonique satisfait la :

Proposition 10 :

1) La hauteur canonique h^ : E(K) → IR satisfait la loi du parallélogramme : h (P + M)+ h (P -M)= 2 h (P)+ 2 h (M) ; pour tous points P et M de E(K).

2) Pour tout point P ∈ E(K) et tout entier m ∈ ZI
h^ (mP)= m²h^ (P) pour tout entier m ≥ 2

3) La hauteur h^ induit une forme quadratique sur E(K)cette forme quadratique est :
E(K)× E(K) → IR
de valeur <M,P>= h^ (P + M)− h^ (P)− h^ (M) .
Cette forme < , > est bilinéaire.

4) Pour tout point P ≠ O_E , h^ (P) ≥ 0 et h^ (P) = 0 si et seulement si P le point de torsion mP = O_E .

Preuve :
C'est le théorème 9-3 de **Néron-Tate [13]**

□

Proposition 10:(Théorème de Mordell-Weil)

Le groupe de Mordell-Weil d'une courbe elliptique est de type fini.

Preuve :

La condition de finitude du groupe quotient $E(K)/2E(K)$ est obtenu avec l'algorithme de descente infinie sur ce groupe

□

La structure algébrique de ce groupe de Mordell-Weil d'une Courbe Elliptique est précisée par le :

Corollaire :

Le groupe de Mordell-Weil d'une courbe elliptique E sur un corps de nombres K est isomorphe au produit de groupes abéliens :

$$E(K) \approx T(E) \times ZI^r$$

où T(E) est le groupe de torsion de la courbe elliptique E, r = r(E)≥0 est un entier naturel et ZI^r désigne r copies du groupe abélien additif ZI des entiers rationnels.

□

Pour calculer le rang *r=r(E)* d'une courbe elliptique,les spécialistes utilisent les hauteurs, la série *L(E,s)*de Dirichlet - Hasse,et toutes les propriétés des courbes elliptiques.

5- Rang d'une courbe elliptique :

Le rang r (E) d'une courbe elliptique E est donc le nombre de points d'ordre infini qui sont linéairement indépendants et qui engendrent la partie infinie du groupe de Mordell-Weil E (K).

Définition 5 :

L'entier naturel $r = r(E) \geq 0$ de cette formule d'isomorphisme est le rang de la courbe elliptique E .C'est aussi le nombre de générateurs indépendants $P_1,..., P_r$ de la partie infinie du groupe E(K).

Ces générateurs peuvent être déterminés à l'aide des fonctions hauteurs.

La structure du groupe de Mordell-Weil est de même type que celle du groupe des unités d'un corps L des nombres algébriques .

Théorème (Dedekind**) :**

Soit un corps de nombres L de degré fini $[L : Q] = n = r_1+2r_2$.
avec r_1 conjugués réels et $2r_2$ conjugués complexes.
Les unités du corps L forment un groupe abélien multiplicatif U (L) isomorphe à un produit de groupes abéliens :

$$U(L) \approx C(L) \times IZ^r$$

C(L)=groupe multiplicatif des racines de l'unité contenues dans L,
$r = r_1 + r_2 - 1$ = rang du groupe des unités.

Citons quelques résultats pris dans la littérature spécialisée.

1-Penny et Pomérance : *« Math. Comp.29-jully1975 -965-967 »*

Ils ont obtenu des courbes elliptiques dont le rang sur le corps Q est au moins égal à 7 .

Ces courbes ont une équation de Weierstrass :

$$y^2 = x^3 + ax^2 + bx = f(x) \in ZI\,[x]$$

Ils ont utilisé un ensemble d'entiers :

$$A = \left\{n \in ZI; n^2 \le b; n + a + n/b = d^2; d \in ZI\right\} \cup \{b\}.$$

et l'application projection : $\pi : Q^* \to Q^{*2}$.

Alors, $card\,(\pi(A)) = 2^s$,pour un certain entier s .

Ces 2 chercheurs obtiennent une borne pour le rang de E :

$$r(E) \le s - 1.$$

Les nombres a et b sont grands :

$$y^2 = x^3 + 169602x^2 - 53005272391x.$$

2- JF Mestre:*« Construction of an Elliptique Curve of rank ≥2 »*
CRAS-Paris (1982) 643-644,

Il a trouvé une courbe elliptique E de rang $r(E(Q))\ge 12$:

$$E : y^2 - 246xy + 365990 = x^3 + 228x^2 - 19339780\,x - 3629244.$$

3- Rubin et Silvester : *« Bull .of the Amer .Math .Soc »*
Vol.36 ; (2002) 455-474.

Ils ont cherché des bornes pour les rangs de courbes elliptiques :

$$E : y^2 = x^3 + a\,x^2 + bx + c = f(x) \in ZI\,[x],$$

avec la condition :

$$a^2 b^2 + 9c\,(2\,ab - 3c) \ne 4\,(a^3 c + b^3).$$

Ils ont utilisé l'ensemble A des entiers u et v :

$$A = \{u, v \in ZI;\ u \text{ et } v \text{ premiers entre eux };\ v^4 f\,(u/v) = 0\ \}$$

Ils ont obtenu une borne $r(E) \le 2j$; pour un certain entier j qui dépend de A et de $f\,(x)$.

CHAPITRE IV : ISOMORPHISME - AUTOMORPHISME - ISOGENIE TWISTS

Dans la théorie des groupes il y a des homomorphismes de groupes.Il en résulte des isomorphismes $E(K) \longrightarrow E'(K)$,des automorphismes $E(K) \longrightarrow E(K)$, des endomorphismes des groupes de Mordell-Weil des courbes elliptiques.
Nous nous intéressons aux isomorphismes.

1- Isomorphismes de courbes elliptiques :

Soient deux courbes elliptiques E et E' d'équations de Weierstrass :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \in K[x,y] \quad ;$$
$$E' : y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6 \in K[x,y] \quad ;$$

Définition 1 :

Un isomorphisme de 2 courbes elliptiques E et E′ est une application de groupes de Mordell- Weil :

$$f : E(K) \longrightarrow E`(K)$$

qui satisfait les formules d'isomorphisme de groupes :

1) $f(P+Q) = f(P) + f(Q)$; *pour tout points P et Q de E*
2) $f(O_E) = O_{E'}$; O_E *=point à l'infini de E ;* $O_{E'}$ *=point à l'infini de E`*
3) *f est bijective* ;

Ces isomorphismes sont caractérisés par des formules spécifiques

Proposition 1 :

Un isomorphisme de 2 courbes elliptiques est défini par le changement de variables linéaire :

$$\begin{cases} x = u^2X + r \\ y = u^3Y + su^2X + t \end{cases} \qquad (1)$$

avec u , r, s, t dans le corps K et u ≠0

Preuve :

Soit un isomorphisme $\lambda : E(K) \longrightarrow E`(K)$
déterminé par les formules (1), et l'isomorphisme réciproque
$\psi : E`(K) \longrightarrow E(K)$.

Pour vérifier les formules d'isomorphisme de groupe, il faut calculer l'image $f(P+Q)$de la somme et la somme $f(P) + f(Q)$des images.
En utilisant les formules des coordonnées de la somme de 2 points d'une courbe elliptique,(**Proposition :2**),nous obtenons la formule (1) d'isomorphisme ; l'image du point neutre O_E est égale à $f((0,1,0)) = (0,1,0) = O_{E'}$.
La condition $u \neq 0$ implique les coordonnées d'un point (X,Y)de la courbe $E`$ isomorphe à E

$$X = (x - r)/u^2 \quad \text{et} \quad Y = (y - sx - t + s\,r)/u^3 \quad .$$

□

La relation (1) implique des relations entre les coefficients et les invariants des 2 courbes isomorphes, les résultats obtenus sont rassemblés dans le:

Corollaire :

Soit 2 Courbes Elliptiques E et E' isomorphes. Alors :

Les coefficients a_i et a_i' sont liés par les relations :

$$\begin{cases} u\,a'_1 = a_1 + 2s \ ; \\ u^2\,a'_2 = a_2 - s a_1 + 3r - s^2 \ ; \\ u^3\,a'_3 = a_3 + r a_1 + 2t \ ; \\ u^4\,a'_4 = a_4 - s a_3 - r s a_1 + 2r a_2 - t a_1 + 3r^2 - 2ts \ ; \\ u^6\,a'_6 = a_6 + r a_4 + r^2 a_2 - t a_3 - t a_1 + 3r^2 - 2ts \ ; \end{cases} \qquad \text{(Isom1)}$$

Les invariants b_{2i} et b'_{2i} sont liés par les relations :

$$\begin{cases} u\,b'_2 = b_1 + 12r \ ; \\ u^4 b'_4 = b_4 + 2b_2 + 6r^2 \ ; \\ u^6 b'_6 = b_6 + 2r\,b_4 + r^2\,b_2 + 4r^3 \ ; \\ u^8 b'_8 = b_8 + 3\,r\,b_6 + 3r^2\,b_4 + r^3\,b_2 + 3r^4 \ ; \end{cases} \qquad \text{(Isom 2)}$$

Relations entre les invariants c_{2i} et c'_{2i} :

$$\begin{cases} u^4 c'_4 = c_4 \ ; \\ u^6 c'_6 = c_6 \ ; \end{cases} \qquad \text{(Isom 3)}$$

Relation entre les discriminants :

$$u^{12}\Delta(E') = \Delta(E) \ ; \qquad \text{(Isom 4)}$$

Relations entre les invariants modulaires j(E) et les invariants différentiels $\omega(E)$:

$$j(E') = j(E) \quad et \quad u^{-1}\omega(E') = \omega(E) \ ; \qquad \text{(Isom 5)}$$

□

Dans la relation (4) le signe de Δ(E) implique le signe de Δ(E´) ≠ 0, donc E´ est une courbe elliptique.La relation (5) est une relation d'équivalence dans l'ensemble des courbes elliptiques qui ont des invariants modulaires égaux.

□

La formule *j(E´) = j(E)* caractérise les courbes elliptiques isomorphes

Proposition 2:

Deux courbes elliptiques E et E′, sont isomorphes si et seulement si elles ont des invariants modulaires égaux :

j(E′) = j(E)

Preuve :

Preuve de « E et E' isomorphes » implique « j(E′) = j(E) »

Soit 2 courbes elliptiques E et E' isomorphes ; alors les coordonnées, d'un point du groupe de Mordell - Weil E (K) sont liées à celles du point de E'(K) correspondant par les formules d'isomorphisme :

$$(x,y) \longrightarrow (u^2X + r,\ u^3Y + su^2X + t)$$

Les relations ((Isom 5) impliquent l'égalité: $j(E) = j(E')$.

Preuve de « j(E′) = j(E) » implique « E et E' isomorphes »

L'invariant modulaire j(E) d'une courbe elliptique E peut prendre trois valeurs : $j(E) = 0,\ j(E) = 1728,\ j(E) = t \neq 0,\ 1728$ sur un corps K de caractéristique ≠ 2,3.

Examinons les 3 cas possibles : $j(E) = j(E')=0,\ 1728$ et $t \neq 0\ ,1728$

Prenons 2 équations de Weierstrass sous la forme :

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

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

le discriminant d'une courbe elliptique est égal à :

$$\Delta\ (E) = -12^3(c_4^3 - c_6^2) \neq 0 \qquad (2)$$

Alors son invariant modulaire vaut :

$$j(E) = 1728\ c_4^3/(c_4^3 - c_6^2) \qquad (3)$$

1er cas :

L'hypothèse d'égalité des invariants $j(E)=j(E')= 0$ implique les relations :

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

Les 2 équations deviennent :

$$E : y^2 = x^3 - 54c_6 \quad ;$$

$$E' : y^2 = x^3 - 54\ c'_6 \quad ; \qquad (5)$$

La relation d'isomorphisme entre les invariants c_i et c'_i des 2 courbes elliptiques implique l'équation :

$$u^6\ c'_6 = c_6 \qquad (6)$$

C'est une équation algébrique de degré 6 en u qui admet donc 6 racines dans une clôture algébrique K_{Alg} du corps K.

$$u = (c_6/c'_6)^{1/6}$$

Cela implique 6 isomorphismes :

$$E(K) \longrightarrow E'(K) \text{ avec } (x, y) \longrightarrow (u^2x, u^3y)$$

2ème cas :

Invariants modulaires $j(E) = j(E') = 1728$
Cette hypothèse implique les 2 conditions $c_4 \neq 0, c'_4 \neq 0$ et $c_6 = c'_6 = 0$.
Les 2 équations deviennent :

$$E : y^2 = x^3 - 27\, c_4\, x \quad ;$$

$$E' : y^2 = x^3 - 27 c'_4 x \quad ;$$

Par les relations d'isomorphismes entre les invariants c_i et c_i' il existe un élémnet $u \in K_{Alg}$ tel que :

$$u^4 c'_4 = c_4$$

C'est une équation du 4ème degré en u ; elle admet 4 racines dans une clôture algébrique K_{Alg} de K.

$$u = (c_4/c'_4)^{1/4}$$

Il en résulte les 4 isomorphismes :

$$E(K) \longrightarrow E'(K) \quad avec \quad (x, y) \longrightarrow (u^2x, u^3y)$$

3ème cas :

Pour $j(E) = j(E') = t \neq 1728, 0$
La formule de $j(E)$ implique l'équation :

$$1728\, c_4^3 / (c_4^3 - c_6^2) = 1728\, c_4'^3 / (c_4'^3 - c_6'^2)$$

l'équation : $1728 c^3{}_4 = t (c_4'^3 - c_6'^2)$ admet la solution :

$$c_4 = t / (t - 1728),\ c_6 = \pm\, t / (t - 1728)$$

Relations d'isomorphismes entre les invariants c_i et c_i' :

$$u^4 c'_4 = c_4 \text{ et } u^6 c'_6 = c_6$$

Ce sont 2 équations algébriques en u de degrés 4 et 6.

Elles admettent, dans un corps algébriquement clos les solutions :

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

Il en résulte les isomorphismes :

$$E(K) \longrightarrow E'(K) \quad \text{avec} \quad (x, y) \longrightarrow (u^2x, u^3y) \quad \square$$

Il en résulte une classification des courbes elliptiques en classes de courbes isomorphes.
Classe des courbes elliptiques d'invariant $j(E)=0$.
Classe des courbes elliptiques d'invariant $j(E)=1728$.
Classe des courbes elliptiques d'invariant $j(E)= t \neq 0,1728$.

Exemple :
Soit une courbe elliptique E d'équation de Weierstrass :
$E : y^2 +4xy +6y = x^3 + 3x^2 - 12x -15 \in Q[x,y]$
Avec le calcul j'obtiens les valeurs :
$b_2 = 28$; $b_4 = 0$; $b_6 = -24$; $b_8 = -168$ et $\Delta(E)=64\times3\times5\times121 >0$; $c_4(E)= 28^2$; l'invariant modulaire $j(E)=14^6/15\times121$
La relation $\Delta(E)>0$ implique la cubique E est une courbe elliptique qui coupe l'axe Ox en 3 point simples.

Courbe elliptique isomorphe E' obtenue par le changement de variables :

$$\begin{cases} x = 4X - 1 \qquad y = 8Y - 8x + 3 \\ u = 2 \quad ; r = -1 \ ; \ s = -2 \ et \ t = 3 \end{cases}$$

J'obtiens l'équation de Weierstrass de la courbe isomorphe :

$$E' = Y^2 + Y = X^3 + X^2 - \frac{11}{16}X - \frac{1}{4}$$

Avec le calcul j'obtiens les invariants de la courbe isomorphe E' :
$b_2 = 4$; $b_4 = -11/8$; $b_6 = 0$; $b_8 = -121/256$; $\Delta(E')=2^{-6}3\times5\times11^2$
L'invariant $c_4(E')= 49$; l'invariant modulaire $j(E')=14^6/15\times121= j(E)$

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

x	0	-1	-1,06	-4,83	1	2,90	2	3
y	Pas de solution réelle	-1 racine double	0	0	$-5\pm\sqrt{2}$	0	$7\pm\sqrt{30}$	$-9\pm\sqrt{84}$

La Courbe Elliptique Ecoupe l'axe Ox en 3 points simples d'abscisses x_i $i=1,2,3$ obtenues avec le logiciel Maple : $x_1 = -1,0667$; $x_2 = -4,8392$; $x_3 = 2,9059$.

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

x	0	-1	-1/2	-1,36	0,64	-0,28
y	-1/2 racine double	$y_1 = -1,32$ $y_2 = 0,32$	$y_1 = -0,80$ $y_2 = -0,19$	0	0	0

La Courbe Elliptique E' coupe l'axe Ox en 3 point simples d'abscisse x_i $i=1,2,3$ obtenus avec le logiciel Maple : $x_1 = -1,36883$; $x_2 = 0,64987$; $x_3 = -0,281039$.

La Courbe Elliptique *E* tracée avec le logiciel « Maple »:

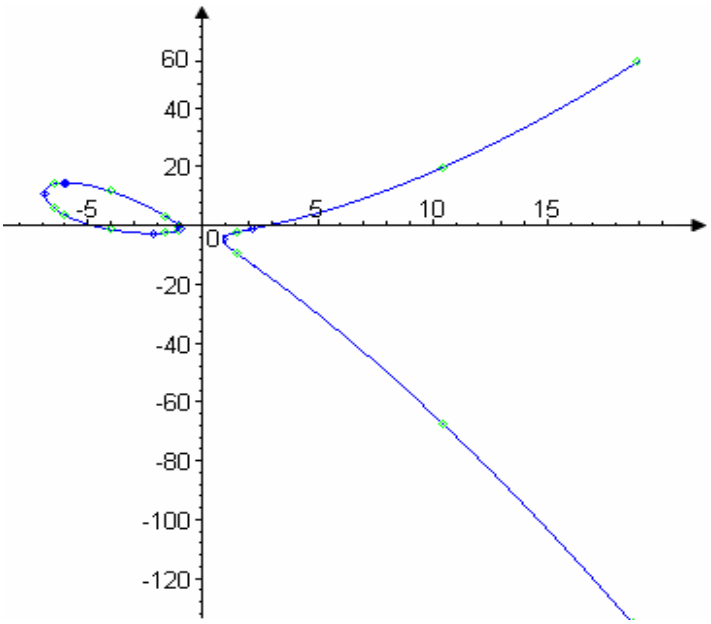


Figure.1

La Courbe Elliptique *E′* tracée avec le logiciel « Maple »:

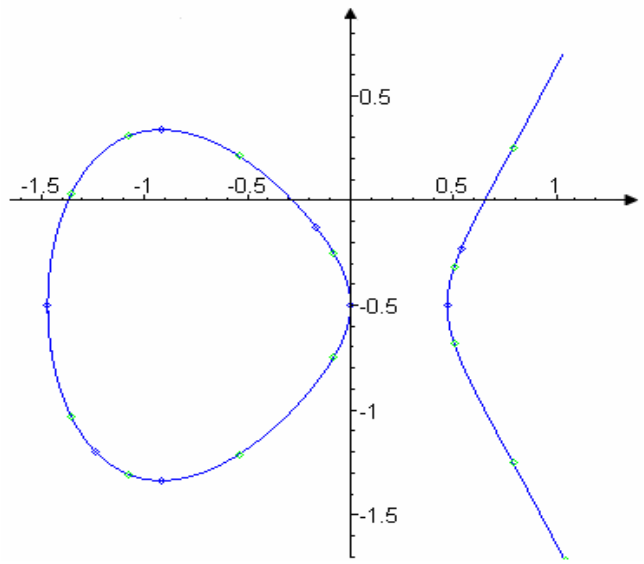


Figure.2

Les automorphismes d'une courbe elliptique *E,* forment un groupe *Aut(E).*

2. Automorphismes d'une courbe elliptique :

Les automorphismes d'une courbe elliptique dépendent de son invariant modulaire *j(E)*et de carac *(K)*

Définition 2 :

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

L'ordre du groupe des automorphismes d'une Courbe Elliptique *E* est un diviseur de 24, comme le montre la :

Proposition 3:

Soit une courbe elliptique E. Alors le groupe Aut (E) des automorphismes de E est un groupe d'ordre un diviseur de 24 :

1)Aut(E) est d'ordre 2 si j(E) ≠ 0,1728

2) Aut(E) est d'ordre 4 si j(E) = 1728 et caractéristique de K différente de 2,3

3) Aut(E) est d'ordre 6 si j(E) = 0 et caractéristique de K différente de 2,3

4) Aut(E) est d'ordre 12 si j(E) = 0 = 1728 et caractéristique de K égale à 3

5) Aut(E) est d'ordre 24 si j(E)=0= j (E)=1728 et caractéristique de K égale à 2

Preuve de (1) :

Soit une courbe elliptique *E*, d'invariant modulaire $j(E) \neq 0,1728$ (1)

Nous prenons une équation de *E* de la forme

$$y^2 = x^3 + Ax + B \quad \text{avec } 4A^3 + 27B^2 \neq 0 \tag{2}$$

Son invariant modulaire vaut :

$$j(E) = 1728.4.\, A^3/(4A^3 + 27\,B^2) \text{ pour } carac\,(K) \neq 2,3 \tag{3}$$

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

$$x = u^2 X\,;\; y = u^3 Y \tag{4}$$

Les formules (1) et (3) impliquent les 2 conditions :

$$A \neq 0 \text{ et } B \neq 0 \tag{5}$$

Les relations d'isomorphismes entre les coefficients de 2 courbes elliptiques isomorphes sont :

$$u^4 A = A \text{ et } u^6 B = B \tag{6}$$

Ce sont 2 équations algébriques de degrés 4 et 6 en *u* :

$$u^4 = 1 \text{ et } u^6 = 1$$

soit $u^2 = 1$

Cette équation admet 2 racines dans *K :*

$$u = 1,\; u = -1$$

Il en résulte 2 automorphismes de E :

$E(K) \longrightarrow E(K)$ de valeur $(x = X, y = Y)$ et $(x = X, y = -Y)$

Le groupe *Aut (E)* est d'ordre 2.

Preuve de (2) :
Soit une courbe elliptique E, d'invariant modulaire $j(E) = 1728$ sur un corps K de caractéristique $\neq 2,3$ (7)
La formule de l'invariant modulaire $j(E)$ et (7) impliquent les 2 conditions :

$$A \neq 0 \text{ et } B = 0 \quad (8)$$

Les formules (6) impliquent l'équation :

$u^4 A = A$; soit $u^4 = 1$

Cette équation admet 4 racines dans le corps $K(i)$:± 1 et $\pm i$
Il en résulte 4 automorphismes :

$E(K) \longrightarrow E(K)$ de valeur

$(x = X, y = Y)$, $(x = X, y = -Y)$,$(x = -X, y = -iY)$ et $(x = -X, y = iY)$

Preuve de (3) :
Soit une courbe elliptique E, d'invariant modulaire $j(E) = 0$ sur un corps K de caractéristique $\neq 2,3$ (9)
La formule (3) de l'invariant modulaire $j(E)$ et (9) impliquent les 2 conditions :

$$A = 0 \text{ et } B \neq 0 \quad (10)$$

Les formules (6) impliquent l'équation :

$u^6 B = B$ soit $u^6 = 1$

Cette équation admet 6 racines dans le corps $K(u)$

$u = \pm 1$, $u = \pm j$, $u = \pm j^2$ où $j = \frac{1}{2}(1 + \sqrt{3})$

Il en résulte 6 automorphismes:

$E(K) \longrightarrow E(K)$ de valeur

$$(x = X, y = Y), (x = X, y = -Y), (x = j^2 X, y = j^3 Y), \quad (11)$$
$$(x = j^2 X, y = -j^3 Y), \ (x = jX, y = jY) \text{ et } (x = jX, y = -jY)$$

Preuve de (4) :
Soit une courbe elliptique E, d'invariant modulaire $j(E) = 0$ sur un corps K de caractéristique égale à 3.
Nous prenons un automorphisme de la courbe de la forme :

$$x = u^2 X + r \ ; \ y = u^3 Y$$

Les relations entre les coefficients des courbes elliptiques isomorphes sont:

$$u^4 A = A \text{ et } u^6 B = B + rA + r^3 \quad (12)$$

Les automorphismes sont déterminés par les couples *(u,r)*d'éléments $u \neq 0$ et r chaque couple *(u, r)* est solution du système :

$$u^4 = 1 \text{ et } r^3 + rA + B(1 - u^2) = 0 \quad (13)$$

Sur une clôture algébrique de K, u engendre un sous groupe C_4 d'ordre 4 et r engendre un sous groupe C_3 d'ordre 3.
Le groupe *Aut(E)* est isomorphe au groupe produit $C_4 \times C_3$, qui est donc d'ordre 12.

Preuve de (5) :
Soit une courbe elliptique E, d'invariant modulaire $j(E) = 0$ sur un corps K de caractéristique égale à 2. (14)
Prenons l'équation de la courbe sous la forme :

$$y^2 + a_3 y = x^3 + a_4 x + a_6 \quad (15)$$

L'équation (15) est préservée par l'automorphisme :

$$x = u^2 X + s^2 \; ; \; y = u^3 Y + u^2 s X + t, \quad u, s, t \in K^*, \; u \neq 0 \quad (16)$$

Les relations entre les coefficients des courbes isomorphes impliquent:

$$\begin{cases} u^3 a'_3 = a_3 ; \\ u^4 a'_4 = a_4 + s a_3 + s_4 \; ; \\ u^6 a'_6 = a_6 + s^2 a_4 + t a_3 + s_6 + t_2 \; ; \end{cases} \quad (17)$$

Le groupe *Aut (E)* de la courbe E est déterminé par les triplets *(u, s, t)* dans une clôture algébrique de K :

$$u^3 = 1, \; s^4 + s a_3 + a_4 (1-u) = 0 \text{ et } t^2 + t a_3 + s^2 a_4 + s^6 = 0 \quad (18)$$

u engendre un groupe cyclique C_3 d'ordre 3 ; s engendre un groupe cyclique C_4 d'ordre 4 et t engendre un groupe cyclique C_2 d'ordre 2 .

Les relations (18) entre s et t impliquent que le groupe C_4 est twisté par le groupe C_2 ; le produit C_2C_4 est un groupe d'ordre 8 isomorphe au groupe Q (8) des quaternions.
Les automorphismes (15) sont liés aux triplets *(u, s, t).*
Donc le groupe *Aut (E)* est d'ordre égal au nombre de triplets *(u, s, t),* soit 24.

Le groupe *Aut (E)* est isomorphe au produit de groupes $C_3 \times Q(8)$.
□

Il y a des homomorphismes particuliers de courbe elliptiques : les Isogénies.

3. Isogénies et endomorphismes de courbes elliptiques :

Signalons que le terme d'isogénie est utilisé pour les Variétés abéliennes, pour les Tores Complexes et dans d'autres cas.

Une Courbe Elliptique *E,* a une structure de groupe abélien de type fini.

Tout morphisme de Courbes Elliptiques :

$$f : E_1(K) \rightarrow E_2(K)$$

satisfait les relations d'homomorphisme de groupes :

Un exemple d'isogénie de courbes elliptiques est constitué par la multiplication Ψ_m par un entier rationnel m :

$$\Psi_m : E(K) \longrightarrow E(K)$$

de valeur $\Psi_m(P) = m\,P$

Cette application satisfait les formules d'homomorphisme de groupe :

$$\Psi_m(P+R) = m(P+R) = m\,P + m\,P = \Psi_m(P) + \Psi_m(R)$$

et $\Psi_m(0_E) = m\,0_E = 0_E$.

Donc Ψ_m est un endomorphisme du groupe $E(K)$.

Selon Shimura (Introduction to the Arithmetic of Automorphic functions), le noyau de cette application Ψ_m est le sous groupe de m -torsion de E :

$$ker(\psi_m) = \{ P \in E(K) \text{ avec } m\,P = 0_E \}$$

Ce groupe est isomorphe à $(ZI/mZI)^2$, produit de deux copies de (ZI/mZI) si

$carac(K) = 0$ ou si $carac(K) = p$ ne divise pas m.

L'ensemble de ces multiplications Ψ_m a une structure d'anneau.

Proposition 4 :

Soit une courbe elliptique E .L'ensemble End $_{ZI}$ (E) des multiplications Ψ_m, dans le groupe E (K) par les entiers rationnels m forme un anneau isomorphe à l'anneau ZI :

$$\textbf{End}_{ZI}(E) \approx Z.$$

Preuve :

Soient 2 entiers rationnels m et n ; les endomorphismes associés :

$$\Psi_m , \Psi_n : E(K) \longrightarrow E(K) \qquad (1)$$

satisfont les formules des endomorphismes d'anneaux :

$$\Psi_{m+n}(P) = (m+n)P = m\,P + n\,P = \Psi_m(P) + \Psi_n(P) ; \quad (2)$$

$$\Psi_{m\,n}(P) = (m\,n)P = m(n\,P) = m\,\Psi_n(P) = \Psi_m(\Psi_n(P)) \qquad (3)$$

$$\Psi_0(P) = 0\,P = 0_E \text{ et } \Psi_m(0_E) = m\,0_E = 0_E \qquad (4)$$

Considérons l'application:

$$f: ZI \longrightarrow End_{ZI}(E)$$

de valeur $f(m) = \Psi_m : E(K) \longrightarrow E(K)$

Les formules (2), (3) et (4) impliquent que l'application f est un isomorphisme d'anneaux :

$$End_{ZI}(E) \approx ZI.$$

□

Il existe d'autres formes d'isogonies $E(K) \longrightarrow E(K)$ et $E(K) \longrightarrow E`(K)$.

Shimura,a indiqué la :

Définition 3 :[16]

Une isogénie de courbes elliptiques E et E′ est un homomorphisme

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

qui satisfait les conditions:

1) *λ n'est pas nul ;*
2) *le noyau de λ est fini ;*
3) *λ est un homomorphisme surjectif.*

Les coordonnées des points mP d'une courbe elliptique E sont des fractions rationnelles du corps $K(x, y)$:

$$m\,P = (x_m, y_m) \text{ avec } x_m = \frac{\varphi_m}{\theta_m^2} \text{ et } y_m = \frac{\omega_m}{\theta_m^3},$$

où φ_m, θ_m et ω_m sont des polynômes de l'anneau $K[x, y]$.

Il en est de même pour toute isogénie $\lambda : E(K) \longrightarrow E`(K)$:

$\lambda(P) = (x_\lambda, y_\lambda)$, où $x_\lambda = \frac{A_\lambda}{D_\lambda^2}$, $y_\lambda = \frac{B_\lambda}{D_\lambda^3}$, A_λ , B_λ et D_λ sont des polynômes de l'anneau $K[x, y]$.

Exemple :
Citons un exemple (Velu dans « isogénies de courbes elliptiques », CRAS, Paris t 273 A (26 juillet 1971) 238-240)
Soit la courbe elliptique *E* d'équation de Weierstrass :

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

Avec le calcul j'obtiens les Invariants :

$$c_4(E) = 2^4 ; \Delta(E) = -11 ; j(E) = -2^{12} / 11$$

Le point P= (0, 0) engendre dans le groupe $E(Q)$ un sous groupe *L* d'ordre 5 :

$$\{P, 2P = (1, -1), 3P = (1, 0), 4P = (0, -1) \text{ et } 5P = 0_E\}$$

Ce groupe *L* permet de construire une 5- isogénie λ d'équations :

$$x_\lambda = x + \frac{1}{x^2} + \frac{2x-1}{(x-1)^2} \quad ;$$

$$y_\lambda = y - \frac{2y + xy + 1}{x^3} - \frac{2y + y(x-1) + x}{(x-1)^3} .$$

Alors, l'équation de la courbe *C* par l'isogénie $\lambda : E \to C$ est :

$$C : y^2 + y = x^3 - x^2 - 10x - 20;$$

d'invariants :

$$c_4(C) = 2^3 \times 31 ; \Delta(C) = -11^5 ; j(C) = -2^{12} \times 31^3 / 11$$

Cette isogénie λ a un noyau qui est un sous groupe d'ordre *5* du groupe $E(K)$.

Toute isogénie λ possède *2* invariants spécifiques : un degré et une isogénie duale.

Définition 4 :

1) Le degré d'une isogénie $\lambda : E(K) \longrightarrow E`(K)$,
de 2 courbes elliptiques E et E` est égal à l'ordre du sous groupe noyau de λ *:*

$$\deg\lambda = card \{ \ker \lambda \}$$

2) Soit une isogénie de courbes elliptiques de degré d :

$$\lambda : E(K) \longrightarrow E`(K).$$

L'isogénie duale de λ *est l'homomorphisme*

$$\hat{\lambda} : E`(K) \longrightarrow E(K).$$

dont les composés satisfont:
$\lambda \circ \hat{\lambda}$ *est la multiplication sur E` (K) par d ;*
$\hat{\lambda} \circ \lambda$ *est la multiplication sur E (K) par d .*

La structure de l'anneau $End_K(E)$ des endomorphismes d'une courbe elliptique E est précisée par la :

Proposition 5:

L'anneau $End_K(E)$ des endomorphismes d'une courbe elliptique E est isomorphe:

1) ***soit à l'anneau ZI des entiers rationnels ;***
2) ***soit à l'anneau A_L des entiers d'un corps quadratique imaginaire L ou à un ordre de cet anneau ;***
3) ***soit à un ordre de l'algèbre des quaternions sur le corps IR des nombres réels.***

Ce 3ème cas se présente seulement pour carac (K) = p> 0

Preuve :
C'est un théorème de **Deuring[4].**
□

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 [19]**.

3-1 Algorithme de Velu de construction d'équation de Weierstrass de courbes elliptiques isogénes .

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

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

Nous associons à tout point $P \neq O_E$ de E , une valuation V_P de valeur :
$V_P(x) \geq 0$; $V_P(y) \geq 0$.
Au point neutre O_E , nous associons la valuation V_0 de valeur :
$V_0(x) = -2$ et $V_0(y) = -3$.
Mettons l'équation de E sous la forme
$H(x,y) = x^3 + a_2x^2 + a_4x + a_6 - y^2 - a_1xy - a_3y = 0$
Par définition, l'invariant différentiel de E est égal à :

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

où les dérivées partielles de la fonction $H(x,y)$ sont égales à :
$H'_x = 3x^2 + 2a_2x + a_4 - a_1y$ et $H'_y = -(2y + a_1x + a_3)$.

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

3) Prendre l'ensemble F_2 des points de F d'ordre 2

4) L'ensemble R des points de F-F_2-O_E , l'ensemble –R des points –P pour $P \in R$, tel que $R \cup -R = F - F_2 - O_2$ et $R \cap -R = \phi$

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

6) l'application $\lambda : E \to E/F = E'$ de valeur $(x,y) \to (X,Y)$ d'équations :

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

est une isogénie de courbe elliptiques.

où $P = (x,y)$; H'_x et H'_y sont les dérivées partielles ;

$t_P = H'_x(P)$ *si* $P \in F_2$, $t_P = 6x^2 + b_2 x + b_4$ si $P \notin F_2$

$u_P = 4x^3 + b_2 x^2 + 2b_4 x + b_6$; $b_2 = a_1^2 + 4a_2$; $b_4 = a_1 a_3 + 2a_4$ *et* $b_6 = a_3^2 + 4a_6$

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

7) l'équation de Weierstrass de la courbe isogène $E` = E/F$ est

$E` = E/F : Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + (a_4 - 5t)X + a_6 - b_2 t - 7\omega$

Application de l'algorithme décrit par Velu [19]:

Soit la courbe elliptique d'équation de Weierstrass :

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

Le calcul implique les invariants :

$b_2 = -3$; $b_4 = -5$; $b_6 = 13$; $b_8 = -16$; $\Delta(E) = -1664 = -2^7 \times 13$ et $j(E) = \dfrac{129^3}{-2^7 \times 13}$

Le groupe $E(Q)$ admet un sous groupe cyclique F d'ordre 7 engendré par le point $L = (1,0)$

$F = \{L, 2L = (-1,-2); 3L = (3,-6); 4L = (3,2); 5L = (-1,2); 6L = (1,-2), 7L = O_E\}$

La relation $7L = O_E$ implique $L = -6L$; $2L = -5L$; $3L = -4L$.

Il en résulte les 3 paries :

$F_2 = \Phi$, $R = \{P, 2P, 3P\}$ *et* $S = \{P, 2P, 3P\}$

Calcul des nombres t , u , w :

Au point L nous obtenons :

$x = 1$, $t = -2$, $u = 4$: $H'_x = -4$ *et* $H'_y = -2$;

Au point $2L$ nous obtenons :

$x = -1$, $t = 4$, $u = 16$: $H'_x = H'_y = 4$;

Au point $3L$ nous obtenons :

$x = 3$, $t = 40$, $u = 64$: $H'_x = 24$ *et* $H'_y = 8$;

Avec le calcul nous obtenons les valeurs : t = 42 et w =198

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

$E` = E / F$: $Y^2 + XY + Y = X^3 - X^2 - 213\,X - 1257$.

Calcul des invariants de la courbe isogène $E`$:

$\Delta(E`) = -125497034$ et $j(E`) = \frac{(3\times 3403)^3}{\Delta(E`)}$. □

4- Twists de courbes elliptiques :

La notion de « twist » est utilisée pour les groupes : un groupe G twisté par un groupe H est un groupe G « tordu » par le groupe H .Cette idée de « tordre » une courbe elliptique E pour obtenir une autre courbe elliptique,devient la notion de « Twist » utilisée par plusieurs auteurs :

1) Weiss : a introduit le twist d'ensembles A et B :

$T : A \times B \to B \times A$ de valeur $T(a,b) = (b,a)$

et le twist de G- modules

$\theta^T : B \times A \to C$, de valeur $\theta^T(b,a) = \theta(a,b)$

Avec l'application

$\theta : B \times A \to C$.

Dans « cohomology of Groups », Academic Press ; (1969)

2) Silverman : dans « The Arithmétic of Ellitic Curves » G.T.M.106(1986), à réservé le paragraphe 2 chapitre X à la théorie des twists des courbes elliptiques .

3) Mazur et Tate : ils ont introduit « le groupe diedral twisté » dans « Points of order 13 on Eliptic Curves », Inv .Math.22 (1973) 41-49.

Ils s'agit d'un groupe Δ, extension diedrale du groupe $ZI / 2ZI$, qui est «Twisté» par le groupe $\Gamma = (ZI/nZI)^* / (\pm 1)$, dans la suite exacte :

$0 \to \Gamma \to \Delta \to ZI / 2ZI \to 0$

Ces groupes satisfont les 3 relations :

(1) $\gamma_m \Gamma_Z = \Gamma_Z^m$.

(2) $\Gamma_z \gamma_m \Gamma_z^{-1} = (\gamma_m)^{-1}$.

(3) $(\Gamma_Z)^2 = 1$.

où z est une racine primitive n^{éme} de 1, $pgcd(n,m) = 1$, Γ_z est un élément du groupe quotient Γ / Δ , et γ_m est l'image de m dans Γ par l'application $ZI / nZI \to \Gamma$.

4) Cassels : « Diophantine Equations with Special Reference to Elliptic Curves » Journal London Mathematical Society 41, (1966) 193-291, à consacré partie II, « The Geometry of Elliptic Curves Twistings »à la théorie des twists des courbes elliptiques.

5) Ligozat : « Courbes modulaires de niveau 11 » **,** a indiqué la possibilité « qu'une courbe elliptique, définie sur le corps des rationnels Q, quotient sur Q de la jacobienne $J_0(121)$, **tordue** sur le corps quadratique $Q(\sqrt{-11})$, soit isogéne sur Q à la courbe modulaire $X_0(11)$».

C'est sur la base de ces références que nous présentons cet exposé sur les twists des courbes elliptiques.

Considérons 2 courbes elliptiques E et E' et leurs groupe de Mordell–Weil $E(K)$ et $E'(K)$. Ces courbes sont choisies telles que leurs corps de fonctions soient isomorphes

$$K(E) \to K(E'). \qquad (1)$$

Soit une extension algébrique finie L du corps K, galoisienne .Il y a 3 groupes de Galois associés à L :

$$\begin{cases} G = G(L/K) = \{S, S_1, ...\}; \\ \Gamma = G(L(E)/K(E)) = \{\sigma, \tau, ...\} \\ \Gamma' = G(L(E')/K(E')) = \{\sigma', \tau', ...\} \end{cases} \qquad (2)$$

Tout K-automorphisme S de L induit un seul automorphisme σ de $L(x)$ de valeur:

$\sigma(x) = S(x)$ pour $x \in K$, $\sigma(x) = x$ et $\sigma(f(x)) = f(x)$ pour $f(x) \in L(x)$. (3)

Il en résulte que les groupes G et Γ sont isomorphes.

Il en résulte un isomorphisme :

$$L(X) \to L(Y) = L(S(X)).$$

Cela implique que les coordonnées de l'image S (x) sont des fonctions Rationnelles de X à coefficients dans l'extension L de K .

Posons :

$$\lambda_S(X) = \sigma'(X). \qquad (4)$$

Des automorphismes $\tau \in \Gamma$ et $\tau' \in \Gamma'$ satisfont les relations :

$$(\tau\lambda_S)(\tau'(X)) = \tau' S(X) \text{ et } (\tau\lambda_S)\lambda_\tau = \lambda_{\tau S}. \qquad (5)$$

Avec ces automorphismes, il faut trouver un changement de variables :

$$E(K) \to E'(K), (x,y) \to (x',y')$$

qui transforme l'équation de Weierstrass de E :

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

en une équation de Weierstrass de E':

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

Alors ,cette courbe E' est le « twist » de la courbe elliptique E par l'extension galoisienne L du corps de base K de E .

Définition 6 :

Un twist d'une courbe elliptique E est une courbe elliptique E_L, définie sur K et L isomorphe à E par une certaine extension galoisienne L de K

Exemple :

Déterminons un twist d'une courbe elliptique d'équation de Weierstrass :

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

Soit une extension quadratique $L = Q(\sqrt{d})$ du corps Q de E

Alors les groupes d'automorphismes

$G = G(L/Q) = \{S, S^2 = Id\}$ et $\Gamma = G(L(E)/Q(E))$ opérent sur la courbe elliptique E et sur les groupes $E(Q)$ et $E(L)$.

Pour le changement de variables :

$$x = x'/d \ , y = y'/\sqrt{d} \ . \quad (2)$$

avec (1) et (2) nous obtenons l'équation d'une courbe E' :

$$E' : y'^2/d = x'^3/d^3 + a_2x'^2/d^2 + a_4x'/d + a_6; \quad (3)$$

Par multiplication par d^3, nous obtenons l'équation :

$$E' : (y'd)^2 = x'^3 + a_2x'^2d + a_4x'd^2 + a_6d^3; \quad (4)$$

Le changement de variables $x' = X$, $dy' = Y$ transforme (4) en :

$$E_d : Y^2 = X^3 + a_2dX^2 + a_4d^2X + a_6d^3 . \quad (5)$$

Cette équation (5) est l'équation du twist E_d de la courbe elliptique E par l'extension quadratique $L = Q(\sqrt{d})$.

Par les formules des invariants nous obtenons le discriminant :

$$\Delta(E) = 16\,[18\,a_2a_4a_6 + a_2^2a_4^2 - 4a_4^3 - 4\,a_2^3a_6 - 27a_6^2] \quad (6)$$

En remplaçant a_2 par a_2d , a_4 par a_4d^2 et a_6 par a_6d^3 dans $\Delta(E)$, nous obtenons le discriminant du twist quadratique E_d de E :

$$\Delta(E_d) = d^6\Delta(E) = \left(\sqrt{d}\right)^{12}\Delta(E)$$

La relation d'isomorphisme de 2 courbes elliptiques :

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

est satisfaite pour le nombre $u = \sqrt{d}$ de $Q(\sqrt{d})$.

CHAPITRE V : REDUCTION DES COURBES ELLIPTIQUES

Dans l'équation de Weierstrass d'une courbe elliptique E :

$E : y^2 + a_1xy + a_3y = x^3 + a_2 x^2 + a_4 x + a_6 \in K[x,y]$

les cinq coefficients a_i sont des éléments d'un corps commutatif K, les deux variables x et y des éléments d'une clôture algébrique K^{alg} du corps K.
La réduction de ces coefficients s'obtient avec une valuation du corps K.
Indiquons un bref aperçu de la théorie des valuations d'un corps de nombres qui se trouve dans les ouvrages **[1] , [7] , [8] , [21] , [22]** etc …

1- Valuations d'un corps :

Définition 1 :

Une valuation d'un corps K est une fonction sur K à valeurs réelles positives :

$$v : K \longrightarrow IR_+$$

qui satisfait les 3 axiomes :

(Val 1) $v(x) \geq 0$ *et* $v(x) = 0$ *équivaut à* $x = 0$ *pour tout élément x du corps K*

(Val 2) $v(xy) = v(x)\,v(y)$ *pour tous les éléments x et y du corps K*

(Val 3) *il existe une constante réelle* $c \geq 1$ *telle que :*

$v(x) \leq 1$ *implique* $v(x+1) \leq c$ *pour tout élément x de K*

L'axiome ***(Val 2)*** implique qu'une valuation v est un homomorphisme du groupe multiplicatif K^* des éléments non nuls du corps K dans le groupe multiplicatif des nombres réels positifs IR_+^*

L'axiome ***(Val 3)*** de la définition peut être remplacé par l'inégalité triangulaire :

(Val 3′) $v(x+y) \leq v(x) + v(y)$ pour tous les éléments x et y du corps K

Exemples :

1) La valuation triviale sur un corps K :

L'application $v : K \longrightarrow IR_+$ de valeurs :

$v(0) = 0$ et $v(x) = 1$ pour $x \neq 0$

est la valuation triviale du corps K ; et c = 2.

2) La valeur absolue ordinaire du corps des nombres réels IR est la fonction v de valeur :

$$v(x) = max\{x, -x\}$$

Pour le $3^{ème}$ axiome, nous prenons la constante $c = 2$.

3) Soit le corps $\mathbb{C}$ des nombres complexes et la fonction v de valeur :

$$v(x) = (a^2 + b^2)^{1/2} \text{ pour } x = a + i\,b$$

Le $3^{ème}$ axiome est vérifié pour $c = 2$

4) La valuation p -adique du corps Q des nombres rationnels :

pour p premier, soit l'application :

$v_p : Q \longrightarrow IR^+$ de valeur :

$v_p(p) = 1/p$ et $v_p(q) = 1$ pour tout nombre premier $q \in ZI$ différent de p .

Alors la valuation d'un nombre rationnel $x = y\,p^n$ tel que y premier à p est égale à :

$$v_p(x) = p^{-n}$$

v_p est la valuation p -adique du corps Q

Pour le $3^{ème}$ axiome, nous prenons la constante $c = 1$.

Proposition 1 :

Toute valuation v d'un corps K est un homomorphisme du groupe multiplicatif K^* dans le groupe multiplicatif IR_+^* des nombres réels positifs.

Preuve :

L'axiome ***(Val 1)*** contient cette formule d'homomorphisme de groupe.

□

1-1 Valuations archimédiennes et valuations non archimédiennes *:*

Dans l'ensemble des valuations d'un corps K , nous distinguons deux types de valuations suivant la valeur de la constante c dans l'axiome ***(Val 3)*** de la définition d'une valuation .

Définition 2 :

1) *Une valuation v d'un corps K est archimédienne si elle satisfait :*

$$v(x) \leq 1 \text{ implique } v(x+1) \leq 2$$

Dans l'axiome (Val 3), la constante c vaut 2

2) *Une valuation v d'un corps K est non archimédienne si elle satisfait :*

$$v(x) \leq 1 \text{ implique } v(x+1) \leq 1$$

Ce qui implique la valeur $c = 1$

Selon **[1]** , 2 valuations v_1 et v_2 non triviales de K sont équivalentes si elles satisfait la relation :

$$v_2(x) = v_1(x)^{\alpha},$$

pour tout élément x de K et un nombre réel positif α .

Il en résulte que les valuations d'un corps K sont classées dans 2 classes disjointes :

Classe des valuations archimédiennes et classe des valuations non archimédiennes.

Dans l'ensemble des valuations v du corps K, les valuations non triviales satisfont la :

Proposition 2:

Toute valuation non triviale d'un corps de caractéristique p > 0 est équivalente à une valuation non archimédienne.

Preuve :

C'est un corollaire prouvé par Artin.

□

Exemples :

1) La valuation triviale sur un corps K est non archimédienne.

2) Les valeurs absolues sur les corps IR et $\mathbb{C}$ sont des valuations archimédiennes.

3) L'ensemble des valuations non équivalentes du corps Q est la réunion disjointe du sous ensemble de valuations non archimédiennes et du sous ensemble des valuations archimédiennes.

4) Les valuations archimédiennes du corps Q sont équivalentes à la valeur absolue

$$| x | = max \{ x , - x \}$$

5) Les valuations non archimédiennes sont équivalentes aux valuations p –adiques.

Une valuation non archimédienne est caractérisée par les 2 propositions

Proposition 3 :

Soit une valuation non archimédienne $v \in V_K$ d'un corps K, alors :

1) $v(x) \neq v(y)$ implique $v(x+y) = max\{ v(x), v(y) \}$

2) Soient n éléments $x_1, ..., x_n$ qui satisfont la condition :

$$v(x_1) \geq v(x_i) \text{ pour } i = 2, ..., n$$

Alors v satisfait la relation :

$$v(x_1 + x_2 + ... + x_n) = v(x_1)$$

Preuve :
Ce théorème se démontre en utilisant les axiomes d'une valuation non archimédienne c'est un corollaire de **Weiss[21]** .
□

Proposition 4 :

Soit une valuation non archimédienne v d'un corps K.

Alors elle satisfait les propriétés :

1) $v(x+y) \leq max\{ v(x), v(y) \}$ pour tout élément $x, y \in K$

2) L'ensemble $\{ v(n1)$; 1 unité de K et $n \in IZ \}$ est borné.

□

Les valuations non archimédiennes discrètes permettent d'obtenir les notions de discriminant minimal et de réduction d'une courbe elliptique sur un corps *K*.
C'est l'objet de la partie qui suit.

1-2 Valuations non archimédiennes discrètes :

Définition 3:

Une valuation non triviale $v : K \longrightarrow IR \cup \{\infty\}$ est discrète lorsque son groupe de valuation $v(K)$ est discret dans le corps IR des nombres réels .

$$v(K) = ZI \cup \{\infty\}$$

A une valuation non archimédienne discrète v sont associés les sous ensembles suivants du corps K :

$A_v = \{ x \in K ;\ v(x) \geq 1 \}$ = *l'anneau des v-entiers de K*

$M_v = \{ x \in K ;\ v(x) > 1 \}$ = *l'idéal maximal en v*

$U_v = \{ x \in K ;\ v(x) = 1 \}$ = *le groupe des v-unités*

Le corps quotient $K = A_v / M_v$ = *le corps de classes résiduelles en v.*

Une uniformisante pour v est un élément $\pi \in A_v$ *tel que* $M_v = \pi A_v$; *la valuation v est normalisée lorsque* $v(\pi) = 1$.

Exemples :

Soit le corps Q des nombres rationnels, et un nombre premier p .

La valuation p -adique est la fonction :

$v_p : IQ \longrightarrow IR_+$ de valeurs :

$v_p(p) = 1/p$ et $v_p(q) = 1$ pour tout nombre premier $q \neq p$

La valuation p -adique est discrète lorsqu'elle satisfait :

$v_p(p^r) = r$ et $v_p(q) = 0$ pour tout nombre premier $q \neq p$.

Toute valuation non archimédienne discrète réduit les invariants d'une courbe elliptique ; elle rend l'équation de Weierstrass minimale en v

1-3 Equation de Weierstrass minimale :

Soit une courbe elliptique E d'équation de Weierstrass :

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

Nous considérons une valuation v de valeur :

$v(x) = r$ *pour* $x = u \pi^r$, π = uniformisante pour v

Définition 4 :

L'équation (1) *de Weierstrass est minimale en v si ses coefficients* a_i *sont v -entiers* $v(a_i) \geq 0$ *et si son discriminant* $\Delta(E)$ *a une valuation* $v(\Delta(E))$ *minimale.*

L'équation minimale d'une courbe elliptique E n'est pas unique à cause de ses transformées en une courbe $E`$ par l'isomorphisme :

$$(x, y) \longrightarrow (u^2 x + r \ , \ u^3 y + s u^2 x + t) \text{ où } r, s, t \in K \ , \ u \neq 0$$

Les relations entre les coefficients de deux courbes elliptiques E et $E`$ isomorphes :

$$u^4 c`_4 = c_4 \ , \ u^6 c`_6 = c_6 \text{ et } u^{12} \Delta(E`) = \Delta(E)$$

impliquent que l'équation (1) est minimale en v dans les 3 cas :

1) Les cinq coefficients a_i sont v- entiers et $v(\Delta(E)) < 12$;

2) Les cinq coefficients a_i sont v- entiers et $v(c_4(E)) < 4$;

3) Les cinq coefficients a_i sont v- entiers et $v(c_6(E)) < 6$;

Lorsque l'équation (1) n'est pas minimale, le changement :

$(x, y) \longrightarrow (u^{-2}x, u^{-3}y)$ la rend minimale.

Exemple :
Soit un nombre premier p et une courbe elliptique E d'équation de Weierstrass :

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

Je calcule les invariants de E :

$c_4(E) = 129 = 3 \times 43$; $c_6(E) = -2241 = -3^3 \times 83$; $\Delta(E) = -1664 = -2^7 \times 13$

Nous obtenons les valuations $v_p(x)$:

$v_2(c_4) = 0 < 4$, $v_2(\Delta(E)) = 7 < 12$;

$v_p(c_4(E)) < 4$ et $v_p(\Delta(E)) < 12$ pour tout nombre premier $p \neq 2$

Il en résulte que l'équation de la courbe E est minimale pour tout nombre premier p.

2- Réduction d'une courbe elliptique :

La réduction d'une courbe elliptique consiste à réduire le corps de base K à un corps « local » possédant un seul idéal premier ; alors les coefficients a_i et les variables x et y de la courbe E sont « réduits » modulo cet idéal premier .

2-1 Réduction modulo une uniformisante :

Dans un corps local obtenus avec une valuation non archimédienne discrète v , l'idéal maximale est unique .Il possède un générateur π de valuation $v(\pi) = 1$,ce générateur est une uniformisante de v.
Tout élément x du corps local se met sous la forme : $x = \pi^r u$, avec un entier r et une v- unité u .

Pour toute valuation non archimédienne discrète v du corps K, la réduction modulo π en v est l'application :

$$\varphi : A_v \longrightarrow K = A_v / M_v$$
$$t \longrightarrow \tilde{t}$$

φ induit la réduction des courbes elliptiques:

$$E(K) \longrightarrow \tilde{E}(K)$$
$$P \longrightarrow \tilde{P}$$

La courbe $\tilde{E}$ est la courbe réduite en v.

Si E est une courbe elliptique sur K d'équation de Weierstrass minimale en v, alors pour obtenir l'équation de la courbe réduite $\tilde{E}$ sur le corps résiduel $K_{rés}$; il suffit de réduire modulo π le coefficients a_i ,donc la courbe réduite $\tilde{E}$ a pour équation :

$$\tilde{E} : y^2 + \tilde{a}_1 x\, y + \tilde{a}_3 y = x^3 + \tilde{a}_2 x^2 + \tilde{a}_4 x + \tilde{a}_6 \qquad \tilde{a}_i \in K$$

Les réductions sont classifiées par la nature de la cubique réduite $\tilde{E}$.

2-2 Classifications des réductions d'une courbe elliptique :

Cette classification repose sur la nature de la courbe réduite $\tilde{E}$:
Courbe elliptique , cubique de Weierstrass avec un nœud , cubique de Weierstrass avec un point de rebroussement .

Définition 5 :

Soit une courbe elliptique E, sur un corps K muni d'une valuation v, avec une uniformisante π d'équation de Weierstrass minimale en v et la courbe réduite $\tilde{E}$ de E .
Alors nous distinguons 3 types de réductions de la courbe elliptique E :

1) *La courbe E a une **bonne réduction** en v si la courbe réduite est une courbe elliptique $\tilde{E}$ sur le corps résiduel , cette **réduction est stable** .*

2) *La courbe E a une **mauvaise réduction** sur K si la courbe réduite $\tilde{E}$ est singulière . Cette **mauvaise** réduction est :*
   - ***a) multiplicative** en v si la courbe réduite $\tilde{E}$ possède **un nœud** ; cette réduction est **semi stable***
   - ***b) additive** sur K si $\tilde{E}$ possède un point de **rebroussement** ; cette **réduction instable**.*

La nature de la réduction d'une courbe elliptique peut être déterminée à partir d'une équation de Weierstrass minimale et avec les 2 invariants $\Delta(E)$, $c_4(E)$ par la :

Proposition 5:

Soit un corps K muni d'une valuation v ayant une uniformisante π et une courbe elliptique E d'équation de Weierstrass minimale en v :

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

Soit son discriminant $\Delta(E)$ et son invariant usuel $c_4(E)$. Alors :

a) La courbe E a une réduction stable en v si et seulement si

$$v(\Delta(E)) = 0 ;$$

alors la courbe réduite $\tilde{E}(K_{res})$ est elliptique , K_{res} = corps résiduel en v

b) La courbe E a une réduction semi stable en v si et seulement si :

$$v(\Delta(E)) > 0 \text{ et } v(c_4(E)) = 0 ;$$

alors la courbe réduite $\tilde{E}(K_{res})$ a un nœud .

c) La courbe E a une réduction instable en v si et seulement si :

$$v(\Delta(E)) > 0 \text{ et } v(c_4(E)) > 0 ;$$

alors la courbe réduite $\tilde{E}(K_{res})$ a un point de rebroussement .

Preuve :

Dans la classification des cubiques planes par leurs discriminants , nous avons montré dans chapitre II Théorème 1 que :

1) *E est singulière si et seulement si $\Delta(E) = 0$.*
2) *E possède un nœud si et seulement si $\Delta(E) = 0$ et $c_4(E) \neq 0$.*
3) *E possède un point de rebroussement si et seulement si $\Delta(E)=0$ et $c_4(E)=0$*

En prenons les valuations des invariants,on obtient les résultats de la proposition
□

3- Courbes semi –stables, exemples numériques :

Exemple 1:

Soit la courbe elliptique E d'équation de Weierstrass :

$$E : \quad y^2 = x^3 + 5x^2 + 1 \quad \in Q[x,y]$$

Calcul des invariants :

$$b_2 = 2^2.5 \; ; \; b_4 = 0 \; ; \; b_6 = 2^2 \; ; \quad b_8 = 2^2.5 \quad ; \quad \Delta(E) = -2^4.17.31 \quad ; \; c_4(E) = 2^4.5^2$$

Appliquons la proposition à cette courbe :
La courbe elliptique E a une réduction stable en tout nombre premier p qui ne divise pas $\Delta(E)$; soit $p \neq 2, 17, 31$

Pour $p = 2$, la valuation 2 -adique v implique :

$$v_2(\Delta(E)) > 0 \text{ et } v_2(c_4(E)) > 0 \; ;$$

C'est une réduction stable .

Pour $p = 17, 31$, la valuation p -adique implique les inégalités :

$$v_p(\Delta(E)) > 0 \text{ et } v_p(c_4(E)) = 0 \; ;$$

C'est une réduction semi stable en v_p .

Exemple 2 : [15]

1) Courbe elliptique d'équation de Weierstrass :

$$E_1 : y^2 + y = x^3 - x^2 \in Q[x,y]$$

Calcul des invariants :

$b_2 = -4 \; ; \; b_4 = 0 = b_6 = b_8 \; ; \; c_4(E_1) = 16 \; ; \; \Delta(E_1) = -11$.

Valuation $v_{11}(\Delta(E_1)) = 1 < 12 \quad ; v_{11}(c_4(E_1)) = 0 < 4$.
la courbe réduite modulo 11 est une cubique singulière avec un nœud donc E admet une réduction semi-stable.

2) Courbe elliptique d'équation de Weierstrass :

$$E_1 : y^2 + xy + y = x^3 - x \in Q[x,y]$$

Calcul des invariants :

$b_2 = 1 \; ; \; b_4 = -1 \; ; \; b_6 = 1 \; ; \; b_8 = 0 \; ; \; c_4(E_2) = -23 \; ; \; \Delta(E_2) = -28$.
Valuation $v_2(\Delta(E_2)) = 0$; donc le corps IF_2 , $\Delta(E_2) = 0$ et $c_4(E_2) = 1$
Donc la courbe réduite $\widetilde{E}_2$ admet une réduction semi stable en $p = 2$, 7

Après ma thèse de magister , je compte étudier les Courbes Elliptiques sur les corps finis et les applications à la cryptographie et au codage .

REFERENCES

📖 **[1] ARTIN - E:**
«Algebraic Number and Algebraic Functions » Gordon and Brea Sciences Publishers - New York; (1960).

📖 **[2] BOREVICH et SHAFAREVICH:**
(1) « Basic Algebraic Geometry »,Springer Verlag (1977).
(2) « Algebraic I», Moscou (1986)-Springer (1987).

📖 **[3] CASSELS - JWS:**
« Diophantine Equations with Special Reference to Elliptic Curves » Journal London Mathematical Society 41 (1966) 193-291.

📖 **[4] DEURING - M:** « Algebren » ; Springer Verlag, New York (1968).

📖 **[5] HARTSHORNE - R:**
« Algebraic Geometry », GTM 52-Springer (1983).
Graduate texte in Mathematics n° 52 (1980)

📖 **[6] HUSEMOLLER :**
« Elliptic Curves » - G.T.M -111 (1987).

📖 **[7] HASSE - H:**
« Number theory » - Springer (1980)

📖 **[8] IYANAGA - S :**
« The Theory of Numbers – North Holland Pub. Company- Amsterdam (1975)

📖 **[9] KOSTRIKIN – A -I:**
« Introduction à l'algèbre » Ed. Mir- Moscou- 2eme edition (1986).

📖 **[10] KUBERT :**
« Universal Bounds on the Torsion of Elliptic Curves » Journal London Mathematical Society 33 (1976) 193 – 237

📖 **[11] LANG - S:**
(1) « Algebra » 2eme édition, Addison Wesley Publishing Company, Inc, Reading, Massachusetts, New York (1984).
(2) « Elliptic Curves – Diophantine Analysis » Springer Verlag (1978) -
(3) « Algebraic Number Theory », Addition – Wesley (1970).
(4) « Cyclotomic Fields », GTM 59 – Springer.

🕮 **[12] MAZUR - B:**
(1) « Rational isogenies of prime degre » Invent. Math. 44 (1978), 129-162.
(2) **«** Rational points on Modular Curves LNM. n° 601 (1977) 107 -147

🕮 **[13] NERON - A:**
« Quasi Fonctions et Hauteurs sur les Variétés Abéliennes », Annals of Mathematics 82 (1965), 249-331.

🕮 **[14] RUBIN - K:**
« Elliptic Curves with Complex Multiplication and the Conjecture of Birch and Swinnerton », – Dyer – Inv. Math. 64 (1981) 455 – 470.

🕮 **[15] SERRE – J-P:**
« Propriétés galoisiennes des points d'ordre fini des courbes elliptiques », Inventions Mathématiques 15 (1972), 259-331.

🕮 **[16] SHIMURA -G:**
«Introduction to the Arithmetic Theory of Automorphic Function », Princeton University Press (1971).

🕮 **[17] SILVERMAN – J-H:**
(1) « The Arithmetic of Elliptic Curves », GTM 106 – Springer (1986). Classification AMS = 1401, 14G 99, 14H 05, 14 K 15.
(2) « Lower Bound for the canonical height on Elliptic Curves », Duke Math. J .48 (1981). 633-648
(3) « The Difference between the Weil Height and the Canonical Height on Elliptic Curves », Math. Comp. 35 (1990) 723-743.

🕮 **[18] TATE - J:**
« The Arithmetic of Elliptic Curves », Inv Math 23 (1974) 179-206.

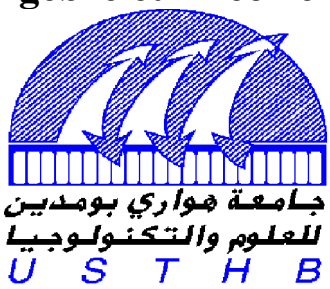
🕮 **[19] VELU - J:**
« Isogénies entre Courbes Elliptiques », C.R.A.S. Paris (1971) 238-241.

🕮 **[20] WEIL - A:**
(1) « Sur un théorème de Mordell », Bull. Sci. Math. 54 (1930).
(2) « L'arithmétique sur les Courbes Elliptiques », Acta Math 52 (1928)281-315

🕮 **[21] WEISS – E-D:**
« Algebraic Number Theory », Mc Graw – Hill. New York (1964).

🕮 **[22] ZITOUNI - M:**
« Courbes Elliptiques ; Géométrie - Arithmétique - Algorithmique (2007)

Université des Sciences et de la Technologie
Houari Boumediene
Département Algèbre et Théorie des Nombres



Faculté de Mathématiques

THESE DE MAGISTER

Sujet

Les courbes elliptiques semi stables sur le corps Q des rationnels

Présentée Par M^me^ : **AZIZI Hanane**

Résumé

Dans ma thèse de Magister, nous nous intéressons aux Courbes Elliptiques semi stables sur le corps Q des rationnels .

Cette théorie est exposée dans l'ouvrage de référence de Silverman et J-P Serre. Nous commençons par l'étude de la géométrie des Courbes Elliptiques et la structure du groupe de Mordell-Weil des points *K*-rationnels d'une Courbe Elliptique.
Ensuite nous décrivons la théorie des isomorphismes, des automorphismes et la notion d'isogénies et twistes des Courbes Elliptiques.
J'ai appliqué la théorie des valuations p-adiques du corps *Q* des nombres rationnels pour obtenir la réduction des courbes elliptiques .

*** Thèse de Magister .**

*****Mr Mohamed- ZITOUNI Professeur à l'U.S.T.H.B Directeur de thèse***