N° d'ordre : 16 / 2004 – M / MT.

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université des Sciences et de la Technologie
Houari Boumediene

جامعة هواري بومدين
للعلوم والتكنولوجيا
U S T H B

Faculté de Mathématiques

Mémoire Présenté pour l'obtention du diplôme de Magister en Mathématiques

Spécialité : Algèbre et théorie des nombres

Par M^elle^ **AZZI SOUAD**

Sujet

Groupes de Selmer de twists de courbes elliptiques

Soutenu publiquement le : 15/07/2004, devant le jury composé de :

Mr M.S.HACHAICHI Maître de conférences à L'U.S.T.H.B Président.
Mr M .ZITOUNI Professeur à L'U.S.T.H.B Directeur de thèse. Mr
K .BETINA Professeur à L'U.S.T.H.B Examinateur.
Mr A .KESSI Professeur à L'U.S.T.H.B Examinateur.
Mr B .BENSEBAA Chargé de cours à L'U.S.T.H.B Invité.

Sommaire

Page

Introduction

Une courbe elliptique est munie d'une structure de variété abélienne de dimension un, c'est pourquoi nous commençons par un exposé sur les variétés algébriques : variétés affines, ensembles algébriques, variétés projectives, variétés abéliennes, morphismes de variétés et diviseurs d'une variété abélienne . C'est l'objet du chapitre I .

Le chapitre II est consacré à la géométrie des courbes elliptiques et à l'arithmétique des courbes elliptiques .
Nous déterminons la structure de groupe abélien d'une courbe elliptique, avec son point neutre et les formules des coordonnées de la somme de 2 points .
Nous indiquons les formules de Cassels qui permettent de calculer les coordonnées des points mP , $m > 2$ du groupe $E(Q)$ de Mordell-Weil
Nous nous intéressons aux sous groupes de m- torsion et au groupe de torsion d'une courbe elliptique . Nous indiquons les formules d'isomorphismes de 2 courbes elliptiques et une application à la classification des courbes elliptiques .

Dans le chapitre III, nous introduisons la notion de twists de courbes elliptiques .
Ensuite nous étudions les espaces homogènes d'une courbe elliptique et leurs groupes associés : le groupe de Châtelet-Weil, de Selmer et le groupe de Chafarevich-Tate .
La structure du m-groupe de Selmer a été étudiée par plusieurs auteurs avec l'isogénie :

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

et la suite exacte :

$$0 \ \rightarrow \ E'(K) / \Phi(E(K)) \ \rightarrow S_{\Phi}(E) \rightarrow \ Ш(E)[\Phi] \rightarrow \ 0$$

Il en résulte que le Φ-groupe de Selmer est fini .
Nous considérons des courbes elliptiques dont le m-groupe de Selmer est trivial .
Selon James et Ono, (Selmer groups of quadratic twists of elliptic curves, Math . Ann . 314 (1999), 1-17) le nombre de courbes elliptiques D-twists E_D de m-groupe de Selmer trivial est estimé par une fonction d'un nombre réel X , $0 < D < X$:
$f(X) = c\,X$ ou $c\,\sqrt{X} / \log X$

CHAPITRE I – VARIETES ABELIENNES

Les variétés algébriques sont du domaine de la Géométrie Algébrique . Parmi les nombreux ouvrages de Géométrie Algébrique, nous avons choisi ceux de R.Hartshorne et I.R.Shafarevich pour préparer ce chapitre . Dans la suite nous traitons les variétés affines, les ensembles algébriques, les variétés projectives, les variétés abéliennes, les morphismes de variétés et les diviseurs d'une variété abélienne .

1 . Espace affine $IA^n(k)$. Ensembles algébriques . Variétés affines

Pour toutes les notions développées ici c'est le vocabulaire géométrique qui est utilisé : espace, dimension, courbe, surface .

Définition 1

Un espace affine sur un corps algébriquement clos k est l'ensemble $IA^n(k)$, formé des n-uples $a = (a_1, \ldots\ldots, a_n)$ d'éléments $a_1, \ldots\ldots, a_n$ de k :

$$IA^n(k) = \{\ a\ ,\ a = (a_1, \ldots\ldots, a_n) \in k^n\ \} \qquad (1)$$

L'élément $a = (a_1, \ldots\ldots, a_n)$ est un point de l'espace $IA^n(k)$ à n coordonnées $a_1, \ldots\ldots, a_n$ dans le corps k ; l'exposant n est égal à la dimension de l'espace affine $IA^n(k)$.

A chaque espace affine $IA^n(k)$, nous associons l'anneau $k[t_1, \ldots., t_n]$ des polynômes F et les fonctions polynomiales :

$$F \ :\ IA^n(k) \longrightarrow k$$

de valeur :

$$F(a) = F(a_1, \ldots\ldots, a_n)$$

Par le théorème de d'Alembert-Gauss, tout polynôme $G(t) = u_0 t^n + u_1 t^{n-1} + \ldots\ldots + u_n$ de degré n admet n racines dans un corps algébriquement clos ou dans une clôture algébrique . Ce sont ces zéros qui forment des ensembles algébriques .

Définition 2

Un ensemble algébrique est le sous ensemble de l'espace $IA^n(k)$ *formé des zéros communs d'une famille* $(F_1,\ldots\ldots,F_d)$ *de polynômes* $F_1,\ldots,F_d$ *de l'anneau* $k[t_1,\ldots\ldots,t_n]$ *:*

$$Z(F_1,\ldots\ldots,F_d) = \{ \text{ zéros communs de } F_1,\ldots\ldots,F_d \}$$
$$= \{ a \in IA^n(k),\quad F_1(a) = F_2(a) = \ldots\ldots F_d(a) = 0 \}$$

D'après le théorème de d'Alembert - Gauss sur les zéros d'un polynôme, les polynômes $F_1(t) = F_2(t) = \ldots\ldots = F_d(t) = 0$ sont les équations de cet ensemble algébrique .

Cet ensemble algébrique est fini . Il est vide si les polynômes $F_d(t_1,\ldots\ldots,t_n)$ n'ont pas de zéro commun.

Exemple

L'ensemble des zéros d'un polynôme $F \in k[t_1, \ldots\ldots, t_n]$ est un ensemble algébrique dans un corps algébriquement clos

Proposition 1

1) La réunion et l'intersection de deux ensembles algébriques sont des ensembles algébriques .

2) L'espace $IA^n(k)$ *et l'ensemble vide sont des ensembles algébriques*

Preuve de 1)

Soient deux ensembles algébriques $Z_1(F_1,\ldots\ldots, F_c)$ *et* $Z_2(G_1,\ldots\ldots, G_d)$

Leur réunion $Z_1(F_i) \cup Z_2(G_j) = Z(F_i\, G_j\ ;\ i, j)$ est l'ensemble des zéros communs des polynômes $F_1 G_1,\ F_1 G_2,\ldots\ldots,\ F_c G_d$.

Leur intersection $Z_1(F_i) \cap Z_2(G_j) = Z(F_1,\ldots\ldots, F_c\ , G_1,\ldots\ldots, G_d)$ est l'ensemble des zéros communs des polynômes $F_1,\ldots\ldots, G_d$

Preuve de 2)

L'ensemble vide est l'ensemble $Z(1)$ des zéros du polynôme $1 \in k[t_1,\ldots\ldots, t_n]$; ce polynôme 1 ne possède pas de zéros .

Le *n*- espace $IA^n(k)$ est l'ensemble $Z(0)$ du polynôme nul : $0\, t_1 + 0\, t_2 + \ldots\ldots + 0\, t_n$

□

Les sous ensembles algébriques du n- espace $IA^n(k)$ et leurs complémentaires définissent une topologie .

Définition 3

la topologie de Zariski sur le n- espace affine $IA^n(k)$ est déterminée par les complémentaires des ensembles algébriques comme des ouverts et les ensembles algébriques comme des fermés .

Cette topologie n'est pas de Hausdorff

Exemples d'ensembles fermés

1) L'espace affine $IA^n(k)$ est fermé comme complémentaire de l'ensemble vide

2) Un sous ensemble $X \subset IA^1(k)$ constitué de tous les points non nuls de l'espace affine $IA^1(k)$ est un ouvert

2 . Fonctions régulières . Applications rationnelles . Morphismes

Soit un ensemble fermé X d'un espace affine $IA^n(k)$

Définition 4

Une fonction sur l'ensemble X à valeurs dans k

$f : X \longrightarrow k$

est régulière s'il existe un polynôme $F \in k[t_1,.....,t_n]$ à n variables satisfaisant l'égalité :

$f(x) = F(x)$ *pour tous les points* $x \in X$

Le polynôme F associé à la fonction régulière f n'est pas unique . Ceci provient des équations $F_i(t)$ de X

L'ensemble $k[X]$ des fonctions régulières sur l'ensemble fermé X est un anneau . C'est l'anneau des coordonnées sur X

Considérons les polynômes F qui s'annulent en tout point d'une partie de l'espace affine $IA^n(k)$

Définition 5

L'idéal d'un sous ensemble X de l'espace affine $IA^n(k)$ est l'ensemble des polynômes

$F \in k[t_1, ..., t_n]$ qui s'annulent en tout point P de X :

$$I(X) = \{ F \in k[t_1, ..., t_n] \ ; \ F(P) = 0 \text{ pour tout } P \in X \}$$

Nous obtenons ainsi un anneau quotient :

$$K[X] = k[t] / I(X)$$

Cet anneau est intègre lorsque l'idéal $I(X)$ est premier . Cet anneau est un corps lorsque l'idéal est maximal (théorie des idéaux dans un anneau)

Exemple

Soit X l'espace affine $IA^n(k)$ et son idéal :

$$I(X) = \{ F \in k[t_1, ..., t_n] \ ; \ F(P) = 0 \text{ pour tout point } P \in IA^n(k) \}$$

Soit un polynôme $F = a_1 t_1 + a_2 t_2 + ... + a_n t_n + a_{n+1} \in k[t_1, ..., t_n]$

Considérons un point P_i de l'espace affine $A^n(k)$ dont toutes les coordonnées sont nulles sauf la $i^{ème}$ qui est égale à 1

$$P_1(1, 0, ..., 0) \neq 0 \ , \ P_2(0, 1, 0, ..., 0) \neq 0 \ , \ P_n(0, ..., 0, n) \neq 0$$

Alors tout point P de l'espace affine est une combinaison linéaire :

$$P = a_1 P_1 + a_2 P_2 + ...a_n P_n$$

L'hypothèse $F(p) = 0$ pour tout point P implique $a_1 = ... = a_n = 0$

Il en résulte que l'idéal $I(IA^n(k))$ est nul :

$$I(IA^n(k)) = 0$$

Définition 6

Soient deux ensembles fermés $X \subset IA^n(k)$, $Y \subset IA^n(k)$ d'un espace affine $IA^n(k)$

Une application $f : X \longrightarrow Y$ est régulière s'il existe m fonctions régulières $f_1, ..., f_m$ sur X telles que :

$$f(x) = (f_1(x), ..., f_m(x)) \text{ pour tout point } x \in X$$

La notion de sous ensemble irréductible est introduite par la :

Définition 7

Dans un espace topologique X, un sous espace Y est irréductible s'il n'est pas la réunion $Y = Y_1 \cup Y_2$ *de deux sous ensembles fermés propres de Y*

L'ensemble vide n'est pas considéré comme irréductible .

Définitions 8

1) Une variété algébrique affine est un sous ensemble X de l'espace affine $IA^n(k)$*, irréductible et fermé pour la topologie de Zariski .*

2) Un sous ensemble ouvert d'une variété affine est une variété quasiaffine .

Exemples

1) l'espace affine $IA^n(k)$ est un espace irréductible
2) Un polynôme irréductible $F \in k[t_1, \ldots\ldots, t_n]$ engendre un idéal premier, alors l'ensemble $Z(F)$ est irréductible

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

Définition 9

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

$\varphi = f / g$

où $f, g \in k[X]$ *avec* $g(x) \neq 0$

Nous admettons qu'une variété affine $IA^n(k)$ est de dimension n. Alors $IA^1(IR)$ est de dimension 1 et $IA^2(IR)$ est de dimension 2 sur le corps IR des nombres réels

Morphismes de variétés algébriques

Ce sont des applications continues de variétés algébriques

Définition 10

Soit une variété quasiaffine $Y \subset IA^n$. *Une fonction* $f : Y \longrightarrow k$ *est régulière en un point* $P \in Y$ *s'il existe un voisinage ouvert* U *de* P *et deux polynômes* $g , h \in k[x_1, ..., x_n]$ *qui satisfont les 2 conditions :*

$h \neq 0$ *sur* U *et* $f = g / h$ *sur* U

f est régulière sur Y si elle est régulière en tout point de Y

Définition 11

Soient deux variétés algébriques X *et* Y

Un morphisme $\varphi : X \longrightarrow Y$ *est une application continue telle que pour tout ensemble ouvert* $V \subseteq Y$ *et toute fonction régulière* $f : V \longrightarrow k$, *la fonction composée :*

$f \circ \varphi : \varphi^{-1}(V) \longrightarrow k$ *est régulière*

La composée de deux morphismes de variétés est un morphisme de variétés
En particulier, un morphisme $\varphi : X \longrightarrow Y$ de deux variétés est un morphisme qui admet un morphisme inverse $\psi : Y \longrightarrow X$ satisfaisant les 2 conditions :

$\psi \circ \varphi = id_X$ et $\varphi \circ \psi = id_Y$ = morphisme identique de la variété Y

A une variété Y sont associés des anneaux de fonctions par la :

Définition 12

Soit l'anneau $O(Y)$ *des fonctions régulières sur une variété* Y *et un point* P *de* Y. *L'anneau local de* P *en* Y *est l'anneau* $O_{P,Y}$ *des classes d'équivalence de couples* (U , f) *où* U *est un sous ensemble ouvert de* Y *contenant* P *et* f *est une fonction régulière sur* U *avec la relation* $\mathfrak{R}$ *d'équivalence :*

$(U , f) \mathfrak{R} (V , g)$ *si* $f = g$ *sur* $U \cap V$

La relation $\mathfrak{R}$ permet de définir le corps des fonctions rationnelles $K(Y)$ d'une variété Y par la :

Définition 13

Le corps des fonctions $K(Y)$ d'une variété Y est l'ensemble des classes d'équivalence de couple d'éléments (U, f), d'un ensemble ouvert U de Y et une fonction régulière f sur U par la relation $\mathfrak{R}$ définie dans la définition **12**

3 . Espaces projectifs . Variétés projectives . Variétés abéliennes

Une variété projective est un ensemble particulier de points ; avec une relation d'équivalence, nous obtenons des classes d'équivalence ; c'est ainsi que les espaces projectifs sont construits .

Définition 14

Un n- espace projectif sur un corps algébriquement clos k est l'ensemble $IP^n(k)$ des classes d'équivalence de points $P = (a_0, \ldots\ldots, a_n)$, à $n + 1$ coordonnées a_i non toutes nulles dans k, avec la relation $\mathfrak{R}$ d'équivalence :

$(a_0, a_1, \ldots\ldots, a_n)$ $\mathfrak{R}$ $(b_0, b_1, \ldots\ldots, b_n)$ *si et seulement si :*

$b_0 = \lambda a_0$, $b_1 = \lambda a_1$, $\ldots\ldots\ldots b_n = \lambda a_n$ *pour tout élément λ non nul du corps k*

Il en résulte que le n- espace projectif $IP^n(k)$ est l'ensemble quotient du $n + 1$- espace affine $IA^{n+1}(k) - \{(0, \ldots\ldots, 0)\}$, privé du point $(0, \ldots\ldots, 0)$, par la relation d'équivalence $\mathfrak{R}$:

$$IP^n(k) = IA^{n+1}(k) - \{(0, \ldots, 0)\} / \mathfrak{R}$$

Exemples

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

$IP^1(IR) = \{ \lambda a , a = (a_0, a_1) ; a_i \in IR , \lambda \neq 0 \} = \{$ classe des couples $(a_0, a_1) \}$

Il existe un représentant canonique dans chaque classe .

2) L'espace projectif $IP^2(IR)$ est l'ensemble :

$$IP^2(IR) = IA^3 - \{(0, 0, 0)\} / \mathfrak{R}$$

$$= \{ \text{classes des triplets } (a_0, a_1, a_2) \}$$

$$= \{ \alpha(1, 1, 1) , \beta(1, 1, 0) , \ldots\ldots \}$$

Les $(n + 1)$ coordonnées d'un point P du n- espace $IP^n(k)$ forment un ensemble de coordonnées homogènes dans la classe de P

3) Considérons la courbe plane C d'équation affine :

$f(x, y) = y^2 + 3xy - 5y - x^3 + 2x^2 - 4x - 7 = 0$

pour obtenir l'équation de la courbe C dans le plan projectif $IP^2(IR)$ nous faisons le changement $x = X/Z$, $y = Y/Z$. Nous obtenons l'équation $f(X/Z, Y/Z) = 0$, qui donne :

$F(X, Y, Z) = Y^2Z + 3XYZ - 5YZ^2 - X^3 + 2X^2Z - 4XZ^2 - 7Z^3 = 0$

Définition 15

Un sous ensemble Y du n-espace projectif $IP^n(k)$ est algébrique , s'il existe un ensemble T de polynômes homogènes de l'anneau $k[t_0, t_1, ..., t_n]$ tel que :

$Y = Z(T) = \{ P \in IP^n(k) \ ; \ F(P) = 0 \text{ pour tout } F \in T \}$

Ces ensembles algébriques déterminent une topologie de Zariski sur l'espace projectif IP^n ; cette topologie implique la construction de variétés algébriques projectives

Définitions 16

1) *Une variété algébrique projective est un ensemble algébrique irréductible de l'espace projectif $IP^n(k)$.*
2) *Un sous ensemble ouvert d'une variété algébrique projective est une variété quasi-projective*
3) *La dimension d'une variété projective ou quasi-projective est égale à sa dimension en tant qu'espace topologique .*

Définition 17

1) *L'idéal homogène d'un sous ensemble Y de IP^n est engendré par l'ensemble des polynômes homogènes $F \in k[t_0, t_1, ..., t_n]$ qui s'annulent en tout point de Y*
$I(Y) = \{ F \in k[t_0, t_1, ..., t_n] \ ; \ F \text{ homogène et } F(P) = 0 \text{ pour tout } P \in Y \}$
2) *L'anneau des coordonnées homogènes d'un ensemble algébrique Y est l'anneau quotient :*
$k[t_0, t_1, ..., t_n] / I(Y)$

Variétés de groupes et variétés abéliennes

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

Définition 18

Une variété de groupe est une variété algébrique G muni de deux applications régulières :

$\varphi : G \longrightarrow G$ *et* $\psi : G \times G \longrightarrow G$

de valeurs :

$\varphi(g) = g^{-1}$ *et* $\psi(g_1, g_2) = g_1 g_2$

Une variété de groupe donne une variété abélienne par la :

Définition 19

Une variété abélienne est une variété de groupe projective et irréductible

4 . Diviseurs de variétés algébriques . Diviseurs de fonctions . Diviseurs de courbes algébriques

La notion de diviseur en Géométrie Algébrique permet de construire des diviseurs de plusieurs types et des groupes de diviseurs .

Définition 20

Soit une variété irréductible X . et une famille Ci de sous variétés irréductibles Ci de X de codimension 1, alors un diviseur de X est une somme formelle :

$$D = l_1 C_1 + l_2 C_2 + \ldots\ldots + l_r C_r \qquad (3)$$

où les l_i *sont des entiers rationnels*

Le diviseur D est nul lorsque tous les coefficients l_i sont nuls : $D = 0$

Le diviseur D est positif lorsque tous ses coefficients $l_i \geq 0$: $D \geq 0$

Somme de deux diviseurs d'une variété

Soient deux diviseurs d'une variété X

$D = n_1 C_1 + \ldots\ldots\ldots + n_r C_r$

$D' = m_1 C_1 + \ldots\ldots\ldots + m_r C_r$

Le diviseur somme $D + D'$ est défini par la formule :

$$D + D' = (n_1 + m_1) C_1 + \ldots\ldots + (n_r + m_r) C_r$$

Il en résulte $D + D_0 = D_0 + D = D$ pour tout diviseur D et $D_0 = 0$.
Alors $D + D' = D_0$ implique $D' = -D$

Il en résulte que les diviseurs d'une variété X forment un groupe, isomorphe à un ZI-module libre engendré par des sous variétés irréductibles de codimension 1 dans X.
C'est le groupe $Div(X)$ des diviseurs de X
La notion de diviseur s'étend aux fonctions

Définition 21

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

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

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

Les courbes algébriques planes admettent des diviseurs

Définition 22

Une courbe algébrique est une variété projective de dimension 1

Définition 23

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

Un diviseur d'une courbe C est une somme formelle :

$$D = \sum_{P \in C} n_P . P$$

où les entiers rationnels n_P sont presque tous nuls

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

Définition 24

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

$$deg\ D = \sum_{P \in C} n_P$$

Exemple

Soit une courbe algébrique plane C d'équation :

$$f(x) = a\frac{(x-a_1)^3(x-a_2)^2}{(x-a_3)^5}$$

Le diviseur de C est :

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

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

La définition **24** implique la valeur du degré de C

$$deg\ C = 3 + 2 - 5 = 0$$

Dans le groupe abélien $Div(X)$ d'une variété X, l'application :

$$\begin{aligned} Div(X) \times Div(X) &\longrightarrow Div(X) \\ (D_1 , D_2) &\longrightarrow D_1 + D_2 \end{aligned}$$

est une loi de composition interne, cette loi est associative et commutative .

Elle admet comme élément neutre le diviseur $D = 0$.

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

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

L'ensemble $P(X)$ des diviseurs principaux est un sous groupe du groupe $Div(X)$

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

Définition 25

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

$$Cl(X) = Div(X) / P(X)$$

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

CHAPITRE II
GEOMETRIE DES COURBES ELLIPTIQUES

1 . Structures algébriques

Commençons par une définition des courbes elliptiques basée sur une équation particulière de l'équation des cubiques planes :

$d_1 x^3 + d_2 x^2 y + d_3 x y^2 + d_4 y^3 + d_5 x^2 + d_6 x y + d_7 y^2 + d_8 x + d_9 y + d_{10} = 0$

Définition 1

Une courbe elliptique est une cubique plane E non singulière, irréductible, d'équation algébrique de la forme :

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

Définition 2

L'équation algébrique (1) *est l'équation de Weierstrass de la courbe elliptique E*

Dans l'équation (1), les cinq coefficients $a_1, a_2, \ldots\ldots, a_6$ sont des éléments d'un corps commutatif *K*, les deux variables *x* et *y* racines de l'équation algébrique (1) sont des éléments d'une clôture algébrique K_{alg} du corps K .
Ce corps *K* est le corps de base de la courbe elliptique *E* . K est soit un corps de nombres algébriques, soit un corps global soit un corps local, soit un corps fini .
La nature du corps de base K a une influence sur les propriétés de la courbe elliptique E

Lorsque K est un corps de nombres algébriques, il s'applique à la courbe elliptique E la théorie des nombres : équations diophantiennes, discriminants, classe d'idéaux, corps de classes, valuations, groupe de Galois, ramification, nombres premiers, fonctions arithmétiques (Euler, Mobius, Riemann ...) .
Ainsi, un article de Cassels a pour titre :

« Equation Diophantine with Special References to Elliptic Curves » .

Lorsque K est le corps des nombres complexes IC, il s'applique à la courbe elliptique E l'analyse complexe (réseaux, tores complexes, isomorphismes analytiques complexes, groupes de Lie, formes automorphes, formes modulaires, ….) et la géométrie algébrique (courbes algébriques, diviseurs d'une courbe algébrique, variétés, schémas, …)

Lorsque K est un corps fini, ou un corps de fonctions, ou un corps local, les propriétés de ces corps sont utiles à l'étude des courbes elliptiques .

Il en résulte plusieurs structures algébriques sur les courbes elliptiques :
une structure de variété abélienne de dimension un,
une structure de courbe algébrique projective non singulière de genre un,
une structure de groupe abélien de type fini,
une structure de schéma de dimension un .

2 . Transformations linéaires de l'équation de Weierstrass

Ces transformations s'obtiennent avec des changements linéaires des deux variables x et y

Soit une courbe elliptique d'équation de Weierstrass :

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

L'équation (1) peut être transformée en d'autres formes par des transformations linéaires des variables convenables .

1) Lorsque le corps K est de caractéristique $\neq 2$, le changement de variables linéaire :

$$(x , y) \longrightarrow (x , 1/2 (y - a_1 x - a_3))$$

élimine les termes en y *dans (1) ; l'équation de la courbe devient :*

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

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

$$b_2 = a_1^2 + 4 a_2 \quad , \quad b_4 = 2 a_4 + a_1 a_3 \quad , \quad b_6 = 4 a_6 + a_3^2 \qquad (3)$$

2) Lorsque le corps K est de caractéristique $\neq 2 , 3$, le changement de variables linéaire

$$(x , y) \longrightarrow ((x - 3 b_2) / 36 , y / 108)$$

élimine le terme en x^2 et le coefficient 4 dans (2) ; l'équation de la courbe se transforme en :

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

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

$$c_4 = {b_2}^2 - 24\, b_4 \quad , \quad c_6 = -{b_2}^3 + 36\, b_2\, b_4 - 216\, b_6 \qquad (5)$$

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

1) Le modèle de Legendre :

$$y^2 = x\,(x-1)\,(x-d) \quad ; \quad d \neq 0\,,\,1$$

2) Le modèle de Cassels :

$$y^2 = x^3 + A\,x + B \quad avec \quad \Delta(E) = -16\,(4\,A^3 + 27\,B^2) \neq 0$$

3) Le modèle de Tate :

$$y^2 + x\,y = x^3 + a_4 x + a_6 \ ; \ pour \ a_4\,,\ a_6 \in IC$$

4) Le modèle de Kubert :

$$y^2 + (1-A)\,x\,y - B\,y = x^3 - B\,x^2 \ ; \ pour \ A\,,\ B \in K$$

etc.....

3 . Invariants d'une courbe elliptique

Chaque courbe elliptique possède de nombreux invariants : le discriminant, l'invariant modulaire, l'invariant différentiel, le conducteur, l'invariant de Hasse, le régulateur, la série L de Dirichlet, etc.....

Les invariants b_{2i} et c_{2i} permettent de les définir

Nous commençons par 4 invariants :

Définitions 3

a) Le discriminant d'une courbe elliptique E est le polynôme « homogène de degré 12 » de l'anneau $ZI\,[\,b_2\,,\,b_4\,,\,b_6\,,\,b_8\,]$ égal à :

$$\Delta(E) = 9\, b_2\, b_4\, b_6 - 8\, {b_4}^3 - 27\, {b_6}^2 - {b_2}^2\, b_8 \qquad (6)$$

où l'on a posé :

$$4\, b_8 = b_2\, b_6 - {b_4}^2 \qquad (7)$$

lorsque le corps K est de caractéristique $\neq 2\,,\,3$

Le discriminant $\Delta(E)$ s'écrit sous la forme d'un polynôme en c_4 et c_6 :

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

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

$$j(E) = c_4^3 / \Delta(E) = 1728\, c_4^3 / [c_4^3 - c_6^2]$$

c) L'invariant différentiel d'une courbe elliptique E est l'élément différentiel :

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

d) Le conducteur d'une courbe elliptique E de discriminant $\Delta(E)$ est l'entier :

$$N(E) = \prod_{p/\Delta(E)} p^{f(p)}$$

où p désigne les facteurs premiers du discriminant $\Delta(E)$, l'exposant $f(p)$ est compris entre 0 et 8 suivant la valuation en p du corps K et la réduction en p de E :

$f(p) = 0$ si p ne divise pas $\Delta(E)$: E a une bonne réduction en p,
$f(p) = 1$ si E a une réduction multiplicative en p,
$f(p) = 2$ si E a une réduction additive en p et $p \geq 5$,
$2 \leq f(2) \leq 8$ si E a une réduction additive en $p = 2$,
$2 \leq f(3) \leq 5$ si E a une réduction additive en $p = 3$.

d'après Velu, Séminaire d'Algèbre et de Théorie de nombres (1975/1976) .

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

L'équation de Weierstrass d'une courbe elliptique E se met sous la forme $y^2 = f(x)$
Pour l'étude du polynôme $f(x)$, il est utile d'utiliser le résultant de 2 polynômes
La théorie des polynômes d'un anneau $K[t]$ de polynômes sur un corps commutatif K donne une relation entre un polynôme $f(t) \in K[t]$ et sa dérivée par le moyen du résultant $Res(f, g)$ de deux polynômes $f(t)$ et $g(t)$:

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

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

Définition 4

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

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

Les autres termes dans ce déterminant sont nuls

Les résultats suivants sont énoncés sans démonstration, ils peuvent être trouvés dans les ouvrages « Algebra » de Lang et « Introduction à l'algèbre » de Kostrikine .

Proposition 1

Soit un scalaire non nul $\lambda \in K$, alors :

Les résultants satisfont les propriétés :

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

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

!

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

Proposition 2

Soit 2 polynômes :

$f(t) = a_0 (t - \alpha_1) \ldots\ldots\ldots (t - \alpha_n)$, de degré n

$g(t) = b_0 (t - \beta_1) \ldots\ldots\ldots (t - \beta_m)$, de degré m

Alors leur résultant est égal au produit :

$$Res(f, g) = a_0^{\,m}\, b_0^{\,n} \prod_{\substack{1 \le i \le n \\ 1 \le j \le m}} (\alpha_i - \beta_j) \qquad (8)$$

!

Le résultant des polynômes f et g s'exprime donc en fonction des racines de ces polynômes par la formule (8) qui implique le :

Corollaire 1

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

2) Le résultant Res (f , g) n'est pas nul si et seulement si les deux polynômes n'ont pas de racine commune

!

Le résultant Res (f , f) d'un polynôme f (t) et de sa dérivée f ' (t) est lié à son discriminant Dis (f) par la :

Proposition 3

Soit un polynôme f (t) de degré n :

$$f(t) = a_0 (t - \alpha_1) \ldots\ldots\ldots (t - \alpha_n) = a_0 \prod_{1 \le i \le n} (t - \alpha_i)$$

et son polynôme dérivé f ' (t), alors :

Le résultant Res (f , f ') est lié au discriminant Dis (f) du polynôme f par les formules :

$$Dis(f) = a_0^{\,2n-2} \prod_{i \ne j} (\alpha_i - \alpha_j)^2 \qquad et \qquad Res(f, f') = (-1)^{\frac{n(n-1)}{2}}\, a_0\, Dis(f)$$

!

Dans les exemples suivants, je m'intéresse à des polynômes cubiques .

Exemples

1) $f(t) = a\,t^3 + b\,t^2 + c\,t + d$

son discriminant est égal à :

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

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

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

Le discriminant du polynôme f (x) *vaut :*

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

Alors :

Le discriminant $\Delta(E)$ de la cubique E est lié à son polynôme par la formule :

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

Proposition 4

Soit une courbe elliptique E d'équation de Weierstrass (2) et de discriminant $\Delta(E)$. *Alors le discriminant Dis (f) du polynôme f (x) est égal à* $Dis\,(f) = 16\,\Delta(E)$.

Classification des cubiques planes

Soit une cubique plane E d'équation de Weierstrass :

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

Cette cubique E *est soit non singulière, donc elliptique, soit singulière, donc cubique non elliptique* .

D'après la théorie des points singuliers d'une courbe algébrique C, une cubique admet 0 ou 1 point singulier . (9)

La présence, éventuelle, d'un point singulier est liée à la résolution du système d'équations :

$$\begin{cases} F(x,y) = y^2 + a_1 x y + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6 = 0 \\ F_x' = a_1 y - 3x^2 - 2\,a_2 x - a_4 = 0 \\ F_y' = 2y + a_1 x + a_3 = 0 \end{cases} \quad (10)$$

Nous commençons par déterminer les cubiques sans point singulier

Proposition 5

Soit une cubique plane E de discriminant Δ (E) et le point à l'infini :

$0_E = (\infty, \infty) = (0, 1, 0)$ associé à E

1) Le point à l'infini 0_E *est un point de E , non singulier,*

2) La cubique E est non singulière si et seulement si $\Delta(E) \neq 0$

Preuve de « 0_E est sur E »

Par le changement de variables :

$x = X / Y \quad , \quad y = Y / Z$

Je mets l'équation (1) sous la forme d'un polynôme homogène de degré 3 :

$E : \; F(X, Y, Z) = Y^2 Z + a_1 X Y Z + a_3 Y Z^2 - X^3 - a_2 X^2 Z - a_4 X Z^2 - a_6 Z^3 = 0$

Le point à l'infini $0_E = (\infty, \infty)$ est représenté dans le plan projectif $IP^2(K)$ par :

$0_E = (0, 1, 0)$

Les coordonnées du point 0_E satisfont l'équation de E :

$F(0_E) = F(0, 1, 0) = 0$

Il en résulte que ce point à l'infini 0_E est sur E

!

Preuve de « 0_E est non singulier »

La dérivée $\frac{\partial F}{\partial Z}$ prend, au point 0_E, la valeur :

$\frac{\partial F}{\partial Z}(0, 1, 0) = 1 \neq 0$

Cela implique que le point 0_E n'est pas singulier sur E

2

Preuve de « la cubique E est non singulière » implique « $\Delta(E) \neq 0$ »

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

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

La définition du discriminant d'un polynôme f (x) *implique la relation :*

$Dis(f(x)) = c \, Res(f, f')$ où $c =$ constante non nulle et $f' =$ dérivée de f (11)

Les discriminants $Dis(f(x))$ du polynôme $f(x)$ et $\Delta(E)$ de la cubique E sont liés par la relation :

$Dis(f(x)) = 16 \, \Delta(E)$ (12)

Les formules (2), (11), et (12) impliquent la relation :

$\Delta(E) = c_1 Res(f, f')$ où $c_1 =$ constante non nulle (13)

L'hypothèse « la cubique E est non singulière » implique que le polynôme $f(x)$ admet trois racines distinctes :

$f(x) = 4 (x - e_1)(x - e_2)(x - e_3)$ (14)

La définition des racines multiples d'un polynôme $f(x)$ et la relation (14) impliquent que les racines de la dérivée $f'(x)$ ne sont pas racines de $f(x)$ (15)

Il en résulte la condition :

$$Res(f, f') \neq 0 \quad (16)$$

Les relations (13) et (16) impliquent la valeur :

$$\Delta(E) \neq 0$$

&

Preuve de « $\Delta(E) \neq 0$ » implique « la cubique E est non singulière »

Prenons la cubique plane d'équation de Weierstrass (2) précédente :

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

L'hypothèse $\Delta(E) \neq 0$ et la relation $Dis(f(x)) = 16\Delta(E)$ impliquent :

$$Dis(f(x)) \neq 0 \quad (17)$$

Les relations (13) et (17) impliquent la valeur :

$$Res(f, f') \neq 0 \quad (18)$$

La définition du résultant de deux polynômes $f(x)$ et sa dérivée $f'(x)$ n'ont pas de racine commune .

Donc le polynôme $f(x)$ admet 3 racines simples

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

!

Il s'en suit qu'une cubique E de discriminant $\Delta(E) = 0$ est singulière . Ce point singulier est soit un nœud de E (point à deux tangentes distinctes), soit un point de rebroussement de E (point à deux tangentes confondues)

La nature du point singulier d'une cubique singulière est déterminée par l'invariant $c_4 = b_2^2 - 24\, b_4$ et la :

Proposition 6

Soit une cubique singulière E, de discriminant $\Delta(E)$ et d'invariant $c_4(E) = c_4$

Alors :

1) E admet un nœud si et seulement si $\Delta(E) = 0$ et $c_4 \neq 0$

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

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

D'après la proposition 5, la cubique E *est singulière lorsque son discriminant est nul :*

$$\Delta(E) = 0 \qquad (19)$$

Prenons une cubique E d'équation de Weierstrass :

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

Les relations liant les invariants $Res(f, f')$, $Dis(f(x))$, $\Delta(E)$ et (19) impliquent que le polynôme $f(x)$ admet une racine double .

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

Les pentes de ces tangentes sont égales à la dérivée y' calculée avec (2) :

$$y' = \frac{6x^2 + b_2 x + b_4}{y} = \frac{g(x)}{y} \qquad (20)$$

L'hypothèse « 2 tangentes distinctes » implique que le polynôme $g(x)$ admet 2 racines distinctes .

Il en résulte que son discriminant $Dis(g(x))$ n'est pas nul
Le calcul donne la valeur :

$$Dis(g(x)) = b_2^2 - 24 b_4 = c_4(E) \qquad (21)$$

Il en résulte la condition $c_4 \neq 0$

+

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

Prenons une courbe elliptique E d'équation de Weierstrass :

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

L'hypothèse « $\Delta(E) = 0$ » implique que « la cubique E est singulière » ;
son équation $y^2 = f(x)$ admet une racine double .

Cette racine double détermine un point singulier de la cubique E

L'hypothèse $c_4 \neq 0$ et la formule (21) impliquent la valeur :

$Dis(g(x)) \neq 0$;

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

Donc ce point singulier est un nœud de la cubique E

Preuve de « E admet un point de rebroussement » implique « $\Delta(E) = C_4 = 0$ »

L'hypothèse « la cubique E admet un point de rebroussement » implique « la cubique E est singulière », cela implique que son discriminant $\Delta(E) = 0$

Prenons la cubique plane E d'équation de Weierstrass (2) précédente :

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

Soit S le point de rebroussement de la cubique E

Par définition d'un point de rebroussement d'une courbe algébrique, la cubique E admet une seule tangente en ce point S.

La pente de la tangente est déterminée par la formule (20)

L'hypothèse d'une seule tangente au point S implique une racine double du polynôme $g(x)$.

Cela implique la valeur du discriminant :

$Dis(g(x)) = 0$ (22)

Les formules (21) et (22) implique la valeur :

$c_4(E) = 0$

!

Exemples

1) Cubique d'équation de Weierstrass qui admet un nœud :

$$E_1 \ : \quad y^2 = x^3 - 2\,x^2 + x$$

Le calcul donne les invariants :

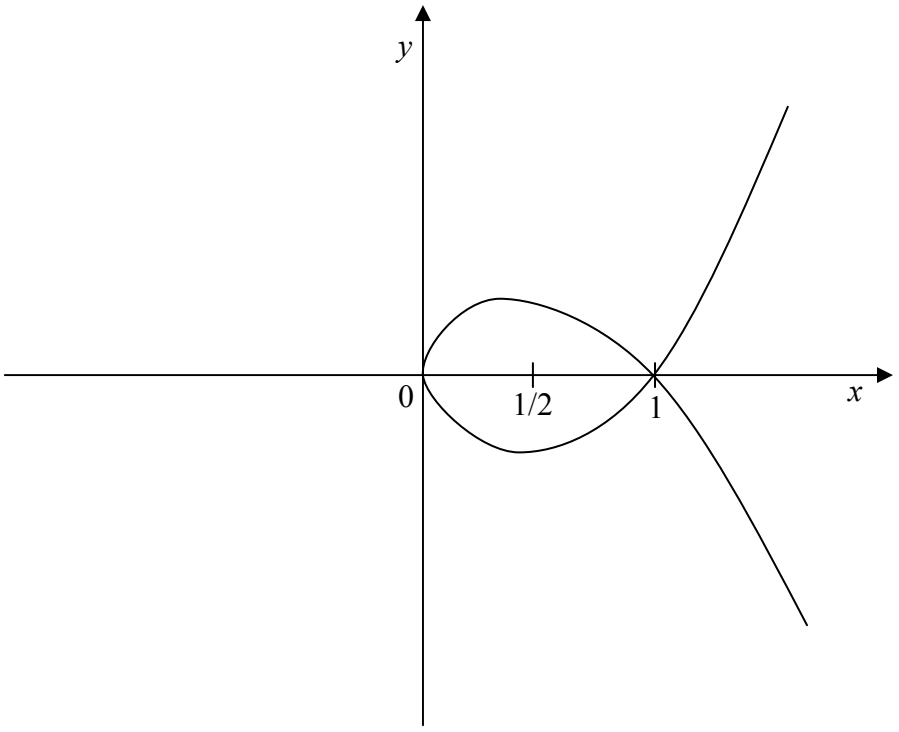
$b_2 = -8$; $b_4 = 2$; $b_6 = 0$; $b_8 = -1$; $\Delta(E_1) = 0$; $c_4(E_1) = 16 > 0$

$\Delta(E_1) = 0$ *implique que la cubique* E_1 *est singulière*

Tableau des coordonnées de quelques points de la cubique :

x	-1	0	1	2	1 / 3	1 / 2
y^2	-4	0	0	2	4 / 27	1 / 8
y	/	0	0	$\pm\sqrt{2}$	$\pm 2/3\sqrt{3}$	$\pm\sqrt{2}/4$

Ce tableau indique que le point $S = (1, 0)$ est un nœud de la cubique .



2) Cubique d'équation de Weierstrass :

$$E_2 \quad : \quad y^2 - 2y = x^3 - 1$$

qui admet un point de rebroussement

Le calcul donne les invariants :

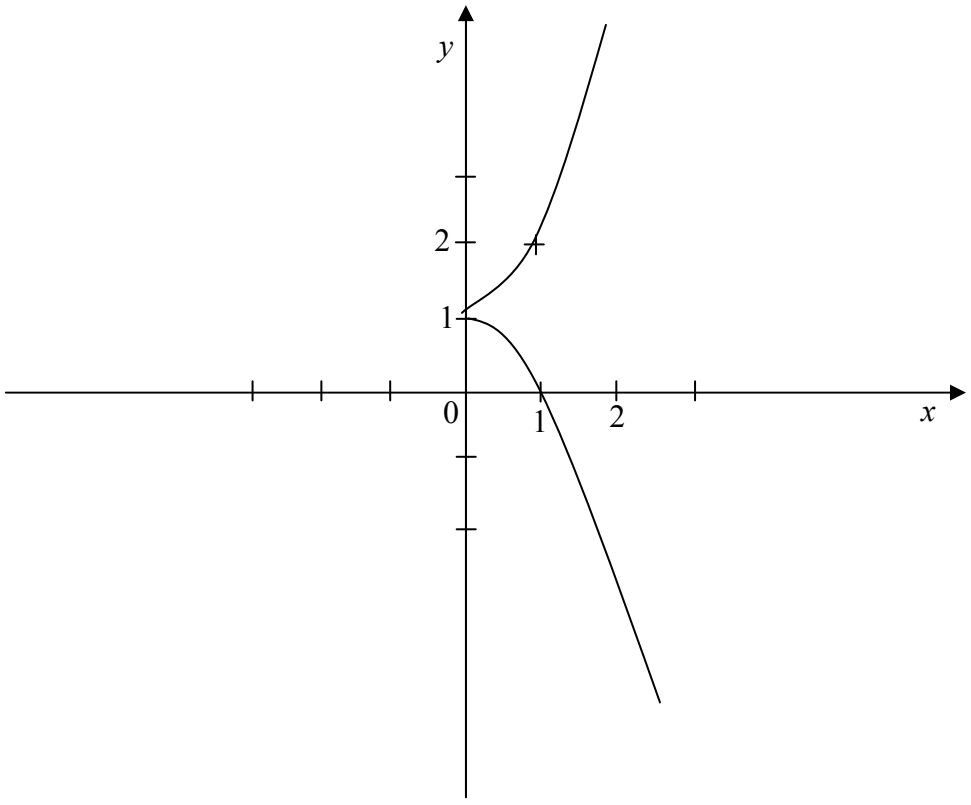
$b_2 = 0$; $b_4 = 0$; $b_6 = 0$; $b_8 = 0$; $\Delta(E_2) = 0$; $c_4(E_2) = 0$

les valeurs $\Delta(E_2) = c_4(E_2) = 0$ impliquent que la cubique E_2 admet un point de rebroussement

Tableau des coordonnées de quelques points de la cubique :

x	- 2	- 1	0	1	2
$y^2 - 2y$	- 9	- 2	- 1	0	7
y	/	/	1 double	0 et 2	$1 \pm 2\sqrt{2}$

Ce tableau indique que le point (0 , 1) est le point de rebroussement de la cubique (2 tangentes confondues à E_2)



Le signe du discriminant d'une courbe elliptique E influe sur l'allure de E ; il en résulte 2 types de courbes elliptiques par la :

Proposition 7

Soit une courbe elliptique E, de discriminant $\Delta(E) \in IR$, *alors :*

1) E *coupe l'axe* Ox *en 3 points simples si et seulement si* $\Delta(E) > 0$

2) E *coupe l'axe* Ox *en un point simple, si et seulement si* $\Delta(E) < 0$

Preuve de « E coupe l'axe Ox en 3 points simples » implique « Δ (E) > 0 »

Prenons une courbe elliptique d'équation de Weierstrass :

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

Alors son discriminant n'est pas nul :

$\Delta(E) \neq 0$;

Soient les 3 points $(e_i , 0)$ avec $i = 1 , 2 , 3$ d'intersection de l'axe Ox par la courbe E

Alors , le polynôme $f(x)$ est un produit :

$$y^2 = 4 (x - e_1) (x - e_2) (x - e_3) = f(x)$$

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

$$Dis\,(f(x)) = 4^4 \prod_{i \prec j} (e_i - e_j)^2 \qquad (23)$$

Les 3 abscisses e_i étant réelles , (23) implique le signe :

$$Dis\,(f(x)) > 0 \qquad (24)$$

La relation entre les discriminant de $f(x)$ et de E, et la formule (24) , impliquent :

$$\Delta(E) > 0$$

!

Preuve de « E coupe O x en un seul point » implique « Δ (E) < 0 »

Prenons une courbe E d'équation de Weierstrass :

$$E \quad : \quad y^2 = 4x^3 + b_2 x^2 + 2 b_4 x + b_6 = f(x) \tag{2}$$

L'hypothèse E coupe l'axe $O x$ en un seul point $(e, 0)$ transforme l'équation (2) en :

$$y^2 = (x - e)(x^2 + r x + s) = f(x) \text{ avec } r^2 - 4 s < 0 \tag{25}$$

Le polynôme du $2^{ème}$ degré $x^2 + r x + s$, admet 2 racines complexes conjuguées :

$$a \pm i b \tag{26}$$

D'après (25) et (26), le discriminant du polynôme $f(x)$ est égal à :

$$Dis\,(f(x)) = -4^5 b^2 ((e - a)^2 + b^2)^2 \tag{27}$$

Les nombres e, a, b sont réels, il en résulte :

$$Dis\,(f(x)) < 0 \tag{28}$$

La relation entre les discriminants $\Delta(E)$ et $Dis\,(f(x))$ et (28) impliquent :

$\Delta(E) < 0$

∃

Exemples

1) cubique d'équation de Weierstrass :

$$E_1 \ : \ y^2 = x^3 + 2\,x^2 - 3\,x$$

Le calcul donne les invariants :

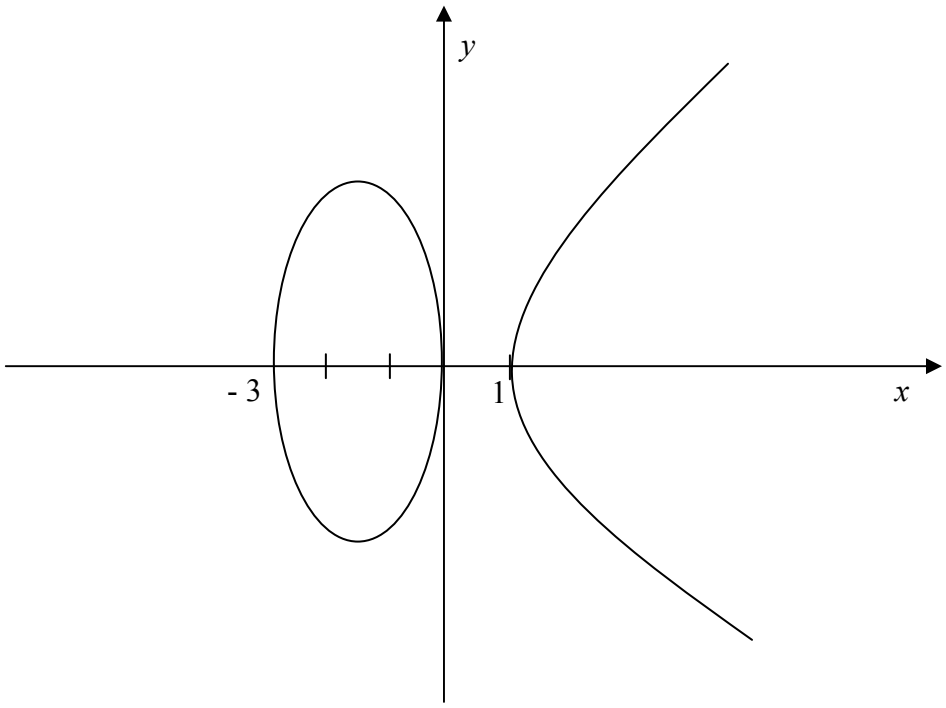
$b_2 = 8 \quad ; \quad b_4 = -6 \quad ; \quad b_6 = 0 \quad ; \quad b_8 = -9 \quad ; \quad \Delta\,(E_1) = 3^2 \times 2^8 > 0$

Donc E_1 est une courbe elliptique qui coupe l'axe $O\,x$ en 3 points simples d'abscisses :

$x_1 = -3 \quad ; \quad x_2 = 0 \quad ; \quad x_3 = 1$

Tableau des coordonnées de quelques points de E_1 :

x	- 3	- 2	-1	0	1	2
y^2	0	6	4	0	0	10
y	0	$\pm\sqrt{6}$	± 2	0	0	$\pm\sqrt{10}$



2) cubique d'équation de Weierstrass :

$\boldsymbol{E_2 \ : \ y^2 = x^3 + 2\,x + 3}$

Le calcul donne les invariants :

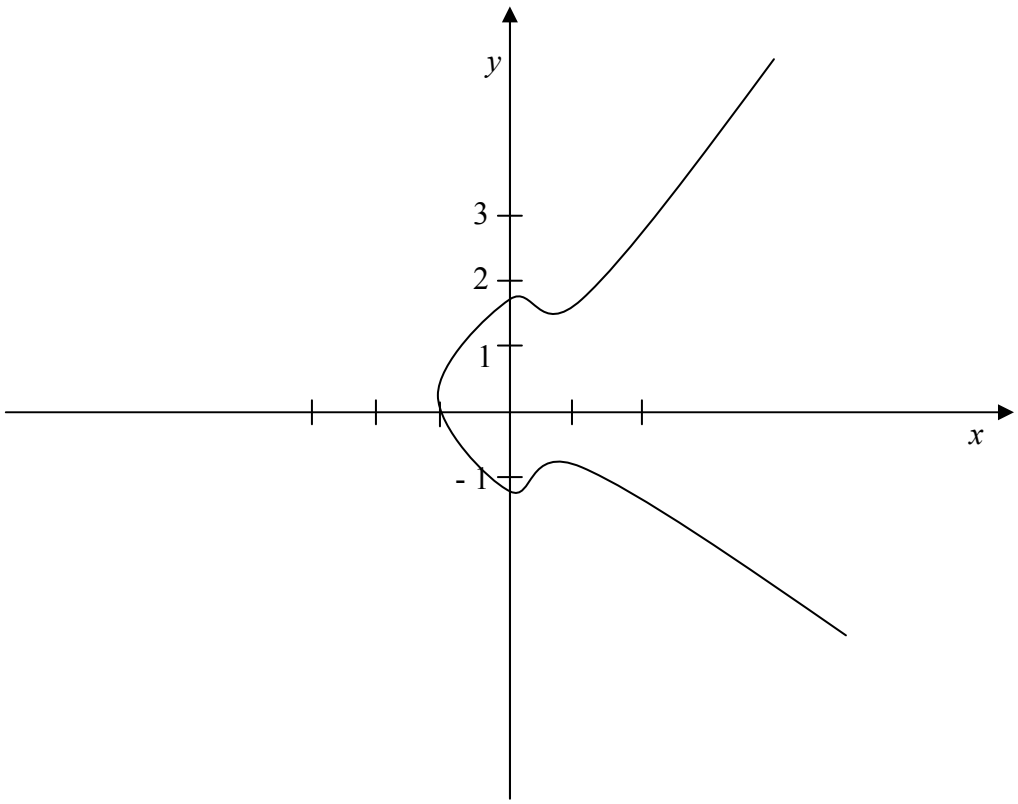
$b_2 = 0 \ ; \ b_4 = 4 \ ; \ b_6 = 12 \ ; \ b_8 = -4 \ ; \ \Delta(E_2) = -16 \times 25 \times 11 < 0$

Donc E_2 est une courbe elliptique qui coupe l'axe $O\,x$ en un point simple
L'équation diophantienne $y^2 = 0$ admet une seule solution : $x = -1 \ , \ y = 0$

Tableau des coordonnées de quelques points de E_2 :

x	- 2	- 1	0	1	2	3
y^2	- 9	0	3	6	15	36
y	/	0	$\pm\sqrt{3}$	$\pm\sqrt{6}$	$\pm\sqrt{15}$	± 6

Ce tableau indique que la courbe E_2 coupe l'axe O x au point (x , y) = (- 1 , 0)



Les cubiques planes E se repartissent dans 4 ensembles suivant leur discriminant $\Delta(E)$ et leur invariant c_4 par le :

Corollaire 2

Les cubiques planes E, sont classifiées en 4 classes par leur discriminant $\Delta(E)$ et leur invariant c_4 :

1) Classe Cub –1 des courbes elliptiques qui coupent O x en 3 points simples, donc :

$\Delta(E) > 0$

2) Classe Cub -2 des courbes elliptiques qui coupent O x en un seul point simple, donc :

$\Delta(E) < 0$

3) classe Cub -3 des cubiques singulières ayant un noeud, donc :

$\Delta(E) = 0$ *et* $c_4(E) \neq 0$

4) Classe Cub -4 des cubiques singulières ayant un point de rebroussement, donc :

$\Delta(E) = c_4(E) = 0$

*****

Nous avons donné un exemple de chaque classe pour illustrer ce corollaire.

5 . Loi de groupe abélien sur une courbe elliptique

Sur l'ensemble $E(K)$ des points K rationnels d'une courbe elliptique E nous allons construire un groupe abélien .

Soit une courbe elliptique E d'équation de Weierstrass :

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

Dans la proposition 5, nous avons démontré que le point à l'infini $0_E = (\infty , \infty) = (0 , 1 , 0)$ est un point simple de toute courbe elliptique .

Par définition du plan projectif $IP^2 (K)$, ce point est déterminé par la direction de l'axe $O y$ des ordonnées.

Proposition 8

Soit l'ensemble $E(K)$ des points K- rationnels d'une courbe elliptique E

Alors, l'application :

$$f : E(K) \times E(K) \longrightarrow E(K)$$
$$(P , Q) \longrightarrow P + Q$$

où $P + Q = M$ est le symétrique, par rapport à l'axe $O x$ du point d'intersection de la droite $P Q$ et de la courbe E, est une loi de groupe abélien d'élément neutre le point $0_E = (\infty , \infty)$, avec la règle géométrique de 3 points colinéaires P , Q , R de E :

$$P + Q + R = 0_E$$

Preuve

Le symétrique d'un point P est le $2^{éme}$ point d'intersection de la courbe E par la parallèle à $O y$ passant par P :

$$P + (-P) = 0_E$$

Une droite $P Q$ n'est pas orientée, donc les droites $P Q$ et $Q P$ sont confondues :

$$P + Q = Q + P$$

La vérification de l'axiome d'associativité se fait par le calcul des points :

$P + Q = S$, $(P + Q) + R = S'$, $Q + R = T$ et $P + (Q + R) = T'$

!

Définition 5

Le groupe $E(K)$ est le groupe de Mordell-Weil de la courbe elliptique E sur un corps K

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

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

Soit un point $P = (x_P , y_P)$ du groupe $E(K)$ et son symétrique $-P = (X , Y)$

$P + (-P) = 0_E$

Le point $-P$ est l'intersection de la courbe E par la parallèle à $0y$ passant par P.

L'équation de cette parallèle passant par P est :

$x = x_P$

L'abscisse du point $-P = (X , Y)$ *est égale à celle du point* P *:*

$X = x_P$

L'ordonnée de $-P$ est racine de l'équation :

$$y^2 + a_1 x_P y + a_3 y = x_P{}^3 + a_2 x_P{}^2 + a_4 x_P + a_6 ;$$

C'est une équation en y du 2ème degré, elle admet 2 racines : y_P et Y

Leur somme est égale à :

$Y + y_P = -(a_1 x_P + a_3)$

Nous en déduisons le symétrique $-P$ du point P :

$$-P = (x_P , -y_P - a_1 x_P - a_3) \qquad (3)$$

Calcul des coordonnées du point somme $P_1 + P_2$ de deux points : $P_i = (x_i , y_i)$, pour $P_1 \neq \pm P_2$ (fig.2) :

La règle géométrique $P_1 + P_2 + P_3 = 0_E$ implique :

$P_1 + P_2 = -P_3 = R$

Le point P_3 est obtenu avec l'intersection de E par la droite $P_1 P_2$:
L'équation de la droite $P_1 P_2$ est :

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

Cette sécante $P_1 P_2$ coupe la courbe en trois points simples P_1, P_2 et P_3
Les abscisses de ces 3 points sont les zéros de l'équation cubique :

$$[\lambda (x - x_1) + y_1]^2 + (a_1 x + a_3)[\lambda (x - x_1) + y_1] = x^3 + a_2 x^2 + a_4 x + a_6$$

La somme de ces zéros est égale :

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

Les calculs donnent les coordonnées du point somme $P_1 + P_2 = -P_3 = R$

$$P_1 + P_2 = \begin{cases} x_R = \lambda^2 + a_1 \lambda - a_2 - x_1 - x_2 \\ y_R = -\lambda^3 - 2 a_1 \lambda^2 + \lambda (a_1 + 2 x_1 + x_2 - a_1^2) + a_1 a_2 - a_3 - y_1 + a_1 (x_1 + x_2) \end{cases} \tag{4}$$

Nous avons démontré la proposition 2 :

Proposition 9

Soit le groupe E (K) de Mordell-Weil d'une courbe elliptique

1) les coordonnées du symétrique $-P$ d'un point $P = (x_P , y_P)$ du groupe E (K) sont égales à :

$$-P = (x_P , -y_P - a_1 x_P - a_3)$$

2) pour 2 points P_1 et P_2 ; $P_1 \neq \pm P_2$ $P_i = (x_i , y_i)$
les coordonnées de la somme sont égales à :

$$P_1 + P_2 = R = \begin{cases} x_R = \lambda^2 + a_1 \lambda - a_2 - x_1 - x_2 \\ y_R = -\lambda^3 - 2 a_1 \lambda^2 + \lambda (a_1 + 2 x_1 + x_2 - a_1^2) + a_1 a_2 - a_3 - y_1 + a_1 (x_1 + x_2) \end{cases}$$

avec $\lambda = (y_1 - y_2) / (x_1 - x_2)$

6 . Points d'ordre fini du groupe de Mordell-Weil E (K)

Le groupe $E(K)$ de Mordell-Weil d'une courbe elliptique E possède plusieurs sous groupes particuliers :
les sous groupes $E(K)[m]$ de m-torsion et le sous groupe $T(E)$ de torsion de E

Coordonnées du point $P + P = 2P$ (fig.3) :

Soit un point $P = (x_P, y_P)$
Nous obtenons les coordonnées du point $2P$ à l'aide de la tangente à la courbe E en P

$$y = t(x - x_P) + y_P$$

Cette tangente a pour pente la dérivée y' :

$$y' = (3x_P^2 + 2a_2 x_P + a_4 - a_1 y_P) / (2y_P + a_1 x_P + a_3) = t$$

Cette tangente coupe la courbe en un point double (x_P, y_P) et un point simple
$R = (x_R , y_R)$
Les abscisses de ces 3 points sont les zéros de l'équation cubique :

$$[t(x - x_P) + y_P]^2 + a_1 x [t(x - x_P) + y_P] + a_3 [t(x - x_P) + y_P] = x^3 + a_2 x^2 + a_4 x + a_6 ;$$

La somme de ces zéros est égale :
$2x_P + x_R = t^2 + a_1 t - a_2$;
Les calculs donnent les coordonnées de la somme $2P = -R = S$

$$\begin{cases} x_S = t^2 + a_1 t - a_2 - 2x_P \ ; \\ y_S = -t^3 - 2a_1 t^2 + t(a_2 - a_1^2 + 3x_P) + a_1 a_2 - a_3 + 2a_1 x_P - y_P \ ; \end{cases}$$

Nous avons obtenu la :

Proposition 10

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

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

avec $t = (3 x_P^2 + 2 a_2 x_P + a_4 - a_1 y_P) / (2 y_P + a_1 x_P + a_3)$

!

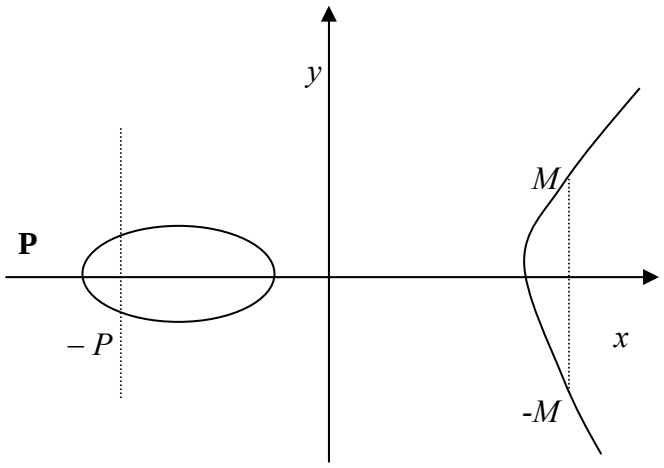


Figure 1 : Symétrique d'un point

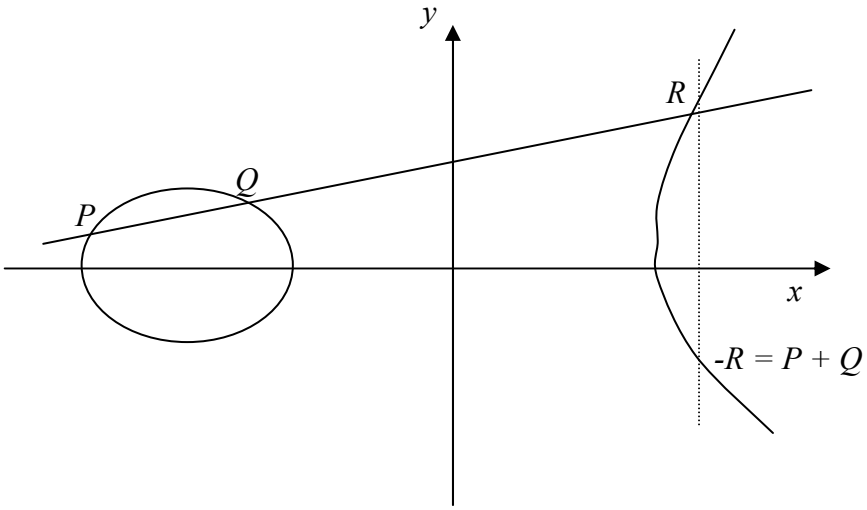


Figure 2 : Somme de deux points

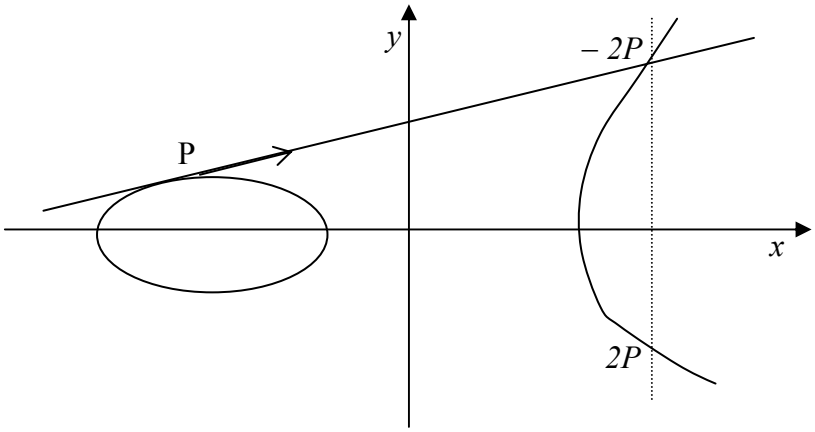


Figure 3 : Double d'un point

Exemple

Soit une courbe elliptique d'équation de Weierstrass :

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

Invariants :

$\Delta(E) = 37 = N(E)$; $j(E) = 27 \times 2^{12} / 37$

Calcul les coordonnées du point $m\,P$, $m = 1, 2, ..., 8$:

$P = (0, 0)$; $2P = (1, 0)$; $3P = (-1, -1)$; $4P = (2, -3)$; $5P = (\frac{1}{4}, -\frac{5}{8})$;

$6P = (6, 14)$; $7P = (-\frac{5}{9}, \frac{8}{27})$; $8P = (\frac{21}{25}, -\frac{69}{125})$, etc……

Ce point P engendre un groupe cyclique infini .

6-1 . Formules de Cassels des coordonnées des points mP , m > 2 :

Cassels **[4]** a obtenu les formules des coordonnées de points mP en prenant une courbe elliptique d'équation de Weierstrass :

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

Soit un point P du groupe E (Q) de Mordell-Weil de E .

Posons :

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

Selon Cassels (Diophantine Equations with special references to elliptic curves) les points m P ont pour coordonnées

$$m\,P = \left(\frac{\phi_m(P)}{\psi_m(P)^2}, \frac{\omega_m(P)}{\psi_m(P)^3} \right)$$

Les polynômes ψ_m sont égaux à :

$\psi_{-1} = -1$, $\psi_0 = 0$

$\psi_1 = 1$, $\psi_2 = 2y$ (6)

$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$ (7)

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

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

$$\psi_{2m+1} = \psi_{m+2}\,\psi_m^3 - \psi_{m-1}\,\psi_{m+1}^3 \quad ; \quad (m \geq 2) \qquad (9)$$

$$2y\,\psi_{2m} = \psi_m(\psi_{m+2}\,\psi_{m-1}^2 - \psi_{m-2}\,\psi_{m+1}^2) \quad ; \quad (m \geq 3) \qquad (10)$$

Les polynômes ϕ_m et ω_m sont déterminés par les formules :

$$\phi_m = x\psi_m^2 - \psi_{m+1}\,\psi_{m-1} \quad ; \quad (m \geq 2) \qquad (11)$$

$$4\,y\,\omega_m = \psi_{m+2}\,\psi_{m-1}^2 - \psi_{m-2}\,\psi_{m+1}^2 \quad ; \quad (m > 2) \qquad (12)$$

Proposition 11

Soit un point $P = (x, y)$ du groupe de Mordell-Weil $E(Q)$ d'une courbe elliptique E sur le corps Q des rationnels d'équation de Weierstrass :

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

Alors les coordonnées d'un point mP du groupe $E(Q)$ sont :

$mP = (x_m, y_m)$ avec :

$$x_m = \frac{\phi_m(P)}{\psi_m(P)^2} \quad , \quad y_m = \frac{\omega_m(P)}{\psi_m(P)^3}$$

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

Les polynômes ψ_m , ϕ_m , et ω_m satisfont les relations :

$$\phi_m = x\psi_m^2 - \psi_{m+1}\,\psi_{m-1} \quad ; \quad (m \geq 2) \qquad (11)$$

$$4\,y\,\omega_m = \psi_{m+2}\,\psi_{m-1}^2 - \psi_{m-2}\,\psi_{m+1}^2 \quad ; \quad (m > 2) \qquad (12)$$

Preuve

C'est le lemme 7-2 de l'article « Diophantine Equations with special references to elliptic curves »

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

Pour $m = -1$, $-P$ est le symétrique du point P, il en résulte $\psi_{-1} = -1$

Les formules se démontrent par récurrence sur l'entier naturel m

+

6-2 . Sous groupes de m- torsion . Groupe de torsion

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

Définitions 6

1) Le sous groupe de m – torsion d'une courbe elliptique E, pour tout entier m > 1, est l'ensemble des points $P \in E(K)$ *d'ordre m :*

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

Ces sous groupes sont cycliques d'ordre m .

2) Le groupe de torsion de la courbe elliptique est l'ensemble des points P d'ordre fini ; c'est la réunion infinie des sous groupes de m- torsion de E :

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

Ce groupe de torsion T (E) est cyclique ou abélien, selon les invariants de la courbe elliptique .

La détermination du groupe de torsion T (E) a été réalisée pour les courbes elliptiques sur le corps Q des nombres rationnels

Proposition 12

Le groupe de torsion d'une courbe elliptique E, sur le corps Q, est l'un des 15 types :

$ZI / m\,ZI$ pour $m = 1, 2, 3, \ldots\ldots, 10$ et $m = 12$

$ZI / 2\,ZI \oplus ZI / 2d\,ZI$ pour $d = 1 , 2 , 3 , 4$

Preuve par Mazur, dans [1] !

Certains résultats ont été obtenus pour des corps quadratiques, des corps cubiques , des corps quartiques.

Théorème de Mordell-Weil

L'ensemble E (K) des points K- rationnels d'une courbe elliptique E définie sur un corps de nombres K est un groupe abélien de type fini .

$\forall$

Preuve par Silverman dans [2]

La structure du groupe de Mordell-Weil d'une courbe elliptique est précisée par le :

Corollaire

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

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

où $T(E)$ est le groupe de torsion de la courbe elliptique E, et $r = r(E) \geq 0$ est un entier naturel et $ZI^r = r$ copies du groupe ZI .

–

Définition 7

L'entier naturel $r = r(E) \geq 0$ de cette formule d'isomorphisme est le rang de la courbe elliptique E.

7. Isomorphisme de courbes elliptiques

Soit l'application :

$$f : E(K) \longrightarrow E'(K)$$
$$(x, y) \longrightarrow (u^2 x + r , u^3 y + u^2 x s + t)$$

de groupes de Mordell-Weil des courbes elliptiques E et E' avec :

u , r , s , t dans K et $u \neq 0$

Cette application satisfait 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 :

$$E : y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 ;$$

en l'équation de la courbe elliptique E' :

$$E' : y^2 + a'_1 x y + a'_3 y = x^3 + a'_2 x^2 + a'_4 x + a'_6 ;$$

Les coefficients a_i et les invariants de E sont liés à ceux de E' par les relations :

$u\,a'_1 = a_1 + 2\,s$

$u^2\,a'_2 = a_2 - s\,a_1 + 3\,r - s^2$

$u^3\,a'_3 = a_3 + r\,a_1 + 2\,t$

$u^4\,a'_4 = a_4 - s\,a_3 + 2\,r\,a_2 - (t + r\,s)\,a_1 + 3\,r^2 - 2\,s\,t$

$u^6\,a'_6 = a_6 + r\,a_4 + r^2\,a_2 + r^3 - t\,a_3 - t^2 - r\,t\,a_1$

$u^2\,b'_2 = b_2 + 12\,r$

$u^4\,b'_4 = b_4 + r\,b_2 + 6\,r^2$

$u^6\,b'_6 = b_6 + 2\,r\,b_4 + r^2\,b_2\ 4\,r^3$ (14)

$u^8\,b'_8 = b_8 + 3\,r\,b_6 + 3\,r^2\,b_4 + r^3\,b_2 + 3\,r^4$

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

$u^6\,c'_6 = c_6$

$u^{12}\,\Delta' = \Delta$

$j(E') = j(E)$

$u^{-1}\,\omega' = \omega$

Exemple

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

$y^2 + 3\,x\,y - 5\,y = x^3 - 6\,x^2 + 7\,x - 8$;

Calcul des invariants :

$b_2 = -15$; $b_4 = 1$; $b_6 = -7$; $b_8 = 26$; $\Delta(E) = -8110$

$c_4(E) = 249$, $j(E) = \dfrac{249^2}{-8110}$

Considérons l'isomorphisme d'équations :

$x = (-2)^2\,x' + 3$; $y = (-2)^3\,y' + (-2)^2 \times 3\,x - 5$

Les formules d'isomorphisme (14) permettent de trouver l'équation de Weierstrass de la courbe E' isomorphe à E :

$$E' \ : \ y'^{2} - \frac{9}{2} x' y' + \frac{3}{4} y' = x'^{3} - \frac{15}{4} x'^{2} + \frac{31}{16} x' - \frac{19}{64}$$

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

Théorème 2

Deux courbes elliptiques E et E′, définies sur un corps algébriquement clos K sont isomorphes si et seulement si leurs invariants modulaires sont égaux

$$j(E') = j(E)$$

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

Soient deux courbes elliptiques E et E' isomorphes :

Alors leurs invariants modulaires $j(E')$ et $j(E)$ sont liés par les formules (14), donc : $j(E') = j(E)$

0

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

Soient deux courbes elliptiques E et E' ayant même invariant $j(E) = j(E')$ sur un corps K de caractéristique $\neq 2, 3$

Nous prenons des équations de Weierstrass de E et E' de la forme :

$$E : \ y^2 = x^3 + A x + B \quad \text{avec la condition} \quad 4A^3 + 27B^2 \neq 0 \qquad (15)$$

$$E' : \ y'^2 = x'^3 + A' x' + B' \quad \text{avec la condition} \quad 4A'^3 + 27B'^2 \neq 0 \qquad (16)$$

L'hypothèse j (E) = j (E') *et la formule de l'invariant* j (E) *impliquent l'égalité :*

$$A^3 B'^2 = A'^3 B^2 \qquad (17)$$

Le seul changement de variables qui transforme (15) en (16) est :

$$x = u^2 x' \quad , \quad y = u^3 y' \qquad (18)$$

où u est un élément non nul d'une clôture algébrique K' de K

(15), (16) et (18) impliquent les relations :

$$u^4 A' = A \quad , \quad u^6 B' = B \quad \text{et} \quad u^{12} \Delta(E') = \Delta(E) \qquad (19)$$

Les formules (17) impliquent trois cas possibles pour les valeurs de A et B :

$$\begin{cases} A = 0 \text{ et } B \neq 0 \\ \quad \text{ou} \\ A \neq 0 \text{ et } B = 0 \\ \quad \text{ou} \\ A\,B \neq 0 \end{cases}$$

Examinons ces 3 cas :

1^er^ cas : $A = 0$ et $B \neq 0$

Les formules (19) impliquent l'équation :

$$u^6 B' = B$$

Nous obtenons des isomorphismes en prenant $u = (B / B')^{1/6}$; 6 valeurs de u suivant les racines 6ème de 1

2ème cas : $A \neq 0$ et $B = 0$

Les formules (14) impliquent l'équation :

$$u^4 A' = A$$

Nous obtenons des isomorphismes en prenant $u = (A / A')^{1/4}$; 4 racines 4ème de 1

3ème cas : $A\,B \neq 0$

Les formules (14) impliquent l'équation :

$$u = (B / B')^{1/6} = (A / A')^{1/4}$$

alors chaque valeur de u donne l'isomorphisme désiré .

0

CHAPITRE III

TWISTS – ESPACES HOMOGENES - GROUPES ASSOCIES

1 . Twists

La notion de « twist » figure dans plusieurs ouvrages :

(1) Weiss a introduit le « twist »

$$T : A \times B \longrightarrow B \times A , \quad T(a , b) = (b , a)$$

d'une paire (A , B) de deux ensembles A et B,

et le « twist » d'une paire de G- modules

$$\theta^T : B \times A \longrightarrow C, \quad \theta^T(b , a) = \theta(a , b)$$

avec l'application

$$\theta : A \times B \longrightarrow C$$

(**2**) Mazur et Tate ont introduit le groupe diedral « twisté ».

Il s'agit d'un groupe Δ, extension diedrale du groupe $ZI / 2ZI$, qui est « twisté » par le groupe $\Gamma = (ZI / nZI)^* / (\pm 1)$, dans la suite exacte :

$$0 \longrightarrow \Gamma \longrightarrow \Delta \longrightarrow ZI / 2ZI \longrightarrow 0$$

Ces groupes satisfont les 3 relations :

$$(1) \ \gamma_m \Gamma_z = \Gamma_z^m \quad , \quad (2) \ \Gamma_z \gamma_m \Gamma^{-1}{}_z = (\gamma_m)^{-1} \quad , \quad (3) \ (\Gamma_z)^2 = 1$$

où z est une racine primitive $n^{ème}$ de 1, pgcd (n , m) = 1, Γ_z est un élément du groupe quotient Γ/Δ, et γ_m est l'image de m dans Γ par l'application

$$(ZI / nZI) \longrightarrow \Gamma$$

(**3**) Silverman a réservé le paragraphe 2 chapitre X à la théorie des twists des courbes elliptiques

(**4**) Cassels a consacré la « Partie II – The geometry of elliptic Curves - Twistings » à la théorie des twists

C'est sur la base de ces références que nous présentons un exposé sur les twists de courbes elliptiques .

Considérons 2 courbes elliptiques E et E' et leurs groupes de Mordell – Weil $E(K)$ et $E'(K)$. Ces 2 courbes sont choisies telles que leurs corps de fonctions soient isomorphes

$$K(E) \xleftrightarrow{\sim} K(E') \tag{1}$$

Soit une extension algébrique finie L du corps K et les groupes d'automorphismes :

$$G = G(L/K)\ ,\ \Gamma = G(L(E)/K(E)) \text{ et } \Gamma' = G(L(E')/K(E')) \tag{2}$$

Un K – isomorphisme $L(E) \longleftrightarrow L^{x}(E')$ n'est pas considéré comme un prolongement d'un isomorphisme $K(E) \longleftrightarrow K(E')$.

Les automorphismes S dans G, $\hat{S}$ dans Γ et S ' dans Γ' sont définis par les relations :

$$\hat{S}(x) = S(x) \text{ pour } x \in L \text{ et } \hat{S}(P) = P \text{ pour tout point } P \in E(K) \tag{3}$$

$$S'(x) = S(x) \text{ pour } x \in L \text{ et } S'(P') = P' \text{ pour tout point } P' \in E'(K)$$

Posons

$$S'(P) = \lambda_S(P) \tag{4}$$

Tout automorphisme T dans G satisfait l'égalité :

$$(T\,\lambda_S)(T'(P)) = T'S'(P) = \lambda_{TS}(P) \tag{5}$$

Il en résulte la formule :

$$(T\,\lambda_S)\,\lambda_T = \lambda_{TS} \tag{6}$$

C'est l'équation d'un cocycle d'un groupe de cohomologie $H^1(G, \Gamma)$

Avec ces automorphismes, il faut trouver un changement de variables :
$(x , y) \longrightarrow (x' , y')$ qui transforme l'équation $y^2 = f (x) \in K [x , y]$ de E, en une équation $y'^{\,2} = f (x') \in K [x' , y']$ de E ' ; alors cette courbe E ' est le twist de E par l'extension *L* de *K* . Ce twist *E '* est *L*- isomorphe à la courbe elliptique *E* .

Définition 1

Un twist d'une courbe elliptique E est une courbe elliptique E_L , définie sur K, comme E, et L- isomorphe à E pour une certaine extension algébrique finie et normale L de K .

Les relations entre ces groupes d'automorphismes et les groupes de cohomologie H^1 peuvent être consultées dans les références .

Exemple :

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

$$E \ : \ y^2 = x^3 + a_2 x^2 + a_4 x + a_6 = f (x) \in Q [x , a_2 , a_4 , a_6] \qquad (7)$$

Soit une extension quadratique $L = Q (\sqrt{d})$ du corps de base *Q* de *E*

Alors les groupes d'automorphisms :

$$G = G (L / Q) = \{ S \ , \ S^2 = Id \} \text{ et } \Gamma = G (L (E) / Q (E)) \qquad (8)$$

opèrent sur la courbe elliptique E *et sur les groupes* E (Q) *et* E (L) .

Pour le changement de variables :

$$x = x' / d \quad , \quad y = y' / \sqrt{d} \, , \qquad (9)$$

l'équation de E *devient :*

$$E' = E_d \ : \ y'^{\,2} / d = x'^{\,3} / d^{\,3} + a_2 \, x'^{\,2} / d^{\,2} + a_4 \, x' / d + a_6 \, , \qquad (10)$$

Par simplification par $d^{\,3}$*, nous obtenons l'équation :*

$$E_d \ : \ d^{\,2} y'^{\,2} = x'^{\,3} + a_2 \, d \, x'^{\,2} + a_4 \, d^{\,2} x' + a_6 \, d^{\,3} \ . \qquad (11)$$

Le changement de variables : (12)

$$x' = X \ \ et \ \ d \, y' = Y$$

donne l'équation du twist E_d *de la courbe elliptique* E *:*

$$E_d \ : \ Y^{\,2} = X^{\,3} + a_2 \, d \, X^{\,2} + a_4 \, d^{\,2} X + a_6 \, d^{\,3} \qquad (13)$$

Par les formules des invariants nous obtenons le discriminant :

$$\Delta (E) = 16 \, [\, 18 \, a_2 \, a_4 \, a_6 - 4 \, a_4^{\,3} - 27 \, a_6^{\,2} - 4 \, a_2^{\,3} a_6 + a_2^{\,2} \, a_4^{\,2} \,] \qquad (14)$$

En remplaçant a_2 par $a_2 d$, a_4 par $a_4 d^2$ et a_6 par $a_6 d^3$ dans $\Delta(E)$, nous obtenons le discriminant du twist quadratique E_d de E :

$$\Delta(E_d) = d^6 \Delta(E) = (\sqrt{d})^{12} \Delta(E) \qquad (15)$$

Ainsi, la relation d'isomorphisme de 2 courbes elliptiques :

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

est satisfaite pour le nombre $u = \sqrt{d}$ de $Q(\sqrt{d})$

2 . Espaces homogènes d'une courbe elliptique

Dans l'ensemble des automorphismes d'un groupe, il y a des translations .

Considérons l'automorphisme du groupe de Mordell – Weil $E(K)$ *:*

$$t : E(K) \longrightarrow E(K) \quad , \quad t(P) = P + a_t \quad , \qquad (16)$$

où a_t est un point défini sur une extension normale finie L du corps K .

Selon Cassels ces automorphismes t forment un groupe Γ, ils satisfont le cocycle identité

$$t a_s + a_t = a_{ts} \quad , \text{ pour } t \text{ dans } \Gamma, \ a_s \ , \ a_t \ , \ a_{ts} \text{ dans } L \qquad (17)$$

Un tel cocycle détermine une variété A, définie sur K, qui peut être une courbe elliptique birationnellement L- équivalente à la courbe elliptique E ; cette variété A est de dimension 1 .

Les cocycles (17) et l'isomorphisme $L(E) \xrightarrow{\sim} L(A)$ permettent de définir la structure d'espaces homogènes d'une courbe elliptique E

Définition 2

Un espace homogène d'une courbe elliptique E, pour une extension finie L, du corps K de E, est une courbe A, munie d'une application :

$$\mu : A \times E \longrightarrow A \quad \text{qui satisfait :}$$

$$\mu(P_A , 0_E) = P_A$$

$$\mu(\mu(P_A , P) , R) = \mu(P_A , P + R)$$

pour tous points P_A de A, P et R de E et $0_E = (\infty, \infty)$

et de l'application réciproque :

$$v : A \times A \longrightarrow E \quad \textit{qui satisfait :}$$

$$v(P_A , R_A) = P \quad \text{avec } \mu(R_A , P) = P_A$$

Ce point P est unique . Cet espace homogène est principal

Il en résulte la valeur $v(P_A, P_A) = 0_E$ pour tout point P_A de la courbe A

Cette définition constitue « le lemme 10-1 » dans **« Equation diophantine »** *de Cassels .*

Le triplet (A , v , μ) d'un espace homogène d'une courbe elliptique est défini sur le même corps que celui de la courbe elliptique E

Dans l'ensemble des espaces homogènes (A , μ , ν) d'une courbe elliptique E, il y a une relation d'équivalence :

Définition 3

2 espaces homogènes (A_1, μ_1, v_1) et (A_2, μ_2, v_2) d'une courbe elliptique E sont dans la même classe s'il existe un isomorphisme :

$$\lambda \ : \ A_1 \longrightarrow A_2 \quad , \quad \lambda(P_1) = P_2$$

qui rend commutatif le diagramme :

$$\begin{array}{ccc} A_1 \times E & \xrightarrow{\mu_1} & A_1 \\ \downarrow & & \downarrow \lambda \\ A_2 \times E & \xrightarrow[\mu_2]{} & A_2 \end{array}$$

Donc $\mu_2(\lambda(P_1), P) = \lambda(\mu_1(P_1, P))$ pour tous points $P_1 \in A_1$ et $P \in E$

D'après les propriétés des classes d'équivalence, la courbe elliptique E appartient à l'une de ces classes

Définition 4

La classe triviale d'espaces homogènes (A , v , μ) d'une courbe elliptique E est la classe de cette courbe, avec pour l'application μ la loi d'addition du groupe E (K) de Mordell-Weil .

Proposition 1.

Un espace homogène (A , μ , v) d'une courbe elliptique E sur K, est dans la classe triviale si et seulement si le groupe de Mordell-Weil A (K) n'est pas vide

!

L'ensemble des classes homogènes (A , μ , ν) d'une courbe elliptique E engendre plusieurs groupes particuliers .

3 . Groupe de Châtelet - Weil d'une courbe elliptique

Définition 5

Le groupe de Châtelet- Weil d'une courbe elliptique E est le groupe $WC(E/K)$ des classes d'équivalence des espaces homogènes pour E

L'ordre de ce groupe peut être déterminé avec la :

Proposition 2

Soit une courbe elliptique E, son groupe de Châtelet – Weil $WC(E/K)$ et le groupe de Galois G d'une clôture algébrique K_{alg} du corps K

Alors il y a une bijection :

$$WC(E/K) \rightarrow H^1(G, E)$$

$$\{ C/K \} \rightarrow \{ \sigma \rightarrow \sigma(P_0) - P_0 \}$$

pour un point P_0 de C,

qui associe à toute classe $Cl(C, \mu)$ d'espaces homogènes un élément :

$$\{ S \longrightarrow S(P) - P \} \text{ de } H^1 \text{ pour un point } P \text{ de } C$$

(Th.3.6-X-Silverman)

!

Un groupe $WC(E/K)$ possède des sous groupes de torsion $WC(E/K)[m]$ et $WC(E/K)[\varphi]$, pour un entier m et une isogenie φ de $E(K)$

Lorsque la courbe E est définie sur un corps local K_v en une valuation $v \in V_K$, son groupe de Châtelet – Weil est $WC(E/K_v)$

4 . Groupe de Selmer - Groupe de Chafarevich – Tate

Ces groupes sont construits à l'aide d'isogénies, de m – torsion, de groupe de cohomologie et de groupes $WC(E/K_v)$.

La multiplication par un entier m :

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

est une isogenie de la courbe elliptique E .

L'ensemble $\{ t_m \ , \ m \in ZI \}$ *de ces isogénies est un anneau* $End(E)$ *isomorphe à l'anneau* ZI .

Le sous groupe $E(K)[m]$ *de* m- *torsion induit une suite de* G- *modules :*

$$0 \longrightarrow E(K)[m] \longrightarrow E(K) \longrightarrow E(K) \longrightarrow 0$$

et une suite exacte de groupes de cohomologie, pour $G = G_{Kalg/K}$

$$0 \longrightarrow E(K) / t_m E(K) \longrightarrow H^1(G, E[m]) \longrightarrow H^1(G, E)[m] \longrightarrow 0$$

Les groupes de Selmer et les groupes de Shafarevich –Tate sont définis dans [2] par la

Définition 6

1) Le m- groupe de Selmer d'une courbe elliptique E relatif à un sous groupe de m torsion E [m] de E (K) est le sous groupe noyau de l'application :

$$S_m(E/K) = \ker \{ H^1(G, E[m]) \to \prod_{v \in V_K} WC(E/K_v) \}$$

où G est le groupe de Galois d'une clôture algébrique K_{alg} *de K,* V_K *est l'ensemble des valuations inéquivalentes de K,*

$WC(E/K_v)$ *est le groupe de Châtelet - Weil de E sur le corps* K_v

Donc le m- groupe de Selmer est un sous groupe du 1^{er} *groupe de cohomologie* $H^1(G, E[m])$ *. Il dépend de l'entier m*

2) Le groupe de Shafarevich - Tate d'une courbe elliptique E, est le sous groupe noyau de l'application :

$$Ш(E/K) = \ker \{ WC(E/K) \to \prod_{v} WC(E/K_v) \}$$

Donc le groupe de Shafarevich – Tate est un sous groupe du groupe de Châtelet – Weil

Proposition 3

Soit une courbe elliptique E, les groupes $S_m(E/K)$ *de Selmer et* $Ш(E/K)$ *de Shafarevich – Tate, l'isogénie* t_m *et le sous groupe E [m] de m- torsion de E. Alors :*

1) la suite de groupes :

$$O \to E(K)/m\,E(K) \to S_m(E/K) \to Ш(E/K)[m] \to O$$

est exacte . C'est une suite de Kummer

2) le m-groupe de Selmer est fini

Preuve

1) découle des définitions des groupes de Selmer et de Shafarevich – Tate et des suites de cohomologie associées .

2) découle du théorème de Mordell – Weil et des applications des valuations à la réduction et à la ramification .

(Th . 4.2 – X – Silverman)

$\forall$

Exemple de 2 - groupe de Selmer

Soit la courbe elliptique E d'équation de Weierstrass :

$$E \; : \; y^2 = x^3 - 12\, x^2 + 20\, x \qquad (18)$$

Cette courbe E coupe l'axe O x en 3 points $(0 , 0)$, $(2 , 0)$ et $(10 , 0)$

Le théorème de 2- descente permet de trouver l'espace homogène de la courbe E, associé à la paire $(b_1 , b_2) \in K (S , 2) \times K (S , 2)$

où $K (S , 2)$ est le sous groupe du groupe K^* / K^{*2} :

$K(S , 2) = \{ \; b \in K^* / K^{*2} \; ; \; ord_v (b) \equiv 0 (\mathrm{mod}\, 2)$ pour tous $v \notin S \; \}$

L'espace homogène de E est une courbe A d'équation :

$$A \; : \qquad b_1 z_1^2 - b_2 z_2^2 = (e_2 - e_1) z_0^2 \; , \; b_1 z_1^2 - b_1 b_2 z_3^2 = (e_3 - e_1) z_0^2 \qquad (19)$$

où e_1 , e_2 , e_3 sont les abscisses des 3 points d'intersection de l'axe O x par la courbe elliptique E

Selon Silverman, le 2–groupe de Selmer et le groupe de Shafarevich –Tate sont égaux à :

$$S_2 (E / Q) \cong (ZI / 2\, ZI)^3 \quad \text{et} \quad Ш (E / Q) [2] = 0 \qquad (20)$$

Exemple d'espace homogène déterminé par l'isogénie :

$$\Phi (x , y) = (y^2 / x^2 , y (b - x^2) / x^2) \qquad (21)$$

de la courbe elliptique d'équation de Weierstrass :

$$E \; : \; y^2 = x^3 + a\, x^2 + b\, x \; ; \qquad (22)$$

Le point $(0 , 0)$ de cette courbe engendre un sous groupe d'ordre 2 :

$$F = \{ (0 , 0) , 2 (0 , 0) = 0_E \} \qquad (23)$$

Avec les formules d'isogénie de Velu, la courbe isogène E' a pour équation :

$$E' \; : \; y^2 = x^3 - 2a\, x^2 + (a^2 - 4b)\, x \; ; \qquad (24)$$

Alors, l'espace homogène de E, associé à un corps quadratique Q ($\sqrt{d}$), est la courbe d'équation :

$$A \ : \ d\,w^2 = d^2 - 2a\,d\,z^2 + (a^2 - 4b)\,z^4 \qquad (25)$$

d'après (Silverman , X – 4)

Exemple de p- groupe de Selmer

Groupes de Selmer de courbes elliptiques d'équation de Weierstrass :

$$E_p : y^2 = x^3 + p\,x \ , \quad p \text{ est un nombre } 1^{er} \geq 5$$

Avec le calcul, nous obtenons les invariants de la courbe :

$$\Delta(E_p) = -64\,p^3 \ , \ j(E_p) = 1728 \ .$$

Le groupe de Selmer de la courbe elliptique E_p dépend de p modulo 16

S_p (E_p / Q) est isomorphe à (ZI / 2 ZI) si $p \equiv 7,11 \bmod 16$,

à (ZI / 2 ZI)^2 si $p \equiv 3,5,13,15 \bmod 16$,

à (ZI / 2 ZI)^3 si $p \equiv 1,9 \bmod 16$

Le groupe de Shafarevich est lié au rang de la courbe elliptique E_p par la relation :

rg (E_p (Q)) + $\dim_2$ III (E_p / Q) [2] = 0 si $p \equiv 7,11 \bmod 16$,

= 1 si $p \equiv 3,5,13,15 \bmod 16$,

= 2 si $p \equiv 1 , 9 \bmod 16$

d'après (Proposition X- 6.2, Silverman)

Signalons que le groupe de Shafarevich III (E / Q) intervient dans la conjecture de Birch and Swinnerton-Dyer (" Notes on elliptic curves (I) and (II)", J.ReineAnge.Math.212 (1963), 7-25 and 218(1965), 79-108)

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

5 . Détermination d'un twist d'une courbe elliptique

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

$$E \ : \ y^2 = 4 x^3 + b_2 x^2 + 2 b_4 x + b_6 \in Q [x , b_2 , b_4 , b_6]$$

Déterminons un twist de la courbe E sur un corps quadratique $Q(\sqrt{d})$

Le changement de variables linéaire :

$(x , y) \longrightarrow (x , y / \sqrt{d})$

transforme l'équation E en l'équation :

$$E_d \ : \ y^2 = 4 d x^3 + d b_2 x^2 + 2 d b_4 x + d b_6$$

Par multiplication par $16 d^2$, nous obtenons l'équation :

$$E_d \ : \ (4 d y)^2 = (4 d x)^3 + 16 d^3 b_2 x^2 + 32 d^3 b_4 x + 16 d^3 b_6$$

Le changement de variables :

$(x , y) \longrightarrow (x / 4 d \ , \ y / 4 d)$

donne l'équation du twist E_d de la courbe elliptique E :

$$E_d \ : \ y^2 = x^3 + b_2 d x^2 + 8 b_4 d^2 x + 16 b_6 d^3$$

Exemple

Soit une courbe elliptique E d'équation de Weierstrass :

$$E \ : \ y^2 = 4 x^3 + x^2 - 6 x - 1$$

Déterminons un twist de la courbe E sur le corps quadratique $Q(\sqrt{2})$

Calcul des invariants de la courbe E :

$b_2 = 1$, $b_4 = - 3$, $b_6 = - 1$, $b_8 = -\frac{5}{2}$, $\Delta (E) = \frac{437}{2}$

$b_2 d = 2$, $8 b_4 d^2 = - 96$, $16 b_6 d^3 = - 128$

Le twist E_2 de la courbe elliptique E a pour équation de Weierstrass :

$$E_2 \ : \ y^2 = x^3 + 2 x^2 - 96 x - 128$$

6 . *Isogénies et Groupe de Selmer de courbes elliptiques*

Par la proposition 3, le groupe de *m*-Selmer est fini pour tout entier *m*

Dans un chapitre précèdent, nous avons défini la suite de Kummer d'une courbe elliptique E sur un corps K par la formule :

$$0 \longrightarrow E(K)/mE(K) \longrightarrow H^1(G, E(K)[m]) \longrightarrow H^1(G, E(K))[m] \longrightarrow 0$$

où $E(K)$ est le groupe de Mordell-Weil de E,

G est le groupe de Galois d'une clôture algébrique K_{alg} du corps K,

H^1 est le 1er groupe de cohomologie,

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

$H^1(G, E(K))[m]$ est un sous groupe de m- torsion du groupe H^1

Cette suite de groupes est exacte, elle induit une suite de Kummer pour les corps :

$$1 \longrightarrow K^{\times}/(K^{\times})^m \longrightarrow H^1(G, \Gamma(m)) \longrightarrow H^1(G, K_{alg}^{\times})$$

où $K^{\times}$ est le groupe multiplicatif des nombres non nuls du corps K,

$\Gamma(m)$ est le groupe multiplicatif des racines d'ordre m de 1.

D'après le « théorème 90 de Hilbert », le groupe $H^1(G, K_{alg}^{\times}) = 0$

Il existe un théorème de Kummer pour le Φ-groupe de Selmer, lié à une isogénie :

$\Phi : E(K) \longrightarrow E'(K)$ de courbes elliptiques .

Proposition 4

Soit une isogénie de courbes elliptiques :

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

le Φ- groupe de Selmer $S_{\Phi}(E) = \ker \{ H^1(G, E[\Phi]) \to \prod_{v \in V_K} WC(E/K_v) \}$

et le noyau de Φ sur le groupe de Chafarevich-Tate $Ш(E)[\Phi]$

1) la suite de Kummer :

$0 \to E'(K)/\Phi(E(K)) \to S_{\Phi}(E) \to Ш(E)[\Phi] \to 0$ est exacte.

2) le Φ- groupe de Selmer $S_{\Phi}(E)$ est fini

Preuve de 1

Cette suite provient du diagramme :

$$\begin{array}{ccccccccc} 0 & \to & E'(K)/\Phi(E(K)) & \to & H^1(G, E[\Phi]) & \to & WC(E/K)[\Phi] & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \prod_{v \in V_K} E'(K_v)/\Phi(E(K_v)) & \to & \prod_{v \in V_K} H^1(G_v, E[\Phi]) & \to & \prod_{v \in V_K} WC(E/K_v)[\Phi] & \to & 0 \end{array}$$

où V_K est l'ensemble des valuations inéquivalentes du corps K, et $G = G(K_{alg}/K)$

Par définition le groupe $S_{\Phi}(E)$ est un sous groupe de $H^1(G, E[\Phi])$
le groupe $Ш(E)$ est un sous groupe de $WC(E/K)$

Preuve de 2 : finitude du groupe de Selmer lié à une isogénie

Elle découle des 2 propositions suivantes

Proposition 5

Soit un G- module fini M, où $G = G(K_{alg} / K)$ et un ensemble fini $S \subset V_K$ de places de K

Soit un groupe $H^1(G, M, S) = \{ Cl \in H^1(G, M) ; Cl$ est non ramifié hors de $S \}$

Alors le groupe $H^1(G, M, S)$ est fini.

Preuve

Puisque M est fini et le groupe G agit de façon continue sur M, il y a dans le groupe G un sous groupe d'indice fini qui fixe chaque élément de M.

Il y a un entier n tel que $nx = 0$ pour tout $x \in M$

Alors pour une extension abélienne L de K d'exposant n, l'application naturelle :

$$\mathrm{Hom}(G(L/K), M) \rightarrow \mathrm{Hom}(G(K_{alg}/K), M, S)$$

est un isomorphisme

Il en résulte que le groupe $\mathrm{Hom}(G(K_{alg}/K), M, S)$ est fini

(c'est le lemme 4.3 du chapitre X, dans Silverman)

Proposition 6

Soit une isogénie :

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

et un ensemble fini S dans V_K de places contenant les places archimédiennes, les places v en lesquelles E a mauvaise réduction et les places v qui divisent deg Φ

Alors le Φ- groupe de Selmer satisfont l'inclusion :

$$S_{\Phi}(E) \subset H^1(G, E[\Phi], S)$$

(Corollaire.4.4-X-Silverman)

Exemple (Silverman X-4-5-1)

Soit la courbe elliptique E d'équation de Weierstrass :

$$E : y^2 = x^3 - 12 x^2 + 20 x$$

Alors son 2- groupe de torsion est égal à :

$E(Q)[2] = \{ (0,0), (2,0), (10,0), 0_E \}$

Par un argument de réduction modulo 3, le groupe de torsion de E est :

$T(E) = E(Q)[2]$

Son 2– groupe de Selmer est égal à :

$$S_2(E/Q) \cong (ZI/2ZI)^3$$

Il y a un résultat relatif aux groupes de Selmer de courbes elliptiques d'équation de Weierstrass $y^2 = x^3 + p x$

Proposition 7

Soit un nombre premier p impair et une courbes elliptique E_p d'équation de Weierstrass :

$$E_p : y^2 = x^3 + p x$$

Une isogénie de degré 2 :

$$\Phi : E_p(Q) \to E'_p(Q)$$

a pour noyau $E_p(Q)[\Phi] = \{ (0,0), 0_E \}$

Alors :

1) le groupe de torsion est $T(E_p(Q)) \approx ZI/2ZI$

2) le Φ- groupe de Selmer de E'_p est $S_\Phi(E'_p(Q)) \approx ZI/2ZI$

3) le Φ- groupe de Selmer de E_p est :

$$S_\Phi(E_p/Q) \approx \begin{cases} (ZI/2ZI) & \text{si } p \equiv 7,11 \bmod 16, \\ (ZI/2ZI)^2 & \text{si } p \equiv 3,5,13,15 \bmod 16, \\ (ZI/2ZI)^3 & \text{si } p \equiv 1,9 \bmod 16 \end{cases}$$

Preuve

On utilise le théorème de 2- descente d'une courbe elliptique *E* qui indique une 2-isogénie et les équations des espaces homogènes *C (E)* de la courbe

On considère un ensemble de représentants des classes dans le corps

$Q(S,2) = \{ x \in Q^*/Q^{*2} \ ; \ ord_v x \equiv 0 \bmod 2 \ ; \ v \notin S \}$:

$\{ \pm 1 , \pm 2 , \pm p , \pm 2p \}$

Les images des points de 2- torsion dans le groupe de Selmer :

$- p \in S_\Phi (E)$ et $p \in S_\Phi (E ')$

On considère l'espace homogène C_2 : $2 w^2 = 4 + p z^4$

Alors $p \in S_\Phi (E ')$ et -1 , ± 2 , $- p$, $- 2 p \notin S^\Phi (E ')$

Il en résulte $S_\Phi (E ') = \{ 1 , p \} \approx ZI / 2 ZI$

plus de détails dans Silverman, X, paragraphe 6, Proposition 6.2

#

Certains auteurs ont étudié les l- groupes de Selmer $S_l (E_D)$ de courbes elliptiques E_D d'équation de Weierstrass :

$$E_D \ : \ y^2 = x^3 + b_2 D x^2 + 8 b_4 D^2 x + 16 b_6 D^3 ,$$

Ces courbes sont des D- twists des courbes elliptiques E d'équation de Weierstrass :

$$E \ : \ y^2 = 4 x^3 + b_2 x^2 + 2 b_4 x + b_6$$

A chaque nombre premier l, correspondent le l- groupe de Selmer $S_l (E_D)$, le l- groupe de Chafarevich-Tate $III (E_D) [l]$ et la suite exacte de Kummer de la courbe E_D :

$$1 \ \rightarrow \ E_D / l E_D \rightarrow S_l (E_D) \rightarrow \ III (E_D) [l] \rightarrow \ 1$$

Kevin a évalué le nombre de nombres congruents D pour lesquels la courbe elliptique E_D : $y^2 = x^3 - D^2 x$ a un l- groupe de Selmer trivial pour $l = 3, 5, 7$ et 11. Il a calculé pour des nombres X, les proportions $t_l (X)$ des nombres de courbes E_D : $1 \leq D \leq X$ de l- groupe de Selmer trivial .

X	$t_3 (X)$	$t_5 (X)$	$t_7 (X)$	$t_{11} (X)$
1.000.000	0,32530	0,39535	0,42117	0,44022
5.000.000	0,32397	0,39543	0,42317	0,44420

Pour les courbes elliptiques E_D à Multiplication complexe, Kohnen et Ono, ont obtenu, avec des théorèmes de Coates, Wiles et Rubin une estimation du nombre de courbes elliptiques E_D de l- groupes $S_l (E_D)$ trivial :

Card { $|D| < X$, $S_l(E_D)$ trivial } $= c\dfrac{\sqrt{X}}{\log X}$,

pour un nombre premier l assez grand et une constante $c = c(l) > 0$.

En utilisant une méthode de Kolyvagin et des résultats de Mazur, Frey, etc.…relatifs aux propriétés des twists, des points - rationnels, des groupes de Selmer de courbes elliptique, James et Ono ont démontré le :

Théorème

Soit une courbe elliptique E de conducteur $N(E)$ ayant un point Q - rationnel d'ordre $l = 3, 5, 7$ et la courbe elliptique twist E_D
si tout facteur premier impair p de $N(E)$ satisfait les congruences :
$p \not\equiv 0, -1 \bmod l$. Alors :

1) pour $l = 3$

$$Card\{ -X < D < 0 , D \text{ sans facteur carré et } S_l(E_D) \text{ trivial } \} = cX,$$

pour une constante $c > 0$

2) pour $l = 5$ ou 7 et si $pgcd(D, l\,N(E)) = 1$ et $D \equiv 3 \bmod 4$ si $N(E)$ est pair et si le symbole de Legendre $\left(\dfrac{D}{p}\right) = -1$, pour tout facteur 1er impair p de $N(E)$ lorsque $ord_p(j(E)) \geq 0$, à $-\left(\dfrac{-c_4 c_6^{-1}}{p}\right)$ sinon, alors :

$$Card\{ -X < D < 0 , D \text{ sans facteur carré et } S_l(E_D) \text{ trivial } \} = c'\frac{\sqrt{X}}{\log X},$$

pour une certaine constante $c' > 0$

Preuve dans « Selmer groups of quadratic twist of elliptic curves », K.James , K.Ono , Math.Ann.314(1999),1-17.

En conclusion, l'étude des l- groupes de Selmer nécessite de nombreuses connaissances : arithmétiques des courbes elliptiques, géométrie des courbes elliptiques, théorèmes de descente infinie et finie, espaces homogènes, formes modulaires, formes paraboliques, séries L de Hasse - Dirichlet, etc…
Nous poursuivons notre recherche dans ces directions .

Références

[1] ***B . Mazur*** '' Rational Isogenies of prime degree '', Inv . Math . 44 (1978), 129-162

[2] ***J . H . Silverman*** '' The Arithmetic of Elliptic curves '' G.T.M 106, Springer Verlag (1986)

[3] ***J . Tate*** '' The Arithmetic of Elliptic Curves '' Invent . Math 23 (1974), 179-206

[4] ***J . W . S Cassels*** ''Diophantine Equations with special reference to elliptic curves '', J . London . Math . Soc 41 (1966), 193-291

[5] ***K . James, K . Ono*** '' Selmer groups of quadratic twists of elliptic curves '', Math . Ann . 314 (1999), 1-17

[6] ***R . Hartshorne*** '' Algebraic Geometry '' Springer Verlag (1977) ''

[7] ***R . Shafarevich*** '' Basic Algebraic Geometry '' Springer Verlag (1977)

[8] ***S . Lang*** '' Complex Multiplication '' Springer Verlag (1983)

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

[10] ***Birch and Swinnerton - Dyer*** '' Notes on Elliptic curves I and II '', J . Reine . Ange . Math .212 (1963), 7-25 and 218 (1965), 79-108 .

[11] ***B . Mazur*** et ***J . Tate*** '' Points of order 13 on Elliptic curves '', Inv.Math.22 (1973) 41-49

[12] **Weiss** '' Cohomology of groups '', Academic press (1969)