N° d'ordre : 12/2007-M/MT

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUES ET POPULAIRE
MINISTÈRE D'ENSEIGNEMENT SUPÉRIEUR DE RECHERCHE SCIENTIFIQUE
UNIVERSIÈ DES SCIENCES ET DE LA TECHNOLOGIE
HAOUARI BOUMEDIENE

MEMOIRE

Présenté pour l'obtention du diplôme de MAGISTER
EN : MATH È MATIQUES

Spécialité : ALGÈBRE ET THEORIE DES NOMBRES

Par : DEBAH Rafika

Sujet

Homomorphismes de Courbes Elliptiques

Soutenu le 12Février 2007, devant le jury composé :

M[r] Méziane AÏDER	Professeur à l'USTHB	Président
M[r] Mohamed ZITOUN	Professeur à l'USTHB	Directeur de Thèse
M[r] Abdelkader KHELLADI	Maître de conférence à l'USTHB	Examinateur
M[r] Mohamed Salah HACHAÏCHI	Professeur à l'USTHB	Examinateur
M[r] Mohaned Ouamar HERNANE	Maître de conférence à l'USTHB	Examinateur

Sommaire

Introduction :

Le sujet de ma thèse concerne les Homomorphismes des Courbes Elliptiques
La théorie des Courbes Elliptiques est basée sur les domaines, des courbes algébriques planes, de la Théorie des Nombres Algébrique, analytique, géométrique, de la Géométrie Algébrique

Les Courbes Elliptiques ont intéressé de nombreux chercheurs :
Weierstrass, Mazur [9], Silverman [14], Koblitz [6], Cassels [1], Lang[8], Ribet[11], Zagier[17], Tate[15], Shafarevich[12], etc.

Certaines Courbes Elliptiques ont été utilisées pour des applications en Codage, en Cryptographie. Pour démontrer le Théorème de Fermat Wiles a utilisé une Courbe Elliptique : $x^3 + y^3 = z^3$.

Ma thèse est composée de 3 chapitres :

Dans le chapitre I j'ai abordé les propriétés Algébriques et Arithmétiques des équations de Weierstrass, les invariants, la classification des cubiques

Dans chapitre II j'ai construit une loi de groupe abélien sur l'ensemble E (K) des points K- rationnels des courbes au moyen de la règle géométrique des 3 points colinéaires et du point à l'infini comme élément neutre :
$P_1+P_2+P_3 = 0_E = (\infty ; \infty)$.
J'ai établi les coordonnées du symétrique – P d'un point P ,la somme P+R de 2 points et de la somme P+P = 2 P

Ce groupe E (K) de Mordell – Weil a une structure de groupe abélien de type fini. J'ai utilisé les travaux de Silverman et Lang pour étudier les hauteurs sur le groupe E (K) de Mordell – Weil. J'ai décrit la structure des sous groupes E [m] de m- torsion et du groupe T(E) de torsion.

Dans le chapitre III j'ai utilisé les résultats de Silverman et de Cassels pour décrire les homomorphismes des groupes de Mordell – Weil E (K)
J'ai trouvé des exemples pour illustrer les théorèmes et les formules énoncés dans ces chapitres.

Les courbes elliptiques possèdent une structure de courbes algébriques planes
Nous nous limitons aux courbes de degré $n \leq 3$

1-Courbes algébriques planes : degré, singularité, genre [1], [8] [14]

Les courbes algébriques planes appartiennent à l'espace IR^2

Définition 1 : ***Une courbe algébrique plane est l'ensemble des points P= (x, y) qui satisfont un polynôme f (x, y) $\in$ IR[x, y] de la forme f (x , y) = $\sum d_{ij} x^i y^j$, i, j $\geq$ 0 ; Son degré est égal au degré maximal i+j des monômes x^i y^j***

Exemples:

Pour n = 1 ; $f = d_1x + d_2 y + d_3 = 0$ est l'équation d'une droite

Pour n = 2 ; $f = (x-d_1)^2 + (x-d_2)^2 - r^2 = 0$ est l'équation d'un cercle de centre (d_1,d_2) et de rayon r

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

$f = y^2 + ax + b = 0$ est l'équation d'une parabole d'axe Ox

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

Les hyperboles, les paraboles les ellipses sont des coniques, géométriquement ce sont des intersections d'un cône de l'espace IR^3 par un plan.

$f = (d_1x + d_2y + d_3)(d_4x + d_5y + d_6) = 0$ est l'équation du produit de 2 droites

Pour n = 3 ; un polynôme cubique irréductible $f(x, y) = f_0 + f_1 + f_2 + f_3$ où

Les f_i sont des polynômes cubiques homogènes de degré i = 0,1, 2, et 3

Un polynôme dégénéré est soit un produit de 3 droites, soit un produit d'une droite par une courbe irréductible de degré 2.

Les courbes algébriques sont classifiées en deux classes suivant leur décomposition :

Classe des courbes algébriques dégénérées si le polynôme f (x, y) est réductible ;
Classe des courbes algébriques non dégénérées si le polynôme f (x, y) est irréductible.

Une courbe algébrique C de degré n est singulière si elle admet des points singuliers ; elle est lisse si elle n'admet pas de points singuliers.

Définition2 : Soit une courbe algébrique plan C d'équation g(x, y) = 0 et ses dérivées partielles. Un point P de la courbe C est singulier s'il satisfait le système d'équations aux dérivées partielles

(1) $$g\,(P) = \frac{\partial g(P)}{\partial x} = \frac{\partial g(P)}{\partial y} = 0$$

Le nombre s des points singuliers S d'une courbe algébrique C permet de définir le genre g(C) de cette courbe

Définition 3 : Le genre d'une courbe algébrique C de degré n qui possède s compter avec leur multiplicités points singuliers est l'entier positif ou nul

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

Exemples : Les droites, les cercles, les coniques, les cubiques singulières ont un genre g (C) = 0
Les cubiques irréductibles non singulières ont un genre g (C) = 1.

2-Cubiques de Weierstrass [13], [14]

Dans l'ensemble des polynômes cubiques d'équation :

$f(x,y) = d_1x^3+d_2x^2y+d_3y^3+d_4x^2+d_5xy+d_6y^2+d_7x+d_8y+d_9 \in K[x,y]$
Il y a 9 coefficients $d_1, \ldots, d_9$

Dans cet ensemble il y a le sous ensemble particulier des polynômes cubiques irréductibles qui ont 5 coefficients :

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

***Définition 4** : L'équation cubique (3) est une équation de Weierstrass*
La courbe E d'équation (3) est une cubique de Weierstrass.

Dans l'ensemble des cubiques de Weierstrass il y a la classe des cubiques singulières et la classe des cubiques non singulières

***Définition 5:** Une courbe elliptique est une cubique de Weierstrass irréductible et non singulière d'équation* **(3)**
Les 5 coefficients a_1, a_2, a_3, a_4, a_6 sont des éléments d'un corps commutatif K global , local ou fini ; les 2 variables x et y , solutions d'une équation algébrique cubique , sont donc des éléments d'une clôture algébrique K_{alg} du corps K

L'équation cubique (3) peut être transformée par des changements de variables convenables en d'autres formes contenant moins de monômes

Les monômes en x y et en y sont éliminés par le changement de variables

(4) $\mathbf{x = X}$ **et** $\mathbf{y = \frac{1}{2}(Y - a_1 X - a_3)}$ pour carac K $\neq 2$

Nous obtenons l'équation de Weierstrass

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

Avec $\mathbf{b_2 = a_1^2+4a_2}$, $\mathbf{b_4= 2a_4+a_1a_3}$ et $\mathbf{b_6= a_3^2+4a_6}$

Les coefficients b_{2i} sont des polynômes homogènes de degré 2i de l'anneau
$Z/[a_1, a_2, a_3, a_4, a_6]$
Le coefficient 4 et le monôme en X^2 de (5) sont éliminés par le changement de variable

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

Nous obtenons l'équation de Weierstrass

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

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

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

Il existe d'autres formes d'équations de Weierstrass

Le modèle de Legendre

(9) $$y^2 = x(x-1)(x-\lambda) \in K[x,y] \text{ , pour } \lambda \neq 0,1$$

L'équation de Weierstrass utilisée en cryptographie et en codage

(10) $$y^2 = x^3 + Ax + B \in Q[x,y] \quad \text{et} \quad 4A^3 + 27B^2 \neq 0$$

Modèle de Deuring

(11) $$y^2 + axy + y = x^3 \in K[x, y]$$

Les invariants b_{2i} et c_{2i} permettent d'introduire d'autres invariants

Pour les invariants nous avons suivi :[5],[6],[14]
Un invariant d'une cubique de Weierstrass dépend des cœfficients a_i ; donc les invariants varient avec les cubiques.
Ils sont utilisés pour des classifications de ces cubiques

Etudions quelques invariants : le discriminant $\Delta(E)$, l'invariant modulaire j(E), l'invariant différentiel $\omega(E)$ …

***Définition 6 : Le discriminant d'une cubique de Weierstrass E est le polynôme homogène de degré 12* égal à**

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

(13) $\text{et } 4b_8 = b_2 b_6 - b_4^2 \quad \text{pour carac de } K \neq 2,3$

Le discriminant et le coefficient c_4 permettent de définir l'invariant modulaire

Définition 7 : L'invariant modulaire d'une cubique de Weierstrass E est l'élément du corps K égal a

(14) $j(E) = c_4^3 / \Delta(E) \quad \text{pour carac de } K \neq 2,3$

Cet invariant peut prendre toutes les valeurs, y compris 0 et ∞
Pour carac (K) = 2 nous obtenons les invariants :

$b_2 = a_1^2, b_4 = a_1 a_3, b_6 = a_3^2 \text{ et } \Delta(E) = b_2 b_4 b_6 + b_6^2 + b_2^2 b_8$

Pour carac (K) = 3 nous obtenons les invariants :
$b_2 = a_1^2 + a_2, \; b_4 = a_1 a_3 + 2a_4, \; b_6 = a_3^2 + a_6 \text{ et } \Delta(E) = b_4^3 - b_2^2 b_8$

Avec la différentielle df de la fonction f
d $f(x,y) = f'_x \, dx + f'_y \, dy$, nous obtenons l'invariant différentiel des cubiques de Weierstrass

Définition 8 : l'invariant différentiel d'une cubique de Weierstrass E égal a

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

3- Classification des cubiques de Weierstrass avec leurs discriminant :

Elle nécessite la connaissance des discriminants des polynômes
$f(x) \in IR[x]$

Il existe des classifications par d'autres invariants : l'invariant modulaire j (E), le conducteur N(E), etc.…

Pour l'étude des discriminants des polynômes (x) nous sommes inspiré d'ouvrages de Théorie des Nombres ''Algebra'' de Lang [8] ''Introduction a l'Algèbre '' de Kostrikin '' [7]
''A classical Invitation to Algébra Numbers and Class Fields '' de H. Cohn [2]

Définition 9 : **soit** ***un polynôme f de degré n ≥1 d'équation***
f (x) = d_0 (x-θ_1)(x -θ_2) . . . (x - θ_n) ∈ IR[x]
Alors son discriminant est égal a la fonction symétrique quadratique de ses racines $\theta_1, \theta_2, \ldots \theta_n$

$$dis\ (f) = d_0^{2n-2} \prod_{1 \le i\ j \le n} (\theta_i - \theta_j)^2$$

Appliquons cette définition à des polynômes particuliers f(x) ∈ IR[x]

Pour $f(x) = ax^2 + bx + c$; alors **dis (f) = $b^2 - 4ac$;**

Pour $f(x) = x^3+Ax+B$; alors **dis (f) = - ($4A^3+27B^2$)**
Pour $f(x) = d_0x^3 + d_1x^2 + d_2 x + d_3$;alors

dis (f) = $18d_0d_1d_2d_3 + d_1^2d_2^2 - 4d_1^3d_3 - 4d_0d_2^3 - 27d_0^2d_3^2$

Nous constatons que le dis (f) est un polynôme ''homogène '' de degré 6 de l'anneau Z/ [d_0, d_1, d_2 , d_3]

Pour $f(x) = x^n + a$; alors = **dis (f) = $(-1)^{\frac{(n)(n-1)}{2}} n^n a^{n-1}$**

Pour $f(x) = x^{n-1}+x^{n-2}+x^{n-3} + \ldots +1$, alors **dis (f) = $(-1)^{\frac{(n-1)(n-2)}{2}} n^{(n-2)}$**

Exemple :
$f(x) = x^3-10x+5$ alors dis (f) = 25×133
$f(x) = x^3+x^2+x+1$ alors dis(f) = $(-1)^3 \times (4)^2 = -16$

Pour calculer les discriminants nous utilisons la théorie du résultant de 2 polynômes **:**[7],[8]

Soit 2 polynômes :

$f(x) = d_0x^n + \ldots + d_n$ de degré $n \geq 1$ et
$g(x) = r_0x^t + \ldots + r_t$ de degré $t \geq 1$

Définition 10 : le résultant de 2 polynômes f et g est le déterminant D'ordre n+t égal à

(6) **Res (f,g) =**

$$\begin{vmatrix} d_0 & d_1 \ldots & d_n & 0 \ldots\ldots & 0 \\ 0 & d_0 & d_{n-1} & d_n\ 0 \ldots\ldots & 0 \\ \ldots\ldots & & & & \\ 0 & \ldots\ldots & 0 & d_0 \ldots\ldots & d_n \\ r_0 & r_1 \ldots\ldots & & r_t\ 0 \ldots\ldots & 0 \\ 0 & r_0 \ldots\ldots & & r_t\ 0 \ldots\ldots & 0 \\ \ldots\ldots & & & & \\ 0 & 0 \ldots\ldots & & 0 \ldots\ldots & r_t \end{vmatrix}$$

Les termes manquants sont remplacés par des zéros
il y a t lignes ($d_0, \ldots, d_n$) et n lignes ($r_0, \ldots, r_t$) , la diagonale principale est formée de t nombres d_0 et n nombres r_t

Exemple :
Soient 2 polynômes :
$f(x) = 5x^3-x^2+3$, $g(x) = x^2-1$
Leur résultant Res (f , g) est d'ordre 3+2 = 5

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

Avec les règles de calcul des déterminants nous obtenons la valeur
Res (f, g) = - 21

Proposition 2 : soient 2 polynômes :
$f(x) = d_0 (x - \theta_1) \ldots (x - \theta n) \in IR [x]$ de degré $n \geq 1$ et
$g(x) = r_0 (x - \lambda_1) \ldots (x - \lambda_t) \in IR [x]$ de degré $t \geq 1$

Alors leur résultant Res (f, g) satisfait les relations

(7) $Res\,(f, g) = d_0^t \prod_i g(\theta_i)$

(8) $Res\,(f, g) = (-1)^{n\,t}\, r_0^n \prod_j f(\lambda_j) = d_0^t r_0^n \prod_{i,j} (\theta_i - \lambda_j)$

Preuve : [7],[8]

□

La formule (8) du résultant implique le :

Corollaire **:** ***le résultant de 2 polynômes est nul si et seulement si ils ont une racine commune***

Preuve

1) " Res (f, g) =0 " implique " $\theta_I = \lambda_J$ "

Res (f, g) =0 implique $d_0^t r_0^n \prod_{i,j} (\theta_i - \lambda_j) = 0$

Il en résulte un facteur nul $\theta_i - \lambda_j = 0$

2) soit " $\theta_I = \lambda_J$ " implique " Res (f, g) =0 "

si $\theta_I = \lambda_J$ ce la implique le facteur $\theta_i - \lambda_j = 0$ et le produit $\prod_{i,j} (\theta_i - \lambda_j) = 0$

Il nous résulte Res (f, g) =0

□

Le polynôme g (x) peut être remplacé par la dérivée $f'(x)$ de f(x)

$f(x) = d_0 x^n + d_1 x^{n-1} + \ldots + d_n \in IR[x]$,de degré n

$f'(x) = n\, d_0 x^{n-1} + (n-1) d_1 x^{n-2} + \ldots + d_{n-1} \in IR[x]$,de degré n-1

Appliquons la définition du résultant à un polynôme f **(x)** et sa dérivée f' **(x)**

Proposition 3 : le résultant d'un polynôme et de sa dérivée est égal a

(9) $\mathbf{Res\,(f, f') = d_0^{n-1} \prod_i f'(\theta_i)}$

Preuve **[7],[8]**

Il existe une relation entre les 2 invariants Res (f , $f^{/}$) et dis (f)

Proposition 4 : soient f un polynôme de degré n et $f^{/}$ sa dérivée
Le Res (f , $f^{/}$) et dis (f) satisfont :

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

Preuve : [7],[8]

Exemple:
Polynôme cubique
$f(x) = x^3+2x^2-5x+3 \in IR[x]$;
La dérivée est égale à $f^{/}(x) = 3x^2+4x-5$;
ce la implique le résultant de f(x) et $f^{/}(x)$;
Res (f, $f^{/}$) est un déterminant d'ordre 3+2 =5 ;

$$\text{Res}(f, f^{/}) = \begin{vmatrix} 1 & 2 & -5 & 3 & 0 \\ 0 & 1 & 2 & -5 & 3 \\ 3 & 4 & -5 & 0 & 0 \\ 0 & 3 & 4 & -5 & 0 \\ 0 & 0 & 3 & 4 & -5 \end{vmatrix}$$

Avec les règles de calcul des déterminants, j'obtiens
Res (f, $f^{/}$) = 279

Le discriminant Δ (E) d'une cubique de Weierstrass
E : $y^2 = f(x) \in IR[x]$
est lié au discriminant du polynôme f(x) par la

Proposition 5 : **soit** ***une cubique de Weierstrass E : $y^2 = f(x)$; alors les discriminants Δ (E) de E et dis (f) de f satisfont:***
1) Δ (E) = 16 dis (f) lorsque $f(x) = x^3+a_2x^2+a_4x+a_6$
2) Δ (E) = 16 dis (f) lorsque $f(x) = x^3+Ax+B$
3) 16 Δ (E) = dis (f) lorsque $f(x) = 4x^3 + b_2x^2+2b_4x+b_6$

Preuve: *de* " $\Delta(E) = 16$ dis (f) lorsque $f(x) = x^3+a_2x^2+a_4x+a_6$ "
Le calcul de Δ (E) nécessite le calcul des invariants b_{2i} de la cubique
de Weierstrass $y^2 = x^3+a_2x^2+a_4x+a_6$:
$b_{2i} = 4a_2$, $b_4 = 2a_4$, $b_6 = 4a_6$, $b_8 = 4a_2a_6 - a_4^2$
Remplaçons ces invariants dans la formule (12) de discriminant ;nous obtenons le résultat

$\Delta(E) = 16\,(18\,a_2a_4a_6 - 4a_4^3 - 27a_6^2 - a_2^3a_6 + a_4^3)$

D'après les règles de calcul des discriminants des polynômes $f(x) \in IR[x]$
$disf(x) = 18\,a_2a_4a_6 - 4a_4^3 - 27a_6^2 - a_2^3a_6 + a_4^3$, lorsque $f(x) = x^3+a_2x^2+a_4x+a_6$
Nous obtenons $\Delta(E) = 16$ dis (f)

Preuve : de " $\Delta(E) = 16$ dis (f) lorsque $f(x) = x^3+a_2x^2+a_4x+a_6$ "
Avec le calcul des invariants b_{2i} de la cubique de Weierstrass
E : $y^2 = x^3+Ax+B$

Nous obtenons : $b_2 = 0$, $b_4 = 2A$, $b_6 = 4B$, $b_8 = B$
Cela implique $\Delta(E) = -16\,(4A^3 + 27B^2)$
Il en résulte $\Delta(E) = 16$ dis f(x)

Preuve : de "$16\,\Delta(E) =$ dis (f) lorsque $f(x) = 4x^3 + b_2x^2+2b_4x+b_6$ "
On utilise la théorie des résultant pour calculer le dis f (x)
dis f $(x) = 16\,(9b_2b_4b_6 - 8b_4^3 - 27b_6^2 - b_2^2b_8)$
D'où le résultat dis f $(x) = 16\,\Delta(E)$
□

Les cubiques de Weierstrass peuvent être classifiées par leur
discriminant $\Delta(E)$ et leur invariant $c_4(E)$.

Proposition 6 : Soit une cubique de Weierstrass
$E : y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6 \in K[x,y]$
de discriminant $\Delta(E)$ et d'invariant $c_4(E)$
Alors :
1) la cubique est singulière si et seulement si $\Delta(E) = 0$
2) elle admet un nœud si et seulement si $\Delta(E) = 0$ et $c_4(E) \neq 0$

3) elle admet un point de rebroussement si $\Delta(E) = 0$ et $c_4(E) = 0$

Preuve **:** 1) "la cubique est singulière " implique " $\Delta(E) = 0$ "
Par définition une cubique singulière admet un point singulier S , ce point à des coordonnées solutions du système :

$$f(x) = f'(x) = 0$$

Donc f et f' ont une racine commune
Le corollaire de la proposition 3 implique la valeur

$$\text{Res}(f , f') = 0$$

La relation entre Res (f , f') , dis (f) et $\Delta(E)$ implique $\Delta(E) = 0$

2) "E admet un nœud " implique " $\Delta(E) = 0$ et " $c_4(E) \neq 0$".
Prenons une équation de Weierstrass

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

L'hypothèse "E admet un nœud " implique que la cubique E est singulière
cela implique $\Delta(E) = 0$
Par définition d'un nœud la cubique E admet 2 tangentes distinctes en ce nœud, les pentes de ces tangentes sont égales à la dérivée y' de y

(2) $$\mathbf{y' = \frac{3x^2 - 27c_4}{2y} = \frac{3N(x)}{2y}} \quad \mathbf{; N(x) = x^2 - 9c_4}$$

Il en résulte que le polynôme N (x) qui admet 2 racines distinctes à un discriminant

(3) $$\text{dis}(N(x)) = 36\, c_4 \neq 0$$

(4) Il en résulte $c_4(E) \neq 0$

3) "E admet un point de rebroussement " implique " $\Delta(E) = 0$ et " $c_4(E) = 0$ "
Prenons l'équation (1) ,et la dérivée y' de la formule (2)

Par définition, au point de rebroussement, la cubique E une racine double.
Il en résulte $\text{dis}(N(x)) = 36\, c_4 = 0$
Donc $\Delta(E) = 0$ et $c_4(E) = 0$
□

Illustrons la proposition 6 par 2 exemples
Exemple 1 :
Cubique de Weierstrass :

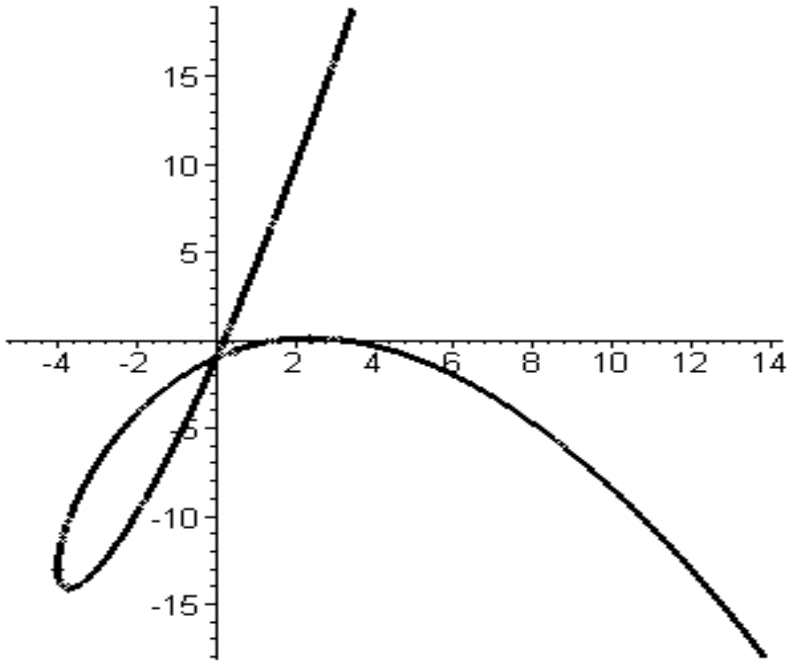
E : $y^2-6xy+2y = x^3-5x^2+6x -1$

Calcul des invariants
$b_2 = 16$, $b_4 = 0$, $b_6 = 0$, $b_8 = 0$, $c_4 = 16^2$ $\Delta (E_1) = 0$

La proposition 6 implique que la cubique E est singulière et admet un nœud
Intersection de la cubique avec les axes :

Pour x = 0, alors $y^2+2y+1= 0$ admet une racine double y =-1
Pour y = 0 alors x^3-5x^2+6x-1 les solutions avec le logiciel Mapple : pas de racines réels .
Il en résulte le nœud S = (0 , -1)

Tracé de la cubique :



$E_1 : y^2-6xy+2y = x^3-5x^2+6x -1$

Exemple 2 :
Cubique de Weierstrass d'équation :

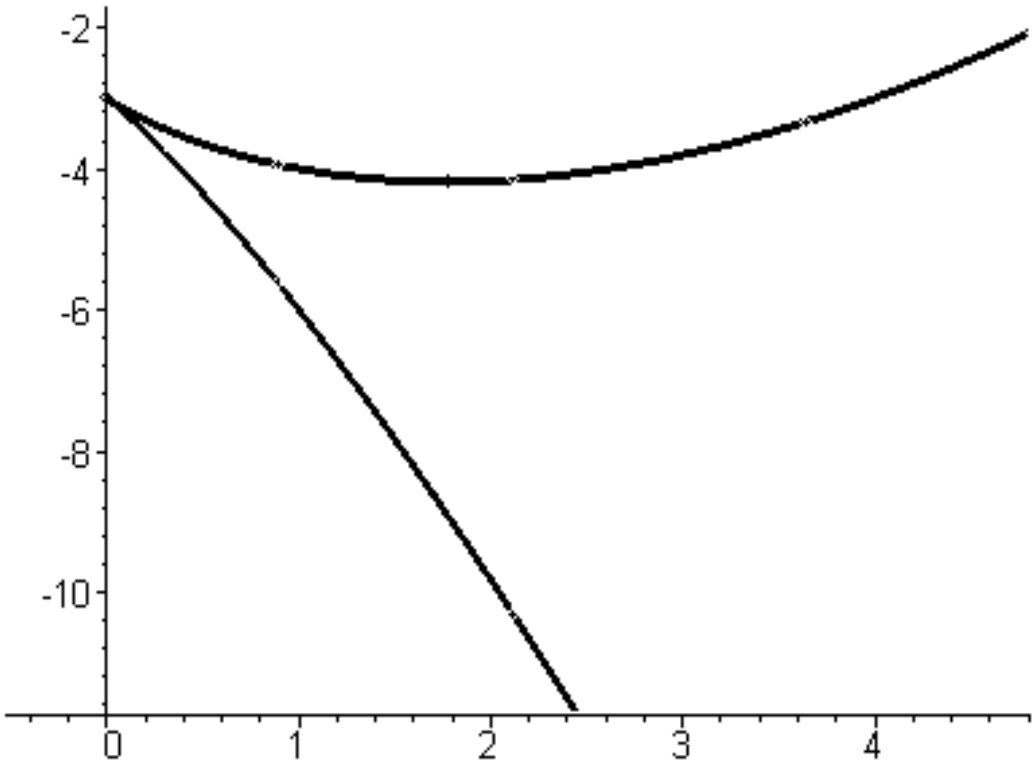
E_2 : y2 +4xy +6y = x^3 -4x^2 -12x-9
Calcul des invariants
$b_2 = 0$, $b_4 = 48$, $b_6 = 0$, $b_8 = 0$, $c_4 = 0$, $\Delta (E) = 0$

$c_4 = 0$, $\Delta (E) = 0$ la proposition 6 implique E_2 admet un point de rebroussement de coordonnées N = (0 , -3)

Intersection de la courbe avec les axes

x = 0 , alors y^2 +6y +9 = 0 une racine double y = -3
y = 0 , alors x^3 -$4x^2$ -12x-9 = 0 1 les solutions avec le logiciel Mapple : pas de racines réels .

Tracé de la courbe :



E_2 : $y2 +4xy +6y = x^3 -4x^2 -12x-9$

J'ai classifié l'ensemble des cubiques de Weierstrass singulières
Maintenant je classifie les cubiques de Weierstrass non singuliers, qui sont, d'après la définition 5 des Courbes Elliptiques

Proposition 7 :
Une cubique de Weierstrass

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

Est une courbe elliptiques si et seulement si $\Delta(E) \neq 0$

Preuve :
C'est un corollaire de la proposition 6
□

Puisqu'une équation cubique a coefficient réels irréductible admet 1 ou 3 racines réelles, il en résulte qu'une courbes elliptiques coupe l'axe Ox en 1 ou 3 points simples

Proposition 8: les Courbes Elliptiques sont classifiées en 2 classes

1) classe des courbes elliptiques qui coupent l'axe Ox en 3 points :
$\Delta(E) > 0$
2) classe des courbes elliptiques qui coupent l'axe Ox en un seul point simple :
$\Delta(E) < 0$

Preuve **:** 1) ''courbe elliptique qui coupe l'axe Ox en 3 points'' implique ''$\Delta(E)>0$''

Soit une courbe elliptique E qui coupe l'axe Ox en 3 points simples
$P_1 = (e_1, 0)$, $P_2 = (e_2, 0)$, $P_3 = (e_3, 0)$
Equation de Weierstrass de la forme :

$f(x) = (x - e_1)(x - e_2)(x - e_3) \in IR$ le discriminant du polynôme est égal à
$dis(f) = (e_1 - e_2)^2 (e_2 - e_3)^2 (e_3 - e_1)^2$

Les 3 racines e_i sont des nombres réels, il en résulte que les carrées $(e_i - e_j)^2$

de nombres réels sont positifs :

(1) $dis(f) > 0$
La formule (1) et la relation entre les discriminants de f et de E impliquent la relation :
$\Delta(E) > 0$

2)''une courbe elliptique coupe l'axe Ox en un seul point''implique ''$\Delta(E) < 0$''
Elle a une équation $y^2 = f(x) \in IR$
Elle coupe l'axe Ox en un seul point $P = (e, 0)$ qui est simple :
$y^2 = f(x) = (x - e)(x - e_1)(x - e_2)$
Donc les 2 racines e_1 et e_2 sont complexes conjuguées

Le discriminants du polynôme f (x) est égal à
dis (f) = $[(e - e_1)(e - e_2)(e_1 - e_2)]^2$

Avec le calcul nous obtenons la valeur :
dis (f) = $-4 s^2 [(e – r)^2 + s^2]^2$

Les carrés des nombres réels sont positifs.
Il en résulte l'inégalité :
dis (f) < 0

La relation entre les discriminants de f et de E implique la relation
Δ (E)< 0'':
□

Illustrons cette classification par un exemple de chaque classe

Exemple 1 :

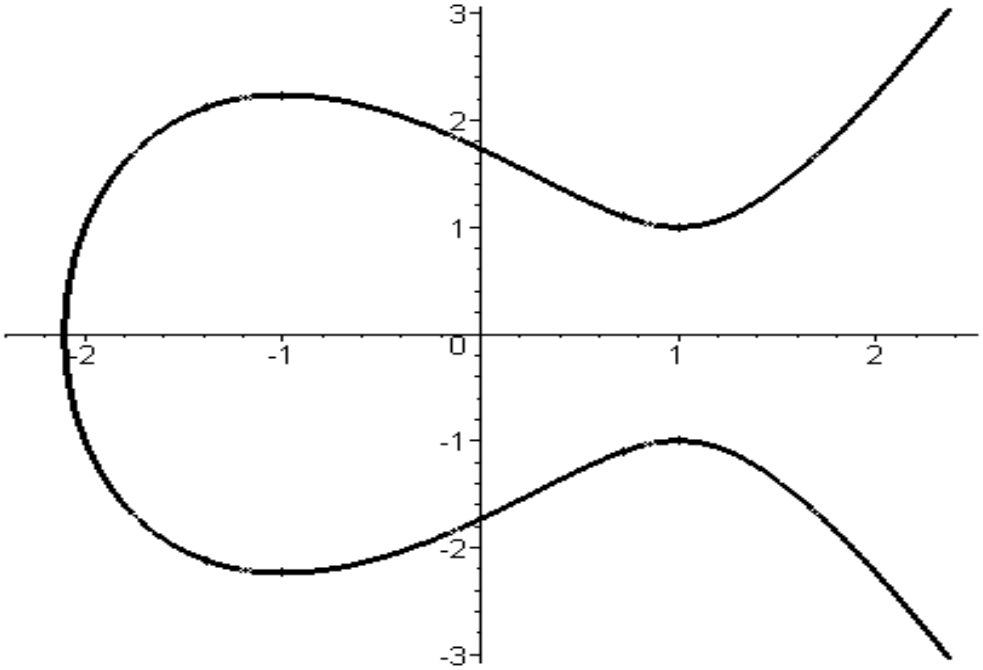
Soit la courbe elliptique d'équation

$$E : y^2 = x^3 - 3x + 3$$

Calcul du discriminant de E
$b_2 = 0$, $b_4 = -6$, $b_6 = 12$, $b_8 = 9$ et $\Delta (E) = -2160 < 0$

Donc la courbe coupe l'axe Ox en un seul point P , qui est simple

Tracé de la courbe E par le logiciel Maple :



$E : y^2 = x^3 - 3x + 3$

Exemple 2 :

Cubique de Weierstrass
$E_2 : y^2 = x^3 - 2x^2 - 22x + 8 = f(x) \in IR[x]$

Calcul du discriminant
$b_2 = -8$, $b_4 = -44$, $b_6 = 32$, $b_8 = -64$, $\Delta(E) = 759296 > 0$.
Donc la cubique E_2 est une courbe elliptique qui coupe l'axe Ox en 3 points simples (proposition 8)

Les solutions de l'équation diophantienne $f(x) = 0$ sont des diviseurs du terme constant (théorème)
Les diviseurs du terme constant 8 sont $d = \pm 1, \pm 2, \pm 4$ et ± 8

Avec le calcul nous obtenons une seule valeur

$f(-4) = 0$

Cela implique la factorisation du polynôme

$f(x) = (x+4)(x^2 - 6x + 2)$

ce polynôme admet 3 racines réelles
$e_1 = -4$, $e_2 = 3-\sqrt{7}$, $e_3 = 3 + \sqrt{7}$

Il en résulte les 3 points d'intersection de la courbe avec l'axe Ox

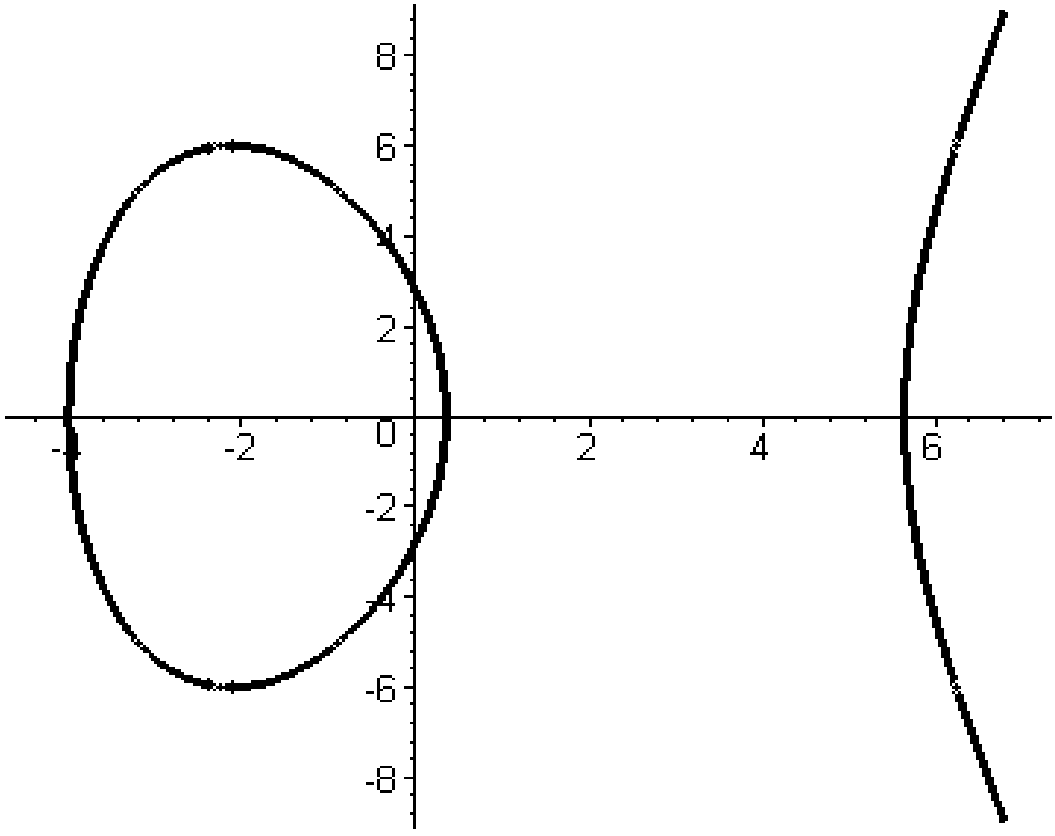
$P_i = (e_i , o)$, i =1,2,3 .

Tableau des coordonnées de quelques points de la courbe :

X	-5	-4	0
Y	Pas de racine réel	0	$2\sqrt{2}$ ou $-2\sqrt{2}$

La courbe E_2 admet l'axe Ox comme axe de symétrie.

Tracé de la courbe E_2 avec le logiciel maple :



$E_2 : y^2 = x^3 -2x^2 -22x +8$

1-Groupe de Mordell – Weil d'une courbe elliptique : [5],[11]
Pour obtenir un groupe, il faut un ensemble, un élément neutre et une loi de composition.

Proposition 1: soit l'ensemble E(K) des points K- rationnels d'une courbe elliptique E et le point à l'infinie $0_E = (\infty, \infty)$, alors l'application

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

De valeur $f(P_1 + P_2) = P_1 + P_2$
est une loi de groupe abélien d'élément neutre $0_E = (\infty, \infty)$
avec la règle géométrique de 3 points colinéaires de E

(1) $\mathbf{P_1 + P_2 + P_3 = 0_E = (\infty, \infty)}$

Vérifions les 4 axiomes d'un groupe abélien

Axiome de l'élément neutre (figure 1)

Le point $0_E = (\infty, \infty)$ dans le plan affine $IA^2(R)$; dans le plan projectif $IP^2(R)$ c'est le point $0_E = (0,1,0)$ il est déterminé par la direction unique de l'axe 0y

D'après la construction du plan projectif $IP^2(IR) = \{(x, y, z)\}$ a partir du plan affine $IA^2(IR) = \{ x, y \}$ et d'une relation d'équivalence.

(2) $\mathbf{P + 0_E + 0_E = P}$

Axiome du symétrique (figure 1)

La parallèle à 0y passant par le point P coupe la courbe E en un 2^{eme} point R qui satisfait la relation :

(3) $\mathbf{P + R + 0_E = 0_E}$

D'ou $R = - P$

Donc le symétrique du point P est ce point $R = - P$

Axiome de commutativité (figure 2)

La sécante P_1P_2 est confondue avec la sécante P_2P_1, cela implique :

(4) $\mathbf{P_1 + P_2 + P_3 = P_2 + P_1 + P_3 = 0_E}$

Axiome d'associativité :

Il n'est pas vérifiable géométriquement.

Cette vérification s'obtient par le calcul des sommes

$P + R = M$, $M + S = T_1$, $R + S = N$ et $P + N = T_2$

Cet ensemble E (K) des points K – rationnels d'une courbe elliptique est un groupe abélien dont le type à été conjecturé par Poincaré ; cette conjecture à été démontrée par Mordell _ Weil (Elliptic Curves –Diophantine Analyse chapitre IV , Lang)

Définition 1 : l'ensemble E (K) des points K – rationnels d'une courbe elliptique est le groupe de Mordell – Weil de E ; c'est un groupe abélien

Déterminons les coordonnées de certaines points

1- *Coordonnées du symétrique - P d'un point P = (x_p , y_p)*

Les points P et – P se trouvent sur une parallèle à l'axe 0y .
L'équation de cette parallèle est $x = x_p$; donc $x_{-p} = x_p$.
L'équation de Weierstrass de E devient :

$$y^2+a_1x_p\,y+a_3y = x^3_p +a_2x^2_p +a_4x_p+a_6 \quad \in K[x,y]$$

C'est une équation en y de degré 2 ; la somme de ses 2 racines est égale à
$y_p + y_{(-p)} = -(a_1x_p – a_3)$
Cela implique les coordonnées

(5) $\mathbf{x_{-p} = x_p}$ et $\mathbf{y_{(-p)} = y_p-a_1x_p-a_3}$

1-2 Coordonnées de la somme =P_1+P_2 de 2 points $P_1 \neq \pm P_2$(figure 2)

La règle géométrique des 3 points colinéaires de E implique la relation

$$P_2 + P_1 + P_3 = 0_E$$

Il en résulte la somme

$$P_2 + P_1 = - P_3 + 0_E = - P_3$$

Donc le point $M = P_1+P_2$ est le symétrique $- P_3$ du point P_3

L'équation de la sécante P_1P_2 égale à

(6) $\mathbf{y = t\,(x-x_1) + y_1}$ avec $\mathbf{t = (y_2-y_1) / (x_2-x_1)}$

L'équation de Weierstrass devient
$[t\,(x-x_1) + y_1]^2 + (a_1x + y)\,(t\,(x-x_1) + y_1) = x^3 + a_2x^2 + a_4x + a_6$
C'est une équation cubique en x de racines x_1 ; x_2 et x_3
La somme des 3 racines de cette équation cubique est une fonction symétrique élémentaire : $x_1 + x_2 + x_3$ = - coefficient x^2 / coefficient de x^3

Les coordonnées du point $M = P_1+P_2 = -P_3$ sont obtenues avec la formule
Du symétrique

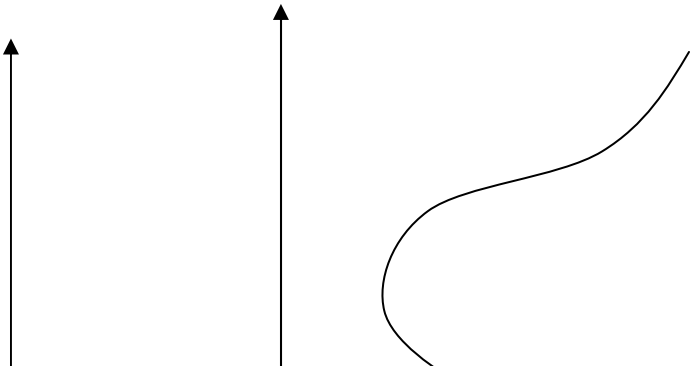
(7)
$$\begin{cases} \mathbf{X_M = t^2 + a_1t - a_2 - x_1 - x_2;} \\ \mathbf{Y_M = -t^3 - 2a_1t^2 + (2x_1 + x_2 - a_1^2 + a_2)t + a_1a_2 - a_3 - y_1 + a_1(x_1 + x_2)\ ;} \\ \mathbf{t = \dfrac{y_2 - y_1}{x_2 - x_1};} \quad \text{pour } x_1 \neq x_2 \end{cases}$$

1-3 Coordonnées de la somme P+P = 2P (figure 3)

La somme P+P = 2P d'un point P (x,y) est déterminée par la tangente à la cubique E au point P .
Avec l'équation de la tangente PT a la cubique E en P et la formule du symétrique

-T = 2P nous obtenons les coordonnées du point $2P = (x_{2p}, y_{2p})$ et
le coefficient y_p'

(8)
$$\begin{cases} \mathbf{x_{2p} = y_p'^2 + a_1y_p' - a_2 - 2x_p\ ;} \\ \mathbf{y_{2p} = y_p'^3 - 2a_1y_p'^2 + (3x_{p1} - a_1^2 + a_2)y_p' + a_1a_2 - a_3 - y_p + 2a_1x_p\ ;} \\ \mathbf{y_p' = \dfrac{3x_p^2 + 2a_1x_p + a_4 - a_1y_p}{2y_p + a_1x_p + a_3}\ .} \end{cases}$$



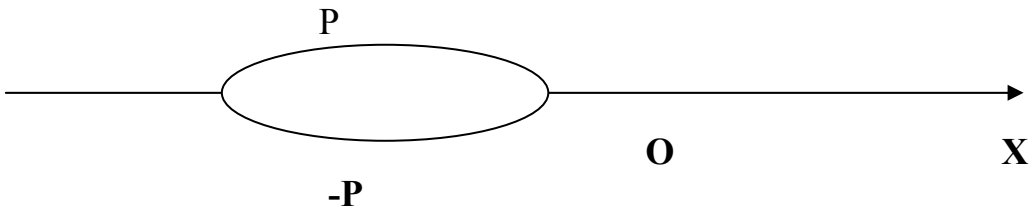


Figure 1 Symétrique -P

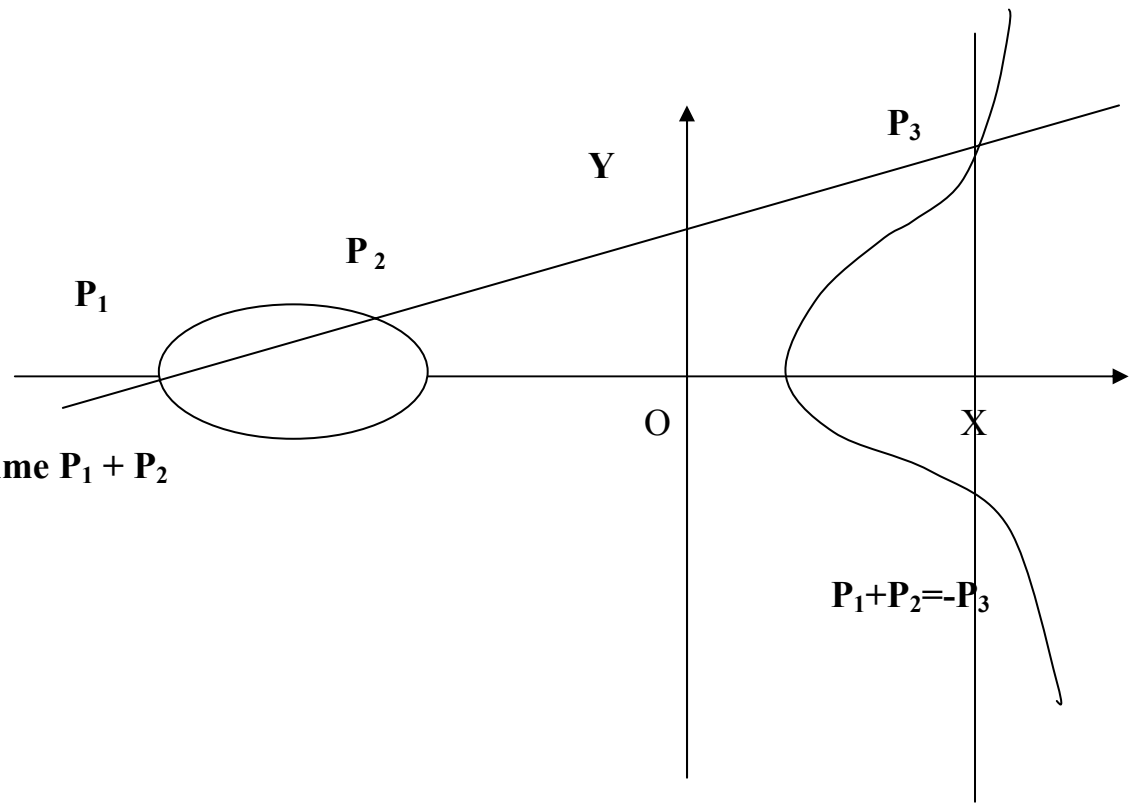
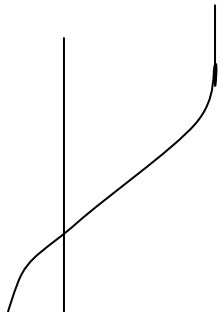


Figure 2 somme $P_1 + P_2$



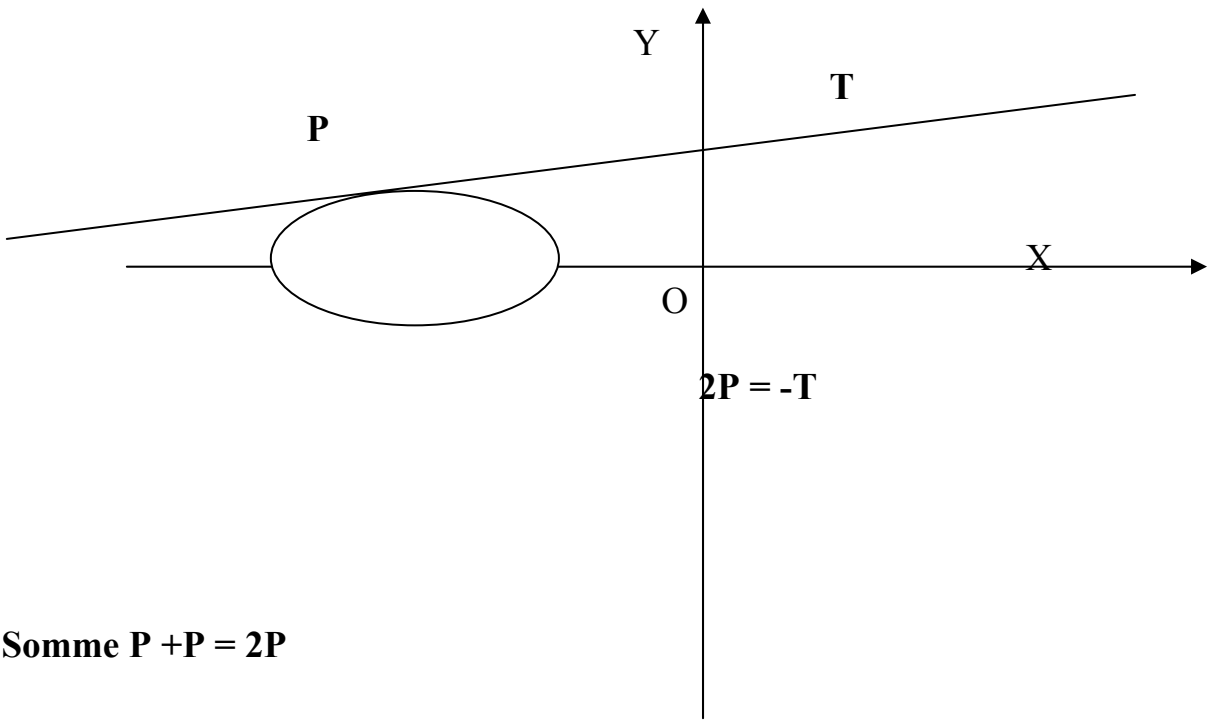


Figure 3 Somme P +P = 2P

Nous avons démontré la :

Proposition2 :soit une courbe elliptique E d'équation de Weierstrass

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

1) Les coordonnées du symétrique - P d'un point P = (x_p , y_p) sont égales à

$x_{(-p)} = x_p$ **et** $y_{(-p)} = y_p-a_1x_p-a_3$

2) Les coordonnées de la somme M = P_1+P_2 , pour P_i = (x_i , y_i) et $P_1 \neq \pm P_2$ sont égales à

$$\begin{cases} X_M = t^2 + a_1t - a_2 - x_1 - x_2 \\ Y_M = -t^3 - 2a_1t^2 + (2x_1 + x_2 - a_1^2 + a_2)t + a_1a_2 - a_3 - y_1 + a_1(x_1 + x_2) \\ t = \dfrac{y_2 - y_1}{x_2 - x_1} \quad \text{pour } x_1 \neq x_2 \end{cases}$$

3) les coordonnées de la somme P+P = 2P = (x_{2p}, y_{2p}) sont égale à

$$\begin{cases} x_{2p} = y_p'^2 + a_1 y_p' - a_2 - 2x_p \\ y_{2p} = y_p'^3 - 2a_1 y_p'^2 + (3x_{p1} - a_1^2 + a_2) y_p' + a_1 a_2 - a_3 - y_p + 2a_1 x_p \text{ et} \\ y_p' = \dfrac{3x_p^2 + 2a_1 x_p + a_4 - a_1 y_p}{2y_p + a_1 x_p + a_3} \end{cases}$$

□

Exemple :

Courbe elliptique E d'équation de Weierstrass

E : $y^2 - 3xy - 3y = x^3 - x^2 - 4x \in IR[x]$
Calcul des invariants de E
$b_2 = 5$; $b_4 = 1$; $b_6 = 9$, $b_8 = 11$, $c_4 = 1$, $\Delta(E) = -2065$

Les points P = (0,0) et R = (-2, 1) sont sur la courbe
Calculons les coordonnées des points –P , , 2P , P+R

La formule de coordonnées du symétrique de la proposition implique les coordonnées des points -P et – R
-P = (0,-3) , – R (-2 , -2)
La formule des coordonnées de la somme $M = P_1 + P_2$ de la proposition implique les coordonnées du point N = P + R
N = (39 /4 , -75/8)

Avec la formule des coordonnées de la somme 2P = P + P de la proposition j'obtient les coordonnées du point 2P pour P = (0,0)

La dérivée $y'' = \dfrac{3x^2 - 2x - 4 + 3y}{2y - 3x - 3}$ la valeur $y'_p = 4/3$ et le point
$2P = (x_{2p}, y_{2p}) = (11/9 , 622/27)$

2-Points d'ordre fini et formules de Cassels :[1]

Définition 2 : un point P d'ordre m d'une courbe elliptique E est un point qui satisfait la relation :

(1)
$$m\,P = 0_E \quad avec :$$
$$m\,P = P+P+P+\ldots+P \ , \ m \text{ fois } P \text{ si } m > 0$$
$$m\,P = (-P) + (-P) +\ldots+(-P) \ (-m) \text{ fois } (-P) \text{ si } m < 0$$
$$et\ 0P = 0_E = (\infty, \infty)$$

Les coordonnées des points 2P , 3P = 2P + P et 4P = 2 (2P)
sont des fonctions rationnelles

(2)
$$x\,(m\,P) = \frac{f_m(x,y)}{d_m(x,y)^2} \quad \text{et} \quad y(mP) = \frac{g_m(x,y)}{d_m(x,y)^3}$$

Cassels a obtenu les formules des coordonnées des points m P des courbes elliptiques particulières

Proposition 3: (lemme 7-2 "Équation Diophantine " Cassels) [1]
Soit une courbe elliptique E d'équation de Weierstrass :

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

Alors les coordonnées d'un point m P de la courbe elliptique E sont égales a

(3)
$$x\ (mP) = \frac{\Phi_m}{\Psi_m^2} \quad \text{et} \quad y\ (m\ p) = \frac{\omega_m}{\Psi_m^3}$$

Ψ_m, Φ_m et ω_m ***sont des polynômes de l'anneau Z [x,y,A,B] qui satisfont les relations***

(4)
$$\begin{cases} \Psi_{-1} = -1, \Psi_o = 0, \Psi_1 = 1, \Psi_2 = 2y \\ \Psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2 \\ \Psi_4 = 4Y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\ \Psi_{2m} = 2\Psi_m(\Psi_{m-2}\Psi_{m-1} - \Psi_{m+1}^2\Psi_{m+2}^2) \ ; \text{pour } m \geq 2 \\ \Psi_{2m+1} = \Psi_{m+2}\Psi_m^3 - \Psi_{m-1}\Psi_{m+1}^3 \ ; \text{ pour } \ m \ \geq 2 \\ \Phi_m = x\Psi_m^2 - \Psi_{m-1}\Psi_{m+1} \\ \omega_m = \Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2 \end{cases}$$

Preuve:

Pour m = -1 la formule du symétrique - (x, y) = (x, -y-a_1x-a_3) implique les valeurs : $\Psi_{-1} = -1$

Pour m = 0 alors 0 (x,y) = $(\infty,\infty) = (\frac{x}{0},\frac{y}{0})$ implique $\Psi_0 = 0$

Pour m = 1 alors 1 (x,y) = (x,y) implique $\Psi_1 = 1$

Pour m =2 alors 2(x,y) = (x_2,y_2) impliquent $\Psi_2 = 2y$

Pour les entiers m > 2 nous utilisons un raisonnement par récurrence sur m

□

Un point P d'ordre m est un point de m – torsion

L'ensemble E[m] des points de m- torsion est un sous groupe du groupe E/K

Définition 3:

1) le sous groupe de m - torsion du groupe E(K) de Mordell – Weil d'une courbe elliptique E est l'ensemble des points d'ordre m fini

E[m] =\{ P ∈ E(K) ; mP = 0_E \}

2) le groupe de torsion d'une courbe elliptique est la réunion infinie des sous groupes de m- torsion

$$T(E/K) = \bigcup_{m \in z} E(K)[m]$$

La structure du groupe de torsion des courbes elliptiques E sur le corps des nombres rationnels Q à été déterminer par MAZUR [9]

Théorème 1: le sous groupe de torsion T(E)(Q) d'une courbe elliptique E/K est isomorphe a l'un des 15 groupes abéliens finis

Z / d Z	***pour 1*** $\leq d \leq 10$ ***et d = 12***
Z / 2Z $\oplus$ ***Z / 2Z***	***pour 1*** $\leq d \leq$ ***4***

Preuve : **[9]**

□

Le groupe T(E) est un sous groupe du groupe de Mordell – Weil

La structure algébrique du groupe E(K) est précisée par le

Théorème 2 *: le groupe de Mordell – Weil E(K) d'une courbe elliptique E est abélien de type fini*

Preuve : selon Lang [8] **,**cette preuve est formée de 2 parties : dans l'une on montre que le groupe quotient E(K)/2E(K) est fini ;dans une autre on utilise la descente infinie et les fonctions hauteurs sur un groupe abélien

□

Définition ***4: [7],[8]*** ***une hauteur sur un groupe abélien A est une fonction h à valeurs réelles***

$$h : A \longrightarrow IR$$

qui satisfait les axiomes

h_1 : à tout point P_0 de A on associe une constante $c_1 = c_1 (P_0, A)$ telle que : $h (P_0, P) \leq 2 h (P) + c_1$ pour tout point P de A .

h_2 : à tout entier $m \geq 2$ on associe une constante $c_2 = c_2 (m, A)$ telle que $h (mP) \geq m^2 h (P) - c_2$ pour tout point P de A .

h_3 : pour toute constante c_3 l'ensemble des points P de A de hauteur bornée $\{ P, h (P) \leq c_3 \}$ est fini .

Supposons que le groupe quotient A/mA est fini.
Pour montrer que le groupe abélien A est de type fini nous utilisons les hauteurs sur ce groupe et la descente infinie .

Proposition 4:soit un groupe abélien A et un entier $m \geq 2$ tel que le groupe A/mA est de fini. Alors le groupe A est de type fini

Preuve soit un groupe quotient A/mA fini et des représentants des classe : $R_1, R_2, \ldots, R_r$ de A/mA
Dans le groupe abélien A, on considère une suite infinie de points $P_1, \ldots P_n, \ldots;$

$P = m P_1 + R_{1i}$, $1 \leq 1i \leq r$
Les points successifs $P_1, \ldots\ldots, P_n$ sont des combinaisons linéaires
$P_1 = m P_2 + R_{2i}$; $P_{j-1} = m P_j + R_{ij}$; $P_{n-1} = m P_n + R_{in}$

Cette suite infinie de points est une ‘’ descente infinie ‘’ selon Fermat.
On introduit une hauteur $h : A \longrightarrow IR$
Soit la relation :

(1) $\mathbf{mP_{n+1} = P_n - R_{n+1}}$

Appliquons l'axiome 2 à gauche et l'axiome (1) à droite
Nous obtenons les inégalités :

$m^2\, h\,(P_{n+1}) - c_2 \le 2\, h\,(P_m) + c_1$
$m^2\, h\,(P_{n+1}) - c_2 \le 2\, h\,(P_n) + c_n^{/}$

L'hypothèse $m \ge 2$ implique

$h\,(P_{n+1}) = \frac{2}{m^2}\, h\,(P_n) + \frac{c_n'}{m^2} \quad 1 \le n \le N$

Pour $n = 1$, $h\,(P_1) \le \frac{2}{m^2}\, h\,(P) + \frac{c_1'}{m^2}$

Pour $n = 2$, $h\,(P_2) \le \frac{2}{m^2}\, h\,(P_1) + \frac{c_2'}{m^2}$

Pour $n = 3$, $h\,(P_1) \le \frac{2}{m^2}\, h\,(P_2) + \frac{c_3'}{m^2}$

Pour $n = N$, $h\,(P_N) \le \frac{2}{m^2}\, h\,(P_{N-1}) + \frac{c_N'}{m^2}$

En additionnant membre à membre ces inéquations nous obtenons l’inégalité :

(1) $h\,(P_N) \le U_N\, h\,(P) + c\,(\frac{1}{m^2} + \frac{1}{m^4} + \ldots + \frac{1}{m^{2N}})$

avec $\lim_{N \longrightarrow \infty} u_N = 0$

Dans (1) le facteur de c est égal à : $\frac{1}{1-u} = 1 + u + u^2 + \ldots ; u = \frac{1}{m^2}$
Il en résulte que l'ensemble des points P_i est fini
$\{ P_1, P_2, \ldots, P_d \}$

Tout point P du groupe abélien A est une combinaison Z/- linéaire
$P = n_1 R_1 + \ldots + n_r R_r + n_{r+1} P_1 + \ldots + n_{r+d} P_d$; $n_i \in Z/$
Donc le groupe abélien A est de type fini.
□

La procédure de descente infinie a été inventée sans doute Fermat d'arithmétiques.

Exemple :
Montrer que le nombre $\sqrt{5}$ n'est pas rationnel.
Supposons $\sqrt{5}$ rationnel.
(1) Alors $\sqrt{5}$ = a / b, a et b entiers rationnels entre eux

En élevant au carré, nous obtenons
(2) $a^2 = 5\, b^2$
Dans (2) , 5 drive a ; donc :
$a = 5\, a_1$ et (2) implique :
(3) $b^2 = 5\, a_1^2$
(4) Dans (3) , 5 divise b : $b = 5\, b_1$

Nous obtenons 2 suites ''infinies '' décroissantes
$a = 5\, a_1$; $a_1 = 5a_2$; $a_2 = 5a_3$; … ; $a_n = 5a_{n+1}$
$b = 5\, b_1$; $b_1 = 5\, b_2$; $b_2 = 5\, b_3$; … ; $b_n = 5\, b_{n+1}$

A la limite a_n et b_n sont égaux
Donc $\sqrt{5}$ = 5 , résultat absurde
D'où $\sqrt{5}$ n'est pas rationnel.

Pour le groupe abélien de Mordell – Weil , il existe plusieurs hauteurs possibles selon la valeur de l'image h (P) : hauteur logarithmique , hauteur de Weil , hauteur canonique , hauteur de Néron – Tate ; hauteurs locales ; etc. …

La décomposition de ce groupe abélien est précisée par la :

Proposition 5 : le groupe abélien E(K) de Mordell _ Weil est isomorphe à un produit de groupes abéliens

$$E(K) \cong T(E) \times Z/^r$$

Où T(E) = le groupe de torsion, qui est fini
$Z/^r$ = r copies du groupe abélien additif infini Z/

□

Cet isomorphisme implique un invariant des courbes elliptiques.

Définition 5 : ***cet entier r = r (E) ≥ 0 est le rang de la Courbe Elliptique E Il est égal au nombre de points P ∈ E (K) d'ordre infini et linéairement indépendants qui engendrent la partie infinie E(K) – T(E)du groupe E(K).***

Cette formule ne permet pas de calculer le rang d'une courbe elliptique.

Homomorphismes des courbes elliptiques : [14],[11],[9],[1],[10],[12],[3],[8]

Il s'agit des homomorphismes des groupes abéliens E (K) de Mordell – Weil des courbes elliptiques .
Ce sont des isomorphismes, des automorphismes des endomorphismes usuels de théorie des groupes .
Les homomorphismes spécifiques aux courbes elliptiques sont des isogénies et

des twists
Ces notions ont fait l'objet de travaux de recherche de plusieurs spécialistes : Silverman [14] , Mazur [9], Cassels [1],Shimura [13], Lang [8] Shafarevish , [12] Tate [15] , etc.

1) Isomorphismes de courbes elliptiques :

Ils sont déterminés par des changements de variables particuliers

Proposition 1: soit le groupe de mordell _ Weil E (K) d'une courbe elliptique E et son point à l'infini 0_E ; alors l'application :

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

(1) ***de valeur : $f(x , y) = (u^2X+r , u^3Y+su^2X+t)$***

avec $u \neq 0$ et $r , s\ t \in K$
est un isomorphisme de courbes elliptiques

Preuve :
Considérons une courbe elliptique E d'équation de Weierstrass

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

Sa transformée par f est la courbe f (E) = E′ d'équation de Weierstrass

(2) $E^{/}: Y^2 + a_1' XY + a_3' Y = X^3 + a_2' X^2 + a_4' X + a_6' \in K[x, y]$

Pour vérifier les formules d'isomorphisme de groupes il faut comparer l'image f (P+R) de la somme de 2 points et la somme f (P) + f (R) des images ;
L'image du point neutre 0_E est égale à f ((∞ , ∞)) = (∞ , ∞) = 0_E

Les coordonnées X et Y sont égales à :

$X = (x - r) / u^2$ et $Y = (y - sx - sr + t) / u^3$

L'hypothèse $u \neq 0$ implique une solution unique (X ,Y)
Le noyau est réduit à l'élément neutre $0_{E/}$
□

2- Relations entre coefficients et invariants de 2 courbes isomorphes E et E'

***Corollaire :** soit l'isomorphisme de la proposition 1 alors les coefficient a_i , b_i , c_i de E et a_i' , b_i' , c_i' de E'*

$$u\, a_1' = a_1 + 2s \quad ; \quad u^2\, a_2' = a_2 - s a_1 + 3r - s^2 \qquad \textbf{(I s - 1)}$$
$$u^3 a_3' = a_3 + r a_1 + 2t$$

$$u^4 a'_4 = a_4 - s a_3 + 2r a_2 - (t + rs) a_1 + 3r^2 - 2st \quad ,$$
$$u^6 a'_6 = a_6 + r a_4 + r^2 a_2 + r^3 - t a_3 - t^2 - rt a_1$$

$$u^2 b'_2 = b_2 + 12r$$
$$u^4 b'_4 = b_4 + r b_2 + 6r^2 \quad ,$$
$$u^6 b'_6 = b_6{}^2 + 2r b_4 + r^2 b_2 + 4r^3 \qquad (\text{Is } -2)$$
$$u^8 b'_8 = b_8 + 3r b_6 + 3r^2 b_4 + r^3 b_2 + 3r^4$$

$$u^4 c'_4 = c_4 \qquad (\text{Is } -3)$$
$$u^6 c'_6 = c_6$$

les invariants de E et E′ satisfont

$$u^{12} \Delta(E') = \Delta(E) \qquad (\text{Is } -4)$$
$$j(E') = j(E) \qquad (\text{Is - 5})$$
$$\omega(E') = u\ \omega(E) \qquad (\text{Is - 6})$$

Preuve :

Il faut remplacer x et y par leurs valeurs
En appliquant les formules des invariants b_{2i} , c_{2i} , Δ (E) , j (E) nous obtenons les relations (I s - 1) à (I s - 6)
□

La relation (I s - 5) permet de classifier les courbes elliptiques E(K) par leurs invariants modulaires j (E)

Proposition 2 : deux courbes elliptiques E/ K et E′ / K sont K _ isomorphes si et seulement si leurs invariants modulaires sont égaux

Preuve :
Soient 2 courbes elliptiques E/ K et E′ / K isomorphe alors par le corollaire précédent la relation (I s - 5) implique j (E) = j (E′)
□

Proposition 3 : pour tout nombre t ∈ K il existe une classe de courbes elliptiques E d'invariant modulaire j (E) = t

Preuve :
Pour t = 0 , nous prenons une courbe E d'équation de Weierstrass ;

$$E : \quad y^2 + y = x^3$$

Calcul des invariants :
La courbe E d'équation de Weierstrass : $E : y^2 + y = x^3$ a des invariants égaux à

$$\Delta (E) = - 27 \quad \text{et} \quad j (E) = 0$$

Selon Silverman [14] , la courbe elliptique E d'équation de Weierstrass

$E (t) = y^2 + xy = x^3 - \frac{36}{t-1728} - \frac{1}{t-1728}$ pour $t \neq 0 , 1728$
a pour invariants

$$\Delta (E) = \frac{t^2}{(t-1728)^3} \qquad \text{et } j (E) = t$$

Donc les Courbes Elliptiques E et E' sont isomorphes

Exemple 1:
Courbe elliptique E d'équation de Weierstrass
$E : y^2 + 3xy - 6y = x^3 + 4x^2 - 5x + 2 \in Q [x , y]$

Calcul des invariants :
$b_2 = 25$, $b_4 = - 28$, $b_6 = 44$, $b_8 = 79$, $c_4 = 601$
$\Delta (E) = -203231$, $j (E) = - (601)^3 / 203231$

Soit l'isomorphisme de formules
$x = u^2X+r$ et $y = u^3Y+su^2X+t$ avec $u = -2/3$, $r = 5/3$, $s = 2$ et $t = 4 /3$

Calcul des coefficients de la courbe isomorphe E'

$a'_1 = -21 / 2$, $a'_2 = - 9 / 4$, $a'_3 = -45/8$, $a'_4 = - 189 / 4$, $a'_6 = 3267/ 32$

$b'_2 = 405 /4$, $b'_4 = 2457 /16$, $b'_6 = 28161/64$, $b'_8 = 10833669 /1024$

$c'_4 = 105057 / 16$

Équation de la courbe $E^{/}$ isomorphe à E

$E^{/} = Y^2 + -21 / 2XY - 45/8\ Y = X^3 - 9 / 4X^2 + 189/4\ X + 3267/32 \in Q[x, y]$

Calcul des invariants

$\Delta(E^{/}) = -7403778725212791/16384$ et $j(E^{/}) - (601)^3 / 203231 = j(E)$

Exemple 2 :

Courbe elliptique d'équation de Weierstrass

$E : y^2 = x(x-1)(x+9)$

Calcul des invariants

$b_2 = 32$, $b_4 = -18$, $b_6 = 0$, $b_8 = -81$

$\Delta(E) = 3^2 293$, $j(E) = 2^7 7 / 5^2$

Déterminons la courbe $E^{/}$ isomorphe à E par l'isomorphe

$x = 2^2 X - 1$ et $y = 2^3 Y - 5(2^2) X + 3$

Calcul des invariants de la courbe isomorphe $E^{/}$

$a^{/}_1 = -5$, $a_2^{/} = 5$, $a^{/}_3 = 3/4$, $a_4^{/} = 13/8$, $a^{/}_6 = -11/26$

Courbe Elliptique isomorphe

$E^{/} = Y^2 + -5XY + 3/4\ Y = X^3 + 5X^2 + 13/8\ X - 11/2^6 \in Q[x, y]$

Avec les relations d'isomorphismes nous obtenons les invariants :

$\Delta(E^{/}) = 3^2 \times 293 / 2^{12}$; $j(E^{/}) = 2^7 \times 7 / 5^2 = j(E)$

2– *Automorphismes de courbes elliptiques :*

Par la théorie des groupes, les automorphisme d'un groupe A forme un groupe Aut (E)

La structure du groupe Aut (E) d'une courbe elliptique E / K dépend de la Caractéristique du corps K et de la valeur de l'invariant modulaire j (E) .

Proposition 4:

Soit une courbe elliptique E d'invariant modulaire j (E) ; alors le groupe Aut (E) des automorphismes de E est d'ordre n .

n = 2 si j(E) ≠ 0 , 1728
n = 4 si j(E) = 1728 et carac (K) ≠ 2 ,3
n = 6 si j(E) = 0 et carac (K) ≠ 2 ,3
n = 12 si j(E) = 0 et carac (K) = 3
n = 24 si j(E) = 0 , 1728 et carac (K) = 2
□

Preuve :

Pour j(E) ≠ 0 , 1728
Nous prenons une courbe elliptique d'équation de Weierstrass E
E : $y^2 = x^3 + A\,x + B \in K[x , y]$, $4A^3 + 27B^2 \neq 0$, $A , B \neq 0$
L'automorphisme E (Q) ⟶ E (Q) ; $x = u^2 X$ et $y = u^3 Y$
Transforme E en E' d'équation de Weierstrass
$E' : Y^2 = X^3 + A\,u^2 X + B\,u^6$

Cela implique $A\,u^2 = A$, $B\,u^6 = B$ et $u^{12}\,\Delta(E') = \Delta(E)$
Nous en déduisons l'équation $u^2 = 1$; elle admet 2 solutions $u = \pm 1$

Cela implique le groupe Aut (E) est d'ordre n = 2 .

2) Preuve pour j (E) = 1728 et carac (K) ≠ 2, 3
La courbe elliptique E a pour invariant modulaire
$j(E) = 1728\,(4A)^3 / -16(4A^3 + 27B^2)$

L'hypothèse j (E) = 1728 implique B = 0 et A ≠ 0
L'automorphisme $x = u^2 X$ et $y = u^3 Y$ implique l'équation
$u^4 = 1$, qui admet 4 solutions
Donc Aut (E) est d'ordre n = 4 .

3) Preuve pour j (E) = 0 et carac (K) ≠ 2 , 3
L'hypothèse j (E) = 0 implique A = 0 , B ≠ 0 .
La courbe elliptique E' devient
$y^2 = x^3 + B$
Il en résulte l'équation : $u^6 = 1$ qui admet 6 solutions
Il en résulte que Aut (E) est d'ordre n = 6 .

4) Preuve de j(E) = 0 = 1728 et carac (K) = 3
Les courbes elliptiques isomorphes ont même équation de Weierstrass

$E' = E_1 = y^2 = x^3 + a_4 x + a_6$ et $Y^2 = X^3 + a'_4 X + a'_6$. $a_4 , a'_4 \neq 0$
Nous prenons l'isomorphisme :
(1) $x = u^2 X + r$ et $y = u^3 y$

Nous obtenons 2 équations

(2) $u^4 = 1$ et $r^3 + a_4 r + (1-u^2)\, a_6 = 0$

Le nombre des automorphismes (1) est égal au nombre de paires (u , r) solutions d'équations (2)
Il a 12 paires (u , r) ; donc Aut (E) est d'ordre n = 12 .

Preuve pour j (E) = 0 = 1728 et carac (K) = 2

Les 2 hypothèses sont réalisées par la courbe elliptique d'équation de Weierstrass

(1) $E_1 : \quad y^2 + a_3 y = x^3 + a_4 x + a_6$ avec $a_3 , a_4 , a_6 \neq 0$

L'automorphisme

(2) $x = u^2 X + s^2$ et $y = u^3 Y + s u^2 X + t$

(3) $E_2 : \quad y^2 + a'_3 y = x^3 + a'_4 x + a'_6$

Les relations entre les coefficients de 2 courbes elliptiques isomorphes impliquent les 3 équations :

(4) $u^3 = 1 , \quad s^4 + a_3 s + (1 - u)\, a_4 = 0$ et $t^2 + a_3 t + s^6 + a_4 s^2 = 0$
Le nombre des automorphismes (3) est égal au nombre de triplets (u, s, t) solutions des 3 équations (4) .
Nous obtenons $3 \times 4 \times 2 = 24$ triplets.

Donc Aut (E) est d'ordre 24 .

Ce groupe Aut (E) est isomorphe au produit d'un un groupe cyclique C_3 d'ordre 3 par le groupe des groupe des quaternions H_8 d'ordre 8

$$\text{Aut (E)} \approx C_3 \times H_8$$

□

Exemple 1

Courbe elliptique d'équation de Weierstrass :

$E_1 : y^2 = x^3 + x + 1 \in IF_3 [x , y]$, IF_3 = corps fini a 3 éléments = {0,1,2}

La caractéristique du corps de base est égale à 3
Avec le calcul nous obtenons $j(E) = 0$, $\Delta(E) = 0$

Il en résulte que l'ordre de Aut (E) n est égal à 12

Exemple 2

Courbe elliptique d'équation de Weierstrass :

$E_2 : y^2 + y = x^3 + x^2 + 1 \in IF_2 [x , y]$; IF_2 = {0,1} corps fini à 2 éléments

La caractéristique du corps de base est égale à 2
Avec le calcul nous obtenons $j(E) = 0$ et $\Delta(E) = 1$

Il en résulte que l'ordre de Aut (E) n est égal à 24

3- Anneau des endomorphismes des courbes elliptiques

Soit une courbe elliptique E de groupe de Mordell – Weil E (K) ; ce groupe est abélienne de type fini

Les endomorphismes

$f : E(K) \longrightarrow E(K)$, forment un anneau End (E) avec les 2 lois

$f, g \in End(E)$:

$f \circ g (P) = f (g (P))$; la composition des applications

$(f+g) (P) = f (P) + g (P)$, $Id (P) = P$ pour l'éléments neutre

Selon Silverman [14] , l'anneau des endomorphismes End (E) a été déterminé complètement par Deuring dans " Die Typen der Multiplikats renringe elliptishes Funktionen Köper " Abh . Maths Séminaire .
Hambourg 14 (1941) ,197 – 272 .

Proposition 5:

L'anneau End (E) des endomorphismes d'une courbes elliptique E est isomorphe à l'anneau Z/ , ou à un ordre d'un corps quadratique imaginaire, ou à un ordre de l'algèbre des quaternions

Preuve : [14] corollaire 9, 4

□

Définition1:

(selon Silverman [14]) un ordre d'un corps quadratique imaginaire K = Q($\sqrt{-d}$) , d > 0 est un sous anneau O(f) = Z/ + f A (K) ou f est un entier > 0 et A (K) est l'anneau des entiers du corps K ; f est le conducteur de l'ordre O (f)

Lorsque le corps K est un corps fini de caractéristique p > 0 , alors l'anneau des endomorphismes End (E) est un ordre d'un corps quadratique imaginaire, ou un ordre de l'algèbre des quaternions

Définition 2:

lorsque l'anneau End (E) est isomorphe à un ordre d'un corps quadratique Q ($\sqrt{-d}$) , la courbe elliptique est une courbe à Multiplication complexe

Une description précise se trouve dans [14], appendice C paragraphe 11
Baker , Heegner et stark ont prouvé qu'il y a exactement 9 corps quadratiques imaginaires K = Q ($\sqrt{-d}$), de nombre de classe h (K) ce sont les corps pour les 9 valeurs

d = 1, 2, 3, 7, 11, 19, 43, 67, et 163

L'ordre de K de conducteur f = 2 est obtenu pour d = 1, 3 et 7
L'ordre de K de conducteur f = 3 est obtenu pour d = 3

Cela implique 13 courbes elliptiques E / Q qui sont à Multiplication Complexe

Exemple :
Multiplication complexe par le nombre complexe i

$$m_i : E(K) \longrightarrow E(K)$$
$$(x , y) \longrightarrow (-x , iy)$$

E **:** $y^2 = x^3 - x$, $E' :$ $y^2 = x^3 - x$

Alors $m_i (E) = E$; c'est donc un automorphisme de E (Q)
d'ordre 4 **:** $\{ i , i^2, i^3, i^4 = 1 \}$ L'anneau End (E) est isomorphe à l'ordre Z/ [i] Cela implique le groupe Aut E ≈ Z/ [i] est un groupe cyclique

4- Isogénies de courbes elliptiques :

La théorie des isogénies des courbes elliptiques se trouve dans plusieurs ouvrages. Citons [1], part II, 8 de Cassels, [13], chapiter 4 de Shimura, [16] de Velu, [14] III-4 de Silverman, etc…

Définition 3 : Une isogénie de 2 courbes elliptiques E_1/K et E_2/K est un homomorphisme de leurs groupes de Mordell-Weil :

$$\lambda : E_1(K) \longrightarrow E_2(K)$$

Qui satisfait les 4 conditions :

1) ***λ n'est pas nul ;***
2) ***Le noyau de λ est un sous groupe fini du groupe $E_1(K)$;***
3) ***λ est surjectif ;***
4) ***$\lambda(0_1) = 0_2$ et $\lambda(P + R) = \lambda(P) + \lambda(R)$ pour les points à l'infini $0_1 = (\infty,\infty)$ de E_1, $0_2 = (\infty,\infty)$ de E_2 et tous points P, R de E_1.***

Cet homomorphisme n'est donc pas injectif. Par la théorie des groupes, le noyau F d'un homomorphisme surjectif f : A $\longrightarrow$ B implique un isomorphisme de groupes A/F $\longrightarrow$ B.

Proposition3 :
Soit une courbe elliptique E/K et un sous groupe fini F du groupe E(K). Alors il existe une isogénie unique

$$\lambda : E(K)/F \longrightarrow E(K)$$

De noyau F.

□

Toute isogénie de courbes elliptiques possède un invariant.

Définition 4 : Le degré d'une isogénie $\lambda : E_1(K) \longrightarrow E_2(K)$ est égal à l'ordre de son noyau.

Exemple : La multiplication par un entier rationnel m sur E(K) :

$$\Pi_m : E(K) \longrightarrow E(K) \text{ , } \Pi_m(P) = mP$$

Son noyau est déterminé par la :

Proposition 4 :([1], Lemma 7-2, corollary)
La multiplication par un entier rationnel m > 1 sur une courbe elliptique E est une isogénie de degré m^2.

□

Preuve :

Soit une courbe elliptique E/Q d'équation de Weierstrass :

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

Pour tout entier rationnel m>2, les coordonnées du point mP, pour tout point $P = (x,y) \neq 0_E$ sont déterminées par les formules de Cassels :

$$x(mP) = f_m / \alpha_m^2 \quad \text{et} \quad y(mP) = g_m / \alpha_m^3.$$

$f_m = f_m(x,y)$ et $g_m = g_m(x,y)$ sont des polynômes en x de degré m^2.

□

La notion de degré d'un morphisme de courbes algébriques :

$$f : C_1/K \longrightarrow C_2/K$$

est liée au degré d'extension de corps :

$$\deg(f) = [K(C_1) : f^*K(C_2)]$$

Pour les détails, consulter [14],II.

Cette notion de degré s'applique donc au degré d'une isogénie de courbes elliptiques.

Chaque isogénie de courbes elliptiques possède une isogénie duale.

Définition 5 : L'isogénie duale d'une isogénie de degré d

$$\lambda : E_1(K) \longrightarrow E_2(K)$$

est l'homomorphisme :

$$\hat{\lambda} : E_2(K) \longrightarrow E_1(K)$$

Tel que la composée :

$$\lambda \circ \hat{\lambda} : E_2(K) \longrightarrow E_2(K) \text{ est la multiplication par } d$$

Proposition 5 :
Soit 2 isogénies de courbes elliptiques :

$\lambda : E_1(K) \longrightarrow E_2(K)$ *et* $\psi : E_2(K) \longrightarrow E_3(K)$

Et leurs isogénies duales :

$\hat{\lambda} : E_2(K) \longrightarrow E_1(K)$ *et* $\hat{\psi} : E_3(K) \longrightarrow E_2(K)$.

Alors la composée ψ o λ est une isogénie de $E_1(K)$:

1) ***son isogénie duale est égale à :***

$$\psi o \lambda := \hat{\lambda} \, o \, \hat{\psi}$$

2) ***les isogénies duales de $\hat{\lambda}$ et de $\hat{\psi}$ sont égales à :***

$$\hat{\hat{\psi}} = \psi \quad et \quad \hat{\hat{\lambda}} = \lambda.$$

□

Il y a une isogénie classique particulière qui se trouve dans [14] III – Exemple 4-5.
Soit 2 courbes elliptiques d'équations de Weierstrass :

$E_1 : y^2 = x^3 + ax^2 + bx \in K[x]$, carac(K) $\neq 2$, $a^2 - 4b \neq 0$;

$E_2 : Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X \in K[X]$;

Ces 2 courbes sont isogènes par une isogénie de degré 2.

$f : E_1(K) \longrightarrow E_2(K)$, $f(x,y) = \left(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right)$;

et la duale :

$\hat{f} : E_2(K) \longrightarrow E_1(K)$, $\hat{f}(X,Y) = \left(\frac{Y^2}{4X^2}, \frac{Y(a^2 - 4b - X^2)}{8X^2} \right)$.

Citons quelques publications parmi celles qui concernent les isogénies de courbes elliptiques.

1- ″Isogenies of prime degre over ″, Compos. Maths: 97(1995)329-348 par Momose;
2- ″ Estimating isogenies on Elliptic Curves″, Invent. Math.100(1990)1-24 par Masser et Wüstholz;
3- ″ A construction of evrywhere good Q-curves with p-isogeny″ Tokyo Journal Math, Vol21,n° 1(1998) 183-200, par Umekagi
4- ″ Algorithms for computing isogenies betwen Elliptic Curves″, (1996) 1-14 , par Lercier et Morain(INRIA).
5- ″ Schoof's algorithm and isogeny cycles″, (1995) 1-16 par couveigne et Morain(INRIA).
6- ″ Isogénies entre courbes elliptiques″, compte rendu de l'Académie des Sciences, Paris, série A (26 juillet 1971)238-241 par Velu.

C'est cette dernière que nous allons exploiter.
Construction d'isigénies de Courbes Elliptiques par la méthode de Velu.
Cette méthode utilise des valuations .
Une valuation d'un corps K est une application

$$V : K \longrightarrow IR$$

Qui satisfait les 3 conditions :

1) $v(x) = 0$ si et seulement si $x = 0$;
2) $v(xy) = v(x)+v(y)$ pour tous éléments x,y de K ;
3) $v(x + y) \leq v(x) + v(y)$ pour tous x,y de K.

La condition (3) est ″ l'inégalité triangulaire″.

A tout point P = (x,y) d'une courbe elliptique E/K on associe une valuation v_p sur le corps K(E) des fonctions x,y sur K.
Considérons les valuations v_0 et v_p telles que

(1) $v_0(x) = - 2$; $v_0(y) = -3$ et $(y^2/x^2)(0) = 1$.
(2) $V_p(x) \geq 0$ et $v_p(y) \geq 0$ pour tout point $P \neq 0$; Ce point 0 peut être le point à l'infini $0_E = (\infty,\infty)$ de E.
(3) Posons $z = -x/y$ alors la x et y sont des fonctions de z ; $v_0(z) = 1$
(4) $x = 1/z^2 = A_1/z – A_2 – A_3z – A_4z^2 – A_5z^3 - \ldots$

(5) $y = - x/z = -1/z^3 + A_1/z^2 + A_2/z + A_3 + A_4z + A_5z^2 + \ldots$

(4) et (5) impliquent l'équation cubique de Weierstrass

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

Les coefficients A_i et a_i sont liés par les relations :

(7) $A_1 = a_1$; $A_2 = a_2$, $A_3 = a_3$;
$A_4 = a_1a_3 + a_4$, $A_5 = a_2a_3 + a_1^2 a_3 + a_1a_4 + \ldots$

(8) Les A_i sont des ″polynômes homogènes de degré i″ de l'anneau $Z/ [a_1,a_2,a_3,a_4,a_6]$.

Dans le chapitre I nous avons déterminé les invariants b_2, b_4, b_6, $\Delta(E)$, $c_4(E)$, $j(E)$ des cubiques de Weierstrass.

La cubique (6) est une courbe elliptique si et seulement si $\Delta(E) \neq 0$
(théorème de classification par $\Delta(E)$ et $c_4(E)$).

Algorithme de détermination de courbes elliptiques isiogènes :

1- Soit une courbe elliptique d'équation de Weierstrass :

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

2- Soit un sous groupe fini F du groupe E(K) et l'isogénie :

f : E(K) ⟶ E' = E(K)/F. de noyau F

3- Soit l'ensemble F_2 des points P d'ordre 2 dans F - $\{0_E\}$;
Alors $F - F_2 - \{0_E\} = R \oplus (-R)$ = somme directe.

Soit l'ensemble $S = F_2 \cup R$.

Equation de l'isogénie f :

4- $$X = x + \sum_{L \in S}\left[\frac{t_L}{x - x_L} + \frac{u_L}{(x - x_L)^3}\right]$$

$$Y = y - \sum\left[\frac{u_L(2y + a_1x + a_3)}{(x - x_L)^3} + \frac{t_L(a_1(x - x_L) + y - y_L + a_1u_L - g'_x(L)g'_y(L)}{(x - x_L)^3}\right] ;$$

Avec :
$L = (x_L, y_L)$ $\quad g_x'(L) = 3x_L^2 + 2a_2x_L + a_4 - a_1y_L$;

$g_y'(L) = -2y_L - a_1x_L - a_3$;

$t_L = g_x'(L)$ si $L \in F_2$ et $t_L = 6x_L^2 + b_2x_L + b_4$ si $L \notin F_2$;

$u_L = 4x_L^3 + b_2x_L^2 + 2b_4x_L + b_6$;

ces formules X et Y sont obtenues avec les formules des coordonnées du symétrique – P de la somme $P_1 + P_2$ et de la somme 2P(chapitre II).

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

Avec $t = \sum_{L \in S} t_L$ et $w = \sum_{L \in S} (u_L + x_L t_L)$;

C'est l'équation de la courbe elliptique isogène

6- Application à la courbe elliptique d'équation de Weierstrass :

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

Calcul des invariants :
$b_2 = -3$, $b_4 = -5$, $b_6 = 13$, $b_8 = -16$, $c_4 = 129$ et $\Delta(E) = -3.16.29$;

Le point L = (1,0) engendre un sous groupe F de E(Q) d'ordre 7

$F = \{L, 2L=(-1,-2), 3L=(3,-6), 4L=(3,2), 5L=(-1,2), 6L=(1,-2), 7L=0_E=(\infty,\infty)\}$
Ce sous groupe F ne contient pas de sous groupe F_2 d'ordre 2.

$F - \{0_E\} = \{L,2L,3L\} \oplus \{4L,5L,6L\} = R \oplus (-R)$.
Calcul des nombres t et w de l'équation de la courbe E' isogène

x_L	t_L	u_L	$g_x'(L)$	$g_y'(L)$
1	-2	4	-2	-2
-1	4	16	4	4
3	40	64	24	8

T= 42 et w = 198.

Alors la courbe isogène E' = E/F a pour équation :

$Y^2 + xy + y = x^3 - x^2 - 213x - 1257$.

Dans [16-1] nous trouvons des exemples d'isogénies de courbes elliptiques.

1- Isogénie f : $E_1 \longrightarrow E_2$ de degré 5.
$E_1 : y^2 + y = x^3 - x^2$; $\Delta(E_1) = -11$.
$E_2 : Y^2 + Y = X^3 - X^2 - 10X - 20$; $\Delta(E_2) = -11^5$.

Equations de f :

$$x \longrightarrow x + \frac{2}{x-1} + \frac{1}{x^2} + \frac{1}{(x-1)^2} \ ;$$

$$y \longrightarrow y - \frac{2y+1}{x^3} - \frac{y}{x^2} - \frac{2y+1}{(x-1)^3} - \frac{y+1}{(x-1)^2} \ ;$$

Le noyau de l'isogénie est le groupe cyclique :

$F = \{P=(0,0), 2P=(1,-1), 3P=(1,0), 4P=(0,-1), 5P=0_E\}$

2- Isogénie f : $E_2 \longrightarrow E_3$ de degré 5 ;

$E_2 : y^2 + y = x^3 - x^2 - 10x - 20$; $\Delta(E_2) = -11^5$.

$E_3 : Y^2 + Y = X^3 - X - 7820X - 263580$; $\Delta(E_3) = -11$:

Equations de f :

$$x \longrightarrow x + \frac{110}{x-5} + \frac{121}{(x-5)^2} + \frac{12 \times 121}{x-16} + \frac{11^4}{(x-16)^2} \ ;$$

$$y \longrightarrow y - \frac{121(2y+1)}{(x-5)^3} - \frac{110y}{(x-5)^2} - \frac{55}{(x-5)^2} - \frac{11^4(2y+1)}{(x-16)^3} - \frac{132y}{(x-16)^2} - \frac{726}{(x-16)^2}$$

Le noyau de cette isogénie est le groupe cyclique :

F = {P=(5,5), 2P=(16,-61), 3P=(16,60), 4P=(5,-6), 5P= 0_E}.

Pour la suite de mes recherches il y a plusieurs pistes : étude des invariants de cubiques de Weierstrass à 1 et à 2 paramètres, courbes elliptiques à multiplication complexe.

Bibliographie:

[1] CASSELS ″ Diophantine Equation with Special References to Elliptic Curves″ ; J. London Math. Soc. 41 (1966) 193/ 291.

[2] COHN : A classical Invitation to Algebraic Numbers and Class Fields – Springer Verlag (1978) .

[3] Deuring : Die Typen der Multiplikat : renringe elliptisscher Funktionen Korper ,’’Abh . Math . Séminaire .

[4] HARTSHONE : Algebraic Geometry ; Graduate Text in Mathematics N : 52 (1980) .

[5] HUSEMÖLLER ″ Elliptic Curves ″ ; 2nd Ed (2004).Graduate Text in Mathematics N° 111.

[6] KOBLITZ ″ Introduction to Elliptic Curves and Modular Forms ″; 2nd. Ed. Graduate Text in Mathematics - Springer- N° 95.

[7] KOSTRIKIN ″ Introduction à l’Algèbre ″ ; Ed. Mir- Moscou- 2nd. Ed.(1986).

[8] S. LANG ″ Algebra ″ 2nd. Ed – Addison Wesley- New York (1984).

[9] B. MAZUR ″ Rational Isogenies of Prime Degree ″ Inv. Math.44 (1978). 129/162.

[10] ROBERT : Elliptique Curves – Lecture Notes in Mathématic 326 - Springer Verlag (1973)

[11] K . A RIBET : On modular representations of Gal (Q’/ Q) arising from modular forms , Invention Math . 100 (1990) 431 - 476

[12] SHAFAREVICH : Basic Algebraic Geometry Springer (1977)

[**13**] SHIMURA ″ Introduction to the Arithmetic Theory of Automorphic Functions ″ ; Princeton Univ.Press(1971).

[14] J. H. SILVERMAN ″ The Arithmetic of Elliptic Curves ″ ; Graduate Text in Mathematics N° 106.(1986).

[15] J. T. TATE ″ The Arithmetic of Elliptic Curves ″ ; Inv. Math.23 (1974). 179/209.

[**16**] J. VELU : 1) ″ Isogénies entre Courbes Elliptiques ″ CRAS. Paris.Ser.A 273 (26 Juillet 1971) 238/241.

2) Courbes elliptiques sur Q ayant bonne réduction en dehors de 11^4 ; Comptes Rendus Académie des Sciences de Paris , t . 273 (26 Juillet 1971) 73 -75 .

[**1**7] ZAGIER: Elliptic Curves_ Lecture Tata Inst. Bombay(Inde)(1988).