N°d'ordre : 20 /2010-M/MT

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE <<HOUARI BOUMEDIENE>>

Faculté de MATHEMATIQUES

MEMOIRE
Présenté pour l'obtention du diplôme de MAGISTER
EN : MATHEMATIQUES
Spécialité : Algèbre et Théorie Des Nombres
Par : DJELLAL Toufik
Sujet

SOUS GROUPES DE TORSION DE COURBES ELLIPTIQUES D'INVARIANT MODULAIRE j(E) DANS L'ANNEAU $\mathbb{Z}$

Soutenue publiquement le : 15/04/2010, devant le jury composé de:
M-AIDER Meziane, Professeur à l'USTHB. Président
M-ZITOUNI Mohamed, Professeur à l'USTHB. Directeur de mémoire
M-HERNANE Mohand Ouamar,Maître de conférences à l'USTHB Examteur
M-HACHAICHI Mohamed Salah,Maître de conférences à l'USTHB Examteur

Dédicaces

A mes 2 mères Kheira et Fatma
et
A mes frères et sœurs

REMERCIEMENTS AUX MEMBRES DU JURY

Je remercie le Professeur Meziane AIDER de m'avoir fait l'honneur de présider mon jury de thèse de

Magister.

Je remercie Monsieur Mohamed Salah HACHAICHI et Monsieur Mohand Ouamar HERNENE d'avoir bien

voulu accepter d'être les examinateurs de mon jury de thèse de Magister.

Et je remercie Monsieur Mohamed ZITOUNI, professeur à USTHB d'avoir dirigé ma thèse de magister avec compétence et sollicitude.

SOMMAIRE

INTRODUCTION:

Ma thèse de magister a pour objet l'étude des sous groupes de torsion de Courbes Elliptiques d'invariant modulaire $j(E)$ dans l'anneau $\mathbb{Z}$ des entiers rationnels.

Comme les Courbes Elliptiques ont une structure de Variété Algébrique Abélienne, j'ai consacré le *chapitre I* à des éléments de Géométrie Algébrique, d'après [4] , [12] . J'ai étudié les espaces affines $IA^n(K)$, les Variétés Algébriques Affines, les Variétés Projectives et les Variétés Abéliennes.

Dans le *chapitre II* , j'ai étudié les cubiques de Weierstrass: leurs équations spécifiques, leurs invariants discriminants $\Delta(E)$ et $c_4(E)$ qui permet de classifier les cubiques en 4 classes .2 pour les cubiques singulières et 2 pour les cubiques non singulières qui sont des Courbes Elliptiques.

Dans le *chapitre III* , j'ai étudié l'arithmétique des Courbes Elliptiques, d'après [14] qui est l'ouvrage de base [15] , [10] , [5] .

L'ensemble $E(\mathbb{Q})$ des points d'une Courbe Elliptique est muni d'une structure de groupe additif abélien d'élément neutre le point à l'infini $O_E = (\infty, \infty)$ et de loi basée sur la règle géométrique de 3 points colinéaires de la Courbe E.

Le groupe $E(K)$ de Mordell-Weil possède des sous groupes de torsion. Il y a des homomorphismes spécifiques de ce groupe.

Dans le *chapitre IV* , j'ai étudié l'action des valuations d'un corps sur les Courbes Elliptiques. C'est l'opération de réduction. A l'aide de la théorie des hauteurs sur un groupe abélien et de la descente infinie j'ai montré que le groupe de Mordell-Weil $E(\mathbb{Q})$ est de type fini.

Le *chapitre* se termine avec des notions sur les Formes Modulaires et sur la série $L(E, s)$ de Dirichlet-Hasse d'une Courbe Elliptique.

CHAPITRE I

Variétés Algébriques

Introduction:

Les Courbes Elliptiques ont une structure de Variété Algébrique Abélienne de dimension un, c'est pourquoi dans ce chapitre nous exposons des éléments de la théorie des espaces Affines, des espaces projectifs et des Variétés Abéliennes. Ces notions sont puisées dans les ouvrages de Géométrie Algébrique: [3], [10].

Dans la suite nous utiliserons les symboles usuels de Théorie des Nombres.

$\mathbb{N}$ = monoïde des nombres entiers naturels 0, 1, 2, ...

$\mathbb{Z}$ = anneau des nombres entiers rationnels 0, ± 1, $\pm 2, ...$

$\mathbb{Q}$ = corps des nombres rationnels.

$\mathbb{R}$ = corps des nombres réels.

$\mathbb{C}$ = corps des nombres complexes.

K = corps commutatif, global, local ou fini.

$IA^n(K)$ = espace Affine de dimension $n \geq 1$ sur un corps K.

$IP^n(K)$ = espace projectif.

1− **Espaces Algébriques Affines $IA^n(K)$:**

Définition 1: un $n-$ espace Affine sur un corps commutatif K, Algébriquement clos, est l'ensemble special X des $n-$ uples d'éléments a_i de K : $/A^n(K) = \{a = a_1, \ldots, a_n,\ a_i \in K\}$.

Le système a est un point de l'espace Affine ; ses coordonnées sont dans le corps K.

A cet espace Affine on associe l'anneau $K[x_1, \ldots, x_n] = B$ des polynômes à n variables par l'application: $f : /A^n(K) \to B$ de valeur $f\ (a) = f\ (a_1, \ldots, a_n)$.

$(a_1, a_2, \ldots, a_n) = a \to f\ (a), f \in B$.

A toute famille $(f_1, f_2, \ldots, f_t)$ de polynômes de l'anneau B, on associe l'ensemble $A(f_1, f_2 \ldots, f_t)$ des zéros de ces polynômes dans une clôture Algébrique du corps K.

Cet espace Affine $/A^n(K)$ peut être muni d'une topologie spéciale: la topologie de *ZARISKI,* qui sera définie plus loin.

La théorie Algébrique des polynômes d'un anneau $K[x_1, \ldots, x_n]$ implique que tout polynôme f admet des zéros dans une clôture Algébrique du corps K.

Proposition 1:

1) **La réunion de deux ensembles Algébriques dans un espace Affine est un ensemble Algébrique.**

2) **L'intersection d'une famille d'ensembles Algébriques est un ensemble Algébrique.**

3) **L'ensemble vide et l'espace Affine $/A^n$ sont des ensembles Algébriques.**

Preuve:

1) soient 2 ensembles Algébriques $X_1 = A(f_i)$ et $X_2 = A(g_j)$ dans l'espace Affine $IA^n(K)$.

Alors leur réunion $X_1 \cup X_2 = A(f_i, g_j)$ est l'ensemble des zéros des polynômes f et g; cet ensemble est donc Algébrique.

2) l'intersection $X_1 \cap X_2 = A(f,g) \in X_i$ pour $i = 1,2$ est l'ensemble des zéros communs des polynômes f et g.

3) Pour le polynôme constant $f = 1$, l'ensemble Algébrique $x = A(1)$ est l'ensemble vide. Pour le polynôme identiquement nul, l'ensemble Algébrique $x = A(0)$ est l'espace Affine lui-même.

□

Corollaire:

Soit une famille $(f_i)_{1 \leq i \leq n}$ de polynômes de l'anneau B. Alors l'ensemble Algébrique $X = A(f_i)$ des zéros de cette famille de polynômes est égal à l'ensemble des zéros des polynômes de l'idéal $I(f_i)$ engendré par ces polynômes.

Preuve:

Tout polynôme de l'idéal $I(f_i)$ est une combinaison linéaire: $g = c_1 f_1 + c_2 f_2 + ... + c_t f_t$.

Donc tout zéro des polynômes f_i est un zéro du polynôme g.

□

Ces ensembles Algébriques permettent de définir une topologie particulière: la topologie de *Zariski.*

Définition 2: un ensemble Algébrique est une partie d'un espace Affine $IA^n(K)$ formée des zéros d'une famille de polynômes $\{f_1, \ldots, f_d, d \geq 1\}$ de l'anneau $K[x_1, \ldots, x_n]$.

Définition 3: la topologie de Zariski sur un espace Affine $/A^n(K)$ est constituée par les ensembles Algébriques comme des fermés et leurs complémentaires comme des ouverts.

Alors on peut vérifier que ces ouverts et ces fermés satisfont les axiomes d'une topologie.

L'ensemble vide et l'espace Affine sont à la fois des ouverts et des fermés, ce sont les seules parties à posséder cette propriété.

Exemples:

$X = \{t$, et $y = \sqrt{t^{\,2} - 1}\}$ pour $t \in \mathbb{C}$.

X est un sous ensemble Algébrique dans l'espace Affine $/A^2(\mathbb{C})$.

Un espace Affine $/A^n(K)$ peut être muni d'une topologie.

Il existe 2 types de sous ensembles dans un espace topologique muni de la topologie des ensembles partiels de Zariski.

Définition 4: un sous-ensemble Y d'un espace topologique X est irréductible s'il n'est pas la réunion de deux sous ensembles fermés non vides disjoints. Il en résulte qu'un sous ensemble réductible est la réunion de composantes irréductibles.

Exemple: l'ensemble vide n'est pas irréductible;

Le sous ensemble $Y = Z(x^4 + x + 1)$ de l'espace Affine $/A^1(\mathbb{Q})$ est irréductible; il admet 4 composantes irréductibles correspondants à la factorisation du polynôme: $x^4 + x + 1$.

2−**Variétés Algébriques Affines:**

Définition 5:1/ une Variété Algébrique Affine est un sous espace irréductible et fermé d'un espace Affine $/A^n(K)$ muni de la topologie de Zariski.

2/ **Une Variété quasi Affine est un ensemble ouvert d'une Variété Affine.**

Exemples de Variétés Affines:

Soit l'espace Affine $/A^3(K)$ sur un corps Algébriquement clos K:

Soit la partie D de cet espace Affine:

$D = \{(x, y, z), y - x^{\,2} = 0, z - x^{\,3} = 0\}$ est formée des zéros.

$X = t \in K, y = t^{\,2} \in K$ et $z = t^{\,3} \in K$.

Donc D est un ensemble Algébrique, c'est une Variété Affine avec la topologie de *Zariski*.

3−**Variétés Projectives $IP^{\,n}(K)$:**

A partir d'un espace Affine$/A^{n+1}(K)$ nous construisons un espace projectif.

Définition 6: l'espace projectif $IP^{\,n}(K)$ est le quotient de l'espace Affine $/A^{n+1}(K)$ privé du point 0 par une relation $\Re$ d'équivalence définie comme suit.

$a = (a_1, ..., a_{n+1})\, \Re b = (b_1, ..., b_{n+1})$ **si et seulement s'il existe un** $\lambda \neq 0$ **dans le corps K tel que:** $a = \lambda b = (\lambda b_1, ..., \lambda b_{n+1})$.

Cette relation $\Re$ satisfait les 3 axiomes d'une relation d'équivalence.

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

L'espace projectif peut donc être représenté par l'ensemble des droites passant par l'origine. Il lui correspond l'anneau $A = K[x_1, x_2, \ldots, x_{n+1}]$ des polynômes homogènes à $n + 1$ indéterminées.

Par exemple un polynôme $f\ (x)$ à 3 indéterminées est homogène de degré $d \geq 1$ s'il satisfait la relation:

$f\ (tx, ty, tz) = t^{\,d} f\ (x)$.

Exemple d'espace projectif:

Soit l'espace projectif $IP^{\,2}(\mathbb{R}) = /A^3(\mathbb{R}) - \{0\}/\Re$.

Le point à l'infini $O_E = (\infty, \infty)$ de l'espace Affine $/A^2(\mathbb{R})$ a pour coordonnées $O_E = (0, 1, 0) \in IP^{\,2}(\mathbb{R})$.

Le point à l'infini est déterminé par la direction de l'axe Oy dans le plan (Ox, Oy).

4−**Variétés de Groupes et Variétés Abéliennes:**

Définition 7**: une Variété de Groupe est une Variété** X **munie d'un morphisme.**

$U : X \times X \to X$ **qui satisfait les** 3 **conditions:**

1/ $U\,(a, b) = a + b$.

2/ **L'ensemble des points de** X **est un groupe pour l'opérateur** U**.**

3/ **L'application inverse** $U_{-1} : X \to X^{-1}$ **est un morphisme de cette Variété.**

Exemple:

1/ Le groupe additif formé par la Variété $X = /A^1(K)$ et le morphisme $U\,(a, b) = a + b$ est une Variété de groupe.

2/ Le groupe multiplicatif formé par la Variété $X = /A^1(K) - (0)$ et le morphisme $U\ (a, b) = ab$ est une Variété de Groupe.

Définition 8**: une Variété Abélienne est une Variété de Groupe Projective et irréductible.**

Dans une Variété Abélienne il y a des points fermés et des ouverts.

Définition 9**: la jacobienne d'une Variété Abélienne** X **est l'ensemble des points fermés de** X**.**

Pour la classification des Variétés Algébriques, les notions de fonctions régulières, d'applications rationnelles, de matrices jacobiennes, sont utiles.

Définition 10**: soit** 2 **Variétés** X **et** Y **et une application** $f : X \to Y$

1/ **L'application** f **est rationnelle s'il existe une classe d'équivalence de paire** (U, g)**, où** U **est un sous ensemble ouvert non vide de** X **et** $g : U \to Y$ **un morphisme.**

2/ **Deux paires** (U, g)**, et** (U', g')**, sont équivalentes si les morphismes** g, g' **coïncident sur l'intersection** $U \cap U'$**.**

3/ **L'application** f **est birationnelle si elle est rationnelle et si elle admet une inverse,** $h : Y \to X$**, de composées** $f \circ h =$ **identité sur** Y **et** $h \circ f =$ **identité sur** X**.**

Alors les 2 **Variétés** X **et** Y **sont birationnellement équivalentes.**

Proposition 2**:**

Toute Variété X **de dimension** n **est birationnellement équivalente à une hypersurface dans l'espace projectif** $IP^{\,n}(K)$**.**

Idée de preuve:[14]

Le corps de fonction $K(X)$ est une extension finie séparable du corps K; donc il existe une base de transcendance $x_1, \ldots, x_{n+1}, y$ dans $K(X)$ telle que: $K(X) = K[x_1, \ldots, x_{n+1}, y]$.

Alors le polynôme irréductible f de cette base définit une hypersurface dans l'espace projectif $IP^{\,n}(K)$ selon une propriété des Variétés birationnellement équivalentes, cette hypersurface est birationnellement équivalente à la Variété X.

□

Le lien entre une Variété Affine X et son idéal $I(K)$ permet de dégager la notion de singularité.

Définition 11**: soit une Variété** X **dans un espace Affine** $/A^n(K)$ **et une famille de générateurs** $f_1, f_2, \dots f_s$ **de l'idéal** $I(X)$ **de la Variété;**

1− **La Variété** X **est non singulière en un point** P **de** X **si le rang de la matrice jacobienne** $(\delta f_i, \delta x_i)(P)$ **est égal à** $n - dim(X)$**.**

2− **La Variété** X **est non singulière si elle est non singulière en tout point de** X**.**

Soit un morphisme $\lambda : X \to Y$ de Variétés sur un corps Algébriquement clos K; alors ce morphisme est une application continue telle que pour chaque ouvert U de Y et pour chaque fonction régulière $f : X \to Y$, la fonction composée: $f \circ \lambda^{-1} : \lambda^{-1}(U) \to K$ est régulière.

Les fonctions régulières sur un espace X forment un anneau qui est local en chaque point de X ; cet anneau local admet donc un idéal maximal et un corps résiduel.

Indiquons un critère de reconnaissance des fonctions régulières.

Une fonction $f : X \to K$ est régulière en un point P de la Variété X s'il existe un ouvert U de X contenant P et 2 polynômes p et q de l'anneau $K[x_1, \dots, x_n]$ tels que q ne s'annule pas sur U et $f = p\ /q$. La fonction est régulière si elle est régulière en tout point de X. [4]

5− **Cohomologie des groupes:**

Cette théorie a été traitée par plusieurs auteurs; [3] , [4] , [16] .

Commençons par un groupe particulier.

Définition 12**: un groupe différentiel** (A, d) **est un groupe abélien additif** A **muni d'un opérateur différentiel** d**, endomorphisme** $d : A \to A$ **tel que** $d \circ d = 0$**, cela implique que l'image** Im **est inclue dans le noyau** $\ker d$ **:** $\operatorname{Im} d \subset \ker d$

$$\overset{d}{A} \to \overset{d}{A} \to \overset{d}{A} \to, \ d \circ d = d^{\,2} = 0 \qquad (1)$$

On en déduit le groupe dérivé, groupe quotient.

$$H(A) = \ker d \ / \operatorname{Im} d. \qquad (2)$$

Soit 2 **groupes différentiels** (A_1, d_1) **et** (A_2, d_2) .

Définition 13**: un homomorphisme de groupes** $f : A_1 \to A_2$ **est admissible lorsqu'il satisfait la relation de composition** $d_2 \circ f = f \circ d_1$ (3)

$$\begin{array}{ccc} A_1 & \underset{\to}{f} & A_2 \\ {\scriptstyle d_1}\downarrow & \searrow_{f \circ d_1}^{\,d_2 \circ f} & \downarrow{\scriptstyle d_2} \\ A_1 & \underset{\overrightarrow{f}}{} & A_2 \end{array}$$

Définition 14 :

Soient $(G_i)_{i\epsilon N}$ des groupes abéliens et $f_i : G_{i\rightarrow G_{i+1}}$ des morphismes de groupes. On dit que la suite :

$$\mathbf{G}_0 \overset{f_0}{\rightarrow} \mathbf{G}_1 \overset{f_1}{\rightarrow} .... \rightarrow \mathbf{G}_i \overset{fi-1}{\rightarrow} \mathbf{G}_{i+1} \overset{f_i}{\rightarrow} ... \overset{f_{i+1}}{}$$

est exacte si pour tout $i\epsilon N$ on a $Im(fi) = Ker(fi + 1)$.

Avec la notion de suite exacte, on obtient la

Proposition 3:
Soit une suite exacte courte de groupes différentiels:

$$O \to A \to^{i} B \to^{j} C \to O \qquad (4)$$

et les groupes dérivés $H(A), H(B)$ et $H(C)$.

Alors il existe un homomorphisme $d' : H(C) \longrightarrow H(A)$ qui rend le triangle suivant commutatif:

$$\begin{array}{ccc} H(C) & \to^{d'} & H(A) \\ {\scriptstyle j'}\nwarrow & & \swarrow{\scriptstyle i'} \\ & H(B) & \end{array}$$

Preuve:[13]

La suite exacte (4) satisfait la relation d'inclusion $i(A) \subset \ker(j)$

On utilise les propriétés des groupes dérivés.

□

Proposition 4:

Soit un diagramme commutatif de groupes différentiels:

$$\begin{array}{ccccccccc} & & & & i' & & j' & & \\ O & \to & A & \to & B & \to & C & \to & O \\ & & & {\scriptstyle f}\downarrow & & {\scriptstyle g}\downarrow & & {\scriptstyle h}\downarrow & \\ O & \to & A' & \to & B' & \to & C' & \to & O \\ & & & & i' & & j' & & \end{array}$$

avec les 2 lignes exactes et les 3 applications f, g, h, admissibles.

Alors le prisme suivant a des triangles exacts et des faces commutatives.

$$\begin{array}{ccccc} H(C) & & \overset{d_x}{\to} & & H(A) \\ & \searrow^{j_x} & & \swarrow_{i_x} & \\ {\scriptstyle h_x}\downarrow & & H(B) & & \downarrow{\scriptstyle f_x} \\ & & \downarrow{\scriptstyle g_x} & & \\ H(C') & & \longrightarrow & & H(A') \\ & {\scriptstyle j'_x}\searrow & & \swarrow{\scriptstyle i'_x} & \\ & & H(B') & & \end{array}$$

Preuve (d'après WEISS) [12]**:**

Un élément j de $H(C)$ est représenté par un élément c de C tel que $dc = 0$; d'où $\gamma = c + dc$

Il existe un élément b dans B tel que $jb = c$ et $j(db) = dc = 0$; alors il existe a dans A tel que $ia = db$ et $da = 0$.

Il existe un élément b dans B tel que $jb = c$ et $j(db) = dc = 0$; alors il existe a dans A tel que $ia = db$ et $da = 0$.

Il en résulte $a + dA = d_x(c + dc)$.

On en déduit les inclusions,

$\operatorname{Im} i_x \subset \ker j_x$; $\operatorname{Im} j_x \subset \ker d_x$, $\operatorname{Im} d_x \subset \ker i_*$; $\ker j \times \operatorname{Im} i_*$; $\ker d_x \subset \operatorname{Im} j_x$; $\ker i_x \subset \operatorname{Im} d_x$.

d'où les propriétés des triangles et des faces du prisme.

□

Définition 14: 1/ **un groupe abélien différentiel gradué est un groupe différentiel** (A,d) **avec un opérateur différentiel** d **tel que** $d : A_n \longrightarrow A_{n+r}$

pour $r = \pm 1$**.**

2/ **un groupe abélien** A **gradué est un groupe somme directe de sous groupes** A_n.

$\mathbf{A} = \sum_{n=-\infty}^{+\infty} \oplus \mathbf{A}_n$ **.**

Cela implique une suite exacte de la forme:

$$\overset{d_{n-1}}{\rightarrow} A_{n-r} \overset{d_n}{\rightarrow} A_n \overset{d_{n+1}}{\rightarrow} A_{n+1} \overset{d_{n+r}}{\rightarrow} A_{n+r} \overset{d_{n+2r}}{\rightarrow} A_{n+2r} \rightarrow A_{n+3r} \rightarrow \text{.....} \quad (5)$$

Avec les relations $d_{n+1} \circ d_n$ pour $r = \pm 1$.

Définition 15**:**

1/ **le cas** $r = +1$ **est la cohomologie des groupes; l'opérateur** d **est l'opérateur cobord; le groupe** A_n **est le groupe des** $n-$ **cochaines; le groupe quotient** $Z_n = A_n \cap \ker d_x$

est le groupe des $n-$ **cocycles.**

Le groupe quotient $B_n = A_n \cap d_{n-1} A_{n-1}$ **est le groupe des** $n-$ **cobords.**

2/ **le cas** $r = -1$ **est l'homologie des groupes.**

Définition 16**:**

le $n^{ème}$ **groupe de cohomologie du groupe** A **est le groupe quotient:** $H_n(A) = Z_n / B_n$**.**

On utilise des homomorphismes admissibles $f_n : A_n \rightarrow B_n$ **pour des groupes gradués différentiels** $(A, d_A, +1)$ **et** $(B, d_B, +1)$.

Proposition 5**:**

Soit un diagramme commutatif de groupes gradués différentiels $(A, d_A, +1)$ **et** $(B, d_B, +1)$ **de types cohormologiques, avec des applications admissibles de lignes exactes:**

$$\begin{array}{ccccccccc} O & \rightarrow & A & \rightarrow & B & \rightarrow & C & \rightarrow & O \\ & & & & \overset{f}{\downarrow} & & \overset{g}{\downarrow} & & \overset{h}{\downarrow} \\ \mathbf{O} & \rightarrow & \mathbf{A}' & \rightarrow & \mathbf{B}' & \rightarrow & \mathbf{C}' & \rightarrow & \mathbf{O} \end{array}$$

Alors le diagramme de groupes de cohomologie suivant est commutatif avec des lignes exactes.

$$\begin{array}{ccccccccccc} \rightarrow & H_{n-1}(C) & \overset{d_*}{\rightarrow} & H_n(A) & \rightarrow & H_n(B) & \overset{i_*}{\rightarrow} & H_n(C) & \overset{f_*}{\rightarrow} & H_{n+1}(A) & \overset{d_*}{\rightarrow} \\ & \downarrow h_x & & \downarrow f_x & & \downarrow g_x & & \downarrow h_x & & \downarrow f_x & \\ \rightarrow & \mathbf{H}_{n-1}(C') & \rightarrow & \mathbf{H}_n(A') & \rightarrow & \mathbf{H}_n(B') & \rightarrow & \mathbf{H}_n(C') & \rightarrow & \mathbf{H}_{n+1}(A') & \rightarrow \end{array}$$

$$\overset{d_*}{} \qquad \overset{i'_*}{} \qquad \overset{j'_*}{} \qquad \overset{d_*}{}$$

Preuve avec les définitions et les propriétés précédentes.

□

Herbrand a étudié une propriété d'un groupe abélien additif A avec 2 endomorphismes σ et τ tels que $\sigma \circ \tau = \tau \circ \sigma = 0$.

Soit un sous groupe B de A d'indice fini et stable par σ et $\tau, \sigma(B) \subset B$ et $\tau(B) \subset B$.

Soient les noyaux A_τ, B_τ,A_σ et B_σ de A et B et les images $A^\sigma, B^\sigma, A^\tau$ et B^τ.

Proposition 6 **(lemme de Herbrand):**

Soient les noyaux et les images ci-dessus.

Si les indices $(B_\sigma$**:**$B^\tau), (B_\tau : B^\sigma), (A_\sigma$**:**$A^\tau)$ **et** (A_τ, A^σ) **sont finis, alors, ils satisfont l'égalité:** $(A_\sigma : A^\tau)/(A_\tau, A^\sigma) = (B_\sigma : B^\tau)/(B_\tau : B_\sigma)$.

Preuve, avec les propriétés des groupes quotients:

$\mathbf{BA}_\tau/\mathbf{B} \simeq \mathbf{A}_\tau/\mathbf{B} \cap \mathbf{A}\boldsymbol{\tau} = \mathbf{A}_\tau/\mathbf{B}_\tau$,

$(A : B) = (A : BA_\tau)(BA_\tau : B)$.

Avec les groupes différentiels $(A, d, 1)$ et les groupes de cohomologie $H_n(A)$ on obtient le quotient de Herband: $\mathbb{Q}(A) = (A_\sigma : A^\tau)/(A_\tau, A^\sigma)$.

Proposition 7**:**

Si A **est fini, alors le quotient de Herbland de** A **est égal à** $\mathbb{Q}(A) = 1$.

Preuve: cf [16].

Ce quotient $\mathbb{Q}(A)$ possède d'autres propriétés [16].

Maintenant nous abordons la notion de G-complexe.

Soit un groupe multiplicatif fini G et son anneau de groupe des entiers $\mathbb{Z}[G\,]$, formé de sommes formelles:

$\sum_{\sigma\in G} x_\sigma\sigma$ pour $x_\sigma \in \mathbb{Z}$.

L'addition et la multiplication dans cet anneau $\mathbb{Z}[G]$ sont définies par les 2 formules:

$\sum_{\sigma\in G} m_\sigma\sigma + \sum_{\sigma\in G} n_\sigma\sigma = \sum_{\sigma\in G}(m_\sigma + n_\sigma\sigma);$ (1)

et

$(\sum_{\sigma\in G} m_\sigma\sigma)(\sum_{\sigma\in G} n_\sigma\sigma) = \sum_{\sigma\in G}(\sum_{\tau\varrho=\sigma} m_\tau n_\varrho)\sigma;$ (2)

Un autre type est constitué par un groupe abélien additif A avec une structure de $G-$ module Γ :

$\sigma(a+b) = \sigma a + \sigma b, \sigma(\tau\omega) = (\sigma\tau)a$ et $1(a) = a$

pour tous éléments σ, τ de G, a, b de A.

Soit un groupe gradué différentiel $X = \sum \oplus\partial_n$, avec $\partial_n : X_n \to X_{n-1}$.

Il en résulte le $G-$ complexe de chaîne sur G.

$$\to X_2 \overset{\partial_2}{\to} X_1 \overset{\partial_1}{\to} X_0 \overset{\partial_0}{\to} X_{-1} \to X_{-2} \overset{\partial_{-1}}{\to} \ldots\ldots\ldots\ldots \overset{\partial_{-2}}{} \quad (3)$$

$$\varepsilon \searrow \quad \nearrow \Gamma$$

$$\mathbb{Z}$$

avec $\partial_0 = \Gamma \circ \varepsilon$.

Dans le diagramme(3) il y a une partie positive

$$\ldots \to X_2 \overset{\partial_2}{\to} X_1 \overset{\partial_1}{\to} X_0 \to \mathbb{Z} \overset{\varepsilon}{\to} O \ldots\ldots\ldots\ldots\ldots\ldots (4)$$

Proposition 8**:**

Pour tout groupe fini G **il existe une partie positive du** $G-$ **complexe de la formule** (3) **ci-dessus.**

Preuve:

Soit l'anneau de groupe $\mathbb{Z}[G] = \Gamma$ des sommes formelles $\sum_{\sigma\in G} x_\sigma\sigma, x_\sigma \in \mathbb{Z}$

Considérons les cellules $X_0 = \Gamma[.], [\sigma_1], [\sigma_2], [\sigma_1, \sigma_2], ...$

Posons: $X_n = \sum_{\sigma_1,...\sigma_n \in G} \oplus \Gamma[\sigma_1, ..., \sigma_n]$, $[.]$ = cellule vide.

Définissons les images de ces cellules par les formules:

$\varepsilon([.]) = 1, \partial_1([\sigma]) = \sigma[.] - [.], \partial_2([\sigma_1, \sigma_2]) = \sigma_1[\sigma_2] - [\sigma_1\sigma_2] + \sigma_1$;

avec la relation de récurrence.

$\partial_n[\sigma_1, \sigma_2, ..., \sigma_n] = \sigma_1[\sigma_2, ..., \sigma_n] + \sum (-1)^i [\sigma_1, ..., \sigma_{i-1}, \sigma_i\sigma_{i+1}, \sigma_{i+2}, ..., \sigma_n] + (-1)^n [\sigma_1, ..., \sigma_{n-1}]$, $n \geq 1$

cette suite (4) est exacte; les $\Gamma-$ homomorphismes ∂_n satisfont les relations $\partial_r\partial_{r+1} = 0$ pour tout entier $r \geq 1$

□

Examinons maintenant la structure des groupes de cohomologie d'un groupe fini G et d'un $G-$ module A.

Soit le $G-$ complexe $(X, \partial), X = \sum \oplus X_n$, avec les opérateurs $\partial = \oplus\partial_n$.

Nous obtenons, avec les $G-$ homomorphismes, un groupe gradué différentiel $Hom(X, A) = \sum \oplus Hom_G(X_n, A)$.

Cela implique la suite de cohomologie:

$$n \to Hom_G(X_{n-1}, A) \overset{d_n}{\to} Hom_G(X_n, A) \overset{d_{n+1}}{\to} Hom_G(X_{n+1}, A) \to ...$$

Dans cette chaine, le groupe des $n-$ cochaines est $\varrho^1(G, A) = \varrho^n$

le groupe des $n-$ cocycle est $Z^n(G, A) = Z^n = \{f \in \varrho^n, df = 0\}$.

le groupe des $n-$ cobords est $B^n = B^n(G, A) = d\varrho^{n-1}$; le n^e groupe de cohomologie de G dans A est le groupe quotient $H_m(Hom_G(X, A)) = \mathbb{Z}^n/B^n$.

Il existe des homomorphismes croisés qui sont des fonctions: $f : G \to A$ telles que $f[\sigma\tau] = \sigma f[\tau] + f[\sigma]$ pour tous $\tau, \sigma \in G$.

Nous n'approfondirons pas la théorie de la cohomologie.

Cette théorie a été introduite, selon [21]

CHAPITRE II

Arithmétique des Courbes Elliptiques

Introduction:

Dans ce chapitre nous exposons quelques points de la théorie arithmétique des Courbes Elliptiques.

Cette théorie se trouve dans plusieurs ouvrages : [2], [5] , [6], [10], [13], [15] , [17] ...

Les Courbes Elliptiques admettent plusieurs applications: factorisations des grands entiers naturels de plus de 10^6 chiffres, codages des messages, cryptographie, etc...

Elles ont des liens avec la Théorie des Nombres, l'Analyse Complexe, la Géométrie Analytique, la Théorie des Groupes, les groupes spéciaux $GL\left(n,\mathbb{R}\right), SL\left(2,\mathbb{Z}\right)$.,etc...

L'ouvrage de référence conseillé par les spécialistes est celui de *Joseph H.SILVERMAN* [14] .

1− **Cubiques de Weierstrass:**

Définition 1**: une cubique de Weierstrass est une courbe cubique plane** E**, d'équation de la forme:**

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

Les cinq coefficients a_i **sont des éléments d'un corps commutatif** K**, global, local ou fini.**

Les deux variables x **et** y **sont des zéros de l'équation** (1)**; donc** x **et** y **sont des éléments d'une clôture Algébrique** K_{al} **de** K**.**

Définition 2**: l'équation** (1) **est l'équation de Weierstrass de la cubique de Weierstrass** E**.**

Dans le plan projectif $IP\ ^2(K)$**, l'équation de Weierstrass se met sous la forme d'un polynôme homogène de degré** 3**:**

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

2− **Changement de variables dans les équations de Weierstrass:**

L'équation de Weierstrass (1), peut être transformée par des changements de variables convenables.

Lorsque le corps K est de caractéristique $carac(K) \neq 2$, nous éliminons les monômes en xy et en y par le changement de variables:

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

Nous obtenons l'équation d'une cubique E_1:

$E_1 : Y^2 = 4X^3 + b_2X^2 + 2b_4X + b_6 \in K[x,y], carac\left(K\right) \neq 2;$

Avec le calcul j'obtiens les valeurs des invariants b_{2i}:

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

Ces 3 coefficients b_{2i} sont des polynômes homogènes de degré $2i$ dans l'anneau $\mathbb{Z}[a_1,a_2,a_3,a_4,a_6]$.

Pour $carac(K) \neq 2,3$, nous éliminons le monôme en X^2 et le coefficient 4 dans la formule (3) avec le changement de variables:

$X = (x - 3b_2)/36,\ Y = y\ /108;$

Nous obtenons l'équation de Weierstrass d'une cubique E_2:

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

Ces deux invariants c_{2i} sont des polynômes homogènes de degré $2i$ dans l'anneau $\mathbb{Z}[b_2,b_4,b_6]$.

$c_4 = b_2^2 - 24b_4; c_6 = 36b_2b_4 - b_2^3 - 216b_6;$

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

Le modèle de Legendre: $E_3 : y^2 = x(x-1)(x-t)$ avec $t \neq 0$ et 1:

Le model de Deuring: $E_4 : y^2 + txy + y = x^3$;avec $t^3 \neq 3$:

Le but de ces changements de variables est d'obtenir des invariants des cubiques de Weierstrass.

3− **Invariants des cubiques de Weierstrass:**

Les cubiques de Weierstrass possèdent plusieurs invariants: un discriminant $\Delta(E)$, un invariant modulaire $j(E)$, un invariant différentiel $\omega(E)$, un conducteur $N(E)$ etc...

Définition 3: un invariant de E est une fonction des coefficients a_i qui permet de classifier les cubiques de Weierstrass.

Définition 4: le discriminant d'une Cubique de Weierstrass E, est le polynôme homogène de degré 12 de l'anneau $\mathbb{Z}[b_2, b_4, b_6, b_8]$, égal à:

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

avec $4b_8 = b_2b_6 - b_4^2$ **et** $car(K) \neq 2, 3$

La cubique de Weierstrass:

(9) $E : y^2 = x^3 - 27c_4 - 54c_6, car(K) \neq 2, 3$**,**

a un discriminant égal à:

(10) $\triangle(E) = (1/1728)(c_4^3 - c_6^2)$**;**

Le discriminant de l'équation de Legendre est égal à:

$(11)\triangle(E) = 16t^2(1-t)^2$**.**

Le discriminant du modèle de Deuring E_4 est égal à:

$\triangle(\mathbf{E}_4) = \mathbf{t}^3\mathbf{-27}$.

Exemple 1:

Calcul du discriminant de la cubique de Weierstrass:

$E : y^2 - 7xy + 4y = x^3 - 5x^2 + 8x - 14 \in \mathbb{Q}[x, y]$.

J'obtiens avec le calcul $b_2 = 29, b_4 = -12, b_6 = -40, b_8 = -326$

Le discriminant $\triangle(E) = 2 \times 5 \times 37007 = 370070$.

Exemple 2 : le discriminant de la cubique $y^2 = x^3 + Ax + B$ est égal à

$\triangle(E) = -16\left(4A^3 + 27B^2\right)$.

Définition 5: l'invariant modulaire d'une Cubique de Weierstrass E d'équation de Weierstrass:

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

est l'élément du corps K, $carac(K) \neq 2, 3$, égal à:

(12) $j(E) = c_4(E)^3/\triangle(E)$**.**

L'invariant modulaire d'une cubique de Weierstrass: $E : y^2 = x^3 + Ax + B \in K[x, y]$**, est égal à:**

$j(E) = 4(12A)^3/(4A^3 + 27B^2)$**.**

Exemple:

L'invariant modulaire de la cubique d'équation de Weierstrass:

$E' : y^2 + 6xy - 12y = x^3 - 10x^2 + 5x - 25 \in K[x, y]$.

$b_2 = a_1^2 + 4a_2 = 6^2 + 4(-10) = 4, b_2 = 4, b_4 = a_1a_3 + 2a_4, b_4 = 6(-12) + 2(5), b_4 = -62, b_6 = a_3^2 + 4a_6 = (-12)^2 + 4(-25) = 44, b_6 = 44,$

$4b_8 = b_2b_6 - b_4^2 = 4(44) - (-62)^2, b_8 = -105$

Le discriminant $\triangle(E) = 2^9 \times 5 \times 769$ et le coefficient $c_4 = 2^5 \times 47$

L'invariant modulaire $j(E) = 2^6 \times 103823/(5 \times 769)$.

Définition 6: le conducteur d'une cubique de Weierstrass E est l'élément : $N(E) = \prod_{v \in M_K} P^{\,f_v}$.

Où M_K désigne l'ensemble des valuations inéquivalentes v du corps K, P est un diviseur premier du discriminant de E, l'exposant f_v prend les valeurs:

0, lorsque E a une bonne réduction en v.

1, lorsque E a une réduction multiplicative en v.

$2+t$, lorsque E a une réduction additive en v,

$t = 0$ pour $p \geq 5, 0 \leq t \leq 3$, pour $p = 3$ et, $0 \leq t \leq 6$, pour $p = 2$, selon Velu.

4− Résultant de 2 polynômes:

Le résultant est une application de l'algèbre multilinéaire à un anneau de polynômes.

Soit un anneau $K[x]$ de polynômes sur un corps commutatif K et 2 polynômes:

(1) $f(x) = c_0 X^{\,r} + c_1 X^{\,r-1} + ... + c_{r-1}X + c_r$, de degré $r \geq 1$

(2) $g(x) = d_0 X^{\,p} + d_1 X^{\,p-1} + ... + d_{p-1}X + d_p$ de degré $p \geq 1$.

Définition 7: le résultant des 2 polynômes f et g ci dessus, est le déterminant d'ordre $r+p$ égal à:

$$\mathbf{Res}(f,g) = \begin{vmatrix} c_0 & c_1 & ..... & c_r & & & & & & \\ 0 & c_0 & & . & c_r & & & & & \\ .. & .. & .. & .. & .. & & & & & \\ 0 & .. & .. & c_0 & c_1 & c_2 & c_3 & .. & .. & c_r \\ d_0 & d_1 & .. & .. & d_p & & & & & \\ & & & & .. & d_p & & & & \\ & & & & & .. & d_p & & & \\ & & & & & & .. & .. & .. & \\ & & & d_0 & d_1 & .. & .. & .. & d_p & \\ & & & 0 & d_0 & d_1 & .. & .. & .. & d_p \end{vmatrix}$$

avec p lignes $L_i = (c_0 ... c_r)$ et r lignes $L'_i = (d_0 ... d_p)$.

Les termes qui manquent dans ce déterminant sont remplacés par des zéros.

Ce déterminant est une fonction de ses vecteurs lignes;

(3) $\mathbf{Res}(f,g) = \det(L_1, L_2, ... L_p, L'_1, L'_2, ..., L'_r,)$.

La théorie des déterminants implique la:

Proposition 1:

Soit le résultant de la formule(3) ; il satisfait la relation:

$\mathbf{Res}(f,g) = (-1)^{pr} . \mathbf{Res}(f,g)$.

Preuve:

Nous appliquons les propriétés de l'algèbre multilinéaire.

□

Proposition 2:

Soit les polynômes f et g des formules$(1), (2)$, un scalaire non nul a et le résultant $Res(f,g)$ des 2 polynômes. Alors:

1) $Res\ (f,g)$ **contient le monôme** $c_0^p d_0^r$;

2) $Res\ (af,g) = a^p Res\ (f,g)$; pour toute constante a.

3) $Res\ (f,ag) = a^r Res\ (f,g)$.

Le résultant des polynômes f **et** g **s'exprime au moyen des racines de ces polynômes.**

Preuve: cf [14] .

Proposition 3:

Soit 2 polynômes f **et** g **factorisés sous la forme:**

$f\ (x) = c_0 (x-\alpha_1)(x-\alpha_2)...(x-\alpha_r)$ **et**

$\mathbf{g}(x) = \mathbf{d}_0 (x-\beta_1)(x-\beta_2)...\left(x-\beta_p\right)$.

Alors leur résultant est égal au produit:

$\mathbf{Res}(f,g) = \mathbf{c}_0^p \mathbf{d}_0^r \prod_{1\leq i\leq r\ ,1\leq j\leq p} \left(\alpha_i - \beta_j\right)$.

Preuve: cf [8] .

□

Cette formule du résultant implique le:

Corollaire:

Soit les hypothèses de la proposition 2.

Alors le résultant est nul si et seulement si les deux polynômes ont une racine commune $\alpha_i = \beta_j$ **pour certains indices** i **et** j**.**

Preuve avec la forme produit.

□

Examinons le cas particulier du résultant d'un polynôme $f\ (x)$ et de sa dérivée $f\ '(x)$.

Proposition 4:

Soit un polynôme $f\ (x) = c \prod_{1\leq i\leq r} (x-\alpha_i)$ **de degré** r**. Alors le résultant de** $f\ (x)$ **et de sa dérivée** $f\ '(x)$ **est égal au produit:** $Res(f, f\ ') = c^{r-1} \prod_{1\leq i\leq r} f\ ''(\alpha_i)$.

Ce résultant est lié au discriminant $D(f\ )$ **du polynôme** $f\ (x)$ **par les formules:**

$D(x) = c^{2r-2} \prod_{i\neq j} (\alpha_i - \alpha_j)^2$ **et** $Res\ (f, f\ ') = c.D(f\ )$.

Preuve: Kostrikin, Algèbre.

□

Exemples:

1− Polynôme cubique:

$f\ (x) = ax^3 + bx^2 + cx + d \in \mathbb{R}[x,y]$.

Son discriminant est égal à:

$D(f\ ) = 18abcd + b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^{\ 2}$:

2− Polynôme cubique:

$f\ (x) = 4x^3 + b_2x^2 + 2b_4x + b_6 \in \mathbb{R}[x,y]$.

$D(f\ ) = 16\left(9b_2b_4b_6 - 8b_4^3 - 27b_6^2 - b_2^2b_8\right)$

Le $2^{ème}$ facteur de $D(f\ )$ est égal au discriminant $\triangle(E)$ de la cubique d'équation:

$E : y^2 = f\ (x) \in \mathbb{R}\,[x, y]\,.$

Alors, les discriminants de f et de E satisfont la relation:

$D(f\ ) = 16\triangle(E)$.

Nous nous basons sur les ouvrages Algébra de *Serge LANG* et Introduction à l'algèbre de *KOSTRIKIN*, pour la théorie du résultant

5− **Classification des cubiques de Weierstrass par leurs discriminants et c_4:**

Proposition 5:

Soit une cubique de Weierstrass C d'équation (1) et le discriminant $\triangle(C)$.

Le point $O_C = (0, 1, 0)$ du plan projectif $IP^{\ 2}$ est un point non singulier sur C.

La cubique C est singulière si et seulement si son discriminant est nul.

Preuve de: "le point $O_C = (0, 1, 0)$ du plan projectif $IP^{\ 2}$ est un point non singulier sur C : "

Le point $(0, 1, 0)$ est un point du plan projectif $IP^{\ 2}$. Dans ce plan, l'équation de C est un polynôme cubique homogène de la forme:

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

Les coordonnées du point $O_C = (0, 1, 0)$ satisfont cette équation:

$F(O_C) = 0$;

Il en résulte que ce point à l'infini est sur la cubique de Weierstrass C.

Considérons les 3 dérivées partielles de la fonction $F(X, Y, Z)$, alors:

$F_{\mathbb{Z}}{}'(0, 1, 0) = 1 \neq 0$; $F_x{}'\,(0, 1, 0) = F_y{}'\,(0, 1, 0) = 0$.

Cette valeur implique que le point O_C n'est pas singulier sur la cubique C.

Preuve de: "C est une cubique singulière" implique "son discriminant est nul:"

Soit une cubique C d'équation de Weierstrass: $y^2 = f\ (x)$;

L'hypothèse C est une cubique singulière implique que le polynôme $f\ (x)$ admet une racine multiple.

La relation entre le $Res\ (f, f\ ')$ et le discriminant $D(f\ )$, impliquent

$D(f\ ) = 0$.

La relation entre les discriminants de f et de la cubique de Weierstrass C implique $\triangle(C) = 0$.

Preuve de: "$\triangle(C) = 0$" implique "la cubique C est singulière:"

Soit une cubique C d'équation (4).

La relation entre discriminant de C et de f implique $D(f\ ) = 0$; par la théorie des points singuliers, cette valeur implique que la cubique C est singulière.

□

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

Définition 8: une cubique de Weierstrass non singulière est une Courbe Elliptique.

Par la proposition 1, une Courbe Elliptique E a un discriminant non nul $\triangle(C) \neq 0$.

Cela implique 2 types de Courbes Elliptiques: le type $\triangle(C) > 0$ et le type $\triangle(C) < 0$.

Proposition 6:

Soit une cubique C de Weierstrass.

1) **cette cubique admet un nœud si et seulement si:**

$\triangle(C) = 0$ **et** $c_4(C) \neq 0$**;**

2) **elle admet un point de rebroussement si et seulement si:**

$\triangle(C) = c_4(C) = 0$**.**

Preuve de: "C admet un nœud" implique "$c_4 \neq 0$":

Par la proposition 1,une cubique de Weierstrass a un discriminant $\triangle(C) = 0$.

Je choisis une équation de Weierstrass de la forme:

$x^3 + 27c_4x + 54c_6 \in K[x, y], carK \neq 2, 3$.

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

Les pentes de ces tangentes sont égales à la drivée:

$y' = 3\left(x^2 - 9c_4\right)/2y = 3N(x)/2y$.

Le polynôme $N(x)$ admet 2 racines distinées:

$x = \pm 3\sqrt{c_4}$ lorsque $c_4 \neq 0$.

□

Preuve de: "la Cubique de Weierstrass C admet un point de rebroussement" implique "$\triangle(C) = 0$ et $c_4(C) = 0$":

Par la proposition 1, la Cubique de Weierstrass singulière a un $\triangle(C) = 0$.

Par définition, en un point de rebroussement, les tangentes à la cubique sont confondues.

Avec l'équation de Weierstrass précédente, les pentes des tangentes à C aux points de rebroussement sont confondues si: $N(x) = x^2 - 9c_4$ admet une racine double, cela implique $c_4(C) = 0$.

Le polynôme $N(x)$ admet une racine double; cela implique $c_4(C) = 0$.

□

Exemple de cubique munie d'un nœud:

Soit la cubique C_1d'équation de Weierstrass:

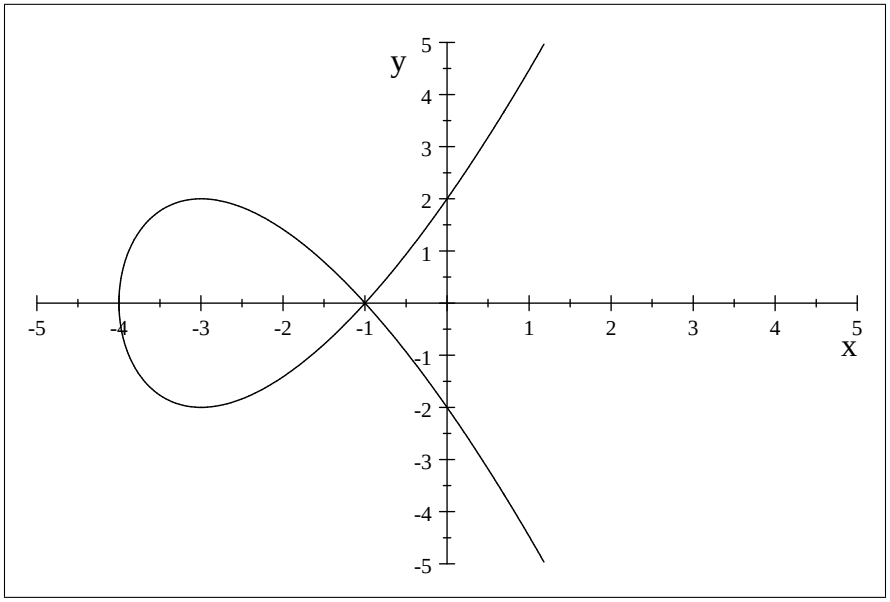
$y^2 = x^3 + 6x^2 + 9x + 4 \in \mathbb{R}[x, y]$

calcul des invariants: $c_4 = 144$ et $\triangle(C_1) = 0$.

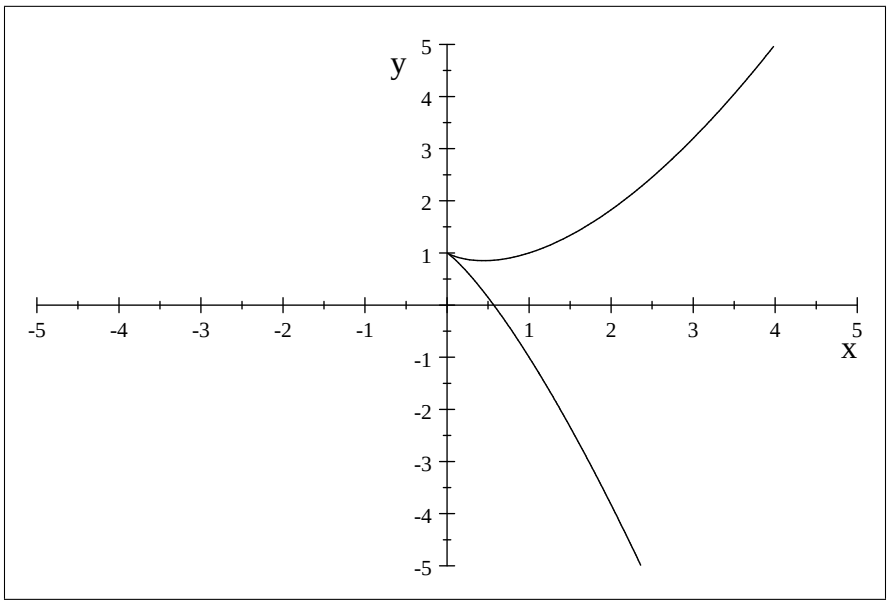
Cette cubique admet un nœud.

Pour $x = -1$, j'obtiens $y^2 = 0$.ll en résulte que le nœud de C_1 est le point $(-1, 0)$.

Je trace la cubique avec un logiciel: Scientific Work Place.



Exemple de cubique munie d'un point de rebroussement:
Soit la cubique C_2 d'équation de Weierstrass:
$y^2 + 2xy - 2y = x^3 - x^2 + 2x - 1 \in \mathbb{R}[x, y]$.
Tableau de quelques points:
$x = 0$, $y^2 - 2y + 1 = 0$, $y_1 = y_2 = 1$
$x = 1$, $y^2 = 1$, $y_1 = 1$, $y_2 = -1$
$x = -1$, $y^2 - 4y = -5$,
$y_1 = 2 + i$, $y_2 = 2 - i$ avec $i^2 = -1$.
$y = 0$, $x^3 - x^2 + 2x - 1 = 0$, 3 zéros $x_1 = 0.215\,08 - 1.\,307\,1i$, $x_2 = 0.215\,08 + 1.\,307\,1i$, $x_3 = 0.569\,84$,



Proposition 7:

Soit une Courbe Elliptique E de discriminant $\triangle(E)$, alors:

1) **La Courbe Elliptique E coupe l'axe Ox en 3 points simples si et seulement si $\triangle(E) > 0$;**

2) **La Courbe E coupe l'axe Ox en un seul point, simple, si et seulement si $\triangle(E) < 0$.**

Preuve de: "E coupe Ox en 3 points" implique "$\triangle(E) > 0$":

Soit une Courbe Elliptique E ; elle n'a pas de point singulier, alors son discriminant n'est pas nul.

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

Alors, E a une équation de Weierstrass :

(1) $y^2 = (x - e_1)(x - e_2)(x - e_3) = f\ (x)\, \mathbb{R}[x]$.

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

(2) $D(f\ ) = \prod_{1 \leq i < j \leq 3} (e_i - e_j)^2$;

Les trois abscisses e_i étant réelles, (2) implique le signe $D(f\ ) > 0$.

La relation entre les discriminants de $f\ (x)$ et de E, impliquent le signe du discriminant de E: $\triangle(E) > 0$;

□

Preuve de: "E coupe l'axe Ox en un seul point" implique "$\triangle(E) < 0$":

Soit une Courbe Elliptique E qui coupe l'axe Ox en un seul point simple $(e, 0)$. Alors E a une équation de Weierstrass de la forme:

(3) $y^2 = (x - e)(x^2 + rx + s) = f\ (x) \in \mathbb{R}[x]$,

$r^2 - 4s < 0$,

$g(x) = x^2 + rx + s \in \mathbb{R}[s]$

Le polynôme $g(x)$ de $2^{ème}$ degré admet 2 racines complexes conjuguées: $m \pm in$;

Le discriminant de ce polynôme $g(x)$ est égal à :

$D(f\ ) = -4n^2((e-m)^2 + n^2)^2$;

Puisque les trois nombres e, m et n sont réels, il en résulte le signe: $D(f\ ) < 0$;

La relation entre les discriminants de E et de $f\ (x)$ impliquent le signe du discriminant: $\triangle(E) < 0$.

□

Exemple de Courbe Elliptique qui coupe l'axe Ox en 3 points:

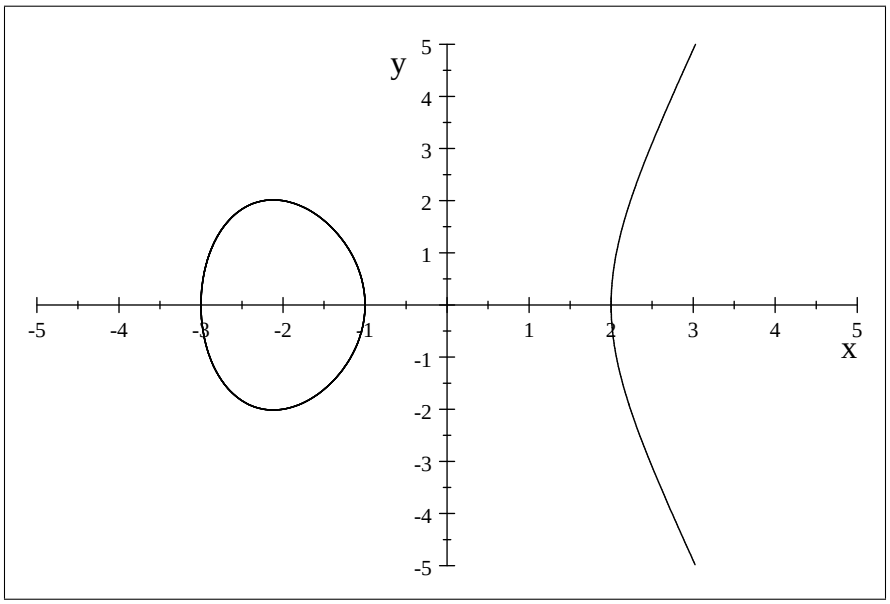
Soit la cubique E_1 d équation de Weierstrass:

$E_1 : y^2 = (x+3)(x+1)(x-2) \in \mathbb{R}[x, y]$.

Tableau de quelques points:

$x = 0$, $y^2 = -6$, $y_1 = -2.449\,5i$, $y_2 = 2.449\,5i$, donc il n'existe pas y réel.

$y = 0$, 3 zéros $x_1 = -3$, $x_2 = -1$, $x_3 = 2$



Calcul du discriminant: $\triangle(E_1) = 64^2 \times 143 > 0$.

Les 3 points d'intersection de E_1par Ox sont:$(-3, 0), (-1, 0), (2, 0)$.

Exemple de Courbe Elliptique qui coupe l'axe Ox en un seul point:

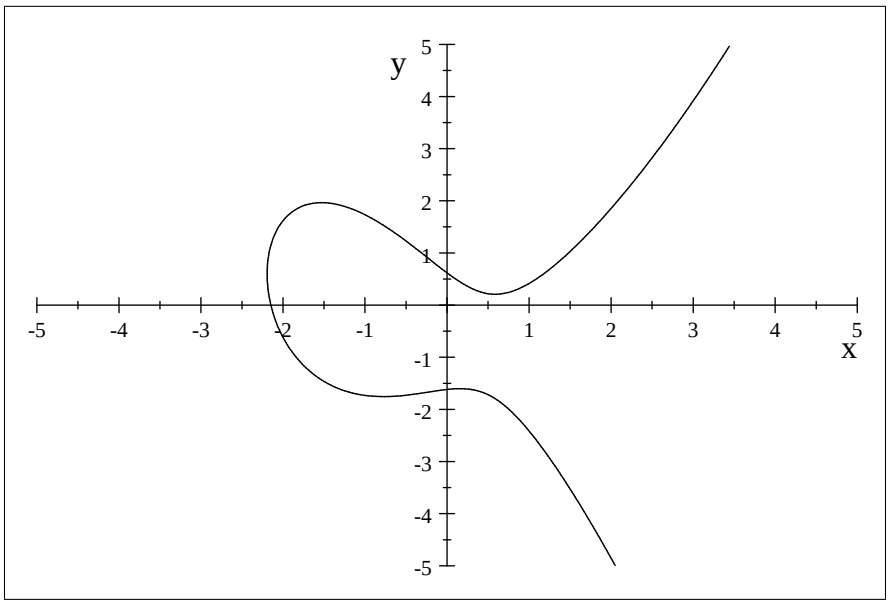
$E_2 : y^2 + xy + y = x^3 + x^2 - 2x + 1$;

Tableau de quelques points:

$x = 0$, $y^2 + y - 1 = 0$, $y_1 = 0.618\,03$, $y_2 = -1.618$

$y = 0$, $x^3 + x^2 - 2x + 1 = 0$, 3 zéros $x_1 = 0.573\,95 - 0.368\,99i$, $x_2 = 0.573\,95 + 0.368\,99i$, $x_3 = -2.147\,9$, donc x_2 et $x_3 \notin \mathbb{R}$ et $x_3 \in \mathbb{R}$.

$y^2 + xy + y = x^3 + x^2 - 2x + 1$



Calcul du discriminant: $\triangle(E_2) = -16 \times 83 < 0$.

CHAPITRE III

Groupe de Mordell-Weil d'une Courbe Elliptique

Introduction.

Dans ce chapitre nous exposons une propriété géométrique "de 3 points colinéaires d'une Courbe Elliptique, le groupe de Mordell-Weil, les homomorphismes et les isogénies de Courbes Elliptiques.

1− **Structure de groupe abélien sur l'ensemble** $E(K)$**:**

Soit une Courbe Elliptique E d'équation de Weierstrass:

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

Les 5 coefficients a_i sont les éléments d'un corps commutatif K, global, local ou fini.

Les 2 variables x et y sont des zéros de l'équation (1); donc x et y sont des éléments d'une clôture Algébrique K_{al} de K.

Sur l'ensemble $E(K)$ des points rationnels de E, nous définissons une loi de groupe abélien, d'élément neutre le point $O_E = (0, 1, 0) \in IP^2$, à l'infini sur E, par la

Proposition 1**:**

L'ensemble $E(K)$ **des points rationnels d'une Courbe Elliptique** E**, admet une structure de groupe additif abélien, d'élément neutre le point** O_E**, avec la règle géométrique:"**3 **points colinéaires de** E **ont une somme nulle:**

$P + R + S = O_E$, **et la loi de composition interne:**

$f : E(K) \times E(K) \longrightarrow E(K)$, **avec** $f(P, R) = P + R$.

Preuve:

1) Le point à l'infini O_E est déterminé par la direction de l'axe OY.

C'est un point simple sur les courbes E.

Pour tout point P de l'ensemble $E(K)$, la règle géométrique des 3 points colinéaire implique:

$P + O_E = P = O_E + P$.

L'axiome de l'élément neutre est vérifié.

2) Le symétrique d'un point P de $E(K)$ est le $2^{ème}$ point R d'intersection de E par la parallèle à Oy qui passe P. Il en résulte le symétrique de P:

$R = -P$.

3) Toute sécante ST de la courbe E est confondue avec la sécante TS.

Il en résulte la relation:

$S + T = T + S$

L'axiome de commutativité est vérifié.

4) Pour vérifier l'axiome d'associativité, il n'y a pas de construction géométrique utilisable. Il faut calculer les sommes de 3 points $P + R + S$:

$P + R = M$; $M + S$;$R + S = T$ et $P + T$.

Alors nous obtenons l'égalité:

$M + S = P + T$.

Il en résulte la formule d'associativité:

$(P + R) + S = P + (R + S) = P + R + S$;

□

Définition 1**: le groupe additif abélien** $E(K)$ **est le groupe de Mordell-Weil de la Courbe Elliptique** E**.**

2− **Coordonnées des points:** $-P$ **et** $P_1 + P_2$:

Pour obtenir les coordonnés du symétrique d'un point, de la somme de 2 points et du point $2P$ des Courbes Elliptiques il faut utiliser la règle géométrique des 3 points colinéaires de la courbe et la théorie des intersections des courbes planes par des droites.

Coordonnées du symétrique $-P$ **d'un point** $P = (x, y)$**:**

Equation de la parallèle à Oy passant par le point $P : x = x_p$.

L'équation de Weierstrass de E devient une équation en y de degré 2 ;

la somme de ses deux racines est égale à:

$y + y\,(-P) = -a_1 x - a_3$.

Nous en déduisons les coordonnées du symétrique $-P$ de P:

(1) $P = (x, y)$ et $-P = (x, -y - a_1 x - a_3)$. Figure 1.

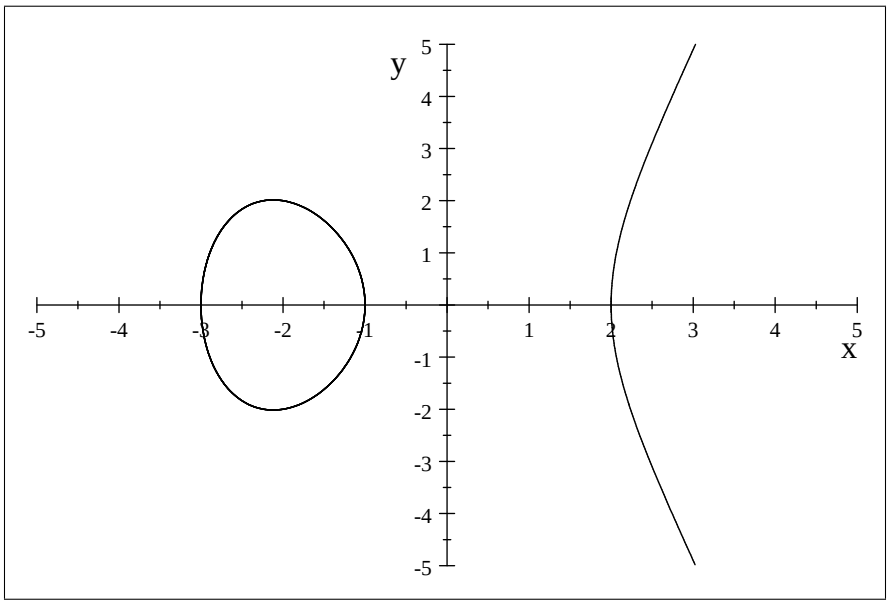


figure 1

Coordonnées de la somme de 2 **points** $P_i = (x_i, y_i)$ **tels que** $P_1 \neq \pm P_2$:

figure 2.

La sécante P_1P_2 a pour équation:

$y = t\,(x - x_i) - y_i$, et $t = (y_1 - y_2)/\,(x_1 - x_2)$.

Elle recoupe la Courbe E en un point P_3. Ces 3 points satisfont la relation: $P_1 + P_2 = P_3$;

Avec la théorie de l'intersection d'une courbe par une sécante, nous obtenons les coordonnées de la somme:

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

$x_M = t^{\,2} + a_1 t - a_2 - x_1 - x_2$;
$y_M = -t^3 - 2a_1 t^2 + \left(a_2 - a_1^2 + 2x_1 + x_2\right) t + a_1 a_2 - a_3 + a_1 \left(x_1 + x_2\right) - y_1$;
(2) pour $t = \left(y_1 - y_2\right) / \left(x_1 - x_2\right)$.

Nous avons démontré la

Proposition 2:

Soit une Courbe Elliptique E d'équation de Weierstrass:

$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \in K[x, y]$.

1) **Le symétrique d'un point $P = (x, y)$ de $E(K)$ est le point:**

$\mathbf{-P} = \left(x, -y - a_1 x - a_3\right)$.

2) **La somme $P_1 + P_2$ pour $P_1 \neq \pm P_2$ est le point $M = P_1 + P_2$.**

$\mathbf{x}_M = \mathbf{t}^2 + \mathbf{a}_1\mathbf{t} - \mathbf{a}_2 - \mathbf{x}_1 - \mathbf{x}_2$;

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

et $t = \left(y_1 - y_2\right) / \left(x_1 - x_2\right)$.

Le point M est le symétrique du 3^e point d'intersection P_3 de $P_1 P_2$ par E.

□

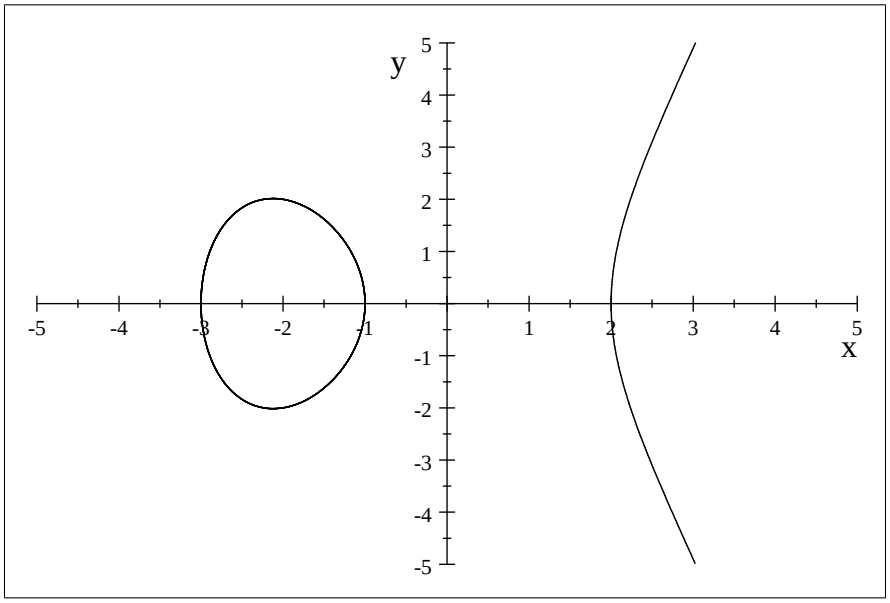


figure 2

3−**Torsion de Courbes Elliptiques:**

Un point d'ordre m d'une Courbe Elliptique E est un point P du groupe abélien additif $E(K)$ tel que: $mP = O_E$ et $dP \neq O_E$ pour tout entiers $d < m$.

Définition 2: pour tout entier rationnel m, un point P du groupe $E(K)$ d'ordre m satisfait la relation:

$mP = O_E$**, le symbole** mP **représente les sommes:**

$mP = P + P + ... + P, m$ **fois** P**, si** m **est positif;**

$mP = (-P) + (-P) ... + (-P), (-m)$ **fois** $(-P)$**, si** m **est négatif;**

et $OP = O_E$.

Définition 3: pour tout rationnel m, l'ensemble $E(K)[m] = E[m]$, des points d'ordre m d' une Courbe Elliptique E, est le sous groupe de m-torsion de E.

Définition 4:

1/ **le sous groupe de m -torsion du groupe $E(K)$ de Mordell- Weil d'une**

Courbe Elliptique E est l'ensemble des points d'ordre m fini

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

2/ **le groupe de torsion d'une Courbe Elliptique E est l'ensemble:**

$T(E) = \cup_{m\in\mathbb{Z}} E(K)[m]$ **des points de E d'ordre fini.**

Déterminons les coordonnées des points d'ordre m du groupe $E(K)$.

Pour $m = 2$, nous utilisons l'équation de la tangente à la Courbe E au point P.

Elle coupe la courbe en un point simple T.

$y = y^{'}(x - x_p) - y_p$.

L'équation de Weierstrass de E devient une équation en x cubique.

Nous utilisons la fonction symétrique élémentaire des racines de cette équation pour calculer l'abscisse du point T. Nous obtenons les coordonnées de $2P$ pour $P = (x, y), 2P = (x_{2P}, y_{2P})$;

$x_{2P} = y'^2 + a_1 y' - 2x$; et

$y' = (3x^2 + 2a_2x + a_4 - a_1y)/(2y + a_1x + a_3)$;

$y_{2P} = -y'^3 - 2a_1y'^2 + \left(a_2 - a_1^2 + 3x\right) y' + a_1a_2 - a_3 + 2a_1x - y$.

Nous avons démontré la:

Proposition 3:

Soit une Courbe Elliptique E d'équation de Weierstrass:

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

Les coordonnées du point $2P$,figure 3, pour tout point $P = (x, y)$ de la courbe E sont égales à:

$x_{2P} = y'^2 + a_1y' - 2x$; **et** $y' = (3x^2 + 2a_2x + a_4 - a_1y)/(2y + a_1x + a_3)$;

$\mathbf{y}_{2P} = -\mathbf{y}^{'3} - \mathbf{2a}_1\mathbf{y}^{'2} + \left(a_2 - a_1^2 + 3x\right)\mathbf{y}^{'} + \mathbf{a}_1\mathbf{a}_2 - \mathbf{a}_3 + \mathbf{2a}_1\mathbf{x} - \mathbf{y}$.

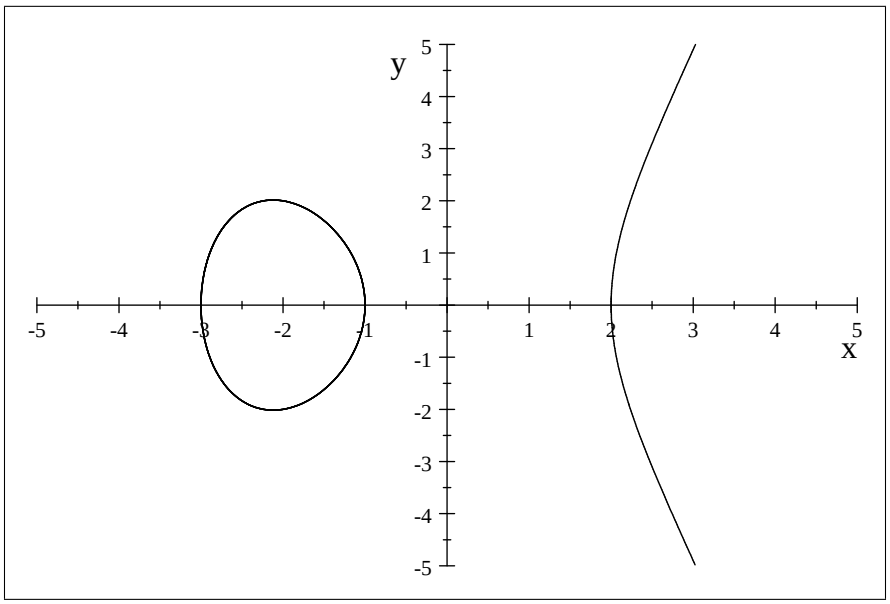


figure 3

$3-1-$ **Cas particulier des Courbes Elliptiques sur le corps** $\mathbb{Q}$**:**

La structure du groupe $T(E)(\mathbb{Q})$ de torsion d'une Courbe Elliptique E sur le corps des nombres rationnels $\mathbb{Q}$ à été démontrée par Mazur [9].

Théorème 1**: le groupe de torsion** $T(E)(\mathbb{Q})$ **d'une Courbe Elliptique** $E(K)$ **est isomorphe à l'un des** 15 **groupes additifs abéliens finis:**

$\mathbb{Z}/d\,\mathbb{Z}$, **pour** $1 \leq d \leq 10$ **et** $d = 12$;

$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$ **pour** $1 \leq m \leq 4$.

Preuve: [18]

Cette structure du groupe de torsion $T(E)(\mathbb{Q})$ est apparue dans la recherche des nombres premiers N tels qu'il existe des Courbes Elliptiques qui admettent des $N-$ isogénies $\mathbb{Q}-$ rationnelles.

Ces nombres premiers sont égaux à:

$N = 11, 17, 19, 37, 67$ et 163.

La représentation de groupe:

$\varrho_N : G(K_{a\lg}/K \to Gl(2; \mathbb{Z}/N\mathbb{Z})$.

Des propriétés de ces points sont utilisées pour la preuve supposons qu'il n'y a pas de point d'ordre $N = 11$ et $N \geq 17$.

Cela implique que la Courbe Elliptique a une bonne réduction en $p = 3$.

Par la théorie de *Néron* sur la spécialisation d'un point de $E(IF_3)$ possède un point d'ordre $N \leq 4$.

Ce résultat est en contradiction avec l'hypothèse $N \geq 7$.

Il en résulte le théorème de *Mazur*.

□

Proposition 3:
Soit une Courbe Elliptique E sur $\mathbb{Q}$, d'équation de Weierstrass:
$y^2 = x^3 + Ax + B \in \mathbb{Q}[x, y]$, **avec** $A, B \in \mathbb{Z}$ **et** $4A^3 + 27B^2 \neq 0$.
Considérons un point $P = (x, y)$ de torsion de E. Alors:
1/ x **et** y **sont des entiers rationnels.**
2/ **Lorsque** $2P \neq O_E$**, alors** y^2 **divise** $4A^3 + 27B^2$.
Preuve: par *LUTZ.*[14]
□
Exemple:
Soit une Courbe Elliptique E, d'équation de Weierstrass:
$y^2 = x^3 + 3x + 6 \in \mathbb{Q}[x, y]$,
$4A^3 + 27B^2 = 8 \times 9 \times 5$.
Les valeurs possibles de y^2 sont $y^2 = 4, 9, 36$.
Pour $y^2 = 4$, $x^3 + 3x + 6 = 4$, implique $x^3 + 3x + 2 = 0$; une solution $x = -1$.
$y^2 = 9$, implique $x^3 + 3x + 2 = 0$;pas de solution.
$y^2 = 36$, implique l'équation diophantienne $x^3 + 3x - 30 = 0$;pas de solution.
Solution avec le

Théorème 2: toute solution d'une équation dianphantienne $d_0x^n + d_1x^{n-1} + ... + d_{n-1}x + d_n = 0$ **est un diviseur du terme constant** d_n.
□

La structure du groupe de Mordell-Weil d'une Courbe Elliptique E sur un corps commutatif K a été déterminée par la théorie des variétés et les fonctions hauteurs.

Il y a de nombreux travaux sur les groupe de torsion nous citons:

1/ Il n'existe pas, sur les Courbes Elliptiques, de point d'ordre 13, [21].

2/ L'ordre du groupe de torsion $T(E)$ d'une Courbe Elliptique E sur un corps quadratique est borné [22].

3/ Il n'y a pas de Courbe Elliptique, sur un corps quadratique, qui posséde un point d'ordre 32, [23].

4/ Le groupe de torsion d'une Courbe Elliptique, sur un corps cubique pur, est isomorphe à l'un des 13 groupes abéliens:

$\mathbb{Z}/n\mathbb{Z}$, pour $n = 1, 2, ...8$ et $n = 10$.
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$, pour $m = 1, 2$ et 3.
$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.
(selon Muller, Stroher et Zimmer dans Arkiv.Math.15(1977)$1 - 19$).

5/ Kishi a montré, dans Tokyo J.Mathan.,vol.$20, 2, (1997), 315 - 327$, le

Théorème 3: Soit un corps K, Quadratique, cyclique, imaginaire, et une Courbe Elliptique E sur K.

Alors, le groupe de torsion de E est isomorphe à l'un des 10 groupes abéliens finis:

$\mathbb{Z}/m\mathbb{Z}$ **pour** $m = 1, 2...6$ **et** $m = 8$.
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2d\ \mathbb{Z}$ **pour** $d = 1, 2,$ **et** 3.

$4-8-$ **Courbe Elliptique à Multiplication Complexe:**

Définition 10**:**

Une Courbe Elliptique E **possède une Multiplication Complexe par un corps quadratique imaginaire**

$K=\mathbb{Q}(\sqrt{-d})$ **lorsque son anneau des endomorphismes** $End\ (E)$ **est est isomorphe à un ordre de ce corps quadratique imaginaire, ou à un ordre de l'algèbre des quaternions.**

Exemples:

1/ Une Courbe Elliptique a une Multiplication Complexe par un ordre du corps quadratique imaginaire $\mathbb{Q}(i)$.

Soit la Courbe Elliptique E, d'équation de Weierstrass:

$E: y^2=x^3+17\in\mathbb{Q}[x,y]$ de discriminant $\Delta(E)=-2^4x3^3x17^2\neq 0$.

Soit un endomorphisme $f: E(\mathbb{Q})\rightarrow E(\mathbb{Q})$ de valeur $f(x,y)=(-x,iy), i=$ nombre complexe $i=\sqrt{-1}$;

Il en résulte que l'anneau $End\ (E)$ est isomorphe à un ordre du corps quadratique imaginaire $K=\mathbb{Q}\left(i\right)$.

2/ Multiplication Complexe par $\sqrt{-7}$ sur la Courbe Elliptique E, d'équation de Weierstrass:

$E': y^2+xy=x^3-x^2-2x-1$.

de discriminant $\Delta\left(E'\right)=-7^3$ et d'invariant modulaire $j(E)=-15^3$.

La Courbe Elliptique a une Multiplication Complexe par l'anneau A_k des entiers du corps quadratique imaginaire $K=\mathbb{Q}\left(\sqrt{-7}\right)$.

Proposition 11**:**

Soit un corps quadratique imaginaire L et des Courbes Elliptiques E à Multiplication Complexe par l'anneau des entiers de L.

1/ Il ya un nombre fini de classes d'isomphisme de Courbe Elliptique E.

2/ l'invariant modulaire $j(E)$ **est algébrique sur le corps** $\mathbb{Q}$.

Preuve:

1/ Le groupe des classes d'idéaux d'un corps de degré fini est fini.

Cela implique la finitude du nombre d'anneaux d'entiers et la finitude du nombre des Courbes Elliptiques associées.

2/ Soit un $\mathbb{Q}-$ automorphisme S du corps $\mathbb{C}$ qui opère sur une Courbe Elliptique E par:

$S\left(x,y\right)=\left(S\left(x\right),S\left(y\right)\right)$ pour tout point (x,y) de la courbe E.

Il en résulte l'égalité: $S\left(E\right)=E$.

S opère sur l'invariant modulaire $S(j(E))=j(S(E))$.

Donc l'ensemble des éléments $j(S(E))$ est fini. Il en résulte que $j(E)$ est algébrique sur $\mathbb{Q}$.

□

CHAPITRE IV

Valuations - Réductions - Hauteurs

Introduction:

La théorie des valuations a de nombreuses applications dans plusieurs domaines des mathématiques: décomposition des idéaux, corps locaux, réductions des Courbes Elliptiques, hauteurs...

Cette théorie se trouve dans les ouvrages:"Algebraic Numtbers and Algebraic fonctions" de Artin, "Number Théory" de Hasse, "Diophatine Géometry" de Lang...

1− **Valuations et réductions:**

a) Valuation d'un corps:

Définition 1: une valuation d'un corps K est une fonction réelle:

$\mathbf{v : K \to \mathbb{R}_+}$

qui satisfait les 3 axiomes:

1/ $v(x) \geq 0$ **et pour tout élément** x **et** $v(x) = 0$ **si et seulement si** $x = 0$**.**

2/ $v(xy) = v(x)v(y)$ **pour tout** x **et** y **de** K**.**

3/ **il existe une constante réelle positive** c **telle que:**

$v(x) \leq 1$ **implique** $v(x + 1) \leq c$.

L'axiome 2 implique la

Proposition 1:

Toute valuation d'un corps K est un homomorphisme du groupe multiplicatif $\mathbf{K^*}$ **dans le groupe multiplicatif** $\mathbb{R}_+^*$ **des nombres réels positifs.**

Preuve:

L'axiome 2 contient la formule de l'homomorphisme de groupes multiplicatifs.

□

Proposition 2:

Soit une valuation: $v : K \to \mathbb{R}_+$ **d'un corps** K**. Elle satisfait les relations:**

$v(-1) = v(1)$; $v(1/x) = 1/v(x)$; **pour** x **non nul;** $v(x\ /y) = v(x)/v(y)$ **pour tout** x **et** y **non nuls de** K**.**

Preuve:

Par l'axiome 2 j'obtiens: $v(xy) = v(x)v(y)$.

Pour $x = y = 1$ cette relation devient $v(1) = v(1)^2$.

Dans l'anneau des entiers du corps K, cette équation admet 2 solutions $v(1) = 1$ et $v(1) = 0$.

L'axiome 1 implique la solution: $v(1) = 1$.

La décomposition:$(-1)^2 = 1$ implique les valuations:

$v(1/x) = 1/v(x)$, pour x non nul.

La décomposition $x\ /y = x(1/y)$ implique les valuations:

$v(x/y) = v(x)/v(y)$ pour$x$ et y non nuls.

□

Proposition 3:

Toute valuation $v : K \to \mathbb{R}_+$ peut être associée à une constante positive c qui satisfait la relation:

$v(x+y) \leq c \max(v(x), v(y))$, **pour tous éléments** x, y **de** K.

□

Exemple: valuation $p-$ adique:

Par définition la valuation $p-$ adique en un nombre premier p a pour valeur $v_p(p^r) = r$ et $v_p(q) = 1$ pour tout nombre premier $q \neq p$.

b) Classification des réductions des Courbes Elliptiques:

Soit E/K une Courbe Elliptique. il y a 2 types de réductions des Courbes Elliptiques; les bonnes qui réduisent une Courbe Elliptique en une Courbe Elliptique, les mauvaises qui réduisent les Courbes Elliptiques en cubiques singulières.

Définition 2: une équation de Weierstrass est minimale lorsqu'elle est minimale pour toute valuation du corps de base K.

Les réductions des courbes Elliptiques sont classifiée selon la:

Définition 3:

1) **une Courbe Elliptique E sur un corps K a une bonne rédution pour une valuation v de K si la courbe réduite $\bar{E}$ est une Courbe Elliptique.**

2) **La réduction est mauvaise si la courbe réduite est une cubique singulière.**

La réduction est multiplicative si la courbe réduite a un nœud.

La réduction est additive si la courbe réduite a un point de rebroussement.

3) **La réduction multiplicative est décomposée si les deux tangentes à la courbe réduite, en son nœud, ont des équations rationnelles.**

Les bonnes réductions sont des réductions stables.

Les réductions multiplicatives sont des réductions semi-stables, les réductions additives sont des réductions instables.

Les 2 invariants $(\Delta(E), c_4(E)$d'une Courbe Elliptique E peuvent déterminer le type de réduction.

Proposition 4:

Soit une Courbe Elliptique E, d'équation de Weierstrass minimale, d'invariants $(\Delta(E), c_4(E)$ et une valuation v du corps de base K de E**.**

1) E **a une bonne réduction en v si et seulement si** $v(\Delta(E)) = 0$.

2) E **a une réduction multiplicative si et seulement si** $v(\Delta(E)) > 0$ **et** $v(c_4(E)) = 0$.

3) E **a une réduction additive en v si et seulement si** $v(\Delta(E)) > 0$ **et** $v(c_4(E)) > 0$.

Preuve:

L'équation de Weierstrass est minimale en v si elle satisfait:

$v(a) > 0$ pour $i = 1, 2, ...6$ et $v(\Delta(E)) < 12$.

Lorsque $v(\Delta(E)) = 0$, alors $\Delta(\bar{E})$ est une $v-$unité; donc le discriminant de la courbe réduite n'est pas nul; d'où la courbe réduite est une Courbe Elliptique. Donc cette réduction est bonne.

Lorsque $v(\Delta(E)) > 0$, alors $\Delta(E) = 0$ et la courbe réduite est singulière; pour $v(c_4(E)) = 0$, l'invariant $c_4(E)$ est une $v-$unité; donc cet invariant $c_4\left(\bar{E}\right)$ n'est pas nul; il en résulte que la courbe réduite a un nœud.

Donc la réduction de E est multiplicative. Lorsque $v(\Delta(E)) > 0$ et $v(c_4(E)) > 0$, alors la courbe réduite a un discriminant et un invariant c_4 nuls; donc elle admet un point de rebroussement.

Donc la réduction de E est additive.

□

Exemples:

1) Cubique $E_1 : y^2 = x^3 + px + 1$, p premier.

Calcul du discriminant $\Delta(E_1) = -16\left(4p^3 + 27\right)$.

Réduction modulo p:

E_1 devient $E'_1 : y^2 = x^3 + 1$

alors $\Delta(E') = -16 \times 27 \neq 0$ pour carac$(K) \neq 2, 3$ la réduction en p est bonne.

2) Cubique $E_2 : y^2 = x^3 + x + p$, p premier.

Réduction modulo p, E_2 devient $E' : y^2 = x^3 + x$.

$\Delta(E') = -16 \times 4 \neq 0$ en car$(K) \neq 2$

la réduction en p est bonne.

3) Cubique $E_3 : y^2 + 6xy - 5y = x^3 - 9x^2 + 3x - 5$.

$\Delta(E_3) = 27\left(8^4 - 5^2\right) = 3^4 \times 59 \times 23$

les réductions v_3, v_{23} et v_{59} impliquent $\Delta(E_3) = 0$, donc mauvaises réductions

les réductions v_p pour les nombres premiers $p \neq 3, 23$ et 59 impliquent $\Delta(E) \neq 0$, donc bonnes réductions.

Les valuations d'un corps K sont classifiées en valuations archimédiennes et valuations non archimédiennes.

Les valuations archimédienne sont dans la classe des valeurs absolues du corps des nombres réels:

$v_\infty(x) = \max(x, -x)$,

exemple: $v_\infty(-5) = 5 = v_\infty(5)$,

$v_\infty(-72/13) = v_\infty(72/13) = 72/13$.

Les valuations non archimédiennes sont dans la classe des valuations $p-$adiques pour chaque nombre premier $p \geq 2$.

L'ensemble $Val(K)$ des valuations de K est la réunion $Val(K) = v_\infty \cup \{v_p, p \text{ premier}\}$ des valuations inéquivalantes.

A chaque valuation <u>*non archimédienne*</u> v de K, sont attachés des sous ensembles de K.

$A(K)$ = anneau des $v-$ entiers de $K = \{x \in K, v(x) \geq 0\}$,

$U(K)$ = groupe des $v-$ unités de $K = \{x \in K, v(x) = 0\}$,

$I(K)$ = idéal maximal en $v = \{x \in K, v(x) \geq 1\}$,

le corps résiduel en $v = K_{res} = A(K)/I(K)$.

Proposition 5:

1) **Lorsque la Courbe Elliptique E a une réduction multiplicative en v, alors le groupe de Mordell-Weil $\bar{E}(K_{res})$ de la courbe réduite est isomorphe au groupe multiplicatif K^*_{res} du corps résiduel.**

2) **Lorsque la Courbe Elliptique a une réduction additive en v, alors le groupe $\bar{E}(K_{res})$ est isomorphe au groupe additif K_{res} du corps résiduel.**

Preuve:

1) Lorsque la réduction en v est multiplicative, la courbe réduite a un nœud s où elle admet 2 tangentes d'équations:

$y = rx + r^{'}$, $y = sx + s^{'}$.

Considérons l'application de groupes multiplicatifs:

$f : \bar{E}(K_{res})^* \rightarrow K_{res}^*$,

de valeur: $f\ (\bar{p} = (\bar{x}, \bar{y})) = (\bar{y} - \bar{r}\bar{x} - \bar{r}^{'})/(\bar{y} - \bar{s}\bar{x} - \bar{s}^{'})$.

Cette application satisfait les formules d'isomorphisme de groupes.

2) Lorsque la réduction en v est additive, la courbe réduite a un point de rebroussement S où elle admet une tangente d'équation:

$y = rx + s$.

Considérons l'application de groupes additifs:

$f : \bar{E}(K_{res}) \rightarrow K_{res}$,

de valeur: $f\ (\bar{p} = (\bar{x}, \bar{y})) = (\bar{x} - \bar{x}(S))/(\bar{y} - r\bar{x} - s)$.

Cette application satisfait les formules d'isomorphisme de groupes abéliens.

□

c) **Réductions et sous groupe de Mordell-Weil** $E(K)$:

Toute valuation v du corps K détermine 2 sous groupes intéressants:

$E_0(K) = \{P \in E(K)\,;\bar{P}$ non singulier$\}$,

$E_1(K) = \{P \in E(K)\,;\bar{P} = O_E\}$.

Proposition 6 :

Soient une Courbe Elliptique E, sur un corps K munie d'une valuation discrète v, ses invariants $\Delta(E)$ et $j(E)$, le sous groupe $E_0(K)$ des points de réduction non singulière.

1) Lorsque E a une réduction multiplicative décomposée en v, le groupe quotient $E(K)/E_0(K)$ est cyclique d'ordre $v(\Delta(E)) = -v(j(E))$;

2) Pour les autres réductions, ce groupe est d'ordre au plus 4.

Preuve:

C'est un Théorème de Kodaïra-Néron. La formule de l'invariant modulaire:

$j(E) = c_4^3/\Delta(E)$ implique la formule:

$v(j(E)) = v(c_4(E))^3 - v(\Delta(E))$.

Pour $v(c_4(E))^3 = 0$, cette formule devient:

$v(j(E)) = -v(\Delta(E))$.

Une équation de Weierstrass est minimale en v à la condition:

$v(c_4(E)) < 4$.

□

Exemple:

Soit la Courbe Elliptique E d'équation de Weierstrass:

$y^2 + 5xy - 2y = x^3 + 4x^2 - 3x - 1$.

Calcul des invariants:

$b_2 = 41, b_4 = -16, b_6 = 0, b_8 = -64, c_4 = 2065$ et $\Delta(E) = 64 \times 3 \times 17 \times 43$;

Valuations discrètes du corps $\mathbb{Q}$ des rationnels:

$v_5(\Delta) = 0$ et $v_5(c_4) = 1$.

Donc la Courbe réduite $E(IF_5)$ est Elliptique.

Le calcul montre que le groupe contient les points $(0,-1),(-1,0)$ et le point à l'infini.

pour la valuation $v_7, v_7(c_4) = v_7(\Delta(E)) = 0$.

Donc la Courbe réduite est Elliptique; son groupe de Mordell-Weil $E(IF_7)$ est formé de 4 points.

Il en résulte que le groupe $T(E)(Q)$ de torsion est trivial.

Exemple:

Soit la Courbe Elliptique E d'équation de Weierstrass:

$E : y^2 + xy + y = x^3 + x^2 - 4x + 5 \in \mathbb{Q}[x, y]$.

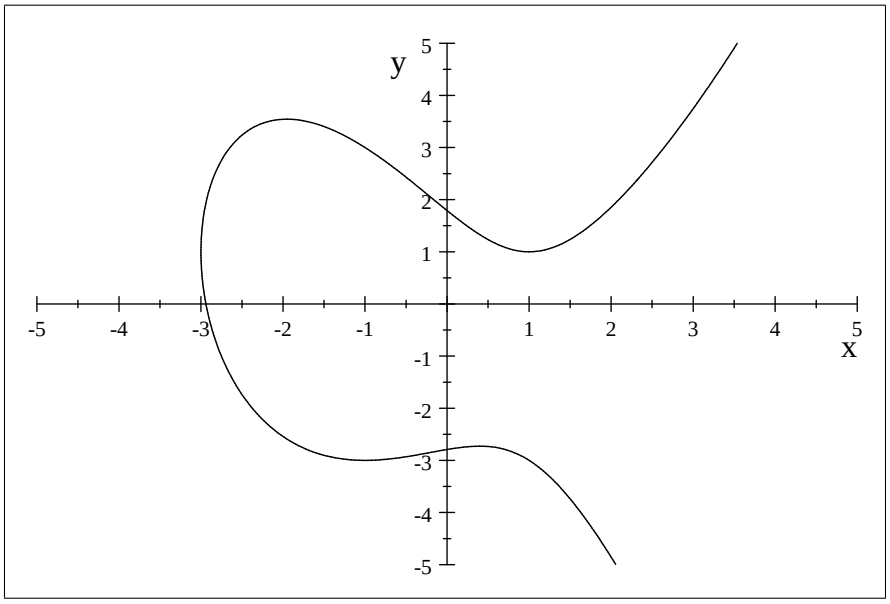
Calcul des invariants:

$\Delta(E) = -2^8 \times 3^2 \times 7, j(E) = 193^3/2^8 \times 3^2 \times 7$;

Cette courbe a une réduction multiplicative en $P = 7$.

D'après le théorème de classification des cubiques de Weierstrass par leurs discriminant, cette cubique coupe l'axe Ox en un seul point.

$E : y^2 + xy + y = x^3 + x^2 - 4x + 5$.



Le groupe abélien $E(K)$ de Mordell-Weil est de type fini.

Utilisons la descente infinie et les hauteurs pour démonter ce résultat.

2/ Hauteurs et descente infinie:

Définition 4: une hauteur sur un groupe abélien A est une fonction: $h : A \to \mathbb{R}_+$, **à valeurs réelles positives, qui satisfait les 3 axiomes:**

$(h1)$ **A tout point** P_1 **de** A **on peut associer une constante** $c_1(A, P_1) = c_1$ **telle que:**

$h(P + P_1) \leq 2h(P) + c_1$ **pour tout point** P **de** A.

$(h2)$ **Il existe un entier m** ≥ 2 **et une constante** c_2 **tels que:**

$h(mP) \geq m^2 h(P) - c_2$ **pour tout point** P **de** A.

$(h3)$ **Tout ensemble de points P de A de hauteur** $h(P)$ **bornée est fini.**

$\{P \in A : h(P) \leq B, B =$ **constante**$\}$ est fini.

La fonction hauteur sur A est utilisée pour démontrer que le groupe A est de type fini dès que le groupe quotient A/mA est fini.

$b/$ **Descente infinie:** c'est un algorithme qui a été utilisé par Fermat pour étudier quelques problèmes mathématiques.

Il a utilisé cet algorithme pour démontrer la différence entre un nombre algébrique et un nombre rationnel.

Pour démontrer que le nombre $\sqrt{7}$ n'est pas rationnel, il a utilisé un raisonnement par l'absurde.

supposons $\sqrt{7} = a\ /b$ rationnel, a, $b \in \mathbb{N}$, a et b premiers entre eux.

Alors $7b^2 = a^2$ (1)

C'est une équation diophantienne.

Pour résoudre (1) nous utilisons le théorème de Gauss;

7 divise a^2 donc 7 divise a cela implique $a = 7a_1$ (2)

Elevons les 2 membres de (2) au carré;

$a^2 = 49a_1^2$ implique

$7b^2 = 49a_1^2$,donc $b^2 = 7a_1^2$, $b = 7b_1$, $7b_1^2 = a_1^2$, $a_1 = 7a_2$. (3)

Nous obtenons 2 suites infinies

$a = 7a_1$, $a_1 = 7a$, $a_2 = 7a_3, ..., a_n = 7a_{n+1}$.. et

$b = 7b_1$, $b_1 = 7b_2$, $b_2 = 7b_3, ...$, $b_n = 7b_{n+1}$..

Le résultat est contraire à l'hypothèse "a et b sont premiers entre eux"; donc $\sqrt{7}$ n'est pas rationnel.

Proposition 7:

Soit un groupe abélien A **et un entier** $m \geq 2$ **tels que le groupe quotient** A/mA **soit fini. Alors le groupe** A **est de type fini.**

Preuve:

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

(1) $R_1, R_2, ..., R_s$.

Considérons une suite infinie de points P de A avec la descente infinie:

(2) $P = mP_1 + R_{i_1}, P_1 = mP_2 + R_{i_2}, ..., P_{n-1} = mP_n + R_{i_n}$, pour $i_n = 1, 2, ..., s$.

Introduisons la hauteur: $h : A \to \mathbb{R}_+$ ci dessus. Dans la suite (2) prenons une combinaison:

(3) $mP_t = mP_{t-1} - R_{t-1}$.

Appliquons à (3) l'axiome $(h2)$ à gauche et l'axiome $(h1)$ à droite. Nous obtenons l'inégalité:

(4) $m^2 h(P_t) - c_2 \leq 2h(P_{t-1}) + c_1$.

Cette inégalité se met sous la forme:

(5) $m^2 h(P_t) \leq 2h(P_{t-1}) + c^{'}; c^{'} = c_1 + c_2$.

Avec les sommes des inégalités (5) $t = 1, 2...$, nous obtenons l'inégalité:

(6) $h(P_n) \leq (2/m^2)h(P) + \left(m^{-2} + m^{-4} + ... + m^{-2n}\right) c_4; c_4(c_1, c_2)$.

Pour $m \geq 2$, (6) devient:

(7) $h(P_n) \leq u(n)\, h(P) + m^{-2}(1 + m^{-2})^{-1}; \lim u(n)_{n\to\infty} = 0$.

Il en résulte que le $2^{ème}$ membre de (7) est borné par un nombre fini B, l'axiome $(h3)$ implique que l'ensemble de ces points P_t est fini.

(8) $P_1, P_2, ..., P_r$.

(1) et (8) impliquent que le groupe A est engendré par les points des suites (1) et (8).

Il en résulte que tout point P de A est une $\mathbb{Z}-$ combinaison linéaire:

(9) $P = n_1 R_1 + ... + n_s R_s + k_1 P_1 + ... + k_r P_r$.

Donc le groupe abélien A est de type fini.

Proposition 8 (Théorème de Mordell-Weil):

Le groupe de Mordell-Weil d'une Courbe Elliptique est de type fini.

Preuve:

Soit une Courbe Elliptique E et son groupe $E(K)$. La finitude du groupe quotient $E(K)/mE(K)$ a été établie précédemment pour $m = 2$.Considérons les générateurs $T_1...T_s$ du groupe de torsion $T(E)$ et des générateurs $P_1, ..., P_r$ du groupe $E(K)/2E(K)$. Alors tout point P de $E(K)$ est une $\mathbb{Z}-$combinaison des générateurs:

$P = m_1 T_1 + ... + m_s T_s + n_1 P_1 + ... + n_r P_r$.

□

3/ **Formes modulaire et série de Dirichlet-Hasse:**

Définition 5**: soit le réseau $L \subset \mathbb{C}$, la fonction $\wp$ de Weierstrass (associée à L) est définie par les séries:**

$\wp(z, L) = \mathbf{1/z^2} + \sum_{\substack{\omega\in L \\ \omega\neq 0}} \mathbf{(1/(z-\omega)^2 - 1/\omega^2}$.

La fonction $\wp(z, L)$ de Weierstrass et sa dérivée $\wp'(z, L)$ satisfont la relation:

$\wp'(z, L)^2 = \wp(z)^3 - g_2(L)\wp(z) - g_3(L)$

le changement de variables $\wp(z, L) = x, \wp'(z, L) = y$ la transforme en équation de cubique de Weierstrass:

$y^2 = x^3 - g_2(L)\, x - g_3(L)$.

Fonctions et formes modulaires (d'après Silverman, Appendice c p 342**):**

Définition 6**: le groupe modulaire $SL(2, \mathbb{Z})$ est le groupe spécial linéaire des matrices A d'ordre** 2 **de** $\det(A) = 1$:

$SL(2, \mathbb{Z}) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}; a, b, c, d \in \mathbb{Z}; ad - bc = 1 \right\}$.

Le groupe modulaire est engendré par 2 **matrices particulières.**

Proposition 9**:**

1) **Le groupe modulaire $SL(2,\mathbb{Z})$ est engendré par les 2 matrices:**
$T=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ **et** $S=\begin{pmatrix}0 & -1\\ 1 & 1\end{pmatrix}$.
2) **Toute matrice A de ce groupe est un produit de type:**
$\mathbf{A}=\mathbf{T}^{n_1}\mathbf{S}\mathbf{T}^{n_2}\mathbf{S}\mathbf{T}^{n_3}...\mathbf{S}\mathbf{T}^{n_k};\mathbf{n}_i\in\mathbb{Z}$.
3) **Cette représentation n'est pas unique.**
Preuve:
Par le calcul nous obtenons les puissances de matrices:
$S^{2}=-I_2; S^{4}=I_2;$
$T^{n}=\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix}$; $ST=\begin{pmatrix}0 & -1\\ 1 & 1\end{pmatrix}$ et $(ST)^3=-I_2$.
Apostol cite la matrice particulière A représentée par:
$A=\begin{pmatrix}4 & 9\\ 11 & 25\end{pmatrix}=ST^{-3}ST^{-4}ST^{2}$.
□

Définition 7: une fonction modulaire f de poids k pour le groupe $SL(2,\mathbb{Z})$ est une fonction f sur le demi plan:
$IH=\{x+iy\in\mathbb{C}, y\geq 0\}$ **qui admet un développement:**
$f(z)=\sum_{n\geq 1}c(n)q^n, q=\exp(2\pi iz)$ **et satisfait:**
$f(Az)=(cz+d)^k f(z)$ **pour toute matrice** $A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ **dans** $SL(2,\mathbb{Z})$

Les coefficients $g_i(L)$ sont des fonctions qui s'exprimes en fonction des séries d'Eisenstein.

Définition 8: les séries d'Eisenstein de poids $2k$ pour un réseau complexe L sont de la forme:
$\mathbf{G}_{2k}(L)=\sum\boldsymbol{\omega}^{-2k};\boldsymbol{\omega}\in\mathbf{L}-\{\mathbf{0}\}$.
Elles se mettent sous la forme:
$G_{2k}(z)=\sum_{s,t}(sz+t)^{-2k};\ s,t\in\mathbb{Z};(s,t)\neq(0,0)$.
Elles sont fonction de la fonction Zéta et de la fonction somme $\sigma(n)$ des diviseurs de n.
$G_{2k}(L)=2\zeta(2k)-2((2\pi i)^{2k}/(2k-1)!)\sum\sigma_{2k-1}(n)q^n$.
Où $\zeta(u)$ = fonction Zêta de Riemann, $\Im(s)=\sum_{n\geq 1}n^{-1}$, $\sigma_t(n)$ = somme des puissances $t-ièmes$ des diviseurs positifs de n.
Les coefficients $g_i(L)=g_i(z)$ sont des fonctions de ces séries:
$g_2(L:z)=60G_4(z)=(2\pi)^4(20X+1/12)$,
avec $X=\sum_{n\geq 1}\sigma_3(n)q^n$, $.q$ premier.
C'est une forme modulaire de poids 4 pour le groupe modulaire $SL(2;\mathbb{Z})$.
$g_3(L:z)=140G_6(z)=(2\pi)^6(72-7Y)$,
avec $Y=\sum_{n\geq 1}\sigma_5(n)q^n$,et $q=\exp(2\pi iz)$.
C'est une forme modulaire de poids $k=6$ pour le groupe modulaire $SL(2;\mathbb{Z})$.
Les séries d'Eisenstein sont normalisées par division par $2\zeta(2k)$:
$E_{2k}(z)=G_{2k}(z)/2\zeta(2k)=1-(4k/B_{2k})\sum_{n\geq 1}\sigma_{2k-1}(n)q^n$,
où B_{2k} = nombre de Bernoulli.
Théorème 1:

Soit une forme modulaire f de poids 2k dont les coefficients c(n) de sa série de Fourier satisfont la relation:

$\mathbf{c(m)c}\left(n\right)=\sum_{m,n}\mathbf{d}^{2k-1}\mathbf{c}\left(mn\ /d^{2}\right)$,

où d =diviseur de pgcd(m, n).

Alors la série de Dirichlet de f est de la forme:

$\mathbf{g(s)}=\prod\left(1-c\left(p\right)p^{-1}+p^{2k-2s-1}\right)^{-1}$,

où p = diviseurs premiers de n.

Preuve: Apostol.□

Il y a une autre application des séries de Dirichlet.

Conjecture (Taniyama-Weil**):**

Soit une Courbe Elliptique E, de conducteur N(E) sur le corps $\mathbb{Q}$ et la transforme de Mellin de la série de Dirichlet L(E; s) de E:

$\mathbf{f}\left(z\right)=\sum_{n\geq1}\mathbf{c}\left(n\right)\mathbf{q}^{n};\mathbf{q}=\exp\left(2i\pi z\right)$.

Cette fonction f est une forme parabolique de poids 2 pour le sous groupe modulaire de congruence $\Gamma_0\left(N\right)$ de niveau N.

Cette conjecture etait vérifiée par Shimura dans [20].

CONCLUSION:

Il y a plusieurs problèmes de la théorie des Courbes Elliptiques que je me propose d'étudier après mon magister:

Groupes de *CHÂTELET-WEIL WC(E(K));*

Groupes de *SHAFAREVICH-TATE ■(E).*

Groupes de *SELMER S(E/K).*

TWISTS de Courbes Elliptiques.

Conjecture de *TANIYAMA-WEIL.*

Courbes Elliptiques sur un corps fini et application à la CRYPTOGRAPHIE...etc

REFERENCES

[1] BIRCH, B.J and KUYK, W.Modular Functions of One Variable IV (Antwerp).

Lecture Notes in Math 476-Springer-Verlag, Berlin (1975).

[2] BIRCH, B.J and H.P.F SWINNERTON-DYER: Notes on Elliptic Curves I and II,

Journal Reine Angew. Math $212(1963)7-25-$et $218(1965)79-108$.

[3] BROWN: Cohomology of Groups-Graduate Texts in Mathématics $n°87$-Springer (1984) .

[4] Robin HARTSHORNE: Algebraic Geometry-GTM $n°$ 52(1980).

[5] D.HUSEMOLLER. Elliptic Curves-GMT $n°111$-Springer-(1987).

[6] Anthony W.KNAPP: Elliptic Curves-Mathematicae Notes- Princeton University Press- New Jersey (1993).

[7] Daniel S KUBERT: Universal bound of the Torsion of Elliptic Curves-London Math Soc 33 (1976) 193/237.

[8] Serge LANG. Diophantine Geometry-Inter Sciences

John wiley-New York(1968) .

[9] Barry MAZUR: Rational Isogénies of Prime Degré

Invention Mathématicae $n°44$ (1978) p $129-162$.

[10] J.S.MILNE: Elliptic Curves-Vol 1- University Michigan (1996).

[11] Jean P.SERRE: Propriétés Galoisiennes des points d'ordre fini de Courbes Elliptiques-Inventiones Mathematicae $n°15$ (1972) p $259-331$.

[12] Igor R.SHAFAREVICH: Basic Algebraic Geometry Springer-Verlag Berlin (1977).

[13] Goro SHIMURA: Introduction to the Arithmetic Théory of Automorphic Functions-Princeton.University Press-(1971) .

[14] Joseph H-SILVERMAN: The Arithmetic of Elliptic Curves-Springer $G.T.M.106(1986)$.

[15] John.TATE: The Arithmetic of Elliptic Curves- Inventiones Matheticae. $23(1975)179-206$.

[16] Edwin WEISS: Cohomology of Groups- Academic Press-New York (1969).

[17] Mohamed ZITOUNI: Géométrie Arithmétique et Algorithmique des Courbes Elliptiques (2007) OPU-Alger.

[18] Mazur:Rational isogénies of prime degrée;

Inv. Maths. $44(1978)129-162$.

[19] J.W.CASSELS, J. of Lond Math soc(1972).

[20]"On the Zêta fonction of abelian variety with complex multiplication";

$Annal.Math.94(1974)504-533$.

[21] *Weiss*, par *S. Eilenberg et S. Maclane* (Annals of Math. 48 (1947) 51 − 78).

[22](Mazur et Tate dans Inv.Math.$(1973)41-49$.

[23](Kenku dans Lond.Math.Soc.$19(1979)233-240$).