N°d'ordre : 15 / 2006- M/MT

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE D'ENSEIGNEMENT SUPERIEURE
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE
« HOUARI BOUMEDIENE»

Faculté des Sciences Mathématiques

MEMOIRE

Présentée pour l'obtention du diplôme de MAGISTER

EN : MATHEMATIQUES

Spécialité : Algèbre et Théorie des Nombres

Par : **ZERROUK Assia**

SUJET

Arithmétique et Géométrie de la famille E(a,N) de cubiques de Weierstrass E(a,N) : $y^2 + aNxy = x^3 + 2aN^2x^2 - N^2$

Soutenue le **: 21 /12/ 2006, devant le jury composé de :**

M. BEBBOUCHI Rachid	Professeur	(U.S.T.H.B)	Président
M. ZITOUNI Mohamed	Professeur	(U.S.T.H.B)	Directeur de thèse
M. HACHAÏCHI M S	Professeur	(U.S.T.H.B)	Examinateur
M. HERNANE Mohand Ouamar	Maitre.Conf	(U.S.T.H.B)	Examinateur

REMERCIEMENTS

Je tiens tout d'abord à exprimer mes plus sincères remerciements et ma gratitude à mon Directeur de thèse Monsieur ***Mohamed ZITOUNI*** *(professeur à l'USTHB) de m'avoir proposé ce sujet et de m'avoir guidé tout le long de la réalisation de cette thèse.*

Je remercie spécialement Monsieur ***Rachid BEBBOUCHI*** *(professeur à l'USTHB) pour l'honneur qu'il m'a fait en présidant mon jury de soutenance ,*

J'adresse également mes remerciements à Monsieur ***M.S HACHAÏCHI*** *(professeur à l'USTHB) et Monsieur* ***Mohamed Ouamar HERNANE*** *(Maître de conférences à l'USTHB) pour le temps consacré à la lecture de cette thèse et leur participation à mon jury de soutenance.*

SOMMAIRE

INTRODUCTION

Les ouvrages et les publications concernant les Courbes Elliptiques sont nombreux. La théorie de ces Courbes est liée à la Théorie des Nombres, à l'Analyse Complexe, à la Géométrie Algébrique.

Dans cette thèse, nous nous sommes intéressés à l'Arithmétique et la Géométrie de la famille E(a,N) de cubiques de Weierstrass :

$$\text{E (a, N) : } y^2 + aNxy = x^3 + 2aN^2x^2 - N^2 \in IR[x, y] \qquad (1)$$

Dans le chapitre 1 nous avons fait un bref exposé sur les Variétés Algébriques : Variétés Affines, Variétés Projectives, Variétés Abéliennes et Diviseurs de Variétés. Cela est en rapport avec la structure de Variété Abélienne des courbes elliptiques
Les cubiques E(a,N) sont des Variétés Abéliennes de dimension 1.

Dans le chapitre 2 nous indiquons quelques notions indispensables de la théorie arithmétique des courbes elliptiques : équations de Weierstrass, invariant discriminant $\Delta(E)$, invariant modulaire $j(E)$, invariant différentiel $\omega(E)$, d'après le formulaire [16-1]
Nous avons calculé les invariants de la famille E(a,N) de cubiques.

Dans le chapitre 3 nous construisons un groupe abélien sur l'ensemble E(K) des points rationnels avec la règle géométrique de 3 points colinéaires et le point à l'infini comme élément neutre. Nous avons suivi la méthode de Lang [9-2] pour démontrer que ce groupe E(K) est de type fini ; nous avons utilisé une fonction hauteur sur un groupe abélien et la descente infinie de Fermat.
Nous avons utilisé un résultat de Silverman pour obtenir la décomposition de ce groupe en produit direct de 2 groupes abéliens dont l'un au moins est fini :

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

Dans le 4eme chapitre et dernier chapitre, nous avons rappelé quelques éléments de la théorie des valuations d'un corps selon Iyanaga [6]
En nous basant sur Silverman [16-1], nous avons étudié les réductions d'une courbe elliptique en détail : bonnes et mauvaises réductions

Nous avons illustré chaque chapitre par une application à la famille E(a,N) de cubiques de Weierstrass.

Chapitre 1 : VARIETES ALGEBRIQUES

Une courbe elliptique admet plusieurs structures algébriques : structure de cubique non singulière, structure de variété abélienne de dimension un, structure de schéma non singulier de dimension un…
« La théorie des courbes elliptiques selon HARTSHORNE, fournit un bon exemple des relations profondes entre la Géométrie Algébrique, l'Analyse Complexe et la Théorie des Nombres.»
La théorie des Variétés Algébriques est décrite par plusieurs auteurs : R-HARTSHORNE [4], I-R-SHAFAREVICH [14], S-LANG [9], etc…
Nous examinerons successivement les Variétés Affines, les Variétés Projectives, les Variétés Abéliennes et les Diviseurs de Variétés.

1-Variétés affines :

Elles sont construites sur des espaces affines.

Définition1 : *Un n-espace affine, sur un corps algébriquement clos K est l'ensemble des n-uples ($a_1,...,a_n$) d'éléments $a_1,...,a_n$ de K.*

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

Dans le vocabulaire de la géométrie analytique, un élément a de l'espace affine est un point de cet espace ; les n éléments $a_1,...,a_n$ sont les coordonnées du point a.

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

Pour n=2, les polynômes sont de la forme :

$$f(X, Y)= \sum C_{ij} X^i Y^j \ ;\ i, j=0, 1,2,\ldots, t \qquad (2)$$

Pour n=3, les polynômes sont de la forme :

$$f(X ,Y ,Z)= \sum C_{i_1 i_2 i_3} X^{i_1} Y^{i_2} Z^{i_3} \ , 0 \le i_1, i_2, i_3 .$$

Puisque le corps de base K est algébriquement clos, tout polynôme f ∈ B admet des racines dans le corps K.

Définition2 : *Un ensemble algébrique de l'espace affine $IA^n(K)$ est une partie F de $IA^n(K)$ formée des zéros d'une famille U ∈ B de polynômes :*

$$F= \{P \in IA^n(K); f(P)=0 \text{ pour tout } f \in U\}. \qquad (3)$$

L'ensemble vide et l'espace affine $IA^n(K)$ sont considérés comme des ensembles algébriques ; la réunion et l'intersection d'une famille d'ensembles algébriques est un ensemble algébrique. Ces propriétés permettent d'introduire une topologie sur l'espace affine.

Définition3 : *La topologie de ZARISKI sur l'espace affine $IA^n(K)$ est constituée par les ensembles algébriques comme des fermés et leurs complémentaires comme des ouverts ; dans*

cette topologie l'ensemble vide et l'espace affine sont les seules parties ouvertes et fermées à la fois. Cette topologie de ZARISKI n'est pas de HAUSDORFF.

C'est l'espace topologique IA^n qui devient une variété.

Définition 4 : *Une Variété algébrique affine est un sous ensemble irréductible et fermé de l'espace affine $IA^n(K)$ avec la topologie de ZARISKI.*

L'espace affine possède des propriétés :

a/ L'espace $IA^n(K)$ est irréductible.

b/ Un polynôme irréductible f de l'anneau B=K [$X_1,...,X_n$] engendre une Variété algébrique affine.

Définition 5 : *Une variété algébrique quasi-affine est un sous ensemble ouvert d'une variété algébrique affine.*

Exemple :

L'ensemble X= {(t, t^2, t^3) ; $t \in K$} est une variété algébrique affine dans l'espace $IA^3(K)$, de dimension 1.
(HARTSHORNE, exercice 1.2).

2-Variétés projectives :

Elles sont construites sur des espaces projectifs

Définition 6 : *Un n-espace projectif est l'ensemble $IP^n(K)$ des classes d'équivalence des (n+1)-uples ($a_1, a_2,..., a_{n+1}$) d'éléments a_i du corps K, par la relation (Eq)*

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

La relation d'équivalence (Eq) est basée sur la propriété:
un point a= $(a_1, a_2,..., a_n, a_{n+1})$ est équivalent à un point b= $(b_1,..., b_n, b_{n+1})$ dans l'espace affine $IA^{n+1}(K)$ si et seulement si b= λ a= $(\lambda a_1, \lambda a_2,..., \lambda a_n)$ pour un élément $\lambda \neq 0$.

Donc l'espace projectif $IP^n(K)$ est l'ensemble quotient

$IA^{n+1}(K) - \{0\}$ par la relation d'équivalence (Eq)

L'anneau des polynômes associés à $IP^n(K)$ est à (n+1) indéterminées X_i.

$B=K[X_1,\ldots,X_n,X_{n+1}]$

La relation d'équivalence (Eq) implique que les polynômes $f \in B$ sont homogènes de degré d=1, 2,3…

Les notions d'ensembles algébriques et de topologie de ZARISKI des espaces affines $IA^{n+1}(K)$ se prolongent aux espaces projectifs

$IP^n(K) = IA^{n+1}(K)/(Eq)$

L'espace projectif $IP^n(K)$ devient un espace topologique avec la topologie de ZARISKI.

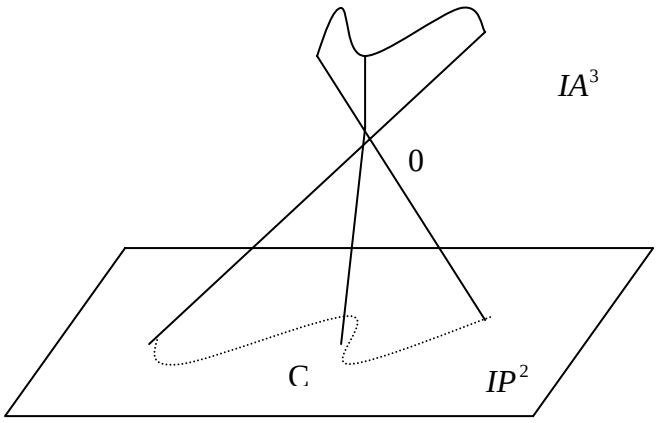
Définition7 **:** *(1)- une Variété algébrique projective est un sous ensemble fermé et irréductible de l'espace projectif* $IP^n(K)$.
(2)- une Variété *algébrique quasi-projective est un sous ensemble ouvert d'une variété algébrique projective.*

Exemples :

(1) toute famille de polynômes $\{f_1,\ldots,f_t\}$ de l'anneau $K[X_1,\ldots,X_n,X_{n+1}]$ admet des zéros qui forment une variété algébrique projective.

(2) Lorsque le polynôme f est linéaire, la variété algébrique est un hyperplan :$H=\{P\in IP^n(K)\ ;f(P)=0\ ;f=C_1X_1+\ldots+C_{n+1}X_{n+1}\}$

(3) Cone sur une courbe C dans l'espace projectif $IP^2(K)$, (HARTSHONE ,exercice2-10)



(4) l'intersection et la réunion de 2 variétés algébriques projectives ne sont pas des variétés : soit 2 variétés Y_1et Y_2 dans $IP^n(K)$,alors $Y_1\cap Y_2$ et $Y_1\cup Y_2$ ne sont pas des variétés.
Exercice 2-16, HARTSHORNE

(5) Soit la famille E(a,N) de cubiques de Weierstrass d'équation affine :
$E(a,N): y^2+aNxy=x^3+2aN^2x^2-N^2;$

Dans le plan projectif $IP^2(K)$, cette équation devient :
$E(a,N): Y^2Z+aNXYZ=X^3+2aN^2X^2Z-N^2Z^3;$

3-Variétés abéliennes

Elles sont construites sur des groupes algébriques.

Définition8 *: Une Variété abélienne est une Variété projective X munie d'une structure de groupe abélien ,d'élément neutre O_X ,et de loi*

$$X \times X \to X ; (P, Q) \to P+Q \quad , P + P^{-1} = O_X$$

$$X \to X \quad , P \to P^{-1}$$

Exemple :

Courbe elliptique E d'équation f(x, y)=0

La loi de groupe abélien provient de la propriété de 3 points colinéaires de la courbe elliptique E

$$P_1+P_2+P_3=O_E$$

La courbe E à un structure de Variété abélienne dans l'espace projectif $IP^2(K)$; sa dimension est égale à (dim $IP^2(K)$)-(relation f(x, y) = 0) =2-1 =1

Cela implique la

Définition9 **:** *Une courbe elliptique a une structure de Variété abélienne de dimension un.*

La loi de groupe abélien sera étudiée complètement dans le chapitre « groupe de MORDELL-WEIL » d'une courbe elliptique.

4-Diviseurs de Variétés

Références : HARTSHORNE (chapitre 2-6 p 129-149)
SHAFAREVICH (chapitre 2-p 127-147)

Dans la théorie des Diviseurs, il y a des diviseurs de WEIL, des diviseurs de CARTIER
Nous ne considérons ici que les diviseurs de WEIL

Définition10 : *Soit une courbe algébrique C non singulière projective dans l'espace $IP^2(K)$; une ligne L de $IP^2(K)$ coupe C en d points avec les multiplicités n_i ; un diviseur de la courbe C est une somme formelle :*

$$D=\sum n_i P_i \ , n_i \in ZI \ , P_i \in C \ .$$

Lorsque la ligne L varie, les points d'intersection $L \cap C$ déterminent un ensemble Div(C) de diviseurs de la courbe algébrique C.

Cet ensemble de diviseurs est muni d'une structure de groupe abélien avec comme élément neutre le diviseur $O = \sum OP_i$.

La loi d'addition pour 2 diviseurs : $D=\sum_i n_i P_i$ et $D'=\sum n_i' P_i$

La somme est le diviseur : D+D'= $\sum_i (n_i + n_i^{'})P_i$.

et le symétrique –D= $\sum_i - n_i P_i$.

Définition11 : *Un diviseur de WEIL est un élément du groupe abélien libre Div(C) engendré par les diviseurs premiers D =nP.*

Les entiers $n_i>0$ correspondent aux zéros de l'équation f(x,y)=0 de la courbe C, les entiers $n_i<0$ correspondent aux pôles de l'équation.
Il y a des diviseurs particuliers.

Définition 12 **:** *(1) un diviseur D=* $\sum_i n_i p_i$ *est effectif si tous les coefficients* n_i *sont positifs.*
(2) un diviseur principal est le diviseur d'une fonction f $\in K^*$

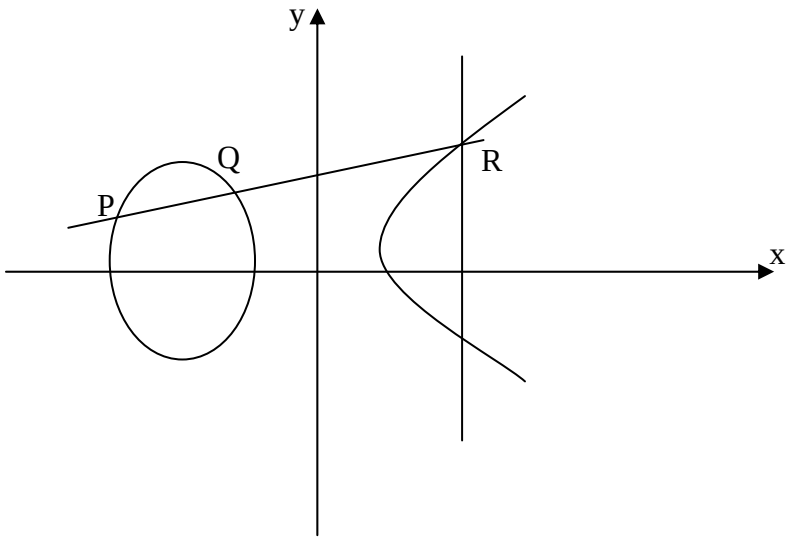
Il existe une relation d'équivalence dans le groupe des Diviseurs.

Définition13: *Dans le groupe Div X des diviseurs d'une Variété X, la relation « D équivalent à D' si le diviseur D-D' est principal » est une relation d'équivalence ; le groupe quotient Div X par le sous groupe P(X) des diviseurs principaux est le groupe des classes de diviseurs de X*

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

Définition14: *Le degré d'un diviseur D=* $\sum_i n_i P_i$ *est égal à l'entier d=* $\sum n_i$.

Exemple1 :
Courbe cubique non singulière d'équation projective :
$Y^2Z = X^3 - XZ^2$ dans l'espace IP^2 (IR).



La relation P + Q + R = O_E implique les diviseurs (P) +(Q) +(R) =3 (O_E)
Le point à l'infini O_E= (∞,∞) = (0, 1,0) est l'élément neutre de la loi du groupe abélien formé des points de la cubique ; il est déterminé par la direction de l'axe Oy.

Exemple2 :
Courbe algébrique plane C d'équation :

$$y^2 = (x-1)^2(x-2)^3(x-3)^{-1}(x-4)^{-3} ;$$

Cette courbe admet 2 zéros : P_1 = (1,0) d'ordre 2 et P_2 = (2,0) d'ordre 3;
et 2 pôles : P_3 = (3,0) d'ordre 1 et P_4 = (4,0) d'ordre 3 ;

Le Diviseur associé à cette fonction est la somme formelle :

$$\text{Div}(f) = 2(P_1) + 3(P_2) - (P_3) - 3(P_4)$$

Exemple3 :
Famille de cubiques de Weierstrass :

$$E(a,N) : y^2 + aNxy = x^3 + 2aN^2x^2 - N^2$$

La droite d'équation $y = 2Nx + 1$ coupe les cubiques E(a,N) en 3 points P_1 ,P_2 et P_3
Les diviseurs associés satisfont :

$$(P_1) + (P_2) + (P_3) = 3\,(O_E)$$

Chapitre 2 : CUBIQUES DE WEIERSTRASS

1-Equation de Weierstrass :

Dans ce chapitre nous nous intéressons à des cubiques particulières.

Définition1 **:** *Une courbe elliptique est une cubique plane, irréductible non singulière, d'équation spécifique de Weierstrass :*

$$E:\ Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \in K[X,Y] \qquad (1)$$

Cette équation détermine une cubique de Weierstrass.
K est un corps commutatif global, local ou fini.
L'équation (1) se transforme en d'autres équations par des changements de variables convenables.
Eliminons les monômes en XY et Y avec le changement de variables linéaire

$$(X,Y) \to \left[x, \frac{1}{2}(y - a_1x - a_3) \right] \qquad (1\text{-}2)$$

Nous obtenons pour un corps K de $carac(K) \neq 2$, l'équation de Weierstrass :

$$E_1:\ y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 \in K[x,y] \qquad (1\text{-}3)$$

Les trois coefficients b_{2i} sont des polynômes « homogènes » de degré 2i de l'anneau $Z/[a_1, a_2, a_3, a_{4,} a_6]$:

$$b_2 = a_1^2 + 4a_2\ ;\ b_4 = a_1a_3 + 2a_4;\ b_6 = a_3^2 + 4a_6 \qquad (1\text{-}4)$$

Eliminons le coefficient 4 et le monôme en x^2 dans l'équation de E_1 avec le changement de variables :

$$(x, y) \to [\frac{X - 3b_2}{36}, \frac{Y}{108}] \qquad (1\text{-}5)$$

Pour $carac(K) \neq 2,3$, nous obtenons l'équation de Weierstrass :

$$E_2 : Y^2 = X^3 - 27c_4X - 54c_6 \quad \in K\ [X, Y] \qquad (1\text{-}6)$$

Les coefficients c_4 et c_6 sont des polynômes « homogènes » de degré 2i de l'anneau $Z\ [b_2, b_4, b_6]$:

$$c_4 = b_2^2 - 24b_4\ ;\quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6\ \mathbf{;} \qquad (1\text{-}7)$$

D'autres transformations permettent d'obtenir d'autres modèles d'équations de Weierstrass :
Le modèle :

$$E_3 : y^2 = x^3 + Ax + B \in K[x, y] \qquad (1\text{-}8)$$

Le modèle de Legendre : $E_4 : y^2 = x(x-1)(x-a) \in K[x, y], a \neq 0,1$ (1-9)

Invariant

2-Invariants d'une cubique de Weierstrass :

Les cubiques possèdent plusieurs invariants, dont le discriminant, l'invariant modulaire, l'invariant différentiel,le conducteur,le régulateur,…

Définition 2 : *Le discriminant d'une cubique de Weierstrass :*

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \in K[X, Y]$$

est le polynôme « homogène » de degré 12 de l'anneau $ZI[b_2, b_4, b_6, b_8]$ *égal à*

$$\Delta(E) = 9b_2b_4b_6 - 8b_4^3 - 27b_6^2 - b_2^2b_8 \qquad (1)$$

sur un corps K de caractéristique $p \neq 2,3$

le coefficient b_8 *est déterminé par la relation :*

$$4b_8 = b_2b_6 - b_4^2 \ ;$$

$4b_8$ *est un polynôme de « degré 8 », de l'anneau ZI* $[b_2, b_4, b_6]$ *;*

Calcul de discriminants des modèles précédents :

1) Modèle : $E_3 : y^2 = x^3 + Ax + B \in K[x, y]$

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

2) Modèle de Legendre : $E_4 : y = x(x-1)(x-a) \in K[x, y], a \neq 0,1$

Résultat : $\Delta(E) = 16a^2(a-1)^2$

Exemple :

Calcul du discriminant de la famille des cubiques de Weierstrass à 2 paramètres a et N :

$$\text{E (a, N)} : y^2 + aNxy = x^3 + 2aN^2x^2 - N^2$$

J'obtiens les coefficients :

$$b_2 = (a^2+8a)N^2, \quad b_4 = 0, \quad b_6 = -4N^2, \quad b_8 = -(a^2+8a)N^4,$$

$$c_4 = (a^2+8a)^2N^4, \quad c_6 = [-(a^2+8a)^3N^4 + 2^5.3^3]N^2.$$

et le discriminant

$$\Delta(\text{E (a, N)}) = [(a^2+8a)^3N^4 - 3^3.2^4]N^4.$$

$\Delta(\text{E (a, N)}) = 0$ pour : 1) N=0, $a \in IR$

2) $N \neq 0$ et $(a^2+8a)^3N^4 - 3^3.2^4 = 0$, solutions $a^2+8a=3$ et $N = \pm 2$

soit $a = -4 \pm \sqrt{19}$

Pour N = 0 et a$\in IR$, $c_4 = 0$.
Pour N$\neq 0$ et a = $-4 \pm \sqrt{19}$, $c_4 \neq 0$.

Définition 3: *L'invariant modulaire d'une cubique de Weierstrass :*

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \in K[X,Y]$$

est l'élément j(E) du corps K égal à

$$j(E) = C_4^3 / \Delta(E)$$

Calculs d'invariants modulaires des modèles précédents :

1) Modèle $E_3 : y^2 = x^3 + Ax + B \in K[x, y]$;
J'obtiens les valeurs : $b_2 = 0$, $b_4 = 2A$, $b_6 = 4B$, $b_8 = -A^2$, $c_4(E_3) = -48A$.

et j (E_3) $= 1728(4A)^3 / (4A^3 + 27B^2)$

2) Modèle de Legendre : $E_4 : y^2 = x(x-1)(x-a) \in K[x, y], a \neq 0,1$;

J'obtiens les valeurs : $b_2 = -4(a+1)$, $b_4 = 2a$, $b_6 = 0$, $b_8 = -a^2$, $c_4(E_4) = -16(a+1)^2 - 48a$

et j (E_4) $= 2^8(a^2 - a + 1) / a^2(a-1)^2$

Exemple :
Famille des cubiques de Weierstrass à 2 paramètres a et N :

E (a, N) : $y^2 + aNxy = x^3 + 2aN^2x^2 - N^2$

Nous obtenons avec le calcul les coefficients : $b_2 = (a^2+8a)N^2$, $b_4 = 0$, $b_6 = -4N^2$,
$b_8 = -(a^2+8a)N^4$, $c_4 = (a^2+8a)^2N^4$; (4)

et le discriminant $\Delta(E(a, N)) = [(a^2+8a)^3N^4 - 3^3.2^4]N^4$

(1), (2) impliquent l'invariant modulaire :

$$j(E(a,N)) = \frac{N^8(a^2+8a)^6}{N^4(a^2+8a)^3 - 3^3 2^4}$$

Définition 4 **:** *L'invariant différentiel d'une cubique d'équation de Weierstrass :*

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

est l'élément différentiel :

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

Où

$f_x^{'} = 3x^2 + 2a_2x + a_4 - a_1y$ *et* $f_y^{'} = 2y + a_1x + a_3$ *sont les dérivées partielles du polynôme* $f(x, y)$.

Calculs d'invariants différentiels :

1) Modèle : $E_3 : y^2 = x^3 + Ax + B \in K[x, y]$

$$\omega(E) = \frac{dx}{2y} = \frac{-dy}{3x^2 + A}$$

2) Cubique d'équation de Weierstrass : E (a, N) : $y^2 + aNxy = x^3 + 2aN^2x^2 - N^2$

Avec le calcul j'obtiens l'invariant différentiel :

$$\omega(E(a, N)) = \frac{dx}{2y + aNx} = \frac{-dy}{3x^2 + 4aN^2x - aNy}$$

3-Points singuliers d'une courbe algébrique :

Dans la théorie des courbes planes, il y a des points ordinaires et des points singuliers sur ces courbes .

Définition 5 : *Un point P=(x, y) d'une courbe algébrique C d'équation f (x, y)=0 est singulier si ses coordonnées satisfont les équations :*

$f(P) = f_x^{'}(P) = f_y^{'}(P) = 0$.

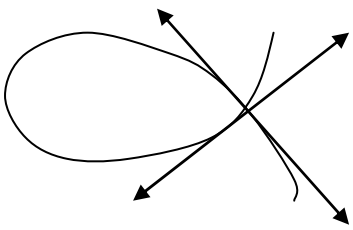
Le nombre de points singuliers des courbes algébriques irréductibles permet de les classifier en 2 classes :

Classe des courbes irréductibles non singulières et

Classe des courbes irréductibles singulières

Ces points singuliers d'une cubique irréductible sont des nœuds, ou des points de rebroussement.

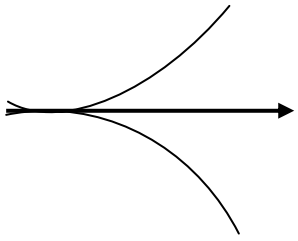
Figure 1



nœud

2 tangentes distinctes à la cubique

Figure 2



point de rebroussement

2 tangentes confondues

Les courbes algébriques admettent un invariant géométrique, qui est le genre de la courbe.

Définition 6 : *soit une courbe algébrique C d'équation f(x, y)=0 de degré n, qui possède s points singuliers , le genre de cette courbe est l'entier positif ou nul :*

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

Exemples :

1) une droite à une équation de degré n=1, son genre est égal à g=0.
2) les cercles et les coniques ont des équations de degré n=2, leur genre est égal à g=0
3) les cubiques singulières ont une équation de degré n=3, leur genre est égal à g=0
4) les cubiques non singulières ont une équation de degré n=3, leur genre est égal à g=1

4-Résultant de polynômes et classification des cubiques planes :

Les points singuliers d'une courbe algébrique C d'équation $y^2 = f(x)$ peuvent être étudiés avec le discriminant $dis(f)$ du polynôme $f(x) \in K[x]$.

Ce discriminant $dis(f)$ est lié au discriminant $\Delta(E)$ d'une cubique de Weierstrass :

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

D'après la théorie des courbes planes, le discriminant d'un polynôme $g(x) \in K[x]$ est un élément du corps K égal à la fonction symétrique des racines θ_i de $g(x)$:

$dis(g) = \prod_{i,j} (\theta_i - \theta_j)^2$ pour $g(x) = \prod_{1 \le i \le n} (x - \theta_i)$

et a $dis(g) = d_0^{2n-2} \prod_{i,j} (\theta_i - \theta_j)^2$ pour $g(x) = d_0 \prod_{1 \le i \le n} (x - \theta_i)$

Ces 2 formules impliquent que le discriminant $dis(g)$ est nul si et seulement si le polynôme g admet une racine multiple.

Exemples :

1) $g(x) = (x-1)(x-2)(x-3)$;

alors $dis(g) = (1\text{-}2)^2 (2\text{-}3)^2 (3\text{-}1)^2 = 4$

2) $g(x) = 3(x-3)(x-5)(x-8)$;

alors $dis(g) = [3]^{2(3)\text{-}2} (3\text{-}5)^2 (5\text{-}8)^2 (8\text{-}3)^2 = 2^2.3^6.5^2$

3) $g(x) = (x-5)^2(x-2)(x-10)$;

alors $dis(g) = (5\text{-}5)^2 (5\text{-}2)^2 (2\text{-}10)^2 (10\text{-}5)^2 = 0$

Définition 7: *(*selon *Kostrikin [8])*

Soient deux polynômes f et g de l'anneau IR[x] :

$f(x) = d_0 x^n + d_1 x^{n-1} + ... + d_n$, *de degré* $n \geq 1$.

et $g(x) = r_0 x^t + r_1 x^{t-1} + ... + r_t$, *de degré* $t \geq 1$.

Leur résultant est le déterminant d'ordre n+t égal à :

$$\mathrm{Res}(f,g) = \begin{vmatrix} d_0 & d_1 & K & K & d_n & 0 & K & K & K & 0 \\ 0 & d_0 & d_1 & K & K & d_n & 0 & K & K & 0 \\ 0 & 0 & d_0 & d_1 & K & K & d_n & 0 & K & K \\ K & K & K & K & K & K & K & K & K & 0 \\ 0 & K & K & 0 & d_0 & d_1 & K & K & K & d_n \\ r_0 & r_1 & K & K & K & r_t & 0 & K & K & 0 \\ 0 & r_0 & r_1 & K & K & K & r_t & 0 & K & 0 \\ K & K & K & K & K & K & K & K & K & K \\ K & 0 & r_0 & r_1 & K & K & K & K & r_t & 0 \\ 0 & K & 0 & r_0 & r_1 & K & K & K & K & r_t \end{vmatrix}$$

formé de t lignes $(d_0, d_1, ... d_n)$ *et n lignes* $(r_0, r_1, ... r_t)$, *les termes manquant sont remplacés par des zéros,*
la diagonale principale est formée de t termes d_0 *et n termes* r_t .

Indiquons quelques propriétés des résultants $\mathrm{Res}(f,g)$ sans démonstration :

Proposition 1 :

Soient deux polynômes :

$f(x) = d_0 \prod_{1 \leq i \leq n} (x - \theta_i)$, *de degré* $n \geq 1$ *et*

$g(x) = r_0 \prod_{1 \leq j \leq t} (x - \varphi_j)$, *de degré* $t \geq 1$

Leur résultant satisfait les relations :

$$\mathrm{Res}(f,g) = d_0^t \prod_{i=1}^{n} g(\theta_i)$$

$$= (-1)^{nt} r_0^n \prod_{j=1}^{t} f(\varphi_j)$$

$$= d_0^t r_0^n \prod_{i,j} (\theta_i - \varphi_j).$$

Preuve : Lang [9-1], et Kostrikin [8].
□
Ces formules admettent 2 corollaires

Corollaire 1 : *Le résultant Res (f, g) de deux polynômes f(x) et g(x) est nul si est seulement si les deux polynôme ont une racine commune.*

Preuve : Lang [9-1], et Kostrikin [8].
□

Corollaire 2 : *le résultant* $\mathrm{Res}(f, f')$ *d'un polynôme* $f(x)$ *et de sa dérivée* $f'(x)$ *est égal à :*

$$\mathrm{Res}(f, f') = d_0^{n-1} \prod_{i=1}^{n} f'(\theta_i).$$

Preuve : Lang [9-1], et Kostrikin [8].
□

Le discriminant $dis(f)$ d'un polynôme $f(x)$ et le résultant $\mathrm{Res}(f, f')$ sont liés par la :

Proposition 2 :

Le discriminant $dis(f)$ *d'un polynôme f(x) et le résultant* $\mathrm{Res}(f, f')$ *satisfont la relation :*

$$\mathrm{Res}(f, f') = (-1)^{\frac{n(n-1)}{2}} d_0 dis(f).$$

Preuve : Lang [9], et Kostrikin [8].
□

Déterminons les liens entre les discriminants $dis(f)$ **d'un polynôme** $f(x) \in K[x]$ **et** $\Delta(E)$ **d'une cubique de Weierstrass** $E : y^2 = f(x)$ **:**

Soit une cubique de Weierstrass :
$E : y^2 = x^3 + Ax + B = f(x).$
Avec le calcul nous obtenons les discriminants :

$$\Delta(E) = -16\,(4A^3 + 27B^2), \text{ et } dis(f) = -(4A^3 + 27B^2)$$

Cela implique la :

Proposition 3 :

Les discriminants $\Delta(E)$ *d'une cubique de Weierstrass* $E : y^2 = x^3 + Ax + B = f(x)$ *et* $dis(f)$ *sont liés par la relation :*

$$\Delta(E) = 16\ dis(f)$$

□
Pour une cubique de Weierstrass :

$$E : y^2 = d_0 x^3 + d_1 x^2 + d_2 x + d_3 = f(x) \in K[x]$$

les discriminants sont égaux à :

$$dis(f) = 18d_0d_1d_2d_3 + d_1^2d_2^2 - 4d_0d_2^3 - 4d_3d_1^3 - 27d_0^2d_3^2 = d_0^2\Delta(E).$$

Nous avons démontré la :

Proposition 4 :

Soit une cubique de Weierstrass :

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 = f(x) \in K[x]$$

Alors les discriminants $\Delta(E)$ *de E et* $dis(f)$ *de* f *satisfont la relation :*

$$dis(f) = 16\Delta(E)$$

□

Nous classifions les cubiques de Weierstrass E grâce aux discriminants $\Delta(E)$ de la courbe E et $dis(f)$ du polynôme f de l'équation de Weierstrass $f(x) = y^2$ de E

La proposition (2) et le corollaire (1) nous permettent de déterminer les cubiques singulières et les cubiques non singulières.

Si $\mathrm{Res}(f, f') = 0$,le polynôme $f(x)$ admet une racine multiple d'ordre 2 ou 3
Cela implique que la cubique est singulière.

Si $\mathrm{Res}(f, f') \neq 0$,le polynôme $f(x)$ admet 3 racines simples
Cela implique que la cubique est une courbe elliptique.

Les invariants $\Delta(E)$ et $c_4(E)$ des cubiques E de Weierstrass permettent de classifier l'ensemble des cubiques de Weierstrass en plusieurs classes selon les valeurs $\Delta(E) = 0$; $\Delta(E) > 0$; $\Delta(E) < 0$; $c_4(E) = 0; c_4(E) \neq 0$.

Proposition 5 :

Soit une cubique E de Weierstrass d'équation $y^2 = f(x)$ *, de discriminant* $\Delta(E)$.
Alors :

1-la cubique E est singulière si et seulement si $\Delta(E) = 0$.

2-la cubique E est une courbe elliptique si et seulement si $\Delta(E) \neq 0$.

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

Soit une cubique E d'équation $f(x) = y^2$ et discriminant $\Delta(E) = 0$;

La théorie du résultant et la relation entre $\Delta(E)$, $dis(f)$ impliquent la valeur

$dis(f) = 0$.

Cela implique que le polynôme f admet une racine multiple

Donc la cubique E est singulière.

2) Preuve de « E est singulière » implique « $\Delta(E) = 0$ ».

Par définition, une cubique singulière est une cubique E ayant un point singulier.
Donc ce point est multiple

.

D'après la théorie des discriminants des polynômes :

$dis(f) = 0$ si et seulement si f a une racine multiple (1)

(1) implique : la valeur $dis(f) = 0$ (2)

La relation $dis(f) = 16\Delta(E)$ et (3) impliquent la valeur $\Delta(E) = 0$

3) Preuve de « $\Delta(E) \neq 0$ » implique « la cubique E est une courbe elliptique » :

Soit une cubique de Weierstrass E d'équation $f(x) = y^2$ et discriminant $\Delta(E) \neq 0$

L'hypothèse $\Delta(E) \neq 0$ implique un résultant $\mathrm{Re}\,s(f, f') \neq 0$.

Il en résulte que le polynôme f admet 3 racines simples

Donc la cubique E est une courbe elliptique.

4) Preuve de « E est une courbe elliptique » implique « $\Delta(E) \neq 0$ » :

Nous prenons l'équation de Weierstrass de E :

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 = f(x)$$

L'hypothèse « E est une courbe elliptique » implique que le polynôme $f(x)$ admet

3 racines distinctes

Cela implique le résultant $\mathrm{Re}\,s(f, f') \neq 0$ (1)

(1) et la proposition (2) impliquent la valeur $dis(f) \neq 0$ (2)

La relation $dis(f) = 16\Delta(E)$ et (2) impliquent la valeur $\Delta(E) \neq 0$

□

Une cubique peut admettre 0 ou un point singulier.

La nature de ce point singulier est déterminée par la

Proposition 6 :

Soit une cubique de Weierstrass E d'équation :

$E: \ Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \in K[X,Y]$

de discriminant $\Delta(E)$ *et de coefficient* $c_4(E)$.

Alors :

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

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

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

Par définition un nœud est un point singulier ôu la cubique admet 2 tangentes distinctes (1)

Cela implique que la cubique est singulière (2)

La proposition (5) et la relation (1) impliquent la valeur $\Delta(E) = 0$

La pente d'une tangente à une courbe est égale à la dérivée y' de y.

Je prends une équation de Weierstrass de E de la forme :

$$E : y^2 = x^3 - 27c_4x - 54c_6 \quad (3)$$

Calcul de la dérivée y' de y :

$$y' = \frac{3x^2 - 27c_4}{2y} = \frac{3N(x)}{2y} \quad (4)$$

L'hypothèse de deux tangentes distinctes au nœud implique :

2 racines distinctes du polynôme $N(x) = x^2 - 9c_4$ (5)

Donc son discriminant n'est pas nul

$dis(N(x)) = 36c_4 \neq 0$ pour $Caract(K) \neq 2,3$ (6)

Cela implique la valeur $c_4(E) \neq 0$.

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

Par la proposition 4 l'hypothèse « $\Delta(E) = 0$ » implique que la cubique E est singulière ;
Soit S le point singulier de la cubique E
Alors la cubique E admet 2 tangentes distinctes ou confondues en ce point S

Les pentes de ces tangentes sont égales à la dérivées y' de y .

Je prends une équation de Weierstrass de E de la forme :

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 = f(x) \qquad (7)$$

Cubiques de Weierstrass singulières

Calcul de la dérivée y' de y :

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

Le discriminant du polynôme P(x) est égal à :

$$dis(P) = b_2^2 - 24b_4 = c_4(E).$$

L'hypothèse « $c_4(E) \neq 0$ » implique 2 tangentes distinctes.
Cela implique que la cubique E admet un nœud

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

L'hypothèse « E admet un point de rebroussement »implique que la cubique est singulière, donc son discriminant est nul :

$$\Delta(E) = 0 \qquad (8)$$

Je garde l'équation de Weierstrass (3) et la dérivée $y' = \frac{3N(x)}{2y}$.

Au point de rebroussement, la cubique admet deux tangents confondues;

Cela implique dis (N(x)) = 0.

D'après (6) dis (N(x)) = $36c_4 = 0$ pour Caract(K) $\neq 2, 3$

Il en résulte $c_4(E) = 0$

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

L'hypothèse « $\Delta(E) = 0$ » implique que la cubique E est singulière ;

Soit S le point singulier, la cubique E admet 2 tangentes distinctes ou confondues en ce point.

Je garde l'équation de Weierstrass (7) et la dérivée $y' = \frac{P(x)}{y}$.

Et $dis(P) = b_2^2 - 24b_4 = c_4(E)$

L'hypothèse « $c_4(E) = 0$ » implique une racine double, donc 2 tangentes confondues.

Il en résulte que la cubique E admet un point de rebroussement.

□

Etudions maintenant les cubiques de Weierstrass non singulières.

Proposition 7 :

Soit une cubique de Weierstrass E de discriminant $\Delta(E) \neq 0$.

1) la courbe elliptique E coupe l'axe Ox en trois points simples si et seulement si $\Delta(E) > 0$.
2) la courbe elliptique E coupe l'axe Ox en un seul point si et seulement si $\Delta(E) < 0$.

Cubique de Weierstrass non singulières

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

Je considère une courbe elliptique E qui coupe l'axe Ox en 3 points simples.
$P_i = (e_i , 0)$; $i = 1,2,3$; $e_i \neq e_j$ (1)

Elle admet une équation de Weierstrass de la forme :
$E : y^2 = (x - e_1)(x - e_2)(x - e_3) = f(x) \in R[x]$ (2)

Le discriminant du polynôme f(x) est égal à :
$dis(f) = \prod_{1 \le i \pi j \le 3} (e_i - e_j)^2$ (3)

Les 3 racines e_i sont des nombres réels, il en résulte que les carrés $(e_i - e_j)^2$ de nombres réels sont positifs et :
$dis(f) > 0$ (4)

La formule (4) et la relation entre les discriminants de f et de E impliquent la relation
$\Delta(E) > 0$ (5)

2) Preuve de « $\Delta(E) > 0$ » implique « la courbe elliptique E coupe l'axe Ox en 3 points distinctes »

Soit une courbe elliptique E d'équation de Weierstrass :

$$E : y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6 = f(x) \in IR[X] \quad (1)$$

La relation $dis(f) = 16\Delta(E)$ et l'hypothèse $\Delta(E) > 0$ impliquent $dis(f) \phi\ 0$ (2)
(1) et (2) impliquent que le polynôme $f(x)$ admet 3 racines simples e_1, e_2, e_3.

Il en résulte 3 points d'intersection $P_i = (e_i, 0)$ de la courbe E avec l'axe Ox.

3) Preuve de "une courbe elliptique coupe l'axe Ox en un seul point" implique " $\Delta(E) < 0$"
Je considère une courbe elliptique qui coupe l'axe Ox en un seul point P = (e,0).

Cela implique que les deux autres racines e_1 et e_2 du polynôme $f(x) = y^2$ sont conjuguées complexes.
$e_1 = r + is$, $e_2 = r - is$, r et s réels (6)

Le discriminant du polynôme f(x) est égal à
$dis(f) = [(e - e_1)(e - e_2)(e_1 - e_2)]^2$ (7)

Avec le calcul j'obtiens la valeur :

$dis(f) = -4s^2[(e-r)^2 + s^2)]^2$ (8)

Les carrés des nombres réels sont positifs. Il en résulte le signe du dis(f).

$dis(f) < 0$ (9)

La relation entre dis (f) et $\Delta(E)$ implique :

$\Delta(E) < 0$ (10)

4) Preuve de « $\Delta(E) < 0$ » implique «une courbe elliptique coupe l'axe Ox en un seul point »

Un polynôme cubique admet 3 racines e_i, simples ou multiples

$E : y^2 = 4(x-e_1)(x-e_2)(x-e_3) = f(x) \in IR[x]$ (1)

La relation $dis(f) = 16\Delta(E)$ et l'hypothèse $\Delta(E) < 0$ impliquent $dis(f)\ \pi\ 0$ (2)

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

$dis(f) = 4^4(e_1-e_2)^2(e_2-e_3)^2(e_3-e_1)^2 \in IR$ (3)

(2) et (3) impliquent un carré négatif

Cela implique une racine e_1 réelle et les deux autres racines e_2 et e_3 du polynôme $f(x)$ conjuguées complexes :

$e_2 = r + is$
$e_3 = r - is$ r et s réels

Alors $dis(f) = -4s^2[(e-r)^2 + s^2)]^2$

Il en résulte un seul point d'intersection $P_1=(e_1,0)$ de la courbe E avec l'axe O x.

□

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

Les propositions (5), (6) et (7) impliquent la classification des cubiques de Weierstrass

Proposition 8 :

Soient les cubiques de Weierstrass :

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

Elles sont classifiées en 4 classes par le discriminant $\Delta(E)$ et l'invariant $c_4(E)$

1) classe des cubiques singulières qui ont un nœud lorsque :

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

2) classe des cubiques singulières qui ont un point de rebroussement lorsque :

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

3) classe des courbes elliptiques qui coupent l'axe Ox en 3 points lorsque :

$\Delta(E) > 0$.

4) classe des courbes elliptiques qui coupent l'axe Ox en un seul point lorsque :
$\Delta(E) < 0$.

Illustrons cette classification par un exemple de chaque classe

1) cubique singulière qui admet un nœud

Soit la cubique E_1 de Weierstrass d'équation :

$$E_1 : y^2 = x^3 + 4x^2$$

Avec le calcul du discriminant $\Delta(E_1)$ et $c_4(E_1)$; j'obtiens les résultats :
$b_2 = 16$; $b_4 = 0$; $b_6 = 0$; $b_8 = 0$; $\Delta(E_1) = 0$; $c_4(E_1) = 16^2$.

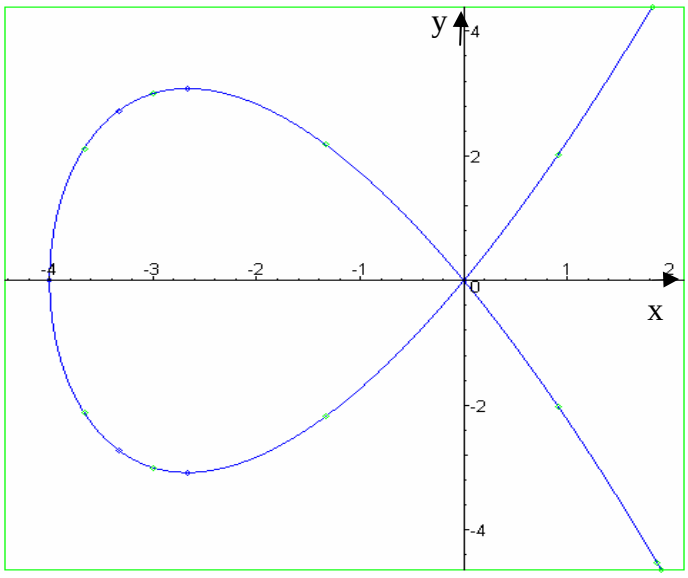
La valeur $\Delta(E_1) = 0$ implique que la cubique E_1 est singulière
La valeur $c_4(E_1) = 16^2 \neq 0$ implique que la cubique E_1 possède un nœud

Tableau des coordonnées de quelques points de E_1 :

x	-5	-4	-2	-1	0	1
y	Pas de solution réelle	0	$\pm 2\sqrt{2}$	$\pm\sqrt{3}$	0	$\pm\sqrt{5}$

La cubique E_1 coupe l'axe Ox en 1 seul point simple (-4,0) et un point double (0,0).
La cubique E_1 coupe l'axe Oy en un point (0,0).

Le tableau implique que la cubique E_1 admet un nœud au point (0, 0).



Courbe tracée avec le logiciel « Maple »

2) cubique de Weierstrass qui admet un point de rebroussement

Soit la cubique E_2 de Weierstrass d'équation :

$$E_2 : y^2 + 4y = x^3 - 4 \in IR[x]$$

Avec le calcul du discriminant j'obtiens les résultats :

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

La valeur $\Delta(E_2) = 0$ implique que la cubique E_2 est singulière

La valeur $c_4(E_2) = 0$ implique que le point singulier est un point de rebroussement.

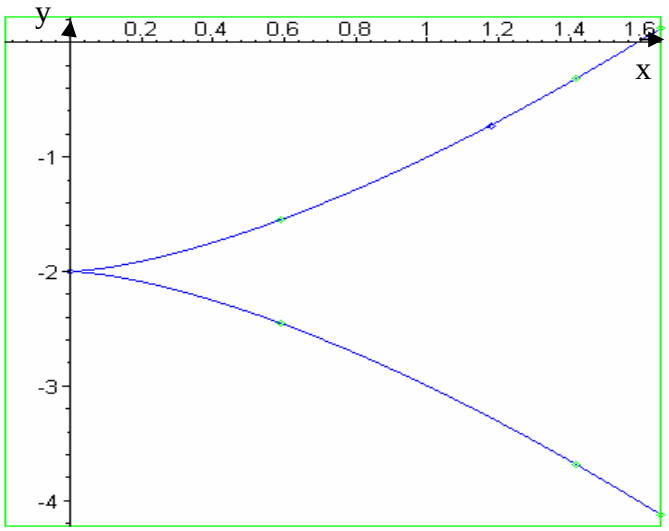
Tableau des coordonnées de quelques points de E_2 :

x	-1	0	1	1.5
y	Pas de solution réelle	-2	-3 et -1	$\frac{-4\sqrt{2} \pm 1}{2}$

La cubique E_2 coupe l'axe Ox en un point simple $(2^{(\frac{2}{3})}, 0)$.

La cubique E_1 coupe l'axe Oy en un point (0,-2).

Le tableau indique que la cubique E_2 admet un point de rebroussement au point (0, -2)



Courbe tracée avec le logiciel « Maple »

3) courbe elliptique qui coupe l'axe Ox en 3 points simples :

Soit la cubique E_3 de Weierstrass d'équation :

E_3 : $y^2 + 2xy - 3y = x^3 - 5x^2 + 2x + 8$

Avec le calcul j'obtiens les résultats :

$b_2 = -16$; $b_4 = -2$; $b_6 = 41$; $b_8 = -165$; $\Delta(E_3) = 8725$.

La valeur $\Delta(E_3) = 8725 > 0$ implique que la cubique E_3 est une courbe elliptique qui coupe l'axe Ox en 3 points simples.

Calcul des abscisses des points d'intersections de la cubique E_3 et l'axe Ox :

L'équation $f(x) = 0$ admet 3 racines :

$e_1 = -1$, $e_2 = 2$, $e_3 = 4$

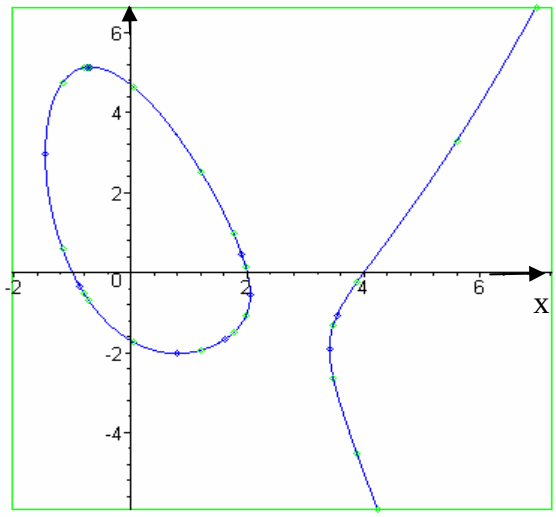
Il en résulte que la courbe elliptique E_3 coupe l'axe Ox aux 3 points :

$P_1 = (-1,0)$, $P_2 = (2,0)$ et $P_3 = (4,0)$.

La cubique E_3 coupe l'axe Oy en 2 points de coordonnées : $(0, \frac{3}{2} + \frac{\sqrt{41}}{2})$ et $(0, \frac{3}{2} - \frac{\sqrt{41}}{2})$

Tableau des coordonnées de quelques points de E_3 :

x	-2	-1	0	1	2	3	4
y	Pas de solution réelle	0 et 5	$\frac{3}{2} \pm \frac{\sqrt{41}}{2}$	-2 et 3	-1 et 0	Pas de solution réelle	-5 et 0



Courbe tracée avec le logiciel « Maple »

4) courbe elliptique qui coupe l'axe Ox en un seul point

Soit la cubique E_4 de Weierstrass d'équation :

$$E_4 : y^2 + 2xy - 3y = x^3 - x^2 + 17x + 87$$

Avec le calcul j'obtiens les résultats :

$b_2 = 0$; $b_4 = 28$; $b_6 = 357$; $b_8 = -196$; $\Delta(E_4) = -3616739$

La valeur $\Delta(E_4) = -3616739 < 0$ implique que la cubique E_4 est une courbe elliptique qui coupe l'axe Ox en un seul point.

Calcul des abscisses des points d'intersections de la cubique E_4 et l'axe Ox :

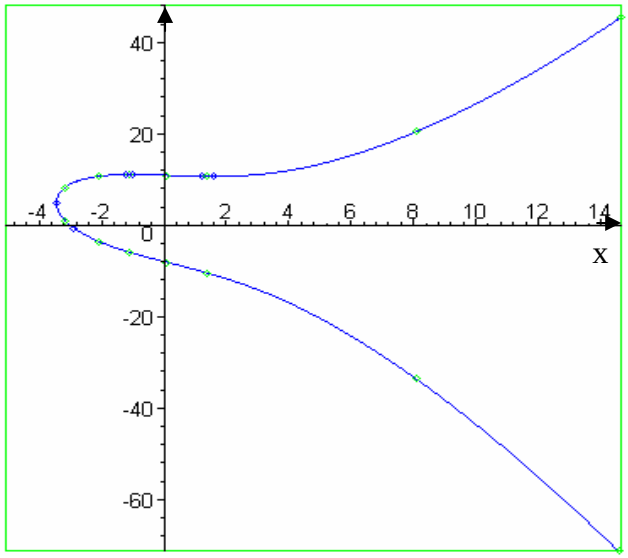
L'équation $f(x) = 0$ admet une racine simple e = -3.

Donc la courbe elliptique coupe l'axe Ox au point P = (-3,0)

La cubique E_4 coupe l'axe Oy en 2 points de coordonnées : $(0, \frac{3}{2} + \frac{\sqrt{357}}{2})$ et $(0, \frac{3}{2} - \frac{\sqrt{357}}{2})$

Tableau des coordonnées de quelques points de E_4 :

x	-4	-3	-1	0	2	4	5
y	Pas de solution réelle	0 et 9	$\frac{5}{1} \pm \frac{3\sqrt{33}}{2}$	$\frac{3}{2} \pm \frac{\sqrt{357}}{2}$	$\frac{-1}{2} \pm \frac{\sqrt{501}}{2}$	$\frac{-5}{2} \pm \frac{\sqrt{825}}{2}$	$\frac{-7}{2} \pm \frac{\sqrt{57}}{2}$



Courbe tracée avec le logiciel « Maple »

6) Application à la famille E (a, N) de cubiques de Weierstrass :

E (a, N) : $y^2 + aNxy = x^3 + 2aN^2x^2 - N^2 \in IR[x, y]$ (1)

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

Avec le calcul j'obtiens les résultats :

$b_2 = 9$; $b_4 = 0$; $b_6 = -4$; $b_8 = -9$; $\Delta(E(1,1)) = 3^3.11 \neq 0$

D'après la classification des cubiques de Weierstrass par leur discriminant
E (1,1) est une courbe elliptique qui coupe l'axe Ox en 3 points simples $p_i = (e_i, 0)$

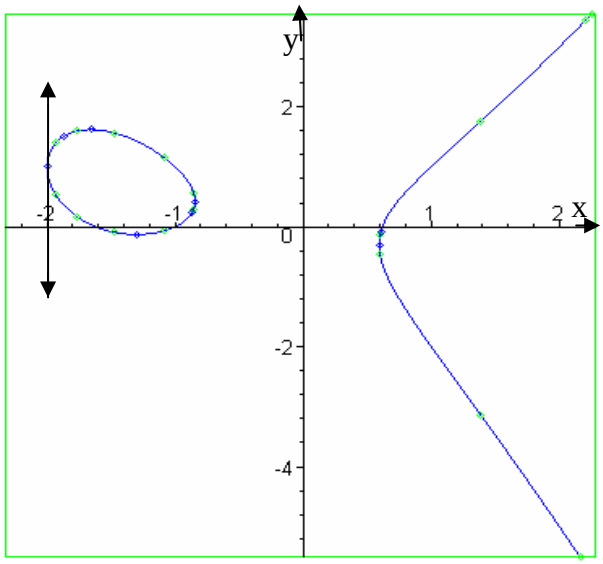
Avec le logiciel Maple j'obtiens les abscisses de ces points :

$e_1 = -1,\ e_2 = -\frac{1}{2} + \frac{\sqrt{5}}{2},\ e_3 = -\frac{1}{2} - \frac{\sqrt{5}}{2}$

Tableau des coordonnées de quelques points de E (1,1) :

x	-3	-2	-1	0 à 3/4	1	2
y	Pas de solution réelle	racine double $y = 1$	0 et 1	Pas de solution réelle	1 et -2	3 et -5

Au point s = (-2,1) la pente de la tangente à la cubique est égale à $y'(-2,1) = \infty$
Il en résulte une tangente parallèle à l'axe Oy.



2- Cubique E (-4,2) : $y^2 - 8xy = x^3 - 32x^2 - 4 \in IR[x, y]$

Avec le calcul j'obtiens les résultats :

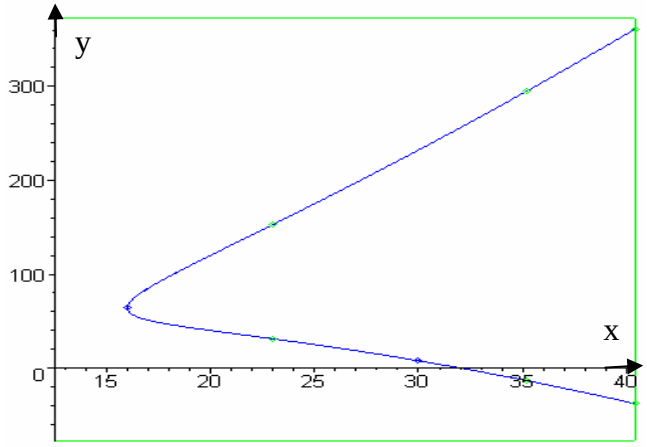
$b_2 = -64$; $b_4 = 0$; $b_6 = -16$; $b_8 = 256$; $\Delta(E(-4,2)) = -16^2(27 + 64^2)$ π 0

D'après la classification des cubiques de Weierstrass par leur discriminant
E (-4,2) est une courbe elliptique qui coupe l'axe Ox en un seul point simple $p = (e,0)$

Avec le logiciel Maple j'obtiens l'abscisse de ce point : $e \approx 31,9$

Tableau des coordonnées de quelques points de E (-4,2) :

x	1à16	18	20	e	35
y	Pas de solution	$72 \pm 2\sqrt{161}$	$80 \pm 2\sqrt{399}$	$140 \pm \sqrt{23271}$	$140 \pm \sqrt{23271}$



Courbe tracée avec le logiciel « Maple »

3-Cubique E (a, 0) d'équation de Weierstrass E : $y^2 = x^3 \in IR[x, y]$

Avec le calcul j'obtiens les résultats :
$b_2 = b_4 = b_6 = b_8 = 0$; $\Delta(E) = c_4(E) = 0$.

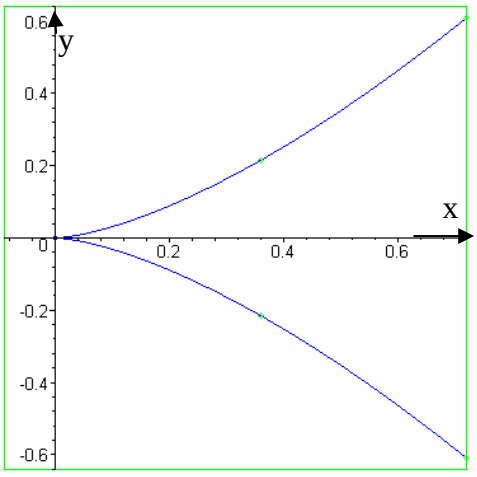
D'après la classification des cubiques de Weierstrass, cette cubique est singulière.

Pour x =0, $y^2 = 0$ l'équation admet une racine double $y = 0$, en ce point s = (0,0) la tangente à la cubique a une pente égale à la dérivée $y' = \frac{3x^2}{2y}$
Ce point (0,0) est un point de rebroussement de la cubique E

Pour $x \pi 0$, $y^2 \pi 0$; donc la cubique est dans le plan $x \geq 0$

Tableau des coordonnées de quelques points de la cubique :

x	-1	0	0.4	0.6	1	2
y	Pas de solution réelle	racine double $y = 0$	± 0.08	± 0.46	± 1	$\pm 2\sqrt{2}$



Courbe tracée avec le logiciel « Maple »

4) Cubique E(a,2) d'équation de Weierstrass :

$E : y^2 + 2axy = x^3 + 8ax^2 - 4 \in IR[x, y]$, $a = -4 - \sqrt{19}$

Avec le calcul j'obtiens les résultats :

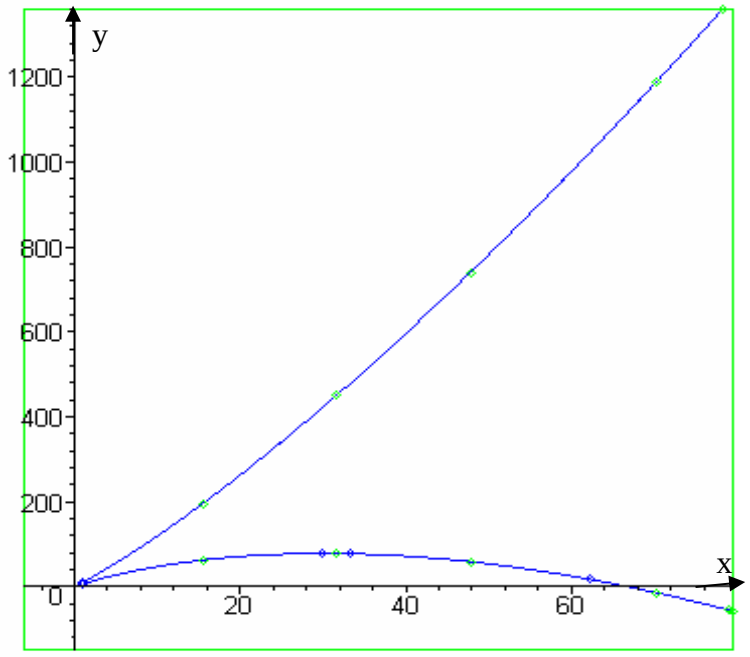
$b_2 = 12$; $b_4 = 0$ $b_6 = -16$; $b_8 = -48$; $\Delta(E) = 0; c_4(E) = 144$.

D'après la classification des cubiques de Weierstrass, cette cubique admet un nœud.

Tableau des coordonnées de quelques points de cette cubique :

x	0	1	2	3
y	Pas de solution réelle	racine double $y = 4 + \sqrt{19} = -a$	$8 + 2\sqrt{19} \pm 2\sqrt{2}$	$12 + 3\sqrt{19} \pm \sqrt{50}$

D'après ce tableau, S = (1,-a) est singulier



Courbe tracée avec le logiciel « Maple »

Chapitre 3 : GROUPE DE MORDELL-WEIL D'UNE COURBE ELLIPTIQUE

Il existe une loi de groupe abélien sur l'ensemble des points rationnels d'une courbe elliptique.
Nous allons étudier ce groupe

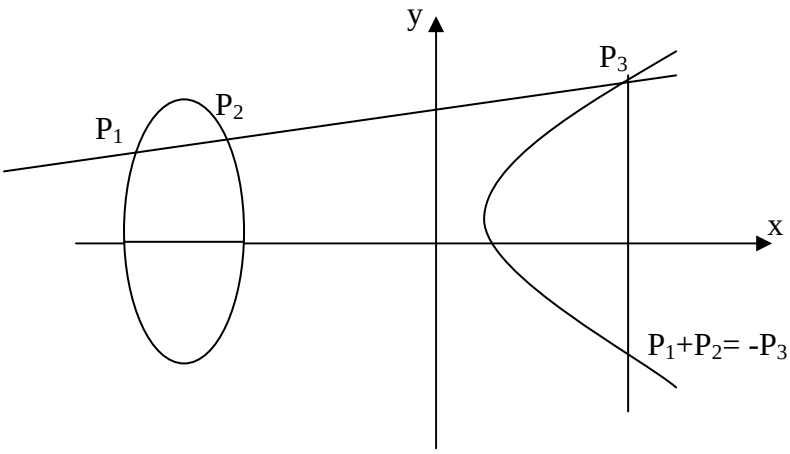
1-Structure de groupe abélien des cubiques de Weierstrass :

Proposition 1 :

L'ensemble E(K)des points K rationnels d'une cubique deWeierstrass, muni de l'application :

$$f : E(K) \times E(K) \to E(K) \text{ de valeur } f(P_1, P_2) = P_1 + P_2$$

est un groupe abélien d'élément neutre le point à l'infini $O_E = (\infty, \infty) = (0,1,0)$, et de loi basée sur la règle géométrique de 3 points colinéaires
$P_1 + P_2 + P_3 = O_E$ de la courbe.



Preuve :
Soit l'ensemble E (K) des points K rationnels de la courbe elliptique E
Considérons l'homomorphisme :

$$f : E(K) \times E(K) \to E(K) \text{ de valeur } f(P_1, P_2) = P_1 + P_2 \text{ et } f(O_E) = O_E$$

Le point $P_1 + P_2$ est déterminé par la règle géométrique :
« 3 points colinéaires d'une courbe elliptique E ont une somme nulle » :

$$P_1 + P_2 + P_3 = O_E \qquad (1)$$

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

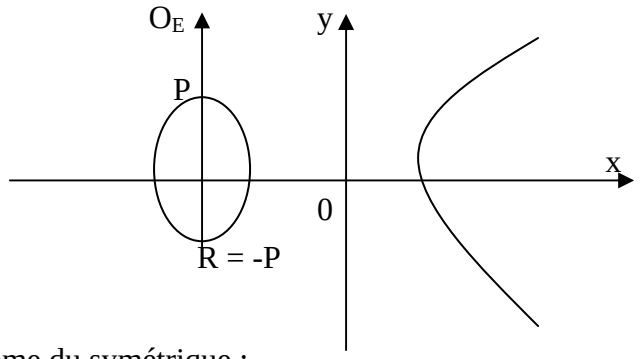
(1)-Axiome de l'élément neutre :

L'élément neutre est le point à l'infini O_E ; il est déterminé par la direction de l'axe Oy. la sécante PO_E est parallèle à l'axe Oy ;ce point O_E satisfait :

$$O_E + O_E = O_E$$

La règle des 3 points colinéaires implique la relation :

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



(2)-Axiome du symétrique :

La symétrique d'un point P est le point R, intersection de la parallèle à l'axe Oy passant par P et de la courbe

La relation : $P + R + O_E = O_E$ (3)

implique le symétrique : -P du point P

$$R = -P \qquad (4)$$

(3)-Axiome de commutativité :

Les sécantes P_1P_2 et P_2P_1 coupent la courbe E au même point P_3

Cela implique la relation de commutativité :

$$P_1 + P_2 = P_2 + P_1 = -P_3 \qquad (5)$$

(4)-Axiome d'associativité :

Il se vérifie par les calculs des coordonnées des points

$(P_1 + P_2)+P_3$ et $P_1+ (P_2+P_3)$, pour des points $P_i \neq \pm P_j$

□

Définition 1: *Le groupe E (K) des points K-rationnels d'une courbe elliptique E est le groupe de Mordell-Weil de la courbe elliptique E.*

2-Calcul des coordonnées du symétrique –P d'un point P et de la somme P_1+P_2 de 2 points $P_1 \neq \pm P_2$ et de la somme P+P=2P:

Soit une courbe elliptique E d'équation de Weierstrass :

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

(1) Calcul des coordonnées du symétrique –P d'un point P : (figure 1)

Le point –P satisfait la relation $P+(-P)=O_E$

Le point –P est le 2éme point d'intersection de la courbe E par la parallèle à Oy passant par P.
L'équation de cette parallèle est $x=x_p$

Cela implique que l'équation (6) est de degré 2 en y ; elle admet deux racines y_p et $y_{(-p)}$

La fonction symétrique élémentaire « somme des racines » d'une équation algébrique implique :

$$y_p + y_{(-p)} = -(a_1 x_p + a_3) \qquad (7)$$

Nous en déduisons la racine y_{-p} : $y_{(-p)} = -(a_1 x_p + a_3 + y_p)$

Rassemblons ces résultats dans la

Proposition 2 : *le symétrique d'un point $P=(x_p,y_p)$ d'une courbe elliptique E est le point -P de coordonnées $x(-P)=x_P$ et $y(-P)=-y_P-a_1x_P-a_3$*

□

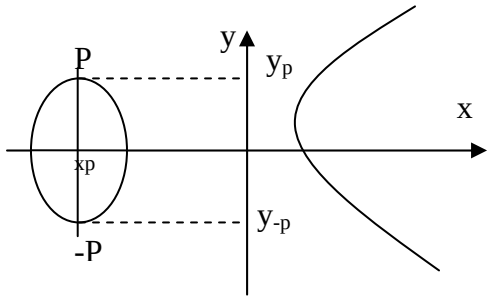


Figure 1

(2) Calcul des coordonnées de la somme P_1+P_2 de 2 points $P_1 \neq \pm P_2$: (figure 2)

La somme est déterminée par la règle géométrique :
$P_1+P_2+P_3=O_E$

Equation de la sécante P_1P_2 :

$$y = t(x-x_1)+y_1 \quad ; \quad \text{pente } t=\frac{(y_1-y_2)}{(x_1-x_2)} \text{ de la sécante } P_1P_2 \qquad (8)$$

La sécante P_1P_2 coupe la courbe en trois points P_1,P_2 et P_3
Avec (6) et (8) nous obtenons l'équation :

$$[t(x-x_1)+y_1]^2+(a_1x+a_3)[t(x-x_1)+y_1]=x^3+a_2x^2+a_4x+a_6 \qquad (9)$$

L'équation (9) est de degré 3 en x ; elle admet 3 racines :x_1,x_2 et x_3

Avec la fonction symétrique élémentaire « somme des racines » d'une équation algébrique nous obtenons : $x_1+ x_2 + x_3 = - (a_2 - t^2 - a_1 t)$

Cela implique l'abscisse x_3 du point P_3 : $x_3=t^2+a_1t-a_2-x_1-x_2$ (10)

Groupe de Mordell-Weil

Posons : $P_1+ P_2 = - P_3 = M$ = symétrique de P_3
La proposition 1 implique : deux points symétriques ont la même abscisse

$$x_M = x_{p_3}$$

L'ordonnée de M est égale à :

$$y_M = -y_3 - a_1 x_3 - a_3 = -[t(x_3 - x_1) + y_1] - a_1 x_3 - a_3 \qquad (11)$$

(10), (11) et (12) impliquent l'ordonnée de M

$$y_M = -t^3 - 2a_1 t^2 + t(a_2 + 2x_1 + x_2 - a_1^2) + a_1 a_2 - a_3 - y_1 + a_1(x_1 + x_2) \qquad (12)$$

Ces résultats sont rassemblés dans la

Proposition 3 :

Les coordonnées de la somme $M=P_1+P_2$ de 2 points $P_1 \neq \pm P_2$ d'une courbe elliptique E sont égales à :

$$x_M = t^2 + a_1 t - a_2 - x_1 - x_2 \ ; \ pour \ t = \frac{y_1 - y_2}{x_1 - x_2}$$

$$y_M = -t^3 - 2a_1 t^2 + t(a_2 + 2x_1 + x_2 - a_1^2) + a_1 a_2 - a_3 - y_1 + a_1(x_1 + x_2)$$

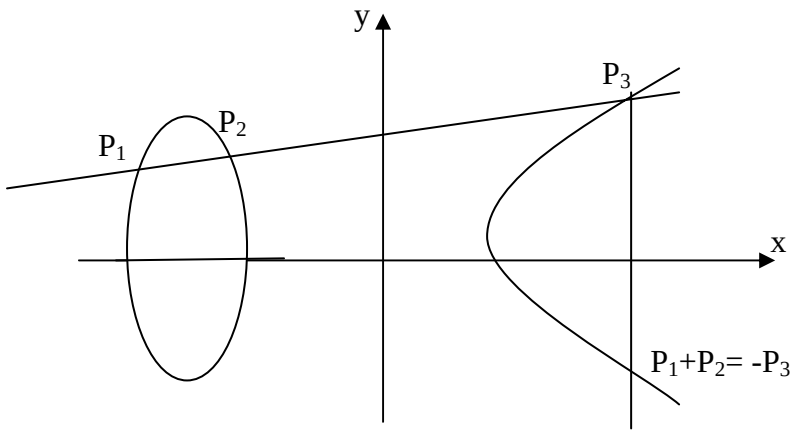


Figure 2

(3) Calcul des coordonnées de la somme P +P = 2P: (figure 3)

La tangente à la courbe E au point P à pour équation :

$$y = y'_p (x - x_p) + y_p \qquad (14)$$

La dérivée y' de y est égale à :

$$y' = \frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3} \qquad (15)$$

La règle géométrique des 3 points colinéaires implique :

P + P + T = O_E soit 2P = -T

Calcul des coordonnées du point T
(6) et (15) impliquent l'équation :

$$[y'_p(x - x_p) + y_p]^2 + [y'_p(x - x_p) + y_p](a_1x + a_3) = x^3 + a_2x^2 + a_4x + a_6 \qquad (16)$$

L'équation (16) en x de degré 3 admet 3 racines :
x_p racine double , x_T racine simple

La fonction symétrique élémentaire « somme des racines» d'une équation algébrique implique

$$2x_p + x_T = -\frac{a_2 - y'^2_p - a_1y'_p}{1}$$

Nous en déduisons l'abscisse x_T :

$$x_T = y'^2_p + a_1y'_p - a_2 - 2x_p$$

et l'ordonnées y_T

$$y_T = y'_p(x_T - x_p) + y_p$$

Les coordonnées du point 2P= -T sont égales à :

$$x_{2p} = x_T$$

$$y_{2p} = -y_T - a_1x_T - a_3$$

J'obtiens avec le calcul

$$x_{2p} = y'^2_p + a_1y'_p - a_2 - 2x_p$$

$$y_{2p} = -y'^3_p - 2a_1y'^2_p + (a_2 + 3x_p - a_1^2)y'_p + a_1a_2 - a_3 + 2a_1x_p - y_p$$

Ces résultats sont rassemblés dans la

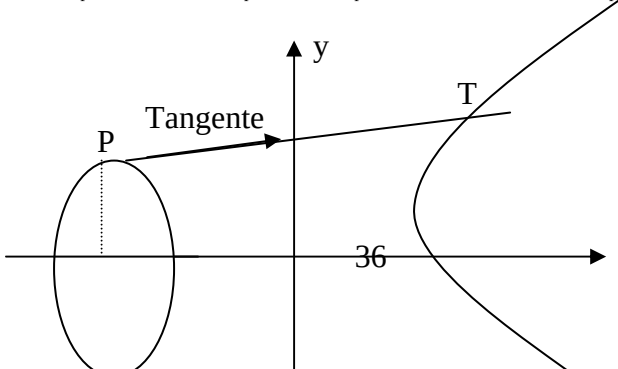
Proposition 4:

Les coordonnées de la somme P+P =2P d'une courbe elliptique E sont égales à :

$$x_{2p} = y'^2_p + a_1y'_p - a_2 - 2x_p \quad ; \textit{pour } y' = \frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3}$$

$$y_{2p} = -y'^3_p - 2a_1y'^2_p + (a_2 + 3x_p - a_1^2)y'_p + a_1a_2 - a_3 + 2a_1x_p - y_p$$

□



x

Figure 3

Application à la famille de cubiques de Weierstrass :

$$E(a,N): y^2 + aNxy = x^3 + 2aN^2x^2 - N^2$$

1) La symétrique d'un point $P = (x_P, y_P)$ est le point –P de coordonnées :

$$x(-P) = x_P$$
$$y(-P) = -y_P - aNx_P$$

2) La somme de 2 points $P_i = (x_i, y_i)$, $P_1 \neq P_2$ est le point $P_1 + P_2 = M = (x_M, y_M)$ de coordonnées :

$$x_M = t^2 + aNt - 2aN^2 - x_1 - x_2 \quad \text{pour } t = \frac{y_1 - y_2}{x_1 - x_2}$$
$$y_M = -t^3 - 2aNt^2 + t(2aN^2 + 2x_1 + x_2 - a^2N^2) + 2a^2N^3 - y_1 + aN(x_1 + x_2)$$

3) Pour tout point $P = (x_P, y_P)$ de la cubique E(a,N) le point $2P = (x_{2P}, y_{2P})$ à pour coordonnées :

$$x_{2P} = y_P'^2 + aNy_P' - 2aN^2 - 2x_P$$
$$y_{2P} = -y_P'^3 - 2aNy_P'^2 + (2aN^2 - a^2N^2 + 3x_P)y_P' + 2a^2N^3 + 2aNx_P - y_P$$

pour $\quad y' = \dfrac{3x^2 + 4aN^2x - aNy}{2y + aNx}$

4) Appliquons ces formules à la cubique E(1,1) de la famille E(a,N) :

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

Le point P = (1,1) est sur la courbe E(1,1)

Avec le calcul nous obtenons : le symétrique –P = (1,-2)

et le point 2P = (2,-5)

Le point R = (-1,0) est sur la courbe E(1,1)

Avec le calcul nous obtenons la somme : P + R = $\left(\dfrac{-5}{4}, \dfrac{11}{8}\right)$.

3-Points d'ordre fini d'une courbe elliptique et formules de Cassels:

Soit une courbe elliptique E d'équation de Weierstrass :

$$E:\ Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \in K[X,Y] \qquad (1)$$

Un point P du groupe de Mordell-Weil de la courbe E est d'ordre m s'il satisfait la relation :
$mP = O_E$;

Le symbole mP signifie :

mP = P + P +…+ P, m fois P lorsque m> 0 ;
mP = (-P) + (-P) +(-P) +…+ (-P) , (-m) fois -P lorsque m< 0 ;
et $mP = O_E$ lorsque m = 0 ;

Cassels a étudié les points mP sur une courbe elliptique particulière pour obtenir des formules utilisables.

Proposition 5:

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

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

Les coordonnées des points mP, pour m>2 et pour tout point P de E, sont déterminées par les formules :

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

avec $\psi_{-1} = -1,\ \psi_0 = 0\ ,\psi_1 = 1,\ \psi_2 = 2y\ ,\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$

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

Les polynômes ψ_m satisfont les relations :

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

Les polynômes ϕ_m et ω_m satisfont les relations :

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

Preuve :

Pour m = -1, le symétrique –P est égal à :-(x, y) = (x,-y) = $\left(\frac{x}{(-1)^2}, \frac{y}{(-1)^3} \right)$; donc $\psi_{-1} = -1$.

Sous groupes de torsion

Pour m = 0, 0(x, y) = $(\infty, \infty) = \left(\frac{x}{0}, \frac{y}{0} \right)$; donc $\psi_0 = 0$.

Pour m = 1, 1(x, y) =(x, y) = $\left(\frac{x}{1^2}, \frac{y}{1^3} \right)$; donc $\psi_2 = 1$.

Pour m= 2 : la formule $2P = (x_{2p}, y_{2p})$ est fonction de $y' = \frac{3x^2 + A}{2y}$ implique $\psi_2 = 2y$.

Un raisonnement par récurrence permet de démontrer cette proposition

C'est le lemme 7.2 de [Cassels]

Définition 1 : *1) un point de m-torsion d'une courbe elliptique E est un point P d'ordre m dans le groupe de Mordell- Weil de E.*

2) un sous groupe de m-torsion de E est l'ensemble E(K)[m] des points d'ordre m.

3) le groupe de torsion de la courbe E est la réunion infinie des sous groupes de m-torsion de E :

$$T(E) = \bigcup_m E[m] = \{P \in E(K) : mP = O_E \text{ pour m} \in \text{Z}\}$$

La détermination des groupes de torsion T(E)(K) dépend du corps de base K de la courbe elliptique.
Ce groupe est complètement déterminé sur le corps Q des nombres rationnels par 2 théorèmes :

Proposition 6 :

Soit une famille de courbes elliptiques E = E(A,B) d'équation de Weierstrass :

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

Alors tout point $P \in E(Q)$ *de torsion à des coordonnées entières :* $x_P, y_P \in ZI$

Lorsque $2P \neq O_E$, *alors* y_P^2 *divise* $4A^3 + 27B^2$.

Preuve :

C'est un théorème prouvé par [Lutz].

□

Proposition 7 :

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

ZI/nZI pour $1 \leq n \leq 10$ ou $n = 12$

$ZI/2ZI \times ZI/2dZI$ pour $1 \le d \le 4$

Preuve :

C'est une conjecture de Ogg prouvée par Mazur [10]

Exemple

Exemple :

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

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

1) Je choisis la courbe elliptique de la famille E(a,N) pour a = 0 et N = 1

$$E(0,1) : y^2 = x^3 - 1 \in IR[x, y] \qquad (1)$$

J'obtiens le discriminant

$$\Delta = -2^4 3^3 \neq 0 \qquad (2)$$

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

$$\begin{cases} x_{2P} = \dfrac{\phi_2}{\psi_2^2} = \dfrac{x^4 - 16x}{(2y)^2} \\ y_{2P} = \dfrac{\omega_2}{\psi_2^3} = \dfrac{x^6 - 20x^3 - 8}{(2y)^3} \end{cases} \qquad (3)$$

L'hypothèse « P est un point de 2-torsion » implique

$$2P = O_E = (\infty, \infty) \qquad (4)$$

Les relations (2), (3) et (4) impliquent la solution :

$$y = 0 \qquad (5)$$

Les formules (1) et (5) impliquent l'unique point P d'ordre deux du groupe E(0,1)(Q) :

P = (1,0)

Cela implique que le point P = (1,0) est le seul point de 2-torsion du groupe abélien E(0,1)(Q).

2) Je choisis la courbe elliptique de la famille E(a,N) pour a = 0 et N = 7

$$E(0,7) : y^2 = x^3 - 49 \in IR[x, y] \qquad (6)$$

J'obtiens le discriminant

$$\Delta = -2^4 3^3 7^4 \neq 0 \qquad (7)$$

Exemple

Je détermine les points d'ordre 3 avec les formules de Cassels :

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

le polynôme d'ordre 4 $\psi_3 = 3x^4 - 588x$ admet 4 racines :

$$x_1 = 0\,, \qquad x_2 = \sqrt[3]{196}\,, \qquad x_3 = -\frac{1}{2}\sqrt[3]{196}(1+\sqrt{-3})\,, \qquad x_4 = -\frac{1}{2}\sqrt[3]{196}(1-\sqrt{-3})$$

Ce sont des nombres du corps de nombres $K = \mathrm{Q}(\sqrt{-3}, \sqrt[3]{196})$ c'est un corps de nombres de degré 6.

Pour $x_1 = 0$, $y^2 = -49$ pas de solution réelle ;

Pour $x_2 = \sqrt[3]{196}$, $y^2 = 147$ admet 2 solutions : $y_1 = 7\sqrt{3}$, $y_2 = -7\sqrt{3}$

Pour $x_3 = -\frac{1}{2}\sqrt[3]{196}(1+\sqrt{-3})$ pas de solution réelle ;

Pour $x_3 = -\frac{1}{2}\sqrt[3]{196}(1-\sqrt{-3})$ pas de solution réelle ;

Cela implique que ces points n'appartienne pas au groupe de Mordell-Weill E(0,7)(Q).

Les points d'ordre 4 de la courbe elliptique E(0,7) ont pour coordonnées :

$$4P = (x_{4P}, y_{4P})$$

Les formules de Cassels impliquent les coordonnées des points mP pour $m \geq 2$

$$x_{4P} = \frac{\phi_4}{\psi_4^2} \; ; \quad y_{4P} = \frac{\omega_4}{\psi_4^3}$$

Un point d'ordre 4 pour la courbe elliptique E(0,7) est déterminé par le système :

$$\begin{cases} \psi_4 = 4y(x^6 - 980x^3 - 19208) = 0 \\ y^2 = x^3 - 49 \end{cases}$$

Ces deux polynômes admettent des solutions dans le corps $\underline{C}$ des nombres complexes.

Exemple

1) $y = 0$; $x^3 - 49 = 0$; admet 3 solutions :

$$x_1 = \sqrt[3]{14}\,, \quad x_2 = -\frac{1}{2}\sqrt[3]{14}(1+\sqrt{-3})\,, \quad x_2 = -\frac{1}{2}\sqrt[3]{14}(1-\sqrt{-3})$$

2) $y \neq 0$ et $f(x) = x^6 - 980x^3 - 19208 = 0$

Il en résulte deux solutions réelles :

$$x_1 = (490 + 294\sqrt{3})^{\frac{1}{3}}, \qquad x_2 = -(-490 + 294\sqrt{3})^{\frac{1}{3}}$$

Ces solutions appartiennent à l'extension $K = \mathrm{Q}(\sqrt[6]{3})$ du corps des rationnels Q.

Donc ces points n'appartiennent pas au groupe de Mordell-Weil E(0,7)(Q), ils appartiennent au groupe abélien E(0,1)(K).

Les groupe de torsion T(E)(Q) ont été déterminés pour des courbes elliptiques particulières.

Proposition 8 :

Soit une famille de courbes elliptiques E(p) d'équation de Weierstrass

$E(p): y^2 = x^3 + px \in Q[x]$

Alors le groupe de torsion T(E(p))(Q) est isomorphe à l'un des 3 groupes abéliens finis

$ZI/4ZI$ *si p=4 ;*

$ZI/2ZI \times ZI/2ZI$ *si –p est un carré parfait ;*

$ZI/2ZI$ *si* $p \neq 4$*, -p non carré et p sans facteur puissance 4 ;*

Preuve :

Détails dans (Silverman), proposition 6.1 et proposition 6.2

□

La réduction des courbes elliptiques fournit un autre moyen d'étude des sous groupes de m-torsion

Proposition 9 :

Soit une courbe elliptique E sur un corps K, qui admet une bonne réduction, un entier m premier à $caract(K)$ *et le sous groupe de m-torsion E(K)[m]*

Alors l'application réduction :

$$E(K)[m] \to \tilde{E}(k) \ , \quad \tilde{E} = \textit{courbe réduite}, \quad k = \textit{corps résiduel}$$
$$P \to \tilde{P}$$

est injective

Preuve :

On utilise les sous groupes $E_0(K) = \left\{P \in E(K);\ \tilde{P} \neq O_{\tilde{E}}\right\}$

$E_1(K) = \left\{P \in E(K);\ \tilde{P} = O_{\tilde{E}}\right\}$

et la suite exacte de groupes abéliens :

$$O \to E_1(K) \to E_0(K) \to \tilde{E}_{ns}(k) \to 0$$

$\tilde{E}_{ns}(k) =$ partie non singulière de la courbe réduite.

□

Exemple : Courbe elliptique E (3,5) de la famille E(a,N) :

$$E(3,5): y^2 + 15xy = x^3 + 150x^2 - 25$$

Calcul du discriminant :

$\Delta(E(3,5)) = 3^3 \times 5^4 (5^8 \times 11^3 - 16) \neq 0$

Exemple

D'après la théorie de la réduction des courbes elliptiques, la réduction modulo p est bonne pour tout nombre premier p qui ne divise pas le discriminant, soit pϕ 5 et p ne divise pas le nombre : A = $5^8 \times 11^3 - 16$

Donc sur le corps fini IF_7 la réduction est bonne :

$\tilde{E}(IF_7) : y^2 + xy = x^3 + 3x^2 + 3$

Appliquons la proposition pour $m \geq 1$; alors l'application

$E(Q)[m] \rightarrow \tilde{E}(Q_7)$ est injective

Avec le calcul j'obtiens :

le groupe $\tilde{E}(IF_7) = \{(1,0),(1,6),(5,0),(5,2),O_E\}$ de 5 points

Sur le corps fini IF_{11} la réduction est bonne :

$\tilde{E}(IF_{11}) : y^2 + 4xy = x^3 + 7x^2 + 8$

L'application $E(Q)[m] \rightarrow \tilde{E}(IF_{11})$ est injective pour $m \geq 1$

Avec le calcul j'obtiens :

le groupe $\tilde{E}(IF_{11}) = \{(1,1),(1,6),(2,0),(2,3)\}$ de 4 points

4-Isomorphismes des courbes elliptiques :

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

Soient deux courbes elliptiques d'équations de Weierstrass :

E : $y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6 \in K[x, y]$ (1)

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

Définition 4 : *un isomorphisme de 2 courbes elliptiques E et E' est un homomorphisme de groupes de Mordell-Weil :*

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

qui satisfait les formules d'isomorphisme de groupes :

$f(P+Q) = f(P) + f(Q)$; $f(O_E) = O_{E'}$ *pour les points à l'infini* O_E *et* $O_{E'}$;
et f *bijective*

Il y a un isomorphisme particulier précisé par la :

Proposition 10 :

Soit deux courbes elliptiques E et E' *et leurs groupes de Mordell-Weil* $E(K)$ *et* $E'(K)$.
Alors l'application f *: E (K)* $\to$ *E' (K) de valeur :*

$x = u^2X + r$, $y = u^3Y + u^2sX + t$, $u \neq 0$. $u,r,s,t \in K$

est un isomorphisme de courbes elliptiques.

Preuve :

Le calcul des images $f(P+Q)$, $f(P)$, $f(Q)$ implique la formule :

$f(P+Q) = f(P) + f(Q)$

La valeur $f(0_E) = (\infty, \infty) = 0_{E'}$ s'obtient avec le calcul

Pour vérifier que f est bijective, je calcule X et Y :

$X = (x-r)/u^2$; $Y = (y - u^2sX - t)/u^3$

La condition $u \neq 0$ implique que f est bijective

□

Cette proposition permet de trouver des relations entre les invariants des 2 courbes

Corollaire :

Soit les hypothèses de la proposition 10
Alors les coefficients a_i, b_{2i}, c_{2i} *de E et* a_i', b_{2i}', c_{2i}' *de E' satisfont les relations:*

Relations entre les coefficients a_i *et* a_i' *:*

$$
\begin{aligned}
&ua_1' = a_1 + 2s \ ; \\
&u^2 a_2' = a_2 - sa_1 + 3r - s^2 \ ; \\
&u^3 a_3' = a_3 + ra_1 + 2t \ ; \\
&u^4 a_4' = a_4 - sa_3 - rsa_1 + 2ra_2 - ta_1 + 3r^2 - 2ts \ ; \\
&u^6 a_6' = a_6 + ra_4 + r^2 a_2 - ta_3 - ta_1 + 3r^2 - 2ts \ ;
\end{aligned}
\qquad (17)
$$

Relations entre les coefficients b_{2i} *et* b_{2i}' *:*

$$
\begin{aligned}
&u^2 b_2' = b_2 + 12r \ ; \\
&u^4 b_4' = b_4 + 2b_2 + 6r^2 \ ; \\
&u^6 b_6' = b_6 + 2rb_4 + r^2 b_2 + 4r^3 \ ; \\
&u^8 b_8' = b_8 + 3rb_6 + 3r^2 b_4 + r^3 b_2 + 3r^4 \ ;
\end{aligned}
\qquad (18)
$$

Relations entre les coefficients c_{2i} *et* c_{2i}' *:*

$$u^4 c_4' = c_4 \ \text{et} \ u^6 c_6' = c_6 \qquad (19)$$

Relation entre les discriminants et les invariants modulaires

$$\Delta(E) = u^{12}\Delta(E') \quad \text{et} \quad j(E) = j(E') \qquad (20)$$

□

La relation $j(E) = j(E')$ / de la formule (20) implique

Proposition 11:

2 courbes elliptiques E et E' sont isomorphes si et seulement si leurs invariants modulaires sont égaux : $j(E) = j(E')$

1) Preuve de « E et E' isomorphes » implique « $j(E) = j(E')$ » :
Soit 2 courbes elliptiques E et E' isomorphes, alors la relation (20) entre les invariants modulaires de E et E' implique l'égalité :

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

2) Preuve de « $j(E) = j(E')$ »implique « E et E' isomorphes » :
L'invariant modulaire $j(E)$ d'une courbe elliptique E peut prendre 3 valeurs :

$j(E)$ =0, $j(E)$ =1728, $j(E)$ = e $\neq$ 0,1728 pour *carac* $K \neq 2,3$

Je choisis une équation de Weierstrass de la forme :

$E : y^2 = x^3 - 27c_4 x - 54c_6$ (21)

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

Isomorphismes de courbes elliptiques

1er cas : une courbe elliptique E d'invariant $j(E)$ =0

Cela implique : $c_4 = 0$ et $c_6 \neq 0$

L'équation (21) devient :

$$E : y^2 = x^3 - 54c_6 \quad (22)$$

La relation entre les invariants c_{2i} et c'_{2i} des 2 courbes elliptiques est :

$$u^6 c'_6 = c_6 \quad (23)$$

C'est une équation algébrique de degré 6 en u qui admet donc 6 racines dans une clôture algébrique K_{Alg} du corps K : $u = [c_6 / c'_6]^{\frac{1}{6}}$

Cela implique 6 isomorphismes :

$$E(K) \rightarrow E'(K) \quad \text{de valeur } f(x, y) = (u^2 x, u^3 y)$$

2er cas : une courbe elliptique E d'invariant $j(E)$ = 1728

Cela implique : $c_4 \neq 0$ et $c_6 = 0$

L'équation (21) devient :

$$E : y^2 = x^3 - 27c_4 x \quad (24)$$

La relation entre les invariants c_{2i} et c'_{2i} des 2 courbes elliptiques est :

$$u^4 c'_4 = c_4 \quad (25)$$

C'est une équation algébrique de degré 4 en u qui admet donc 4 racines dans une clôture algébrique K_{Alg} du corps K : $u = [c_4 / c'_4]^{\frac{1}{4}}$

Cela implique 4 isomorphismes :

$$E(K) \rightarrow E'(K) \quad \text{de valeur } f(x, y) = (u^2 x, u^3 y)$$

3er cas : une courbe elliptique E d'invariant $j(E)$ = e $\neq$ 0,1728

La formule de l'invariant modulaire implique la relation :

$$ec_6^2 = c_4^3 (e - 1728)$$

La relation entre les invariants c_{2i} et c'_{2i} des 2 courbes elliptiques :

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

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

Ce sont 2 équations algébriques en u de degré 4 et 6, Elles admettent des solutions dans une clôture algébrique K_{Alg} du corps K : $u = [c_4 / c'_4]^{\frac{1}{4}} = [c_6 / c'_6]^{\frac{1}{6}}$

Cela implique 24 isomorphismes :

$$E(K) \rightarrow E'(K) \quad \text{de valeur } f(x, y) = (u^2 x, u^3 y)$$

□

Il en résulte une classification des courbes elliptiques en classes de courbes de même invariant modulaire.

Isomorphismes de courbes elliptiques

Classe des courbes elliptiques d'invariant j(E)=0.
Classe des courbes elliptiques d'invariant j(E)=1728.
Classe des courbes elliptiques d'invariant j(E)= e $\neq$ 0,1728.

Exemple de courbes elliptiques isomorphes :

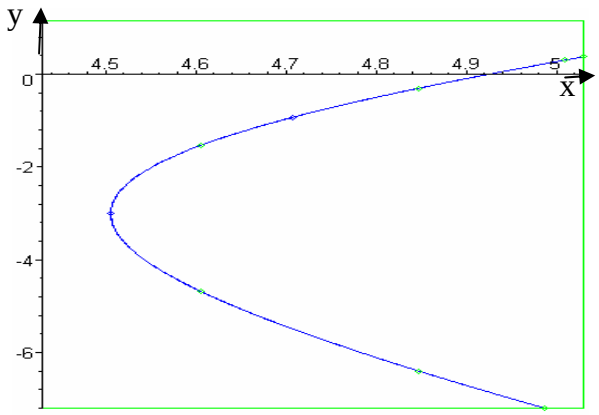
Soit une courbe elliptique E_1d'équation de Weierstrass :

$$E_1 : y^2 + 2xy - 3y = x^3 - 5x^2 + 2x - 8$$

Avec le calcul j'obtiens les valeurs :

$b_2 = -16$; $b_4 = -2$; $b_6 = -23$; $b_8 = 91$; $\Delta(E_1) = -42483 = -3.7^2.17^2 \neq 0$

Cette courbe elliptique coupe l'axe Ox en un seul point



Courbe tracée avec le logiciel « Maple »

Courbe elliptique isomorphe E_2 obtenue par le changement de variables :

x=4X+1, y = 8Y+4X

u=2 ; r = s = 1 ; t= 0 ;

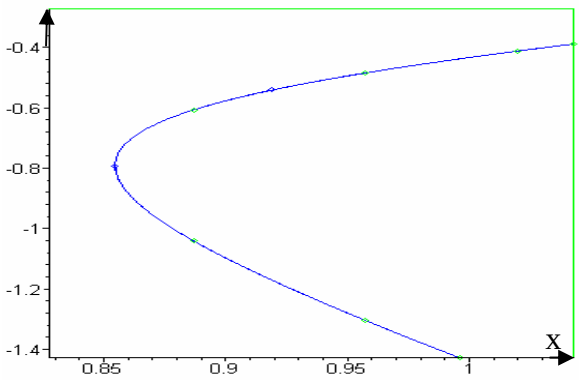
j'obtiens l'équation de Weierstrass de la courbe isomorphe :

$$E_2 : Y^2 + 2XY - \frac{1}{8}Y = X^3 - \frac{5}{4}X^2 - \frac{1}{4}X - \frac{1}{8}$$

Avec le calcul j'obtiens les invariants de la courbe isomorphe E_2 :

$$b_2 = -1,\ b_4 = -\frac{7}{4},\ b_6 = -\frac{39}{64},\ b_8 = \frac{3}{256} \text{ et } \Delta(E_2) = -\frac{3.7^2.17^2}{2^{12}}$$

y



Courbe tracée avec le logiciel « Maple »

5) Structure algébrique du groupe de Mordell-Weill E(K):

Selon (Lang -1), Poincaré a conjecturé que le groupe E(K) des points K –rationnels d'une courbe elliptique E est de type fini.

En 1922, Mordell a prouvé cette conjecture dans (Mordell)
En 1930, Weil a étendu cette propriété aux Variétés Abéliennes dans (Weil-1)

Cela explique que le groupe E(K) est le groupe de Mordell-Weil.

La preuve de la finitude du groupe E(K) est constituée de 2 parties selon ses auteurs : la preuve que le groupe quotient $E(K)/2E(K)$ est fini et la preuve que le groupe E (K) est de type fini

Proposition 12 :

Soit un corps de nombres K, une courbe elliptique E sur K et le groupe abélien E(K) Alors le groupe quotient $E(K)/2E(K)$ *est fini.*

Preuve :(selon Lang)
Soit une courbe elliptique d'équation de Weierstrass :

$$E : y^2 = (x-e_1)(x-e_2)(x-e_3) = h(x) \in K[x]$$

Alors les 3 points $P_i = (e_i, 0)$ sont d'ordre 2.

Considérons les 3 homomorphismes de groupes :

$f_i : E(K) \to K^* / K^{*2}$, i = 1,2,3 de noyaux

tels que $\prod_{1 \le i \le 3} \ker f_i \subset 2E(K)$

Prenons les valeurs :

$f_i(O_E) = 1$, $f_i(x,y) \equiv x - e_i \bmod K^{*2}$ si $x \neq e_i$

et $f_i(e_i,0) = (e_i - e_j)(e_i - e_k) \bmod K^{*2}$

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

Cette proposition est le théorème « faible » de Mordell-Weil
□

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

Descente infinie

Définition 5 : (selon Silverman / p 199)
Une hauteur sur un groupe abélien A est une fonction

$$h : A \to IR$$

qui satisfait les 3 conditions :

(h1) à un point P_1 de A on associe une constante $c_1(A,P_1) = c_1$ telle que :

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

(h2) à un entier $m \geq 2$ on associe une constante $c_2(A) = c_2$ telle que :

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

(h3) pour toute constante c_3 l'ensemble des points P de hauteur bornée est fini :

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

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

Proposition 13 :
Soit un groupe abélien A tel que le groupe quotient A/ mA est fini pour un certain entier $m \geq 2$ Alors le groupe abélien A est de type fini.

Preuve :
Soit un groupe abélien A, le groupe quotient A/mA fini et des représentants R_i, $1 \leq i \leq t$ des classes de ce groupe quotient. (1)

Prenons un point $P_0 \in A$ sous la forme de combinaison linéaire :

$$P_0 = mP_1 + R_{i_1} \ ; \ 1 \leq i_1 \leq t \qquad (2)$$

Construisons une suite infinie de points $P_2, P_3, ..., P_n$, par récurrence :

$$P_1 = mP_2 + R_{i_2} \;\; ; \;\; 1 \le i_2 \le t \qquad (3)$$

$$P_2 = mP_3 + R_{i_3} \;\; ; \;\; 1 \le i_3 \le t$$

M

$$P_j = mP_{j+1} + R_{i_{i+1}} \;\; ; \;\; 1 \le i_{j+1} \le t \qquad (4)$$

M

$$P_n = mP_{n+1} + R_{i_{n+1}} \;\; ; \;\; 1 \le i_{n+1} \le t \qquad (5)$$

Descente infinie

La relation (4) implique la combinaison linéaire :

$$mP_{j+1} = P_j - R_{i_{j+1}} \qquad (6)$$

L'axiome (h2) et la relation (6) impliquent l'inégalité :

$$h(mP_{j+1}) \ge m^2 h(P_{j+1}) - c_1 \qquad (7)$$

L'axiome (h1) implique l'inégalité :

$$h(P_j - R_{i_{j+1}}) \le 2h(P_j) + c_0 \qquad (8)$$

(6), (7) et (8) impliquent les inégalités :

$$m^2 h(P_{j+1}) - c_1 \le h(mP_{j+1}) \le 2h(P_j) + c_0 \qquad (9)$$

En posant $c' = c_0 + c_1$, nous obtenons l'inégalité :

$$h(P_{j+1}) \le \frac{2}{m^2} h(P_j) + \frac{c'}{m^2} \qquad (10)$$

Avec ces relations de récurrence, nous obtenons l'inégalité :

$$h(P_n) \le \left(\frac{2}{m^2}\right)^n h(P) + \left(\frac{1}{m^2} + \frac{2}{m^4} + \frac{4}{m^6} + ... + \frac{2^{n-1}}{m^{2n}}\right) c' \;\pi\; \left(\frac{2}{m^2}\right)^n h(P) + \frac{c'}{m^2 - 2} \qquad (11)$$

L'hypothèse $m \ge 2$ implique l'inégalité :

$h(P_n) \le 1 + c'/2$

(11) implique que les points P_j sont de hauteur bornée.

L'axiome (h3) implique que l'ensemble des points $P_1, P_2, \ldots, P_n$ est fini ;
soit $\{P_1, ..., P_r\}$ cet ensemble fini

Cela impliquent que ces points engendrent le groupe A/mA

Donc tout point P du groupe abélien A est combinaison linéaire des points R_i et $P_1,...,P_r$

$$P = n_1R_1 + ... + n_tR_t + n_{t+r}P_1 + ... + n_{t+r}P_r, \quad n_i \in ZI .$$

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

Le théorème s'applique à tout groupe abélien A tel que le groupe quotient A/mA soit fini. Donc il s'applique au groupe abélien de Mordell-Weil d'une courbe elliptique.

Groupe de Mordell-Weil

Proposition 14 :*(Théorème de Mordell-Weil)*

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

Preuve :
La condition de finitude du groupe quotient $E(K)/2E(K)$ est remplie grâce au « Théorème faible de Mordell-Weil »

Les points $R_1,...,R_t$ sont d'ordre fini, les points $P_1,...,P_r$ sont d'ordre infini.
□

Corollaire :

Le groupe de Mordell-Weil E(K) d'une courbe elliptique E est isomorphe à un produit de groupes abéliens :

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

$T(E(K)) =$ *groupe de torsion de la courbe elliptique E qui est fini*

$ZI^r = r$ *copies du groupe additif ZI infini*
□

Définition 6 : *L'entier* $r = r(E) \geq 0$ *est le rang de la courbe elliptique E , il est égal au nombre de générateurs de la partie infinie* $E(K)/T(E(K))$ *de la courbe elliptique.*

Cette structure du groupe de Mordell-Weil d'une courbe elliptique est de même type que la structure du groupe des unités d'un corps de nombres algébriques.

Théorème des unités *:(Dedekind)*

Soit un corps de nombres L de degré $[L : Q] = n = n_1 + 2n_2$ *, avec* n_1 *conjugués réels* $\sigma(L)$ *et* $2n_2$ *conjugués complexes* $\sigma_t(L) = \sigma_{t+n_2}(L)$.

L'ensemble $\Upsilon(L)$ *des unités du corps L est un groupe abélien isomorphe à un produit de 2 groupes abéliens :*

$$\Upsilon(L) \cong C(L) \times ZI^r$$

$C(L) =$ *groupe multiplicatif des racines de 1 contenues dans L*

$ZI^r = r$ *copies du groupe abélien ZI*

Alors toute unité u du corps L est de la forme :

$$u = \varepsilon\, u_1^{t_1} ... u_r^{t_r}\,, \varepsilon \in C(L)\,,\ \ u_1,...,u_r \text{ sont des unités linéairement indépendantes}$$

Définition 7 : *(1) les r unités $u_1,...,u_r$ forment un système d'unités fondamentales du corps L ;*
(2) l'entier r est le rang du groupe $\mathrm{Y}(L)$ des unités de L ;

Le rang $r(E) \geq 0$ d'une courbe elliptique n'est pas exprimé par une formule calculatoire,Ce rang r du groupe $\mathrm{Y}(L)$ des unités d'un corps de nombres L est déterminé par le :

Le rang des unités

Théorème : *(du rang des unités d'un corps L)*
Soit un corps de nombres algébriques L de degré $[L:Q] = n = n_1 + 2n_2$;alors le rang des unités de L est égal à :

$$r(\mathrm{Y}(L)) = r = n_1 + n_2 - 1$$

□

Exemples :

(1) Corps quadratique réel $L = Q(\sqrt{10})$; alors $n_1 = 2$ et $n_2 = 0$.
Donc $r(\mathrm{Y}(L)) = 2 + 0 - 1 = 1$
L contient une unité fondamentale.

(2) Corps quadratique imaginaire $L = Q(\sqrt{-19})$; alors $n_1 = 0$ et $n_2 = 1$.
Donc $r(\mathrm{Y}(L)) = 0 + 1 - 1 = 0$;
L ne possède pas d'unité fondamentale.

(3) Le 10^{eme} corps cyclotomique $L = Q(z)$:

Les corps cyclotomiques :

Définition 8: *le n^{eme} corps cyclotomique est l'extension algébrique $Q(z_n)$ du corps Q par une racine primitive n^{eme} de l'unité*

$$z_n = \exp\frac{2i\pi}{n} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

Théorème : *(structure du n^{eme} corps cyclotomique)*
Le n^{eme} corps cyclotomique $Q(z_n)$ est une extension abélienne du corps Q de degré $\varphi(n)$, φ = fonction arithmétique d'Euler.
Son groupe de Galois est isomorphe au groupe multiplicatif $(ZI/nZI)^{\times}$ des entiers rationnels premiers à n et inférieures à n.
Le n^{eme} corps cyclotomique est cyclique pour les puissances $n = p^r$, d'un nombre premier $p \phi\ 2$ et $r \geq 1$, et pour $n = 4$, il est abélien pour les autres valeurs n.

Exemple : le 5^{eme} corps cyclotomique et le 10^{eme} ont méme degré $\varphi(5) = \varphi(10) = 4$
Le 4^{eme} corps cyclotomique est le corps $Q(i)$; il est cyclique d'ordre $\varphi(4) = 2$

Les polynômes cyclotomiques :

Définition 9 : *le n^{eme} polynôme cyclotomique est égal à :*

$$f_n(X) = \prod (X - z), \quad z = \exp\frac{2\pi i}{n}k$$

z : racine primitive n^{eme} de l'unité , k premier à n

Exemples :

Le 2eme polynôme cyclotomique $f_2(X) = X + 1$

Le 3eme polynôme cyclotomique $f_3(X) = X^2 + X + 1$

Le 4eme polynôme cyclotomique $f_4(X) = X^2 + 1$

Théorème :

Le n^{eme} polynôme cyclotomique est égal à :

$$f_n(X) = (X^n - 1)\Big/\prod f_d(X), \quad \textit{pour tous les diviseurs de } d \ \pi \ n .$$

Exemples :

$f_{15}(X) = (X^{15} - 1)\big/ f_1 f_3 f_5$ et $f_1 = X - 1$

Pour les nombres premiers p $\varphi(p) = p - 1$ et $f_p(X) = X^{p-1} + X^{p-2} + ... + X + 1$

Théorie des extensions

Définition 10: *le n^{eme} corps cyclotomique $Q(z)$ est le corps de décomposition du n^{eme} polynôme cyclotomique*

$z_n = \exp\frac{2i\pi}{n}$ *est un élément primitif du corps* $Q(z)$.

Le 10^{eme} corps cyclotomique $L = Q(z)$, $z = \exp(2i\pi/10)$; est de degré $\varphi(10) = 4$

Le 10^{eme} polynôme cyclotomique : $f_{10}(X) = X^4 - X^3 + X^2 - X + 1$, alors $n_1 = 0$ et $n_2 = 2$

Donc $r = 1$; le corps L contient une unité fondamentale.

Revenons aux courbes elliptiques.

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

Décrivons quelques types de hauteurs

6) Hauteurs sur une courbe elliptique :

Définition 11 : *(1) la hauteur logarithmique sur une courbe elliptique E est la fonction :*

$$h_L : E(K) \to IR$$

de valeur $h_L(P) = \log(\max\{|N|, |D|\}, \ x(P) = N/D$

et $h_L(O_E) = 0$.

(2) la hauteur logarithmique relative à une fonction $f \in K(E)$ *est la fonction*

$$h_f : E(K) \to IR$$

de valeur $h_f(P) = h_L(f(P))$

Ces hauteurs satisfont les 3 axiomes d'une hauteur sur un groupe abélien.
Pour certains auteurs, cette hauteur logarithmique est la hauteur de Weil.

Hauteurs de Neron-Tate

Proposition 15 :

Soit une courbe elliptique E sur un corps K et une fonction paire $f \in K(E)$
Alors la hauteur logarithmique h_f *satisfait :*

$$h_f(R+S) + h_f(R-S) = 2h_f(R) + 2h_f(S)$$

pour tous points R et S du groupe E(K).

Preuve :
Dans (Silverman), Théorème 6-2
□

La hauteur h_L *de* Weil est utilisée pour construire un autre type de hauteur.

Définition 12 : *la hauteur de Neron-Tate sur une courbe elliptique E est la fonction :*

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

de valeur $\hat{h}(P) = \lim_{n\to\infty} 4^{-n} h_L(2^{-n}P)$,

où h_L *= hauteur logarithmique sur E(K).*

Pour certains auteurs, la hauteur $\hat{h}$ est la hauteur canonique sur le groupe E(K).
La hauteur de Néron-Tate posséde des propriétés précisées par la :

Proposition 16 :

Soit une courbe elliptique E et la hauteur canonique $\hat{h}$ *sur le groupe E(K)*
(1) $\hat{h}$ *satisfait la loi du parallélogramme :*

$$\hat{h}(R+S) + \hat{h}(R-S) = 2\hat{h}(R) + 2\hat{h}(S)\text{, pour tous points } R, S \in E(K)$$

(2) $\hat{h}(mP) = m^2\hat{h}(P)$ *pour tout* $m \in ZI$ *et pour tout point* $P \in E(K)$

(3) $\hat{h}$ *induit une forme quadratique sur E(K) :*

$$\langle .,. \rangle : E(K) \times E(K) \to IR$$

de valeur $\langle R, S \rangle = \hat{h}(R+S) - \hat{h}(R) - \hat{h}(S)$, *pour tous points* $R, S \in E(K)$
Cette forme quadratique est bilinéaire ;

(4) Pour toute point $P \neq O_E$, $\hat{h}(P) \phi\ 0$ et $\hat{h}(P) = 0$ *si et seulement si P est un point d'ordre fini.*

Preuve :
Dans (Silverman) Théorème 9-3

□

Cette forme bilinéaire quadratique de Néron-Tate est liée à l'invariant « régulateur » d'une courbe elliptique.

Hauteur locale

Définition 13 : *le régulateur d'une courbe elliptique E de rang* $r(E) = r$ *est égal au déterminant :*

$$R(E/K) = \det(\langle P_i, P_j \rangle),\ 1 \leq i, j \leq r \quad si\ r \phi\ 0$$

et $R(E/K) = 1$ si r = 0 *;*

$$\langle P_i, P_j \rangle = \hat{h}(P_i + P_j) - \hat{h}(P_i) - \hat{h}(P_j)$$

Examinons un autre type de hauteur sur une courbe elliptique

Définition 14 : *Soit une courbe elliptique E, et une valuation non triviale v du corps K. La hauteur locale en v de la courbe elliptique E est la fonction :*

$h_v : E(K_v) - \{O_E\} \to IR$, $K_v =$ *complété de K en v*

de valeur $h_v(P)$ *qui satisfait les relations :*

(1) $\lim_{P \to O_E} [h_v(P) + \frac{1}{2} v(x(P))]$ *existe*

(2) $h_v(2P) = 4h_v(P) + v(2y + a_1 x + a_3) - \frac{1}{4} v(\Delta(E))$

pour tout point $P(x, y) \in E(K)$, *et* $2P \neq O_E$ *;*

(3) $h_v(P + R) + h_v(P - R) = 2h_v(P) + 2h_v(R) + v(x_P - x_R) - \frac{1}{6} v(\Delta(E))$

Pour tous points P, R *et* $P \neq R \neq O_E$

Cette hauteur locale h_v en une valuation v est continue pour la topologie v-adique sur $E(K_v)$ et la topologie sur IR.

Silverman (théorème 18.3) distingue plusieurs valeurs $h_v(P)$ suivant la nature de la valuation v du corps K :
a) lorsque la valuation v est archimédienne, alors

$$h_v(P) = -\log[v[\Delta(L)^{1/12} . \exp(-\frac{z.\eta(z)}{2} . \sigma(z, L)]$$

L = réseau complexe dans le corps CI des nombres complexes

$\eta =$ fonction Eta de Dedekind : $CI \to IR$, $\eta(z) = q^{1/24}\prod_{n\geq 1}(1-q^n)$, $q = \exp(2\pi iz)$

$\sigma(z, L)$ = fonction Sigma de Weierstrass

b) lorsque la valuation v est non archimédienne, alors

$$h_v(P) = \max\left\{-\frac{1}{2}v(z),0\right\} + \frac{1}{12}v(\Delta(E)) \text{ , pour tout point } P = (x, y)$$

Cette théorie des hauteurs sur une courbe elliptique a fait l'objet de plusieurs recherches. Signalons quelques resultants:

(1) ZIMMER: « On the Difference of the Weil Height and the Neron-Tate Height » Math Z 147(1976)

(2) ANDERSON and MASSER: « Lorver Bounds for Heights an Elliptic Curves » Math Z 174(1980) 23-34;

(3) J.H.SILVERMAN: « The Difference between The Weil Height and The Canonical Height an Elliptic Curves » Math Comp 35(octobre 1990) 723-743
Classification AMS = 11 GOS, 11D25, 14K07;

(4) A.BREMNER and D.A.BUELL: « Three Points of Great Height an Elliptic Curve »;
Math .Comp.61 (juby 1993)-111-115;
AMS = 11GOS, 11-04, 14H52;

7) Rang de Courbes Elliptiques :

La définition du rang $r(E)$ d'une courbe elliptique E ne contient pas d'algorithme de calcul de cet invariant :

(1) Conjecture : il existe des courbes elliptiques E sur le corps Q des nombres rationnels de tout rang $r \geq 0$.

(2) Néron a trouvé une famille infinie de Courbes Elliptiques de rang $r \geq 11$dans « Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps » ; Bull.Soc. Math. France 80(1952) 101-166 ;

(3) Mestre a montré que la courbe elliptique :

$$E : y^2 - 246xy + 36599029y = x^3 - 89199x^2 - 19339780x - 36239244$$

a un rang $r(E) \geq 12$;
dans « Construction of an Elliptic Curve of rank ≥ 12 », CRAS-295-Paris(1982) 643-644.

(4) A.Brumer and K.Kramer ont étudié des rangs dans « The Rank of Elliptic Curve », Duke

Math. Journal 44(1977) 715-743

(5) Une autre procédure de calcul du rang est basée sur la série de Dirichlet-Hasse L(E, s) et la conjecture de Birch and Swnnerton-Dyer :

« La série L(E, s) d'une courbe elliptique E admet en s =1 un zéro d'ordre égal au rang de E(Q) ». Cette série est définie par le produit d'Euler :

$$L(E,s) = \prod_{p/\Delta(E)} (1-\varepsilon_p p^{-s})^{-1} \prod_{p/\Delta(E)} (1-t_p p^{-s} + p^{1-2s})^{-1}$$

Exemple $r(E) = r_{ana}$

où $t_p = 1 + p - A_p$ et A_p est le nombre de points de la courbe E modulo p et $\varepsilon_p = -1$ pour une réduction multiplicative et $\varepsilon_p = 0$ pour une réduction additive.

Définition 15 : *Cet entier r est le rang analytique de la courbe elliptique :* r_{ana}

Cette conjecture $r(E) = r_{ana}$ a été vérifiée dans de nombreux cas.
Elle n'est pas encore été démontrée.

(6) P.BUHLER, H.GROSS et Don B.ZAGIER ont utilisé la hauteur canonique et la série L(E, s) pour montrer que la Courbe Elliptique E d'équation de Weierstrass :

$$E : y^2 + y = x^3 - 7x + 6 \in Q[x, y]$$

a un rang analytique r_{ana} égal au rang $r(E)$: $r_{ana} = r(E) = 3$
dans « On The Conjecture of Birch and Swnnerton-Dyer for an Elliptic Curve of Rank 3 », Math.Comp.45(april (1985) 473-481
classification AMS = 14K07,14G10.

Selon ces auteurs, cette courbe elliptique est transformée par le changement de variable $y \to 2y + 1$ en :

$$E : y^2 = 4x^3 - 28x + 25.$$

Son discriminant vaut $\Delta(E) = 5077$

La hauteur utilisée à pour valeur :

$$\hat{h}(P) = \log b + \log|x| + \sum_{n\geq 0} 4^{-n-1} \log z_n = \log b + F(x)$$

$$z_n = 1 + \frac{14}{x_n^2} - \frac{50}{x_n^3} + \frac{49}{x_n^4}, \quad x_0 = x, \; x_{n+1} = \frac{x_n^4 + 14x_n^2 - 50x_n + 49}{4x_n^3 - 28x_n + 25}$$

Ce groupe E(Q) est engendré par les 3 points :

$$P_0 = (0;2) \; ; \quad P_1 = (1;0) \quad \text{et} \quad P_2 = (2;0)$$

La série de Dirichlet associée à la courbe elliptique a pour valeur :

$$L(E,s) = (1+5077^{-1})^{-1} \prod_{p\neq 5077} (1 - a_p\, p^{-s} + p^{1-2s})^{-1} = \sum_{n\geq 1} a_n n^{-s}$$

Les 3 auteurs obtiennent la valeur :

$$\lim_{s\to 1} \frac{L(E;s)}{(s-1)^3} = 1{,}731...$$

Ils en déduisent l'égalité $r(E) = r_{ana}(E)$.

□

Chapitre 4 : REDUCTIONS D'UNE COURBE ELLIPTIQUE

Les 5 coefficients $a_1,...,a_6$ d'une équation de Weierstrass d'une courbe elliptique E sont des éléments d'un corps commutatif K.
La réduction de ces coefficients s'obtient avec une valuation du corps K.
Commençons par un bref exposé de la théorie des valuations.

1-Valuations d'un corps de nombres :

La théorie des valuations d'un corps se trouve dans « Algebraic Numbers and Algebraic Functions », de Artin [1], chapitre 1 page 3-17 et dans d'autres ouvrages «Théorie des Nombres»: Lang [9-3], Iyanaga [6], Weiss [20],etc.…

Définition 1 : *une valuation d'un corps de nombres K est une fonction à valeurs réelles* $v : K \to /R_+$

qui satisfait les 3 axiomes :

(V 1) $v(x) \geq 0$ *pour tout élément* $x \in K$, *et* $v(x) = 0$ *si et seulement si* $x = 0$;

(V 2) $v(xy) = v(x)\, v(y)$ *pour tous éléments* $x, y \in K$;

(V 3) si $v(x) \leq 1$, *il existe une constante réelle* $c \geq 1$ *telle que :* $v(x+1) \leq c$;

L'axiome (v2) implique qu'une valuation v est un homomorphisme de groupes multiplicatifs.
L'axiome (v3) peut être remplacé par l'inégalité triangulaire :
$v(x+y) \leq v(x) + v(y)$ pour tous les éléments $x,y \in K$

Exemples :
1) la valuation triviale sur un corps K
$v : K \to /R_+$ de valeurs :
$v(0) = 0$ et $v(x) = 1$ pour $x \neq 0$.
Pour l'axiome (v 3) : $c = 1$

2) la valeur absolue ordinaire du corps /R
$v : /R \to / R_+$ de valeurs :
$v(x) = Max\{ x , -x \}$
Pour l'axiome (v3) : $c = 2$

3) la valuation p-adique du corps Q pour tout nombre premier p :

$v_p : \mathrm{Q} \to / R_+$ de valeur :

$v_p(\mathrm{p}) = \frac{1}{p}$ et $v_p(\mathrm{q}) = 1$ pour tout nombre premier $\mathrm{q} \in ZI$, différent de p

Alors la valuation d'un nombre rationnel $a = y\, p^n$ tel que y premier à p est égale à :

$v_p(\mathrm{a}) = \frac{1}{p^n}$.

Pour l'axiome (v 3) : $c = 1$

Classification des Valuations

Dans l'ensemble V(K) des valuations d'un corps K il existe une relation d'équivalence :

Définition 2 : *Deux valuation v_1 et $v_2 : K \to IR$ sont équivalentes si elles satisfont l'égalité : $v_2 = v_1^a$, pour un nombre $a \neq 0$.*

Il en résulte des classes de valuations équivalentes. Nous considérons que des valuations inéquivalentes dans la suite
Ces valuations inéquivalentes possèdent des propriétés

Proposition 1 :

Soient n valuations $v_1, ..., v_n$ non triviales et non équivalentes d'un corps K

Alors :

1) il existe un élément $x \in K$ tel que :

$v_1(x) \neq 1$ et $v_i(x) \neq 1$ *pour i = 2, 3,…, n.*

2) il existe un élément $x \in K$ et un nombre réel $c \neq 0$ tels que :

$v_1(1-x) < c$ et $v_i(x) < c$ *pour tout i = 2 , 3,…, n*

□

2-Classification des valuations :

Les valuations d'un corps K sont classifiées dans deux classes par la valeur de la constante c de l'axiome (v 3).

Définition 3 :

1) *une valuation v est archimédienne si l'inégalité : $v(x) \leq 1$ implique $v(x+1) \leq 2$*

2) une valuation v est non archimédienne si l'inégalité : $v(x) \leq 1$ implique $v(x+1) \leq 1$

Exemples :

1) la valuation triviale sur un corps K est non archimédienne.
2) Les valeurs absolues sur les corps *IR* et *CI* sont des valuations archimédiennes.
3) Les valuations archimédiennes du corps Q sont équivalentes à la valeur absolue $|x| = \max\{x, -x\}$, Théorème d'ostrowski
4) Les valuations non archimédiennes sont équivalentes aux valuations p-adiques
5) Toute valuation d'un corps K de caractéristique $p \neq 0$ est non archimédienne.

Les valuations non archimédiennes possèdent des propriétés

Proposition 2 :

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

1) $v(x) \neq v(y)$ implique $v(x+y) = Max\{v(x), v(y)\}$

2) soient n éléments $x_1, ..., x_n$ *du corps K de valuation :*

$v(x_1) \geq v(x_i)$ pour $i = 2, ..., n$

Alors v satisfait la relation : $v(x_1 + x_2 + ... + x_n) = v(x_1)$

□

Valuations additives

Proposition 3 :

Une valuation v d'un corps K est non archimédienne si et seulement si l'ensemble $\{v(n1)\ ; n = 1,2,3,...\}$ *est borné.*

□

L'image v(K) est un sous groupe du corps IR .
Pour certaines valuations, ce groupe est isomorphe à ZI.

Définition 4 : *une valuation non triviale* $v : K \to / R \cup \{\infty\}$ *est discrète lorsque son groupe de valuation v (K) est égal à* $v(K) = ZI \cup \{\infty\}$.

A toute valuation v non archimédienne discrète d'un corps K correspondent 4 sous ensembles du corps K :

L'anneau des v-entiers de K $= \{ a \in K ; v(a) \leq 1\} = A_v$

L'idéal maximal en $v = \{ a \in K ; v(a)\ \pi\ 1\} = M_v$

Le groupe de v-unités $= \{ a \in K ; v(a) = 1\} = U_v$

Le corps de classes résiduelles en v = k = A_v / M_v .

Toute valuation $v : K \to IR$ induit une topologie dans laquelle un système fondamental de voisinages d'un point a du corps K est l'ensemble : $Vois(a) = \{x \in K ; v(x-a)\ \pi\ \varepsilon\}$
pour une famille de nombres réels ε positifs

Il en résulte que les valuations équivalentes induisent la même topologie.
L'axiome (v 3) implique que cette topologie est de Hausdorff.

Définition 5 : *(1) une suite de Cauchy dans un corps K value par une valuation v est une suite d'éléments* $x_1, x_2, ..., x_n$ *de K telle que :*

$v(x_r - x_s)\ \pi\ \varepsilon$ *, pour un élément* $\varepsilon\ \phi\ 0$ *et des entiers* $r, s \geq N$ *, pour un certain entier N*

(2) un corps K où toute suite de Cauchy pour une valuation v converge est un corps complet pour v .

Pour plus de détails, consulter les ouvrages cités.

3-Valuations additives :

L'axiome (v 2) d'une valuation indique que la valuation est multiplicative

Soit une valuation non archimédienne discrète multiplicative

$v : K \to IR \cup \{\infty\}$

Nous associons à une valuation v une valuation additive ϕ par l'application logarithme.

Nous obtenons une valuation exponentielle

$\phi : K \to IR \cup \{\infty\}$ de valeur :

$\phi(x) = -Log|v(x)|$

Equation minimale

Une valuation exponentielle ϕ satisfait les axiomes :

(v1) $\phi(x)$ réel et $\phi(x) = +\infty$ si et seulement si x = 0

(v2) $\phi(xy) = \phi(x) + \phi(y)$ pour tous éléments x, y $\in K$

(v3) $\phi(x + y) \geq \min\{\phi(x), \phi(y)\}$ pour tous éléments x, y $\in K$

Cette valuation exponentielle ϕ détermine des sous ensembles du corps K :

Anneau des ϕ-entiers de K $= \{x \in K ; \phi(x) \geq 0\} = A_\phi$

Anneau maximal en $\phi = \{x \in K ; \phi(x)$ ϕ $0\} = M_\phi$

Le groupe des ϕ-unités $= \{x \in K ; \phi(x) = 0\} = U_\phi$

4-Equation de Weierstrass minimale

Toute valuation non archimédienne discrète réduit les invariants d'une courbe elliptique ; elle rend l'équation de Weierstrass minimale en v.

Définition 6 : *(selon Silverman)*

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

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

Cette équation est minimale en v si la valuation $v(\Delta(E))$ est minimale.

Critère de minimalité :

Une équation de Weierstrass minimale en v satisfait les conditions $v(a_i) \geq 0$ et $v(\Delta(E))$ π 12 ou les conditions $v(a_i) \geq 0$, $v(c_4(E))$ π 4 et $v(c_6(E))$ π 6.

Exemple :(1-2-Silverman)

Equation de Weierstrass :

$E : y^2 + xy + y = x^3 + x^2 + 22x - 9 \in Q_p[x, y]$ et corps p-adique Q_p (1)

Calcul du discriminant et de c_4

$\Delta(E) = -2^{15}.5^2$ et $c_4(E) = -5.211$

Le critère de minimalité précédent implique que l'équation (1) est minimale pour toute valuation p-adique v_p, $p \in ZI$

5-Réductions d'une courbe elliptique

Soit une valuation p-adique du corps Q:

$v_p : Q \to IF_P$ de valeur $v_p(a) = \bar{a} =$ classe de a modulo p

La réduction modulo p de la courbe elliptique E d'équation de Weierstrass :

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

implique une courbe réduite $\tilde{E}$

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

Cette courbe réduite est soit elliptique, soit singulière

Exemple :

Réduction de la courbe elliptique E d'équation de Weierstrass :

$E : y^2 + 3xy - 7y = x^3 - 5x^2 + 2x + 1 \in Q[x, y]$

La courbe réduite $\tilde{E}$ modulo v_2 a pour équation de Weierstrass :

$\tilde{E}_1 : y^2 + xy + y = x^3 + x^2 + 1 \in IF_2[x, y]$

son discriminant est égal à $\Delta(\tilde{E}_1) = 0$

donc la courbe réduite est singulière.

La courbe réduite $\tilde{E}$ modulo v_3 a pour équation :

$\tilde{E}_2 : y^2 + 2y = x^3 + x^2 + 2x + 1 \in IF_3[x, y]$

son discriminant est égal à $\Delta(\tilde{E}_2) = 0$

donc la courbe réduite est singulière.

La courbe réduite $\tilde{E}$ modulo v_7 a pour équation :

$\tilde{E}_2 : y^2 + 3xy = x^3 + 2x^2 + 2x + 1 \in IF_7[x, y]$

son discriminant est égal à $\Delta(\tilde{E}_3) = 0$

donc la courbe réduite est singulière.

Les courbes réduites sont classifiées par les invariants $\Delta(E)$ et $c_4(E)$ en trois types : bonne réduction et mauvaise réduction ; les mauvaises réductions sont multiplicative ou additive

Définition 7*: (selon Silverman)*

(1) une courbe elliptique E a une bonne réduction en une valuation v si la courbe réduite $\tilde{E}$ est une courbe elliptique ; alors la réduction est stable.

(2) la réduction est multiplicative si la courbe réduite a un nœud ; alors la réduction est semi stable.
(3) la réduction est additive si la courbe réduite a un point de rebroussement ; alors la réduction est instable.

Il y a un critère de reconnaissance pour la nature de la réduction d'une courbe elliptique.

Proposition 4 :

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

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

(1) E a bonne réduction en une valuation v si et seulement si $v(\Delta(E)) = 0$ *; alors* $\Delta(E)$ *est une v-unité et la courbe réduite* $\tilde{E}$ *est elliptique ;*

(2) E a une réduction multiplicative si et seulement si $v(\Delta(E)) \neq 0$ et $v(c_4(E)) = 0$ *; alors il y a un isomorphisme de groupes multiplicatif*

$$\tilde{E}_{ns}(K_{red}) \cong K^*_{red}\ ,\ K_{red} = \text{corps résiduel en v,}$$

(3) E a une réduction additive si et seulement si $v(\Delta(E)) \neq 0$ et $v(c_4(E)) \neq 0$ *; alors il y a un isomorphisme de groupes additifs*

$$\tilde{E}_{ns}(K_{red}) \cong K^+_{red}\ ,\ \tilde{E}_{ns} = \text{partie non singulière de } \tilde{E}\ .$$

Preuve :
Dans le cas d'une cubique de Weierstrass E singulière, la partie non singulière est $E_{ns} = E - \{\text{point singulier}\}$.
Lorsque la cubique a un nœud S, soit les tangentes à E en S : $y = t_i x + r_i$, i = 1,2 ;
L'application : $E_{ns} \to K^*$ de valeur

$$(x, y) \to \frac{y - t_1x - r_1}{y - t_2x - r_2}$$

est un isomorphisme de groupes abélien ;

Lorsque le point singulier S est un point de rebroussement, soit la tangente en S : $y = tx + r$;
L'application : $E_{ns} \to K^+$ de valeur

$$(x, y) \to \frac{x - x(S)}{y - tx - r}$$

est un isomorphisme de groupes abéliens

□

Exemple :
(1) Soit la courbe elliptique E d'équation de Weierstrass :

$$E : y^2 = x^3 + 2x^2 + 3x + 1 \in Q[x, y]$$

Calcul des invariants :
$b_2 = 8,\ b_4 = 6,\ b_6 = 4,\ b_8 = 1,\ \Delta(E) = -2^4.31,\ \ c_4(E) = 2^4.5$

La courbe elliptique E a une bonne réduction en tout nombre premier p qui ne divise pas $\Delta(E)$: v_p pour $p \neq 2$ et 31.

Pour p = 31, la valuation p-adique v prend les valeurs :
$v_{31}(\Delta(E)) \phi\ 0$ et $v_{31}(c_4(E)) = 0$;
C'est une réduction multiplicative en v_{31}

Pour p=2, la valuation p-adique v implique :
$v_2(\Delta(E)) \phi\ 0$ et $v_2(c_4(E)) \phi\ 0$;
C'est une réduction additive en v_2

2) Soit la courbe elliptique E(2.5) d'équation de Weierstrass :
$E(2.5) : y^2 + 10xy = x^3 + 100x^2 - 25$

Calcul des invariants :
$b_2 = 500,\ b_4 = 0,\ b_6 = -100,\ b_8 = -12500,\ \Delta(E) = 2^4.5^4.7^3.911 \quad c_4(E) = 2^4.5^6$

La courbe elliptique E a une bonne réduction en tout nombre premier p qui ne divise pas $\Delta(E)$: v_p pour $p \neq 2, 5, 7$ et 911.

Pour p = 7, 911 la valuation p-adique v prend les valeurs :
$v_p[\Delta(E(2,5))] \phi\ 0$ et $v_p(c_4(E(2,5))] = 0$;
C'est une réduction multiplicative en v_p (p =7,911).

Pour p=2, 5 la valuation p-adique v implique :
$v_p[\Delta(E(2.5))] \phi\ 0$ et $v_p[c_4(E(2,5))] \phi\ 0$;
C'est une réduction additive en v_p (p =2,5).

En conclusion, la famille E(a,N) de cubiques de Weierstrass est intéressante. Il reste beaucoup de recherche à faire sur cette famille : étude des conducteurs N(E(K)) étude des régulateurs, études des twists, des groupes de Selmer, des groupes de Shafarévich-tate, étude sur les corps finis, etc…
Ces recherches figurent dans mon programme prochain.

REFERENCES

[1] ARTIN: « Algebraic Number and Algebraic Functions » Gordon and Breach; sciences Publishers; New York; (1960).

[2] CASSELS: « Diophantine Equations with Special Reference to Elliptic Curves », Journal London Mathematical Society 41 (1966) 193-291.

[3] FULTON: « Algebraic Curves », Benjamin, New York (1969).

[4] HARTSHORNE: « Algebraic Geometry », GTM 52-Springer (1983).
Classification: 14 A 10 – 14 Fxx – 14Hxx – 14 Ixx.

[5] HUSEMOLLER: « Elliptic Curves » -G.T.M 111 (1987).

[6] IYANAGA: « The Theory of Numbers » North Holland Pub. Company-Amsterdam (1975).

[7] KOBLITZ: (1) « Introduction to Elliptic Curves and Modular Forms » 2eme édition Springer (1984) GTM 97.

[8] KOSTRIKIN: « Introduction à l'algèbre » Ed. Mir- Moscou- 2eme edition (1986).

[9] LANG: (1) « Algebra » 2eme édition, Addison Wesley Publishing Company, Inc, Reading, Massachusetts, New York (1984).
(2) « Elliptic Curves – Diophantine Analysis » Springer Verlag (1978) - Classification AMS = 10 B 45 – 10 F 99 -14 G 25 – 14 H 25.
(3) « Algebraic Number Theory », Addition – Wesley (1970).
(4) « Cyclotomic Fields », GTM 59 – Springer.

[10] MAZUR: (1) Modular curves and the Eisenstein ideal, IHES Publ. Math. 47. (1977), 33-186
(2) « Rational isogenies of prime degre » Invent. Math. 44 (1978), 129-162.

[11] NERON: « Quasi Fonctions et Hauteurs sur les Variétés Abéliennes », Annals of

Mathematics 82 (1965), 249-331.

[12] RUBIN: « Elliptic Curves with Complex Multiplication and the Conjecture of Birch and Swinnerton », – Dyer – Inv. Math. 64 (1981) 455 – 470.

[13] SERRE: (1) « Géométrie Algébrique et Géométrie Analytique », Ann. Inst. Fourier 6 (1956) – 1 – 42.
(2) « Propriétés galoisiennes des points d'ordre fini des courbes elliptiques », Inventions Mathématiques 15 (1972), 259-331.

[14] SHAFAREVICH: (1) « Basic Algebraic Geometry », Springer Verlag (1977).
(2) « Algebraic I», Moscou (1986)-Springer (1987).
Classification AMS = 12 – xx, 20 – xx.

[15] SHIMURA: « Introduction to the Arithmetic Theory of Automorphic Function », Princeton University Press (1971).

[16] SILVERMAN: (1) « The Arithmetic of Elliptic Curves », GTM 106 – Springer (1986).
Classification AMS = 1401, 14G 99, 14H 05, 14 K 15.
(2) « Lower Bound for the canonical height on Elliptic Curves », Duke Math. J .48 (1981). 633-648.
(3) « The Difference between the Weil Height and the Canonical Height on Elliptic Curves », Math. Comp. 35 (1990) 723-743.
Classification = 11G 05, 11 Y 50.

[17] TATE: « The Arithmetic of Elliptic Curves », Inv Math 23 (1974) 179-206.

[18] VELU: « Isogénies entre Courbes Elliptiques », C.R.A.S. Paris (1971) 238-241.

[19] WEIL : (1) « Sur un théorème de Mordell », Bull. Sci. Math. 54 (1930).
(2) « L'arithmétique sur les Courbes Elliptiques », Acta Math 52 (1928) 281-315.

[20] WEISS: « Algebraic Number Theory », Mc Graw – Hill. New York (1964).

[21] ZIMMER: « On the Difference of the Weil Height and the Neron-Tate Height. Math. Zeit 147 (1976) 35-51.

Résumé :

La famille E(a,N) de cubiques de Weierstrass qui est l'objet de ma thèse est paramétrée par 2 paramètres a et N. Son discriminant est un polynôme de degré 8 en N et de degré 4 en a :

$$\Delta(\text{E (a, N)}) = [(a^2+8a)^3N^4 - 3^3.2^4]N^4 = f(a,N)$$

Lorsque $f(a,N) \neq 0$, les cubiques sont des courbes elliptiques.

Lorsque $f(a,N) = 0$, les cubiques sont singulières.

Ces cubiques de Weierstrass ont une structure de groupe de Mordell-Weil de type fini. J'ai étudié les points P d'ordre finis : $mP = O_E$. J'ai appliqué la théorie des valuations p-adiques du corps Q des nombres rationnels pour obtenir la réduction de cette famille aux corps finis IF_p.