N^{0}d'ordre : 29/2002 –M / MT

Université des Sciences et de la Technologie
Houari Boumediene

جامعة هواري بومدين
للعلوم والتكنولوجيا
U S T H B

Faculté de Mathématiques
Laboratoire d'Algèbre et Théorie des Nombres

THESE

Présentée à L'**USTHB**

Pour l'obtention du grade de : **Magister en MATHEMATIQUES**

Spécialité : **Algèbre et Théorie des Nombres**

Par M^{elle} **ZAHOUR Fadila**

Thème

Sur les groupes de torsion de courbes elliptiques définies sur des corps de nombres de degrés 2 et 3

Soutenue le 17 décembre 2002 devant le jury composé de :

M^r HACHAICHI. M.S	Maître de conférences à l'USTHB	Président
M^r ZITOUNI . M	Professeur à l'USTHB	Directeur de thèse
M^r BETINA . K	Professeur à l'USTHB	Examinateur
M^r KESSI . A	Professeur à l'USTHB	Examinateur
M^r BOUCHENA .R	Chargé de cours à l'USTHB	Examinateur

DEDICACES

A la mémoire de mon père .

A ma mère qui a toujours été prés de moi .

A mes sœurs :

Karima

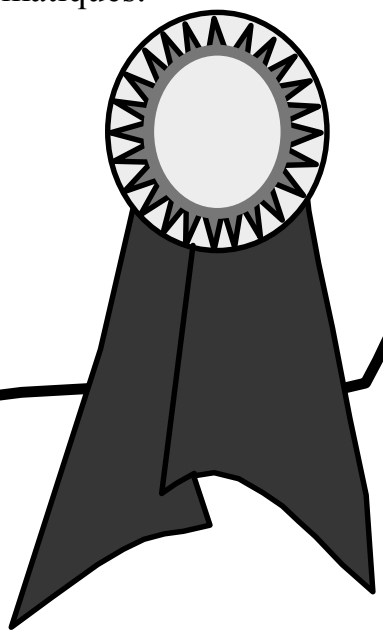
Zohra

A Zahia et ses enfants .

A toute ma famille .

A ma chère amie Madame *Fatma* et ses enfants .

A toutes mes amies de la faculté de Mathématiques.



REMERCIEMENTS

Je remercie Monsieur **Mohamed ZITOUNI** , professeur à l'USTHB , mon directeur de thèse pour l'aide , les orientations et les encouragements qu'il ma apportés tout le long de la réalisation de cette thèse .

Je remercie Monsieur **Mohamed Salah HACHAICHI**, Maître de conférences à l'USTHB d'avoir accepter de présider le jury .

Je remercie également Messieurs **Kamel BETINA** , professeur à l'USTHB , **Arezki KESSI** , professeur à l'USTHB et **Rachid BOUCHENA** , chargé de cours à l'USTHB pour leurs participation au jury .

Sommaire

Introduction

Toute courbe elliptique E sur un corps commutatif K possède une structure de groupe abélien d'élément neutre le point à l'infini 0_E .

Ce groupe est le groupe de MORDELL-WEIL de la courbe elliptique E .

Selon la théorie de la torsion d'un groupe , le groupe abélien E(K) possède des sous-groupes de m-torsion et un sous-groupe de torsion $E(K)_{tors}$.

La structure du groupe E(K) est semblable à la structure du groupe des unités U(K) d'un corps K : $U(K) \cong Z(K) \times \mathbf{Z}^r$, où Z(K) est le sous-groupe des racines de l'unité qui est fini , et r est l'entier : $r = r_1+r_2-1$ où r_1 est le nombre des conjugués réels et $2r_2$ celui des conjugués complexes de K.

Le groupe abélien E(K) est isomorphe au produit de groupes :

$E(K) \cong \mathbf{Z}^r \times E(K)_{tors}$

où $r = r(E) \geq 0$ est un invariant de la courbe elliptique E .C'est le rang de cette courbe .

Contrairement au groupe U(K) , il n'y a pas de formule donnant le rang r(E) .

Pour les courbes elliptiques définies sur le corps Θ des nombres rationnels, la structure du groupe de torsion est complètement déterminée par MAZUR cf [13, (a)] .

Plusieurs auteurs ont étudié l'existence de points d'ordre fini de courbes elliptiques sur des corps quadratiques et sur des corps cubiques purs (M.A .KENKU , F .MOMOSE cf[7] KAMIENNY cf [6] , STROHER , MULLER , ZIMMER , WILLIAMS et FUNG cf [5],[14] et [15]) .

Nous étudions les groupes de torsion de courbes elliptiques E sur des corps de nombres de degrés 2 et 3 en suivant les méthodes employées dans [5] et [6] .

Dans le chapitre I , nous décrivons la structure des corps de nombres quadratiques et des corps de nombres cubiques purs (anneau des entiers , décomposition des idéaux) .

Dans le chapitre II, nous exposons quelques éléments de la théorie arithmétique des courbes elliptiques : structures , loi de groupe abélien , morphismes de courbes elliptiques et la théorie de la réduction des courbes elliptiques .

Dans le chapitre III, nous étudions la théorie de la torsion sur les groupes de MORDELL-WEIL de courbes elliptiques .

Nous indiquons la structure des groupes de torsion des courbes elliptiques E sur le corps Θ des nombres rationnels et nous étudions le lien avec les nombres congruents .

Le chapitre IV est consacré aux groupes de torsion T(E) des courbes elliptiques sur les corps quadratiques K= $\Theta(\sqrt{D})$.

Le chapitre V est consacré aux groupes de torsion T(E) des courbes elliptiques E sur des corps cubiques purs $\Theta(\sqrt[3]{D})$; quelques exemples illustrent ce chapitre et montrent qu'un ordinateur est indispensable pour calculer des points de torsion .

Chapitre I

Entiers et idéaux d'un corps de nombres

Les courbes elliptiques étant définies sur des corps de nombres , nous commençons par une description de ces corps .

Dans la théorie des corps de nombres algébriques de degré fini , se trouvent les notions d'entiers algébriques , de décomposition des idéaux , de valuations .

Un corps des nombres K= $\Theta(\theta)$ de degré n admet un élément primitif θ .

La famille (1 , θ , … θ^{n-1}) de puissances de θ est une base du corps K sur le corps Θ des nombres rationnels .

1.Corps de nombres quadratiques :

La détermination d'une base d'entiers d'un corps de nombres de degré 2 est précisée par les résultats suivants :

Théorème 1 :

Soit un corps quadratique K = $\Theta(\sqrt{D})$, avec D entier rationnel sans facteur carré .

Alors K admet une base d'entiers :

$\left\{1 , \frac{1+\sqrt{D}}{2}\right\}$ *si D ≡ 1 modulo 4 , {1 ,* $\sqrt{D}$ *} sinon*

Le discriminant du corps K est égal à :

dis(K)= D si D ≡ 1 modulo 4 , 4D si D ≡ 2 ou 3≡ mod 4

Preuve : Cf [1]

Lorsque l'entier rationnel D est congru à 1 modulo 4 , le corps K admet une base normale d'entiers $\left\{ \frac{1\pm\sqrt{D}}{2} \right\}$.

Le groupe de Galois $G_{K/\Theta}$ = { S , S^2= Id} opère sur cette base par la formule :

$S\left(\frac{1+\sqrt{D}}{2} \right) = \frac{1-\sqrt{D}}{2}$.

Lorsque l'entier rationnel D satisfait les congruences $D \equiv 2$ ou $3 \equiv \text{mod } 4$, le corps K n'admet pas de base normale d'entiers.

Dans les deux cas , le discriminant dis(K) satisfait les congruences :

$D \equiv 1 \text{ mod } 4$, $4D \equiv 0 \text{ mod } 4$

Cette propriété du discriminant est valable pour tout corps de nombres de degré $n \geq 2$. c'est le ″théorème de STICKELBERGER cf [12] ″: $dis(K) \equiv 0$ ou $1 \text{ mod } 4$

La structure de l'ensemble A_K des entiers algébriques d'un corps de nombres algébriques K est décrite par les notions d'anneau , de **Z** - module et d'ordre :

L'anneau A_K des entiers du corps K est un Z – module libre de rang fini n .On peut trouver alors n entiers $e_1, \ldots\ldots, e_n$ de K tels que : $A_K = \mathbf{Z}e_1 + \mathbf{Z}e_2 + \ldots + \mathbf{Z}e_n$

La famille $\{e_1, \ldots\ldots, e_n\}$ est une base d'entiers de K .

L'ordre maximal A_K et les ordres non maximaux :

Définition 1:

*Un ordre du corps K est un **Z**- module complet de K qui est un sous anneau de K contenant le nombre 1 .(**Z** est l'anneau des entiers rationnels) .*

Dans un corps quadratique $K = \Theta(\sqrt{D})$, l'ordre maximal est le sous-anneau A_K engendré par 1 et ω, avec $\omega = \sqrt{D}$ si $D \equiv 2$ ou $3 \equiv \text{mod } 4$ et $\omega = \frac{1}{2}(1+\sqrt{D})$ si $D \equiv 1 \text{ mod } 4$.

Les ensembles $O_f = \mathbf{Z} + f A_K$ sont des ordres non maximaux du corps K de conducteur f .

La décomposition d'un nombre premier rationnel p dans un corps de nombres $K = \Theta(\theta)$ de degré $n \geq 2$ est de la forme :

$pA_K = P_1^{e_1} \ldots P_g^{e_g}$, où les P_1 , ….., P_g sont g idéaux premiers de K de norme : $N_{K/\Theta} = p^{f_i}$

les degrés f_i et les indices de ramification e_i pour tout i = 1, ……g , satisfont la relation :

$e_1 f_1 + e_2 f_2 + \ldots + e_g f_g = n$

Théorème 2 :

Les seuls nombres premiers qui se ramifient dans un corps de nombres K sont les diviseurs premiers du discriminant du corps K .

Théorème 3 :

Soient un corps quadratique K de discriminant dis(K)=D et d' anneau des entiers A_K ; alors :

a) Un nombre premier p admet une décomposition de type :

$p A_K = P^2$ *avec* $N(P) = p$ *si et seulement si p divise D*

b) Un nombre premier impair p qui ne divise pas le discriminant admet une décomposition de type :

$p A_K = P P'$ *avec* $P \neq P'$ *et* $N(P)=N(P') = p$ *si* $\left(\frac{D}{p}\right)=1$

et $p A_K = P$ *avec* $N(P)= p^2$ *si* $\left(\frac{D}{p}\right)= -1$ *; ou* $\left(\frac{\cdot}{p}\right)$ *est le symbole de LEGENDRE .*

c) le nombre premier 2 admet la décomposition de type :

$2A_K = PP'$ *avec* $N(P)=N(P')=2$ *si* $D \equiv 1 \bmod 8$

et $2A_K = P$ *avec* $N(P) = 4$ *si* $D \equiv 5 \bmod 8$

Preuve : Cf[1]

2. Corps de nombres cubiques purs :

Par définition , un corps de nombres cubique pur est un corps engendré sur le corps Θ par un nombre irrationnel cubique : $\theta_1 = \sqrt[3]{ab^2}$, où a et b sont deux entiers rationnels satisfaisant :

a , b et a b sans facteurs carré et a > b > 0 (1)

alors $K= \Theta(\theta_1) = \Theta(\theta_2)$ où $\theta_2 = \sqrt[3]{a^2 b}$; (2)

Posons $\theta_1 = \sqrt[3]{m}$. Le polynôme minimal de $\sqrt[3]{m}$ est $f(x) = x^3 - m$

Les racines du polynôme f(x) dans C étant θ_1 , j θ_1 et $j^2\theta_1$ et K étant un corps réel , il ne contient pas tous les conjugués de θ_1 sur Θ .

Par suite l'extension K sur Θ n'est pas normale , donc pas galoisienne .

D'après la théorie des extensions de corps de nombres , le corps cubique pur admet une Θ - base : $1 , \theta_1 , \theta_2$; (3)

tout élément x de K admet une représentation unique :

$x = t_0 + t_1 \theta_1 + t_2 \theta_2$ avec $t_i \in \Theta$; (4)

la norme de x vaut :

$N_{K/\Theta}(x) = t_0^3 + t_1^3 ab^2 + t_2^3 a^2 b - 3 t_1 t_2 t_3 ab$ (5)

L'ensemble des corps cubiques purs est réparti en 2 classes :

La classe des corps de type I , qui satisfont : $a \neq \pm b \bmod 9$,

La classe des corps de type II , qui satisfont : $a \equiv \pm b \bmod 9$ (6)

Les entiers d'un corps K forment un anneau A_K qui a une structure d'ordre maximal et de Z-module libre de rang 3 (7)

La structure de l'anneau A_K des entiers est précisée par le :

Théorème 4 :

Soit un corps de nombres cubique pur $K = \Theta(\theta_1) = \Theta(\theta_2)$ *, avec* $\theta_1 = \sqrt[3]{ab^2}$ *et* $\theta_2 = \sqrt[3]{a^2 b}$ *, d'anneau des entiers* A_K .

1) $a \neq \pm b \bmod 9$ *implique pour* A_K *une* $\boldsymbol{Z}$*- base* $\{1, \theta_1, \theta_2\}$.

Alors $A_K = 1.\boldsymbol{Z} + \theta_1 \boldsymbol{Z} + \theta_2 \boldsymbol{Z}$ *est un* $\boldsymbol{Z}$ *–module libre de rang 3 .*

Le discriminant du corps K vaut : $dis(K) = -27a^2 b^2$

2) La congruence $a \equiv \pm b \bmod 9$ *implique pour* A_K *une* $\boldsymbol{Z}$*- base :* $\{\frac{1}{3}(1+\theta_1+\theta_2), \theta_1, \theta_2\}$.

Alors : $A_K = \frac{1}{3}(1+\theta_1+\theta_2)\boldsymbol{Z} + \theta_1 \boldsymbol{Z} + \theta_2 \boldsymbol{Z}$ *est un* $\boldsymbol{Z}$ *–module de rang 3 .*

Le discriminant du corps K vaut $dis(K) = -3 a^2 b^2$

Preuve : cf [3] .

La décomposition des nombres rationnels premiers dans K est précisée par le :

Théorème 5 :

Soit un corps de nombres cubique pur $K = \Theta(\theta_1)$, $\theta_1 = \sqrt[3]{ab^2}$ *, d'anneau des entiers* A_K .

1) Les nombres premiers p ramifiés dans K sont les diviseurs premiers du nombre 3ab.

a) *Si p divise ab , alors il est totalement ramifié :*
   $pA_K = P^3$ *, avec P = idéal premier de norme* $NP = p$
b) *Si* $p = 3$, $ab \neq 0 \bmod 3$ *et* $a \neq \pm b \bmod 9$ *, alors 3 est totalement ramifié :*
   $3A_K = P^3$ *, avec P = idéal premier de norme* $NP = 3$
c) *Si* $p = 3$, $ab \neq 0 \bmod 3$ *et* $a \equiv \pm b \bmod 9$ *, alors 3 est ramifié en un idéal* P_1 *:*
   $3A_K = P_1^2 P_2$ *, avec* P_1 *= idéal premier de norme* $NP_1 = 3$

2) Les nombres premiers q non ramifiés dans K sont ceux ne divisent pas 3 ab :

a) *Si* $q \equiv -1 \bmod 3$ *, alors q est décomposé dans K :*
   $qA_K = P_1 P_2$ *avec les normes* $NP_1 = q^2$ *et* $NP_2 = q$

b) Si $q \equiv 1 \bmod 3$ *et* ab^2 *est un reste cubique modulo q , alors q est totalement décomposé dans K :* $qA_K = P_1 P_2 P_3$, *avec les normes* $NP_i = q$ *pour* $i = 1, 2, 3$.

b) *Si* $q \equiv 1 \bmod 3$ *et* ab^2 *n'est pas un reste cubique modulo q , alors q est inerte dans K :*
   $qA_K = P$ *, avec la norme* $NP = q^3$

Preuve : cf [3] .

Chapitre II

Théorie arithmétique des courbes elliptiques

Dans ce qui suit nous exposons quelques éléments de la théorie arithmétique des courbes elliptiques : structures, équations, loi de groupe abélien ,..etc.

1.Structures algébriques :

Une courbe elliptique est une cubique plane non singulière d'équation particulière :

$$E : y^2+a_1 x y+a_3 y = x^3 +a_2 x^2 + a_4 x + a_6 \qquad (1)$$

Elle possède une structure de courbe algébrique projective, lisse, irréductible, de genre un. Elle possède aussi une structure de variété abélienne de dimension 1 .

Les 5 coefficients a_i de l'équation (1) sont des éléments d'un corps commutatif K . Les 2 variables x et y sont racines de l'équation algébrique (1) . Donc ce sont des éléments d'une clôture algébrique K^{alg} du corps K .

Définition 2:

L' équation (1) est l'équation de WEIERSTRASS de la courbe elliptique E .

Les notions de courbes lisses , de courbes irréductibles et de courbes projectives se trouvent dans la théorie des courbes algébriques :

Définition 3:

1) Une courbe algébrique lisse est une courbe qui n'a pas de point singulier .

2) Une courbe algébrique est irréductible si son équation f (x,y)=0 ne se décompose pas en un produit f_1 (x,y) f_2 (x ,y) = f (x,y) de 2 polynômes de degrés ≥ 1 .

3)Une courbe elliptique d'équation f(x,y)=0 est projective si ,dans le plan projectif $IP^2(K)$ son équation est homogène de degré 3 .

4) Le genre d'une courbe plane lisse projective de degré n est l'entier $g = \frac{(n-1)(n-2)}{2}$.

2. Transformations d'équations et invariants arithmétiques:

L'équation (1) peut être transformée en d'autres formes par des changements linéaires convenables de variables :

a) Lorsque caract(K) ≠2 , on élimine les monômes en xy et en y dans l'équation (1) par le changement linéaire de variables :

$$(x, y) \longrightarrow (x , ½ (y – a_1 x – a_3) \quad (2)$$

On obtient l'équation :

$$E_1 : y^2 = 4 x^3 + b_2 x^2 + 2 b_4 x + b_6 \quad (3)$$

Les coefficients b_i sont des polynômes homogènes de degré i de l'anneau $\mathbf{Z}[a_1,\ldots,a_6]$:

$$b_2 = a^2_1 + 4a_2 \text{ et } b_4 = a_1 a_3 + 2 a_4 \text{ et } b_6 = a^2_3 + 4 a_6 \quad (4)$$

b) Lorsque caract (K) ≠2 , 3 , le changement linéaire :

$$X = x + \frac{a_1^2 + 4a_2}{12} \quad , \quad Y = 2y + a_1 x + a_3 \quad (5)$$

élimine les monômes en xy , en y et en x^2 dans (1).

On obtient l'équation :

$$E_2 : Y^2 = 4X^3 + g_2 X + g_3 \quad (6)$$

Les coefficients g_i sont des polynômes en b_i :

$$g_2 = -\frac{1}{12} b_2^2 + 2b_4 \quad , \quad g_3 = \frac{b_2^3}{216} - \frac{1}{6} b_2 b_4 + b_6 \quad (7)$$

Les coefficients b_i sont les polynômes définis par les formules (4)

c) On élimine les termes en x^2 et le coefficient 4 dans l'équation (3) pour un corps de caractéristique différente de 2 et 3 avec le changement linéaire de variables :

$$(x , y) \longrightarrow \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right) \quad (8)$$

On obtient l'équation :

$$E_3 : y^2 = x^3 – 27 c_4 x - 54 c_6 \quad (9)$$

Les coefficients c_4 et c_6 sont des polynômes de l'anneau $\mathbf{Z}[b_2 , b_4 , b_6]$ homogènes de degré i

$$c_4 = b_2^2 - 24 b_4 \text{ et } c_6 = - b_2^3 + 36 b_2 b_4 – 216 b_6 \quad (10)$$

Par des substitutions linéaires , on peut obtenir d'autres formes d'équations de courbes elliptiques ; citons :

1)L'équation de WEIERSTRASS courte : $y^2 = x^3 + Ax + B$ avec A , B∈ K (11)

2)L'équation de LEGENDRE : $y^2=x(x-1)(x-\lambda)$ avec $\lambda\neq 0,1$ (12)

3)la forme de KUBERT : $y^2+(1-c)xy-by = x^3-bx^2$ ($b , c \in K$) (13)

Les coefficients b_i et c_i permettent de définir 2 invariants arithmétiques de la courbe elliptique E :

Définition 4 :

Pour une courbe elliptique E définie sur un corps K de caract $\neq 2 , 3$, le discriminant de E est l'élément du corps K défini par la formule :

$\Delta(E) = 9b_2b_4b_6 - 8b^3_4 - 27b^2_6 - b^2_2b_8$ *avec* $4\, b_8 = b_2b_6-b_4^2$; *(14)*

C'est un polynôme de l'anneau $\boldsymbol{Z}\,[b_2 , b_4 , b_6 , b_8]$ *homogène de degré 12 .*

Le discriminant Δ(E) s'écrit aussi sous la forme :

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

qui est un polynôme de l'anneau : $(1/1728)\ \boldsymbol{Z}\,[c_4 , c_6]$ *homogène de degré 12*

Définition 5 :

L'invariant modulaire d'une courbe elliptique E pour caract(K) $\neq 2 , 3$ est le nombre défini par la formule :

$j(E) =c_4^3 /\Delta(E)$ *(15)*

Ces invariants permettent d'étudier certains aspects des courbes elliptiques .

3. Structure de groupe abélien sur une courbe elliptique :

Une loi de groupe abélien sur l'ensemble E(K) des points K- rationnels de la courbe elliptique E est définie en prenant le point $0_E = (\infty , \infty)$ à l'infini comme élément neutre et la propriété géométrique :

« 3 points colinéaires $P_i = (x_i , y_i)$ de la courbe elliptique E ont une somme nulle »

$P_1 + P_2 + P_3 = 0_E$ (figure 2) (16)

La loi de groupe abélien est la loi de composition :

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

$$(P_1 , P_2) \longrightarrow P_1 + P_2 \qquad (17)$$

Le point $O_E = (\infty ,\infty)$ est le point à l'infini dans le plan affine ; il est déterminé par la direction de l'axe Oy .

Dans le plan projectif $IP^2(K)$, ce point a pour coordonnées $O_E = (0,1,0)$ .Certains auteurs l'appellent point neutre , point de base de la courbe elliptique .

Vérifions les axiomes de ce groupe :

L'axiome de l'élément neutre se vérifie au moyen de la règle géométrique :

Le point $P+0_E$ est sur la parallèle à Oy passant par P : donc $P+0_E = P$ pour tout point P de E .

L'axiome de l'élément symétrique se vérifie au moyen de la règle géométrique :

Le symétrique(- P) est le $2^{ème}$ point d'intersection de la courbe elliptique E par la parallèle à Oy passant par P : donc $P+(-P) = 0_E$ pour tout point P de E

L'axiome de commutativité est vérifié avec la règle géométrique :

La sécante passant par les points P_1 et P_2 coïncide avec la sécante passant par les points P_2 et P_1 .Il en résulte : $P_1+P_2 = P_2+P_1$.

L'axiome d'associativité se vérifie en calculant les coordonnées des 4 points $P_1+P_2=M_1$, M_1+P_3 , $P_2+P_3 = M_2$ et P_1+M_2 .

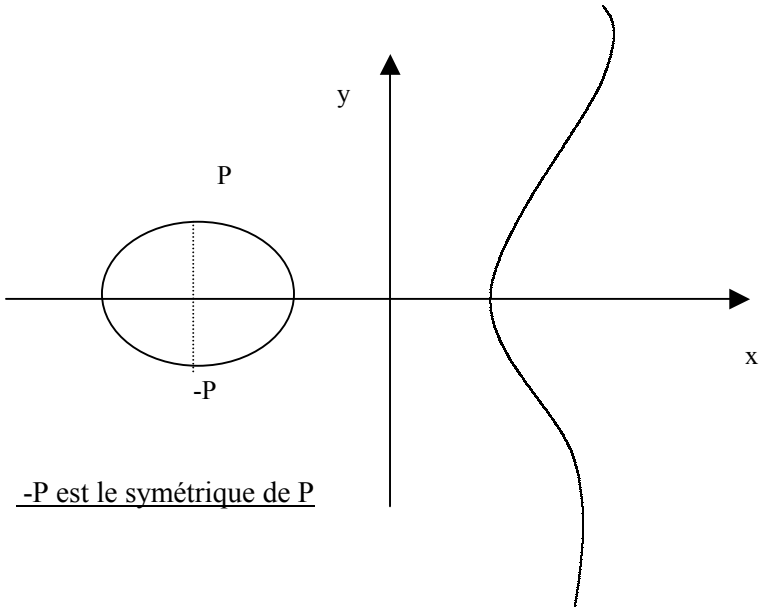
Les coordonnées du symétrique d'un point , de la somme P_1+P_2 de deux points distincts $P_1 \neq \pm P_2$, de la somme de deux points confondus $P+P = 2P$ s'obtiennent par la théorie de l'intersection de la courbe E par une droite convenable .On obtient les résultats suivants :

a. Calcul du symétrique –P d'un point P = (x ,y) :

La relation géométrique $P+(-P) =0_E$ implique que le symétrique du point P est le $2^{ème}$ point d'intersection de la courbe E par la parallèle à 0y passant par le point P (figure1)

Les calculs donnent les formules du symétrique :

$$-P = - (x , y) = (x , -y - a_1 x - a_3) \qquad (18)$$



-P est le symétrique de P

Figure.1

b. Calcul de la somme P_1+P_2 de deux points $P_i=(x_i,y_i)$, $P_1 \neq \pm P_2$:

La relation géométrique $P_1+P_2+P_3=0_E$ implique la somme $P_1+P_2=-P_3$

Il en résulte que le point $P_1+P_2=M$ est le symétrique $-P_3=M$ du 3ème point d'intersection P_3 de la courbe E par la sécante P_1P_2 : (figure 2)

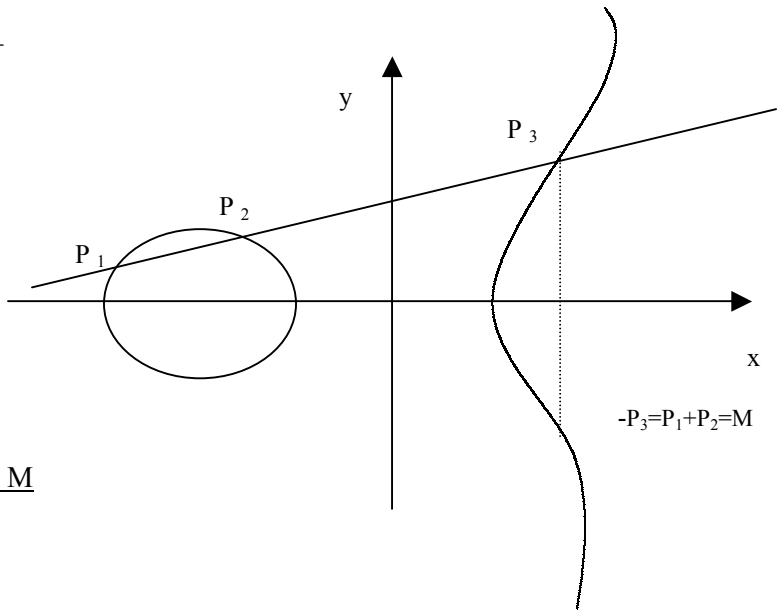
Les calculs donnent les coordonnées :

$P_1+P_2=M=(x_M, y_M)$;

$$x_M = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \qquad (19)$$

$$y_M = -\lambda^3 - 2a_1\lambda^2 + (a_2 - a_1^2 + 2x_1 + x_2)\lambda + a_1a_2 - a_3 + a_1(x_1 + x_2) - y_1 \ ;$$

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



La somme $P_1+P_2=M$

Figure.2

On a donc démontré le :

Théorème 6:

Soit une courbe elliptique E sur un corps K . Alors l'ensemble :

E(K) = { P∈ E , P= (x, y) , x ,y ∈ K satisfaisant à l'équation (1) de E} ∪{O_E }muni de la loi définie par la formule (17) est un groupe abélien d'élément neutre le point à l'infini $O_E = (\infty,\infty)$

Définition 6 *:*

Le groupe des points K- rationnels E(K) est le groupe de MORDELL –WEIL de la courbe elliptique E .

Sa structure est précisée par le :

Théorème7 :

Le groupe de MORDELL –WEIL E(K) d'une courbe elliptique E sur un corps commutatif K est un groupe de type fini .

Il est isomorphe au produit de groupes :

$E(K) \cong E(K)_{tors} \times \mathbf{Z}^r$;

où $E(K)_{tors}$ *désigne le sous- groupe de torsion de la courbe E*

et r(E)= r≥0 un entier rationnel.

Preuve : Cf [11]

C'est le théorème de MORDELL-WEIL des courbes elliptiques et des variétés abéliennes de dimension 1 .

Définition 7 :

L 'entier naturel r(E) = r du théorème 7 est le rang de la courbe elliptique E ; c'est le nombre de générateurs de la partie infinie de la courbe elliptique E .

Lorsque le corps de définition d'une courbe elliptique E est un corps fini K , le groupe E(K) des points K- rationnels de la courbe elliptique E est un groupe fini :

Théorème 8 :

Soit une courbe elliptique E définie sur un corps fini K à q éléments , q =p^f et p premier

Alors le groupe abélien E(K) est d'ordre $\leq 1 + q + 2\sqrt{q}$

Preuve : cf [18]

Le discriminant Δ(E) peut être utilisé pour caractériser les courbes non singulières .

4.Points singuliers d'une cubique plane :

Soit une cubique plane C sur un corps K et d'équation :

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0 \qquad (1)$$

Les points singuliers de cette cubique s'obtiennent par la théorie des singularités des courbes algébriques :

Si le système des 3 équations algébriques :

$$\begin{cases} f(x,y) = 0 \\ \dfrac{\delta f}{\delta x}(x,y) = 0 \\ \dfrac{\delta f}{\delta y}(x,y) = 0 \end{cases} \qquad (I)$$

n'admet pas de solutions ,alors la cubique C est lisse , c'est une courbe elliptique .

Si le système (2) admet une solution $P_o = (X_o , Y_o)$,alors la cubique C est singulière .

Le point singulier $P_o = (X_o , Y_o)$, quand il existe , est soit un nœud de la cubique , soit un point de rebroussement de la cubique.

Théorème 9 :

On considère une cubique plane C d'équation affine :

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0 \qquad (1)$$

1) *Le point à l'infini 0_C n'est pas singulier sur la cubique C .*

2) *"La cubique C n'a pas de point singulier" équivaut à"l'invariant discriminant Δ(C)≠0"*

Alors la cubique C est une courbe elliptique .

Preuve de " Le point à l'infini 0_C n'est pas singulier sur la cubique C "

Le changement de variable : x = X / Z , y =Y / Z

transforme l'équation (1) en une équation homogène :

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

Posons : $f(\frac{X}{Z}, \frac{Y}{Z}) = g(X,Y,Z)$

Le système d'équations (I) et le changement de variables impliquent le système de 4 équations algébriques :

$$\begin{cases} g(X, Y, Z) = 0 \\ g_x'(X, Y, Z) = 0 \\ g_y'(X, Y, Z) = 0 \\ g_z'(X, Y, Z) = 0 \end{cases} \quad \text{(II)}$$

Au point neutre $0_C = (\infty, \infty) = (0,1,0)$, on obtient les quatre équations algébriques :

$$\begin{cases} (1)\ g(0,1,0) = 0 \\ (2)\ g_x'(0,1,0) = 0 \\ (3)\ g_y'(0,1,0) = 0 \\ (4)\ g_z'(0,1,0) = 1 \neq 0 \end{cases} \quad \text{(III)}$$

La relation (4) implique que le système (III) n'a pas de solution .

On en déduit que le point $0_C = (0,1,0)$ n'est pas un point singulier de la cubique C .

Preuve de ″ la cubique C non singulière ″ implique ″ le discriminant Δ(C) de la cubique C n'est pas nul ″

Soit une cubique C sur un corps de caractéristique différente de 2 et 3 et d'équation :

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

L'hypothèse ″ la cubique C non singulière ″ implique que le polynôme h(x) admet 3 racines distinctes α_i .

$y^2 = h(x) = 4(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ (2)

Il en résulte que la cubique C est une courbe elliptique (3)

Le discriminant Δ(C) d'une courbe elliptique C est lié au résultant Res (h , h') du polynôme h(x) et à sa dérivée h' par la formule :

Δ(C) = d Res (h , h') pour une certaine constante d (4)

Le polynôme h(x) , d'après (2) admet 3 racines distinctes α_i , donc son polynôme dérivé est de la forme :

$h'(x) = 4(x-\beta_1)(x-\beta_2)$, (5)

où les zéros β_i sont distincts des zéros α_i :

Les formules (2) et (5) impliquent que le résultant Res (h , h') ≠ 0 (6)

(4) et (6) impliquent la valeur du discriminant : Δ (C) ≠ 0

La classification des cubiques planes singulières est déterminée par le :

***Théorème* 10 :**

Soit une cubique plane C d'équation :

$y^2 + a_1 xy + a_3 y = x_3 + a_2 x^2 + a_4 x + a_6$

à coefficients a_i dans un corps K .

Soient son discriminant Δ(C) et son coefficient usuel $c_4(C)=c_4$. Alors :

(1) La cubique C admet un nœud si et seulement si $\Delta(C)=0$ et $c_4\neq 0$, et dans ce cas cette cubique C n'est pas une courbe elliptique .

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

Preuve de " la cubique C admet un nœud " implique "$\Delta(C) = 0$ et $c_4 \neq 0$ "

Le théorème 9 implique ″ la cubique C non singulière ″ équivaut à ″$\Delta(C)\neq 0$ ″ .

Il en résulte que l'hypothèse ″ C singulière ″ équivaut à ″$\Delta(C) = 0$ ″.

Soit une cubique plane C d'équation :

C : $y^2 = 4x^3+b_2x^2+2b_4x+b_6 = g(x)$ (1)

L'hypothèse " la cubique C admet un nœud S " implique l'existence de deux tangentes distinctes à la courbe C au point S.

Les pentes de ces tangentes sont données par la dérivée de l'équation (1) :

$2yy' = 12x^2+2b_2x+2b_4$

Les pentes des tangentes sont égales à :

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

L'hypothèse ″ Les 2 tangentes sont distinctes au nœud S ″ implique que le polynôme h(x) possède 2 racines distinctes . (3)

La relation (3) implique que le discriminant du polynôme h(x) :

$\delta(h) = b_2^2-24\, b_4 \neq 0$ (4)

Or : $b_2^2-24\, b_4 = c_4(C)$ (5)

Les relations (4) et (5) impliquent : $c_4(C) \neq 0$

Preuve de ″$\Delta(C)=0$ et $c_4(C) \neq 0$″ implique ″ La cubique C *a*dmet un nœud″

Soit une cubique plane C d'équation (1)

L'hypothèse $\Delta(C)=0$ implique que C est singulière .

Le point singulier de C est soit un nœud , soit un point de rebroussement .

La dérivée partielle $g'(x) = 12x^2+2b_2x+2b_4$ est un polynôme quadratique de discriminant :

$\delta = c_4(C)$ (6)

l'hypothèse $c_4(C) \neq 0$ et la relation (6) impliquent que le polynôme g'(x) admet deux racines différentes .

Il en résulte deux tangentes distinctes à la cubique C au point singulier ; donc ce point est nœud .

Preuve de " la cubique C admet un point de rebroussement " implique "Δ (C) = c_4 =0 "

L'hypothèse " la cubique C admet un point de rebroussement R" implique l'existence de deux tangentes confondues à la courbe C au point R .

Les pentes de ces tangentes sont les racines du polynôme h(x) défini dans (2) :

L'hypothèse ″ L'existence de 2 tangentes confondues au point de rebroussement R ″ implique que le polynôme h(x) possède une racine double (7)

La relation (7) entraîne le discriminant δ (h) du polynôme h(x) est nul .

Il en résulte $c_4 = 0$.

Preuve de ″Δ(C)= c_4= 0 ″ implique ″ La cubique C *a*dmet un point de rebroussement ″ l'hypothèse $c_4(C) = 0$ et la relation (6) impliquent que le polynôme g'(x) admet une racine double .

Il en résulte deux tangentes confondues à la cubique C au point singulier .

Cela implique que ce point est point de rebroussement .

Exemples :

1.Cubique plane non singulière "C'est une courbe elliptique" :

Soit la cubique plane E sur Θ , d'équation :

E : $y^2 + x\,y + y = x^3 + x^2 - 3\,x + 1$

Les calculs donnent les coefficients b_i : $b_2 = 5$, $b_4 = -5$, $b_6 = 5$ et $b_8 = 0$ et le discriminant $\Delta(E) = -800 = -2^5\,5^2 \neq 0$, cela implique que cette cubique est une courbe elliptique .

La valeur $\Delta(E) < 0$ implique la forme particulière de la courbe en une seule branche .

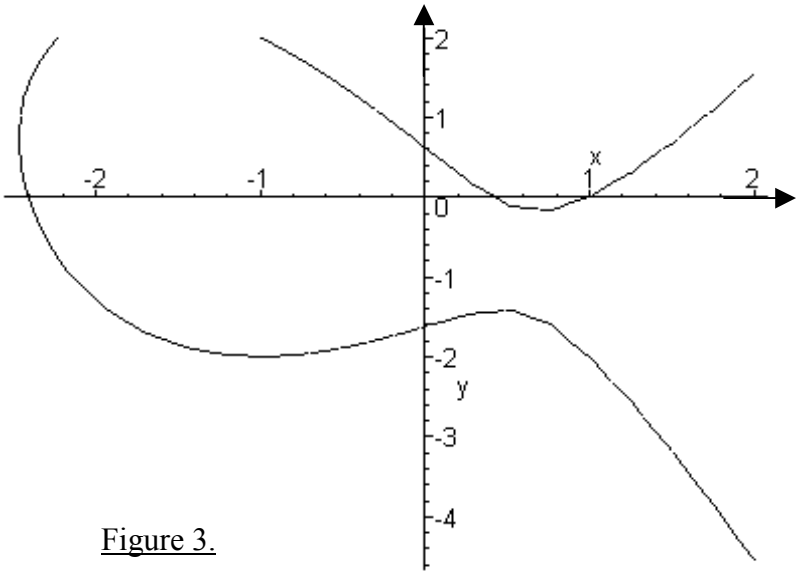


Figure 3.

2.Cubique plane avec un nœud ″ : ce n'est pas une courbe elliptique ″ :

Soit une cubique plane d'équation de WEIERSTRASS courte de la forme :

E : $y^2 = x^3 - 12x + 16 \in \Theta[x, y]$

Les calculs donnent : le discriminant $\Delta(E) = -16(-4 \times 12^3 + 27 \times 16^2) = 0$

Il en résulte que cette cubique plane est singulière .

Déterminons la nature de la singularité de la cubique E ; pour cela calculons le coefficient usuel c_4 :

Les calculs donnent : $c_4 = -48(-12) = 576 \neq 0$

Le théorème 10 implique que la cubique E admet un nœud S .

Déterminons les coordonnées du point S :

Posons : $f(x, y) = y^2 - x^3 + 12x - 16 = 0$

Par définition le point S est solution du système de 3 équations algébriques :

$$\begin{cases} f(x, y = 0 \\ f_x'(x, y) = -3x^2 + 12 = 0 \\ f_y'(x, y) = 2y = 0 \end{cases}$$

Les calculs donnent : S = (2 , 0)

Il en résulte que la courbe algébrique E possède un nœud au point (2 , 0).

Pour la représentation géométrique , nous utilisons les points :

(x , y) = (- 4 ,0) , (0, -4) , (0, 4) , (2,0) et le logiciel 'Maple '

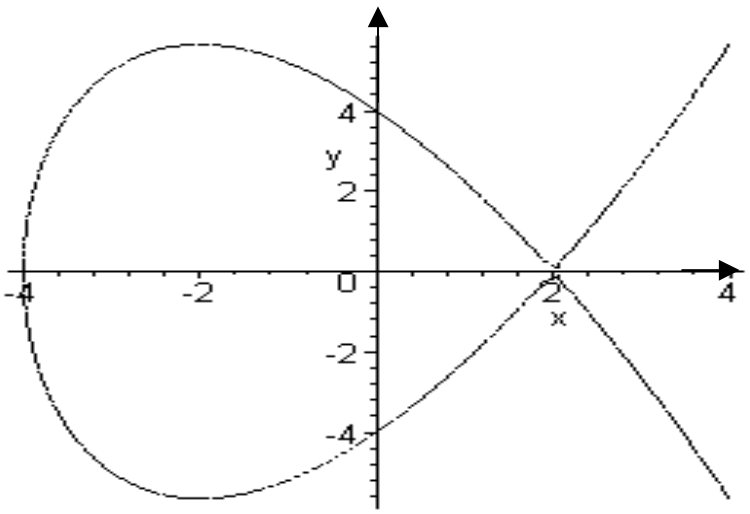


Figure 4

3.Cubique plane avec un point de rebroussement ″: ce n'est pas une courbe elliptique ″

Considérons la cubique plane E sur Θ , d'équation :

E : $y^2 = x^3 + 3x^2 + 3x + 1$ (2)

Les calculs donnent les invariants : $b_2 = 12$, $b_4 = 6$, $b_6 = 4$, le discriminant $\Delta(E) = 0$ et le coefficient usuel $c_4 = 0$

Il en résulte que la cubique plane d'équation (2) est une cubique singulière qui possède un point de rebroussement .

Le polynôme $g(x) = x^3 + 3x^2 + 3x + 1$ est une identité algébrique ; c'est $(x+1)^3$.

E : $y^2 = (x+1)^3$

Nous en déduisons que la cubique E possède un point de rebroussement de coordonnées (-1,0) .

Pour la construction géométrique , nous utilisons les points :

(-1 , 0) , (0 ,-1) , (0 , 1) et le logiciel 'Maple' .

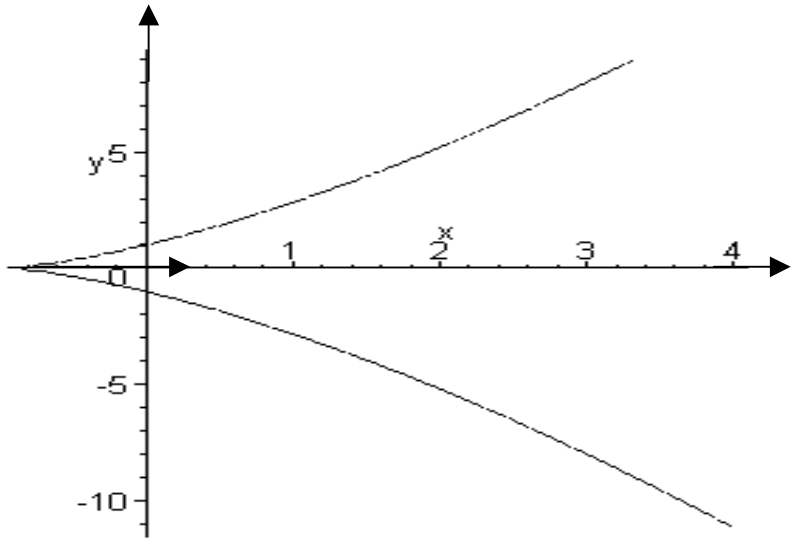


Figure 5

Les morphismes de courbes elliptiques peuvent être des endomorphismes , des isomorphismes ,des automorphismes , des translations ou des isogénies.

Nous nous intéressons aux isomorphismes , aux endomorphismes et aux isogénies de deux courbes elliptiques sur un corps K .

5.Isomorphismes de courbes elliptiques E et E' :

Soit deux courbe elliptiques E et E' sur un corps K .

Soit l'application $f : E(K) \longrightarrow E'(K)$

$$(x, y) \longrightarrow (u^2 x + r, u^3 y + s u^2 x + t) \qquad (1)$$

de groupes de MORDELL - WEIL .

avec : $u \in K^*$ et $r, s, t \in K$.

l'application f est un isomorphisme de courbes elliptiques E et E'sur K .

Cette application vérifie les relations d'isomorphisme de groupes abéliens .

$f(0_E)=0_{E'}$, où 0_E = point neutre de la courbe E et $0_{E'}$= point neutre de la courbe E'

$f(P_1+P_2) = f(P_1)+f(P_2)$ pour tout couple (P_1 , P_2) de points de la courbe elliptique E .

Cette application transforme l'équation de la courbe E :

$$E : y^2+a_1 x y+a_3 y = x^3 +a_2 x^2 + a_4 x + a_6 \text{ avec } a_i \in K \qquad (2)$$

en l'équation de la courbe elliptique E' :

$$E' : y^2+a'_1 x y+a'_3 y = x^3 +a'_2 x^2 + a'_4 x + a'_6 \text{ avec } a'_i \in K \qquad (3)$$

Les calculs donnent les relations entre :

a) Les coefficients a_i et a'_i :

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

b) Les coefficients b_i et b'_i :

$$\begin{aligned} u^2 b'_2 &= b_2 + 12r \\ u^4 b_4' &= b_4 + rb_2 + 6r^2 \\ u^6 b_6' &= b_6 2rb_4 + r^2 b_2 + 4r^3 \\ u^8 b'_8 &= b_8 + 3rb_6 + 3r^2 b_4 + r^3 b_2 + 3r^4 \end{aligned} \qquad (5)$$

c)Les coefficients c_i et c'_i :

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

d) Les discriminants Δ (E) et Δ (E')

$$u^{12}\Delta(E') = \Delta(E) \qquad (7)$$

e) Les invariants modulaires j(E) et j(E') :

$$j(E') = j(E) \qquad (8)$$

La relation (8) implique un critère de reconnaissance de 2 courbes elliptiques isomorphes E et E' sur un corps K ; elle détermine la classe des courbes elliptiques isomorphes à une courbe elliptique donnée .

***Théorème* 11 :**

Deux courbes elliptiques E et E' sur un corps K sont isomorphes sur une clôture algébrique du corps K si et seulement si elles ont des invariants modulaires égaux

j(E)= j(E')

Preuve de ″E et E' isomorphes ″ implique ″ j(E) =j(E') ″

Soient deux courbes elliptiques E et E' isomorphes sur un corps K .

Leurs équations sont de la forme :

E : $y^2+a_1 x y+a_3 y = x^3 +a_2 x^2 + a_4 x + a_6$ avec $\Delta(E) \neq 0$ (1)

E' : $y^2+a'_1 x y+a'_3 y = x^3 +a'_2 x^2 + a'_4 x + a'_6$ avec $\Delta(E') \neq 0$ (2)

Les relations entre les coefficients a_i et a'_i sont celles des formules (4) .

Les formules (8) précédentes impliquent que les invariants modulaires sont égaux.

Preuve de ″j(E) =j(E') ″ implique ″ E et E' isomorphes ″

Soient un corps K de caractéristique ≠2,3 , deux courbes elliptiques E et E'sur K ; d'invariants modulaires égaux $j(E)=j(E')$ (3)

Prenons les équations des courbes sous la forme courte :

$E : \ y^2= x^3+ a_4x + a_6 \qquad avec\ 4a_4^3+27a_6^2 \neq 0$ (4)

$E' : \ y^2= x^3+a_4'x+a_6' \qquad avec\ 4a'^3_4+27a'^2_6 \neq 0$ (5)

La formule qui donne l'invariant modulaire j d'une courbe elliptique E est :

$j = c_4^3/ \Delta(E)$ (6)

Les calculs donnent les valeurs de c_4 et du discriminant

$c_4= - 48a_4$ et $\Delta(E)=-16(4a_4^2+27a_6^2)$ (7)

L'hypothèse (3) , les formules (6) et (7) impliquent l'égalité :

$a_4^3a_6'^2=a'^3_4\, a_6^2$ (8)

Il y a 3 cas possibles suivant les valeurs j =0 , j =1728 et j ≠0 , j ≠1728 .

Pour j=0 , la formule (7) donne les valeurs :

$a_4=0$, $\Delta(E)\neq0$, $a_6 \neq0$, $a_4'=0$ et $a'_6\neq0$ (9)

Il en résulte l'existence d'un élément non nul u du corps K tel que : $a_6=u^6 a'_6$ (10)

Les formules liant les coefficients a_6 et a'_6 de deux courbes elliptiques isomorphes et (10) impliquent les formules d'isomorphismes des courbes E et E' :

$$(x , y) \longrightarrow (u^2x , u^3y) \quad \text{avec} \quad u=\left(\frac{a_6}{a'_6}\right)^{1/6} \qquad (11)$$

Pour j=1728 , les formules (6) et (7) donnent les valeurs :

$a_4 \neq0$, $a_4'\neq0$, $a_6= a_6'=0$ (12)

(12) implique l'existence d'un élément non nul u du corps K tel que :

$a_4=u^4a'_4$ (13)

Les formules liant les coefficients a_4 et a'_4 de deux courbes elliptiques isomorphes et (13) impliquent les formules d'isomorphismes données dans (11) avec $u=\left(\frac{a_4}{a'_4}\right)^{1/4}$

Pour j ≠0,1728 , les formules (6) et (7) donnent les valeurs :

$a_4a_6\neq0$ et $a'_4\, a'_6\neq0$ (14)

(14) implique les valeurs : $a_4\neq0$, $a_6\neq0$, $a'_4\neq0$ et $a'_6 \neq0$ (15)

On en déduit l'existence d'un élément non nul u du corps K tel que :

$a_6=u^6a'_6$ et $a_4=u^4a'_4$ (16)

Les formules liant les coefficients a_4 et a'_4 , a_6 et a'_6 de deux courbes elliptiques isomorphes et (16) impliquent les formes d'isomorphismes :

$(x , y) \longrightarrow (u^2x , u^3y)$ avec $u = \left(\frac{a_4}{a'_4}\right)^{1/4} = \left(\frac{a_6}{a'_6}\right)^{1/6}$

Exemple :

Considérons les deux courbes elliptiques définies sur un corps K de caractéristique différente de 2 , d'équations :

E : $y^2= x^3 +4x^2+2x$ avec $\Delta(E) = 2^9 \neq 0$

E' : $y^2= x^3 -8x^2+8x$ avec $\Delta(E') = 2^{15} \neq 0$

Les coefficients a_i et a'_i : $a_1 = a_3 = a'_1 = a'_3 = 0$, $a_2 = 4$, $a_4 = 2$, $a'_2 = -8$ et $a'_4 = 8$ (1)

Les calculs donnent des invariants modulaires égaux : j(E) = j(E') = 8000

Le théorème 11 implique que les courbe elliptiques E et E' sont isomorphes sur une clôture algébrique du corps K .

Cherchons une formule d'isomorphisme des courbes elliptiques E et E'.

Les formules générales d'isomorphismes des courbes elliptiques E et E' ont été données au début de ce paragraphe par :

$$f_{u,r,s,t}(x, y) = (u^2x + r, u^3y + su^2x + t) \quad (2)$$

avec : $u \in K^*$ et r , s , t $\in$ K.

En utilisant les formules (4) du paragraphe 5 , les calculs donnent : s = t =0 (3)

Et la relation entre les coefficients a_i et a'_i :

$$u^2(-8) = 2 + 3r \quad (4)$$

$$u^4.8 = 2 + 8r + 3r^2 \quad (5)$$

$$r^3 + 4r^2 + 2r = 0 \quad = h(r) \quad (6)$$

La relation (6) implique que : r =0 est une racine du polynôme h(r) de degré 3 en r .

Pour la valeur r = 0 , la formule (4) devient :

$u^2(-8) = 2$

Cela entraînent les deux valeurs de u :

$$u = \pm\frac{1}{\sqrt{-2}}$$

Pour la valeur $u = \frac{1}{\sqrt{-2}}$, les relations (2) , (3) donnent l'isomorphisme :

$$f: E \longrightarrow E'$$

$$(x, y) \longrightarrow \left(-\frac{1}{2}x\ ,\ -\frac{1}{2\sqrt{-2}}y\right)$$

Les 2 courbes elliptiques sont isomorphes sur le corps quadratique imaginaire $\Theta(\sqrt{-2})$.

6.Endomorphismes et isogénies de courbes elliptiques :

Définition 8:

*Un endomorphisme d'une courbe elliptique E est un homomorphisme du groupe abélien E(K) L'ensemble des endomorphismes d'une courbe elliptique E sur K est un anneau noté $End_K(E)$. Cet anneau est intègre de caractéristique 0 , il est donc isomorphe à l'anneau des entiers rationnels **Z** ou à un anneau contenant **Z** .*

Définition 9 :

*Une courbe elliptique dont l'anneau des endomorphismes $End_K(E)$ contient l'anneau des entiers rationnels **Z** est une courbe elliptique à multiplication complexe .*

Exemples:

1) Toute courbe elliptique sur un corps fini a une multiplication complexe .
2) Une courbe elliptique sur un corps quadratique imaginaire $\Theta(\sqrt{-D})$ est à multiplication complexe , l'anneau des endomorphismes $End_K(E)$ est isomorphe à l'anneau des entiers du corps quadratique imaginaire $\Theta(\sqrt{-D})$ ou à un ordre de cet anneau .

SHIMURA cf[17] a défini la notion d'isogénie de courbes elliptiques comme suit :

Définition 10 :

Soient deux courbes elliptiques E_1 et E_2 sur un même corps K d'éléments neutres 0_1 et 0_2 .

Une isogénie de courbes elliptiques est un morphisme de groupes de MORDELL-WEIL:

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

satisfaisant les relations :

1) $g(0_1)= 0_2$;

2) $g(P_1+P_2)= g(P_1)+g(P_2)$ pour tous les points P_i de E ;

3) le noyau $g^{-1}(0_2)$ est un sous groupe fini du groupe E_1

4) $g(E_1)=E_2$ pour toute isogénie non nulle (g est surjective)

Définition 11 :

Le degré de l'isogénie g est égal à l'ordre de son noyau .

A chaque isogénie g : $E_1 \longrightarrow E_2$, on peut associer l' application

$\hat{g} : E_2 \longrightarrow E_1$, déterminée par le :

***Théorème* 12 :**

Soit une isogénie de degré m de courbes elliptiques :

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

Alors il existe une isogénie unique :

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

dont les composées : $\hat{g}$ o g : $E_1(K) \longrightarrow E_1(K)$ et g o $\hat{g}$: $E_2(K) \longrightarrow E_2(K)$

sont les multiplications m_E *par l'entier m sur les courbes E_1 et E_2 respectivement .*

Preuve : Cf [18] , théorème 6.1 page 84.

Définition 12 :

Cette application $\hat{g} : E_2 \longrightarrow E_1$ est l'isogénie duale de l'isogénie g .

En particulier, la multiplication sur une courbe elliptique E par un entier rationnel m est une isogénie de cette courbe elliptique définie par :

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

$$P \longrightarrow m_E(P) = mP$$

$$mP = \begin{cases} P+P+\ldots\ldots\ldots\ldots P & (m \text{ fois }) \quad \text{si } m > 0 \\ (-P)+(-P)+\ldots\ldots(-P) & (-m \text{ fois }) \quad \text{si } m < 0 \\ 0_E & \text{si } m=0 \end{cases}$$

Cette multiplication satisfait les relations :

$m_E(P_1+P_2) = m_E(P_1) + m_E(P_2)$ et $m_E(0_E) = m_E(0_E)$ pour tout points P_i de E .

Si m > 0 , noyau de cette isogénie m_E est le sous groupe de m- torsion de la courbe elliptique E :

$m_E^{-1}(0_E) = \{P \in E , mP = 0_E\} = E(K)[m]$

L'application " multiplication par un entier rationnel m" est un outil très efficace dans la détermination des sous groupes de m- torsion .

Théorème 13:

La multiplication m_E *sur une courbe elliptique E est une isogénie de degré* m^2 .

Preuve : cf [18] et [2] , corollaire du lemme 7.2 , p 215 .

Dans l'ensemble des courbes elliptiques E , la relation d'isogénie satisfait les relations :

1) E est isogène à E

2) E_1 est isogène à E_2 implique E_2 est isogène à E_1

3) E_1 est isogène à E_2 et E_2 est isogène à E_3 implique E_1 est isogène à E_3 .

Donc c'est une relation d'équivalence sur l'ensemble des courbes elliptiques sur un corps K .

Pour les courbes elliptiques sur le corps des nombres rationnels Θ ,VELU a donné des formules d'isogénies [Compte Rendus de l'Académie des sciences PARIS , série A (1971) , t273 , p 238 -241].

7.Valuations d'un corps de nombres :

La théorie des réductions d'une courbe elliptique E sur un corps K , repose sur la théorie des valuations d'un corps .

Définition 13 :

Une valuation sur un corps K est une fonction $\nu : K \to IR_+$

à valeurs réelles positives qui satisfait aux trois axiomes :

(VAL 1) $\nu(x) > 0$ *pour tout élément x non nul de K et* $\nu(x)=0$ *équivaut à* $x=0$

(VAL 2) $\nu(x.y)=\nu(x).\nu(y)$ *pour tous les éléments x , y de K*

(VAL 3) $\nu(x+y)\leq \nu(x)+\nu(y)$ *pour tous les éléments x , y de K .*

Cet axiome (VAL 3) est appelé l'axiome de l'inégalité triangulaire , il peut être le remplacé par :

(VAL 3') Il existe une constante réelle $C\geq 1$ *telle que :*

$\nu(x)\leq 1$ *implique* $\nu(1+x) \leq C$

L'axiome (VAL 3) peut être remplacé par un axiome plus fort :

(VAL 4) $\nu(x+y)\leq max\ \{\nu(x) , \nu(y)\ \}$

Cet axiome implique la propriété : $\nu(x)\leq 1$ implique $\nu(1+x) \leq 1$

Les valuations d'un corps sont réparties dans deux sous ensembles :

Les valuations non- archimédiennes qui satisfont : $\nu(x) \leq 1$ implique $\nu(1+x) \leq 1$

Les valuations archimédiennes qui satisfont : $\nu(x) \leq 1$ implique $\nu(1+x) \leq 2$

Exemples

1. La valuation triviale ν satisfait : $\nu(x) = 1$ si $x \neq 0$ et $\nu(x) = 0$ si $x = 0$.

2. La valeur absolue sur le corps des nombres réels IR , $\nu(x) = \max\{x, -x\}$ et la valuation sur le corps des nombres complexes C , $\nu(a+ib) = \sqrt{a^2+b^2}$ sont des valuation archimédiennes .

Chaque valuation ν d'un corps K définit une structure topologique sur ce corps :

Théorème 14:

Une valuation ν d'un corps K détermine sur ce corps une topologie de HAUSDORFF.

Pour chaque élément a de K , un système fondamental de voisinages de a est formé par l'ensemble $U(a, \varepsilon) = \{ x \in K ; \nu(a-x) < \varepsilon , \varepsilon$ est un nombre réel positif $\}$.

Preuve : Cf[20] , proposition 1.1.2

Sur l'ensemble des valuations d'un corps , on définit une relation d'équivalence :

Définition 14 :

Deux valuations non triviales ν_1 et ν_2 sur un corps K sont équivalentes si elles satisfont l'une des conditions suivantes :

$\nu_1(x) < 1$ implique $\nu_2(x) < 1$;

$\nu_1(x) > 1$ implique $\nu_2(x) > 1$;

$\nu_1(x) = 1$ implique $\nu_2(x) = 1$

Les valuations équivalentes sont déterminées par le :

Théorème 15:

Deux valuations ν_1 et ν_2 d'un corps K sont équivalentes si elles satisfont la relation :

$\nu_1 = \nu_2^{\,s}$ pour un certain nombre réel $s > 0$

Preuve : Cf [20]

Cette relation d'équivalence permet de définir les diviseurs premiers d'un corps :

Définition 15 :

Toute classe d'équivalence d'une valuation ν d' un corps est un diviseur premier de ce corps .

Il en résulte que les valuations non triviales d'un corps K sont groupées en un ensemble V_0 des valuations non - archimédiennes non équivalentes et en un ensemble V_∞ des valuations archimédiennes non équivalentes , de sorte que l'ensemble des valuations d'un corps K est :

$VAL(K) = V_0 \cup V_\infty$

Pour le calcul des valuations sur un corps K , il y a des théorèmes d'approximation :

Théorème 16:

Soit un ensemble ν_1 ,... ν_n de valuations inéquivalentes et non triviales d'un corps K .Alors:

1) Il existe un élément x dans K tel que : $\nu_1(x) > 1$ et $\nu_t(x) < 1$ pour t= 2,3....n .

2) Pour tout nombre réel positif a et pour tous nombres x_1 , x_2 ,.....x_n de K , il existe un nombre b tel que : $\nu_t(b - x_t) < a$ pour t =1,2.....n

Le calcul de la valuation d'une somme se fait avec le :

Théorème 17:

Soit une valuation non archimédienne ν d'un corps K . Alors :

1) $\nu(a + b) \leq \max\{\nu(a), \nu(b)\}$
2) $\nu(a_1) > \nu(a_i)$ pour i= 2 ,3 , ...n implique $\nu(a_1+a_2+.....+a_n) = \nu(a_1)$

Pour un diviseur premier P non archimédien d'un corps K , on associe à un représentant ν de cette classe des sous ensembles particuliers du corps K :

$A_\nu = \{ x \in K ; \nu(x) \leq 1 \}$, anneau de la valuation ν de K = anneau des ν- entiers de K .

$P_\nu = \{ x \in K ; \nu(x) < 1 \}$, idéal ν- premier de K

$U_\nu = \{ x \in K ; \nu(x) = 1 \}$, groupe des ν -unités .

et $K_\nu = A_\nu / P_\nu$ le corps résiduel du corps K en ν .

Définitions 16 :

a) L'application canonique : $f : A_\nu \to A_\nu / P_\nu$ est une place de K en ν .

b) A chaque valuation non archimédienne ν sur un corps K , on associe la fonction φ appelée valuation exponentielle sur le corps K de valeur :

$\varphi(x) = -\log \nu(x)$ pour tout élément x du corps K .

Cela implique la relation : $\nu(x) = \exp(-\varphi(x))$ qui justifie le nom de valuation exponentielle

Alors les axiomes des valuations exponentielles φ deviennent :

(VAL' 1) $\varphi(x) = +\infty$ équivaut à x=0

(VAL' 2) $\varphi(x\,y) = \varphi(x) + \varphi(y)$ pour tous les éléments x, y de K

(VAL' 3) $\varphi(x+y) \geq \min\{\varphi(x), \varphi(y)\}$ pour tous les éléments x ,y de K

A toute valuation non –archimédienne φ on associe les sous ensembles du corps K :

$A_\varphi = \{ x \in K , \varphi(x) \geq 0 \}$, anneau des φ- entiers de K .

$M_\varphi = \{ x \in K , \varphi(x) > 0 \}$, idéal maximal en φ de K .

$U_\varphi = \{ x \in K , \varphi(x) = 0 \}$, groupe des φ- unités .

L'ensemble quotient : $A_\varphi / M_\varphi = K_{rési}$ est le corps résiduel du corps K en φ.

Cette valuation $\varphi : K \rightarrow IR_+$ détermine un homomorphisme du groupe multiplicatif K* dans le groupe additif 3_+.

La valuation φ est discrète si le groupe des valeurs $\varphi(K^*) = \{ \nu(a) , a \in K \text{ avec } a \neq 0 \}$ est un ensemble discret .

Dans ce cas l'anneau A_φ est un anneau de valuation discrète .

Définition 17:

Un anneau de valuation discrète est un anneau principal A qui admet un seul idéal premier non nul P ; alors cet idéal premier admet un générateur π appelé uniformisante de P ; il en résulte : $P = \pi A$

Tout anneau A de valuation discrète est un anneau de DEDEKIND . Alors l'idéal premier non nul P est maximal .

Exemples :

1. Les valuations p-adiques associées à un nombre premier p

Tout nombre rationnel x possède une décomposition unique :

$x = p^r a / b$ où a et b sont des entiers rationnels premiers à p et $r \in \mathbf{Z}$.

La fonction $\nu_p : \Theta \longrightarrow Z \cup \{+\infty\}$.

de valeur $\nu_p(x) = r$ est une valuation appelée valuation p- adique du corps Θ des nombres rationnels .C'est une valuation non archimédienne discrète .

2. Soient un corps de nombres algébriques K et son anneau des entiers A_K .

D'après la théorie des nombres , cet anneau est un anneau de DEDEKIND .

La théorie des anneaux de DEDEKIND montre que tout idéal non nul I de l'anneau A_K se décompose de manière unique en produit d'idéaux premiers sous la forme :

$$I = P_1^{e_1} P_2^{e_2} \cdots P_r^{e_r}$$

Les exposant e_1 , e_2 ,……,e_r sont les indices de ramification de l'idéal I en l'idéal premier P_i

L'idéal I est principal ; il admet un générateur x : $I = x A_K$ pour tout idéal premier P de l'anneau A_K ; l'application :

$A_K \longrightarrow Z \cup \{+\infty\}$

$x \longrightarrow \nu_P(x) = e_i$ est une valuation non - archimédienne discrète .

Chaque valuation possède des prolongements :

Définition 18 :

Soient un corps K muni d'une valuation non archimédienne discrète ν et une extension finie L de K et le groupe des valeurs $\nu(K^*)$ de ν dans IR .

1) Soit un prolongement w de la valuation ν à L et le groupe des valeurs $w(L^*)$ de w dans IR Alors l'ordre du groupe quotient : $e_\nu = [\, w(L^*) : \nu(K^*)\,]$ est l'indice de ramification du prolongement w à L .

2) Soit le corps résiduel $K_{rési}$ du corps K en ν et le corps résiduel $L_{rési}$ du corps L en ν . Alors la dimension $f_\nu = [\, K_{rési} : L_{rési}\,]$ est le degré résiduel de la valuation ν .

Les entiers naturels e_ν et f_ν sont liés par l'inégalité : $e_\nu \, f_\nu \leq n = [\, L : K]$

8. Réduction d'une courbe elliptique en une valuation non archimédienne discrète ν :

Dans la suite le symbole VNAD désigne une valuation non archimédienne discrète .

Définition 19:

Soit une courbe elliptique E de discriminant $\Delta(E)$ sur un corps K muni d'une VNAD ν .

Une équation de WEIERSTRASS de E est minimale en ν si la valuation des coefficients a_i : $\nu(a_i) \geq 0$ et $\nu(\Delta(E)) \geq 0$ et si la valuation de l'invariant discriminant $\nu(\Delta(E))$ a une valeur minimale .

Les formules d'isomorphismes de deux courbes elliptiques E et E' permettent de caractériser l'équation minimale par le :

Théorème 18 :

Soient une VNAD sur un corps K et une courbe elliptique E sur K .

Une équation de WEIERSTRASS de E est minimale en ν si l'une des trois relations est satisfaite : (1) $\nu(a_i) \geq 0$ et $\nu(\Delta(E)) < 12$

(2) $\nu(a_i) \geq 0$ et $\nu(c_4) < 4$

(3) $\nu(a_i) \geq 0$ et $\nu(c_6) < 6$

où $c_4(E) = c_4$ et $c_6(E) = c_6$ désignent des coefficients usuels de l'équation de E

Preuve :

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

$E : y^2+a_1 x y+a_3 y = x^3 +a_2 x^2 + a_4 x + a_6$ avec $a_i \in K$ (1)

Cette application est unique à isomorphisme prés .

l'isomorphisme défini au § 5 transforme l'équation (1) de E en une équation :

$y^2+a'_1 x y+a'_3 y = x^3 +a'_2 x^2 + a'_4 x + a'_6$ avec $a'_i \in K$ (2)

l'isomorphisme défini au § 5 implique les relations entre :

Les coefficients c_i et c'_i :

$u^4 c'_4 = c_4$ et $u^6 c'_6 = c_6$ (3)

Les discriminants Δ et Δ' :

$\Delta = u^{12} \Delta'$ (4)

L'équation de E est minimale si $\nu(a_i)\geq 0$ et $\nu(\Delta(E))$ est minimale (5)

La relations (4) et (5) impliquent que l'équation de E est minimale si $\nu(a_i)\geq 0$ et $\nu(\Delta(E))< 12$.

La relations (3) et (5) impliquent que l'équation de E est minimale si $\nu(a_i)\geq 0$ et ($\nu(c_4)< 4$ ou $\nu(c_6)< 6$) .

Définition 20:

Soient une courbe elliptique sur un corps K muni d'une VNAD ν , l'anneau A_ν de la valuation ν , l'idéal maximal M_ν associé , une uniformisante π de K et le corps des classes résiduelles $K_{rési} = A_\nu / M_\nu$.

La réduction modulo la valuation ν (ou modulo l'uniformisante π) de la courbe elliptique E est l'application qui à tout point $P \in E(K)$ associe son point réduit $\widetilde{P} \in \widetilde{E}(K_{rési})$

$$E(K) \longrightarrow \widetilde{E}(K_{rési})$$

$$P=(x , y) \longrightarrow \widetilde{P} = (\widetilde{x}, \widetilde{y}) \qquad \text{où} \quad \widetilde{x} \equiv x \ \text{modulo}\ \pi \ \text{et} \ \widetilde{y} \equiv y \ \text{modulo}\ \pi$$

La réduction modulo la valuation ν transforme une courbe elliptique E d'équation :

$E : y^2+a_1 x y+a_3 y = x^3 +a_2 x^2 + a_4 x + a_6$, $a_i \in K$, *point neutre* 0_E .

en une courbe réduite $\widetilde{E}$ d'équation :

$\widetilde{E} : \widetilde{y}^2 + \widetilde{a}_1\widetilde{x}\,\widetilde{y} + \widetilde{a}_3\widetilde{y} = \widetilde{x}^3 + \widetilde{a}_2\widetilde{x}^2 + \widetilde{a}_4\widetilde{x} + \widetilde{a}_6$, $\widetilde{a}_i \in K_{rési}$, de point neutre $0_{\widetilde{E}}$

La réduction modulo une VNAD ν , permet de définir deux sous-groupes du groupe E(K) :

Le sous -groupe des points de la courbe E de réduction non singulière :

$E_o(K) = \{P \in E(K) : \widetilde{P} \in \widetilde{E}_{ns}(K_{rési}) \}$ qui est un groupe d'indice fini de E(K)

et le noyau de l'application réduction modulo la VNAD ν :

$E_1(K) = \{P \in E(K) : \widetilde{P} = 0_{\widetilde{E}} \}$

La classification des réductions des courbes elliptiques est précisée par la :

Définition 21 :

Soient une courbe elliptique sur un corps K , une VNAD *ν et la courbe réduite $\widetilde{E}$ en ν.*

***1)** la courbe E a une bonne réduction en ν si $\widetilde{E}$ est non singulière . Donc $\widetilde{E}$ est une courbe elliptique .*

***2)** la courbe E a une mauvaise réduction en ν si $\widetilde{E}$ est singulière ; alors $\widetilde{E}$ n'est pas une courbe elliptique . On désigne par $\widetilde{E}_{ns}$ la partie non singulière de $\widetilde{E}$.*

la mauvaise réduction est :

***a)** multiplicative si la courbe réduite $\widetilde{E}$ possède un nœud.*

***b)** additive si la courbe réduite $\widetilde{E}$ possède un point de rebroussement .*

Une bonne réduction est une réduction stable. Une réduction multiplicative est une réduction semi- stable .Une réduction additive est une réduction instable.

La nature de la réduction en *ν* d'une courbe elliptique est déterminée par le :

Théorème 19 :

Soit une courbe elliptique E sur un corps K muni d'une valuation non archimédienne discrète ν d'équation de WEIERSTRASS de E minimale et de discriminant Δ(E) , de coefficient usuel $c_4(E) = c_4$. Alors :

a) E a une bonne réduction en ν si et seulement si ν(Δ(E))=0

b) E a une réduction multiplicative en ν si et seulement si ν(Δ(E))>0 et ν(c_4)=0.

c) E a une réduction additive en ν si et seulement si ν(Δ(E))>0 et ν(c_4)>0

Preuve de ″ E a une bonne réduction en ν ″ implique ″ ν(Δ(E)) =0 ″

Soit une courbe elliptique E sur un corps K de discriminant Δ(E)

Alors Δ(E) ≠0 .

Soit la courbe réduite $\widetilde{E}$ de la courbe elliptique E en ν .

L'hypothèse ″ E a une bonne réduction en ν ″ implique que la courbe réduite $\widetilde{E}$ sur $K_{résі}$ est une courbe elliptique .

Il en résulte que le discriminant Δ($\widetilde{E}$) de $\widetilde{E}$ est non nul .

A la valuation non archimédienne ν sur le corps de base K de la courbe elliptique correspond un nombre premier p ; les valuations ν(a) des nombres a premiers à p ont une valeur nulle .

Pour une telle valuation ν , ν (Δ(E)) = 0

Pour la preuve de (a) et (b) , on applique le théorème 10 à la courbe réduite de la courbe elliptique E modulo la valuation ν .

Réduction d'une courbe elliptique sur le corps Θ en une valuation p –adique :

Soit une courbe elliptique sur Θ :

$E : y^2+a_1 x y+a_3 y = x^3 +a_2 x^2 + a_4 x + a_6$ (1)

La réduction de E en une valuation p –adique est l'application :

$\nu_p : \Theta \longrightarrow IF_p$, $E \longrightarrow \widetilde{E}$

de valeur : ν_p (a) = $\widetilde{a}$ = classe de a mod p (2)

l'équation réduite modulo p de la courbe réduite $\widetilde{E}$ *en* ν_p est de la forme :

$\widetilde{E} : y^2+\widetilde{a}_1 x y+\widetilde{a}_3 y =x^3+\widetilde{a}_2 x^2+\widetilde{a}_4 x+\widetilde{a}_6$ (3)

Par définition le discriminant *Δ(E) n'est pas nul ; mais le discriminant de la courbe réduite est soit* $\Delta(\widetilde{E}) = 0$ *soit* $\Delta(\widetilde{E}) \neq 0$.

Trois cas se présentent :

$\Delta(\widetilde{E}) \neq 0$; *la réduction de E modulo p est bonne* .

$\Delta(\widetilde{E})=0$ *et* $\widetilde{c}_4(E) \neq 0$; *la réduction est multiplicative* .

$\Delta(E)= \widetilde{c}_4(E)= 0$; *la réduction est additive* .

Exemple:

1. Soit une courbe elliptique E d'équation :

E : $y^2= x^3+11x^2+11x$

Ses invariant valent : $\Delta(E) = 2^4 \times 7 \times 11^3$ et $c_4(E) = 2^7 \times 11$

Le théorème 19 implique que la courbe elliptique E a une réduction multiplicative en la valuation ν_7 , une réduction additive en les valuations ν_2 et ν_{11} et une bonne réduction en les valuations ν_p pour les nombres premiers $p \neq 2, 7$ et 11

Les qualificatifs de réductions multiplicatives et additives sont liées au :

Corollaire 1 :

Soient un corps K muni d'une VNAD , et son corps résiduel $K_{résI}$.

Soient une courbe elliptique E sur le corps K et la courbe réduite $\widetilde{E}(K_{résI})$ *modulo* ν *. Alors :*

1) Lorsque la courbe elliptique E a une réduction multiplicative en ν *, la partie non singulière* $\widetilde{E}(K_{résI})_{ns}$ *du groupe* $\widetilde{E}(K_{résI})$ *est isomorphe au groupe multiplicatif* $(K_{résI})^*$.

2) Lorsque la courbe elliptique E a une réduction additive en ν *, la partie non singulière* $\widetilde{E}(K_{résI})_{ns}$ *du groupe* $\widetilde{E}(K_{résI})$ *est isomorphe au groupe additif* $(K_{résI})^+$.

Preuve de ″ E a une réduction multiplicative en ν implique la partie non singulière de la courbe réduite $\widetilde{E}(K_{résI})_{ns} \cong K_{résI})^+$ ″

Soient un corps K muni d'une VNAD v, une courbe elliptique E sur le corps K , de discriminant Δ(E).et de coefficient c_4(E) .

Soient la courbe réduite $\widetilde{E}$ de discriminant Δ($\widetilde{E}$).et de coefficient $c_4(\widetilde{E})$.

Selon le théorème 19 , l'hypothèse ″la courbe elliptique E a une réduction multiplicative en ν″ est équivaut à : $\nu(\Delta(E))>0$ et $\nu(c_4)=0$.

Il en résulte que les invariants réduits $\Delta(\widetilde{E})=0$ et $c_4(\widetilde{E})\neq 0$. (1)

Le théorème 10 et (1) impliquent que la courbe réduite $\widetilde{E}$ de la courbe elliptique E modulo ν possède un nœud S .

Cela implique l'existence de deux tangentes à $\widetilde{E}$ au point S .

Soient les deux tangentes de la courbe $\widetilde{E}$ au nœud S : $y=\alpha_1 x+\beta_1$ et $y=\alpha_2 x+\beta_2$.

Soit la partie non singulière $\widetilde{E}_{ns}(K_{résI}) = \widetilde{E}_{ns}$ de la courbe réduite $\widetilde{E}$ / $K_{résI}$.

On considère l'application :

$$f : \widetilde{E}_{ns}(K_{résI}) \longrightarrow K^*_{résI}$$

$$(x , y) \longrightarrow \frac{y-\alpha_1 x-\beta_1}{y-\alpha_2 x-\beta_2}$$

Cette application est une bijection d'ensembles .

La partie non singulière $\widetilde{E}_{ns}$ est un groupe abélien par [19] .

Il en résulte que f est un isomorphisme de groupes abéliens .

Preuve de : ″E a une réduction additive en ν implique que la partie non singulière de la courbe réduite : $\widetilde{E}(K_{résI})_{ns} \cong (K_{résI})^+$ ″

Selon le théorème 19 , l'hypothèse ″la courbe elliptique E a une réduction additive en ν″ est équivaut à $\nu(\Delta(E))>0$ et $\nu(c_4)>0$. (2)

Il en résulte que les invariants réduits $\Delta(\widetilde{E})$ et $c_4(\widetilde{E})$ sont nuls . (3)

Le théorème 10 et (3) impliquent que la courbe réduite $\widetilde{E}$ de la courbe elliptique E modulo ν possède un point de rebroussement M .

Cela implique l'existence d'une seule tangente à $\widetilde{E}$ au point M : $y = \alpha x + \beta$

Alors , l'application définie par :

$$g : \widetilde{E}_{ns}(K_{résі}) \longrightarrow K^{+}_{résі}$$

$$(x , y) \longrightarrow \frac{y - x(M)}{y - \alpha x - \beta}$$

est un isomorphisme du groupe de MORDELL-WEIL $\widetilde{E}_{ns}(K_{résі})$ dans le groupe additif $K^{+}_{résі}$.

L'invariant modulaire j(E) d'une courbe elliptique E intervient dans la réduction selon le :

Théorème20 :

Soient un corps de nombres L muni d'une valuation non archimédienne discrète ν et une courbe elliptique E sur L , d'équation de WEIERSTRASS minimale en ν et d'invariant modulaire j(E) . Si l'invariant modulaire j(E) est entier sur L , alors la courbe elliptique E a une bonne réduction ou une réduction additive en ν .

Preuve :

Par définition , l'invariant modulaire d'une courbe elliptique E est la fraction :

$j(E)=c_4^3/\Delta(E)$. où $c_4= c_4(E)$

L'hypothèse ″ j(E) entier sur L ″ implique que $\nu(j) \geq 0$, pour toute valuation discrète ν de L .

Le résultat découle de l'équation minimale de E , le deuxième axiome de la définition d'une valuation et le théorème 19 .

Chapitre III

Torsion sur les courbes elliptiques

La structure de groupe abélien de type fini pour le groupe de MORDELL-WEIL E(K) d'une courbe elliptique sur un corps K implique , selon la théorie générale des groupes , des sous groupes de torsion du groupe E(K) .

Pour cette courbe elliptique le point P+P = 2P est déterminé par la règle géométrique de 3 points colinéaires de la courbe E

Les coordonnées de ce point 2P sont obtenues avec la théorie de l'intersection de la courbe elliptique E par la tangente au point P .

1.Coordonnées du point P+P =2P avec P=(x_P,y_P) et P ≠ 0_E :

Soit une courbe elliptique E d'équation de WEIERSTRASS :

$$E : y^2+a_1 x y+a_3 y = x^3 +a_2 x^2 + a_4 x + a_6 \qquad (1)$$

La tangente à la courbe elliptique E au point P coupe la courbe en un point simple M et au point double P.

Le point 2P est le symétrique –M du point simple M (figure 6)

L'équation de la tangente à la courbe E au point P=(x_P , y_P) est :

$$y - y_P = y'_P (x - x_P) \qquad (2)$$

En dérivant l'équation (1) de WEIERSTRASS par rapport à la variable x , on obtient :

$$2yy'+a_1 y + a_1 xy'+a_3 y' = 3x^2 + 2a_2 x + a_4 \ ;$$

les calculs donnent la dérivée :

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

(1) ,(2) et (3) impliquent une équation du 3ème degré en x qui admet 3 racines : une racine double x_p et une racine simple x_M , abscisse du point M.

La fonction symétrique ″ somme des racines ″ est égale à :

$$2x_P + x_M = y'^{2}_P + a_1 y'_P - a_2$$

On en déduit les coordonnées du point M :

$$\begin{cases} x_M = y'^{2}_P + a_1 y'_P - a_2 - 2x_P \\ y_M = y'_P (x_M - x_P) + y_P \end{cases} \qquad (4)$$

Le point 2P est le symétrique –M du point M .

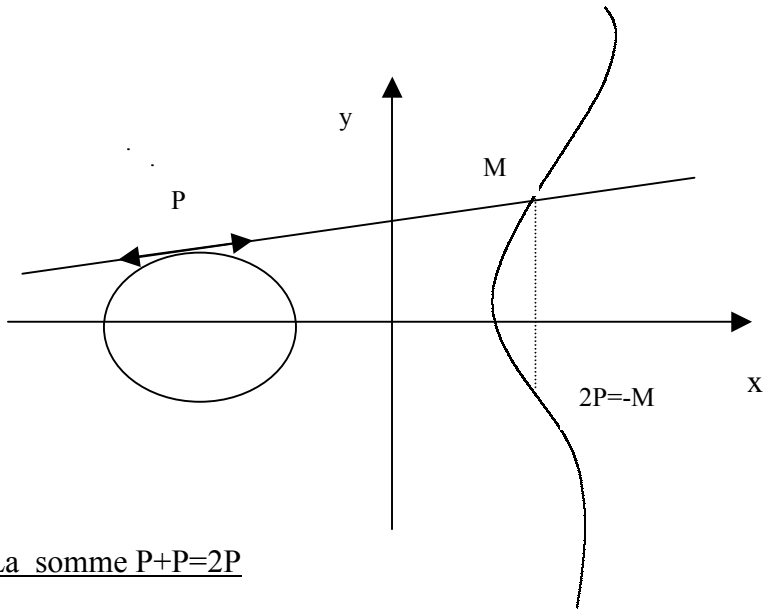
Les formules du symétrique et (4) donnent les coordonnées du point 2P :

$2P=(x_{2p}, y_{2p})$

$$x_{2p} = y_p'^2 + a_1 y_p' - a_2 - 2x_p = \frac{x^4 - b_4 x^2 - 2b_6 x - b_8}{4x^3 + b_2 x^2 + +2b_4 x + b_6} \quad ;$$

$$y_{2p} = -y_p'^3 - 2a_1 y_p'^2 + (3x_p - a_1^2 + a_2) y_p' + a_1(a_2 + 2x_p) - a_3 - y_p \qquad (5)$$

avec $y_p' = \frac{3x_p^2 + 2a_2 x_p + a_4 - a_1 y_p}{a_1 x_p + 2y_p + a_3}$



La somme P+P=2P Figure.6

2. Coordonnées du point P+P+P= 3P :

La relation 3P = 2P+P implique les coordonnées du point 3P avec la formule d'addition :

P_1+P_2 où $P_1=2P$, $P_2=P$ et $\lambda=\frac{y_{2p}-y_p}{x_{2p}-x_p}$

$3P= (x_{3P}, y_{3P})$

les calculs donnent les valeurs :

$x_{3P} = \lambda^2 + a_1\lambda - a_2 - x_{2P} - x_P$;

$y_{3P} = -\lambda^3 - 2a_1\lambda^2 + (a_2 - a_1^2 + 2x_{2P} + x_P)\lambda + a_1(a_2 + x_{2p} + x_P) - a_3 - y_{2p}$. (6)

Les formules (6) donnent la valeur *de* λ *en fonction des* a_i , x_p , y_p et y'_p

$$\lambda=\frac{-y_p'^3-2a_1y_p'^2+(a_2-a_1^2+3x_p)y_P'+a_1a_2-a_3+2a_1x_P-2y_P}{y'^2_P+a_1y_P-a_2-3x_P} \quad (7)$$

Les relations (6) et (7) impliquent des calculs prenant beaucoup de place et sans intérêt particulier .

Les coordonnées x_{3P} et y_{3P} du point 3P sont simplifiées en prenant l'équation de la courbe elliptique de la forme :

$E : y^2= x^3 + a_4 x + a_6$

C'est ce qu'a utilisé CASSELS pour obtenir des formules exploitables ; exposons sa méthode de calcul :

3. Coordonnées du point mP :

Soit un point P d'une courbe elliptique E , le point mP désigne :

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

Théorème 21 :

Soit une courbe elliptique E d'équation de WEIERSTRASS :

$E : y^2=x^3+A\,x+B \quad$ *avec* $4A^3+27B^2 \neq 0$

Soient les 6 polynômes ψ_m *de l'anneau* $9[x , y]$ *:*

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

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

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

Soit les deux formules de récurrence pour $m\geq 2$ *:*

$\psi_{2m} = 2\,\psi_m \ (\psi_{m+2} \ \psi_{m-1} \ - \psi^2_{m+2} \ \psi^2_{m+1})$

$\psi_{2m+1} = \psi_{m+2} \ \psi^3_m \ - \ \psi_{m-1} \ \psi^3_{m+1}$

Soient les deux polynômes :

$\Phi_m =x\,\psi^2_m \ - \psi_{m-1} \ \psi_{m+1} \quad$ *, polynôme en x , A ,B de degré* m^2.

$4y\,\omega_m =\psi_{m+2} \ \psi^2_{m-1} - \psi_{m-2} \ \psi^2_{m+1} \quad , \quad y^{-1}\,\omega_m$ *(pour m impair) et* ω_m *(pour m pair) sont des polynômes en x , A , B .*

Alors les coordonnées du point mP sont égales à :

$$mP = \left(\frac{\Phi_m}{\Psi_m^{\,2}}, \ \frac{\omega_m}{\Psi_m^{\,3}}\right) \qquad \text{pour des entiers naturels } m\geq 1$$

Preuve :

Elle est basée sur le procédé de raisonnement par récurrence , les formules d'addition P_1+P_2 et les coordonnées du point P+P =2P . Cf :[2] , lemme 7.2 , p 214 .

4. Sous groupes de m- torsion et groupe de torsion du groupe E(K) :

Définition 22 :

Soient une courbe elliptique E sur un corps K , un entier naturel m premier à la caractéristique du corps K et le groupe E(K) de MORDELL - WEIL de la courbe elliptique E .

Un point de m- torsion du groupe E(K) est un point P de E(K) d'ordre m :

$m\,P = 0_E$ *(1)*

Le groupe E(K)[m] est le sous groupe de m- torsion du groupe E(K)

$E(K)[m] = \{ P \in E(K) ; \ mP = 0_E \ \}$ *(2)*

Le groupe de torsion de la courbe elliptique E est l'ensemble:

$$E(K)_{tors} = \sum_{m\geq 0} E(K)[m] = T(E) \qquad (3)$$

Lorsque car(K) = m , le sous groupe de m- torsion est trivial :

E(K) [m]= E(K)[0] =$\{ 0_E \}$

Exemple :

Soit la courbe elliptique E sur un corps K d'équation :

$E: \quad y^2 = x^3 + 3x + 1$

Son discriminant vaut $\Delta(E) = -2^4.3^3.5 \neq 0$

Pour déterminer les points de 3- torsion , nous appliquons les formules de J.W.S.CASSELS pour n= 3 ; nous obtenons les coordonnées du point 3P :

$3P=(\frac{\Phi_3}{\Psi_3^2} , \frac{\omega_3}{\Psi_3^3})$

Un point de 3-torsion P =(x, y) a pour abscisse les racines du polynôme $\psi_3(x)=3x^4+18x^2+12x-9$

Ce point a pour coordonnées les solutions du système des deux équations :

$$\begin{cases} y^2 = x^3 + 3x + 1 & (1) \\ x^4 + 6x^2 + 4x - 3 = 0 & (2) \end{cases}$$

L'équation diophantienne (2) admet , éventuellement , comme solutions l'un des diviseurs de 3 : $\pm 1 , \pm 3$; seul le diviseur -1 est solution .

Pour x = -1 , $y^2 = -3$

Donc , il n' y a pas de points de 3-torsion sur un corps réel .

D'autre part , il y a deux points de 3 - torsion sur la courbe elliptique E sur le corps quadratique imaginaire K= $\Theta(\sqrt{-3})$:

$P_1 = (-1, -i\sqrt{3}) \quad et \; P_2 = (-1, i\sqrt{3}).$

5. Isogénie , réduction et sous groupes de m – torsion :

Le sous groupe de m- torsion d'une courbe elliptique E sur une clôture algébrique K^{alg} du corps K est un sous groupe du groupe $E(K^{alg})$; c'est aussi le noyau de l'isogénie ″multiplication m_E par m ″ sur la courbe elliptique E .

$E(K^{alg})[m] = \{ P \in E(K^{alg}) : m P = 0_E \} = Ker (m_E)$

La structure de ce groupe est déterminée par le :

Théorème 22 :

Soient une courbe elliptique E sur un corps algébriquement clos K , un entier naturel m premier à la caractéristique du corps K et le sous groupe de m- torsion E(K)[m] de la courbe elliptique E sur K . Alors , ce sous groupe est isomorphe au groupe produit :

$E(K)[m] \cong \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$

Preuve :

Selon le théorème 13 du chapitre II , l'application multiplication m_E par l'entier m est une isogénie de degré m^2 . (1)

Par définition le sous groupe de m- torsion E(K)[m] est le noyau de cette application (2)

(1) et (2) impliquent que le sous groupe de m- torsion E[m] est d'ordre m^2 .

Soient d un diviseur de m et le sous groupe de d- torsion E(K)[d] du groupe E(K)[m] :

Ce sous groupe de d- torsion est un sous groupe d'ordre d^2 .

Il en résulte que le sous groupe de m- torsion de la courbe elliptique E sur le corps K est isomorphe au produit de groupes cycliques :

$E(K)[m] \cong \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$.∎

Ce théorème implique que le sous groupe de m- torsion d'une courbe elliptique E sur un corps K est d'ordre au plus m^2 .

Le sous groupe de m- torsion est lié à la réduction des courbes elliptiques par le :

Théorème 23 :

Soit une courbe elliptique E sur un corps local K muni d' une valuation non archimédienne discrète v et le corps résiduel $K_{rési}$.

Soit la courbe réduite $\widetilde{E}$ modulo v , un entier m ≥1 premier à la caractéristique du corps résiduel $K_{rési}$ et le sous groupe E(K)[m] de m- torsion de la courbe elliptique .

Si la courbe réduite $\widetilde{E}(K_{rési})$ est une courbe elliptique , alors l'application réduction :

E(K)[m] ⟶ $\widetilde{E}(K_{rési})$ est injective.

Preuve :

Soit l'application réduction :

u : E(K) ⟶ $\widetilde{E}(K_{rési})$ (1)

Soient son noyau $E_1(K)$, la partie non singulière $\widetilde{E}_{ns}(K_{rési})$ de la courbe réduite $\widetilde{E}(K_{rési})$ et le sous groupe $E_0(K) = \{ P \in E(K) : \widetilde{P} \in \widetilde{E}(K_{rési})_{ns} \}$

On considère la suite de groupes abéliens :

$0 \to E_1(K) \to E_0(K) \to \widetilde{E}_{ns}(K_{rési}) \to 0$

Cette suite est exacte par [18] , Chapitre VII , proposition 2.1 , p174 (2)

L'hypothèse " la courbe réduite $\widetilde{E}$ est elliptique sur le corps résiduel $K_{rési}$ " implique que la partie non singulière $\widetilde{E}_{ns}$ de la courbe réduite $\widetilde{E}$ est identique à $\widetilde{E}$.

Il en résulte l'égalité : $E_0(K) = E(K)$. (3)

(2) et (3) impliquent que la suite des groupes abéliens :

$$0 \to E_1(K) \xrightarrow{i} E(K) \xrightarrow{u} \widetilde{E}(K_{rési}) \to 0$$ est une suite exacte .

Cela implique l'image du groupe $E_1(K)$ est égale au noyau de l'application u (4)

Soit la restriction u_1 de l'application u au sous groupe de torsion E(K)[m]

Son noyau : $\text{Ker } u_1 = \{ P \in E(K)[m] , \widetilde{P} = 0_{\widetilde{E}} \}$ un sous groupe de $E_1(K)$.

Le sous groupe $E_1(K)$ n'a pas de points non triviaux d'ordre m . cf [19] (5)

(5) implique que le noyau de u_1 est trivial : $\text{Ker } u_1 = 0_E$

Il en résulte que l'application : $u_1 : E(K)[m] \to \widetilde{E}(K_{rési})$ est injective.

Ce théorème donne une méthode de calcul des sous groupes de m - torsion des courbes elliptiques à l'aide de la théorie de réduction .

6. Racines de l'unité et sous groupes de torsion :

Définition 23 :

Soient une courbe elliptique E sur un corps K et Z_m le groupe des racines $m^{ème}$ de l'unité .

L'application bilinéaire de WEIL est l'application e_m :

$e_m : E(K)[m] \times E(K)[m] \to Z_m = \{ z =$ racines m^{es} de 1$\}$

de valeur : $e_m(P_1 , P_2) = g(P+P_1)/g(P)$

où P est un point du groupe E(K) tel que $g(P+P_1) \neq 0$ et $g(P) \neq 0$, une fonction $f \in K^{alg}(E)$ qui admet un point multiple d'ordre m , la fonction g est liée à f par : $f \circ m_E = g^m$

Cette application est :

1) Bilinéaire : $e_m(P_1+P_2 , P_3) = e_m(P_1 , P_3) . e_m(P_2 , P_3)$

$e_m(P_1 , P_2+P_3) = e_m(P_1 , P_2) . e_m(P_1 , P_3)$ pour tout point P_1 , P_2 , P_3 de E(K)[m]

2) Alternée : $e_m(P_1 , P_2) = e_m(P_2 , P_1)^{-1}$

3) Non dégénérée : si $e_m(P_1 , P_2) = 1$ pour tout point P_1 de E[m] , alors $P_2 = O_E$.

4) invariante par le groupe de Galois :

Pour tout point P de E (K)[m] et pour tout élément σ du groupe de Galois $G_{K^{alg}/K}$:

$$e_m(P_1, P_2)^\sigma = e_m(P_1^\sigma, P_2^\sigma)$$

L'application bilinéaire de WEIL , le groupe des racines m^e de 1et le sous groupe de m-torsion sont liés par le :

Théorème 24 :

Soient une courbe elliptique E sur un corps K , le sous groupe de m- torsion E(K)[m] de E et l'application bilinéaire de WEIL e_m. Alors :

1) Il existe un couple de points (P_1 , P_2) de E(K)[m] tels que l'image e_m (P_1 , P_2) est une racine primitive m^e de l'unité .

2) si E(K)[m] $\cong Z/mZ \oplus Z/mZ$ alors le corps K contient le groupe des racines m^e de 1 .

Preuve :cf [18],chapitre III , corollaire 8.11 , p98] .

7. Structure du groupe de torsion $E(\Theta)_{tors}$:

La détermination du groupe de torsion d'une courbe elliptique E définie sur le corps des nombres rationnels a été résolue entièrement par MAZUR .

***Théorème 25* :**

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

Les 11 groupes abéliens : $\mathbf{Z} / N\mathbf{Z}$ *pour* $1 \le N \le 10$ *et* $N = 12$

Les 4 groupes abéliens : $\mathbf{Z} / 2\mathbf{Z} \times \mathbf{Z} / 2N\mathbf{Z}$ *pour* $1 \le N \le 4$

Preuve : Cf [13 , (a)] .

Ce théorème implique que l'ordre du groupe de torsion T(E) d'une courbe elliptique sur le corps des nombres rationnels est au plus égal à 16 .

On peut déterminer le groupe de torsion d'une courbe elliptique sur Θ , en utilisant la théorie de la réduction modulo les nombres premier p qui ne divisent pas le discriminant des courbes elliptiques , avec l'application injective :

$E(\Theta)[m] \longrightarrow \widetilde{E}(IF_p)$

Exemple 1:

Soit la courbe elliptique E sur Θ , d'équation :

$E : y^2 + y = x^3 - x^2$ (1)

Les calculs donnent les invariants : $\Delta(E) = -11$; $c_4(E) = 2^4$; $j(E) = -2^{12}/11$

La courbe elliptique E a une bonne réduction pour tous les nombres premiers $p \neq 11$; il en résulte que les courbes réduites modulo p sont des courbes elliptiques sur le corps fini IF_p .

Calculons les points des courbes $\widetilde{E}(IF_p)$ réduites modulo p .

Pour p =2 , l'équation de la courbe réduite $\widetilde{E} / IF_2$ est :

$y^2 + y = x^3 + x^2$ (2)

Le calcul donne $\Delta(\widetilde{E}) = -43 = 1$ dans IF_2 ; cela implique que la courbe $\widetilde{E}$ est elliptique .

L'équation (2) admet 4 solutions dans le corps IF_2 .Donc le groupe $\widetilde{E}(IF_2)$ contient 5 points :

$\widetilde{E}(IF_2) = \{ 0_{\widetilde{E}} , (0,0) , (0 , 1) , (1 , 0) , (1 , 1) \}$

Pour p =3 , l'équation de courbe réduite $\widetilde{E} / IF_3$ est : $y^2 + y = x^3 + 2x^2$

Son discriminant vaut $\Delta(\widetilde{E}) = - 155 = 1$ dans IF_3 ; cela implique que la courbe $\widetilde{E}$ est elliptique .

Son équation admet 4 solutions dans le corps IF_3 . Donc le groupe $\widetilde{E}(IF_3)$ contient 5 points :

$\widetilde{E}(IF_3) = \{ 0_{\widetilde{E}} , (0,0) , (0 , 2) , (1 , 0) , (1 , 2) \}$

Pour p = 5 , l'équation de courbe réduite $\widetilde{E} / IF_5$ est : $y^2 + y = x^3 + 4x^2$

Son discriminant vaut $\Delta(\widetilde{E}) = 4$ dans IF_5 ; cela implique que la courbe $\widetilde{E}$ est elliptique .

Son équation admet 4 solutions dans IF_5 . Donc le groupe $\widetilde{E}(IF_5)$ contient 5 points :

$\widetilde{E}(IF_5) = \{ 0_{\widetilde{E}} , (0 , 0) , (1, 0) , (0 , 4) , (1 , 4) \}$

les points de $\widetilde{E}(IF_p)$ sont des point non triviaux sur la courbe elliptique E /Θ pour p = 2 , 3 et 5

Ces 4 points appartiennent à la courbe elliptique E (Figure 7.)

Le théorème 23 implique que l'application $E(\Theta)[m] \longrightarrow \widetilde{E}(IF_p)$ est injective

pour les nombres premiers p = 2 , 3 , 5 avec m et p premiers entre eux .

Il en résulte l'isomorphisme de groupes *:* $E(\Theta)_{tors} \cong \mathbf{Z} / 5\,\mathbf{Z}$

Ce résultat est conforme au théorème de MAZUR .

Le groupe de torsion est un groupe d'ordre premier , donc c'est un groupe cyclique .

Cherchons un générateur du sous groupe de torsion $E(\Theta)_{tors}$:

Le point P= (0 , 0) est un point de la courbe elliptique E .

En utilisant les règles de construction graphique (le symétrique d'un point , la somme de deux points distincts et confondus) (figure7) , on obtient les coordonnées des points 2P, 3P , 4P et 5P :

2P=(1 , -1) , 3P= (1 , 0) , 4P = (0 , -1) , 5P = (∞ , ∞) .

Cela implique : le point P =(0, 0) est un point d'ordre 5 .

Il en résulte que le point P=(0,0) est un générateur du groupe de torsion T(E) :

T(E) ={P= (0,0) , 2P=(1 , -1) , 3P= (1 , 0) , 4P = (0 , -1) , 5P = (∞ , ∞) } .

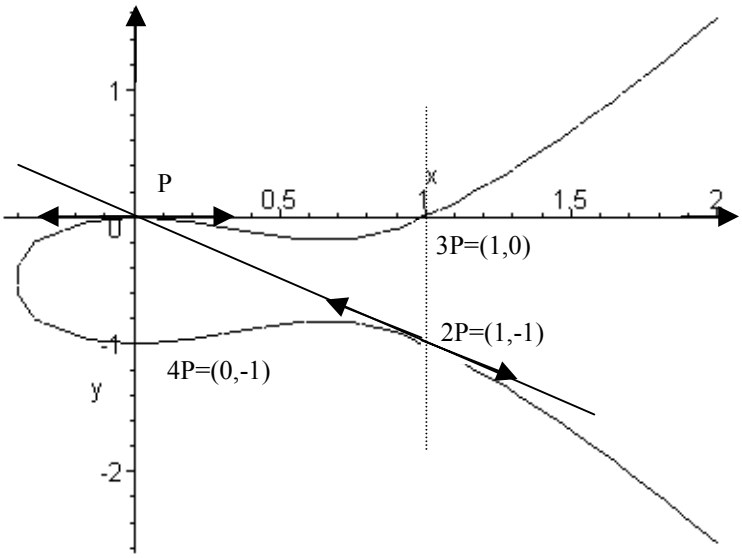


Figure 7

Les groupes de torsion ont été calculés pour des familles de courbes elliptiques particulières :

Théorème 26:

Soit la famille de courbes elliptiques E_t sur le corps Θ :

$E_t : y^2 = x^3 + t\,x$

Pour un entier rationnel $t \neq 0$ et sans facteur puissance $4^{ème}$, le groupe de torsion $T(E_t)$ est isomorphe à :

1) $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ *si* $t = -t'^2$ *(t'^2 = carré parfait d'un entier rationnel t')*

2) $\mathbf{Z} / 4\mathbf{Z}$ *si* $t = 4$

3) $\mathbf{Z}/ 2\mathbf{Z}$ *dans les autres cas .*

Preuve de : *" T(* E_t) $\cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ implique $t = -t'^2$, $t' \in \mathbf{Z}$ "

Soit la famille de courbes elliptiques sur Θ , d'équation :

$E_t : y^2 = x^3 + t\,x$ (1)

Les invariants de la famille E_t sont égaux à :

$\Delta(E_t) = -64t^3 \neq 0$ et $j(E_t) = 1728$.

Soit la courbe réduite $\widetilde{E_t}(IF_p)$ de la courbe elliptique E_t modulo p , $p \neq 2$

Le groupe $\widetilde{E}_t(IF_p)$ est d'ordre p+1 , pour tous les nombres premiers $p \equiv 3 \bmod 4$. par [K .IRELAND and M.ROSEN , A classical introduction to modern number theory , Springer - verlag 1982 , Théorème 5 , p 307] .

Pour $p \neq 2$, les courbes elliptiques E_t ont une bonne réduction modulo p

Le théorème 23 implique que pour tout entier naturel m premier à p , l'application :

$E(\Theta)[m] \rightarrow \widetilde{E}_t(IF_p)$ est injective .

Cela implique que le groupe de torsion $T(E_t)$ est d'ordre un diviseur de p+1 , pour tous les nombres premiers $p \equiv 3 \bmod 4$. (2)

L'hypothèse " $p \equiv 3 \bmod 4$ " implique $p+1 \equiv 0 \bmod 4$ (3)

(2) et (3) impliquent que le groupe de torsion $T(E_t)$ est d'ordre un diviseur de 4 . (4)

(4) et la théorie des groupes abéliens finis impliquent que le groupe de torsion $T(E_t)$ est isomorphe à l'un des 3 groupes abéliens : $\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z}$.

Si le groupe de torsion $T(E_t) \cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$, il en résulte que le groupe de torsion $E_t(\Theta)_{tors}$ contient 3 points d'ordre 2 . (5)

Les points $P = (x, y)$ d'ordre 2 de la courbe elliptique E_t ont pour ordonné $y = 0$ (6)
(1) et (6) impliquent que l'abscisse x est racine de l'équation : $x^3 + t\,x = 0$ (7)

(5) et (7) impliquent que :

l'équation $x^3 + t\,x = 0$ admet 3 racines rationnelles $x_1 = 0$, $x_2 = \sqrt{-t}$ et $x_3 = -\sqrt{-t}$ (8)

(8) implique : $-t = t'^2$ est le carré d'un rationnel t' .

Preuve de : " $T(E_t) \cong \mathbf{Z}/4\mathbf{Z}$ implique $t = 4$ "

L'hypothèse " $T(E_t) \cong \mathbf{Z}/4\mathbf{Z}$ " implique l'existence d'un point d'ordre 4 sur la courbe E .

Un point d'ordre 4 de la courbe elliptique E vérifie la relation : $4P = 0_E$

Cela implique que 2P est point d'ordre 2 .

(1) implique que le point (0,0) est un point d'ordre 2 de la courbe elliptique E .

Il en résulte : 2P = (0 , 0)

La formule d'abscisse du point 2P :

$$x_{2p} = \frac{x^4 - 2x^2t + t^2}{4(x^3 + tx)} = \frac{(x^2 - t)^2}{4(x^3 + tx)} \qquad (2)$$

l'hypothèse 2P = (0 , 0) et (2) impliquent :

$P = (t^{1/2}, (4t^3)^{1/4})$

L'hypothèse " t sans facteur puissance $4^{ème}$ " implique t = 4

Pour t = 4 , le point P = (2 , 4) est un point d'ordre 4 de $E_t(\Theta)$.

Preuve de : " $T(E_t) \cong \mathbf{Z}/2\mathbf{Z}$ implique $t \neq -t'^2$, $t' \in \mathbf{Z}$ et $t \neq 4$ "

L'hypothèse $T(E_t) \cong \mathbf{Z}/2\mathbf{Z}$ implique que le groupe $E_t(\Theta)$ contient un seul point d'ordre 2

D'après la preuve de (1) , l'abscisse d'un point P = (x , y) d'ordre 2 est solution de l'équation :

$x^3 + t\,x = 0$

Donc cette équation admet une seule racine rationnelle x = 0 et $x^2 + t$ n'admet pas de racine rationnelle .

8.Nombres congruents et torsion :

Définition 24 :

Un nombre congruent est un nombre rationnel positif égal à l'aire d'un triangle rectangle de cotés rationnels .

Les nombres congruents impliquent des courbes elliptiques sur Θ d'équation particulière .

Soit un triangle rectangle de côtés X< Y < Z ; alors l'aire de ce triangle est égal à :

$XY / 2 = n$ = nombre congruent

Les changements de variables : u = Z/2 et $v = (X^2-Y^2)/4$ impliquent l'équation :

$u^4 - n^2 = v^2$

La multiplication par u^2 donne l'équation :

$u^6 - n^2 u^2 = (u\,v)^2$,

Le changement $u^2 = x$, $u\,v = y$ donne l'équation :

$y^2 = x^3 - n^2x$

Le nombre congruent n est lié au groupe de torsion $T(E_n)$ de la courbe elliptique E_n par le :

Théorème 27:

Soit une famille de courbes elliptiques E_n sur le corps Θ paramétrée par un nombre congruent n

$E_n : y^2 = x^3 - n^2x$

Alors :

1) le groupe de torsion $T(E_n)$ est d'ordre 4

2) Le rang de la famille de courbes elliptiques E_n est différent de 0 équivaut à ″n est un nombre congruent ″.

Preuve de ″ le groupe de torsion T(E_n) est d'ordre 4 ″

Soit une famille de courbes elliptiques E_n sur le corps Θ paramétrée par un nombre congruent n

$E_n : y^2 = x^3 - n^2 x$

Les calculs donnent le discriminant : $\Delta(E_n) = (2n)^6$.

Soient un nombre premier p et la courbe elliptique $E_n(IF_p)$ sur le corps fini IF_p

Considérons l'application :

$T(E_n) \longrightarrow E(IFp)$

Cette application est un homomorphisme de groupes par [8] ,proposition 17 . (1)

En plus cette application est injective par [8] , lemme , p 44 . (2)

Pour les nombres $q = p^f$, avec p ne divise pas 2n et $q \equiv 3 \bmod 4$; le groupe $E_n(IF_p)$ est d'ordre q+1 par [8] , proposition 16. (3)

(1) , (2) et (3) impliquent que le groupe de torsion $T(E_n)$ est d'ordre un diviseur de 4 . (4)

Le groupe des points Θ rationnel contient 3 points non triviaux d'ordre 2 : (0 , 0) , (0 , ± n) (5)

(4) et (5) impliquent que le groupe de torsion $T(E_n)$ est d'ordre 4 .

Preuve de(2) : cf [8] , chapitre 1, §9, proposition18 .

Lorsque le corps de définition de la courbe elliptique E est différent du corps des nombres rationnels , la détermination du groupe de torsion n'est pas encore résolue entièrement ; il y a quelques résultats partiel.

Chapitre IV

Courbes elliptiques sur un corps quadratique

La détermination des groupes de torsion de courbes elliptiques sur un corps quadratique $K = \Theta(\sqrt{d})$ peut être étudiée par plusieurs théories : courbes modulaires et leurs jacobiennes , valuations d'un corps de nombres , réductions des courbes elliptiques .

1.Courbes elliptiques E/$\Theta(\sqrt{d})$ et points d'ordre premier :

Nous suivons la méthode de KAMIENNY développée dans [6] .

Selon KAMIENNY , il n' y a pas de courbes elliptiques sur un corps quadratique $K= \Theta(\sqrt{d})$ possédant un point d'ordre p pour p = 17 , 19 , 23 , 29 et 31 . Dans ce cas , la courbe modulaire $X_1(p)$ admet une jacobienne $J_1(p)$ dont le groupe de MORDELL-WEIL est fini . Les seules autres valeurs de p possédant cette propriété sont : p = 41, 47 , 59 et 71 . (1)

A tout nombre rationnel premier p , on associe la courbe $Y_0(p)$, sur le corps Θ , qui classifie les classes d'isomorphisme de courbes elliptiques E possédant un sous groupe rationnel $E(\Theta)[p]$ d'ordre p . Le complété de cette courbe par les pointes zéro et l'infini est la courbe modulaire :

$X_0(p) = Y_0(p) \cup \{ \text{les pointes 0 et } \infty \}$; (2)

Il y a une courbe $Y_1(p)$, sur le corps Θ , qui classifie les classes d 'isomorphisme de courbes elliptiques possédant un point d'ordre p . Le complété de cette courbe $Y_1(p)$ par les (p-1) pointes est la courbe modulaire :

$X_1(p) = Y_1(p) \cup \{ \text{les (p-1) pointes} \}$ (3)

Les courbes $Y_1(p)$ et $X_1(p)$ sont soumises à l'action du sous groupe modulaire :

$$\Gamma_1(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(Z);\ c \equiv 0,\ a \equiv d \equiv 1 \bmod p \right\} \quad (4)$$

Les courbes $X_0(p)$ et $Y_0(p)$ sont soumises à l'action du sous groupe modulaire :

$$\Gamma_0(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(Z);\ c \equiv 0 \bmod p \right\} \qquad (5)$$

Chaque courbe modulaire $X_i(p)$ admet une courbe jacobienne :

$J_i(p)$ pour $i = 0 , 1$

D'après la théorie des courbes modulaires cf [6] , [17] et [13 (b)] , l'application :

$X_1(p) \longrightarrow X_0(p)$ est de degré $\frac{p-1}{2}$.

Pour tout diviseur n du degré $\frac{p-1}{2}$, il existe une courbe unique $X^{(n)}(p)$ telle que :

L' application $X^{(n)}(p) \longrightarrow X_0(p)$ est de degré n . cf[6]

Les courbes $X_0(p)$, $X^{(n)}(p)$ et leurs jacobiennes sont des variétés abéliennes .

La courbe modulaire $X^{(n)}(p)$ admet la jacobienne $J^{(n)}(p)$.

La variété abélienne $J^{(n)}(p)$ possède une bonne réduction en tout nombre rationnel premier $q \neq p$ .Les jacobiennes $J_1(p)$, pour p = 17 , 19 , 23 et les courbes $J^{(7)}(29)$ et $J^{(5)}(31)$ sont des variétés abéliennes .

Dans chaque cas , le quotient $A = J^{(n)}(p) / J_0(p)$ est une courbe qui a une bonne réduction sur l'unique sous corps L du p-ème corps cyclotomique , de degré $[L : \Theta] = n$ .cf[6]

Nous désignons par X les courbes modulaires : $X_1(17)$, $X_1(19)$, $X_1(23)$, $X^{(7)}(29)$, $X^{(5)}(31)$, par J leurs jacobiennes associées respectivement : $J_1(17)$, $J_1(19)$, $J_1(23)$, $J^{(7)}(29)$, $J^{(5)}(31)$ et par d le degré de l'application : $X \longrightarrow X_0(p)$

Les caractérisations des 10 courbes X et J précédentes sont portées dans le tableau extrait de [6] .

X	genre	d	J	Dim J
$X_1(17)$	5	8	$J_1(17)$	5
$X_1(19)$	7	9	$J_1(19)$	7
$X_1(23)$	12	11	$J_1(23)$	12
$X^{(7)}(29)$	8	7	$J^{(7)}(29)$	8
$X^{(5)}(31)$	6	5	$J^{(5)}(31)$	6

Les groupes de MORDELL-WEIL des jacobiennes sont précisés par :

Théorème 28 :

Le groupe J(Θ) est fini pour les cinq variétés abéliennes :

$J = J_1(17)$, $J_1(19)$, $J_1(23)$, $J^{(7)}(29)$ et $J^{(5)}(31)$.

Preuve :

Dans chacun des 5 cas , la variété abélienne J se décompose sur le corps Θ , à isogénie près , en un produit $J_0(p) \times A$, où A est une variété abélienne de genre un .Donc A est une courbe elliptique .

B . MAZUR a montré que les groupes $J_0(p)(\Theta)$ sont finis pour p = 17 , 19 , 23 , 29 et 31 cf [13, (b)] .

Le groupe A(Θ) est fini par la proposition 3.2 et le lemme 3.3 de[6] .

Il en résulte que le groupe J(Θ) est fini .

L'inexistence d'un point K- rationnel d'ordre p sur la courbe elliptique est établie par le :

Théorème 29 :

Il n'existe pas de courbe elliptique E sur un corps quadratique $K = \Theta(\sqrt{d})$ dont le groupe de MORDELL –WEIL $E(\Theta(\sqrt{d}))$ possède un point d'ordre premier p = 17 , 19 , 23 , 29 et 31 .

Preuve :

Soient les courbes modulaires $X_1(p)$ lorsque p= 17 ,19 et 23 et $X^{(n)}(p)$ lorsque p = 29 ou 23 .
On désigne par X ces courbes modulaires .

Soit un corps de nombres quadratique $K = \Theta(\sqrt{d})$.

On suppose l'existence d'une courbe elliptique E sur K possédant un point P d'ordre p pour p =17, 19 , 23 , 29 et 31 .

Cela implique l'existence d'une paire (E, P) constitué de la courbe elliptique E et du point P .

Cette paire (E , P) correspond à un point K-rationnel Y de la courbe modulaire X .

La suite de la preuve repose sur plusieurs résultats de la théorie des courbes modulaires : point K- rationnels de la courbe $X_1(P)$ et $X^{(n)}(p)$, réduction modulo 3 , diviseurs et équivalence linéaire de diviseurs sur une courbe .cf [6] .

2. Groupe de torsion et invariant modulaire :

Pour la détermination des groupes de torsions d'une courbe elliptique sur un corps quadratique K = $\Theta(\sqrt{d})$, nous suivons la méthode exposée par FUNG et ses co- auteurs dans [5] et [14] .

Soit une courbe elliptique E sur un corps quadratique K = $\Theta(\sqrt{d})$, où d est un entier rationnel sans facteur carré , de discriminant Δ (E) , d'invariant modulaire j(E) , de groupe de MORDELL-WEIL E(K) et de groupe de torsion T(E) .

D'après le théorème de MODELL-WEIL , ces groupes de torsion T(E) sont finis .

Utilisons la théorie des valuations sur un corps de nombres algébriques L .Toute valuation non archimédienne discrète ν : L $\longrightarrow$ IR détermine un anneau A_ν des ν- entiers de L , un idéal I_ν maximal , un groupe U_ν des ν -unités , un corps résiduel $L_{résI}$ =A_ν / I_ν et une place P_ν associée à l'idéal I_ν . Considérons l'ensemble $\sum(L)$ des places du corps L , une partie finie S_0 de l'ensemble $\sum(L)$ contenant la place infinie P_∞ (place associée à la valuation archimédienne de L) et le complémentaire :

$\sum(L)$ -S_0 = S

Selon la théorie des places , cet ensemble S détermine les sous ensembles particuliers : l'anneau O_S des S –entiers de L , l'idéal maximal I_S et le groupe U_S des S - unités .

La structure du groupe U_S est déterminée par le théorème de DIRICHLET – HASSE :

U_S est isomorphe à $W \times Z^{s-1}$,

où W = groupe des racines de 1 contenu dans le corps L et s = card(S_0).

Alors , toute S –unité u admet une représentation unique :

$$u = z\, u_1^{r1} u_2^{r2} \ldots\ldots\ldots\ldots u_{s-1}^{rs-1}$$

avec z $\in$ W , $r_i \in$ Z et (u_1 ,u_2 ,……., u_{s-1}) = système de S - unités fondamentales de L .

Nous considérons des courbes elliptiques E sur un corps quadratique K = $\Theta(\sqrt{d})$, avec un invariant modulaire j(E) S- entier de K .

Théorème 30 :

Il y a un nombre fini de courbes elliptiques E sur un corps quadratique K , dont l'invariant modulaire j(E) est S – entier de K , qui possèdent un groupe de torsion T(E) contenant un sous groupe isomorphe à :

$\boldsymbol{Z}/n\boldsymbol{Z}$ *pour n = 4 , 5 , 7 , 9 , 11 ;*

$\boldsymbol{Z}/3\boldsymbol{Z} \oplus \boldsymbol{Z}/d\boldsymbol{Z}$ *pour d = 2 , 3*

où S est le complémentaire d'une partie finie S_0 de places contenant la place P_∞ dans l'ensemble des places du corps K .

Preuve de ″ il y a un nombre fini de courbes elliptiques E sur un corps quadratique K , dont j(E) est S – entier de K et T(E) contenant un sous groupe isomorphe à $\boldsymbol{Z}/5\boldsymbol{Z}$ ″

Soient un ensemble fini S_0 de places contenant la place P_∞ de K , l'ensemble $\sum(K)$ des places de K et le complémentaire $S = \sum(K) - S_0$.

Selon REICHERT [16] , il y a seulement un nombre fini t dans K satisfaisant les 2 conditions :

(1) t est une S –unité ;

(2) $0 \leq \nu_p(t^2 - 11t - 1) \leq 3\,\nu_p(5)$, pour toute valuation P – adique , P dans S .

Considérons l'extension quadratique $K(\sqrt{5})$ de K et l'ensemble fini S' de places de $K(\sqrt{5})$ qui prolongent les places de K .

Le polynôme $t^2 - 11t - 1$ se factorise dans le corps $K(\sqrt{5})$;

$$t^2 - 11t - 1 = \left(t - \tfrac{11}{2} + \tfrac{5}{2}\sqrt{5}\right)\left(t - \tfrac{11}{2} - \tfrac{5}{2}\sqrt{5}\right)$$

Chaque facteur est une S ' – unité dans $K(\sqrt{5})$

Prenons une courbe elliptique E d'équation :

E : $y^2 + (1-t)xy - by = x^3 - t\,x^2$, avec t ci dessus .

Alors les relations ″ t est une S –unité qui satisfait la condition (2) ″ implique que l'invariant modulaire j(E) est S – entier .

Pour achever la preuve, il faut utiliser [16] .

€

Chapitre V

Courbes elliptiques sur un corps cubique pur

Soit un corps de nombres cubique pur $K = \Theta(\theta_1)$, $\theta_1 = \sqrt[3]{ab^2}$, d'anneau des entiers A_K .

Considérons une valuation non archimédienne discrète :

$\nu : K \longrightarrow IR$, $K= \Theta(\theta_1)$.

Soit le complété K_ν du corps K en la valuation ν ; il en résulte la relation d'inclusion :

$E(K) \subset E(K_\nu)$

Soit son anneau de valuation A_ν , son idéal maximal I_ν , le corps résiduel $K_{résí} = A_\nu / I_\nu$; on suppose ce corps résiduel fini à $q = p_\nu^f$ éléments .

L'équation de WEIRSRTASS d'une courbe elliptique E sur K est minimale lorsque la valuation ν satisfait :

$\nu(\Delta(E)) \geq 0$ et $\nu(\Delta(E)$ minimale et $\nu(a_i) \geq 0$.

Cette équation minimale est définie à isomorphisme prés .

l'application réduction modulo ν

$f_\nu : E(K_\nu) \longrightarrow \widetilde{E}(K_{résí})$

réduit la courbe elliptique E en une courbe $\widetilde{E}$ et les coefficients a_i en $\nu(a_i) = \widetilde{a}_i$

Lorsque la courbe réduite $\widetilde{E}$ n'est pas elliptique , elle admet un point singulier $\widetilde{S}$ et une partie non singulière $\widetilde{E}(K_{résí})_{ns}$.

D'après la classification des réductions d'une courbe elliptique E , il y a 3types de réduction :

E a une bonne réduction en ν lorsque $\widetilde{E}(K_{résí}) = \widetilde{E}(K_{résí})_{ns}$;

E a une réduction multiplicative en ν lorsque $\widetilde{E}(K_{résí})_{ns}$ est isomorphe au groupe multiplicatif $K^*_{résí}$;

E a une réduction additive en ν lorsque $\widetilde{E}(K_{résí})_{ns}$ est isomorphe au groupe additif $K^+_{résí}$.

L'ensemble $E(K_\nu)_0 = \{P \in E(K_\nu) : \widetilde{P} \in \widetilde{E}_{ns}(K_{résí})\}$ est un sous groupe de $E(K_\nu)$.

Le groupe quotient $E(K_\nu)/ E(K_\nu)_0$ est cyclique d'ordre $\nu(\Delta(E))=-\nu(j(E))$ si E a une réduction multiplicative ; ce groupe est d'ordre ≤ 4 si E a une bonne réduction ou une réduction additive .

Dans le cas d'une bonne réduction en ν , la courbe réduite $\widetilde{E}$ modulo ν satisfait le théorème de HASSE relatif aux courbes elliptiques sur un corps fini :

card $\widetilde{E}(K_{rési}) \leq 1+ q_\nu + 2\sqrt{q_\nu}$, où q_ν = card ($K_{rési}$)

Alors , l'ordre du groupe de torsion T(E) est borné :

Théorème 31 :

Soit une courbe elliptique E sur un corps de nombres cubique pur K , une VNAD ν sur K , l'anneau de valuation A_ν , l'idéal maximal I_ν , le corps résiduel $K_{rési}$ en ν à q_ν éléments et les groupes de torsion T(E) et T($\widetilde{E}$) des courbes E et $\widetilde{E}$ respectivement .

1) Lorsque E a une bonne réduction en ν , alors :

$$cardT(E) \,.card\, T(\widetilde{E}) \leq (1+ q_\nu + 2\sqrt{q_\nu})\, p^{2t} \quad ; \qquad (1T)$$

2) Lorsque l'idéal maximal I_ν divise p_ν =2 et lorsque E a une réduction additive en ν , alors :

$$cardT(E) \text{ divise } 2^{2t} \times 48 \quad ; \qquad (2T)$$

3) Lorsque l'idéal maximal I_ν divise p_ν = 3 et E a une réduction additive en ν , alors :

$$cardT(E) \text{ divise } 3^{2t} \times 108 \quad ; \qquad (3T)$$

4) Lorsque l'idéal maximal I_ν divise p_ν = 5 et E a une réduction additive en ν , alors :

$$cardT(E) \text{ divise } 5^{2t} \times 300 \quad ; \qquad (4T)$$

où t = 0 si $p_\nu - 1 > e_\nu$, e_ν = indice de ramification de p_ν dans $K_{rési}$;

et t = max $\{n \in IN ; \ (p_\nu - 1)p_\nu^{n-1} \leq e_\nu \}$ si $p_\nu - 1 > e_\nu$.

Preuve :

Elle découle des propriétés des courbes réduites et des groupes de T(E)

Pour plus de détails , consulter cf[5] .

Les groupes de torsion T(E) de courbes elliptiques sur un corps cubique pur peuvent être déterminés avec les résultats à l'aide du :

Théorème 32 :

Soit une courbe elliptique E sur un corps cubique pur K , d'invariant modulaire j(E) et une valuation non archimédienne ν sur le corps K .On suppose que $\nu(j(E)) \geq 0$ pour toute valuation ν d'idéal maximal I_ν divisant 2 ou 3 .

Alors le groupe de torsion T(E) de E est isomorphe à l'un des 9 groupes abéliens :

$\boldsymbol{Z}/N\boldsymbol{Z}$ *pour N = 2 , 3 , 4 , 5 et 12*

$\boldsymbol{Z}/2\boldsymbol{Z} \oplus \boldsymbol{Z}/D\boldsymbol{Z}$ *pour D = 2 , 3 , 6 .*

{ 0_E }

Preuve :

Le théorème 5 relatif à la décomposition des nombres rationnels premiers dans un corps cubique pur K implique que pour toute place P_ν divisant 2 , la norme de P_ν vaut

$N(P_\nu) = q_\nu = p_\nu^1 = 2$; (1)

et pour toute place P_ν divisant 3 , la norme de P_ν vaut $N(P_\nu) = q_\nu = p_\nu^1 = 3$; (2)

(1) et (2) et le théorème de HASSE relatif aux courbes elliptiques sur un corps fini , impliquent les deux inégalités :

card $\widetilde{E}(K_{résî}) < 6$; si E a une bonne réduction modulo une place P_ν qui divise 2 , (3)

card $\widetilde{E}(K_{résî}) < 8$; si E a une bonne réduction modulo une place P_ν qui divise 3 . (4)

L'hypothèse $\nu(j(E)) \geq 0$ implique que E a une bonne réduction ou une réduction additive modulo ν (5)

Les relations (3) et (4) et le théorème 31 impliquent :

card T(E) = 5 , lorsque le groupe E(K) contient un point d'ordre premier $p \geq 5$. (6)

Lorsque le groupe E(K) ne contient pas de point d'ordre premier $p \geq 5$, alors :

card T(E) est un diviseur de $2^8 \times 3$ si E a une réduction additive en une place P_ν divisant 2 (7)

card T(E) est un diviseur de 4×3^5 si E a une réduction additive en une place P_ν divisant 3 (8)

avec les formules (6) , (7) et (8) nous obtenons les résultats énoncés .

Le cas où l'invariant modulaire j(E) de la courbe elliptique E est un entier du corps K est résolu par le :

Théorème 33 :

Soit une courbe elliptique E sur un corps cubique pur , avec un invariant modulaire j(E) entier de K . Alors le groupe de torsion T(E) est isomorphe à l'un des 7 groupes abéliens :

$\boldsymbol{Z}/N\boldsymbol{Z}$ *pour N = 2 , 3 , 4 , 5 et 6* ; $\boldsymbol{Z}/2\boldsymbol{Z} \oplus \boldsymbol{Z}/2\boldsymbol{Z}$, *{* O_E *}*

Preuve :

On utilise tous les résultats précédents : arithmétique des corps cubiques purs , structure d'anneau des entiers , théorème de décomposition des idéaux , relation valuation – réduction - groupes de torsion .cf [5]

Donnons quelques exemples tirés de [5] :

Exemple 1 :

Courbe elliptique E : $y^2 = x^3 + A\,x + B$ sur le corps cubique pur $K = \Theta(\sqrt[3]{2})$ et $T(E) \cong \mathbf{Z}/4\mathbf{Z}$.

Les calculs donnent les valeurs de A , B et j(E) dans A_K :

$A = -27(16 - 16\sqrt[3]{2} + \sqrt[3]{4})$; $B = 4 \times 81(11 - 16\sqrt[3]{2} + 5\sqrt[4]{4})$ et $j(E) = 16 \times 9(-450 + 270\sqrt[3]{2} + 71\sqrt[3]{4})$

Exemple 2 :

Courbe elliptique E : $y^2 = x^3 + A\,x + B$ sur le corps cubique pur $K = \Theta(\sqrt[3]{5})$ et $T(E) \cong \mathbf{Z}/4\mathbf{Z}$.

Les calculs donnent les valeurs de A , B et j(E) dans A_K :

$A = -81(43 + 23 + \sqrt[3]{5} + 19\sqrt[3]{25})$; $B = 162(143 + 91\sqrt[3]{5} + 55\sqrt[3]{25})$ et $j(E) = 18(327 - 13\sqrt[3]{5} + 15\sqrt[3]{25})$

Exemple 3 :

Courbe elliptique E : $y^2 = x^3 + A\,x + B$ sur le corps cubique pur $K = \Theta(\sqrt[3]{31})$ et $T(E) \cong \mathbf{Z}/4\mathbf{Z}$.

Les calculs donnent les valeurs de A , B et j(E) dans A_K :

$A = -27(427 + 133\sqrt[3]{31} + 43\sqrt[3]{961})$; $B = 162(463 + 145\sqrt[3]{31} + 47\sqrt[3]{961})$ et

$j(E) = 18(-1713 + 529\sqrt[3]{31} + 15\sqrt[3]{961})$

Exemple 4 :

Courbe elliptique E : $y^2 = x^3 + A\,x + B$ sur le corps cubique pur $K = \Theta(\sqrt[3]{2})$ et $T(E) \cong \mathbf{Z}/5\mathbf{Z}$.

Les calculs donnent les valeurs de A , B et j(E) dans A_K :

$A = 108(132 - 96\sqrt[3]{2} - 7\sqrt[3]{4})$; $B = 16 \times 27(1303 + 576\sqrt[3]{2} - 1278\sqrt[3]{4})$ et $j(E) = 256(103 + 26\sqrt[3]{2} + 32\sqrt[3]{4})$

(Note de FUNG et ses 3 co auteurs ; les calculs ont été effectués sur PCMX- 2 , système algébrique de calcul SIMATH)

En conclusion , ces résultats sur les groupes de torsion sur les corps de nombres sont partiels ; il reste beaucoup à faire : les courbes elliptiques sur les corps cubiques purs $\Theta(\sqrt[3]{ab^2})$ avec a > 1 , b> 1 , les corps cubiques galoisiens , et tous les corps de nombres de degré [L : K] > 3 .

Bibliographie

[1] **Z.I . BOREVITCH et I.R CHAFAREVITCH** , Théorie des nombres , GRATHIER-VILLARS , Paris , 1967 .

[2] **J.W. CASSELS** ,Diophantines equations with spécial référence to elliptic curves , J London Math . Soc (1965/1966) p193-291 .

[3] **R .DEDEKIND ,** Über die anzahle der Idealklassen in reinen kubischen zahlkorpern , J. Reine .Angew .Math .121 (1900) 40 – 123 .

[4] H .FARKAS and I .KRA , Riemann surfaces , G .T , Berlin – Heidelberg – New York , Springer –verlag , 1980 .

[5] **G. FUNG , H. STROHER , H . WILLIAMS and H . ZIMMER** , Torsion groups of elliptic curves with integral j- invariant over pure cubic fields ,J of N . Th 36(1990), 12-45.

[6] **S . KAMIENNY** , Torsion points on elliptic curves over all quadratic fields , Duke .Math .J .vol 53 , No1 (1986) , p 157-162 .

[7] **M. A . KENKU and F . MOMOSE** ,Torsion points on elliptic curves defined over quadratic fields , Nagoya . Math .J .vol 109 (1988) , p125-149 .

[8] **N . KOBLITZ** ; introduction to elliptic curves and modular forms , Springer -verlag (1984).

[9] **D.S.KUBERT** , Universel bounds on the torsion of elliptic curves , Proc .London .Math . Soc (3) 33(1976) , p193-237 .

[10] **D.S .KUBERT** , Modular units , Springer –verlag , New York , 1981 **.**

[11] S. LANG , Elliptic curves , Diophantine analysis , Springer –verlag , 1978 .

[12] **D.A .MARCUS** , Number fields , Springer –verlag , New York , 1977 .

[13] **B . MAZUR** ,

a) Rational isogenies of prime degree , Invent.Math.44 (1978), p129-162

b) Modular curves and the Eiseintein Ideal , I.H.E.S , Publi. Math 47(1977) , 33-186 .

[14] **H.H.MULLER , H. STROHER and H.G ZIMMER** ,Torsion groups of elliptic curves with integral j-invariant over quadratic fields , J. Reine .Angew . Math (1989) 397 , p100-161 .

[15] H.H.MULLER , H. STROHER and H.G ZIMMER , Complete determination of all torsion groups of elliptic curves with integral j –invariant over quadratic and cubic number fields ; proceedings .intern .Numb .Th , Laval university , Quebec , Canada (1987) , 671-698

[16] M . A .REICHERT , Explicit determination of non trivial torsion structures of elliptic curves over quadratic number fields , Math .Comp .46 (1986) 637-658 .

[17] **G.SHIMURA** , Introduction to the arithmetic theory of automorphic functions, Princeton .U .Press N^0 11 (1971) .

[18] **J.H .SILVERMAN** , The arithmetic of elliptic curves, G.T.M 106 , Springer -verlag (1986).

[19] **J.TATE** , The arithmetic of elliptic curves , Invent. Math 23 (1974) , p 179-206 .

[20] **E .WEISS ,** Algebraic number theory , Mac Grew – Hill , New York .