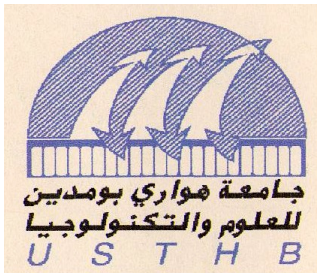
N° d'ordre : 12 / 2004 – M / MT

Université des Sciences et de la Technologie Houari Boumédiène



Faculté de Mathématiques

MEMOIRE

Présenté pour l'obtention du diplôme de **MAGISTER**
En : MATHEMATIQUES
Option : **ALGEBRE ET THEORIE DES NOMBRES.**

Par : MR. *AISSAOUI SAID*

SUJET

« Points rationnels d'ordre fini sur les courbes elliptiques »

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

Mr. BETINA Kamel	Professeur	USTHB	: Président
Mr. ZITOUNI Mohamed	Professeur	USTHB	: Directeur de thèse
Mr. KESSI Arezki	Professeur	USTHB	: Examinateur
Mr. HACHAICHI M. Salah	Maître de conférence	USTHB	: Examinateur
Mr. BENSEBAA Boualem	Chargé de cours	USTHB	: Examinateur

.

SOMMAIRE

INTRODUCTION……...…….…1

CHAPITRE I

VARIETES ALGEBRIQUES

§1-Variétés affines dans l'espace affine $\mathbb{A}^n(k)$…….....3

§2-Variétés projectives dans l'espace projectif $\mathbb{P}^n(k)$……6

§3-Diviseurs d'une variété, d'une courbe algébrique……..10

§4-Variétés abéliennes…….14

CHAPITRE II

ARITHMETIQUE DES COURBES ELLIPTIQUES

§1-Structures algébriques d'une courbe elliptique ……..……15

§2-Transformations de l'équation de Weierstrass…….……...16

§3-Invariants d'une courbe elliptique ……17

§4-Cubiques singulières et cubiques non singulières……..18

§5-Classification des cubiques planes……..26

CHAPITRE III

GROUPE DE MORDELL--WEIL ET SOUS GROUPE DE TORSION

§1-Structure de groupe de Mordell –Weil d'une courbe elliptique $E(K)$……31

§2-Sous groupe de $m-$ torsion d'une courbe elliptique ……36

§3-Homomorphismes de courbes elliptiques……...39

§4-Hauteurs et descente infinie sur une courbe elliptique ……..…41

CHAPITRE IV

VALUATION D'UN CORPS ET REDUCTION DE COURBES ELLIPTIQUES

§1-Valuations d'un corps.……45

§2-Réductions de courbes elliptiques ……..…50

§3-Courbe modulaire X_1 (13) …….……...54

REFERENCES……...……..…60

INTRODUCTION

Dans cette étude, nous nous sommes inspirés d'ouvrages et d'articles traitant les courbes elliptiques et les courbes modulaires, comme ceux de Cassels (1966), Shafarevich (1970), Shimura (1971), Tate (1974), Silverman (1986).

L'ensemble $A(K)$ des points rationnels d'une courbe elliptique A est un groupe abélien, le groupe de Mordell-Weil. Ce groupe est de type fini (Théorème de Mordell-Weil).Il est isomorphe au produit de 2 groupes abéliens

$$A(K) \cong T(A) \times \mathbb{Z}^r$$

où $T(A)$ est le groupe de torsion de la courbe elliptique A, $\mathbb{Z}^r$ désigne r copies du groupe abélien $\mathbb{Z}$ et $r = r(A) \geq 0$ est le rang de la courbe elliptique A.

L'ordre de ce groupe $A(K)$ a fait l'objet de nombreuses études suivies de résultats, pour des cas particuliers. Aucune formule générale n'a été trouvée ni pour le rang $r(A)$ de A, ni pour le groupe de torsion $T(A)$.

Pour le corps des nombres rationnels, Mazur a déterminé complètement le groupe de torsion $T(A)(\mathbb{Q})$.

Théorème

Le groupe de torsion $T(A)(\mathbb{Q})$ d'une courbe elliptique A est isomorphe à l'un des 15 groupes abéliens:

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

2) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$; pour $1 \leq m \leq 4$.

("Rational isogenies of prime degree" Inv. Math. 44 (1978) 129 – 162, Mazur) □

Nagell et Lutz ont obtenu un critère pour la détermination du groupe de torsion d'une courbe elliptique d'équation de Weierstrass

$$y^2 = x^3 + ax + b \in \mathbb{Z}[x, y]$$

avec $4a^3 + 27b^2 \neq 0$

Pour un corps de nombres K, extension finie du corps $\mathbb{Q}$, Kubert [6] a montré le

Théorème

Le groupe de torsion d'une courbe elliptique définie sur un corps de nombres K est borné par une constante qui ne dépend que du corps K. □

Une des questions posées par les spécialistes des courbes elliptiques est:
est ce qu'une courbe elliptique possède des points de tous ordres ?
Il y a des réponses partielles à cette question
Selon Billing et Mahler [2], il n'y a pas de courbes elliptiques qui possèdent un point d'ordre 11.
Ogg [10, 2] a démontré l'inexistence d'une courbe elliptique qui contient un point d'ordre 17.
Mazur et J Tate [9], en utilisant la courbe modulaire $X_1(13)$ ont montré qu'il n'existe pas de courbe elliptique qui contient un point d'ordre 13.

Dans le chapitre I, nous étudions les variétés abéliennes parce qu'une variété abélienne de dimension 1 est une courbe elliptique.

Dans le chapitre II, nous examinons l'arithmétique des courbes elliptiques: équations de Weierstrass, quelques invariants (discriminant, invariant modulaire, série L-de Dirichlet, conducteur, invariant différentiel).

Dans le chapitre III, nous établissons la structure de groupe abélien $A\,(K)$ de Mordell –Weil avec le point à l'infini comme élément neutre et la règle géométrique de 3 points colinéaires de la courbe.
Nous étudions les points d'ordre fini, les sous groupes de m-torsion $A\,(K)\,[\,m\,]$ et le groupe de torsion $T\,(\,A(K)\,)$.

Dans le chapitre IV, nous introduisons quelques notions sur les valuations d'un corps.
Nous les appliquons aux réductions des courbes elliptiques.
Nous étudions l'action du groupe modulaire Γ = SL(2, $\mathbb{Z}$) sur le demi plan supérieur $\mathbb{H}$. Les sous groupes modulaires de congruences $\Gamma_0\,(\,N\,)$, $\Gamma_1\,(\,N\,)$ et $\Gamma\,(\,N\,)$ déterminent sur ce demi plan une orbite qui est munie d'une structure de courbes modulaires $X_0\,(\,N\,)$, $X_1\,(\,N\,)$ et $X(\,N\,)$. Nous utilisons la méthode de Mazur et Tate pour montrer qu'il n'y a pas de point d'ordre 13 sur une courbe elliptique A .

CHAPITRE I VARIETES ALGEBRIQUES

Les variétés algébriques sont du domaine de la Géométrie Algébrique.
Parmi les nombreux ouvrages de Géométrie Algébrique, nous avons choisi celui de R.Hartshorne [4] pour préparer ce chapitre. Nous traiterons les ensembles algébriques, les variétés affines, les variétés projectives, les variétés abéliennes, les morphismes de variétés, les courbes algébriques et la théorie des diviseurs des courbes algébriques.

§1.Variétés affines dans l'espace affine $\mathbb{A}^n(k)$

Nous utilisons un vocabulaire géométrique pour traiter les espaces:
points, dimensions, courbes, surfaces.

Définition 1

Un n - espace affine est un ensemble $\mathbb{A}^n(k)$, formé des n - uples $a = (a_1, ..., a_n)$ d'éléments d'un corps algébriquement clos k.

$$\mathbb{A}^n(k) = \{ a, a = (a_1, ..., a_n) \in k^n \} \qquad (1)$$

L'élément $a = (a_1, ..., a_n)$ est un point à n coordonnées $a_1, ..., a_n$ dans le corps k.
A chaque espace affine $\mathbb{A}^n(k)$, de dimension n, associons l'anneau $k[X_1, ..., X_n]$ des polynômes f à n variables $X_1, ..., X_n$, sur le corps k, et les fonctions polynomiales

$$f : \mathbb{A}^n(k) \to k, \text{ de valeurs } f(a) = f(a_1, ..., a_n).$$

Par le théorème de d'Alembert – Gauss, tout polynôme

$$g(t) = u_0\, t^n + u_1\, t^{n-1} + \ldots + u_n$$

admet n racines dans un corps algébriquement clos et dans une clôture algébrique k_{alg} de k.

Ce sont ces zéros qui forment des ensembles algébriques.

Définition 2

Un ensemble algébrique d'un espace affine $\mathbb{A}^n(k)$ est un sous ensemble de l'espace $\mathbb{A}^n(k)$ formé des zéros communs d'une famille $(f_1, \ldots, f_d)$ de polynômes $f_1, \ldots, f_d$ de l'anneau $k[x_1, \ldots, x_n]$:

$$Z(f_1, \ldots, f_d) = \{\text{zeros communs de } f_1, \ldots, f_d\}$$
$$= \{ a \in \mathbb{A}^n(k),\ f_1(a) = f_2(a) = \ldots = f_d(a) = 0 \}. \quad (2)$$

Proposition1

1. *La réunion et l'intersection de deux ensembles algébriques sont des ensembles algébriques;*
2. *L'espace affine $\mathbb{A}^n(k)$ et l'ensemble vide sont des ensembles algébriques.*

Preuve de 1

Soient deux ensembles algébriques $Z_1\ (f_1, \ldots, f_c)$ et $Z_2\ (g_1, \ldots, g_d)$.

Leur réunion

$$Z_1(f_1, \ldots, f_c) \cup Z_2(g_1, \ldots, g_d) = Z(f_i\, g_j,\ 1 \le i \le c,\ 1 \le j \le d)$$

est l'ensemble des zéros communs des polynômes $f_1 g_1,\ f_1 g_2, \ldots, f_c\, g_d$.

Leur intersection

$$Z_1(f_1, \ldots, f_c) \cap Z_2(g_1, \ldots, g_d) = Z(f_1, \ldots, f_c, g_1, \ldots g_d)$$

est l'ensemble des zéros communs des polynômes $f_1, \ldots, f_c, g_1, \ldots g_d$.

Preuve de 2

L'ensemble vide est l'ensemble $Z(1)$ des zéros du polynôme $1 \in k[x_1, \ldots, x_n]$; ce polynôme 1 ne possède pas de zéros .

L'espace affine $\mathbb{A}^n(k)$ est l'ensemble $Z(0)$ du polynôme nul $0x_1 + 0x_2 + \ldots + 0x_n$. □

Les sous ensembles algébriques du n-espace affine $\mathbb{A}^n(k)$ et leurs complémentaires permettent de construire la topologie de Zariski.

Définition 3

La topologie de Zariski sur le n-espace affine $\mathbb{A}^n(k)$ est déterminée par les complémentaires des ensembles algébriques comme des ouverts.
Donc les ensembles algébriques $X \subset \mathbb{A}^n(k)$ sont des fermés.

Cette topologie n'est pas de Hausdorff. La notion de sous ensemble irréductible est introduite par la :

Définition 4

Dans un espace topologique X, un sous espace Y est irréductible s'il n'est pas la réunion, $Y = Y_1 \cup Y_2$, de deux sous espaces propres Y_1 et Y_2.
L'ensemble vide n'est pas considéré comme irréductible.

L'espace affine $\mathbb{A}^n(k)$ contient des sous espaces particuliers qui sont les variétés affines.

Définition 5

Une variété algébrique affine est un sous ensemble X de l'espace affine $\mathbb{A}^n(k)$, irréductible et fermé pour la topologie de Zariski.

Un sous ensemble ouvert de l'espace affine $\mathbb{A}^n(k)$ est une variété quasi – affine.

L'ensemble des zéros d'un polynôme $f \in k[x_1, ..., x_n]$ est un ensemble algébrique.
Considérons les polynômes f qui s'annulent en tout point d'une partie d'une variété affine.

A tout ensemble algébrique Y associons un idéal $I(Y)$ de l'anneau des polynômes $k[x_1, ..., x_n]$ avec la formule :

$$I(Y) = \{ f \in k[x_1, ..., x_n],\ f(P) = 0,\ \textit{pour tout point } P \textit{ appartenant à } Y \} \qquad (3)$$

Définition 6

Cet idéal $I(Y)$ est l'idéal de l'ensemble algébrique Y.

L'idéal $I(Y)$ de la variété Y est caractérisé par la :

Proposition 2

Soit un ensemble algébrique Y,

Y est une variété affine si et seulement si son idéal associé $I(Y)$ est premier.

Preuve

Consulter "*Algebraic Geometry*" de Hartshorne et "*Basic Algebraic Geometry*" *de* Shafarevich, par exemple. □

Exemples

1. L'espace affine $\mathbb{A}^n(k)$ est un ensemble irréductible.
2. Un polynôme irréductible $f \in k[x_1, ..., x_n]$ engendre un idéal premier, alors l'ensemble $Z(f)$ des zéros de f est irréductible.

3. Soit $f(x, y) = x^2 + 2y^2 + 3 \in \mathbb{R}[x, y]$, ce polynôme n'a pas de zéro dans le corps $\mathbb{R}$ des nombres réels.

Nous admettons que la variété affine $\mathbb{A}^n(k)$ est de dimension n.

En particulier, la droite affine $\mathbb{A}^1(k)$ est de dimension 1.

Le plan affine $\mathbb{A}^2(k)$ est de dimension 2.

§2 Variétés projectives dans l'espace projectif $\mathbb{P}^n(k)$

Nous introduisons une relation d'équivalence $\mathcal{R}$ sur l'espace affine $\mathbb{A}^{n+1}(k)$, pour construire l'espace projectif $\mathbb{P}^n(k)$.

Considérons dans l'espace affine $\mathbb{A}^{n+1}(k)$, la relation $\mathcal{R}$ entre deux points :

$$(a_0, ..., a_n) \; \mathcal{R} \; (b_0, \; ..., \; b_n)$$

si et seulement si il existe $\lambda \neq 0$ tel que

$$(b_0, \; ..., \; b_n) = \lambda \, (a_0, ..., a_n) \, .$$

Pour $\lambda = 1$, nous obtenons la réflexivité de la relation $\mathcal{R}$,

$$(a_0, \; ..., \; a_n) \; \mathcal{R} \; (a_0, \; ..., \; a_n)$$

Soit la relation

$$(a_0, ..., a_n) \; \mathcal{R} \; (b_0, \; ..., \; b_n) \qquad (4)$$

Cela implique qu'il y a un élément non nul λ tel que

$$(b_0, \ ..., \ b_n) = \lambda \ (a_0, ..., a_n) \qquad (5)$$

L'hypothèse $\lambda \neq 0$ implique $\lambda^{-1} \neq 0$, il en résulte la relation

$$(a_0, ..., a_n) = \lambda^{-1} \ (b_0, \ ..., \ b_n) \qquad (6)$$

(4) et (6) impliquent que la relation $\mathcal{R}$ est symétrique.

Pour montrer que cette relation $\mathcal{R}$ est transitive nous prenons les relations

$$(a_0, ..., a_n) \ \mathcal{R} (b_0, \ ..., \ b_n) \quad \text{et} \quad (b_0, \ ..., \ b_n) \ \mathcal{R} \ (c_0, ..., c_n) \qquad (7)$$

Par définition de $\mathcal{R}$, cette relation (7) implique qu'il y a 2 éléments non nuls λ, τ dans le corps k tels que

$$(b_0, ..., b_n) = \lambda \ (a_0, ..., a_n) \quad \text{et} \quad (c_0, ..., c_n) = \tau \ (b_0, ..., b_n) .$$

Il en résulte $$(c_0, ..., c_n) = \tau \ \lambda \ (a_0, ..., a_n) \qquad (8)$$

Par définition de $\mathcal{R}$, cette relation (8) implique

$$(a_0, ..., a_n) \ \mathcal{R} \ (c_0, ..., c_n)$$

donc la relation $\mathcal{R}$, est transitive.

Il en résulte que $\mathcal{R}$ est une relation d'équivalence sur l'espace affine $\mathbb{A}^{n+1}(k) - \{(0, \ ..., 0)\}$.

Définition 7

L'espace projectif $\mathbb{P}^n(k)$ est l'espace quotient de l'espace affine $\mathbb{A}^{n+1}(k)$ privé du point $0 = (0, 0, ..., 0)$ par cette relation d'équivalence $\mathcal{R}$:

$$\mathbb{P}^n(k) = [\mathbb{A}^{n+1}(k) - \{(0, \ ..., 0)\}] \ / \mathcal{R}$$

donc $\mathbb{P}^n(k)$ est l'ensemble des classes,

$$\text{Cl} \ (a_0, \ ..., \ a_n) = \{\lambda \ (a_0, a_1, ..., a_n), \text{ pour } \lambda \neq 0 \text{ dans } k\}$$

Exemples

1. $\mathbb{P}^1(k)) = \{\lambda \ (a_0, a_1), \ a_i \in k, \ \lambda \neq 0\}$

Nous choisissons un représentant canonique de chaque classe cl(1, 0), cl(0, 1), cl(1, 2), …

2. $\mathbb{P}^2(k) = \mathbb{A}^3 - \{(0,0,0)\}/\mathcal{R}$

$= \{$ classes des triplets $(a_0, a_1, a_2)\ \}=\{$ cl(1, 0, 0), cl(0, 1, 0),…$\}$

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

Cl(1, 1, 1) = {(1, 1, 1), (2, 2, 2), (3, 3, 3), (-1, -1, -1), …}

Cl(0, 1, 0) ={ (0, 1, 0), (0, -1, 0), (0, λ , 0), …}

3. $\mathbb{P}^3(k) = \mathbb{A}^4 - \{(0, 0, 0, 0)\} / \mathcal{R}$

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

Les racines d'un polynôme homogène $f(x_0, x_1, \ldots, x_n)$ de degré $d = 0, 1, 2, \ldots$, de l'anneau des polynômes $k[x_0, x_1, \ldots, x_n]$, forment un sous ensemble algébrique de l'espace projectif $\mathbb{P}^n(k)$.

Exemple:

Les ensembles

1) $A_1 = \{(a_0, a_1, a_2) \in \mathbb{P}^2(k), f_1(a_0, a_1, a_2) = 0$,où $f_1(x, y, z) = ax + by + cz \in k[x, y, z]\}$;

2) $A_2 = \{(a_0, a_1, a_2) \in \mathbb{P}^2(k), f_2(a_0, a_1, a_2) = 0$,

où $f_2(x, y, z) = ax^2 + by^2 + cz^2 + dxy + eyz + fxz \in k[x, y, z]\}$;

3) $A_3 = \{(a_0, a_1, a_2) \in \mathbb{P}^2(k),\ f_3(a_0, a_1, a_2) = 0$, où

$f_3(x, y, z) = d_1x^3 + d_2x^2y + d_3xy^2 + d_4y^3 + d_5x^2z + d_6xyz + d_7y^2z + d_8xz^2 + d_9yz^2 + d_{10}z^3 \in k[x, y, z]\}$,

sont des sous ensembles algébriques du plan projectif $\mathbb{P}^2(k)$.

Définition 8

Un sous ensemble X du n-espace projectif $\mathbb{P}^n(k)$ est algébrique, s'il existe un ensemble T de polynômes homogènes de l'anneau $k[X_0, \ldots, X_n]$ tel que le sous ensemble X soit égal à l'ensemble des zéros des polynômes de l'ensemble T .

$$X = Z(T) = \{P\ ,\ f(P) = 0, \textit{ pour tout élément } f \in T\}.$$

Ces ensembles algébriques permettent de construire une topologie de Zariski sur l'espace projectif $\mathbb{P}^n(k)$.

Cette topologie implique la construction de variétés algébriques projectives .

Définition 9

Une variété algébrique projective est un sous ensemble algébrique irréductible de l'espace projectif $\mathbb{P}^n(k)$ muni de la topologie de Zariski.

Un sous ensemble ouvert d'une variété algébrique projective est une variété quasi-projective.

La dimension d'une variété projective est égale à sa dimension en tant qu'espace topologique.

Introduisons la notion d'anneau de fonction associé à une variété.

A tout anneau $A = k[X_1, X_2, ..., X_n]$ de polynômes correspond le corps $k(X_1, X_2, ..., X_n)$ des fonctions rationnelles $f = p_1 / p_2$ de deux polynômes de l'anneau A.

Une courbe plane, algébrique, d'équation implicite $f(x, y) = 0$ est rationnelle s'il existe deux fonctions rationnelles $t \to \varphi(t)$, $t \to \psi(t)$, non constantes, qui satisfont l'équation

$$f(\varphi(t), \psi(t)) = 0 .$$

Définition 10

Une fonction $f : V \to k$ d'une variété quasi - projective V est régulière en un point P de V s'il existe un voisinage ouvert U de ce point P, et deux polynômes g, $h \in k[X_0, ..., X_n]$, tels que $h \neq 0$ et $f = \frac{g}{h}$ sur l'ouvert U.

Une fonction $f : V \to k$ est régulière sur V si elle est régulière en chacun des points de V.

Les fonctions régulières f sur V forment un anneau.

Définition 11

L'anneau local d'un point P d'une variété V est l'ensemble des fonctions régulières

$$f : V \to k \text{ qui satisfont :}$$

deux sous ensembles ouverts U_1 et U_2 de V, contenant le point P, deux fonctions régulières

$$f : U_1 \to k \quad \text{et} \quad g : U_2 \to k$$

sont équivalentes si $f = g$ sur l'intersection $U_1 \cap U_2$

Les variétés algébriques dans l'espace projectif $\mathbb{P}^n$ sont classifiées par leur dimension *n*

Une variété projective de dimension un est une courbe algébrique;
Une variété projective de dimension deux est une surface;
Une variété projective de dimension $n \succ 2$ est une hypersurface.

La définition d'une courbe X implique que X est définie par une équation implicite, homogène de degré *d*, égal ou différent de la dimension de l'espace projectif $\mathbb{P}^n(k)$.

Exemple

$F(x, y, z) = y^2z+a_1xyz+a_3yz^2- x^3 - a_2x^2z - a_4xz^2 - a_6z^3 = 0$ est l'équation d'une cubique plane.

§3 Diviseurs d'une variété, d'une courbe

Il y a plusieurs manières de définir les diviseurs ("*Algebraic Geometry*" de Hartshorne, etc…).

Considérons une courbe projective, non singulière, C dans le plan projectif $\mathbb{P}^2(k)$

Chaque ligne L du plan $\mathbb{P}^2(k)$ coupe la courbe C en un nombre fini de points $P_1, P_2, ..., P_d$ avec les multiplicités $n_1, n_2, ..., n_d$.

Définitions 12

(1) *Un diviseur d'une courbe plane C est une somme formelle*

$$D = n_1P_1 + n_2P_2 + ... + n_dP_d.$$

où les n_i sont égaux aux ordres de multiplicités des points d'intersection de la ligne L par la courbe C.

Lorsque la ligne L varie, la somme formelle D décrit l'ensemble $Div(C)$ des diviseurs de C

Selon Shafarevich, un diviseur d'une fonction rationnelle $f(x)=\frac{g(x)}{h(x)}$

qui admet des zéros multiples d'ordre n_i aux zéros du numérateur $g(x)$ et des pôles multiples d'ordre m_j aux zéros du dénominateur $h(x)$ est une somme formelle

$$D = n_1P_1 + n_2P_2 + ... + n_dP_d - m_1P_1' - m_2P_2' - ... - m_sP_s'.$$

(2) *Un diviseur d'une variété irréductible C est une somme formelle*

$$D = n_1 C_1 + n_2 C_2 + ... + n_d C_d ,$$

où $C_1, C_2, ..., C_d$ sont des sous variétés de C de codimension 1,

et où $n_1, n_2, ..., n_d$ sont des entiers rationnels.

L'ensemble $Div(X)$ des diviseurs d'une variété irréductible X, est muni d'une structure de groupe abélien avec les opérations :

La somme de deux diviseurs D et D' est égale au diviseur $D'' = D + D'$:

$$D = n_1 P_1 + n_2 P_2 + ... + n_d P_d \quad \text{et} \quad D' = n'_1 P_1 + n'_2 P_2 + ... + n'_d P_d .$$

$$D + D' = (n_1 + n'_1) P_1 + (n_2 + n'_2) P_2 + ... + (n_d + n'_d) P_d$$

Le symétrique du diviseur D est le diviseur - D

$$-D = -n_1 P_1 - n_2 P_2 - ... - n_d P_d .$$

Le diviseur nul $0 = 0P_1 + 0P_2 + ... + 0P_d$ est l'élément neutre de l'addition des diviseurs.

Il en résulte que l'ensemble $Div(X)$ des diviseurs d'une variété irréductible X engendre un groupe abélien avec la loi :

$$(D, D') \rightarrow D + D'$$

La commutativité de l'addition dans l'anneau des entiers $\mathbb{Z}$ implique que le groupe $Div(X)$ des diviseurs de X est abélien .

Nous avons démontré la

Proposition 3

L'ensemble $Div(X)$ des diviseurs d'une variété irréductible X est un groupe abélien.

Introduisons une relation d'équivalence $\sim$ sur le groupe $Div(X)$ des diviseurs d'une variété X .

Définition 13

Deux diviseurs D et D' de la variété irréductible X sont linéairement équivalents si leur différence est égale au diviseur (f) d'une fonction rationnelle f sur X :

$$D \sim D' \text{ si et seulement si } D - D' = (f) .$$

Les diviseurs sont de plusieurs types

Définition 14

Un diviseur $D = n_1P_1 + n_2 P_2 + ... + n_d P_d$ *est effectif lorsque tous les entiers* n_i *sont positifs ou nuls,* $n_i \geq 0$ *pour* $i = 1, 2, 3, ..., d$.

D *premier lorsqu' il est de la forme* $D = nP$ *sur une courbe,* $D = nC$ *sur une variété.*

D *est principal lorsqu'il est égal au diviseur* (f) *d'une fonction* f.

Les diviseurs construits avec ces définitions sont des diviseurs de Weil.
Il existe d'autres diviseurs qui ne sont pas construits comme les diviseurs de Weil : ce sont les diviseurs de Cartier.
Un diviseur possède un invariant qui est son degré.

Définition 15

Le degré d'un diviseur $D = n_1P_1 + n_2 P_2 + ... + n_d P_d$ *est la somme*

$$\deg(D) = \sum_{1=1}^{d} n_i \qquad (9)$$

Exemple

Soit une courbe elliptique E d'équation de Weierstrass projective

$$y^2z + a_1 xyz + a_3 yz^2 = x^3 + a_2 x^2 z + a_4 xz^2 + a_6 z^3.$$

Considérons une sécante L qui coupe la courbe E en 3 points P_1 , P_2 , P_3 .

Le point à l'infini O_E appartient à la courbe E.

Les diviseurs de L et le diviseur associé au point O_E forment deux diviseurs linéairement équivalents

$$(P_1) + (P_2) + (P_3) \cong 3(O_E)$$

Proposition 4

L'ensemble $Div(C)$ *des diviseurs d'une courbe irréductible C est un groupe abélien additif d'élément neutre le diviseur* $D = 0$.

Cette proposition est valable pour une variété projective et pour un schéma.

Définition 16

1. *Le groupe de Picard Pic (C) d'une courbe algébrique* C *est le quotient du groupe* $Div(C)$ *des*

diviseurs de la courbe C par le sous groupe de diviseurs principaux $P(C)$ du groupe $Div(C)$

$$Pic(C) = Div(C)/P(C).$$

2. *Le groupe de Picard $Pic^0(C)$ de degré 0, est le quotient du groupe $Div^0(C)$ des diviseurs de degré 0 de la courbe C par le sous groupe $P(C)$ des diviseurs principaux du groupe $Div(C)$.*

$$Pic^0(C) = Div^0(C)/P(C). \qquad (10)$$

Parmi les invariants d'une courbe algébrique, il figure le genre de cette courbe.

Définition 17

Le genre d'une courbe algébrique projective plane, C, non singulière de degré d est égal à

$$g(C) = \frac{1}{2}(d-1)(d-2). \qquad (11)$$

Lorsque la courbe admet s points singuliers, alors son genre est égal à

$$g(C) = \frac{1}{2}(d-1)(d-2) - s. \qquad (12)$$

(Cf. "*Algebraic Geometry*" exemple 8.20.3, Hartshorne);

(Cf. "*Basic Algebraic Geometry"* p .173, Shafarevich).

Exemple

1) Une cubique singulière a une équation de degré d =3 et admet s =1 point singulier.
   Son genre est donc égal à

$$g(C)=\frac{1}{2}(3-1)(3-2)-1=0.$$

2) Une courbe elliptique C est une cubique non singulière, donc son genre est égal à

$$g(C)=1$$

Le genre d'une courbe C, d'une variété X, intervient dans le théorème de Riemann – Roch, avec les diviseurs de C, de X.

A tout diviseur D, nous associons l'ensemble $L(D)$,

$$L(D) = \{f \in k(C), div(f)+D \geq 0\} \cup \{0\}. \qquad (13)$$

Cet ensemble $L(D)$ est un k - espace vectoriel de dimension finie $l(D)$.

Cet espace vectoriel $L(D)$, sa dimension $l(D)$ et le genre g de la courbe plane C sont liés par le :

Théorème de Riemann – Roch

Soit une courbe plane C, un diviseur D de C, de degré $\deg(D)$ et l'espace vectoriel $L(D)$ associé à D de dimension $l(D)$

Alors il existe un entier g qui satisfait la relation

$$l(D) \geq \deg(D) + 1 - g,$$

avec égalité si $\deg(D) \succ 2g-2$.

Définition 18

L'entier g de cette formule est le genre de la courbe C.

§ 4 Variétés abéliennes

Certaines variétés projectives peuvent être munies d'une structure de variété abélienne.

Définition 19

Une variété abélienne est une variété projective X munie d'une structure de groupe abélien

$$X \times X \to X$$

$$(x, y) \mapsto x + y$$

et d'une application continue $X \to X$ de valeur $x \mapsto x^{-1}$

Exemple 1

Dans le groupe $Div(X)$ des diviseurs d'une variété X le groupe

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

des classes des diviseurs de X est une variété abélienne.

("*Basic Algebraic Geometry"* p 155, Shafarevich).

Définition 20

Une variété abélienne simple est une variété abélienne A qui n'a pas d'autre sous variété abélienne qu'elle même et la variété réduite au point 0.

Exemple 2

Les cubiques planes non singulières sont des variétés abéliennes de dimension 1, donc des courbes elliptiques.

CHAPITRE II ARITHMETIQUE DES COURBES ELLIPTIQUES

La place des courbes elliptiques dans les mathématiques a été soulignée par plusieurs auteurs (Shimura, Silverman, Koblitz, Cassels, etc.) qui ont mis en relief les liens avec la Théorie des Nombres, l'Analyse Complexe et la Géométrie Algébrique.

§1-Structures algébriques

Une courbe elliptique admet plusieurs structures algébriques :

Structure de variété abélienne de dimension 1,

Structure de courbe projective irréductible de genre 1,

Structure de schéma séparé, non singulier, de dimension 1,

Structure de groupe abélien de type fini .

Chacune de ces structures algébriques peut être prise comme définition, nous choisissons la :

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

$$E: y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6 \in k\,[\,x,\,y\,]; \qquad (1)$$

les deux variables x et y, racines de l'équation algébrique (1) sont des éléments d'une clôture algébrique $k_{a\lg}$ d'un corps commutatif k, global, local ou fini .

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

L'équation de Weierstrass se distingue de l'équation ordinaire d'une cubique.

$$E\ :\ s_1\,y^3+s_2y^2x+s_3yx^2+s_4x^3+s_5y^2+s_6\,y\,x+s_7\,x^2+s_8\,y+s_9x+s_{10}\ =0\,.$$

Cette équation contient 10 coefficients $s_1,\ s_2,\ s_3,\ s_4, s_5, s_6,\ s_7,\ s_8,\ s_9,\ s_{10}$.

§1.1. Influence du corps de base de la courbe elliptique sur l'étude de cette courbe

Le corps $\mathbb{Q}$ des nombres rationnels influe sur les courbes elliptiques par les équations diophantiennes, les valuations, les fonctions arithmétiques (fonctions d'Euler, de Riemann, de Möbius, …)

Les corps de nombres algébriques influent sur les courbes elliptiques par les entiers, les classes d'idéaux, les valuations, les discriminants, les groupes de Galois, la décomposition des idéaux, la ramification,… etc.

Le corps des nombres complexes influe sur les courbes elliptiques par l'Analyse Complexe (fonctions elliptiques, fonctions modulaires, fonctions automorphes, …) et par la Géométrie Algébrique, (variétés abéliennes, diviseurs, genre,…).

Les corps de fonctions, les corps locaux, les corps finis influent sur les courbes elliptiques par leurs propriétés et leurs théories.

§2. Transformations de l'équation de Weierstrass

Cherchons les transformations qui éliminent des monômes ou des coefficients dans l'équation (1).

La transformation qui élimine les monômes en y et en xy a pour formules :

$$x = X\ ,\ y\ = \frac{1}{2}\,(Y - a_1 X - a_3) \qquad (2)$$

avec la condition car$(k) \neq 2$.

En faisant les calculs, nous obtenons l'équation:

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

Les coefficients b_{2i} sont des polynômes « homogènes » de degré $2i$

de l'anneau $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$.

$$b_2 = a_1^2 + 4a_2\ \ ;\ \ b_4 = 2a_4 + a_1 a_3\ ;\ \ b_6 = a_3^2 + 4a_6\ . \qquad (4)$$

Dans l'équation (3), le coefficient 4 et le monôme en x^2 sont éliminés avec la transformation :

$$X\ =\ \frac{x - 3b_2}{36}\ ;\ Y\ = \frac{y}{108} \qquad (5)$$

avec la condition car$(k)\ \neq 2, 3$.

En faisant les calculs, nous obtenons l'équation:

$$E_2 \quad : \quad y^2 = x^3 - 27\,c_4 x - 54\,c_6 \tag{6}$$

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

$$c_4 = b_2^2 - 24 b_4 \ ;$$

$$c_6 = 36 b_2 b_4 - b_2^3 - 216 b_6 \ ;$$

Il existe d'autres modèles d'équations d'une courbe elliptique :

1- Le modèle de Legendre

$$E_3 \ : \quad y^2 = x(x-1)(x-\lambda) \tag{7}$$

avec la condition $\lambda \neq 0, 1$

2-Le modèle

$$E_4 \ : \quad y^2 = (x-e_1)(x-e_2)(x-e_3)\,. \tag{8}$$

avec la condition $e_i \neq e_j$ *pour* $i \neq j$ *et* $i, j = 1,2,3$

§3. Invariants d'une courbe elliptique

Chaque courbe elliptique possède de nombreux invariants , nous en définissons cinq

Définition 3

1.*Le discriminant* d'une courbe elliptique E est le polynôme ''homogène'' de degré 12 de l'anneau $\mathbb{Z}[b_2, b_4, b_6, b_8]$.

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

où l'on a posé :

$$4\,b_8 = b_2\,b_6 - b_4^2 \ ;$$

2.*L'invariant différentiel* est l'élément différentiel

$$\omega(E) = \frac{dx}{2y + a_1 x + a_3}$$

$$= -\frac{dy}{3x^2 + 2a_2\,x + a_4 - a_1 y} \tag{10}$$

3.*L'invariant modulaire* de E est l'élément du corps k

$$j(E) = \frac{c_4^3}{\Delta(E)} \quad . \tag{11}$$

4.*Le conducteur* de la courbe elliptique E est le produit de facteurs premiers

$$N(E) = \prod_{p \in S_E} p^{n(p)} \qquad (12)$$

où S_E est l'ensemble des nombres premiers p en lesquels E a une mauvaise réduction, c'est donc l'ensemble des diviseurs premiers de $\Delta(E)$.L'exposant $n(p)$ satisfait, selon Velu les conditions $n(p) = 0$ si p ne divise pas $\Delta(E)$

$n(p) = 1$ si E a une réduction multiplicative

$n(p) = 2$ si E a une réduction additive et $p \geq 5$.

$2 \leq n(2) \leq 8$ si E a une réduction additive en $p = 2$

$2 \leq n(3) \leq 5$ si E a une réduction additive en $p = 3$

5.*Série L-de Dirichlet*

La série L de Dirichlet – Hasse d'une courbe elliptique E sur le corps $\mathbb{Q}$ des nombres rationnels est le produit eulerien complexe :

$$L_E(s) = \prod_{p \nmid \Delta} \frac{1}{1 - t_p p^{-s}} \prod_{p \mid \Delta} \frac{1}{1 - t_p p^{-s} + p^{1-2s}} \qquad (13)$$

où $t_p = 1 + p - A_p$, p nombre premier,

A_p est le nombre de points rationnels de la courbe réduite $\tilde{E}$ sur le corps fini $\mathbb{F}_p$.

§5. Cubiques singulières et cubiques non singulières

Pour déterminer les points singuliers du polynôme f de l'équation $y^2 = f(x)$, nous disposons du résultant des polynômes f et f'

§5.1 Résultant de deux polynômes.

Définition 4

Soient deux polynômes $f(x)$ et $g(x)$ à coefficients dans un corps k :

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$. *de degré n ;*

et $g(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0$. *de degré m .*

Le résultant de ces deux polynômes f et g est le déterminant $\mathrm{Res}(f, g)$ d'ordre $m + n$:

$$Res(f, g) = \begin{vmatrix} a_n & a_{n-1} & . & . & . & a_0 & 0 & . & . & 0 \\ 0 & a_n & a_{n-1} & . & . & . & a_0 & 0 & . & 0 \\ 0 & 0 & a_n & & & & & & & 0 \\ . & . & . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & & & & & a_0 \\ b_m & b_{m-1} & b_{m-2} & . & . & . & b_0 & 0 & . & 0 \\ 0 & b_m & . & . & . & . & b_1 & b_0 & 0 & 0 \\ . & . & . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & . & & & b_1 & b_0 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \} \, m \text{ lignes} \\ \\ \\ \\ \\ \} \, n \text{ lignes} \\ \\ \\ \\ \end{matrix}$$

Le résultant possède plusieurs propriétés, citons les sans démonstration.

Théorème 1

Le résultant $\mathrm{Res}(f, g)$ *est égal à*

$$\mathrm{Res}(f, g) = a_n^m \, b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (t_i - u_j), \tag{14}$$

où les t_i *sont les zéros du polynôme* f *et les* u_j *sont les zéros du polynôme* g . □

Cette formule du résultant implique une condition pour que $\mathrm{Res}(f, g)$ soit nul

Corollaire

Le résultant $\mathrm{Res}(f, g)$ *de deux polynômes* f *et* g *est nul si et seulement si ces deux polynômes ont un zéro commun.* □

Définition 5

Le discriminant d'un polynôme

$$f(x) = a(x - t_1)(x - t_2) \ldots (x - t_n)$$

de degré n *, est égal à :*

$$disc(f) = (-1)^{\frac{n(n-1)}{2}} \, a^{2n-2} \prod_{1 \le i \prec j \le n} (t_i - t_j)^2 \tag{15}$$

Le résultant d'un polynôme f et de sa dérivé f' est lié au discriminant de ce polynôme par la :

Proposition 2

Le résultant d'un polynôme $f(x)$ et de sa dérivé $f'(x)$ est égal à

$$\begin{aligned} \mathrm{Res}(f,\ f') &= (-1)^{\frac{n(n-1)}{2}}\ a^{2n-1} \prod_{i<j} (t_i - t_j)^2 \\ &= (-1)^{\frac{n(n-1)}{2}}\ a\ \ dis(f). \end{aligned}$$

Pour les démonstrations, consulter «*Algebra V §10 the résultant* » de S. Lang, «*Introduction to algebra*» de Kostrikine, par exemple.

□

Exemples

1. Polynôme quadratique $f(x) = ax^2 + bx + c$; $a \neq 0$,

et sa dérivé $f'(x) = 2a\ x + b$

Le résultant $\mathrm{Res}(f, f')$ de f et f' est égal à

$$\begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = -\ a\ (b^2 - 4\ a\ c)\ ;$$

D'où $\mathrm{disc}(f) = b^2 - 4ac$

C'est le discriminant usuel d'un polynôme de degré 2.

2 Polynôme cubique**.** $f(x) = d_0\ x^3 + d_1 x^2 + d_2 x + d_3$,

Par le calcul, nous obtenons la valeur du résultant :

$$Res(f,\ f') = d_0\ [\ 18 d_0 d_1 d_2 d_3 + d_1^2 d_2^2 - 4 d_1^3 d_3 - 27 d_0^2 d_3^2\ ].$$

Son discriminant est égal à

$$disc(f) = 18 d_0 d_1 d_2 d_3 + d_1^2 d_2^2 - 4 d_1^3 d_3 - 27 d_0^2 d_3^2. \qquad (16)$$

3. Polynôme cubique $f(x) = x^3 + px + q$.

La définition du résultant et le calcul d'un déterminant impliquent la valeur

$$R(f,\ f') = \begin{vmatrix} 1 & 0 & p & q & 0 \\ 0 & 1 & 0 & p & q \\ 3 & 0 & p & 0 & 0 \\ 0 & 3 & 0 & p & 0 \\ 0 & 0 & 3 & 0 & p \end{vmatrix} = 4p^3 + 27q^2$$

Le discriminant est égal à $disc\ (f) = -(4p^3 + 27q^2)$

("*Algebra"* p 141, de S.Lang,)

4. Polynôme cubique $f(x) = 4x^3 + b_2 x^2 + 2b_4 x + b_6$,

Avec les formules du $Res\ (f,\ f')$ et du discriminant de f nous obtenons

$$disc(f) = 16[9\ b_2 . b_4\ b_6 - b_2^2\ b_8 - 8\ b_4^3 - 27\ b_6^2].$$

La formule (9) du discriminant $\Delta(E)$ de la courbe elliptique E implique la relation

$$disc\ (f) = 16\ \Delta(E) \qquad (17)$$

Proposition 3

Soit une courbe elliptique E d'équation de Weierstrass

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

Le discriminant $disc(f)$ du polynôme f et le discriminant $\Delta(E)$ de la courbe elliptique E satisfont la relation

$$\text{disc}(f) = 16\ \Delta(E) \qquad \square$$

§5.2 Points singuliers d'une cubique plane

La théorie des courbes algébriques implique que toute cubique possède 1 point singulier ou zéro point singulier .

Les coordonnées du point singulier éventuel d'une cubique d'équation implicite

$$f\ (x, y) = 0$$

sont les racines du système de 3 équations algébriques :

$$f\ (x, y) = 0,\ f'_x (x, y) = 0\ ,\ f'_y (x, y) = 0\ . \qquad (18)$$

Si le système n'admet pas de solutions, la cubique est non singulière; c'est une courbe elliptique, par définition.

La nature géométrique de ce point singulier est déterminée par le nombre de tangentes à la courbe en ce point singulier .

Ce point singulier est un nœud, si la courbe possède deux tangentes distinctes en ce point .

Ce point singulier est un point de rebroussement, si la courbe possède deux tangentes confondues en ce point.

Un critère de reconnaissance d'une cubique singulière, repose sur la valeur de son discriminant .

Proposition 4

Soit une cubique plane A, d'équation de Weierstrass

$$A : y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6.$$

1) Le point à l'infini, $O_A=(\infty,\infty)$ dans le plan affine $\mathbb{A}^2(k)$ et $O_A=(0,1,0)$ dans le plan projectif $\mathbb{P}^2(k)$, est un point non singulier de la cubique A.

2) La cubique A est une courbe elliptique si et seulement si son discriminant $\Delta(A)$ n'est pas nul.

Preuve de 1)

Dans le plan projectif $\mathbb{P}^2(k)$, la cubique A a pour équation un polynôme implicite

$$g(x,\ y,\ z) = y^2z+a_1xyz+a_3yz^2-x^3-a_2x^2z-a_4xz^2-a_6.z^3 = 0$$

Les trois dérivées partielles de ce polynôme sont égales à :

$$\begin{aligned} g'_x(x,y,z) &= a_1yz-3x^2-2a_2xz-2a_4z^2 \\ g'_y(x,y,z) &= 2yz+a_1xz+a_3z^2 \\ g'_z(x,y,z) &= y^2+a_1xy+2a_3yz-a_2x^2-2a_4xz-3a_6z^2 \end{aligned} \qquad (1)$$

Au point $O_A=(0,1,0)$, ce système (1) prend les valeurs :

g(0,1,0) = 0, implique que le point $O_A=(0,1,0)$ est sur la courbe A

$g'_z(0,1,0) = 1$, implique que le point à l'infini est non singulier.

Preuve de « La cubique A est une courbe elliptique » implique « $\Delta(A) \neq 0$ ».

Soit une courbe elliptique A d'équation de Weierstrass

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

Puisque la courbe n'a pas de point singulier le polynôme $f(x)$ admet 3 racines simples .

Par la théorie des racines d'un polynôme $f(x)$, sa dérivée $f'(x)$ n'a pas de zéro commun avec $f(x)$. Il en résulte que le résultant $Res(f, f') \neq 0$.

La relation $disc(f) = c\, Res(f, f')$ entre résultant $Res(f, f')$ et $disc(f)$ et la relation $disc(f) = 16\,\Delta(A)$ entre discriminant de $f(x)$ et le discriminant de la courbe A impliquent $\Delta(A) \neq 0$.

□

Proposition 5

Soit une cubique plane A d'équation de Weierstrass

$$y^2 = f(x)$$

de discriminant $\Delta(A)$ *et d'invariant* $c_4(A) = b_2^2 - 24b_4$

1) *La cubique A admet un nœud si et seulement si* $\Delta(A) = 0$ *et* $c_4(A) \neq 0$.
2) *La cubique A admet un point de rebroussement si et seulement si* $\Delta(A) = 0$ *et* $c_4(A) = 0$.

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

Soit une cubique A d'équation de Weierstrass:

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

L'hypothèse «A admet un nœud» implique que la cubique A est singulière .

Par la proposition 4, $\Delta(A) = 0$

Une cubique A admet deux tangentes distinctes au nœud

Les pentes des tangentes au nœud sont égales à la dérivée

$$y' = \frac{(6x^2 + b_2 x + b_4)}{y} = \frac{N(x)}{y} \qquad (19) \quad .$$

L'hypothèse de deux tangentes distinctes implique deux valeurs de y'

Cela implique que le polynôme $N(x)$ admet deux racines distinctes, il en résulte que son discriminant est différent de zéro.

En faisant les calculs, nous obtenons

$$dis(N(x)) = b_2^2 - 24b_4 = c_4(A) \neq 0 .$$ □

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

Soit une cubique A de discriminant $\Delta(A) = 0$.

Par la proposition (4), $\Delta(A) = 0$ implique que la cubique est singulière .

La relation $c_4 = b_2^2 - 24b_4 \neq 0$, et la proposition 3 impliquent que la courbe possède deux tangentes distinctes en ce point. Donc ce point singulier est un nœud.

□

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

Par la proposition 4, la cubique singulière a un discriminant $\Delta(A) = 0$

L'hypothèse de deux tangentes confondues implique que le polynôme $N(x)$ de la formule (19) admet une racine double, d'où son discriminant $disc\,(N(x))$ est nul.

$$disc\,(N(x)) = b_2^2 - 24b_4 = c_4(A) = 0 .$$

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

Le discriminant $c_4 = b_2^2 - 24b_4$ du polynôme $N(x)$ est nul implique

le polynôme $N(x)$ possède une solution double et deux tangentes confondues,

d'où la cubique admet un point de rebroussement.

□

Exemple 1

Cubique E_1 d'équation de Weierstrass

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

Calcul des invariants ; nous obtenons les valeurs

$b_2 = 4$; $b_4 = b_6 = b_8 = 0$;

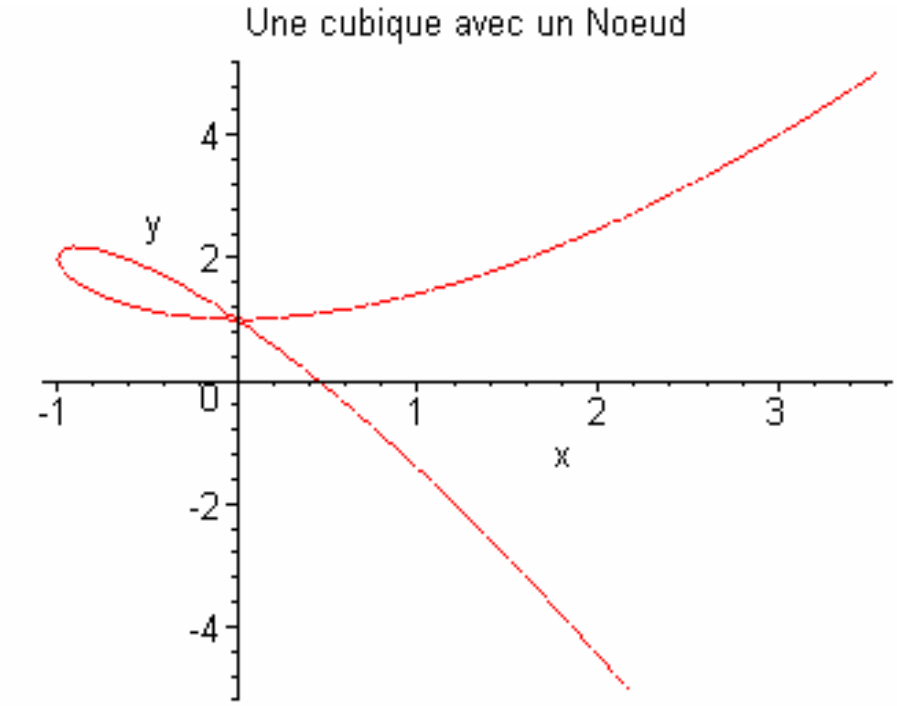
$c_4(E_1) = 16$; $\Delta(E_1) = 0$; cela implique que la cubique possède un nœud.

Tableau des coordonnées réelles de quelques points de la cubique.

X	0	-1	1	-2
$y^2 + 2xy - 2y = x^3 + 2x - 1$	$y^2 - 2y = -1$	$y^2 - 4y = -4$	$y^2 = 2$	$y^2 - 6y = -13$
Y	1, racine double	2, racine double	$\pm\sqrt{2}$	n'existe pas.

X	2	-1/2	- 4/5
$y^2+2xy-2y=x^3+2x-1$	$y^2+2y=11$	$y^2-3y=-\frac{17}{8}$	$y^2-\frac{18}{5}y=-\frac{139}{125}$
Y	$-1\pm\sqrt{14}$	$3\pm\frac{\sqrt{2}}{2}$	$\frac{2}{5}\left(9\pm\sqrt{\frac{66}{5}}\right)$

Le point (0, 1) est le nœud



Exemple 2

Cubique E_2 d'équation de Weierstrass

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

avec le calcul des invariants, nous obtenons

$b_2=12;\ b_4=6;\ b_6=4;\ b_8=3$

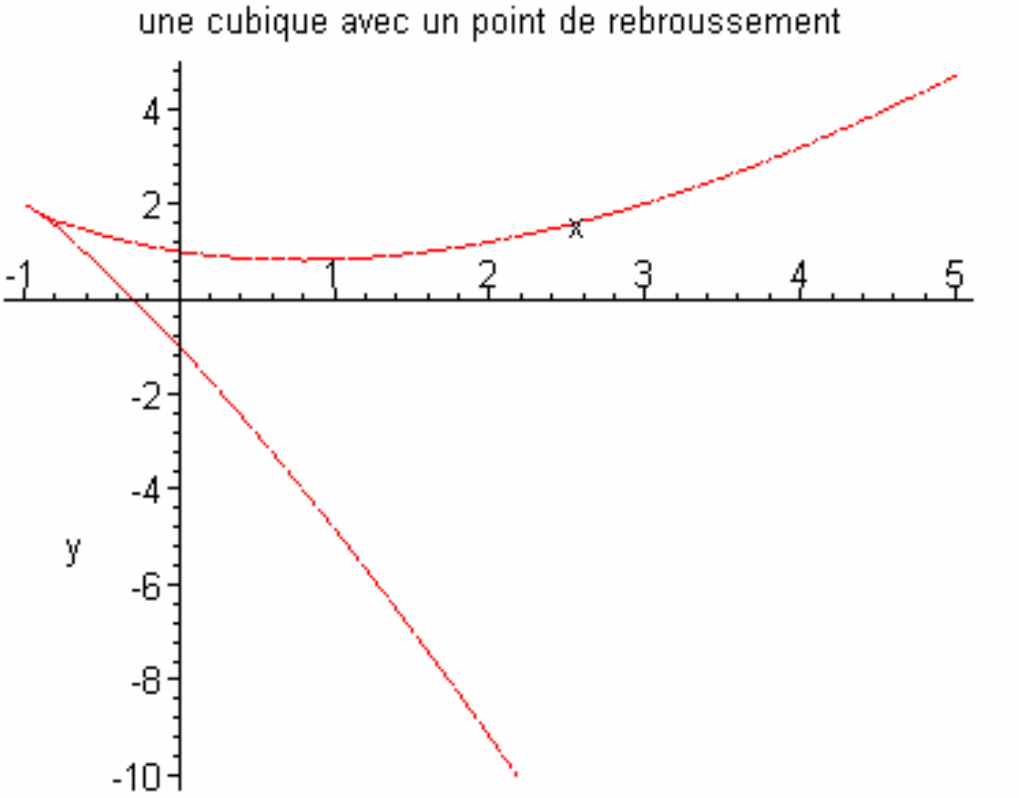
$c_4(E_2)=c_6(E_2)=0;\ \Delta(E_2)=0$

Ces valeurs impliquent que la cubique E_2 admet un point de rebroussement

Tableau des coordonnées réelles de quelques points de la cubique E_2

x	0	-1	1	-2
$y^2+4xy=x^3-x^2+3x+1$	$y^2=1$	$y^2-4y=-4$	$y^2+6y=0$	$y^2-6y=-6$
y	-1, 1	2 = racine double.	-6, 0	$3\pm\sqrt{3}$.

- 0.2	- 0.3	- 1/4
$y^2 - 0{,}8y = 0.352$	$y^2 - 1.2y = -0.017$	$y^2 - y = \frac{11}{64}$
$\frac{1}{2}\sqrt{\frac{3}{2}}$	$-0.6 \pm \sqrt{0.312}$	$-0.4 \pm \sqrt{0.043}$



§6 Classification des courbes elliptiques suivant le nombre de points d'intersection avec l'axe Ox

Un polynôme f du 3ème degré admet, soit 3 racines réelles, soit une racine réelle et deux racines complexes conjuguées. Il en résulte qu'une courbe elliptique coupe l'axe Ox en 3 points ou en un seul point .

Soit une courbe elliptique d'équation de Weierstrass

$$E : y^2 = x^3 + Ax + B \in \mathbb{R}[x, y],$$

avec la condition

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

Déterminons le nombre de points d'intersection de la courbe E avec l'axe Ox suivant le signe de Δ :

Proposition 6

1.*Une courbe elliptique* E *coupe l'axe Ox en 3 points si et seulement si* $\Delta(E) \succ 0$.

2.Une courbe elliptique E *coupe l'axe Ox en un seul point si et seulement si* $\Delta(E) \prec 0$.

Preuve de « E coupe l'axe Ox en 3 points» implique « $\Delta(E) \succ 0$ ».

Soit une courbe elliptique d'équation de Weierstrass

$$y^2 = x^3 + Ax + B = g(x) \in \mathbb{R}[x, y]$$

D'après la proposition 3, le discriminant de la courbe elliptique $\Delta(E)$ et le discriminant $disc(g)$ du polynôme g satisfont la relation

$$disc(g) = 16\ \Delta(E)$$

L'hypothèse « 3 points d'intersections » implique que le polynôme $g(x)$ admet 3 racines réelles

$$g(x) = (x - e_1)(x - e_2)(x - e_3)$$

Par définition, le discriminant d'un polynôme $g(x)$ est égal à :

$$disc(g) = \prod_{1 \le i \prec j \le 3} (e_i - e_j)^2$$

L'hypothèse « e_i » réel implique les carrés $(e_i - e_j)^2 \succ 0$

Il en résulte $disc(g) \succ 0$ et $\Delta(E) \succ 0$.

Preuve de « E coupe Ox en un seul point » implique « $\Delta(E) \prec 0$ »

Soit une courbe elliptique E d'équation de Weierstrass

$$E: \ y^2 = x^3 + ax^2 + bx + c = f(x) \in \mathbb{R}[x, y] \qquad (20)$$

Par l'hypothèse E coupe l'axe Ox en un seul point $(e, 0)$ (21)

(20) et (21) impliquent la factorisation de $f(x)$

$$y^2 = (x - e)(x^2 + rx + s), \text{ avec } r^2 - 4s \prec 0,$$

$a = r - e, \quad b = s - er, \quad c = -se$

Le polynôme $(x^2 + rx + s)$ admet 2 racines complexes conjuguées :

$$e_1' = -\frac{1}{2}(r + i\sqrt{4s - r^2})$$

$$e_2' = -\frac{1}{2}(r - i\sqrt{4s - r^2})$$

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

$$disc(g) = (e - e_1')^2 (e - e_2')^2 (e_1' - e_2')^2$$

$$= [(e + \frac{1}{2}r)^2 + \frac{1}{4}(4s - r^2)]^2 (-(4s - r^2)) \prec 0. \square$$

Exemple 1

Soit une courbe elliptique E d'équation de Weierstrass

$$E : y^2 + xy - 9y = x^3 - 5x^2 - 7x + 3$$

Avec le calcul des invariants, nous obtenons

$b_2 = -19$; $b_4 = -23$; $b_6 = 93$; $b_8 = -574$;

$\Delta(E_2) = 158713 \succ 0$

Tableau des coordonnées réelles de quelques points de la courbe elliptique E

X	0	0.4	1
$y^2 + xy - 9y = x^3 - 5x^2 - 7x + 3$	$y^2 - 9y = 3$	$y^2 - 8.6\,y = -0.536$	$y^2 - 8\,y = -8$
Y	$\approx 4.5 \pm 4.82$	$\approx 4.3 \pm 4.24$	$\approx 4 \pm 2.83$

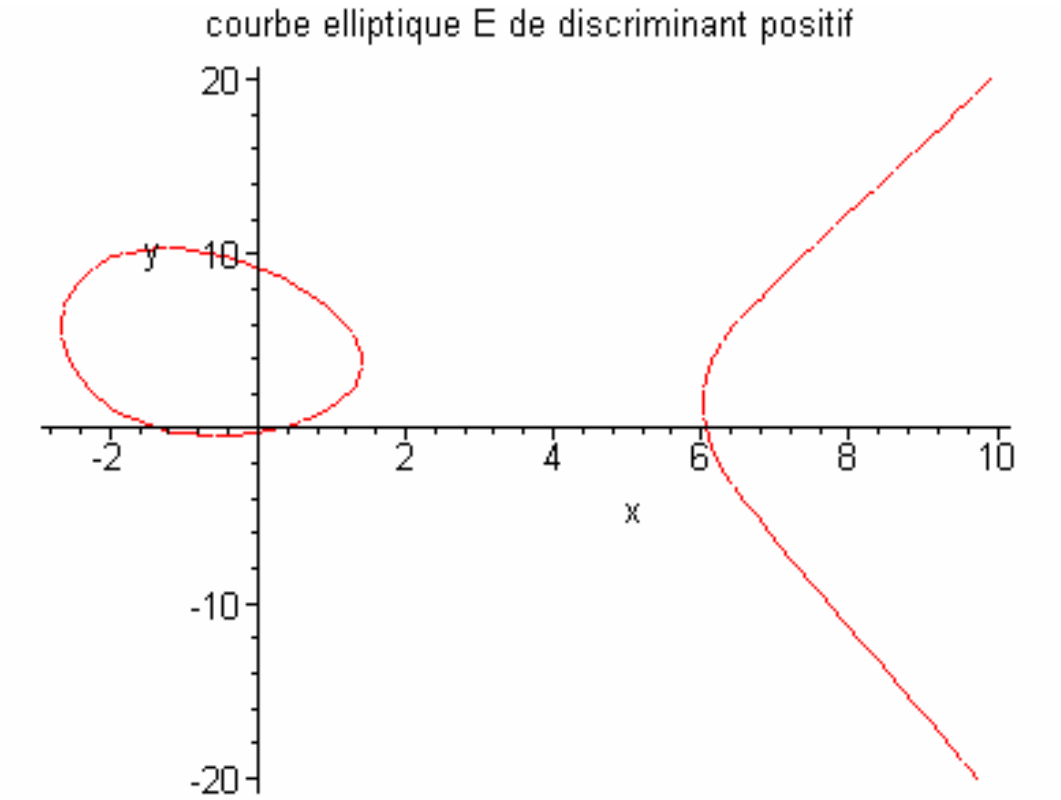
2	6	6.1
$y^2 - 7y = -23$	$y^2 - 3y = -3$	$y^2 - 2.9\,y = 1.231$
n'existe pas	n'existe pas	$\approx 1.95 \pm 1.82$

- 0.5	- 1.4	- 2
$y^2 - 9.5\,y = 5.125$	$y^2 - 10.4y = 6.744$	$y^2 - 11y = -11$
$\approx 4.75 \pm 5.26$	$\approx 5.2 \pm 5.81$	$\approx 5.5 \pm 4.38$

Ces valeurs impliquent que les abscisses x_1 , x_2 et x_3 des trois points d'intersection satisfont les inégalités: $6 \leq x_1 \leq 6.1$

$0 \leq x_2 \leq 0.4$

$-2 \leq x_3 \leq -1.4$



Exemple 2

Soit une courbe elliptique E d'équation de Weierstrass

$$y^2 + 8y = x^3 - 3x^2 + 3x + 9$$

Avec le calcul des invariants, nous obtenons

$b_2 = -12;\ b_4 = 6;\ b_6 = 100;\ b_8 = -308$;

$\Delta(E) = -232848 \prec 0$

Tableau des coordonnées réelles de quelques points de la courbe elliptique E

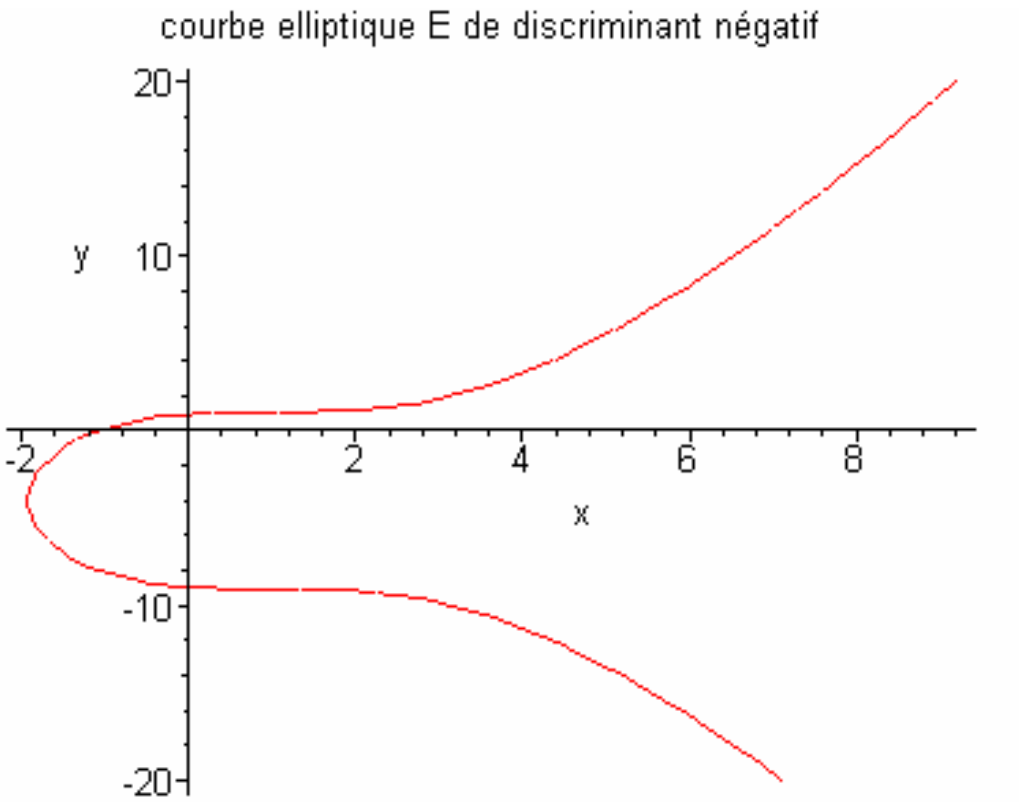
X	*0*	- 0.4	- 0.5
$y^2 + 8y = x^3 - 3x^2 + 3x + 9$	$y^2 + 8y = 9$	$y^2 + 8y = 7.256$	$y^2 + 8y = 6.875$
Y	1, -9	$\approx -4 \pm 4.87$	$\approx -4 \pm 4.78$

- 0.8	- 1	- 1.4
$y^2 + 8y = 4.168$	$y^2 + 8y = 2$	$y^2 + 8y = -3.824$
$\approx -4 \pm 4.49$	$\approx -4 \pm 4.12$	$\approx -4 \pm 3.49$

-2	- 1.9	-1.98
$y^2 + 8y = -17$	$y^2 + 8y = -14.39$	$y^2 + 8y = -16.46$
n'existe pas	$\approx -4 \pm 1.27$	n'existe pas

Ces valeurs impliquent que l'abscisse x du point d'intersection de la courbe E et l'axe Ox satisfait l'inégalité

$$-1 \leq x \leq -1.4 .$$



CHAPITRE III
GROUPE DE MORDELL - WEIL ET SOUS - GROUPE DE TORSION

§1 - Structure de groupe de Mordell –Weil d'une courbe elliptique

Pour obtenir un groupe abélien, considérons l'ensemble $E(k)$ des points k - rationnels d'une courbe elliptique E et le point à l'infini O_E de E.

Une application

$$f : E(k) \text{ x } E(k) \to E(k)$$

de valeur $f(P,Q)=P+Q$;

est déterminée par la règle géométrique de trois points colinéaires.

«*trois points colinéaires de la courbe E ont une somme nulle*»

$$P_1 + P_2 + P_3 = O_E \quad .$$

Proposition 1

L'ensemble $E(k)$, des points k-rationnels d'une courbe elliptique E, muni de la loi de composition déterminée par la règle géométrique de 3 points colinéaires de la courbe E est un groupe abélien d'élément neutre le point à l'infini $O_E = (\infty,\infty)$.

Preuve

Vérifions les axiomes d'un groupe.

1. L'axiome de l' élément neutre est satisfait par le point O_E à l'infini.

La droite PO_E est parallèle à l'axe Oy

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

Le point à l'infini est déterminé par la direction de l'axe Oy .

2. L'axiome du symétrique est satisfait par la règle géométrique,

deux points symétriques B et D satisfont:

$$B + D + O_E = O_E,$$

la sécante BD est parallèle à l'axe Oy .

Le symétrique du point B est le point D intersection de la parallèle à Oy passant par B , avec la courbe E .

3. L'axiome d'associativité est satisfait par les calculs des points

$$P_1 + (P_2 + P_3) \text{ et } (P_1 + P_2) + P_3$$

4. L'axiome de commutativité est satisfait par la coïncidence des sécantes

$P_1 P_2$ et $P_2 P_1$.

Les figures 1, 2 illustrent ces axiomes.

fig.1 : Somme de deux points $P_1 + P_2$ pour $P_1 \neq \pm P_2$ et le symétrique $-P_2$ du point P_2

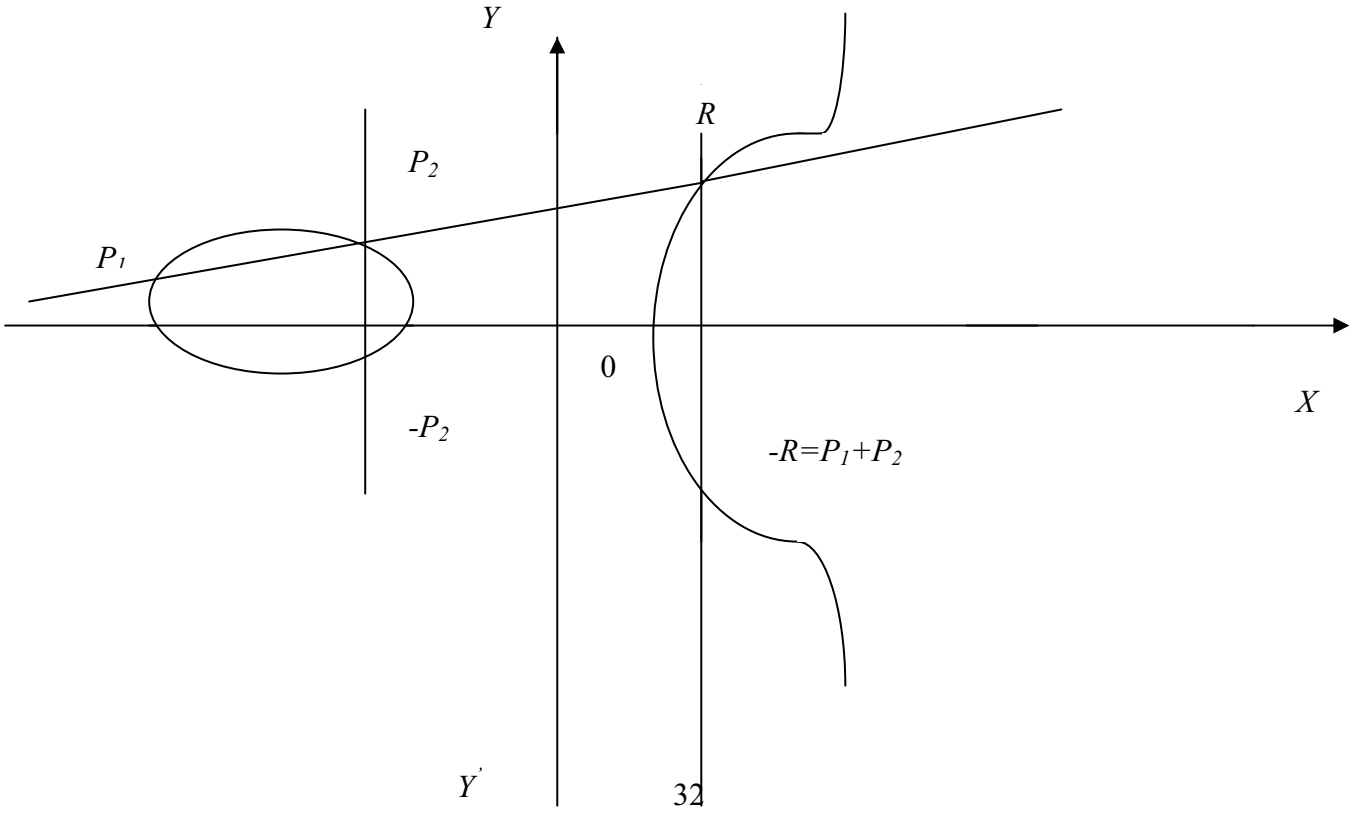
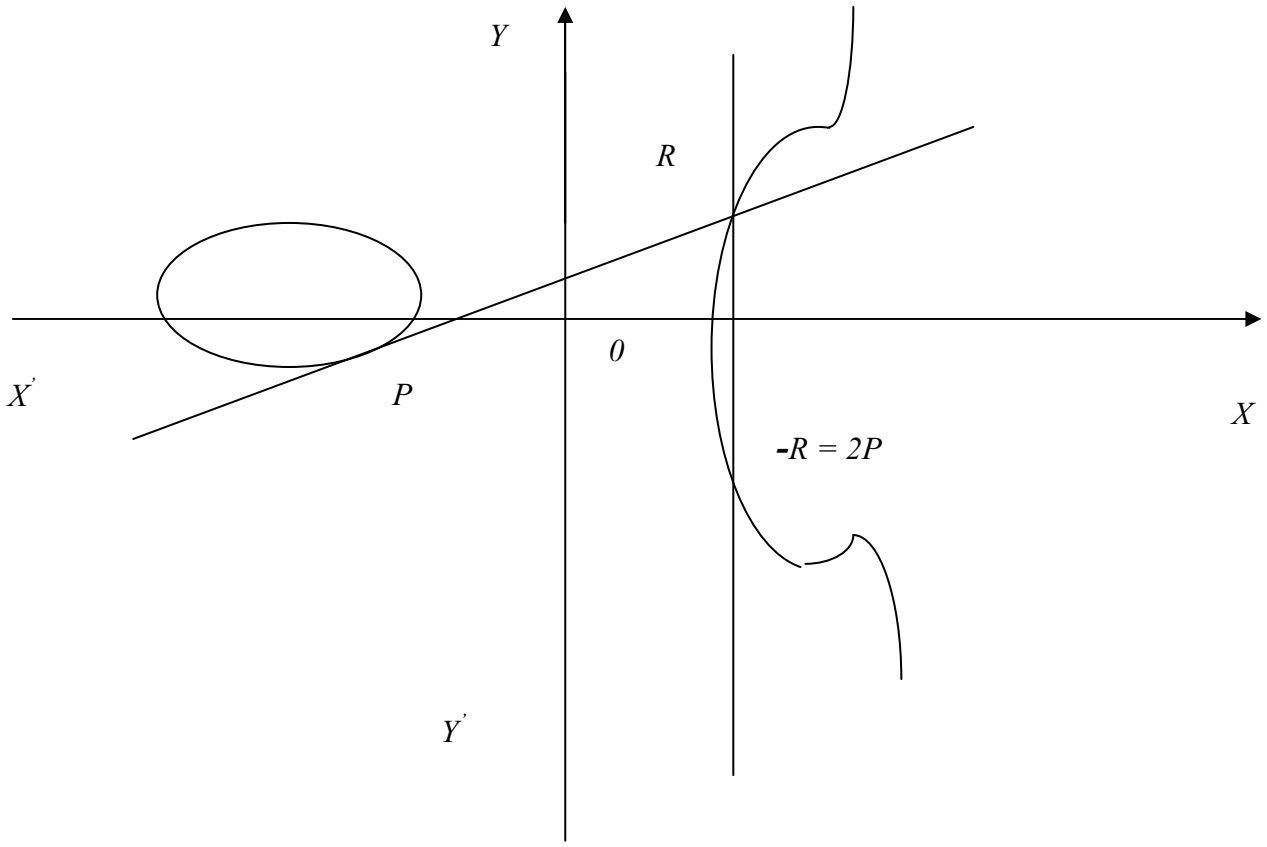


fig .2 : Somme $P + P = 2P$.



Déterminons la formule du symétrique $-P$ d'un point P de $E(k)$, la formule de la somme $P_1 + P_2$ et la formule du point $2P$.

Proposition 2

Soit une courbe elliptique E d'équation de Weierstrass

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

le symétrique d'un point $P=(x_P, y_P)$ de E est le point

$$-P=(x_P\ ,\ -a_1x_P-y_P-a_3) \qquad (2)$$

Preuve

Le symétrique $-P$ du point P se trouve à l'intersection de la parallèle à Oy, passant par le point P, avec la courbe E.

L'équation de cette parallèle est

$$x = x_P \qquad (3)$$

Nous obtenons une équation du 2ème degré en y, elle admet deux solutions y_P, y_{-P}.

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

$$y_{-P} + y_P = -a_1 x_P - a_3$$

Il en résulte l'ordonnée y_{-P} du point $-P$

$$y_{-P} = -a_1 x_P - a_3 - y_P \qquad (4)$$

de (3) et (4) nous déduisons les coordonnées du symétrique

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

□

Proposition 3

Soient deux points $P_1 = (x_1\ ,\ y_1)$, $P_2 = (x_2\ ,\ y_2)$, $P_1 \neq \pm P_2$, *d'une courbe elliptique* E *d'équation de Weierstrass*

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

Les coordonnées du point $P_1 + P_2 = M$ *sont*

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

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

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

Preuve

Equation de la sécante $P_1 P_2$

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

cette sécante recoupe la courbe en un point $P_3 = (x_3, y_3)$

Les abscisses x_i des 3 points P_i sont racines de l'équation cubique en x

$$[\lambda(x - x_1) + y_1]^2 + [\lambda(x - x_1) + y_1][a_1 x + a_3] = x^3 + a_2 x^2 + a_4 x + a_6 \qquad (5)$$

La somme $x_1 + x_2 + x_3$ est une fonction symétrique élémentaire des racines de l'équation (5)

$$x_1 + x_2 + x_3 = \lambda^2 + a_1\lambda - a_2 \qquad (6)$$

Il en résulte l'abscisse x_3

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \qquad (7)$$

La règle géométrique « $P_1 + P_2 + P_3 = O_E$ » implique

$$P_1 + P_2 = -P_3$$

La formule du symétrique d'un point permet de calculer les coordonnées de la somme

$P_1 + P_2 = -P_3 = M = (x_M, y_M)$

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

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

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

□

Exemple

Soit une courbe elliptique E d'équation

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

Les points. $P_1 = (1, 3)$, $P_2 = (2, 2)$ sont dans le groupe $E(\mathbb{Q})$

Appliquons la formule des coordonnées du symétrique

Nous obtenons

$$-P_1 = (x_P, -a_1x_P - y_P - a_3) = (1, 2)\ ,\quad -P_2 = (x_{P_2}, -a_1x_{P_2} - y_{P_2} - a_3) = (2, 5)$$

Appliquons la formule des coordonnées de la somme

$$P_1 + P_2 = M$$

Nous obtenons les coordonnées de la somme M

$x_M = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 = 4, \qquad \lambda = \dfrac{y_2 - y_1}{x_2 - x_1} = -1$

$y_M = -\lambda^3 - 2a_1\lambda^2 + (a_2 - a_1^2 + 2x_1 + x_2)\lambda + a_1a_2 - a_3 + a_1(x_1 + x_2) - y_1 = 11$

Appliquons la formule des coordonnées de la somme au calcul du point

$$P_1 - P_2 = M = (x_M, y_M)\ .$$

La pente de sécante $P_1(-P_2)$ est égale à $\lambda = 2$

$x_M = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 = 1$

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

Définition1

Le groupe abélien $E(k)$ est le groupe de Mordell – Weil de la courbe elliptique E.

§2 Sous groupe de m – torsion

Selon la théorie des groupes, tout groupe abélien possède des sous groupes.

Définition 2

Le sous groupe de m –torsion d'une courbe elliptique est l'ensemble des points d'ordre m ,

$$E(k)[m] = \{P \in E(k) \ , \ mP = O_E\} \tag{8}$$

Le symbole $m\ P$ signifie

$$m\ P = P+P+...+P,\ m\,fois\,P \ \ si \ \ m \succ 0 \tag{9}$$

$$m\ P = (-P)+(-P)+...+(-P),\ -m\,fois\ \ (-P)\ \ si\ \ m \prec 0$$

$$0P = O_E \ \ si \ \ m = 0$$

La réunion des sous groupes de m – torsion est le groupe de torsion de la courbe .

Définition 3

Le groupe de torsion $T(E)$ d'une courbe elliptique E est l'ensemble des points d'ordre fini du groupe de Mordell –Weil

$$T(E) = \{P \in E(k), mP = O_E\} = \bigcup_{m \in Z} E(k)[m].$$

Les points d'ordre infini servent à calculer le rang de E

Les coordonnées du point $2P = P + P$ d'une courbe elliptique sont déterminées par

Proposition 4

Soit une courbe elliptique E d'équation de Weierstrass

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

Les coordonnées du point $2P = (x_{2P},\ y_{2P})$ sont égales à

$$x_{2P} = \ (y'_P)^2 + a_1\ y'_P - a_2 - 2x_P\ .$$

$$y_{2P} = \ -(y'_P)^3 - 2a_1\ (y'_P)^2 + (\ a_2 - a_1^2 - 3x_P)\ y'_P + a_1 a_2 \ - a_3 \ + 2a_1\ x_P - y_P\ ,$$

pour tout point $P=(x_P,\ y_P) \neq O_E$ de la courbe E et $y'_P = \dfrac{3x_P^2 + 2a_2 x_P + a_4 - a_1\ y_P}{2y_P + a_1 x_P + a_3}$

Preuve

La tangente au point P a pour équation

$$y = y'_P\ (x - x_P\ )\ +\ y_P\ ;\ \text{où}\ \ y'_P \ \text{est la dérivée de}\ \ y$$

La tangente passe par un 2ème point $R = (x_R , y_R)$ de la courbe

Les abscisses x_P et x_R sont les racines de l'équation cubique en x.

$$[y'_P(x-x_P) + y_P]^2 + [y'_P(x-x_P) + y_P][a_1 x + a_3] = x^3 + a_2 x^2 + a_4 x + a_6 \qquad (10)$$

L'abscisse x_P est une racine double et x_R une racine simple.

La somme $2x_P + x_R$ est la fonction symétrique «somme des racines» de l'équation (10)

$$2x_P + x_R = (y'_P)^2 + a_1 y'_P - a_2$$

Il en résulte les coordonnées du point R

$$x_R = (y'_P)^2 + a_1 y'_P - a_2 - 2 x_P$$

$$y_R = y'_P (x_R - x_P) + y_P$$

La formule du symétrique d'un point permet de calculer les coordonnées du point $2P$

$$2P = -R$$

nous obtenons

$$x_{2P} = (y'_P)^2 + a_1 y'_P - a_2 - 2x_P$$

$$y_{2P} = -(y'_P)^3 - 2a_1 (y'_P)^2 + (a_2 - a_1^2 + 3x_P) y'_P + a_1 a_2 - a_3 + 2a_1 x_P - y_P .$$

□

Exemple

Courbe elliptique d'équation de Weierstrass

$$E : y^2 + 3xy + 4y = x^3 + x^2 - 21 x - 15 \qquad (11)$$

Le groupe $E(\mathbb{Q})$ contient les points $P_1 = (-1, 2)$ et $P_2 = (3, -6)$

Appliquons la formule des coordonnées du symétrique

Nous obtenons

$$-P_1 = (-1, -3), \; -P_2 = (3, -6)$$

Appliquons la formule des coordonnées de la somme

$P_1 + P_2 = M$; avec $\lambda = \frac{y_2 - y_1}{x_2 - x_1} = -2$

Nous obtenons

$$x_M = \lambda^2 + a_1 \lambda - a_2 - x_1 - x_2 = -5$$

$$y_M = -\lambda^3 - 2a_1 \lambda^2 + (a_2 - a_1^2 + 2 x_1 + x_2) \lambda + a_1 a_2 - a_3 + a_1 (x_1 + x_2) - y_1 = 1$$

Appliquons la formule des coordonnées de $2P$ au point P_1 ,

$$y'_{P_1} = \frac{3x_{P_1}^2 + 2a_2 x_{P_1} + a_4 - a_1 y_{P_1}}{2y_{P_1} + a_1 x_{P_1} + a_3} = -26/5$$

Nous obtenons

$$x_{2P_1} = (y'_{P_1})^2 + a_1 y'_{P_1} - a_2 - 2x_{P_1} = 311/25$$

$$y_{2P_1} = -(y'_P)^3 - 2a_1 (y'_{P_1})^2 + (a_2 - a_1^2 + 3x_{P_1}) y'_{P_1} + a_1 a_2 - a_3 + 2a_1 x_{P_1} - y_{P_1} = 927/25$$

La forme de y'_P implique que les coordonnées du point $2P$ du groupe $E(k)$ sont des fractions rationnelles de la forme

$$x_{2P} = \frac{f_1(x, y)}{d(x, y)^2}, \; y_{2P} = \frac{f_2(x, y)}{d(x, y)^3}$$

Les polynômes dénominateurs sont des puissances d'un même polynôme $d(x, y)$.

Pour un point mP, les degrés de ces 3 polynômes deviennent très grands. C'est pour des raisons de commodité qu'il faut prendre une équation de Weierstrass particulière pour obtenir des formules « raisonnables ».

C'est ce qu' a appliqué Cassels dans la publication:

"Diophantine equation with special reference to elliptic curves J. London. Math. Soc. 41 pp 193-291 (1966)"lemme7-2, formules (7.23, 7.24 et 7.25).

Théorème 1

Soit une courbe elliptique E d'équation de Weierstrass

$$y^2 = x^3 + Ax + B \in Q[x, y]$$

avec $4A^3 + 27B^2 \neq 0$

Alors pour tout entier $m \succ 2$, les coordonnées du point mP sont égales à

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

où les polynômes ψ_m, ϕ_m et ω_m satisfont les relations

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

$$\psi_4 = 4y\,(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \qquad (12)$$

$$\psi_{2m} = 2\psi_m[\psi_{m+2}\ \psi_{m-1}^2 - \psi_{m-2}\ \psi_{m+1}^2] \quad et \quad \psi_{2m+1} = \psi_{m+2}\ \psi_m^3 - \psi_{m-1}\ \psi_{m+1}^3$$

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

Preuve

Pour $m = -1$, $-P = (x, -y)$ alors $\frac{y}{(-1)^3}$ et $x = \frac{x}{(-1)^2}$ donc $\psi_{-1} = -1$

Pour $m = 0$, $0\,P = (\infty, \infty) = (\frac{x}{0^2}, \frac{y}{0^3})$ donc $\psi_0 = 0$

Pour $m = 1$, $1.P = (x, y) = (\frac{x}{1^2}, \frac{y}{1^3})$ donc $\psi_1 = 1$

Pour $m = 2$, $2\,P = (\frac{\phi_2}{(2y)^2}, \frac{\omega_2}{(2y)^3})$ donc $\psi_2 = 2y$

Pour $m \succ 2$, la preuve se fait par récurrence sur m. □

§3 Homomorphismes de courbes elliptiques

Les groupes de Mordell–Weil de courbes elliptiques peuvent intervenir dans les homomorphismes de groupes.

Définition 4

Un homomorphisme f d'une courbe elliptique E_1 dans une courbe elliptique E_2 est un homomorphisme de groupes abéliens

$$f : E_1(k) \to E_2(k)\ ;$$

donc il satisfait les formules d' homomorphisme :

$$f(O_{E1}) = O_{E2} \quad \text{et} \quad f(P_1 + P_2) = f(P_1) + f(P_2).$$

Ces homomorphismes de groupes de Mordell –Weil peuvent être des isomorphismes de groupes, des automorphismes de groupes, des translations, des isogènies,…

Nous nous limitons aux isomorphismes et aux isogènies.

§3.1. Isomorphismes

Soit une courbe elliptique E d'équation de Weierstrass.

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

Un isomorphisme f de E dans une courbe elliptique E' est une application

$$f : E(k) \to E'(k);$$

de valeur

$$f(x,y) = (u^2x + r\ ,\ u^3y + u^2sx + t) \qquad (13)$$

où r, s, t, $u \neq 0$ sont des éléments de k

Nous obtenons les coefficients a_i' de la courbe isomorphe E' par le calcul.

$ua_1' = a_1 + 2s$; Invariants b_{2i}'

$u^2a_2' = a_2 - sa_1 + 3r - s^2$; $u^2b_2' = b_2 + 12r$;

$u^3a_3' = a_3 + ra_1 + 2t$; $u^4b_4' = b_4 + rb_2 + 6r^2$; (14)

$u^4a_4' = a_4 - sa_3 + 2ra_2 - (t+rs)a_1 + 3r - 2st$; $u^6b_6' = b_6 + 2rb_4 + r^2b_2 + 4r^3$.

$u^6a_6' = a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1$; $u^8b_8 = b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4$.

Invariants c_{2i}'

$u^4c_4' = c_4$; $u^6c_6' = c_6$;

Invariants $\Delta(E')$ et $j(E')$

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

Proposition 5

Deux courbes elliptiques E et E' *sont isomorphes si et seulement si leurs invariants modulaires sont égaux.* □

Donc l'invariant modulaire permet de classifier les courbe elliptiques isomorphes.

§3.2. Isogénies de courbes elliptiques

Selon Shimura «Introduction to the Arithmetique Theory» Chapitre 4, «Isogenies and endomorphisms» ,

Définition 5

Une isogènie de deux courbes elliptiques E_1 *et* E_2 *définies sur un même corps* k *est un homomorphisme* f *de courbes elliptiques*

$$f : E_1(k) \to E_2(k)\ ;$$

qui satisfait les conditions :

1) f *n'est pas nul*

2) *Le noyau de l'homomorphisme* f *est un sous groupe* F *du groupe* $E_1(k)$ *d'ordre fini;*

3) f *est surjective;*

4) $f\ (O_{E_1}) = O_{E_2}$ et $f(P_1 + P_2) = f(P_1) + f(P_2)$.

La multiplication par un entier m est un exemple d'isogénie.

Les exemples d'isogènies de courbes elliptiques sont nombreux ; on peut en trouver dans les publications de Velu, dans l'ouvrage de Silverman.[*The Arithmetic of elliptic curves*, Graduate Texts in Math 106 (1986), Springer], etc…

Exemple ("*The Arithmetic of elliptic curves"*, [III - 4- 5], Silverman)

Soit une courbe elliptique E_1 d'équation de Weierstrass

$$E_1 : y^2 = x^3 + ax^2 + bx \in k\,[\,x,\,y\,]$$

avec les conditions $a^2 - 4\,b \neq 0$ et $car\,k \neq 2$.

Alors l'homomorphisme

$$\Phi : \quad E_1(k) \rightarrow E_2(k)$$

de valeur: $$\Phi\ (x,\ y\ ) = (\frac{y^2}{x^2},\ \frac{y\,(\,b - x^2)}{x^2}\,)$$

est une isogénie qui transforme E_1 en E_2 d'équation de Weierstrass

$$E_2 : y^2 = x^3 - 2ax^2 + (\,a^2 - 4b\,)x\ ;$$

Son noyau est un sous groupe d'ordre 2, donc Φ est une 2 – isogénie.

Pour $a = 9$ et $b = 16$, la condition $a^2 - 4b \neq 0$ est satisfaite.

Nous obtenons la courbe elliptique E_1 l'équation de Weierstrass

$$E_1 : y^2 = x^3 + 9x^2 + 16x\,,$$

avec la 2- isogénie Φ , nous obtenons la courbe elliptique E_2 isogéne à E_1

$$E_2 : y^2 = x^3 - 18x^2 + 17x.$$

§ 4.Hauteurs et descente infinie sur une courbe elliptique

Selon Lang (chapitre V Height, «*Elliptic curves, Diophantine analysis*»
Springer Verlag (1978) classification AMS = 10b45-10f99-14g25-14h251, Mordell a prouvé en 1922 une conjecture de Poincaré, selon laquelle le groupe des points rationnels d'une courbe elliptique est de type fini

La preuve est divisée en deux étapes; une étape pour démontrer que le groupe quotient $E(k)\ /\ m\,E(k)$ est fini pour $m = 2$, une autre consistant en une « descente infinie» qui utilise des fonctions hauteurs sur un groupe abélien .

Théorème de Mordell – Weil

Le groupe $E(k)$ de Mordell – Weil d'une courbe elliptique est de type fini. □

Ce type de groupe abélien est comparable au groupe des unités d'un corps de nombres:

Théorème des unités de Dedekind

Soit un corps de nombres k de degré fini $[k:Q]=n$ possédant t conjugués réels et 2s conjugués complexes

$$t+2s = n$$

Alors les unités de k forment un groupe abélien U(k) de type fini, isomorphe au produit de groupes

$$\mathrm{U}(k) \cong Z(k) \times \mathbb{Z}^r$$

$Z(k)$ = {racines de 1 contenues dans k}

$\mathbb{Z}^r$ = r copies du groupe abélien $\mathbb{Z}$

et $r = s + t - 1$ = rang du groupe U(k) des unités du corps k.

□

Pour le groupe de Mordell- Weil, ce type est déterminé par la

Proposition 6

Soit une courbe elliptique E. Alors son groupe de Mordell - Weil $E(k)$

est isomorphe au produit de 2 groupes abéliens

$$E(k) \cong T(E) \times \mathbb{Z}^r$$

où $T(E)$ = groupe de torsion de $E(k)$

$\mathbb{Z}^r$ = r copies du groupe $\mathbb{Z}$

r = entier positif ou nul.

□

Définition 7

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

Le rang r du groupe $U(k)$ des unités est calculable avec une formule simple.

Mais il n'y a pas de formule pour calculer le rang $r = r(E)$ d'une courbe elliptique.

Pour l'ordre du groupe de torsion $T(E)(k)$ il y a des résultats qui ont étés obtenus .

Citons un résultat relatif au groupe de torsion $T(E)$ sur le corps $\mathbb{Q}$ des nombres rationnels .

Proposition 7

Le groupe de torsion $T(E(\mathbb{Q}))$ *d'une courbe elliptique E sur le corps des nombres rationnels* $\mathbb{Q}$ *est de l'un des 15 types*

$$T(E(\mathbb{Q})) \cong \mathbb{Z}/m\mathbb{Z}; \quad pour \quad 1 \leq m \leq 10 \quad et \quad m=12.$$

$$\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}; \quad pour \quad 1 \leq m \leq 4.$$

Preuve

"*Rational isogenies of prime degree*" Invent. Math. 44 (1978) 129 – 162. de Mazur.

□

Il en résulte que l'ordre du groupe de torsion $T(E(\mathbb{Q}))$ est ≤ 16.

Les coordonnées d'un point de torsion d'une courbe elliptique d'équation $y^2 = f(x)$ sont déterminées par

Proposition 8

Soit une courbe elliptique E d'équation de Weierstrass

$y^2 = x^3 + Ax + B \in \mathbb{Z}[x, y]$, *avec la condition* $4A^3 + 27B^2 \neq 0$

Alors

1) Les coordonnées d'un point $P=(x, y) \in T(E(\mathbb{Q}))$ *sont des entiers rationnels.*

2) Soit un point $P \neq O_E$ *de torsion; alors il satisfait* $2P = O_E$ *ou bien* $y(P)^2$ *divise* $4A^3 + 27B^2$.

Preuve

«Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps $p-adiques$ » Ange. Math 177 (1937) 237–247.de Lutz

«Solution de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre »Wid. Akad.Skufter, Oslo (1935)de Nagell.

□

Ce résultat est compatible avec la proposition 7 (théorème de Mazur).

Exemple

Soit une courbe elliptique E_1 d'équation de Weierstrass

$$E_1 \quad y^2 = x^3 - 6x + 5 \tag{15}$$

Avec le calcul nous obtenons la valeur du nombre

$$4A^3 + 27\,B^2 = -189 \neq 0.$$

Appliquons la proposition 8 pour déterminer son groupe $T(E_1)(\mathbb{Q})$ de torsion

La formule $2P = (x_{2P}, y_{2P}) = O_E$, $x_{2P} = \dfrac{N(x)}{(2y)^2} = \infty$ implique la valeur $y = 0$

L'abscisse x est solution de l'équation diophantienne $f(x) = x^3 - 6x + 5 = 0$.

Par le théorème relatif aux zéros d'une équation diophantienne, un zéro est un diviseur du coefficient constant .

Donc un zéro α divise 5, soit $\alpha = \pm 1, \pm 5$.

Les valeurs $f(1) = 0, f(-1) = 10, f(5) = 100, f(-5) = -90$ impliquent une seule solution $x = 1$.

Donc le point (1, 0) est d'ordre 2.

Pour trouver les autres points d'ordre fini, nous testons les diviseurs d^2 de –189 qui sont

$d^2 = 1, 9$

Les équations diophantiennes $f(x) = 1$ et $f(x) = 9$ admettent 2 solutions $x = 2, -2$.

Il en résulte 4 points sur le groupe $E_1(\mathbb{Q})$

$$P_2 = (2, 1),\ P_3 = (2, -1),\ P_4 = (-2, 3),\ P_5 = (-2, -3).$$

Il faut trouver les points d'ordre fini parmi ces quatre points, soit en calculant les points $2P, 3P, 4P, ..., mP = 0$ soit en appliquant le théorème de réduction mod. *p*

Théorème

Soit une courbe elliptique E , sa courbe réduite $\tilde{E}$ sur un corps fini $\mathbb{F}_p$ à p éléments et un sous groupe $E(\mathbb{Q})[m]$ de m - torsion de la courbe E .

Si la courbe réduite $\tilde{E}$ est une courbe elliptique, alors l'application réduction

$$E(\mathbb{Q})[m] \to \tilde{E}(\mathbb{F}_p)$$

est injective

□

CHAPITRE IV

REDUCTIONS DE COURBES ELLIPTIQUES

COURBE MODULAIRE $X_1(13)$

La théorie des valuations des corps se trouve dans plusieurs ouvrages de Théorie Algébrique des Nombres

1. "Algebraic Number theory " de E .Weiss;
2. "Algebraic Numbers and Algebraic Functions"; de E. Artin
3. "Diophantine geometry" de S.Lang;
4. "Algebraic Number Theory" de H. Hasse, etc.…

§1-Valuations d'un corps

C'est sur la base de ces ouvrages que ce chapitre des valuations est traité .
Ces valuations ont des applications à la réduction des courbes elliptiques.

Définition 1

Une valuation d'un corps K est une fonction φ sur K dans l'ensemble des nombres réels positifs, qui satisfait les trois conditions :

1. $\varphi(a) = 0$ *si et seulement si* $a = 0$. *et* $\varphi(a) > 0$, *pour tout élément* $a \in K^*$ (1)
2. $\varphi(a\,b) = \varphi(a)\,\varphi(b)$. *pour tous éléments* $a, b \in K$ (2)
3. *Il existe une constante réelle positive c telle que*

$$\varphi(a) \leq 1 \text{ implique } \varphi(1 + a) \leq c\,. \quad (3)$$

Exemples

1. $K = \mathbb{R}$ = corps des nombres réels. La valeur absolue

$$\varphi(a) = \max(a, -a); \text{ alors } c = 2$$

est une valuation.

2. $K = \mathbb{C}$ = corps des nombres complexes. La valuation φ est la norme du nombre complexe $a + ib$

$$\varphi(a + ib) = (a^2 + b^2)^{1/2}; \text{ alors } c = 2 .$$

3. La valuation triviale d'un corps K est définie par ses valeurs

$$\varphi(0) = 0, \varphi(a) = 1, \text{ pour tout élément } a \in K^*$$

4. $K = \mathbb{Q}$ = corps des nombres rationnels .Pour tout nombre premier p,

la valuation p – adique φ_p a pour valeur :

$$\varphi_p(x) = \frac{1}{p^\alpha} \text{ où } x = p^\alpha \frac{a}{b} \text{ , } p \text{ ne divise pas le pgcd}(a, b)$$

pour tout nombre rationnel $x \in \mathbb{Q}^*$.

Une valuation φ détermine un homomorphisme du groupe multiplicatif K^* du corps K dans le groupe multiplicatif des nombres réels positifs $\mathbb{R}_{>0}$

Proposition 1

Soit une valuation φ d'un corps K

$$\varphi: K \to R_{>0}$$

Alors φ satisfait:

1. *φ est un homomorphisme des groupes K^* et $R_{>0}$*
2. *$\varphi(1) = 1$.*
3. *$\varphi(a^{-1}) = 1/\varphi(a)$, pour tout élément $a \in K^*$*
4. *$\varphi(b / a) = \varphi(b) / \varphi(a)$, pour tous éléments $a \in K^*$ et $b \in K$*
5. *$\varphi(-1) = 1$ et $\varphi(-a) = \varphi(a)$, pour tout élément $a \in K$*
6. *$\varphi(\zeta) = 1$, où ζ est une racine nième de l'unité.*

Preuve

1. La condition (2) de la définition d'une valuation implique que la valuation φ est un homomorphisme de groupes multiplicatifs

$$\varphi(a\ b) = \varphi(a)\ \varphi(b),\ \text{pour tous éléments } a,\ b \in K$$

2. Pour $a = 1$, la condition (2) et l'égalité $b = 1.\ b$ impliquent

$$\varphi(b) = \varphi(1)\ \varphi(b),$$

d'où $\varphi(1) = 1$

3. Soit l'inverse a^{-1} d'un élément a du groupe multiplicatif K^*

La condition (2) implique la relation

$$\varphi(a\ a^{-1}) = \varphi(a)\ \varphi(a^{-1}) = 1$$

Il en résulte la formule

$$\varphi(a^{-1}) = 1/\varphi(a)$$

4. La condition (2) implique la relation

$$\varphi(b) = \varphi(a\ .\ b/a) = \varphi(a)\ \varphi(b\ /\ a)$$

Il en résulte la relation

$$\varphi(b\ /\ a) = \varphi(b) / \varphi(a).$$

5. La relation $(-1)^2 = 1$ implique la relation

$$\varphi(1) = \varphi(-1)\ \varphi(-1)$$

Il en résulte $\varphi(-1) = \pm 1$

La condition (1) implique $\varphi(-1) = 1$

Il en résulte la formule

$$\varphi(-a) = \varphi(-1).\varphi(a) = \varphi(a),\ \text{pour tout élément } a \in K.$$

6. Soit une racine nième ζ de l'unité; elle satisfait $\zeta^n = 1$; la valuation φ implique

$$\varphi(\zeta^n) = (\varphi(\zeta))^n = 1\ ;$$

d'où $\varphi(\zeta) = 1$. □

La condition (3) peut être remplacée par la condition

"*Il existe une constante réelle c telle que*

$$\varphi(a + b) \le c\ max\ \{\varphi(a), \varphi(b)\}"$$

Dans l'ensemble $V(K)$ des valuations d'un corps K, il y a une relation d'équivalence .

Définition 2

Deux valuations φ_1 et φ_2 d'un *corps K sont équivalentes s'il existe un réel $\alpha > 0$, tel que*

$$\varphi_2 = (\varphi_1)^{\alpha} \quad . \tag{4}$$

Alors l'ensemble $V(K)$ des valuations de K est la réunion de ces classes d'équivalence.

Ces classes d'équivalence sont considérées comme des diviseurs premiers du corps K

$$P_1 = \{ \varphi \in V(K), \varphi = (\varphi_1)^{\alpha} \}$$

Le diviseur premier trivial est la classe d'équivalence qui contient la valuation triviale .

Les valuations d'un corps K sont réparties en deux sous ensembles disjoints:

Le sous ensemble V_∞ des valuations archimédiennes non équivalentes;

et le sous ensemble V_0 des valuations non archimédiennes non équivalentes .

Définition 3

Une valuation est archimédienne lorsqu'elle satisfait

$$\varphi(a+b) \leq 2 \max \{ \varphi(a), \varphi(b) \}. \tag{5}$$

pour tous éléments a, b dans K.

Une valuation est non archimédienne lorsqu'elle satisfait

$$\varphi(a+b) \leq \max \{ \varphi(a), \varphi(b) \}. \tag{6}$$

pour tous éléments a, b dans K.

Exemples

1) La valeur absolue usuelle sur le corps des nombres réels $\mathbb{R}$

$$\varphi(a) = \max (a, -a);$$

est archimédienne

2) La valuation $\varphi(a + ib) = (a^2 + b^2)^{1/2}$ satisfait

$$\varphi(z + z') \leq \varphi(z) + \varphi(z'). \tag{7}$$

l'inégalité (7) implique la valuation φ est archimédienne.

3) La valuation p- adique sur le corps $\mathbb{Q}$

$\varphi_p\ (p^r\ a/b) = p^{-r}$

$\varphi_p(\ p^r \frac{a}{b} + \ p^{r'}\ \frac{a'}{b'}\ ) = p^{-r} = \max\ (\varphi_p(\ p^r \frac{a}{b}\ ),\ \varphi_p(\ p^{r'}\ \frac{a'}{b'}\ )\ )$

Il en résulte que la valuation p-adique est non archimédienne.

Chaque valuation non archimédienne détermine des parties du corps K

1) L'anneau de valuation de φ est l'ensemble:

$$O_\varphi = \{\, a \in K,\ \varphi(a) \le 1\ \}\ ; \tag{8}$$

2) L'idéal de la valuation φ:

$$\mathcal{M}_\varphi = \{\, a \in K,\ \varphi(a) < 1\}; \tag{9}$$

C'est un idéal maximal

3) Le groupe des φ - unités :

$$\mathcal{U}_\varphi = \{\ a \in K,\ \varphi(a) = 1\ \}. \tag{10}$$

4) Le corps résiduel $O_\varphi\ /\ \mathcal{M}_\varphi = K_{resi}$

Toute valuation φ précédente est multiplicative .Elle devient additive à l'aide du logarithme.

Définition 4

Soit une valuation multiplicative

$$\varphi:\ K \to R$$

La valuation exponentielle associée

$$v: K \to R \cup \{\infty\}$$

de valeur $v(x) = \log|\varphi\ (x)|$ *pour tout élément* x *du corps* K.

Alors v est additive, par les propriétés du logarithme

$\log\ (xy) = \log(x) + \log(y)$

$\log(0) = -\infty\ ,\ \log(1) = 0$

Déterminons les ensembles associés à la valuation exponentielle v.

L'anneau de valuation O_v, l'idéal maximal de valuation $\mathcal{M}_v$ et le groupe des unités $\mathcal{U}_v$

$$\mathcal{O}_v = \{ a \in K, \nu(a) \geq 0 \} \; ; \tag{11}$$

$$\mathcal{M}_v = \{ a \in K, \nu(a) > 0 \}; \tag{12}$$

$$\mathcal{U}_v = \{ a \in K, \nu(a) = 0 \}. \tag{13}$$

Toute valuation exponentielle ν détermine un homomorphisme du groupe multiplicatif K^* du corps K dans le groupe additif du corps $\mathbb{R}$ des nombres réels .

$$\nu : K^* \to \mathbb{R}$$

La valuation v est discrète lorsque son image $\nu(K^*)$ est un sous ensemble discret de l'ensemble des nombres réels.

La valuation v est *discrète normalisée* si l'ensemble $\nu(K^*) = \mathbb{Z}$.

Une uniformisante d'une valuation v , discrète normalisée, est un élément $\pi \in K$ de valuation

$$\nu(\pi) = 1$$

Proposition 2

Soit une valuation discrète normalisée v .

L'anneau de valuation $\mathcal{O}_v$ est un anneau intègre, unitaire, local .

L'idéal de valuation $\mathcal{M}_v$ est un idéal maximal et principal. □

Définition 5

Un anneau local est un anneau qui admet un idéal maximal unique.

Un idéal I d'un anneau A est principal s'il est engendré par un seul élément .

I = g A , pour un certain élément g de l'anneau A .

§ 2 Réduction d'une courbe elliptique

Une valuation φ du corps de base K d'une courbe elliptique « réduit » ce corps au corps résiduel K_{resi} .

La valuation p-adique du corps $\mathbb{Q}$ d'une courbe elliptique «réduit» ce corps au corps fini $\mathbb{F}_p$ de p éléments .

Cela implique que les coefficients a_1 , a_2,..., a_6 de l'équation de Weierstrass qui sont des éléments du corps, sont également réduits.

Définition 6

Soit une courbe elliptique E d'équation de Weierstrass,

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

1) La réduction modulo un nombre rationnel premier p est l'application

$E(Q) \rightarrow \overline{E}(\mathbb{F}_p)$,

$a_i \rightarrow \overline{a}_i \bmod p$, $x \rightarrow \overline{x} \bmod p$, $y \rightarrow \overline{y} \bmod p$ *et* $P=(x, y) \rightarrow \overline{P}=(\overline{x}, \overline{y})$

2) La réduction modulo une valuation φ est l'application

$$E(K) \rightarrow \overline{E}(K_{resi}),$$

$$(x, y) \rightarrow (\varphi(x), \varphi(y))$$

Exemple 1

Courbe elliptique *E* d'équation de Weierstrass

$$E : y^2 - 5xy + 13y = x^3 + 15x^2 - 14x + 37 \qquad (14)$$

Avec le calcul nous obtenons ses invariants

$b_2 = 85$; $b_4 = -93$; $b_6 = 317$; $b_8 = 4574$;

$c_4 = 9457$; $c_6 = -967177$; $\Delta(E) = -51878462$.

La réduction modulo 5 transforme l'équation (14) en l'équation de la courbe réduite

$$\overline{E} : y^2 + 3y = x^3 + x + 2 \in \mathbb{F}_5[x, y] \qquad (15)$$

Les invariants de la courbe réduite sont des éléments du corps $\mathbb{F}_5$

$b_2 = 0$; $b_4 = 2$; $b_6 = 2$; $b_8 = 4$;

$c_4 = 2$; $c_6 = 3$; $\Delta(\overline{E}) = 3$.

IV Réductions de courbes elliptiques et Courbe modulaire $X_1(13)$

Selon Silverman, une équation de Weierstrass E sur un corps local K muni d'une valuation discrète et normalisée v est minimale lorsque les coefficients a_1, a_2, a_3, a_4, a_6 sont v-entiers et lorsque la valuation $v(\Delta(E))$ est minimale

Avec les formules d'isomorphismes de courbes elliptiques

$$u^4 c_4' = c_4 ; \qquad u^6 c_6' = c_6 ; \qquad u^{12}\Delta(E') = \Delta(E)$$

nous obtenons un critère de minimalité de l'équation de E.

Une équation de Weierstrass

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

est minimale en une valuation v si elle satisfait :

$v(a_i) \geq 0$ et $v(\Delta(E)) \prec 12$

ou bien $v(a_i) \geq 0$ et $v(c_4) \prec 4$

ou bien $v(a_i) \geq 0$ et $v(c_6) \prec 6$

Application de ce critère à l'équation (14)

$v_5(-5) = v_5(15) = 1, \; v_5(-14) = v_5(13) = v_5(37) = 0$

$v_5(c_4) = v_5(\Delta(\mathrm{E})) = 0$

Ces valeurs impliquent que l'équation de la courbe est minimale.

§ 2.1 Classification des réductions

Les réductions d'une courbe elliptique sont classifiées par la nature de la courbe réduite

Définition 7

1) Une réduction est bonne lorsque la courbe réduite est une courbe elliptique.

2) Une réduction est mauvaise lorsque la courbe réduite est singulière.

2.1) Une réduction est multiplicative lorsque la courbe réduite a un nœud.

2.2) Une réduction est additive lorsque la courbe réduite a un point de rebroussement.

Il y a un autre vocabulaire en usage

Une bonne réduction est une réduction stable;

Une réduction multiplicative est une réduction semi-stable;

Une réduction additive est une réduction instable .

Définition 8

Une courbe elliptique a une bonne réduction potentielle sur un corps K lorsqu'elle a une bonne réduction sur toute extension finie L de K.

§ 2.2 Sous groupes de $E(K)$ et réduction

Soit une valuation φ et les réductions $\widetilde{P}$ d'un point P et $\widetilde{E}$ d'une courbe elliptique E

Alors les ensembles

$E_0(K) = \{ P \in E(K) \ ; \ \widetilde{P} \in \widetilde{E}_{ns} \ (K_{resi}) \ \}$ où $\widetilde{E}_{ns}(K_{resi})$ désigne la courbe réduite $\widetilde{E}$ privée de son point singulier .

et $$E_1(K) = \{ P \in E(K) \ , \ \widetilde{P} = O_{\widetilde{E}} \}$$

sont des sous groupes du groupe de Mordell - Weil de la courbe elliptique E

Ces sous groupes déterminent une suite exacte de groupes

$$0 \rightarrow E_1(K) \rightarrow E_0(K) \rightarrow \widetilde{E}_{ns}(K_{resi}) \rightarrow 0$$

Cette suite exacte implique quelques résultats

Proposition 3

Soit une courbe elliptique E, son groupe de Mordell –Weil $E(K)$, un entier $m \geq 1$ premier à la caractéristique de K_{resi} le sous groupe $E(K)[m]$ de m –torsion et les sous groupes $E_0(K)$ et $E_1(K)$ ci dessus

1) *Le sous groupe $E_1(K)$ n'a pas de points $P \neq O_E$ d'ordre m ,*
2) *Lorsque la courbe réduite $\widetilde{E}$ est elliptique, l'application «réduction»*

$$E(K)[m] \rightarrow \widetilde{E}(K_{resi})$$

est injective.

□

Lorsque la courbe elliptique admet une réduction multiplicative, l'indice de $E_0(K)$ dans le groupe $E(K)$ est fini .

Proposition 4

Soit une courbe elliptique E d'invariants $\Delta(E)$ et $j(E)$ qui admet une réduction multiplicative décomposée en une valuation v sur un corps K.

1) Le groupe quotient $E(K) / E_0(K)$ *est cyclique d'ordre égal à* $v(\Delta(E)) = -v(j(E))$

2) Dans les autres cas de réduction, ce groupe quotient est fini d'ordre au plus 4 .

3) Le groupe $E_0(K)$ *est d'indice fini dans le groupe E(K).*

Preuve

C'est un théorème de Kodaira et de Néron.
□

Exemple

Soit une courbe elliptique E d'équation de Weierstrass

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

son discriminant $\Delta(E) = -32710 = -37 . 83 . 2 . 5 .$

La courbe réduite $\overline{E}(\mathbb{F}_p)$ est non singulière, pour $p \neq 2, 5, 37, 83 .$

En réduisant la courbe E modulo $p = 3, 7$, après les calculs, nous obtenons

Card ($\overline{E}(\mathbb{F}_3)$) = 5, Card ($\overline{E}(\mathbb{F}_7)$) = 7, pgcd (5, 7) = pgcd (3, 7) = 1

La proposition (3) implique que le seul point de torsion de la courbe E est l'élément neutre O_E .

$$T(E)(\mathbb{Q}) = \{ O_E \}$$

§3-Courbe modulaire $X_1(13)$

Pour démontrer qu'il n'existe pas de courbe elliptique qui possède un point $\mathbb{Q}$-rationnel d'ordre 13, Mazur et Tate ont utilisé une méthode basée sur des propriétés de la courbe modulaire $X_1(13)$; («Points of order 13 on elliptic curves», Invent Math .22 (1973) – 41-49) .

Nous commençons par décrire la construction des courbes modulaires .

Selon Shimura [14], le groupe linéaire général GL(2; $\mathbb{C}$) des 2 x 2 matrices $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ inversibles et ses sous groupes opèrent sur le demi plan supérieur

$$\mathbb{H} = \{ x + i y = z \in \mathbb{C},\ y \succ 0 \} \qquad (16)$$

par les transformations homographiques:

$$A z = \frac{a z + b}{c z + d}; \qquad (17)$$

Le demi plan supérieur $\mathbb{H}$, complété par l'espace $\mathbb{Q} \cup \{\infty\}$ devient le demi plan supérieur complet:

$$\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\} \qquad (18)$$

Le groupe GL(2; C) et ses sous groupes opèrent sur $\mathbb{H}^*$ par les transformations homographiques .Il y a un sous groupe particulier: le groupe modulaire.

Définition 9

Le groupe modulaire Γ *est le groupe spécial linéaire des 2 x 2 matrices* A *de det (A) = 1*

$$SL(2, \mathbb{Z}) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} = A ; \ a, b, c, d \in \mathbb{Z}; \ a\,d - b\,c = 1 \} = \Gamma \qquad (19)$$

Le groupe projectif spécial linéaire PSL (2, $\mathbb{Z}$*) des 2 x2 matrices A est le groupe quotient*

$$PSL(2, \mathbb{Z}) = \Gamma / \{ \pm I_2 \}; \qquad (20)$$

Le groupe modulaire possède des sous groupes particuliers qui sont les sous groupes modulaires de congruences, de niveau N , $N \geq 1$

$$\Gamma_0 (N) = \{ A \in \Gamma ; \ c \equiv 0 \mod N \} \qquad (20-1)$$

$$\Gamma_1 (N) = \{ A \in \Gamma ; \ c \equiv 0 , \ a \equiv d \equiv 1 \mod N \} \qquad (20-2)$$

Le sous groupe de congruence de niveau N , principal est :

$$\Gamma (N) = \{ A \in \Gamma ; \ A \equiv I_2 \mod N \} \qquad (20-3)$$

Ces sous groupes sont d'indices finis dans le groupe modulaire Γ .

Les points z de l'espace $\mathbb{H}^*$ invariants par un sous groupe G de Γ sont répartis dans la classe des points elliptiques et dans la classe des pointes

Définition 10

Une pointe pour un sous groupe G *du groupe modulaire* Γ *est un point rationnel* $s \in \mathbb{Q}$ *invariant par* G

$$G\ s = s$$

Par la théorie des groupes à opérateurs, l'orbite d'un sous groupe G du groupe modulaire Γ est un espace quotient

$$\mathbb{H}^* / G \qquad (21)$$

Cet espace peut être muni d'une structure analytique de «Surface de Riemann» .

Définition 11

Les espaces quotients

$$H^* / \Gamma_0 (N) \cong X_0 (N); \qquad (21-1)$$

$$H^* / \Gamma_1 (N) \cong X_1 (N); \qquad (21-2)$$

$$H^* / \Gamma (N) \cong X(N). \qquad (21-3)$$

sont des « courbes modulaires de niveau N ».

Ces courbes modulaires possèdent une structure de variétés abéliennes.

Elles possèdent des jacobiennes $J_0(N)$, $J_1(N)$, $J(N)$, groupes des points fermés des variétés abéliennes . A chaque courbe algébrique X de genre g est associée une variété abélienne $J(X)$ de dimension g .

La structure d'une jacobienne $J(X)$ de la courbe X est déterminée par des points génériques $M_1, ..., M_g$ de la courbe algébrique X . Alors la jacobienne $J(X)$ est liée à une fonction

$$\varphi: \ X \to J(X)$$

la somme $z = \sum_{1 \le i \le g} \varphi(M_i)$ est un point générique de la jacobienne $J(X)$.

Les corps de fonctions $k(z)$ et $k(M_1, ..., M_g)$ sont égaux .

Une description des jacobiennes $J(X)$ se trouve dans l'ouvrage de Weil et dans d'autres ouvrages .

Les courbes modulaires de genre 1 sont des courbes modulaires elliptiques.

Celles qui sont de genre g = 0 et g $\succ$ 1 ne sont pas elliptiques. Elles peuvent être produit de courbes elliptiques .

Ainsi, d'après Ligozat, «Courbes Modulaires de genre 1, mémoire 43, de la Société Math. de France», la courbe modulaire $X(N)$ est de genre 1 pour 12 valeurs de N

$$N = 11, 14, 15, 19, 20, 21, 24, 27, 32, 36, 49.$$

Proposition 5 (Ligozat)

Le groupe $X(N)(\mathbb{Q})$ des points de la courbe modulaire elliptique $X(N)$, rationnels sur $\mathbb{Q}$, est un groupe fini, et engendré par les pointes de $\Gamma_0(N)$ qui sont rationnelles sur $\mathbb{Q}$.

□

Ligozat a déterminé un modèle singulier de la courbe modulaire $X(26)$

$$y^2 = x^6 - 8x^5 + 8x^4 - 18x^3 + 8x^2 - 8x + 1.$$

La jacobienne $J(26)$ de la courbe modulaire $X(26)$ est isogène au produit de 2 courbes elliptiques de conducteur 26.

La courbe modulaire $X_0(121)$ est de genre 6.

Proposition 6 (Ligozat)

Il existe 12 courbes elliptiques définies sur $\mathbb{Q}$ qui sont quotient de la jacobienne $J_0(121)$ de la courbe modulaire $X_0(121)$ de niveau 121 : trois d'entre elles ont pour conducteur 11 et sont liées par des isogènies de degré 5.

Les neuf autres courbes elliptiques ont pour conducteur 121 et sont liées par des isogènies de degré 5 ou 11.

□

Ces résultats ont été obtenus avec les fonctions modulaires, les involutions d'Atkin-Lehmer, les opérateurs de Hecke, les symboles modulaires, …

Les courbes modulaires $X_1(N)$ de niveau N sont liées aux «surfaces de Riemann $\mathcal{H}^* / \Gamma_1(N)$» par l'intermédiaire de fonction modulaire $j(z)$ de poids 0

$$j(z) = \frac{1}{q} + 744 + \sum_{n \geq 1} c(n) q^n \text{, avec } c(n) \in \mathbb{Z} \text{ et } q = \exp(2\pi i z)$$

("*Modular Functions and Dirichlet Series*" .G T M 41, Apostol)

Proposition 7 ("*The Arithmetic of elliptic curves*", Theorem13.1, Silverman)

Soit le demi plan supérieur complété $\mathcal{H}^*$ et un sous groupe modulaire $\Gamma_1(N)$ de congruence de niveau N. Alors, il existe une courbe projective lisse $X_1(N)$ sur le corps $\mathbb{Q}$ des rationnels et un isomorphisme analytique complexe

$$j_N : \quad \mathcal{H}^* / \Gamma_1(N) \rightarrow X_1(N)(\mathbb{C})$$

qui satisfait les conditions:

à tout point $z \in H^* / \Gamma_1(N)$ *et au corps de fonctions* $Q(j_N(z))$ *il correspond une classe d'équivalence de courbes elliptiques* E *possédant un point* T *d'ordre* N,
avec $j_N(z) = j(Nz)$.

□

En tant que courbe algébrique projective lisse, une courbe modulaire est elliptique lorsqu'elle a un genre g =1

En tant que variété abélienne irréductible la courbe modulaire est une courbe elliptique lorsque sa dimension est égale à 1, cela d'après les structures algébriques d'une courbe elliptique.

Selon Ogg, la courbe modulaire $X_1(13)$ de niveau 13 est de genre 2.Elle est isomorphe au produit de 2 courbes elliptiques isogènes. Sa jacobienne $J(13)$ est une variété abélienne, de dimension 2 sur le corps des nombres rationnels $\mathbb{Q}$. Elle admet une mauvaise réduction au seul nombre 13 .

La courbe modulaire $X_1(13)$ possède 12 pointes, dont 6 rationnelles sur $\mathbb{Q}$ et 6 dans le sous corps réel maximal $K_0(13)$ du 13ème corps cyclotomique $K(13)$.

Le groupe de Galois G du 13ème corps cyclotomique est cyclique d'ordre 12; le groupe de Galois G' du sous corps réel maximal est un groupe cyclique d'ordre 6,

$$G' = G / \{\pm 1\}.$$

Le groupe G' opère cycliquement sur les 6 pointes rationnelles du sous groupe de congruence $\Gamma_1(13)$ de niveau 13.

Les points de 19 – division de la jacobienne $J(13)$ sont étudiés avec des propriétés arithmétiques :

(**1**) 13 et 19 sont des nombres premiers dans la progression arithmétique de raison 6.

(**2**) $13 \not\equiv 1 \bmod 19$;

(**3**) Le nombre de classe d'idéaux du 13ème corps cyclotomique est premier à 13.

En utilisant ces propriétés arithmétiques, des arguments de descente et des propriétés des jacobiennes $J(N)$, et des résultats dans [9] et [10], Mazur et Tate ont obtenu les résultats qui sont rassemblés dans la:

Proposition 8

1/ *La jacobienne de la courbe modulaire* $X_1(13)$ *de niveau 13 possède exactement 19 points rationnels .*

2/ *Les 6 pointes* Q *rationnelles de cette courbe modulaire* $X_1(13)$ *sont les seuls points* Q*-rationnels de la courbe* $X_1(13)$.

3/ *IL n'y a pas de courbe elliptique sur le corps* Q *qui possède un point rationnel d'ordre 13.*

□

Pour plus de détails, se référer à [9]

Nous nous proposons de les décrire dans une recherche personnelle ultérieure dans le domaine des courbes modulaires.

C'est un sujet passionnant. Je me propose de poursuivre mes recherches sur les sous groupes modulaires de congruences $\Gamma_0(N)$, $\Gamma_1(N)$, $\Gamma(N)$ et les courbes modulaires $X_0(N)$, $X_1(N)$, $X(N)$ attachées à ces groupes modulaires.

REFERENCES

[1] B.G.BERKOVIC "*Rational points on the jacobians of modular curves*", Math. USSR. Sbornik 30, 478-500 (1976)

[2] G.BILLING, K.MAHLER "*On exceptional points on cubic curves*" J.London.Math.Soc. 15, 32-43 (1940).

[3] J.CASSELS "*Diophantine equations with special reference to elliptic curves*" J. London. Math. Soc. 41, 193-291 (1966).

[4] R.HARTSHORNE "*Algebraic geometry*" Graduate Texts in Mathematics, vol. 53, Springer-Verlag, (1977)

[5] KENKU 1) "*On the modular curves* $X_0(125)$, $X_1(25)$ *and* $X_1(49)$" J London Math Soc (2) 23, 415-427 (1981)

2) "*The modular curves* $X_0(65)$ *and* $X_0(91)$ *and rational isogeny*" Math.Proc.Cambridge.Philos.Soc.87, 15-20 (1980)

[6] D.KUBERT "*Torsion of Elliptic Curves.* Universal bound on the torsion of elliptic curves" Proc.London Math. Soc.(3) 33, 193-237 (1976)

[7] S.LANG "*Elliptic functions*" .Addison-Wesley Publishing Company, Inc, (1973).

[8] B. MAZUR "*Rational point of modular curves*" LNM349, (1976)

[9] B. MAZUR et J. TATE "*Points of order 13 on elliptic curves*" Invent math 22, 41 - 49.(1973)

[10] A. OGG **1)** "*Rational points on certain elliptic modular curves*" Talk given at AMS Symposium on analytic Number Theory and related parts of analysis st Louis, Mimeographed notes, Berkeley, (1972).

2) "*Rational points of finite order on elliptic curves*" Invent math 12, 105 - 111.(1971)

3) "*Modular forms and Dirichlet series*" New –York Benjamin (1969)

[11] SERRE "*Propriètés galoisiennes des points d'ordre fini des courbes elliptiques*", Invent.Math.15, 259-331 (1972)

[12] I.R.SHAFAREVICH "*Basic Algebraic Geometry*" Springer Verlag Berlin Heidelberg New York (1977)

[13] I.SHI "*Modular curves and diophantine Equation*" Math. Japonica 25.n°2, 245-250, (1980).

[14] G.SHIMURA "*Introduction to the Arithmetic Theory of automorphic functions*" Publ. Math. Soc. Japan 11 Iwanami. (1971)

[15] J.SILVERMAN "*The Arithmetic of elliptic curves*" Graduate Texts in Math 106 (1986) Springer

[16] J.TATE "*The Arithmetic of elliptic curves*" Invent Math.23, 171-206 (1974)

[17] A.WEIL "*Les courbes algébriques et variétés abéliennes*" Hermann (1971).

[18] E.WEISS "*Algebraic Number Theory*" (1972).