République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université des Sciences et de la Technologie
Houari Boumediene

Faculté de Mathématiques

N° d'ordre : 28 / 2010 — M / MT

Mémoire

Présenté pour l'obtention du diplôme de MAGISTER
en : MATHEMATIQUES
Spécialité : Algèbre et Théorie des Nombres

Par : M^me^ KOUACHI Samia

Sujet

Espaces Homogènes de Courbes Elliptiques et groupes associés

Soutenu publiquement le : 01 / 07 / 2010 , devant le jury composé de :

Président : Mr AIDER Meziane	Professeur	à L'U. S. T. H. B
Directeur de thèse : Mr ZITOUNI Mohamed	Professeur	à L'U. S. T. H. B
Examinateurs : Mr BOUTABIA Hacene	Professeur	à L'U. B. M. Annaba
Mr HERNANE Mohand Ouamar	Maître de Conférence	à L' U. S. T. H. B
Mr HACHAÏCHI Mohamed Salah	Maître de Conférence	à L'U. S. T. H. B

Remerciements

J'exprime mes vifs remerciements et ma gratitude à mon directeur de thèse monsieur ZITOUNI Mohamed, professeur à l'.U.S.T.H.B de m'avoir proposé ce sujet, pour les conseils précieux qu'il m'a prodigués et pour sa total disponibilité à mon égard, tout au long de la réalisation de cette thèse.

Je remercie monsieur AÏDER Méziane, professeur à l'.U.S.T.H.B de l'honneur qu'il me fait en présidant mon jury.

Mes remerciements vont également à messieurs HERNANE Mohand Ouamar , maître de conférence à l'U.S.T.H.B, HACHAICHI Mohamed Salah, maître de conférence à l'U.S.T.H.B, BOUTABIA Hacene, professeur à L'Université Badji Mokhtar de Annaba pour avoir accepter d'examiner ma thèse et de participer au jury.

Notations usuelles de la Théorie Algébrique des Nombres

D'après « Théorie Algébrique des Nombres », Pierre SAMUEL, Masson Ed, Paris (1975)

$\mathbb{N}$ = monoïde des entiers naturels {0, 1, 2,…, n,…}, $\mathbb{N}$ pour naturel ;

$\mathbb{Z}$ = anneau des entiers rationnels $\{0, \pm 1, \pm 2, \dots, \pm n, \dots\}$, $\mathbb{Z}$ pour Zahlen = nombre en allemand ;

$\mathbb{Q}$ = corps des nombres rationnels $\left\{0, \frac{a}{b}, a \in \mathbb{Z}, b \in \mathbb{N}^*, a\ et\ b\ premiers\ entre\ eux\right\}$, $\mathbb{Q}$ pour quotient ;

$\mathbb{R}$ = corps des nombres réels $\{0, r_1, r_2, \dots\}$, $\mathbb{R}$ pour réel ;

$\mathbb{C}$ = corps des nombres complexes $\{a + ib, a\ et\ b\ réels, i^2 = -1, i \neq \pm 1, i\ non\ réel\}$

$/F_q$ = corps fini à $q = p^n$ élèments, *F* pour fini et pour Field = corps en anglais ;

A[x] = anneau des polynômes $f(x) = a_0 + a_1 x + \cdots + a_n x$, à coefficients a_i dans $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$;

Nombre algébrique = zéro θ d'un polynôme $f(\theta) = 0$;

A(x) = corps des fractions rationnelles

$$\frac{f(x)}{g(x)} = quotient\ de\ 2\ polynomes\ f(x) et\ g(x) premiers\ entre\ eux\ et\ g(x) \neq 0$$

A[x, y]= anneau des polynômes $(x, y) = \sum_{i,j \geq 0} a_{i,j} x^i y^j$, $a_{i,j}$ dans *A*

A(x, y)= corps des fractions rationnelles $f(x, y)/g(x, y)$ polynômes *f* et *g* premiers entre eux et $g \neq 0$.

Sommaire

Chapitre I *Cubiques de WEIERSTRASS*

Chapitre II *Groupes de MORDELL-WEIL* $E(K)$

Chapitre III *Espaces homogènes*

Introduction

Les espaces homogènes qui nous intéressent concernent les Courbes Elliptiques. Nous sommes donc amenés à décrire quelques aspects de la Théorie des Courbes Elliptiques: Cubiques de WEIERSTRASS

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

Espaces affines $IA^n(K)$, Espaces projectifs $IP^n(K)$, Point à l'infini, transformations linéaires de l'équation de WEIERSTRASS, invariants des cubiques de WEIERSTRASS, les deux types des Courbes Elliptiques. C'est l'objet du chapitre I.

Dans le chapitre II, nous déterminons la structure algébrique du groupe de MORDELL-WEIL, les coordonnées des points $-P$, $P_1 + P_2$, $2P$. Nous calculons les coordonnées mP de torsion pour $m > 0$ du groupe de MORDELL-WEIL. Nous nous intéressons aux sous groupes de m-torsion et aux groupes de torsion des Courbes Elliptiques.
La dernière partie de ce chapitre est consacrée aux valuations et aux réductions des Courbes Elliptiques.

Dans le chapitre III, nous étudions les isomorphismes des groupes de MORDELL-WEIL. Ensuite nous étudions les espaces homogènes liés aux Courbes Elliptiques et les groupes associés : les groupes de Chatelet-Weil, les groupes de Selmer et les groupes de Chafarevich-Tate.
Ces groupes sont construits à l'aide d'isogénies, de m −torsion, des groupes de cohomologie et des groupes $WC(E/K_v)$.

CHAPITRE I – CUBIQUES DE WEIERSTRASS ET COURBES ELLIPTIQUES

D'après CASSELS [15] et SILVERMAN [12] la théorie des espaces homogènes est basée sur les groupes de MORDELL-WEIL et les groupes de cohomologie H^n de groupes abélien finis.

Nous commençons par la théorie des Courbes Elliptiques, qui est exposée dans plusieurs ouvrages: [3], [7], [12], [15], [16].

1. Cubiques de WEIERSTRASS – équation affine - équation projective

Les Cubiques de WEIERSTRASS sont des courbes algébriques planes, particulières dans l'ensemble des cubiques planes.

Définition 1

Une cubique de WEIERSTRASS est une courbe algébrique plane d'équation particulière formée de sept monômes :

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

$K = corps\ commutatif, global, local\ ou\ fini.$

Exemples

$$y^2 - 10xy + 21y = x^3 + 3x^2 + 14x + 40 \ \in \mathbb{Q}[x,y]$$

Définition 2

Un espace affine sur un corps algébriquement clos K est l'ensemble $I\mathrm{A}^{\mathrm{n}}(K)$ *formé des n-uples* $a = (a_1, \dots, a_n)$ *d'éléments* $a_1, \dots, a_n$ *de K :*

$$I\mathrm{A}^{\mathrm{n}}(K) \ = \{a = (a_1, \dots, a_n) \, , a_i \in K \}$$

En langage géométrique l'élément $a = (a_1, \dots, a_n)$ est un point de l'espace $\mathrm{IA}^{\mathrm{n}}(\mathrm{K})$ à n coordonnées $a_1, \dots, a_n$ dans le corps K ; l'exposant n est égal à la dimension de l'espace affine $IA^n(K)$.

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

$$f : \ IA^n(K) \longrightarrow K$$

de valeur :

$$f(a) = f(a_1, \dots, a_n)$$

Dans les espaces affines $IA^{n+1}(K)$ nous déterminons une relation d'équivalence $\mathcal{R}$ entre deux points de $IA^{n+1}(K)$, $a = (a_1, \dots, a_{n+1})$ et $b = (b_1, \dots, b_{n+1})$ avec la relation $a\,\mathcal{R}\,b$ si et seulement si $b = ta$ pour un certain élément $t \neq 0$ du corps K avec $b = (ta_1, \dots, ta_{n+1})$.

Définition 3

Un n-espace projectif sur un corps algébriquement clos K est l'ensemble $IP^n(K)$ des classes d'équivalence de points $P = (a_1, \dots, a_{n+1})$, à $n+1$ coordonnées a_i non toutes nulles dans K, avec la relation $\mathcal{R}$ d'équivalence :
$(a_1, \dots, a_{n+1})\ \mathcal{R}\ (b_1, \dots, b_{n+1})$ *si et seulement si :*

$$b_1 = ta_1\ ,\ \dots\ \dots\ \dots,\ b_{n+1} = ta_{n+1}$$ *pour tout élément t non nul du corps K.*

Cette relation satisfait les axiomes de réflexivité, symétrie, et transitivité.

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

$$IP^n(K) = IA^{n+1}(K) - \{(0,0, \dots, 0)\}/\mathcal{R}$$

Pour obtenir l'équation (1) de la courbe C dans le plan projectif $IP^2(K)$, nous faisons le changement de variables :

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

Alors l'équation (1) devient, après multiplication par Z^3 :

$$C' : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \ \in IP^2(K)[X, Y, Z]$$

Le plan projectif $IP^2(K)$ contient un point remarquable: $O_C = (0,1,0)$

Proposition 1

Le point $O_C = (0,1,0)$ est un point simple des cubiques de WEIERSTRASS.

Preuve

Soit $F(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 \ \in IP^2(K)[X, Y, Z]$

Alors $F(O_C) = F(0,1,0) = 0$; donc le point O_C est un point de la cubique C.

Par la théorie des courbes algébriques, les points singuliers $P = (X, Y, Z)$ sont solutions du système de quatre équations algébriques :

$$F(P) = 0$$
$$F'_X = a_1YZ - 3X^2 - 2a_2XZ - a_4Z^2 = 0$$
$$F'_Y = 2YZ + a_1XZ + a_3Z^2 = 0$$
$$F'_Z = Y^2 + a_1XY + 2a_3YZ - a_2X^2 - 2a_4XZ - 3a_6Z^2 = 0$$

Alors $F'_X(O_C) = 0$; $F'_Y(O_C) = 0$ et $F'_Z(O_C) = 1$ cela implique que ce point $O_C = (0,1,0)$ est simple.

■

Dans le plan Oxy, ce point O_C est égal à $O_C = (\infty, \infty)$; c'est le point à l'infini des cubiques de WEIERSTRASS.

IL est déterminé par la direction de l'axe Oy selon les coordonnées $O_C = (0,1,0)$ projectives.

2. Transformations linéaires des équations de WEIERSTRASS

L'équation (1) peut être transformée par des changements linéaires convenables des variables x et y.

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

$$x = X \quad ; \quad y = \frac{1}{2}(Y - a_1X - a_3) \qquad (1)$$

élimine les monômes en xy et en y dans l'équation (1) ; l'équation (1) de la cubique devient :

$$C_1 : \ Y^2 = 4X^3 + b_2X^2 + 2b_4X + b_6 \qquad (2)$$

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

$$b_2 = a_1^2 + 4a_2 \quad , \quad b_4 = a_1a_3 + 2a_4 \quad , \quad b_6 = a_3^2 + 4a_6 \qquad (3)$$

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

$$X = \frac{x - 3b_2}{36} \quad ; \quad Y = \frac{y}{108}$$

élimine le monôme en X^2 et le coefficient 4 du monôme en X^3 dans l'équation (2), l'équation (2) devient :

$$C_2 : \ y^2 = x^3 - 27c_4x - 54c_6 \qquad (4)$$

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

$$c_4 = b_2^2 - 24b_4 \quad ; \quad c_6 = 36\, b_2 b_4 - b_2^3 - 216 b_6 \tag{5}$$

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

1) Le modèle de Cassels :

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

3) *Le modèle de Deuring :*

$$y^2 + txy + y = x^3 \,, \ avec\ t^3 \neq 3$$

2) Le modèle de Legendre :

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

4) *Le modèle lié aux nombres congruents* n ***: [10]***

$$y^2 = x(x^2 - n^2)\,, \qquad n \in \mathbb{Z}$$

5) *Le modèle de Tate :*

$$y^2 + xy = x^3 + a_4 x + a_6 \,, \ \ pour\ a_4, a_6 \ \in \mathbb{C}$$

3. Invariants des cubiques de WEIERSTRASS

Définition 4

Un invariant d'une cubique C *est une fonction* $f(a_i)$ *des coefficients* a_i *de* C *; cela implique que ces invariants prennent des valeurs qui varient avec les coefficients* a_i*; ils permettent de classifier l'ensemble des cubiques.*

Les invariants b_{2i} et c_{2i} ont été calculés dans $(2-3)$ et $(2-4)$ précédents.

Définition 5

Le discriminant d'une cubique de WEIERSTRASS (1) *est égal à:*

$$\Delta(C) = 9b_2 b_4 b_6 - 8b_4^3 - 27b_6^2 - b_2^2 b_8 \ \in K\ avec\ carac(K) \neq 2,3 \ ; \ et\ 4b_8 = b_2 b_6 - b_4^2$$

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

Exemples

1) Modèle $y^2 = x^3 + Ax + B$; alors $\Delta(C) = -16(4A^3 + 27B^2)$;
2) Modèle de Deuring ; alors $\Delta(C) = t^3 - 27$;
3) Modèle de Legendre ; alors $\Delta(C) = -16t^2(t+1)^2$.

Définition 6

L'invariant modulaire d'une cubique de WEIERSTRASS est égal à:

$$j(C) = \frac{c_4^3}{\Delta(C)} \quad pour \quad carac(K) \neq 2,3$$

4. Résultant de deux polynômes

Définition 7

Soit deux polynômes $f(x)$ et $g(x)$ à coefficients dans un corps K :

$$f(x) = a_0x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \quad de\ degré\ n > 0\ ;$$

et (6)

$$g(x) = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0 \quad de\ degré\ m > 0\ ;$$

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

$$Res(f,g) = \begin{vmatrix} a_0 & a_1 & \dots\ \dots & a_n & \dots \\ 0 & a_0 & \dots\ \dots & a_{n-1} & a_n \\ 0 & \dots & a_0a_1 & \dots & \dots \\ b_0 & b_1 & \dots b_m & \dots & \dots \\ 0 & b_0 & b_1\ \dots & b_m & \dots \\ \dots & \dots & b_0\ b_1 & \dots & b_m \end{vmatrix}$$

Avec m lignes $L_i = (a_0 \dots a_n)$ et n lignes $L'_i = (b_0 \dots b_m)$, les termes qui manquent dans ce déterminant sont remplacés par des zéros ; la diagonale principale est formée de m termes a_0 et n termes b_m.

Les résultats suivants sont énoncés sans démonstration ; ils peuvent être consultés dans les ouvrages ≪ Algebra ≫ **[13]** de Lang et ≪ Introduction à l'Algèbre ≫ **[11]** de Kostrikin.

Proposition 2

Soient les polynômes f et g des formules (1)*, un scalaire non nul λ et le résultant $Res(f,g)$ des deux polynômes, alors :*

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

2) $Res(f,g)$contient le monôme $a_0^m b_0^n$; (7)

3) $Res(\lambda f, g) = \lambda^m Res(f,g)$;

4) $Res(f,\lambda g) = \lambda^n Res(f,g)$.

Preuve

Cf. [11], [13]

■.

Proposition 3

Soient deux polynômes f et g factorisés sous la forme :

$f(x) = a_0(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$, *de degré* n

$g(x) = b_0(x-\beta_1)(x-\beta_2)\dots(x-\beta_m)$, *de degré* m.

alors leur résultant est égal au produit :

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

Preuve cf. **[11]**

■

Cette formule du résultant implique le:

Corollaire

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

Preuve cf. **[11]**

■

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

Proposition 4

Soit un polynôme $f(x)$ de degré n :

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

alors le résultant de $f(x)$ et de sa dérivée $f'(x)$ est égal au produit :

$$Res(f,f') = a_0^{n-1}\prod_{1\le i\le n} f'(\alpha_i)$$

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

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

Preuve cf. **[11]**

■

Exemples

1. Polynôme quadratique $f(x) = ax^2 + bx + c$; $a \neq 0$ et sa dérivée $f'(x) = 2ax + b$

   Le résultant $Res(f, f')$ de f et f' est égal à :

   $$Res(f, f') = \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = -a(b^2 - 4ac)$$; d'où $Dis(f) = b^2 - 4ac$

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

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

   Par le calcul nous obtenons la valeur du résultant :

   $$Res(f, f') = a\left[18abcd + b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2\right];$$

   son discriminant est égal à :

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

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

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

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

   le discriminant est égal à

   $$Dis(f) = -(4p^3 + 27q^2)$$ (« Algebra » p 141. de S. Lang)

4. Soit une cubique C d'équation de WEIERSTRASS *:*

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

   avec les formules du $Res(f, f')$ et du discriminant de$f$, nous obtenons :

   $$Dis(f) = 16[9b_2b_4b_6 - 8b_4^3 - 27b_6^2 - b_2^2b_8]$$;

   alors, les discriminants de f et de C sont liés par la formule :

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

Proposition 5

Soit une cubique C d'équation de WEIERSTRASS :

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

Le discriminant $Dis(f)$ du polynôme f et le discriminant $\Delta(C)$ de la cubique C satisfont la relation :

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

Preuve cf. **[22]**

■

5. Nature des points d'une cubique de WEIERSTRASS - Le genre

Soit une cubique C dans le plan Oxy. Alors, un point P est soit ordinaire, soit singulier avec un nœud, soit singulier avec un point de rebroussement.

Proposition 6

Soit une cubique C de discriminant $\Delta(C)$ et d'invariant $c_4 = b_2^2 - 24b_4$, alors :

1) *C est non singulière si et seulement si $\Delta(C) \neq 0$.*

2) *C est singulière et admet un nœud si et seulement si $\Delta(C) = 0$ et $c_4 \neq 0$.*

3) *C est singulière et admet un point de rebroussement si et seulement si $\Delta(C) = c_4 = 0$.*

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

Soit une cubique C non singulière ; alors elle admet une équation de la forme :

$$C : y^2 = (x - e_1)(x - e_2)(x - e_3) = f(x) \ \ avec\ e_i \neq e_j\ pour\ i \neq j \qquad (1)$$

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

$$Dis\big(f(x)\big) = cRes(f, f')\ ou\ c = constante\ non\ nulle\ et\ f' = dérivée\ de\ f \qquad (2)$$

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

$$Dis\big(f(x)\big) = 16\,\Delta(C) \qquad (3)$$

Les formules (9), (10), et (11) impliquent la relation :

$$\Delta(C) = c_1 Res(f, f')\ ou\ c_1 = constante\ non\ nulle \qquad (4)$$

La définition des racines multiples d'un polynôme $f(x)$ et la relation (1) impliquent que les racines de la dérivée $f'(x)$ ne sont pas racine de $f(x)$.

Il en résulte la condition :

$$Res(f, f') \neq 0 \qquad (5)$$

Les relations (12) et (13) impliquent la valeur :

$$\Delta(C) \neq 0$$

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

Soit une cubique plane C d'équation :

$$C : y^2 = f(x) = 4x^3 + b_2x^2 + 2b_4x + b_6\ ; \qquad (1)$$

De discriminant :

$$\Delta(C) \neq 0 \qquad (2)$$

L'hypothèse"$\Delta(C) \neq 0$"et la relation $\Delta(C) = c_1 Res(f, f')$ implique :

$$Res(f, f') \neq 0 \quad (3)$$

La définition du résultant de deux polynômes $f(x)$ et sa dérivée $f'(x)$ n'ont pas de racine commune. Donc le polynôme $f(x)$ admet trois racines simples.

Il en résulte que la cubique C est non singulière donc la cubique C est une Courbe Elliptique.

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

D'après la proposition 6, la cubique est singulière lorsque son discriminant est nul :

$$\Delta(C) = 0 \quad (1)$$

L'équation de la cubique C est de la forme :

$$C : \mathrm{y}^2 = (\mathrm{x} - \mathrm{e}_1)^2(\mathrm{x} - \mathrm{e}_2) = \mathrm{h(x)} \quad (2)$$

Les polynômes h et h′ ont un zéro commun e_1, il en résulte la valeur du résultant de h(x) et de sa dérivée h′(x) :

$$\mathrm{Res(h, h')} = 0 \quad (3)$$

L'hypothèse « la cubique 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 dérivée y′ calculée avec la dérivée de la courbe E :

$$2\mathrm{yy'} = 12\mathrm{x}^2 + 2\mathrm{b}_2\mathrm{x} + 2\mathrm{b}_4 = \mathrm{h'(x)} \quad (4)$$

Les pentes au nœud ont pour valeurs :

$$\mathrm{y'} = \frac{6\mathrm{x}^2 + \mathrm{b}_2\mathrm{x} + \mathrm{b}_4}{\mathrm{y}} = \frac{\mathrm{N(x)}}{\mathrm{y}} \quad (5)$$

Le discriminant du polynôme quadratique N(x) vaut :

$$\mathrm{Dis}\big(\mathrm{N(x)}\big) = \mathrm{b}_2^2 - 24\mathrm{b}_4 = \mathrm{c}_4 \quad (6)$$

Il en résulte la condition $\mathrm{c}_4 \neq 0$ (7)

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

Soit la cubique C d'équation de WEIERSTRASS :

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

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

Cette racine double détermine un point singulier de la cubique C. (2)

L'hypothèse $c_4 \neq 0$ et $Dis\big(N(x)\big) = b_2^2 - 24b_4 = c_4(C)$ implique la valeur :

$$Dis\big(N(x)\big) \neq 0 \quad (3)$$

Cela implique que le polynôme $N(x)$ admet deux racines simples. Donc ce point singulier est un nœud de la cubique C. (4)

■

Preuve de « la cubique C admet un point de rebroussement » implique « $\Delta(C) = c_4 = 0$ »

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

Soit la cubique plane C d'équation de WEIERSTRASS :

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

Par définition d'un point de rebroussement d'une courbe algébrique, la cubique C admet deux tangentes confondues en ce point de rebroussement.

Cela donne une racine double du polynôme :

$$N(x) = 6x^2 + b_2x + b_4 \quad (2)$$

Cela implique la valeur du discriminant :

$$Dis\big(N(x)\big) = 0 \quad (3)$$

Les formules (22) et (24) impliquent la valeur :

$$c_4(C) = 0 \quad (4)$$

Preuve de « $\Delta(C) = c_4 = 0$ » implique « la cubique C admet un point de rebroussement »

Soit une cubique plane C d'invariant $\Delta(C) = c_4(C) = 0$.

L'hypothèse $\Delta(C) = 0$ implique que la cubique C est singulière. (1)

L'hypothèse $c_4 = 0$ et la formule du discriminant :

$$Dis\big(N(x)\big) = b_2^2 - 24b_4 = c_4 \quad (2)$$

Impliquent que le polynôme $N(x)$ admet une racine double. Il en résulte deux tangentes confondues au point singulier. Ce point singulier est donc un point de rebroussement. (3)

■

Exemples

1. Cubique de WEIERSTRASS singulière qui admet un nœud :

$$C_1 \ : \ y^2 = x^3 + 6x^2 + 9x + 4$$

Je calcule les invariants :

$b_2 = 24$, $b_4 = 18$, $b_6 = 16$, $b_8 = 15$, $\Delta(C_1) = 0$, $c_4(C_1) = 144 \neq 0$

$\Delta(C_1) = 0$ implique que la cubique C_1 est singulière avec un nœud.

Tableau des coordonnées de quelques points de la cubique:

x	-5	-4	-1	0	1	2
y^2	-16	0	0	4	20	54
y	Non réels	0	0	± 2	$\pm 2\sqrt{5}$	$\pm 3\sqrt{6}$

Ce tableau indique que le point $S = (-1,0)$ est le nœud de la cubique C_1. (fig.1)

2. Cubique de WEIERSTRASS singulière qui admet un point de rebroussement :

$$C_2 \ : \ y^2 - 2xy = x^3 - x^2$$

Je calcule les invariants :

$$b_2 = 0 \, , \quad b_4 = 0 \ , \quad b_6 = 0 \, , \quad b_8 = 0 \, , \quad \Delta(C_2) = 0 \, , \quad c_4(C_2) = 0$$

Les valeurs $\Delta(C_2) = c_4(C_2) = 0$ impliquent que la cubique C_2 admet un point de rebroussement.

Tableau des coordonnées de quelques points de la cubique :

x	-2	-1	0	1	2
$y^2 - 2xy$	-12	-2	0	0	4
y	Non réels	Non reels	0	$0 \ et \ 2$	$2 \pm 2\sqrt{2}$

Ce tableau indique que le point $S = (0,0)$ est le point de rebroussement de la cubiqueC_2. (fig.2).

$C_1 : y^2 = x^3 + 6x^2 + 9x + 4$

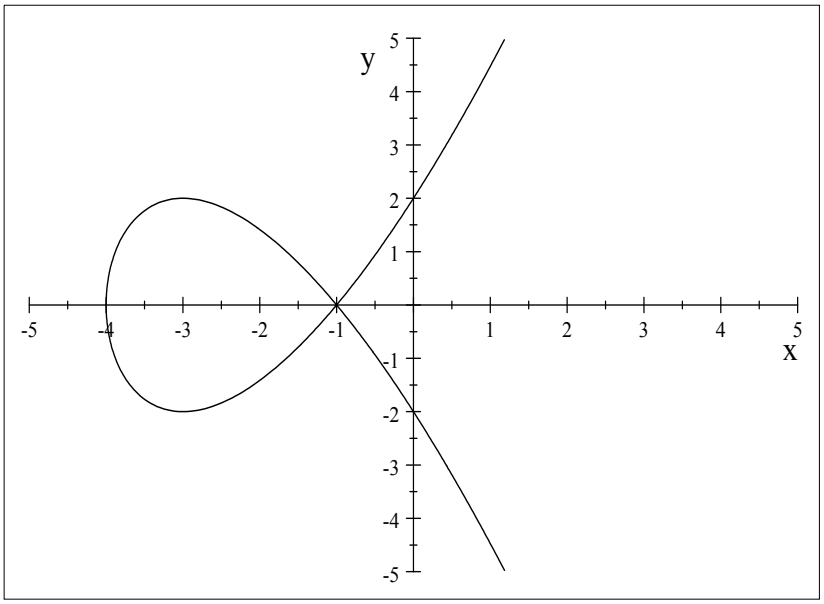


*fig.*1. *avec le logiciel Scientific WorkPlace*

$C_2 : y^2 - 2xy = x^3 - x^2$

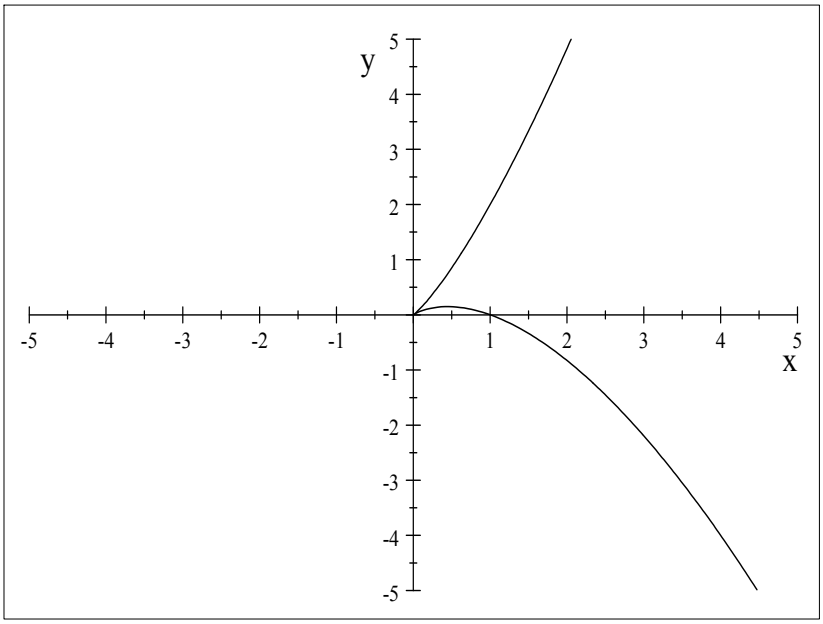


*fig.*2. *avec le logiciel Scientific WorkPlace*

Définition 8 [7]

Le genre d'une courbe algébrique plane C de degré $n \geq 2$ est l'entier naturel :

$$g(C) = \frac{(n-1)(n-2)}{2} - s\,,\ s = nombre\ de\ points\ singuliers.$$

Les courbes algébriques d'équations $d_1x + d_2y + d_3 = 0$ de degré 1, sont des droites ; elles sont de genre $g(C) = 0$.

Les courbes algébriques d'équations $d_1x^2 + d_2xy + d_3y^2 + d_4x + d_5y + d_6 = 0$, de degré 2, sont des coniques (paraboles, ellipses, hyperboles, cercles) ; elles sont de genre $g(C) = 0$.

Les courbes algébriques d'équations $d_1x^3 + d_2x^2y + d_3xy^2 + d_4y^3 + d_5x^2 + d_6xy + d_7y^2 + d_8x + d_9y + d_{10} = 0$, de degré 3, sont des cubiques ; elles sont de genres 0 ou 1. Celles qui sont de genre $g(C) = 1$ sont des Courbes Elliptiques ; celles qui sont de genre $g(C) = 0$ sont des cubiques singulières.

6. Les deux types de Courbes Elliptiques

D'après la proposition 6, les Courbes Elliptiques ont des discriminants $\Delta(C) \neq 0$; cela implique 2 cas : Courbes Elliptiques de discriminants $\Delta(C) > 0$ et celles de $\Delta(C) < 0$.

Définition 9

Les Courbes Elliptiques sont des cubiques de WEIERSTRASS non singulières, les Courbes Elliptiques sont de deux types suivant le signe de $\Delta(C)$.

Proposition 7

1) La Courbe C coupe l'axe Ox en trois points simples si et seulement si $\Delta(C) > 0$.

2) La Courbe C coupe l'axe Ox en un seul point, qui est simple, si et seulement si $\Delta(C) < 0$.

Preuve de « C coupe l'axe Ox en trois points simples » implique « $\Delta(C) > 0$ »

Soit une Courbe Elliptique d'équation de WEIERSTRASS :

$$C : \ y^2 = f(x) = x^3 + a_2x^2 + a_4x + a_6 \qquad (1)$$

alors son discriminant n'est pas nul : $\Delta(C) \neq 0$; (2)

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

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

$$y^2 = (x - e_1)(x - e_2)(x - e_3) = f(x) \qquad (3)$$

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

$$Dis\big(f(x)\big) = \prod_{1 \leq i < j \leq 3} \big(e_i - e_j\big)^2 \ ; \qquad (4)$$

Les trois abscisses e_i étant réelles ; la formule (24) implique :

$$Dis\big(f(x)\big) > 0 \qquad (5)$$

Les relations entre les discriminants de $f(x)$ et de C et la formule (25), implique le signe du discriminant de C :

$$\Delta(C) > 0 \qquad (6)$$

Preuve de « C coupe l'axe Ox en un seul point simple » implique « $\Delta(C) < 0$ »

Soit une Courbe Elliptique C d'équation de WEIERSTRASS :

$$C : \ y^2 = f(x) = x^3 + a_2x^2 + a_4x + a_6 \qquad (1)$$

L'hypothèse C coupe l'axe Ox en un seul point simple $(e, 0)$ transforme l'équation (2) en :

$$y^2 = f(x) = (x - e)(x^2 + mx + n) \ \ avec \ \ r^2 - 4s < 0 \qquad (2)$$

Le polynôme du deuxième degré $x^2 + mx + n$, admet deux racines complexes conjuguées :

$$c \pm id \qquad (3)$$

D'après (27) et (28), le discriminant du polynôme $f(x)$ est égal à :

$$Dis\big(f(x)\big) = -4^5b^2((e - c)^2 + d^2)^2 \qquad (4)$$

Les nombres e, c, d sont réels, il en résulte :

$$Dis\big(f(x)\big) < 0 \qquad (5)$$

La relation entre les discriminants de C, de $f(x)$ et la formule (30) impliquent :

$$\Delta(C) < 0 \qquad (6)$$

■

Les cubiques planes C se répartissent dans 4 classes suivant leurs discriminants $\Delta(C)$ et leurs invariants c_4. Nous avons démontré le :

Corollaire

Les Cubiques de WEIERSTRASS sont classifiées dans 4 classes :

1- *Classe des cubiques singulières avec un nœud lorsque* $\Delta(C) = 0$ *et* $c_4 \neq 0$
2- *Classe des cubiques singulières avec un point de rebroussement lorsque* $\Delta(C) = c_4 = 0$.
3- *Classe des Courbes Elliptiques formées d'une branche fermée finie et d'une branche infinie qui coupe l'axe* Ox *en trois points simples lorsque* $\Delta(C) > 0$.
4- *Classe des Courbes Elliptiques formées d'une branche infinie qui coupe l'axe* Ox *en un seul point simple lorsque* $\Delta(C) < 0$.

■

Exemples

1. Courbe Elliptique qui coupe l'axe Ox en trois points simples:

$$C_1 \ : \ y^2 = x^3 - 4x$$

Je calcule les invariants :

$$b_2 = 0\,, \quad b_4 = -8\,, \quad b_6 = 0\,, \quad b_8 = -16\,, \quad \Delta(E_1) = 8^4 > 0$$

Donc C_1 est une Courbe Elliptique qui coupe l'axe Ox en trois points simples de coordonnées :

$$(x_1, y_1) = (-2,0) \ ; \quad (x_2, y_2) = (0,0) \ ; \quad (x_3, y_3) = (2,0) \qquad \text{(fig. 3)}$$

Tableau des coordonnées de quelques points de C_1 :

x	-4	-3	-2	-1	0	1	2	3
y^2	-48	-15	0	3	0	-3	0	15
y	Non réels	Non rée	0	$\pm\sqrt{3}$	0	Non réels	0	$\pm\sqrt{15}$

2. Courbe Elliptique qui coupe l'axe Ox en un seul point simple:

$$C_2 \ : \ y^2 = x^3 + x - 2$$

Je calcule les invariants :

$$b_2 = 0\,, \quad b_4 = 2\,, \quad b_6 = -8\,, \quad b_8 = -1\,, \quad \Delta(C_2) = -2^2 \times 7 \times 8^2 < 0$$

Donc C_2 est une Courbe Elliptique qui coupe l'axe $0x$ en un seul point simple de coordonnées $(1,0)$. (fig. 4)

Tableau des coordonnées de quelques points de C_2 :

x	-2	-1	0	1	2	3
y^2	-12	-4	-2	0	8	28
y	Non réels	Non réels	Non reels	0	$\pm 2\sqrt{2}$	$\pm 2\sqrt{7}$

$C_1 : y^2 = x^3 - 4x$

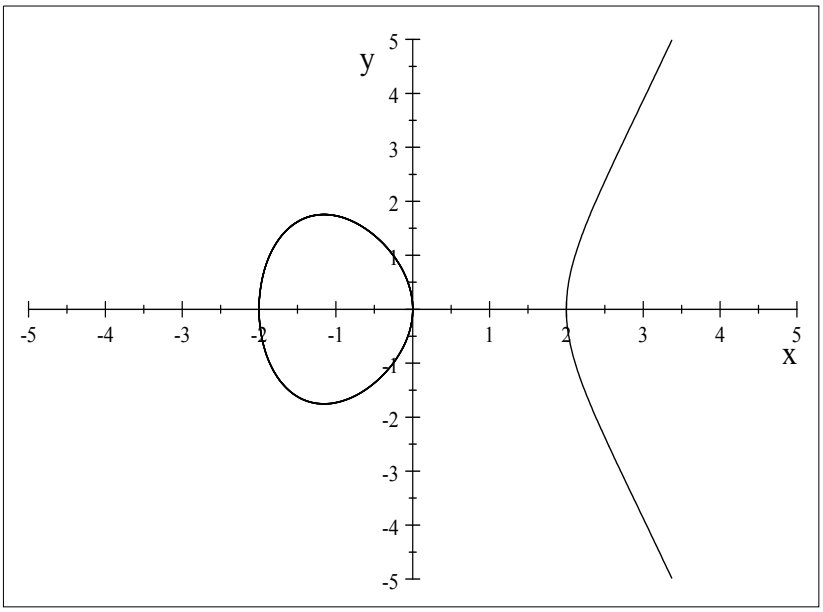


*fig.*3. *avec le logiciel Scientific WorkPlace*

$C_2 : y^2 = x^3 + x - 2$

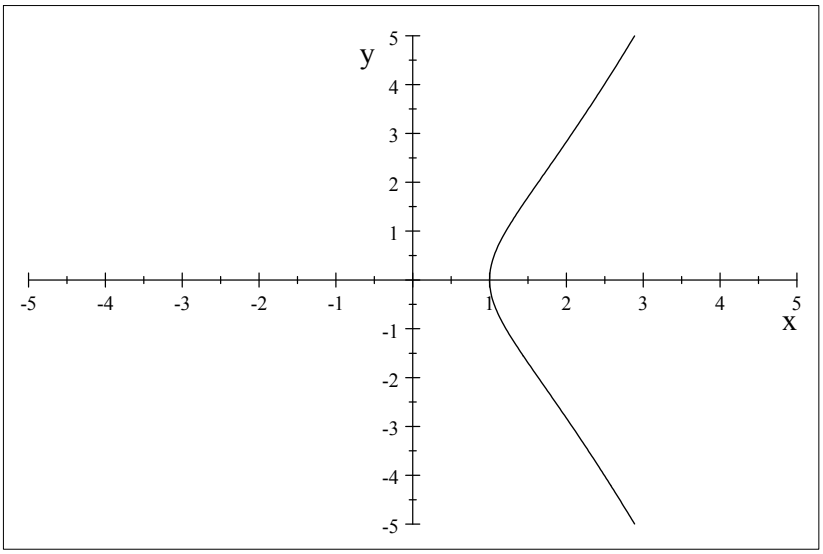


*fig.*4. *avec le logiciel Scientific WorkPlace*

CHAPITRE II – GROUPES DE MORDELL-WEIL DES COURBES ELLIPTIQUES

1. Les groupes de MORDELL-WEIL $E(K)$

Soit une Courbe Elliptique E sur un corps K, d'équation de WEIERSTRASS :

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

Sur la Courbe Elliptique E, nous construisons un groupe additif abélien, d'élément neutre le point $O_E = (\infty, \infty)$ à l'infini, par la :

Proposition 1

L'ensemble $E(K)$ des points K-rationnels d'une Courbe Elliptique E, admet une structure de groupe additif abélien, d'élément neutre le point $O_E = (\infty, \infty)$, avec la règle géométrique :

« Trois points colinéaires de E ont une somme nulle : $P_1 + P_2 + P_3 = O_E$ » ; (2)

et la loi de composition interne :

$$f \ : \ E(K) \times E(K) \longrightarrow E(K), avec\ f(P_1, P_2) = P_1 + P_2$$

Preuve

1) Soit un point P ; alors $P + O_E = O_E + P = P$, puisque le point O_E est déterminé par la direction de l'axe Oy.

L'axiome de l'élément neutre est vérifié.

2) Soit deux points $P\ et\ R$ sur E tels que $P + R + O_E = O_E$; alors PR est parallèle à Oy.

D'où $R = -P$.

L'axiome du symétrique est vérifié.

3) Toute sécante PR de la courbe E est confondue avec la sécante RP. Il en résulte la relation :

$$P + R = R + P$$

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 trois points $P_1 + P_2 + P_3$:

$$P_1 + P_2 = M_1 \ ; \ P_2 + P_3 = M_2 \text{ et } M_1 + P_3 = P_1 + M_2.$$

■

Définition 1

Les groupes abéliens $E(K)$ sont les groupes de MORDELL-WEIL des Courbes Elliptiques.

2. Coordonnées des points $-P$, $P_1 + P_2$, $2P$

Nous obtenons les coordonnées du symétrique $-\mathrm{P}$ d'un point P et de la somme $\mathrm{P}_1 + \mathrm{P}_2$ de deux points distincts $\mathrm{P}_1 \neq \mathrm{P}_2$, en utilisant la théorie algébrique des intersections d'une droite et d'une courbe.

Calcul des coordonnées du symétrique $-P$ d'un point P

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

$$P + (-P) = O_E$$

Le point $-P$ est l'intersection de la courbe E par la parallèle à Oy passant par P:

$$x = x_p$$

L'équation de WEIERSTRASS de E devient une équation en y du $2^{ème}$ degré, elle admet deux zéros y_p et Y ; leur somme est égale à la fonction symétrique élémentaire somme des zéros d'un polynôme :

$$Y + y_p = -(a_1 x_p + a_3)$$

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

$$-P = (x_p, -y_p - a_1 x_p - a_3)$$

Calcul des coordonnées du point somme $P_1 + P_2$ de deux points

$P_i = (x_i, y_i)$, pour $P_1 \neq P_2$:

La règle géométrique $P_1 + P_2 + P_3 = O_E$ implique $P_1 + P_2 = -P_3 = M$

Le point P_3 est obtenu avec l'intersection de E par la droite P_1P_2:

L'équation de la droite P_1P_2 est :

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

Cette sécante P_1P_2 coupe la courbe en trois points simples $P_1, P_2\ et\ P_3$.

Les abscisses de ces trois points sont les zéros de l'équation cubique en x :

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

La somme de ces zéros est égale à la fonction symétrique élémentaire somme des zéros d'un polynôme.

$$x_1+x_2+x_3=\lambda^2+a_1\lambda+a_3$$

Je calcule les coordonnées du point somme $P_1+P_2=-P_3=M=(x_M,y_M)$

$$P_1+P_2=M=\left.\begin{cases}x_M=\lambda^2+a_1\lambda-a_2-x_1-x_2\\ y_M=-\lambda^3-2a_1\lambda^2+\lambda(a_1+2x_1+x_2-a_1^2)+a_1a_2-a_3-y_1+a_1(x_1+x_2)\end{cases}\right\}\ avec\ \ \lambda=\frac{y_1-y_2}{x_1-x_2}$$

Nous avons démontré la :

Proposition 2

Soit une Courbe Elliptique E d'équation de WEIERSTRASS :

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

1) Le symétrique d'un point $P=(x,y)$ de $E(K)$ est le point : $-P=(x,-y-a_1x-a_3)$

2) La somme P_1+P_2 pour $P_1\neq\pm P_2$ est le point $M=P_1+P_2$ de coordonnées :

$$P_1+P_2=M=\left.\begin{cases}x_M=\lambda^2+a_1\lambda-a_2-x_1-x_2 \qquad , \quad x_1\neq x_2\\ y_M=-\lambda^3-2a_1\lambda^2+\lambda(a_1+2x_1+x_2-a_1^2)+a_1a_2-a_3-y_1+a_1(x_1+x_2)\end{cases}\right\}\ avec\ \ \lambda=\frac{y_1-y_2}{x_1-x_2}$$

■

Calcul des coordonnées du point $2P=P+P$:

Nous utilisons l'équation de la tangente à la courbe E au point $P=(x_P,y_P)$

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

Cette tangente a pour pente la dérivée $y'=t$:

$$y'=\frac{(3x_P^2+2a_2x_P+a_4-a_1y_P)}{(2y_P+a_1x_P+a_3)}=t$$

L'équation de WEIERSTRASS devient une équation en x cubique. Nous utilisons la fonction symétrique élémentaire somme des zéros de cette équation. Nous obtenons les coordonnées de $2P$ pour $P = (x_P, y_P)$.

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

$$\left\{ \begin{array}{l} x_{2P} = t^2 + a_1 t - a_2 - 2x_P \quad , \quad t = y'_P \\ \\ y_{2P} = -t^3 - 2a_1 t^2 + t(a_2 - a_1^2 + 3x_P) + a_1 a_2 - a_3 + 2a_1 x_P - y_P \end{array} \right\}$$

Nous avons démontré la :

Proposition 3

Soit une Courbe Elliptique E d'équation de WEIERSTRASS

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

Pour tout point $P = (x_P, y_P)$ du groupe de MORDELL-WEIL $E(K)$ de la Courbe Elliptique E, le point $2P$ a pour coordonnées :

$$\left\{ \begin{array}{l} x_{2P} = t^2 + a_1 t - a_2 - 2x_P \\ \\ y_{2P} = -t^3 - 2a_1 t^2 + t(a_2 - a_1^2 + 3x_P) + a_1 a_2 - a_3 + 2a_1 x_P - y_P \\ \\ avec\ t = \dfrac{(3x_P^2 + 2a_2 x_P + a_4 - a_1 y_P)}{(2y_P + a_1 x_P + a_3)} \quad ;\ carac(K) \neq 2, 3 \end{array} \right\}$$

■

3. Formules de torsion de CASSELS [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 désigne les sommes :

$$mP = \left\{ \begin{array}{ccc} P + P + \cdots + P & ; & m\ fois\ P \ ;\ si\ m\ est\ un\ entier\ naturel \\ -P - P - \cdots - P & ; & (-m) fois\ P \ ;\ si\ m\ est\ un\ entier\ négatif \\ O_E & ; & si\ m = 0 \end{array} \right\}$$

Calcul des coordonnées des points mP ; $m > 2$

Pour déterminer les coordonnées des points mP, nous utilisons la méthode de J.W.CASSELS [2].

Nous prenons des Courbes Elliptiques d'équation de WEIERSTRASS :

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

Les points mP ont pour coordonnées des fractions rationnelles :

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

Les polynômes ψ_m sont égaux à :

$\psi_{-1} = -1, \quad \psi_0 = 0\,, \quad \psi_1 = 1, \ \ \psi_2 = 2y,$ (1)

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

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

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

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad ; \quad m \geq 2 \tag{2}$$

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

Les polynômes ϕ_m et ω_m sont déterminés par les formules :

$$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1} \ ; \quad m \geq 2 \tag{4}$$

$$4y\omega_m = \psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2 = \frac{2y\psi_{2m}}{\psi_m} ; \quad m > 2 \tag{5}$$

Il en résulte la :

Proposition 4

Soit un point $P = (x, y)$ du groupe de MORDELL-WEIL $E(\mathbb{Q})$ d'une Courbe Elliptique E sur le corps $\mathbb{Q}$ des rationnels d'équation de WEIERSTRASS :

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

alors les coordonnées des points $mP = (x_m, y_m)$ du groupe $E(\mathbb{Q})$ sont :

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

Preuve

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

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

Pour $m > 2$, on utilise une relation de récurrence sur m.

C'est le lemme 7-2 dans **[2]**.

■

4. Sous groupes de m-torsion. Groupes de torsion

Définition 2

Pour tout entier 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

$$E(K)[m] = E[m] = \{P \in E(K)\ ; mP = O_E\} \qquad (1)$$

Définition 3

Le groupe de torsion d'une Courbe Elliptique E/K *est la réunion des sous groupes de*

m-torsion :

$$T(E) = \bigcup_{m\in\mathbb{Z}} E(K)[m] = \{P \in E(K)\ ;\ mP = O_E\ ; m \in \mathbb{Z}\}$$

Les groupes de torsion $\mathrm{T(E)}(K)$ sont d'ordre fini.

MAZUR a déterminé la structure des groupes de torsion $\mathrm{T(E)}(\mathbb{Q})$.

Théorème

Les groupes de torsion des Courbes Elliptiques $\mathrm{E}/\mathbb{Q}$ *sont des groupes additifs abéliens isomorphes à l'un des 15 groupes abéliens finis :*

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

$\mathbb{Z}/2\,\mathbb{Z} \oplus \mathbb{Z}/2d\,\mathbb{Z}\,,\ pour\ \ 1 \le d \le 4.$

Preuve cf. **[17]**

■

5. Théorème de MORDELL-WEIL

L'ensemble $E(K)$ des points K- rationnels d'une Courbe Elliptique E/K est un groupe additif abélien de type fini.

Preuve

Elle fait intervenir des fonctions spéciales : les fonctions hauteurs sur les groupes abéliens.

cf. **[13], [17]**

■

Corollaire

Les groupes de MORDELL-WEIL $E(K)$ des Courbes Elliptiques E/K sont isomorphes au produit de groupes abéliens additifs :

$$E(K) \approx T(E) \times \mathbb{Z}^r$$

où $T(E)$ sont les groupes de torsion des Courbes Elliptiques E, $r = r(E) \geq 0$ sont des entiers naturels et $\mathbb{Z}^r = r$ copies du groupe additif abélien $\mathbb{Z}$.

Preuve cf. **[13], [17]**

■

6. Valuations des corps-Réductions des Courbes Elliptiques

Définition 4

Une valuation d'un corps K est une fonction réelle :

$$v : K \longrightarrow \mathbb{R}_+,$$

qui satisfait les trois axiomes :

(val-1) $v(x) \geq 0$ *pour tout élément x et* $v(x) = 0$ *si et seulement si x=0 ;*

(val-2) $v(xy) = v(x)v(y)$ *pour tous x et y de K ;*

(val-3) il existe une constante réelle positive c telle que :

$$v(x) \leq 1 \; implique \; v(x+1) \leq c$$

Exemples

1. $K = corps\ \mathbb{R}\ des\ nombres\ réels$; $v(x) = \max(+x, -x)$; c'est la valeur absolue ordinaire des nombres réels x. L'axiome *(val-3)* est satisfait pour $c = 2$:
$$v(x) \leq 1 \; implique \; v(x+1) \leq 2$$

2. $K = corps\ \mathbb{C}\ des\ nombres\ complexes$; $v(x+iy) = (x^2 + y^2)^{\frac{1}{2}}$; c'est le module d'un nombre complexe. L'axiome *(val-3)* est satisfait pour $c = 2$:
$$v(x+iy) \leq 1 \; implique \; v(x+iy+1) \leq 2$$

3. Valuations $p-adiques\ du\ corps\ \mathbb{Q}$ des nombres rationnels, p premier. $v(p) = p^{-1}$; $v(q) = 1$ pour tout nombre premier q premier à p et $v(0) = 0$. L'axiome *(val-3)* est satisfait pour $c = 1$:

$$v(x) \leq 1\ implique\ v(x+1) \leq 1$$

4. La valuation triviale d'un corps K satisfait :

$$v(x) = 1\ pour\ tout\ x\ de\ K\ non\ nul\ et\ v(0) = 0$$

Une valuation v détermine un homomorphisme du groupe multiplicatif $K^\star$ du corps K dans le groupe multiplicatif $\mathbb{R}_+$ des nombres réels positifs.

Proposition 5

Soit une valuation : $v : K \longrightarrow \mathbb{R}_+$; d'un corps K.

Elle satisfait les relations :

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

Preuve

Par l'axiome *(val-2)* nous obtenons : $v(xy) = v(x)v(y)$

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

Dans l'anneau des entiers du corps K, cette équation admet deux solutions :

$$v(1) = 1\ et\ v(1) = 0$$

L'axiome *(val-1)* implique la solution : $v(1) = 1$

Le carré : $(-1)^2 = 1$ implique les valuations :

$$v(-1) = v(1) = 1\ ;\ v(-x) = v(x)\ ;\ \text{pour tout } x \in K$$

Le produit : $x(1/x) = 1$ implique les valuations :

$$v(1/x) = 1/v(x)\ ;\ \text{pour } x \text{ non nul}$$

Le quotient : $x/y = x(1/y)$ implique les valuations :

$$v(x/y) = v(x)/v(y)\ ;\ \text{pour } y \text{ non nul}$$

■

Dans la définition 1, il n'y a pas de valuation $v(x+y)$ d'une somme, alors l'axiome *(val-3)* peut être remplacé par « l'inégalité triangulaire » :

(val-4) $$v(x+y) \leq v(x) + v(y)$$

Cette relation est valable pour les triangles de sommets A, B *et* C : $AB + AC \leq BC$.
Dans l'ensemble $V(K)$ des valuations d'un corps K, il y a une relation d'équivalence.

Définition 5

Deux valuations v_1 *et* v_2 *d'un corps K sont équivalentes s'il existe un réel* $r > 0$, tel que :

$$v_1 = v_2^r$$

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

$$cl(v) = \{v^r, pour\ des\ réels\ r\ positifs\}$$

Définition 6

Chaque classe de valuation d'un corps K est un diviseur premier de K ; la classe de la valuation triviale est le diviseur premier trivial ; les classes des valuations non triviales sont des diviseurs premiers non triviaux.

Les valuations qui seront utilisées sont des valuations inéquivalentes qui sont donc des représentants des diviseurs premiers.

Classification des valuations d'un corps

Les valuations d'un corps sont classifiées dans trois classes :
les valuations archimédiennes, les valuations non archimédiennes et la valuation triviale.

Définition 7

Une valuation $v : K \longrightarrow \mathbb{R}_+$, *est archimédienne si elle satisfait :*

$$v(x) \leq 1\ implique\ v(x+1) \leq 2\ ;$$

une valuation v est non archimédienne si elle satisfait :

$$v(x) \leq 1\ implique\ v(x+1) \leq 1$$

Exemples

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

$$v(x) = \max(x, -x) \text{ est archimédienne}$$

2) *Les valuations p-adiques du corps* $\mathbb{Q}$ *des nombres rationnels p premiers.* $v(p) = 1/p$ *et* $v(q) = 1$ *pour tout nombre premier q premier à p et* $v(0) = 0$*, il en résulte que ces valuations p-adiques sont non archimédiennes.*

Proposition 6

Soit une valuation non archimédienne $v : K \longrightarrow \mathbb{R}_+$*, alors :*

1) $v(x+y) \leq \max\big(v(x), v(y)\big)$;
2) *Si* $v(x) < v(y)$ *alors* $v(x+y) = v(y)$;
3) *Si* $v(x_1) \geq v(x_t)$ *pour* $t = 2, 3, \dots, n$*, alors* $v(x_1 + \cdots + x_n) = v(x_1)$
4) *La relation :* $x_1 + x_2 + \cdots + x_n = 0$ *implique que* $v(x_t)$ *est maximal pour deux indices au moins.*

Preuve cf. WEISS [21], Corollary 1-3-2.

■

Valuations non archimédiennes et parties d'un corps K

A toute valuation non archimédienne : $v : K \longrightarrow \mathbb{R}_+$ nous associons les quatre parties de K :

l'anneau $A(v)$ des v-entiers ; c'est l'anneau de la valuation

$$A(v) = \{x \in K \,;\, v(x) \leq 1\} ;$$

le v-idéal maximal en v :

$$M(v) = \big\{x \in K \,; v(x) < 1\big\} ;$$

le groupe des v-unités :

$$U(v) = \{x \in K \,;\; v(x) = 1\} ;$$

le corps résiduel de la valuation :

$$K_{res} = A(v)/M(v)$$

Ce corps est de caractéristique non nulle p.

Ces quatre parties ne sont pas définies pour les valuations archimédiennes.

Valuations additives

Les valuations déjà étudiées sont multiplicatives par la formule :

$$v(xy) = v(x)\, v(y)$$

La fonction logarithme qui transforme un produit en une somme permet d'obtenir des valuations additives :

$$\log v(xy) = \log v(x) + \log v(y), \text{ pour } v(x), v(y) > 0$$

Définition 8

Toute valuation $v : K \longrightarrow \mathbb{R}_+$ *d'un corps K induit une valuation additive*

$$\lambda : K \cup (\infty) \longrightarrow \mathbb{R} \text{ ; de valeur } \lambda(x) = -\log\big(v(x)\big)$$

Cette valuation satisfait les trois relations :

$$\lambda(x) \in \mathbb{R} \ ; \ \lambda(0) = \infty \ ; \ et\ \lambda(1) = 0$$

$\lambda(xy) = \lambda(x) + \lambda(y), pour\ x, y \neq 0$;

$\lambda(x + y) \geq min\big(\lambda(x), \lambda(y)\big)$.

Réductions des Courbes Elliptiques

Dans les équations de Weierstrass des Courbes Elliptiques E, les cinq coefficients a_i et les deux variables x et y peuvent prendre des valeurs considérables dans un corps infini.

L'un des moyens de borner ces valeurs est la réduction avec une valuation non archimédienne discrète du corps. Le discriminant réduit peut être nul ; la courbe réduite est une cubique singulière.

Cela implique deux types de réductions : les bonnes qui réduisent les Courbes Elliptiques en Courbes Elliptiques, les mauvaises qui réduisent les Courbes Elliptiques en cubiques singulières.

Réductions des équations de WEIERSTRASS

Soit des Courbes Elliptiques E, d'équations de WEIERSTRASS :

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

Le corps commutatif K est pourvu d'une valuation v, non archimédienne, discrète, additive, et des objets associés $A_v, M_v, et\ K_{res} = A(v)/M(v)$.

Définition 9 [17]

Soit des Courbes Elliptiques E, d'équations de WEIERSTRASS :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \in \mathbb{Q}[x, y] \quad (1)$$

1. *La réduction modulo un nombre rationnel premier p est l'application :*

$$E(\mathbb{Q}) \longrightarrow \bar{E}(\mathbb{F}_p)$$

Alors les valuations p-adiques du corps $\mathbb{Q}$ réduisent ce corps aux corps finis $\mathbb{F}_p$ de p éléments.

$$a_i \longrightarrow \bar{a}_i \, mod \, p \, , x \longrightarrow \bar{x} \, mod \, p \, , y \longrightarrow \bar{y} \, mod \, p \, et \, P(x, y) \longrightarrow \bar{P}(\bar{x}, \bar{y})$$

2. *La réduction modulo une valuation v est l'application :*

$$E(K) \longrightarrow \bar{E}(K_{res})$$
$$(x, y) \longrightarrow \big(v(x), v(y)\big)$$

Exemple

Courbe Elliptique E d'équation de WEIERSTRASS :

$$E : y^2 - 5xy + 13y = x^3 + 15x^2 - 14x + 37 \in \mathbb{Q}[x, y]$$

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* (1) *en l'équation de la courbe réduite :*

$$\bar{E} : y^2 + 3y = x^3 + x + 2 \; \in \mathbb{F}_5[x, y]$$

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

$$b_2 = 0 \, ; b_4 = 2 \, ; \; b_6 = 2 \, ; \; b_8 = 4 \, ; \; c_4 = 2 \, ; \; c_6 = 3 \, ; \; \Delta(\bar{E}) = 3$$

Définition 10

L'équation (1) *de WEIERSTRASS est minimale en v si ses coefficients a_i sont v-entiers et son discriminant est minimal et v-entier.*

Les formules d'isomorphismes des Courbes Elliptiques impliquent des conditions de minimalité de l'équation :

$$v(a_i) \geq 0 \, pour \, i = 1, 2, 3, 4, 6 \; ; \; v\big(\Delta(E)\big) < 12 \; ; \; v(c_4) < 4 \; ; \; v(c_6) < 6.$$

Application de ce critère à l'exemple précèdent :

$$v_5(-5) = v_5(15) = 1 \ ; \ v_5(-14) = v_5(13) = v_5(37) = 0 \ ; \ v_5(c_4) = v_5\big(\Delta(E)\big) = 0$$

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

Classification des réductions

Les réductions des Courbes Elliptiques sont classifiées par la nature de la courbe réduite.

Définition 11

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) elle est multiplicative lorsque la courbe réduite a un nœud.*
    - *2.2) elle est additive lorsque la courbe réduite a un point de rebroussement.*

Il y a un autre vocabulaire en usage :

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

CHAPITRE III – ESPACES HOMOGENES

1. Isomorphismes de Courbes Elliptiques

Ce sont des isomorphismes des groupes de MORDELL-WEIL des Courbes Elliptiques

Proposition 1

Soit une Courbe Elliptique E, sur un corps K, et son groupe de MORDELL-WEIL $E(K)$. Alors l'application :

$$\text{f: } E(K) \longrightarrow E'(K),$$

de valeur $$\text{f}(x,y) = (\mu^2 X + r \quad , \quad y = \mu^3 Y + \mu^2 sX + t),$$

avec $$\mu, r, s, t \text{ dans } K \text{ et } \mu \neq 0,$$

est un isomorphisme des Courbes Elliptiques E et E'.

Preuve

Considérons une Courbe Elliptique E d'équation de WEIERSTRASS *:*

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad \in K[x,y] \tag{1}$$

La transformée de E par f est une courbe $\text{f}(E) = E'$, d 'équation de WEIERSTRASS :

$$E': \ Y^2 + a_1'XY + a_3'Y = X^3 + a_2'X^2 + a_4'X + a_6' \quad \in K[X,Y] \tag{2}$$

Le calcul des discriminants montre que :

$$\Delta(E') \neq 0 \tag{3}$$

Pour vérifier les formules d'isomorphisme de groupes, il faut comparer l'image $\text{f}(P+R)$ à la somme $\text{f(P)} + \text{f(R)}$ des images.

L'image du point à l'infini O_E est égale à $\text{f}\big((0,1,0)\big) = (0,1,0) = O_{E'}$. La condition $\mu \neq 0$ implique que l'image réciproque $\text{f}^{-1}(X,Y)$ contient un seul point (X,Y) :

$$X = \frac{x-r}{\mu^2}, \qquad Y = \frac{y - s(x-r) + t}{\mu^3}$$

■

Les relations entre les coefficients et les invariants des courbes isomorphes E et E' sont obtenues par des calculs. Les résultats obtenus sont résumés ci-dessous.

Relations entre coefficients et invariants de deux Courbes Elliptiques isomorphes

Les coefficients a_i et a_i' sont liés par les cinq relations :

$$\begin{aligned}
&\mu a_1' = a_1 + 2s\ ;\\
&\mu^2 a_2' = a_2 - sa_1 + 3r - s^2\ ;\\
&\mu^3 a_3' = a_3 + ra_1 + 2t\ ;\\
&\mu^4 a_4' = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st\ ;\\
&\mu^6 a_6' = a_6 + ra_4 + r^2 a_2 + r^3 - ta_3 - t^2 - rta_1.
\end{aligned} \qquad \text{(Is-1)}$$

Les coefficients b_i et b_i' sont liés par les quatre relations :

$$\begin{aligned}
&\mu^2 b_2' = b_2 + 12r\ ;\\
&\mu^4 b_4' = b_2 + rb_2 + 6r^2\ ;\\
&\mu^6 b_6' = b_6 + 2rb_4 + r^2 b_2 + 4r^3\ ;\\
&\mu^8 b_8' = b_8 + 3rb_6 + 3r^2 b_4 + r^3 b_2 + 3r^4\ ;
\end{aligned} \qquad \text{(Is-2)}$$

Les coefficients c_i et c_i' sont liés par les deux relations :

$$\begin{aligned}
&\mu^4 c_4' = c_4\ ;\\
&\mu^6 c_6' = c_6\ .
\end{aligned} \qquad \text{(Is-3)}$$

Les discriminants des deux courbes sont liés par la formule :

$$\mu^{12}\Delta(E') = \Delta(E) \qquad \text{(Is-4)}$$

Les invariants modulaires des deux courbes sont égaux :

$$j(E') = j(E) \qquad \text{(Is-5)}$$

La formule (Is-5) ci-dessus caractérise les Courbes Elliptiques isomorphes.

Proposition 2

Deux Courbes Elliptiques E et E' sur un corps K de $carac(K) \neq 2, 3$, sont isomorphes si et seulement si leurs invariants modulaires sont égaux.

Preuve de « E et E' sont isomorphes » implique « $j(E') = j(E)$ »

Soient deux Courbes Elliptiques E et E' isomorphes ; alors la formule (Is-5) implique l'égalité :

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

Preuve de « $j(E) = j(E')$ » implique « E et E' sont isomorphes »

Nous examinons les 3 cas :

$$j(E) = \text{ j}(E') = 0\ ,\ 1728\ et\ t \neq 0, 1728.$$

1. Pour $j(E) = \text{ j}(E') = 0$, nous prenons deux équations de WEIERSTRASS, un corps K de $carac(K) \neq 2, 3$.

   E : $y^2 = x^3 + a_4 x + a_6$, avec la condition $4a_4^3 + 27a_6^2 \neq 0$

   E' : $y'^2 = x'^3 + a'_4 x' + a'_6$ avec la condition $4a_4'^3 + 27a_6'^2 \neq 0$

   L'invariant modulaire d'une Courbe Elliptique est égal à :

   $$j(E) = 4(1728a_4^3)/(4a_4^3 + 27a_6^2)$$

   L'hypothèse d'égalité des invariants $j(E) = \text{ j}(E')$ implique les relations :

   $$a_4 = a'_4 = 0\ ,\ \ a_6 \neq 0\ \ et\ \ a'_6 \neq 0;$$

   Par les formules (Is-1) d'isomorphisme, il existe un élément $\mu \in K_{alg}$ tel que :

   $$\mu^6 a'_6 = a_6\ ;$$

   Cette équation admet, dans une clôture algébrique K_{alg} , 6 racines :

   $$\mu = \left(\frac{a_6}{a'_6}\right)^{1/6}\ ;$$

   Il en résulte les 6 isomorphismes : f : $E(K) \longrightarrow E'(K)$, de valeur :

   $$\text{f(x, y)} = (\mu^2 x, \mu^3 y)$$

2. Pour $j(E) = \text{ j}(E') = 1728$, nous gardons les équations de WEIERSTRASS des courbes $E\ et\ E'$.

   L'hypothèse sur $j(E)\ et\ \text{j}(E')$ implique les conditions :

   $$a_4 \neq 0, a'_4 \neq 0\ \ et\ \ \ a_6 = \ a'_6 = 0;$$

   Par les formules (Is-1) d' isomorphismes, il existe un élément $\mu \in K_{alg}$, tel que :

   $$\mu^4 a'_4 = a_4;$$

   Cette équation admet 4 racines :

   $$\mu = \left(\frac{a_4}{a'_4}\right)^{1/4}\ ;$$

   Il en résulte les 4 isomorphismes : f : $E(K) \longrightarrow E'(K)$;

   $$f(x, y) = (\mu^2 x, \mu^3 y);$$

3. Pour $j(E) = \text{j}(E') = t \neq 0,1728$, nous gardons les équations de WEIERSTRASS.

   La formule de $j(E)$ et l'hypothèse $j(E) = \text{j}(E') = t$, impliquent l'équation :

   $$4a_4^3(1728 - t) = 27a_6^2 t \ , \ t \neq 0,1728$$

   Cette équation admet la solution :

   $$a_4 = \frac{3t}{1728-t}; a_6 = \frac{2t}{1728-t} \quad , \quad t \neq 0,1728$$

   L'égalité $j(E) = \text{j}(E')$ implique la relation :

   $$a_4^3 a_6'^2 = a_4'^3 a_6^2,$$

   Par les formules (Is-1) d'isomorphismes, il existe un élément μ non nul tel que :

   $$\mu^4 a_4' = a_4 \; et \; \mu^6 a_6' = a_6;$$

   Nous en déduisons les solutions :

   $$\mu = \left(\frac{a_4}{a_4'}\right)^{1/4} = \left(\frac{a_6}{a_6'}\right)^{1/6};$$

   Il en résulte les isomorphismes : $E(K) \longrightarrow E'(K)$,

   $$(x, y) = (\mu^2 x \quad , \quad \mu^3 y)$$

   Alors la Courbe Elliptique E a pour équation de WEIERSTRASS :

   $$y^2 = x^3 + \frac{3tx}{1728-t} + \frac{2t}{1728-t} \quad \in K[x, y] \quad , \quad t \neq 0,1728$$

■

2. Isogénies de Courbes Elliptiques

Définition 1 [16]

Soit deux Courbes Elliptiques E et E' sur le même corps K, d'éléments neutres respectifs O_E et $O_{E'}$, de groupes de MORDELL-WEIL $E(K)$ et $E'(K)$.
Une isogénie de E sur E' est un homomorphisme $\lambda : E(K) \longrightarrow E'(K)$ qui satisfait les conditions :

1) $\lambda(O_E) = O_{E'}$;
2) $\lambda \neq 0$;
3) *λ est surjectif ;*
4) *le noyau de λ est un sous groupe fini de $E(K)$;*
5) $\lambda(P + R) = \lambda(P) + \lambda(R)$ *pour tous points P et R du groupe $E(K)$.*

Cette isogénie λ induit un homomorphisme :

$$\sum \text{n}_\text{P}\text{P} \longrightarrow \sum \text{n}_\text{P}\, \lambda(\text{P});$$

du groupe des classes de diviseurs de degré 0 sur E(K), dans le groupe correspondant de E′(K). Une isogénie possède des invariants : degré, isogénie duale.

Définition 2

Lorsqu'une courbe E est isogène à une courbe E', alors la courbe E' est isogène à E ; le noyau de cette isogénie est un sous groupe fini du groupe $E(K)$.
Le degré de l'isogénie λ est égal à l'ordre de ce sous groupe. A chaque isogénie est associée une isogénie duale par la :

Définition 3

L'isogénie duale d'une isogénie de degré d :

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

est le morphisme de groupes :

$$\hat{\lambda} : E'(K) \longrightarrow E(K)$$

qui satisfait les deux composées :

$\lambda\hat{\lambda}$ *est la multiplication par* d *sur* $E'(K)$
et $\hat{\lambda}\lambda$ *est la multiplication par* d *sur* $E(K)$.

Les isogénies de Courbes Elliptiques, étant des morphismes de variétés abéliennes, sont soumises à l'opération de composition des applications.

La construction d'une courbe isogène à une Courbe Elliptique E peut être réalisée avec la :

Proposition 3

Soit une Courbe Elliptique E, son groupe de MORDELL-WEIL $E(K)$. A chaque sous groupe fini F de $E(K)$, d'ordre d, correspond une isogénie λ, unique, séparable, de noyau F et de degré d:

$$\lambda : E(K) \longrightarrow E(K)/F = E'(K).$$

Preuve

Les points du sous groupe F sont simples ; donc l'isogénie est séparable. L'image $\lambda(O_E)$ du point neutre est la classe du sous groupe F, qui contient ce point neutre.
Cette application canonique est donc surjective. Elle satisfait les conditions des isogénies.

■

Formules d'isogénie de VELU [19]

Indiquons la technique utilisée par VELU.

Soit une Courbe Elliptique E d'équation de WEIERSTRASS :

$$E \ : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad \in \mathbb{Q}[x,y] \ ; \tag{1}$$

Sur le corps $\mathbb{Q}(E) = \mathbb{Q}(x,y)$ des fonctions rationnelles sur $\mathbb{Q}$, nous associons à tout point $P \neq O_E$, une valuation v_P de valeur :

$$v_P(x) \geq 0 \ ; \quad v_P(y) \geq 0 \tag{2}$$

Au point à l'infini O_E, nous associons la valuation v_0 de valeur :

$$v_0(x) = -2 \quad et \quad v_0(y) = -3 \tag{3}$$

Mettons l'équation de E sous la forme :

$$H(x,y) = x^3 + a_2x^2 + a_4x + a_6 - y^2 - a_1xy - a_3y \ = 0 \tag{4}$$

Par définition, l'invariant différentiel de E est égal à :

$\omega(E) = \frac{dx}{-H'_y} = \frac{dy}{H'_x}$, $dH = H'_x dx + H'_y dy$

où les dérivées partielles de la fonction $H(x,y)$ sont égales à :

$$H'_x = 3x^2 + 2a_2x + a_4 - a_1y \ \text{ et } \ H'_y = -(2y + a_1x + a_3) \tag{5}$$

En posant $z = -x/y$, nous obtenons les développements de x et de y en z :

$$x = z^{-2} - d_1\, z^{-1} - 1 - d_2 - d_3z - d_4z^2 - d_5z^3 \ldots ; \tag{6}$$
$$y = -x/z = -z^{-3} + d_1z^{-2} + d_2z^{-1} + d_3 + d_4z + d_5z^2 + \cdots$$

Il en résulte des relations entre les coefficients d_i et a_i

$$d_1 = a_1 \ ; \ d_2 = a_2 \ ; \ d_3 = a_3 \ ; \ d_4 = a_4 + a_1a_3 \ ; \ d_5 = a_1a_4 + a_2a_3 + a_1^2a_3 \ ;$$
$$d_6 = a_6 + a_1^2a_4 + a_1^3a_3 + a_2a_4 + 2a_1a_2a_3 \ ; \ldots . \tag{7}$$

L'invariant différentiel de E est une fonction de z :

$$\omega(E) = dz\{1 + a_1z + (a_1^2 + a_2)z^2 + (a_1^3 + 2a_1a_2 + a_3) + ..\} \tag{8}$$

Soit un point (X,Y) de la courbe isogène à E.

A chaque point $P = (x,y)$ de E, nous associons le point (X,Y) par les relations :

$$X = x + \sum_{T \in F - O_E} \big(x(P+T) - x(T)\big) \ ; \tag{9}$$

$$Y = y + \sum_{T \in F - O_E} \big(y(P+T) - y(T)\big)\,;$$

Nous obtenons les développements de X et Y en z :

$$X = z^{-2} - a_1\, z^{-1} - a_2 - a_3 z - \cdots \qquad (10)$$
$$Y = -z^{-3} + a_1 z^{-2} + a_2 z^{-1} + \cdots$$

La formule $Z = -X/Y$ implique le développement de Z :

$$Z = z + 2z^3 + 3a_1 z^6 + \cdots \qquad (11)$$

Nous en déduisons une relation entre X et Y indépendante de z :

$$Y^2 + A_1 XY + A_3 Y = X^3 + A_2 X^2 + A_4 X + A_6\,; \qquad (12)$$

avec $A_1 = a_1\,;\ A_2 = a_2\ ;\ A_3 = a_3\ ;\ A_4 = a_4 - 5t\ et\ A_6 = a_6 - b_2 - 7w,$

$$t = \sum_{Q \in S} t_Q\,, \qquad w = \sum_{Q \in S} \big(\mu_Q + x_Q t_Q\big)\,, \qquad S = F_2 \cup R$$

Exemple de VELU

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

Sous groupes $F \subset \mathbb{Q}$ d'ordre 7 formé des 7 points :

$Q = (1{,}0)\,;\ 2Q = (-1,-2)\,;3Q = (3,-6)\,;4Q = (3{,}2)\,;\ 5Q = (-1{,}2)\,;6Q = (1,-2)\ et\ 7Q = O_E$

alors $E' = E/F\ :\ y^2 + xy + y = x^3 - x^2 - 213x - 1257$

3. Cohomologie des Groupes

La théorie de la cohomologie des groupes est construite avec des groupes différentiels, des groupes abéliens gradués, des G-complexes, des morphismes. C'est cette théorie que nous exposons.

Groupes différentiels

Définition 4

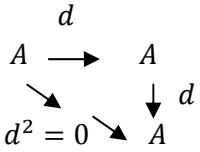
Un groupe différentiel est une paire(A, d), formée d'un groupe abélien A et d'un endomorphisme d de A qui satisfait la relation :

$$d^2 = d \circ d = 0.$$

Il en résulte l'inclusion du sous groupe-Image de d dans le sous groupe Noyau de d :

$$Im\ d \subset \ker d,$$

Diagramme de composition :



Définition 5

Le groupe quotient $H(A) = \ker d/Im\ d$ *est le groupe dérivé du groupe différentiel* (A, d).

Pour deux groupes différentiels, on introduit la notion de "admissible" par la :

Définition 6

Un homomorphisme f *de deux groupes différentiels* (A, d) *et* (B, h) *est admissible si* $f: A \to B$ *satisfait la relation de composition :* $f \circ d = h \circ f$ *et le diagramme commutatif :*

$$\begin{array}{ccc} & f & \\ A & \longrightarrow & B \\ d\downarrow & f\circ d \nearrow h\circ f & \uparrow h \\ A & \longrightarrow & B \end{array}$$

Proposition 4

Toute application admissible de groupes différentiels, $f: (A, d) \to (B, h)$, *induit un homomorphisme de groupes dérivés,* $f_* : H(A) \to H(B)$, *de valeur :*

$$f_*(a + dA) = f(a) + hB, \qquad avec\ f(da) = 0.$$

Preuve

Les groupes différentiels (A, d) et (B, h) sont construits avec :

$$d : A \to A\ et\ \ h : B \to B.$$

Il leur correspond les groupes dérivés :

$$H(A) = ker\ d/Im\ d \text{ et } H(B) = ker\ h/Im\ h.$$

La valeur $f(da) = 0$ provient de la condition $d^2 = 0$ de l'endomorphisme d.

■

Groupes abéliens gradués différentiels

Un groupe différentiel A devient gradué avec une condition supplémentaire.

Définition 7

1) *un groupe abélien A gradué est un groupe abélien somme directe de sous groupes* A_n

$$A = \oplus_0^\infty A_n$$

2) *un groupe abélien, gradué, différentiel, est un groupe gradué muni d'un opérateur différentiel d, qui satisfait, pour chaque* A_n *de la somme directe :*

$$d_n : A_n \to A_{n+r}\ ,\quad pour\ \ r = 1\ ou\ r = -1.$$

Ces opérateurs déterminent une suite infinie du groupe gradué différentiel, (A, d, r) de la forme :

$$\dots \to A_{n-1} \to A_n \to A_{n+r} \to A_{n+2r} \to A_{n+3r} \to \cdots$$
$$d_{n-r} \quad d_n \qquad d_{n+r} \qquad d_{n+2r}$$

Dans cette suite les composées ont pour valeurs :

$d_{n+r} \circ d_n = 0$, pour $r = 1$ ou $r = -1$.

Pour un groupe gradué différentiel (A, d, r), on pose :

$$d = \bigoplus_0^\infty d_n$$

Définition 8

1) *pour un groupe gradué différentiel* (A, d, r), le cas $r = 1$ *est la cohomologie de groupes ; l'opérateur* d *est l'opérateur cobord.*
2) *Le cas* $r = -1$ *est l'homologie de groupes ; l'opérateur* d *est l'opérateur bord*.

Une suite de cohomologie de groupes est de la forme :

$$\dots \to A_{n-1} \to A_n \to A_{n+1} \to A_{n+2} \to \cdots$$
$$d_{n-1} \quad d_n \qquad d_{n+1} \qquad d_{n+2}$$

Une suite d'homologie de groupes est de la forme :

$$\dots \to A_{n+2} \to A_{n+1} \to A_n \to A_{n-1} \to \cdots$$
$$d_{n+3} \qquad d_{n+2} \qquad d_{n+1} \quad d_n \qquad d_{n-1}$$

Groupes de cohomologie

Soit une suite de cohomologie de groupes :

$$\longrightarrow A_{-2} \longrightarrow A_{-1} \longrightarrow A_0 \longrightarrow A_1 \longrightarrow A_2 \longrightarrow \cdots$$
$$d_{-2} \qquad d_{-1} \quad d_0 \qquad d_1 \qquad d_2$$

Dans cette suite apparaissent de nouveaux groupes.

Définition 9

1) *chaque groupe* A_n *est le groupe des n-cochaines ;*
2) *le groupe des n-cocycles est le groupe quotient*
$$Z_n = A_n \cap ker\ d_n\ ;$$
3) *le groupe des n-cobords est le groupe quotient*
$$B_n = A_n \cap d_{n-1} A_{n-1}\ ;$$
4) *le n-ème groupe de cohomologie est le groupe quotient*
$$H^n(A) = Z_n / B_n$$

Avec ces groupes, on construit des diagrammes commutatifs.

Proposition 5

Soit un diagramme commutatif de groupes gradués différentiels :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & B & \xrightarrow{j} & C & \longrightarrow & 0 \\ & & f\downarrow & & g\downarrow & & h\downarrow & & \\ 0 & \longrightarrow & A' & \xrightarrow{i'} & B' & \xrightarrow{j'} & C' & \longrightarrow & 0 \end{array}$$

Ce diagramme induit le diagramme de groupes de cohomologie :

$$\begin{array}{ccccccccccc} & & & \xrightarrow{d_*} & & \xrightarrow{i_*} & & \xrightarrow{j_*} & & \xrightarrow{d_*} & \\ \cdots & \longrightarrow & H_{n-1}(C) & \longrightarrow & H_n(A) & \longrightarrow & H_n(B) & \longrightarrow & H_n(C) & \longrightarrow & H_{n+1}(A) \longrightarrow \cdots \\ & & h_*\downarrow & & f_*\downarrow & & g_*\downarrow & & h_*\downarrow & & f_*\downarrow \\ \cdots & \longrightarrow & H_{n-1}(C') & \longrightarrow & H_n(A') & \longrightarrow & H_n(B') & \longrightarrow & H_n(C') & \longrightarrow & H_{n+1}(A') \longrightarrow \cdots \\ & & & \xrightarrow{d_*'} & & \xrightarrow{i_*'} & & \xrightarrow{j_*'} & & \xrightarrow{d_*'} & \end{array}$$

Preuve

Il faut s'assurer que ce diagramme est commutatif en utilisant les données et les définitions.

■

Pour étudier des groupes quotients, on dispose de la :

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

Soit un groupe A, additif, abélien , et deux endomorphismes f et g, de composés :

$$fog = gof = O.$$

Soit un sous groupe B de A , d'indice fini, stable par f et g.
Alors les indices satisfont :

$$\frac{(\ker f : g(A))}{(\ker g : f(A))} = \frac{(\ker f_B : g_B(B))}{(\ker g_B : f_B(B))}$$

où f_B et g_B sont les restrictions de f et g au sous groupe B de A.
Ce quotient est le ''Quotient de Herbrand''

Preuve cf. [21]

On utilise les données et les propriétés des groupes abéliens et des endomorphismes.

■

G-complexes (partie positive)

Soit un groupe, fini, multiplicatif, d'éléments neutre 1 :

$$G = \{1, \sigma, \tau, \partial, \lambda, \dots\}$$

et l'ensemble :

$$\Gamma = \mathbb{Z}[G] = \{somme\ formelles\ \textstyle\sum_{\sigma\in G} n_\sigma \sigma\ ,\ n_\sigma \in \mathbb{Z}\}.$$

où $\mathbb{Z}$ est l'anneau des entiers rationnels.

Cet ensemble est muni d'une structure d'anneau de groupe, intègre, avec les deux lois : une addition :

$$\sum_\sigma n_\sigma \sigma + \sum_\sigma r_\sigma \sigma = \sum_\sigma (n_\sigma + r_\sigma)\, \sigma;$$

et une multiplication :

$$\left(\sum_\sigma n_\sigma \sigma\right)\left(\sum_\sigma r_\sigma \sigma\right) = \sum_\sigma \left(\sum_{\tau\lambda=\sigma} n_\tau r_\lambda\right).$$

Alors cet anneau de groupe Γ est un $\mathbb{Z}[G]$-module.
Soit un groupe gradué différentiel, de type homologique :

$$(X = \bigoplus X_n, \qquad d = \bigoplus d_n)$$

Définition 10

Le triplet $(X, d, -1)$ est un G-complexe de chaîne, sur l'anneau de groupe Γ si X_n est un Γ-module et si d est un Γ-homomorphisme.
Ce G-complexe est libre si chaque X_n est un Γ-module libre. Il est libre fini si chaque X_n admet une base finie sur Γ. Il est acyclique si son groupe dérivé est nul ; donc
$im\,(d_n) = ker d_{n-1}$.
Il y a d'autres types de G-complexes.

Définition 11

Un G-complexe standard est un triplet (X, Γ, d) formé d'un groupe gradué différentiel X, d'un anneau de groupe intègre $\Gamma = \mathbb{Z}[G]$, où G est un groupe fini et multiplicatif, et d'un opérateur différentiel d.
On en déduit une suite exacte longue :

$$\dots \longrightarrow X_2 \underset{d_2}{\longrightarrow} X_1 \underset{d_1}{\longrightarrow} X_0 \underset{d_0}{\longrightarrow} X_{-1} \underset{d_{-1}}{\longrightarrow} X_{-2} \underset{d_{-2}}{\longrightarrow} \cdots$$

où $X_0 = \Gamma[.]$, $X_n = \bigoplus \Gamma[\sigma_1, \dots, \sigma_n]$, pour $\sigma_i \in G$ et $n \in \mathbb{N}$ et $X_{-n} = \bigoplus \Gamma\langle\sigma_1, \dots, \sigma_n\rangle$.

Les cobords sont les images des opérateurs d :

$$d_1 = ([\sigma] = \sigma[.] - [.]), \text{ et pour les entiers } n \geq 2,$$
$$d_n([\sigma_1, \dots, \sigma_n]) = \sigma_1[\sigma_2, \dots, \sigma_n] + (-1)^n[\sigma_1, \dots, \sigma_{n-1}] + \sum(-1)^i [\sigma_1, \dots, \sigma_{i-1}, \sigma_i\sigma_{i+1}, \dots, \sigma_n] \text{ , pour } 1 \leq i \leq n-1.$$

Définition 12

Un homomorphisme $f: G \longrightarrow A$, est croisé lorsqu'il satisfait :

$$f[\sigma\tau] = \sigma f[\tau] + f[\sigma],\ \sigma, \tau \in G$$

Un homomorphisme croisé, f,est principal, lorsqu'il satisfait :

$$f[\sigma] = \sigma a - a,\ \text{pour tout } \sigma \in G$$

$A = G$-module, G=groupe fini.

Examinons quelques cas particuliers de groupes H^1 et H^0 de cohomologie.

Proposition 7

Soit un groupe fini G, un G-module A et le premier groupe de cohomologie de groupes. Alors :

1) *le groupe $H^1(G, A)$ est isomorphe au groupe $Hom(G, A)$;*
2) *le groupe $H^1(G, \mathbb{Z})$ est trivial.*

Preuve

La définition du premier groupe de cohomologie du G-module A implique l'isomorphisme du (1) est la trivialité du (2)

■

4. Espaces homogènes

Pour faire des calculs dans le groupes de MORDELL-WEIL $E(K)$; on introduit des courbes auxiliaires (espaces homogènes, twists) et des groupes auxiliaires (groupes de Châtelet-Weil, groupes de Selmer et groupes de Shafarevich-Tate).

Espaces homogènes d'une Courbe Elliptique

Dans l'ensemble des automorphismes d'un groupe, il y a des translations. Considérons l'automorphisme translation du groupe de Mordell-Weil d'une Courbe Elliptique E :

$$t : E(K) \longrightarrow E(K), t(P) = P + a_t\ ; \qquad (1)$$

où a_t est un point défini sur une extension normale finie L du corps K.
Selon Cassels ces automorphismes t forment un groupe Γ, ils satisfont le cocycle identité :

$$ta_s + a_t = a_{ts}\ ; pour\ t\ dans\ \Gamma, a_s, a_t, a_{ts}\ dans\ L \qquad (2)$$

Un tel cocycle détermine une variété algébrique A ; définie sur K ; qui peut être une Courbe Elliptique birationnellement L-équivalente à la Courbe Elliptique E ; cette variété A est de dimension 1.
Le cocycle (2) et l'isomorphisme $L(E) \longrightarrow L(A)$ permettent de définir la structure d'espaces homogènes d'une Courbe Elliptique E.

Définition 13

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

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

$$f(P_A, O_E) = P_A$$

$$f(f(P_A, P), R) = f(P_A, P + R)$$

pour tous points P_A de A, P et R de E et $O_E = (\infty, \infty) = (0,1,0)$.

et de l'application réciproque :

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

$$g(P_A, R_A) = P \qquad \textit{avec } f(R_A, P) = P_A$$

Ce point P est unique. Cet espace homogène est principal.
Il en résulte la valeur $g(P_A, P_A) = 0$ pour tout point P_A de la courbe A.
Cette définition constitue « le lemme 10-1 » dans « équation diophantine » de Cassels.

Dans l'ensemble des espaces homogènes (A, f, g) d'une Courbe Elliptique E, il y a une relation d'équivalence :

Définition 14

Deux espaces homogènes (A_1, f_1, g_1) et (A_2, f_2, g_2) d'une Courbe Elliptique E sont dans la même classe s'il existe un isomorphisme :

$$h : A_1 \longrightarrow A_2\ , \qquad h(P_1) = P_2$$

qui rend commutatif le diagramme :

$$\begin{array}{ccc} A_1 \times E & \xrightarrow{f_1} & A_1 \\ \downarrow & & \downarrow h \\ A_2 \times E & \underset{f_2}{\rightarrow} & A_2 \end{array}$$

Donc $f_2(h(P_1), P) = h\big(f, (P_1, P)\big)$ *pour tous points* $P_1 \in A_1$ *et* $P \in E$.

Définition 15

La classe triviale d'espaces homogènes (A, f, g) *d'une Courbe Elliptique* E *est la classe de cette courbe, avec pour application* f *la loi d'addition du groupe* $E(K)$ *de MORDELL-WEIL.*

Proposition 8

Un espace homogène (A, f, g) *d'une Courbe Elliptique* E *sur* K*, est dans la classe triviale si et seulement si le groupe de Mordell-Weil* $A(K)$ *n'est pas vide.*

L'ensemble des classes homogènes (A, f, g) *d'une Courbe Elliptique* E *engendre plusieurs groupes particuliers.*

Cf. [17]

■

Les types d'espaces homogènes (C, f, g) d'une Courbe Elliptique dépendent de la forme de son équation de WEIERSTRASS.

Proposition 9

Dans l'ensemble des espaces homogènes (C, f, g) *d'une Courbe Elliptique* E *d'équation de WEIERSTRASS :*

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

pour un corps K *de carac*$(K) \neq 2, 3$*, le nombre de types d'espaces homogènes est fini.*

1) Il y a au plus 2 types pour les Courbes E *d'équation* (1) *;*

2) Il y a au plus 4 types pour les Courbes E *d'équation* (2)

$$E : y^2 = x^3 + Ax \; ; \qquad (2)$$

3) Il y a au plus 6 types pour les Courbes E *d'équation* (3)

$$E : y^2 = x^3 + B \qquad (3)$$

Preuve

Cf. "Corollary-Lemma 10-3" CASSELS [15]

■

Groupes de CHÂTELET-WEIL des Courbes Elliptiques

Définition 16

Les groupes de CHÂTELET - WEIL des Courbes Elliptiques E sont les groupes $WC(E/K)$ des classes d'équivalence des espaces homogènes de E.
Les ordres de ces groupes peuvent être déterminés avec la :

Proposition 10

Soit une Courbe Elliptique E, son groupe de CHÂTELET – WEIL $WC(E/K)$ et le groupe de GALOIS G d'une clôture algébrique K_{alg} du corps K.
Alors il y a une bijection :

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

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

Pour un point P_0 de C, qui associe à toute classe $Cl(C,\mu)$ d'espaces homogènes un élément :

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

Preuve cf. (Th.3.6-X)[12]

■

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

Lorsque la courbe E est définie sur un corps local K_v en une valuation $v \in V_k$, son groupe de CHÂTELET - WEIL est $WC(E/K_v)$

Groupes de SELMER et Groupes de CHAFAREVICH – TATE

Ces groupes sont construits à l'aide d'isogénies, de m –torsion, de groupes de cohomologie et de groupes $WC(E/K_v)$.
Exemple la multiplication par un entier m:

$$t_m : E(K) \longrightarrow E(K)\ ;\ t_m(P) = mP\ ;$$

est une isogénie de la Courbe Elliptique E.

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

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

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

et des suites exactes de groupes de cohomologie, pour le groupe de Galois $G = G_{K_{alg}/K}$

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

Les groupes de SELMER et les groupes de CHAFAREVICH–TATE sont des noyaux de certaines applications.

Définition 17 [17]

1) *Le m −groupe de SELMER d'une Courbe Elliptique E relatif à un sous groupe de m-torsion $E(m)$ de $E(K)$ est le sous groupe noyau de l'application :*

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

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

$WC(E/K_v)$ est le groupe de CHÂTELET – WEIL de E sur le corps K_v

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

2) *le groupe de CHAFAREVICH–TATE d'une courbe elliptique E, est le sous groupe noyau de l'application :*

$$Ш(E/K) = ker\{WC(E/K) \longrightarrow \prod_v WC(E/K_v)\}$$

Donc le groupe de CHAFAREVICH–TATE est un sous groupe du groupe de CHÂTELET – WEIL.

Proposition 11

Soit une Courbe Elliptique E, les groupes $S_m(E/K)$ de SELMER et $III(E/K)$ de CHAFAREVICH–TATE, l'isogénie t_m et le sous groupe $E[m]$ de m-torsion de E. Alors :

1) la suite de groupes :

$$0 \longrightarrow E(K)/m\,E(K) \longrightarrow S_m(E/K) \longrightarrow III(E/K)[m] \longrightarrow 0$$

est exacte. C'est la suite de KUMMER

2) le m – groupe de SELMER est fini

Preuve

1) découle des définitions **[17]** des groupes de SELMER et de CHAFAREVICH–TATE et des suites de cohomologie associées.

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

Cf. (Th. 4.2 – X) [12]

■

Exemple de 2 – groupes de SELMER

Soit la Courbe Elliptique E d'équation de WEIERSTRASS :

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

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

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

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

$$K(S,2) = \left\{b \in K^*/K^{*2}\,;\, ord_v(b) \equiv 0(mod2) pour\ tous\ v \notin S\right\}$$

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

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

où e_1, e_2, e_3 sont les abscisses des 3 points d'intersection de l'axe Ox par la Courbe Elliptique E.

Selon [12], le $2^{ème}$-groupe de SELMER et le groupe de CHAFAREVICH–TATE sont égaux à :

$$S_2(E/Q) \cong (\mathbb{Z}/2\mathbb{Z})^3 \text{ et } III(E/Q)[2] = 0$$

Exemple d'espace homogène déterminé par l'isogénie

$$\phi(x, y) = (y^2/x^2, y(b - x^2)/x^2)$$

de la Courbe Elliptique d'équation de WEIERSTRASS :

$$E: y^2 = x^3 + ax^2 + bx \ , \ a^2 \neq 4b$$

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

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

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

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

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

$$A: dw^2 = d^2 - 2adz^2 + (a^2 - 4b)z^4$$

d'après ([12], X – 4)

Isogénies et Groupe de SELMER de Courbes Elliptiques

Par la proposition 11, le groupe de m-SELMER est fini pour tout entier m ;

la suite de KUMMER d'une Courbe Elliptique E sur un corps K est égale à :

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

où $E(K)$ est le groupe de MORDELL- WEIL de E,

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

H^1 est le 1^{er} groupe de cohomologie,

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

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

Cette suite de groupes est exacte, elle induit une suite de KUMMER :

$$1 \longrightarrow K^*/(K^*)^m \longrightarrow H^1\big(G, \Gamma(m)\big) \longrightarrow H^1\big(G, K^*_{alg}\big)$$

où K^*est le groupe multiplicatif des nombres non nuls du corps K,

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

D'après le « théorème 90 de Hilbert », le groupe $H^1\big(G, K^*_{alg}\big) = 0$; **[21]**

Il existe un théorème de KUMMER pour le ϕ −groupe de SELMER, lié à une isogénie :

ϕ : $E(K) \longrightarrow E'(K)$ de Courbes Elliptiques.

Proposition 12

Soit une isogénie de Courbes Elliptiques :

ϕ : $E(K) \longrightarrow E'(K)$

le ϕ- groupe de SELMER $S_\phi(E) = ker\big\{H^1(G, E[\phi]) \longrightarrow \prod_{v\in V_K} WC(E/K_v)\big\}$

et le noyau de ϕ sur le groupe de CHAFAREVICH–TATE $Ш(E)[\phi]$

Alors :

1) la suite de KUMMER :

$$0 \longrightarrow E'(K)/\phi\big(E(K)\big) \longrightarrow S_\phi(E) \longrightarrow Ш(E)[\phi] \longrightarrow 0 \text{ est exacte.}$$

2) le ϕ- groupe de SELMER $S_\phi(E)$ est fini

Preuve de 1

Cette suite provient du diagramme :

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

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

Par définition le groupe $S_\phi(E)$ est un sous groupe de $H^1(G, E[\phi])$ le groupe $III(E)$ est un sous groupe de $WC(E/K)$.

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

Elle découle des 2 propositions suivantes :

Proposition 13

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

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

Preuve

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

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

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

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

est un isomorphisme

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

Cf. [17]

■

Proposition 14

Soit une isogénie :

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

et un ensemble fini S dans l'ensemble V_K de places contenant les places archimédiennes, les places v en lesquelles E a mauvaise réduction et les places v qui divisent $deg\phi$

Alors le ϕ-groupe de Selmer satisfait l'inclusion :

$$S_\phi(E) \subset H^1(G, E[\phi], S)$$

Preuve cf. [17], Corollary 4-4-X

Exemple ([12] X – 4-5-1)

Soit la Courbe Elliptique E d'équation de Weierstrass :

$$E: y^2 = x^3 - 12x^2 + 20x \quad \in \mathbb{Q}[x, y]$$

Alors son 2-groupe de torsion est égal à :

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

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

$$T(E) = E(\mathcal{Q})[2]$$

Son $2^{ème}$- groupe de SELMER est égal à :

$$S_2(E/\mathcal{Q}) \cong (\mathbb{Z}/2\,\mathbb{Z})$$

Il y a un résultat relatif aux groupes de SELMER de Courbes Elliptiques d'équation de WEIERSTRASS $E: y^2 = x^3 - px$

Proposition 15

Soit un nombre premier p impair et une Courbe Elliptique E_p d'équation de WEIERSTRASS :

$$E: y^2 = x^3 - px \ \in \mathbb{Q}[x, y]$$

Une isogénie de degré 2 :

$$\phi : E_p(\mathcal{Q}) \longrightarrow E_p{}'(\mathcal{Q}) \qquad \textit{a pour noyau } \ E_p(\mathcal{Q})[\phi] = \{(0,0), 0_E\}$$

Alors :

1) le groupe de torsion $T\big(E_P(\mathcal{Q})\big)$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$

2) le ϕ −groupe de SELMER de $E_p{}'$ est $S_\phi\left(E_p{}'(\mathcal{Q})\right)$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$

3) le ϕ −groupe de SELMER de E_P est :

$$S_\phi\left(E_p(Q)\right) \approx \begin{cases} (\mathbb{Z}/2\mathbb{Z}) & si \quad p \equiv 7,11 mod 16 \\ (\mathbb{Z}/2\mathbb{Z})^2 & si \quad p \equiv 3,5,13,15 mod 16 \\ (\mathbb{Z}/\mathbb{Z})^3 & si \quad p \equiv 1,9 mod 16 \end{cases}$$

Preuve

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

On considère un ensemble de représentants des classes dans le corps

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

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

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

$$-p \in S_\phi(E) \; et \; p \in S_\phi(E')$$

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

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

Il en résulte $S^\phi(E') = \{1, p\} \approx \mathbb{Z}/2\mathbb{Z}$

Plus de détails dans [17], X, paragraphe 6, Proposition 6.2

■

Espaces homogènes - groupes de SELMER et Groupe de CHAFAREVICH–TATE

Les Courbes Elliptiques d'équation de WEIERSTRASS :

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

Ont ,au plus, 4 types d'espaces homogènes ; ce résultat influe sur les groupes de Selmer et de Chafarevich-Tate associés à ces espaces homogènes.

Calcul des invariants pour le cas des nombres premiers $p \geq 5$;

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

Alors, selon [17] (proposition X-6-2) Le groupe de SELMER de la Courbe Elliptique E_p dépend de p modulo 16

Proposition 16

Soit une Courbe Elliptique $E_p: y^2 = x^3 + px$, *p premier* ≥ 5.

Alors :

Le groupe de *CHAFAREVICH–TATE* est lié au rang de la Courbe Elliptique E_p par les relations :

$$rg\left(E_p(Q)\right) + dim_2 III(E/Q)[2] = 0 \; si \; p \equiv 7{,}11 mod 16$$

$$rg\left(E_p(Q)\right) + dim_2 III(E/Q)[2] = 1 \; si \; p \equiv 3{,}5{,}13{,}15 mod 16$$

$$rg\left(E_p(Q)\right) + dim_2 III(E/Q)[2] = 2 \; si \; p \equiv 1{,}9 mod 16$$

Preuve

Cf. Proposition X-6-2, [17]

■

Signalons que le groupe de *CHAFAREVICH* $III(E/Q)$ intervient dans la conjecture de BIRCH and SWINNERTON – DYER (« Notes on Elliptic Curves (I) and (II) », J. Reine Ange. Math .212 (1963), 7-25 and 218 (1965), 79-108)

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

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

$t_p = 1 + p - \{nombre\ de\ points\ de\ la\ courbe\ réduite\ mod\ p\}$

$R(E) = régulateur\ de\ E, c_p = t_p$

r = rang analytique de la Courbe Elliptique.

En conclusion, l'étude des espaces homogènes des Courbes Elliptiques et leurs groupes associés nécessite de nombreuses connaissances arithmétiques des Courbes Elliptiques, géométrie des Courbes Elliptiques, cohomologie des groupes.

Il existe d'autres pistes de recherche sur ce sujet comme Courbes Elliptiques à Multiplication Complexe, Courbes Elliptiques d'invariants modulaires nuls, …

Tableau récapitulatif

Courbes Elliptiques = Cubiques de WEIERSTRASS de discriminants $\Delta(C) \neq 0$:

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

Théorème de MORDELL-WEIL : le groupe $E(K)$ est additif, abélien, de type fini,

d'élément neutre le point $O_E = (\infty, \infty) = (0,1,0)$, déterminé par la direction de l'axe *Oy*

Isogénies de Courbes Elliptiques satisfait 3 conditions :

$$\lambda : \ E(K) \longrightarrow E'(K) \ de\ noyau\ fini, \ \lambda \ \text{surjective}$$

$\lambda(O_E) = O_{E'}$ et $\lambda(P+R) = \lambda(P) + \lambda(R)$, pour tous points *P* et *R* de *E(K)*

Groupes de cohomologie [21] : $A = \oplus_0^\infty A_n$ somme directe

$$\ldots \to A_{n-1} \to A_n \to A_{n+1} \to A_{n+2} \to \cdots$$
$$d_{n-1} \quad d_n \qquad d_{n+1} \qquad d_{n+2}$$

$$Im\, d_{n-1} \subset \ker d_n,$$

$$Z_n = A_n \cap \ker d_n\,, \qquad B_n = A_n \cap d_{n-1}A_{n-1}$$

$H^n(A) = Z_n/B_n$; $n^{ème}$ groupe de cohomologie.

Espaces homogènes de E = Courbes algébriques A avec 2 applications :

1) $f : A \times E \longrightarrow A$, $f(P_A, O_E) = P_A$

2) $g : A \times A \longrightarrow E$, $f(f(P_A, P), R) = f(P_A, P+R)$

$g(P_A, R_A) = P$ $\quad pour\ \ f(R_A, P) = P_A$

Références

[1] ***Z- I- BOREVICH et I- R- CHAFAREVICH*** **:** " Théorie des Nombres" Ed. Gauthier Villars- Paris (1967)

[2] ***J-W-S-CASSELS*** **:** " Diophantine Equations with special references to Elliptic Curves ", Jour London Math. Soc. 41 (1966) p-193- 291

[3] ***I- R- CHAFAREVICH*** **:** " Basic Algebraic Geometry ", Springe (1977)

[4] ***François CHÂTELET*** **:** Professeur Univ. de Franche Comté- Besançon- France
(1) " Variation sur un thème de POINCARRE ", Annales Scientifiques de l'E- N- S- 61 (1944)
(2) " Méthode galoisienne et courbe de genre 1 ", Annales de l'Univ. de lyon- Section A- 89- (1946)p 40-49
(3) " Introduction à la Théorie des Corps de Nombres", Publication de la Faculté des Sciences d'Alger-(1966)

[5] ***J- F- CREMONA*** **:** " Algorithme for Modular Elliptic Curves ", 2^{nd} Cambridge Univ. Press (1998)

[6] ***Jean DIEUDONNE*** **:** " Algèbre Linéaire et Géométrie élémentaire ", Ed. Hermann- Paris (1963)

[7] ***Robin HARTSHORNE*** **:** " Algebraic Geometry ", GTM- 52 (1980)

[8] ***HUSEMÔLLER*** **:** " Elliptic Curves ", GTM- 111 (1980)

[9] ***A- W- KNAPP*** **:** " Elliptic Curves- Princeton " Univ- Press 40 (1992)

[10] ***Neal KOBLITZ*** **:** (1) " Introduction to Elliptic Curves and Modular Forms ", 2^{nd} GTM- 97 (1984)
(2) " A course in Number Theory and Cryptography ", GTM- 114 (1988)

[11] ***Anatoly I- KOSTRIKIN*** **:** " Introduction à l'Algèbre ", Mir (1986)

[12] ***Jean P. LAFON*** **:** " Formalismes fondamentaux de l'Algèbre Commutative ", Ed. Hermann- Paris (1974)

[13] ***Serge- LANG*** **:** " Elliptic Curves- Diophantine Analysis ", Springer (1978)

[14] ***M- P- MALLIAVIN*** **:** " Algèbres commutative- Applications en Géométrie et en théorie des Nombres ", Ed. Masson- Paris (1985)

[15] ***J- S- MILNE*** **:** " Elliptic Curves ", Univ- Michigan (1996)

[16] ***Goro SHIMURA*** **:** " Introduction to the Arithmetic Theory of Automorphic Functions", Princeton Univ Press- 11 (1971)

[17] ***Joseph H- SILVERMAN*** **: "** The Arithmetic of Elliptic Curves " GTM- 106 (1986)

[18] ***John TATE*** **:** " The Arithmetic of Elliptic Curves ", Invent- Math- 23 (1974) p- 179- 206

[19] ***VELU Jacques :*** 1) Courbes Elliptiques sur Q ayant bonne reduction en dehors de 11 – CRAS – Paris (12juillet 1971) p73-74
2) Isogénies entre Courbes Elliptiques – CRAS-Paris (26 juillet 1971) p238-241

[20] ***André WEIL- Mthématicien américain d'origine Française Professeur à Princeton Univ.*** **: "** Fondations of Algebraic Geometry " (1969)

[21] ***Edwin WEISS*** **:** " Cohomology of Groups ", Academic Press (1969)

[22] ***Mohamed ZITOUNI*** **:** " Géomètrie- Arithmétique et Algorithmique des Courbes Elliptiques ", Ed- OPU- Alger (2007)