N° d'ordre: 28/2002-M/MT

UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE
HOUARI BOUMEDIENNE (ALGER)

جامعة هواري بومدين
للعلوم والتكنولوجيا
U S T H B

FACULTE DE MATHEMATIQUES
DEPARTEMENT D'ALGEBRE ET THEORIE DES NOMBRES

THESE

Présentée à l'**USTHB**

Pour l'obtention du grade de : ***Magistère***
en : ***Mathématiques***
spécialité : ***Algèbre et théorie des nombres***

Par

Mlle AIT-AMRANE Nacima-Rosa

SUJET

RANGS D'UNE FAMILLE DE TWISTS QUADRATIQUES DE COURBES ELLIPTIQUES

Soutenue publiquement le : 17/12/2002 **devant le jury composé de :**

Mr.M.S.HACHAICHI	Maître de conférences à l'**USTHB**	Président.
Mr. M.ZITOUNI	Professeur à l'**USTHB**	Directeur de thèse.
Mr. K.BETINA	Professeur à l'**USTHB**	Examinateur.
Mr. A.KESSI	Professeur à l'**USTHB**	Examinateur.
Mr. B.BENSABAA	Chargé de cours à l'**USTHB**	Examinateur.

Dédicaces

Je dédie ce présent travail à ma très tendre grand-mère « Habou », sans qui je n'aurais pas étais ce que je suis.

A mes deux parents que j'aime beaucoup et à mes bien-aimées sœurs Lilia et Rachida.

Aussi à mes chers cousins très présents dans ma vie et à toute ma famille, une dédicace particulière à Tarik. Surtout un spécial remerciement à Nouredine.

A mes très chers amis Azrou Nadia et Nouredine Mouloud, que je remercie pour leur présence dans ma vie et leurs compréhensions. Et surtout Mouloud qui ma témoigné d'une très grande patience que je n'oublierai jamais.

Je n'oublierai pas d'adresser mes sympathies à tous mes amis de la B.I.M et du cursus universitaire, depuis 1993.

Bonne Année 2003

Remerciements

Je remercie Monsieur Mohamed ***Zitouni****, professeur à l'USTHB de m'avoir proposé ce sujet et de m'avoir guidé tout le long de la réalisation de cette thèse.*

Je remercie spécialement Monsieur M.S. ***Hachaichi,*** *maître de conférences à l'USTHB d'avoir accepté de présider le jury et d'avoir apprécié ce présent travail.*

Je remercie également Messieurs K. ***Betina,*** *professeur à l'USTHB, A.* ***Kessi,*** *professeur à USTHB et B.* ***Bensabaa*** *chargé de cours à l'USTHB pour leur participation au jury.*

Table des matières

Introduction

Dans la théorie des courbes elliptiques, le rang d'une courbe elliptique est un invariant arithmétique important. C'est l'entier naturel $r(E) = r \geq 0$ de la formule d'isomorphisme de groupes dans le théorème de Mordell-Weil :

$$E(K) \simeq E_{tor}(K) \times \mathbb{Z}^r.$$

Il en résulte que le rang d'une courbe elliptique E est le nombre minimal de générateurs de la partie infinie de son groupe de Mordell-Weil. C'est le calcul de ce rang qui est une entreprise difficile. Il existe diverses méthodes de calcul pour sa détermination : méthode de descente locale, méthode de D.E.Penney et C.Pomerance, méthode de Mazur (qui utilise les schémas), méthode de J.Tate, etc...

Il existe des courbes elliptiques E sur le corps des nombres rationnels $\mathbb{Q}$ de tout rang $r \geq 0$. Voici quelques exemples pris dans la littérature spécialisée :

Deux courbes elliptiques de rang $r = 0$:

$$E_P : y^2 = x^3 + px \quad ; \quad p \text{ nombre premier}.$$
$$E : y^2 + xy + y = x^3 - x^2 - 9x - 8.$$

Quatre courbes elliptiques de rang $r = 1$:

$$E_1 : y^2 = x^3 + 877x \quad ; \quad E_2 : y^2 + y = x^3 - x;$$
$$E_3 : y^2 + xy = x^3 - 1 \quad ; \quad E_4 : y^2 + 9xy + y = x^3 - 7x^2.$$

Deux courbes elliptiques de rang $r = 2$:

$$E_1 : y^2 = x^3 - 1513^2 x \quad \text{et} \quad E_2 : y^2 = x^3 - 7361^2 x.$$

Deux courbes elliptiques de rang $r \geqslant 4$:

$$E_1 : y^2 + 8\,xy + 11\,y = x^3 + 2\,x^2 - 3\,x;$$
$$E_2 : y^2 + 14\,xy + 29\,y = x^3 + 2\,x^2 - 15\,x.$$

Une courbe elliptique de rang $r = 9$:

$$E_1 : y^2 + 525\,xy = x^3 + 228\,x^2 - 14972955\,x + (856475)^2\,.$$

Une courbe elliptique de rang $r \geqslant 22$:

$$E_1 : y^2 + xy + y = x^3 - 940299517776391362903023121165864\,x +$$
$$1070736307071974303342529551544927453465112501136 2.$$

(recueilli sur internet).

Une courbe elliptique de rang $r \geq 24$:

$$E_1 : y^2 + xy + y = x^3 - 120039822036992245303534619191166796374\,x +$$
$$5042249924849106700108017991680827267594437562229114151 16.$$

(recueilli sur internet).

Le rang r d'une courbe elliptique intervient en particulier dans la conjecture de Birch et Swinnerton-Dyer :La série $L_E(s)$ de Dirichlet d'une courbe elliptique E admet en $s = 1$ un zéro d'ordre égal au rang $r(E)$ de la courbe E. Cette série est définie par le produit d'Euler :

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

où $t_p = 1 + p - A_p$ et A_p est le nombre de points de la courbe E modulo p et $\varepsilon_p = -1$

pour une réduction multiplicative et $\varepsilon_p = 0$ pour une réduction additive.

Dans le chapitre 1, nous indiquons quelques notions indispensables de la théorie arithmétique des courbes elliptiques : équation de Weierstrass, transformations linéaires, coefficients b_i et c_i, discriminant, invariant modulaire, invariant différentiel.

Dans le chapitre 2, nous traitons la théorie des réductions d'une courbe elliptique.

Dans le chapitre 3, nous étudions les propriétés du groupe $E(K)/mE(K)$, les hauteurs sur une courbe elliptique, les espaces homogènes et les twists, les rangs du groupe de Mordell-Weil $E(\mathbb{Q})$.

Chapitre 1

Notions de base de la théorie des courbes elliptiques

1.1 Structures algébriques

Définition 1 : *Une courbe elliptique est une cubique plane E non dégénérée, non singulière, de genre un et d'équation affine particulière :*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6; \tag{1}$$

Son équation projective dans le plan projectif $\mathbb{P}^2(K)$ est de la forme :

$$E : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3;$$

Les cinq coefficients a_i sont des éléments d'un corps commutatif K, les couples de variables (x, y) sont des zéros de l'équation algébrique (1); ce sont donc des éléments d'une clôture algébrique K^{alg} du corps K.

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

Le groupe de Galois $G_{K^{alg}/K}$ de la clôture algébrique K^{alg} agit sur les points $P = (x, y)$ de la courbe elliptique par les $K-$automorphismes du corps K^{alg} :

$$\sigma(P) = \sigma(x, y) = (\sigma(x), \sigma(y)) \ , \quad \text{pour tout point } P \text{ de la courbe.}$$

La nature du corps K influe sur les propriétés de la courbe elliptique E.

Lorsque le corps K est un corps de nombres algébriques, la courbe elliptique a des liens avec la théorie des nombres (entiers, discriminants, valuations, idéaux, ramifications, analyse p-adique, équations diophantiennes, etc...)

Lorsque le corps K est le corps des nombres complexes, la courbe a des liens avec l'analyse complexe (réseaux et tores, fonctions elliptiques, fonctions modulaires, fonctions automorphes, groupes formels...) et avec la géométrie algébrique (variétés, théorie des diviseurs, théorie des faisceaux et des schémas, homologie et cohomologie...)

Lorsque le corps K est un corps fini, la courbe a des liens avec la cryptographie, la factorisation en nombres premiers des grands nombres entiers, etc...

Le corps K peut être un corps local ou un corps de fonctions, ou le corps des nombres réels. Il en résulte des structures particulières selon la nature du corps de définition de la courbe elliptique sur lequel elle est définie :

structure de groupe abélien de type fini ;

structure de variété abélienne non singulière de dimension 1 ;

structure de courbe algébrique projective lisse de genre 1 ;

structure de schéma irréductible de dimension 1.

Selon la théorie des courbes algébriques, le genre d'une courbe plane C de degré n est déterminé par la formule :

$$g(C) = \frac{(n-1)(n-2)}{2} - d_1 - d_2; \qquad (2)$$

où $d_1$et d_2 sont respectivement le nombre de noeuds et le nombre de points de rebroussements de la courbe C. Pour une courbe elliptique E de degré $n = 3$ non singulière, $d_1 = d_2 = 0$, la formule (2) implique la valeur : $g(E) = 1$.

1.2 Transformations linéaires d'équations

L'équation (1) peut être transformée en d'autres équations. Lorsque le corps K est de caractéristique différente de 2, le changement linéaire de variables :

$$(x, y) \longmapsto (x, \frac{1}{2}(y - a_1 x - a_3));$$

élimine les monômes xy et y dans l'équation (1).

L'équation (1) de la courbe elliptique devient :

$$E : y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6. \tag{3}$$

Les coefficients b_i sont des polynômes "homogènes de degré i" dans l'anneau $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$:

$$\begin{cases} b_2 = a_1^2 + 4a_2; \\ b_4 = a_1 a_3 + 2a_4; \\ b_6 = a_3^2 + 4a_6. \end{cases} \tag{4}$$

Lorsque le corps est de caractéristique différente de 2 et 3, le changement linéaire de variables :

$$(x, y) \longmapsto \left(\frac{x - 3\,b_2}{36}, \frac{y}{108}\right);$$

élimine le monôme x^2 et le coefficient 4 dans l'équation (3).

L'équation (3) de la courbe elliptique devient :

$$E : y^2 = x^3 - 27\,c_4 x - 54\,c_6. \tag{5}$$

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

$$\begin{cases} c_4 &= b_2^2 - 24\, b_4; \\ c_6 &= 36\, b_2 b_4 - b_2^3 - 216\, b_6. \end{cases} \tag{6}$$

L'équation (5) de la courbe elliptique E peut se mettre sous la forme :

$$E : y^2 = x^3 + Ax + B; \tag{7}$$

Les coefficients A et B sont des polynômes "homogènes de degré i" de l'anneau $\mathbb{Z}[c_4, c_6]$:

$$\begin{cases} A &= -27\, c_4; \\ B &= -54\, c_6. \end{cases}$$

Puisque, par définition, une courbe elliptique est une courbe lisse, son équation admet trois zéros simples. Cette équation est de la forme :

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3); \tag{8}$$

où $e_i \neq e_j$, *pour* $i \neq j$; $e_i \in K^{\text{alg}}$.

1.3 Trois invariants d'une courbe elliptique et classification des cubiques planes

Ces trois invariants sont le discriminant $\Delta(E)$, l'invariant modulaire $j(E)$ et l'invariant différentiel $\omega(E)$. Les coefficients b_i permettent de définir le discriminant de la courbe elliptique E.

Définition 3 : *Le discriminant d'une courbe elliptique E sur un corps K de caractéristique $caracK \neq 2$ et 3 est le polynôme"homogène de degré douze" de l'anneau $\mathbb{Z}[b_2, b_4, b_6, b_8]$:*

$$\Delta(E) = 9b_2b_4b_6 - 8b_4^3 - 27b_6^2 - b_2^2b_8 \neq 0; \tag{9}$$

où l'on a posé :

$$4b_8 = b_2b_6 - b_4^2; \tag{10}$$

c'est aussi le polynôme "homogène de degré douze" de l'anneau $\frac{1}{1728}\mathbb{Z}[c_4, c_6]$ *:*

$$\Delta(E) = \frac{c_4^3 - c_6^2}{1728} \neq 0; \tag{11}$$

Pour une courbe elliptique E d'équation $y^2 = x^3+Ax+B$, le discriminant est un polynôme de l'anneau $\mathbb{Z}[A, B]$:

$$\Delta(E) = -16(4A^3 + 27B^2) \neq 0. \tag{12}$$

Définition 4 : *L'invariant modulaire d'une courbe elliptique E est la fraction rationnelle :*

$$j(E) = \frac{c_4^3}{\Delta(E)}; \tag{13}$$

c'est aussi :

$$j(E) = \frac{1728.4.A^3}{4A^3 + 27B^2}. \tag{14}$$

Définition 5 : *Soit une courbe elliptique E d'équation:*

$$E : F(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0; \tag{15}$$

L'invariant différentiel d'une courbe elliptique E est la forme différentielle :

$$\omega(E) = \omega = \frac{dx}{F'_y} = -\frac{dy}{F'_x}; \tag{16}$$

où F'_x et F'_y désignent les dérivées partielles de la fonction $F(x,y)$:

$$\begin{cases} F'_x &= a_1 y - 3x^2 - 2a_2 x - a_4 \neq 0; \\ F'_y &= 2y + a_1 x + a_3 \neq 0. \end{cases} \tag{17}$$

Points singuliers d'une courbe cubique plane

Par la théorie des courbes algébriques, une courbe de degré trois non lisse admet un seul point singulier ; ce point $P = (x, y)$ est solution du système de trois équations algébriques :

$$\begin{cases} F(x,y) = 0; \\ F'_x = 0; \\ F'_y = 0; \end{cases} \tag{18}$$

Ce point singulier est soit un noeud (si $c_4 \neq 0$), soit un point de rebroussement (si $c_4 = 0$). Une courbe elliptique est une courbe lisse ; donc elle n'a pas de point singulier.

Exemple 1 : Soit une cubique plane E_1 d'équation :

$$E_1 : y^2 = 4x^3 - 3x + 1;$$

Pour savoir s'il y a un point singulier nous calculons le discriminant. La formule du discriminant donne la valeur $\Delta(E) = 0$; il en résulte que la courbe E_1 admet un point singulier S.

Les coordonnées du point S sont solutions du système (18). Le système d'équations algébriques :

$$\begin{cases} F(x,y) & = y^2 - 4x^3 + 3x - 1 & = 0; \\ F'_x & = -12x^2 + 3 & = 0; \\ F'_y & = 2y & = 0; \end{cases}$$

admet une seule solution $(x,y) = (\frac{1}{2}; 0)$; il en résulte un point singulier $S = (\frac{1}{2}, 0)$, ainsi la cubique E_1 est singulière. Pour déterminer la nature de ce point singulier (noeud ou point de rebroussement) ; nous étudions la fonction :

$$x \longmapsto f(x) = 4x^3 - 3x + 1 = y^2;$$

Tableau de variations de la fonction $f(x)$:

x	-∞	-1	$-\frac{1}{2}$	0	$\frac{1}{2}$	1	2	+∞
$f\prime(x)$		+	0	-	0	+		
$f(x)$	-∞	↗	2	↘	0	↗		+∞
$y^2 = f(x)$			2	1	0	2	3^3	
y		0	$\pm\sqrt{2}$	± 1	0	$\pm\sqrt{2}$	$\pm 3\sqrt{3}$	

Ce tableau montre que la cubique E_1 coupe l'axe Ox en deux points, le point $(-1, 0)$ et le point $S = (\frac{1}{2}, 0)$; ce point singulier S est donc un noeud. Consulter le graphe de la cubique E_1 en figure 1.

Exemple 2 :

Soit une cubique plane E_2 d'équation :

$$E_2 : y^2 = 4x^3 + 12x^2 + 12x + 4;$$

Etudions l'existence d'un point singulier.

Les relations (4) et (10) impliquent les valeurs :

$$b_2 = 12, \qquad b_4 = 6, \qquad b_6 = 4, \qquad b_8 = 3.$$

La formule (9) donne la valeur du discriminant $\Delta(E) = 0$. Donc la courbe E_2 n'est pas lisse ; elle admet un point singulier S.

Les coordonnées du point singulier S sont solutions du système :

$$\begin{cases} F(x,y) &= y^2 - 4x^3 - 12x^2 - 12x - 4 &= 0; \\ F'_x &= -12(x^2 + 2x + 1) &= 0; \\ F'_y &= 2y &= 0; \end{cases}$$

nous obtenons une solution unique $(x, y) = (-1; 0)$. Cela donne le point singulier $S = (-1, 0)$. Pour déterminer la nature de ce point (noeud ou point de rebroussement), nous étudions la fonction :

$$x \longmapsto f(x) = 4x^3 + 12x^2 + 12x + 4 = y^2;$$

Tableau de variations de la fonction $f(x)$

x	$-\infty$		-1		0		1		$+\infty$
$f'(x)$		$+$	0			$+$			
$f(x)$	$-\infty$	↗	0	↗	2	↗	2^5	↗	$+\infty$
$y^2 = f(x)$			0		2		2^5		$+\infty$
y			0		± 2		$\pm 4\sqrt{2}$		

Ce tableau montre que la cubique E_2 coupe l'axe Ox en un seul point $S = (-1, 0)$; ce point singulier est donc un point de rebroussement. Consulter le graphe de la cubique E_2 en figure 2.

Cubique plane $E_1 : y^2 = 4x^3 - 3x + 1$; avec un noeud $S = (\frac{1}{2}, 0)$.

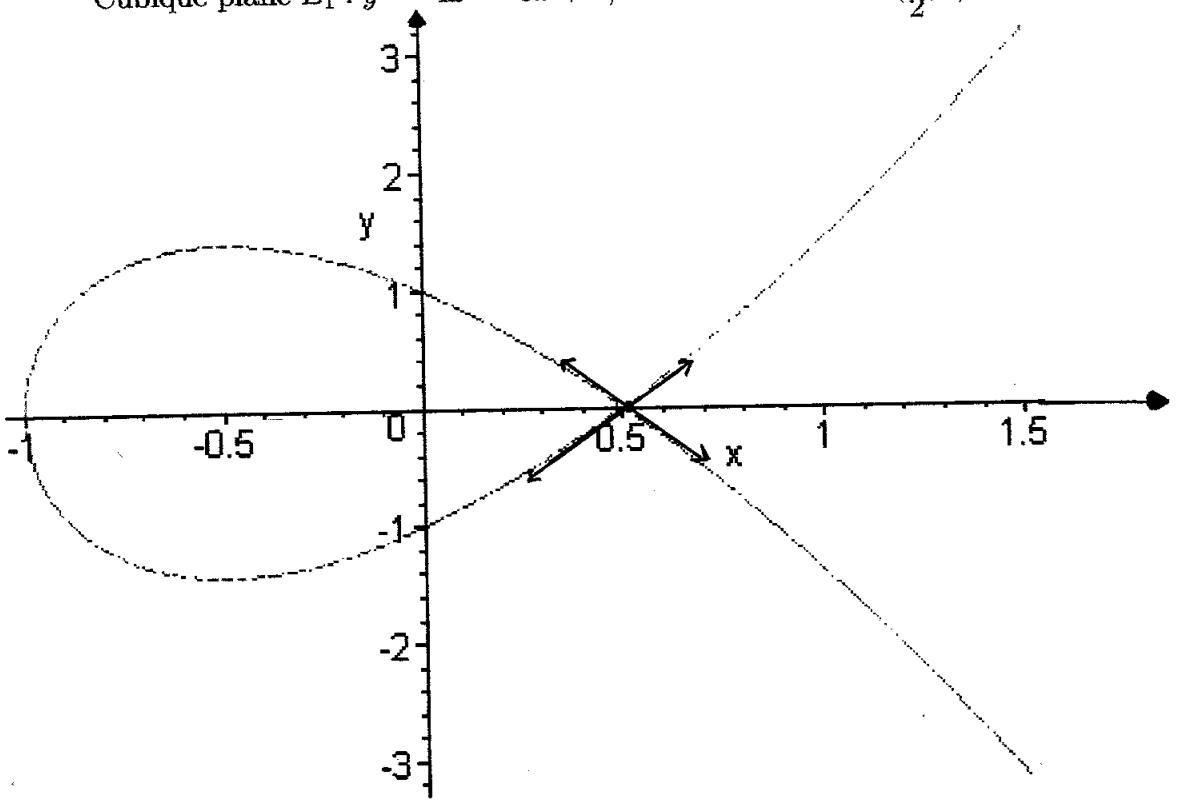

Figure 1

Cubique plane $E_2 : y^2 = 4x^3 + 12x^2 + 12x + 4$; avec un point de rebroussement $S = (-1, 0)$.

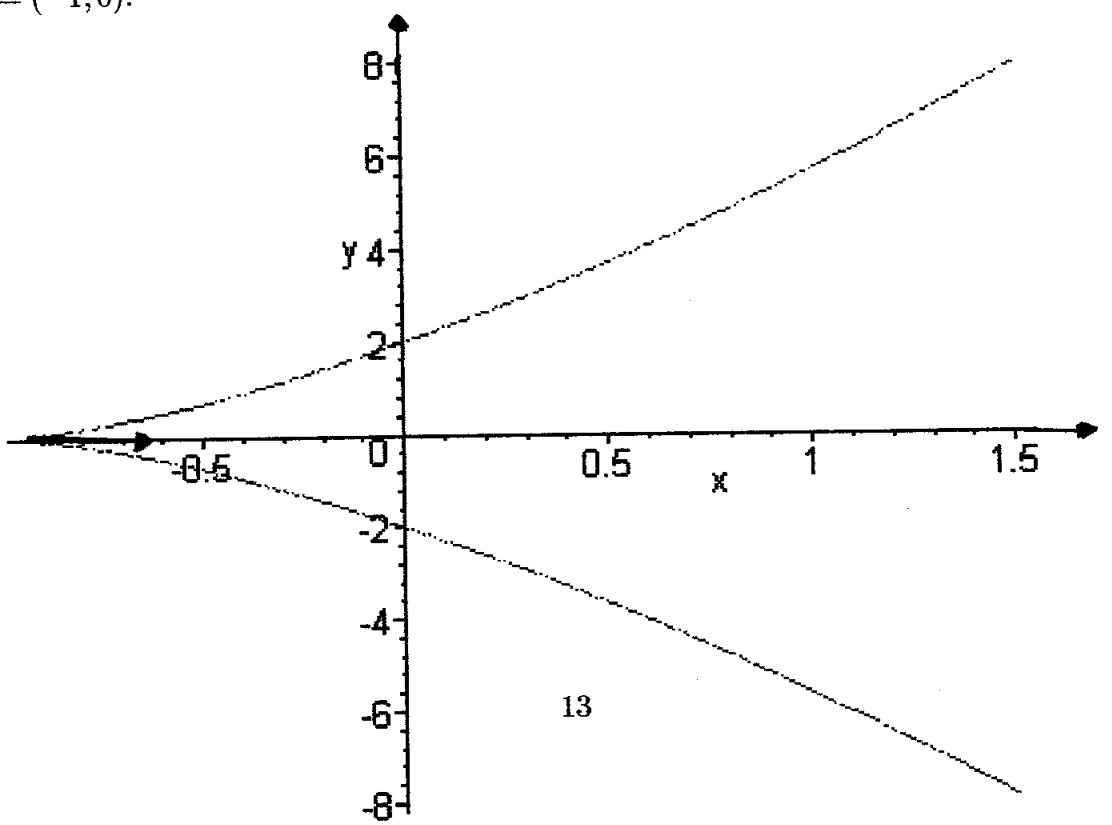

Figure 2

Les points singuliers d'une cubique plane C ont été obtenus par la résolution d'un système de trois équations algébriques ; la construction de la courbe C est obtenue avec l'étude de la fonction :

$$x \longmapsto f(x) = y^2.$$

Il existe une méthode propre à la théorie des courbes elliptiques pour distinguer les cubiques singulières des cubiques non singulières.

Proposition 1 : *Soit une courbe algébrique C cubique d'équation affine :*

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6;$$

de discriminant $\Delta(C)$ et de point à l'infini $O_C = (\infty, \infty)$. *Alors :*

1) *la cubique n'admet pas de point singulier si et seulement si $\Delta(C) \neq 0$. Dans ce cas la cubique est une courbe elliptique.*

2) *le point O_C n'est pas singulier sur la courbe C.*

Preuve de "la cubique C n'admet pas de point singulier"implique"$\Delta(C) \neq 0$"

Soit une cubique C sans point singulier ; alors elle admet une équation de la forme :

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

Selon la théorie du résultant de deux polynômes, le discriminant $\Delta(C)$ est proportionnel au résultant $\mathrm{Res}(f, f')$ du polynôme f et de son polynôme dérivée f' :

$$\Delta(C) = c\,\mathrm{Res}(f,\, f') \quad , \quad \text{pour une certaine constante non nulle } c. \qquad (2)$$

ce polynôme $f(x)$ a trois racines simples ; il est donc premier à sa dérivée $f'(x)$. Il en résulte la valeur du résultant :

$$\text{Res}(f,\, f') \neq 0. \tag{3}$$

Les relations (2) et (3) donnent la valeur :

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

Preuve de"$\Delta(C) \neq 0$"implique"la cubique C n'admet pas de point singulier"

Soit une cubique plane C d'équation :

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

de discriminant :

$$\Delta(C) \neq 0. \tag{5}$$

L'hypothèse (5) et la relation (2) entre le discriminant et le résultant impliquent la valeur du résultant :

$$\text{Res}(f,\, f') \neq 0.$$

Le polynôme $f(x)$ admet donc trois racines simples. Cela implique que la cubique plane C est non singulière ; la courbe C est donc une courbe elliptique.

Preuve de"le point à l'infini O_C n'est pas singulier"

On écrit l'équation (5) sous sa forme homogène dans l'espace projectif $\mathbb{P}^2(K)$:

$$C : y^2z = 4x^3 + b_2x^2z + 2b_4xz^2 + b_6z^3;$$

Nous posons $F(x,y,z) = y^2z - 4x^3 - b_2x^2z - 2b_4xz^2 - b_6z^3$. (6)

Par la théorie des courbes algébriques, un point singulier $P = (x,y,z)$ est solution du système de quatre équations algébriques :

$$\begin{cases} F(x,y,z) = 0; \\ F'_x = -12x^2 - 2b_2xz - 2b_4z^2 = 0; \\ F'_y = 2yz = 0; \\ F'_z = y^2 - b_2x^2 - 4b_4xz - 3b_6z^2 = 0; \end{cases} \quad (7)$$

Au point $O_C = (0,1,0)$, $F'_z = 1$, la quatrième équation n'admet donc pas de solution ; il en résulte que le point à l'infini O_C n'est pas singulier sur la courbe elliptique C. ■

Corollaire : *Soit une courbe algébrique C cubique d'équation affine :*

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6;$$

de discriminant $\Delta(C)$ et de coefficient usuel c_4. Alors :

1) *la cubique C admet un noeud si et seulement si $\Delta(C) = 0$ et $c_4 \neq 0$.*

2) *la cubique C admet un point de rebroussement si et seulement si $\Delta(C) = c_4 = 0$.*

Preuve de"la cubique C admet un noeud "implique"$\Delta(C) = 0$ et $c_4 \neq 0$"

Soit une cubique plane C avec un noeud ; alors son discriminant vaut :

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

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

$$C : y^2 = (x - e_1)^2(x - e_2) = g(x); \tag{2}$$

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

$$\mathrm{Re}\, s(g, g') = 0. \tag{3}$$

Le discriminant $\Delta(C)$ de la cubique C est proportionnel au résultant $Res(g, g')$. (4)

Les deux relations (3) et (4) impliquent la relation :

$$\Delta(C) = c\,\mathrm{Re}\, s(g, g') = 0 \ ; \quad c = c(g) \text{ est une constante non nulle.}$$

Au noeud $P_0 = (x_0, y_0)$, la cubique C admet deux tangentes distinctes. Leurs pentes sont calculées avec la dérivée de l'équation de la courbe C :

$$2yy' = 12x^2 + 2b_2x + 2b_4 = g'(x); \tag{5}$$

les pentes au point P ont pour valeurs :

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

le discriminant du polynôme quadratique $N(x)$ vaut :

$$\delta(N(x)) = b_2^2 - 24b_4 = c_4; \tag{7}$$

l'hypothèse d'un noeud implique deux tangentes dinstinctes, donc deux valeurs différentes pour la pente y'.

La théorie des équations algébriques de degré deux, donne la condition d'existence de deux racines :

$$\delta(N(x)) = c_4 \neq 0.$$

Preuve de"$\Delta(C) = 0$ et $c_4 \neq 0$" implique"la cubique C admet un noeud"

Soit la cubique plane C d'équation :

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

dans un corps K de $carac(K) \neq 2$ et de discriminant $\Delta(C)$.

Son discriminant est lié au résultant $\mathrm{Res}(g, g')$ par la formule :

$$\Delta(C) = c\,\mathrm{Res}(g, g'); \qquad \text{pour } c = c(g) \neq 0.$$

L'hypothèse $\Delta(C) = 0$; implique la valeur du résultant $\mathrm{Res}(g, g') = 0$. D'après la partie (1), la courbe C admet un point singulier. La théorie des résultants implique le polynôme $g(x)$ admet une racine double :

$$g(x) = 4(x - e_1)^2(x - e_2).$$

L'hypothèse $c_4 \neq 0$ et la relation (6) impliquent l'existence de deux tangentes distinctes en ce point singulier P_0. Il en résulte que ce point P_0 est un noeud.

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

Soit une cubique C d'équation :

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

de discriminant $\Delta(C)$ dans un corps K de $carac(K) \neq 2$. Nous supposons que la courbe C admet un point de rebroussement S. D'après la partie (1) une cubique singulière a son discriminant $\Delta(C) = 0$. Il en résulte que le résultant $\mathrm{Res}(g, g')$ de ce polynôme $g(x)$ et de sa dérivée $g'(x)$ est nul. Par définition, un point de rebroussement S admet deux tangentes confondues à la courbe C ; cela donne une racine double du polynôme $N(x)$ de (6). Les relations (6) et (7) donnent l'invariant $c_4 = 0$.

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

Soit une cubique plane C d'invariants $\Delta(C) = c_4 = 0$. La partie (1) du corollaire et $\Delta(C) = 0$ impliquent que la cubique C est singulière. L'hypothèse $c_4 = 0$ et la formule du discriminant :

$$\delta(N(x)) = c_4;$$

impliquent 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. ■

1.4 Le groupe de Mordell-Weil d'une courbe elliptique

Soit une courbe elliptique E sur un corps K, d'équation de Weierstrass :

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

Soit $E(K)$ l'ensemble des points K-rationnels de la courbe E. Nous munissons cet ensemble d'une structure de groupe abélien. Pour cette loi de groupe, nous considérons le point à l'infini O_E comme élément neutre et la règle géométrique :

"*trois points colinéaires de la courbe algébrique E ont une somme nulle*". (2)

Le point à l'infini O_E est déterminé par la direction de l'axe Oy. Pour tout point P, la droite PO_E est donc parallèle à l'axe Oy.

La règle géométrique (2), sur les courbes algébriques, montre qu'une sécante coupe la courbe elliptique en trois points simples, ou en un point double et un point simple, ou en deux points simples et le point à l'infini.

Dans le premier cas, la règle géométrique (2) donne la formule :

$$P_1 + P_2 + P_3 = O_E. \tag{3}$$

Dans le deuxième cas, la règle donne la formule :

$$P_1 + P_1 + P_3 = 2P_1 + P_3 = O_E; \tag{4}$$

qui permet le calcul d'un point P de 2-torsion.

Dans le troisième cas, la règle donne la formule :

$$P_1 + P_2 + O_E = P_1 + P_2 = O_E; \tag{5}$$

qui permet le calcul du symétrique P_2 d'un point P_1.

Proposition 2 : *L'application :*

$$\begin{array}{rccl} f: & E(K) \times E(K) & \longrightarrow & E(K) \\ & (P_1, P_2) & \longmapsto & f(P_1, P_2) = P_1 + P_2. \end{array}$$

qui satisfait la règle géométrique (2) *des trois points colinéaires est une loi de groupe abélien d'élément neutre le point à l'infini* $O_E = (\infty, \infty)$.

Preuve :

L'axiome de l'élément neutre O_E est vérifié avec la règle géométrique :

$$P + O_E = O_E + P = P; \qquad \text{pour tout point } P \text{ de } E(K).$$

Cet élément neutre est unique : $O_E = (0, 1, 0)$ dans le plan projectif $\mathbb{P}^2(K)$. Donc la sécante PO_E coupe la courbe elliptique E au point simple P et au point double O_E. Cette sécante PO_E est parallèle à l'axe Oy. L'axiome du symétrique d'un point P_1 est vérifié

avec la parallèle P_1P_2 à l'axe Oy qui coupe la courbe E en deux points simples P_1 et P_2 et au point O_E.

L'axiome de commutativité de la loi est vérifié avec la coincidence des sécantes P_1P_2 et P_2P_1.

L'axiome d'associativité de la loi est vérifié par le calcul :

$$(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3). \quad \blacksquare$$

Nous obtenons les formules donnant les coordonnées du symétrique $-P$ d'un point P, de la somme $P_1 + P_2$ de deux points distincts $P_1 \neq \pm P_2$ en utilisant la théorie algébrique des intersections d'une droite et d'une courbe. Les calculs donnent les résultats suivants :

Les coordonnées du symétrique d'un point $P = (x, y)$ de la courbe elliptique E sont :

$$-P = -(x, y) = (x, -y - a_1x - a_3); \tag{1}$$

Les coordonnées de la somme $P_1 + P_2$ de deux points distincts; $P_i = (x_i, y_i)$ $i = 1, 2$ et $P_1 \neq \pm P_2$ s'obtiennent avec le calcul :

$$\begin{cases} x_{(P_1+P_2)} &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2; \\ y_{(P_1+P_2)} &= -\lambda^3 - a_1\lambda^2 + (a_2 - a_1^2 + 2x_1 + 2x_2)\lambda - a_3 + a_1(a_2 + x_1 + x_2) - y_1; \end{cases} \tag{2}$$

où le coefficient λ est la pente de la droite P_1P_2 :

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

Ainsi, avec la relation géométrique liant trois points colinéaires de la courbe elliptique E et le point à l'infini O_E, nous avons muni l'ensemble $E(K)$ d'une structure de groupe abélien.

Définition 6 : *Le groupe abélien $E(K)$ des points $K-$rationnels d'une courbe elliptique E est le groupe de Mordell-Weil de la courbe elliptique E sur un corps K.*

Proposition 3 : *Le groupe de Mordell-Weil d'une courbe elliptique est de type fini. Il est isomorphe au produit de groupes abéliens :*

$$E(K) \simeq E(K)_{tor} \times \mathbb{Z}^r;$$

où : $E(K)_{tor}$ est le sous groupe de torsion du groupe de Mordell-Weil $E(K)$.

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

$r(E) = r$ est un entier positif ou nul.

Preuve :

Elle comporte deux parties dont l'une a pour objet de montrer la finitude du groupe quotient $E(K)/mE(K)$; l'autre partie utilise une fonction hauteur sur un groupe abélien cf [14]. ■

Définition 7 : *Cet entier naturel $r(E) = r \geq 0$ est le rang de la courbe elliptique E.*

La détermination du rang d'une courbe elliptique est un probleme difficile qui constitue un sujet de recherches actuelles ; on signale qu'il n'existe pas de formule effective donnant la valeur du rang $r(E)$ d'une courbe elliptique E, contrairement au rang du groupe des unités $U(K)$ d'un corps de nombres K qui admet $2r_2$ conjugués complexes et r_1 conjugués réels : $r(U(K)) = r_1 + r_2 - 1$ et $U(K) \simeq W \times \mathbb{Z}^{r_1+r_2-1}$ où W est le groupe des racines de l'unité contenues dans le corps K (théorème de Dirichlet).

Illustration de la loi de groupe de Mordell-Weil sur une courbe elliptique E.

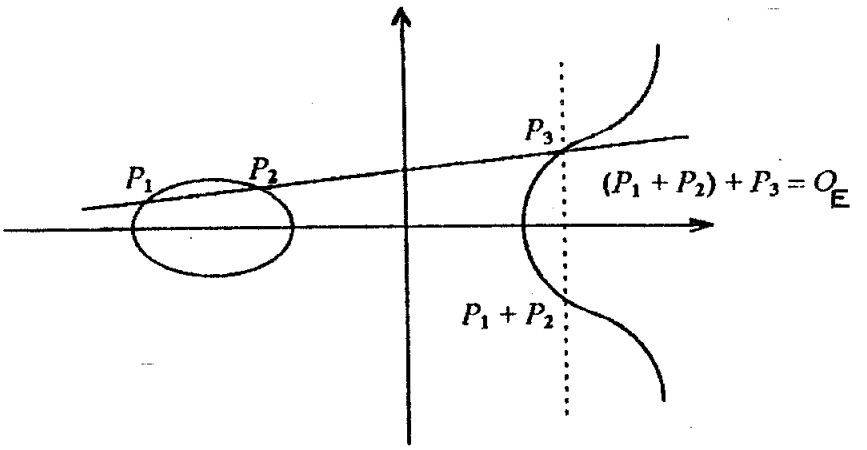

Figure 3 : $P_1 + P_2$ avec $P_1 \neq \pm P_2$.

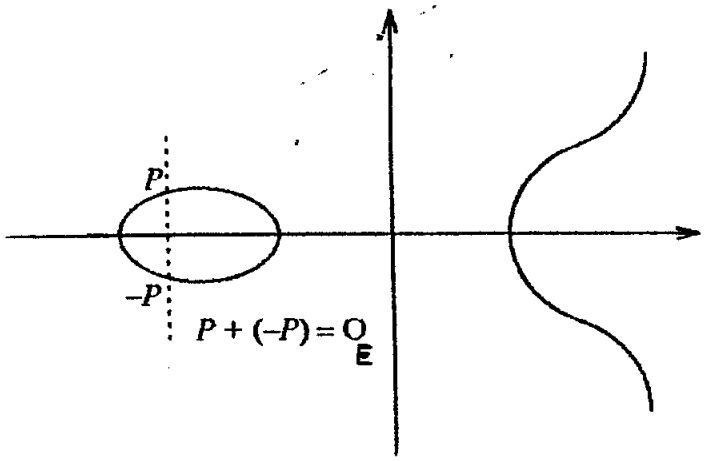

Figure 4 : Symétrique $-P$ de P.

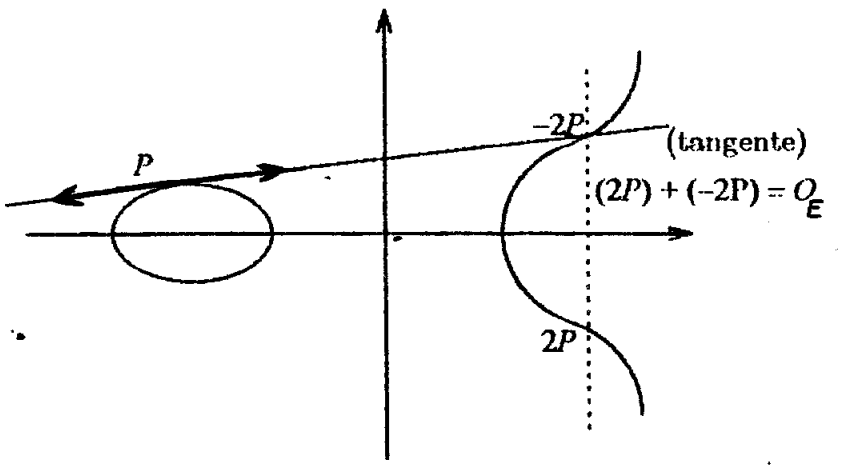

Figure 5 : Somme $P + P = 2P$.

1.5 Sous groupes de torsion d'une courbe elliptique

Soit une courbe elliptique E sur un corps K, de groupe abélien $E(K)$ de Mordell-Weil et le point à l'infini O_E. Par convention, pour tout entier rationnel m premier à la caractéristique du corps K, le symbole mP désigne :

$$mP = \begin{cases} P + P + \ldots\ldots + P; & m \text{ fois } P & si \quad m \text{ est un entier naturel.} \\ -P - P - \ldots\ldots - P; & -m \text{ fois } P & si \quad m \text{ est un entier négatif.} \\ O_E; & & si \quad m = 0. \end{cases}$$

Définition 8 : *Un point de $m-$torsion d'une courbe elliptique E est un point P du groupe de Mordell-Weil $E(K)$ qui satisfait la relation : $mP = O_E$.*

Définition 9 : *L'ensemble $E(K)[m]$ est l'ensemble des points de $m-$torsion de la courbe elliptique E.*

Proposition 4 : *L'ensemble $E(K)[m]$ des points de $m-$torsion d'une courbe elliptique E sur un corps K est un sous groupe du groupe de Mordell-Weil $E(K)$.*

Preuve :

Soit m un entier naturel et O_E le point neutre du groupe abélien $E(K)$.

Soit deux points P_1, P_2 de m-torsion ; les relations $mP_1 = mP_2 = O_E$ impliquent :

$m(P_1 - P_2) = mP_1 - mP_2 = O_E - O_E = O_E$.

Il en résulte que le point $P = P_1 - P_2$ est de $m-$torsion.

Donc $E(K)[m]$ est un sous groupe du groupe $E(K)$. ■

Proposition 5 : *L'ensemble des points P de torsion de la courbe elliptique E :*

$$\begin{aligned} E_{tor}(K) &= \{P \in E(K)/mP = O_E; m \geq 1\} \\ &= \bigcup_{m\geq 1} E(K)[m] \end{aligned}$$

est un sous-groupe du groupe de Mordell-Weil $E(K)$.

Preuve :

Pour tous $m_1 \geq 1$ et $m_2 \geq 1$; il existe $m_3 = ppcm(m_1, m_2)$ tel que $E(K)[m_1] \subset E(K)[m_3]$ et $E(K)[m_2] \subset E(K)[m_3]$, ce qui implique que la réunion $\bigcup_{m\geq 1} E(K)[m]$ est un sous groupe de $E(K)$. ■

Les coordonnées du point mP :

Pour déterminer les coordonnées du point mP, nous utilisons la méthode de J.W.Cassels. Nous prenons une courbe elliptique E d'équation:

$$E : y^2 = x^3 + Ax + B \quad \text{avec} \quad A, B \in \mathbb{Q} \quad \text{et} \quad 4A^3 + 27B^2 \neq 0. \tag{1}$$

Nous considérons les six polynômes $\Psi_i(x, y)$ de l'anneau $\mathbb{Z}[x, y]$:

$$\begin{aligned} &\Psi_{-1} = -1 \quad ; \quad \Psi_0 = 0 \quad ; \quad \Psi_1 = 1 \quad ; \quad \Psi_2 = 2y; \\ &\Psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2; \\ &\text{et } \Psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2). \end{aligned} \tag{2}$$

Les polynômes Ψ_m sont déterminés par deux relations de récurrence :

$$\begin{aligned} &\Psi_{2m+1} = \Psi_{m+2}\Psi_m^3 - \Psi_{m-1}\Psi_{m+1}^3 \; ; && m \geq 2 \\ &\text{et } \Psi_{2m} = 2\Psi_m(\Psi_{m+2}\Psi_{m-1} - \Psi_{m+2}^2\Psi_{m+1}^2) \; ; && m \geq 3 \end{aligned} \tag{3}$$

Nous introduisons deux autres familles de polynômes ϕ_m et ω_m par les formules :

$$\begin{aligned} \phi_m &= x\Psi_m^2 - \Psi_{m-1}\Psi_{m+1}\,; && m \geq 2 \\ \text{et}\quad 4y\,\omega_m &= \Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2\,; && m \geq 3 \end{aligned} \tag{4}$$

Alors, les coordonnées du point mP, sont données par la formule :

$$mP = \left(\frac{\phi_m}{\Psi_m^2}, \frac{\omega_m}{\Psi_m^3}\right). \tag{5}$$

L'application de ces formules pour $m = 2$, donne les polynômes :

$$\begin{cases} \Psi_2 &= 2y; \\ \phi_2 &= x^4 - 2Ax^2 - 8Bx + A^2; \\ \omega_2 &= x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2; \end{cases} \tag{6}$$

et les coordonnées du point $2P$:

$$\begin{cases} x_{2P} &= \dfrac{x^4 - 2Ax^2 - 8ABx + A^2}{(2y)^2}; \\ \\ y_{2P} &= \dfrac{x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2}{(2y)^3}. \end{cases} \tag{7}$$

L'application de ces formules pour $m = 3$, donne les polynômes :

$$\begin{aligned} \phi_3 = {} & x^9 - 12Ax^7 - 96Bx^6 + 30A^2x^5 - 24ABx^4 + 12(3A^3 + 4B^2)x^3 + \\ & 48A^2Bx^2 + 3A(3A^3 + 32B^2)x + 8B(A^3 + 8B^2); \end{aligned} \tag{8}$$

qui est un polynôme de l'anneau $\mathbb{Z}[x, A, B]$ de degré 9 en x, et

$$\begin{aligned}\omega_3 = \; & y[x^{12} + 22Ax^{10} + 220Bx^9 - 165A^2x^8 - 528ABx^7 - 4\left(23A^3 + 444B^2\right)x^6 + \\ & 264A^2Bx^5 - 5A\left(37A^3 + 576B^2\right)x^4 - 80B\left(4B^2 + A^3\right)x^3 - \\ & 6A^2\left(15A^3 + 104B^2\right)x^2 - 28AB\left(3A^3 + 32B^2\right)x - 3A^6 - 96A^3B^2 - 512B^4];\end{aligned} \tag{9}$$

où $\dfrac{\omega_3}{y}$ est un polynôme de l'anneau $\mathbb{Z}[x, A, B]$ de degré douze en x.

Le polynôme :

$$\Psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2; \tag{10}$$

est donné dans la partie (2) du théorème de Cassels.

Le calcul donne le carré du polynôme Ψ_3 :

$$\Psi_3^2 = 9x^8 + 36Ax^6 + 72Bx^5 + 30A^2x^4 + 144ABx^3 + 12(12B^2 - A^3)x^2 - 24A^2Bx + A^4; \tag{11}$$

Ψ_3^2 est un polynôme de l'anneau $\mathbb{Z}[x, A, B]$ de degré 8 en x. Le calcul donne le cube du polynôme Ψ_3 :

$$\begin{aligned}\Psi_3^3 = \; & 27x^{12} + 162Ax^{10} + 324Bx^9 + 297A^2x^8 + 1296ABx^7 + 108(A^3 + 12B^2)x^6 + 1080A^2Bx^5 \\ & + 9A(288B^2 - 11A^3)x^4 + 432B(4B^2 - A^3)x^3 + 18A^2(A^3 + 24B^2)x^2 - 12A^4Bx - A^6;\end{aligned}$$

Ψ_3^3 est un polynôme de l'anneau $\mathbb{Z}[x, A, B]$ de degré 12 en x.

Les formules (5), (8), (9), (11) et (12) donnent les coordonnées du point $3P$:

$$\begin{cases} x_{3P} = \dfrac{\phi_3}{\Psi_3^2}; \\ \\ y_{3P} = \dfrac{\omega_3}{\Psi_3^3}. \end{cases} \tag{13}$$

Exemple 3 :

Considérons la courbe elliptique E d'équation :

$$E : y^2 = x^3 + x + 2 = (x+1)(x - \frac{1+\sqrt{-7}}{2})(x - \frac{1-\sqrt{-7}}{2}); \qquad (1)$$

sur le corps quadratique $\mathbb{Q}(\sqrt{-7})$. Son discriminant vaut $\Delta(E) = -2^8.7 \neq 0$ en caractéristique $carac(K) \neq 2, 7$.

En utilisant les formules Ψ_i on obtient les coordonnées du point $2P$ en fonction de $P = (x, y)$:

$$\begin{cases} x_{2P} = \dfrac{x^4 - 2x^2 - 16x + 1}{(2y)^2}; \\ \\ y_{2P} = \dfrac{x^6 + 5x^5 + 40x^3 - 5x^2 - 8x - 33}{(2y)^3}. \end{cases} \qquad (2)$$

Par définition, un point de 2-torsion satisfait la relation :

$$2P = O_E = (\infty, \infty)\,. \qquad (3)$$

Les formules (2) et (3) donnent l'ordonnée du point P :

$$y = 0. \qquad (4)$$

Les égalités (1) et (4) donnent trois solutions $(x, y) = (-1, 0), (\frac{1+\sqrt{-7}}{2}, 0)$ et $(\frac{1-\sqrt{-7}}{2}, 0)$ dans le corps quadratique imaginaire $\mathbb{Q}(\sqrt{-7})$ et une unique solution $(x, y) = (-1, 0)$ dans le corps des nombres réels $\mathbb{R}$. Le point $P = (-1, 0)$ est donc le seul point de 2-torsion du groupe abélien $E(\mathbb{Q})$. ■

Exemple 4 :

Certains points de 2−torsion d'une courbe elliptique E d'équation :

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3);$$

avec $e_i \in \mathbb{Q}$ et $e_i \neq e_j$ pour $i \neq j$, peuvent être obtenus avec la règle géométrique qui a permis la construction du groupe de Mordell-Weil $E(\mathbb{Q})$.

Au point d'intersection $T_i = (e_i, 0)$, la parallèle à l'axe Oy est la tangente à la courbe elliptique au point T_i. Il en résulte que ces trois points d'intersection T_i sont des points de 2 -torsion du groupe abélien $E(\mathbb{Q})$.

Dans le cas particulier de la courbe :

$$E : y^2 = (x + 1)(x^2 + x + 2) = f(x);$$

le polynôme $f(x)$ se factorise sous la forme :

$$f(x) = (x + 1)(x + \frac{1 + \sqrt{-7}}{2})(x + \frac{1 - \sqrt{-7}}{2});$$

Les zéros $\frac{1 - \sqrt{-7}}{2}$ et $\frac{1 + \sqrt{-7}}{2}$ ne sont pas des nombres rationnels, mais des nombres irrationnels du corps quadratique imaginaire $\mathbb{Q}(\sqrt{-7})$. Il en résulte un seul point de 2-torsion sur le groupe abélien $E(\mathbb{Q})$ et trois points de 2-torsion sur le groupe abélien $E(\mathbb{Q}(\sqrt{-7}))$.

La structure des sous groupes de torsion du groupe abélien $E(\mathbb{Q})$ est déterminée par la :

Proposition 6 : *Le groupe de torsion $E_{tor}(\mathbb{Q})$ d'une courbe elliptique E est isomorphe à l'un des quinze groupes additifs :*

$$1)\mathbb{Z}/d\mathbb{Z} \qquad \text{avec} \quad 1 \leq d \leq 10 \quad \text{ou} \quad d = 12;$$
$$2)\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2d\mathbb{Z} \qquad \text{avec} \quad 1 \leq d \leq 4.$$

Preuve :

C'est le théorème de Mazur cf [12]. ■

Exemple 5 :

Détermination du groupe de torsion du groupe $E(\mathbb{Q})$ de la courbe elliptique E :

$$E : y^2 = x^3 + 4x; \tag{1}$$

Le calcul donne la valeur du discriminant

$$\Delta(E) = -2^{10} \neq 0; \tag{2}$$

sur un corps K de $caracK \neq 2$.

Détermination des points de 2-torsion. Les calculs donnent les coordonnées du point $2P$:

$$\begin{cases} x_{2P} = \dfrac{\phi_2}{\Psi_2^2} = \dfrac{x^4 - 8x^2 + 16}{(2y)^2}; \\ y_{2P} = \dfrac{\omega_2}{\Psi_2^3} = \dfrac{x^6 + 20x^4 - 80x^2 - 64}{(2y)^3}; \end{cases} \tag{3}$$

L'hypothèse "P est un point de 2-torsion " implique :

$$2P = O_E = (\infty, \infty). \tag{4}$$

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

$$y = 0. \tag{5}$$

Les formules (1) et (2) donnent l'unique point P d'ordre deux du groupe $E(\mathbb{Q})$:

$$P = (0, 0).$$

Détermination des points d'ordre trois en utilisant les formules de J.W.Cassels :

$$x_{3P} = \frac{\phi_3}{\Psi_3^2} \quad ; \quad y_{3P} = \frac{\omega_3}{\Psi_3^3}.$$

Un point d'ordre 3 est déterminé par le polynôme :

$$\Psi_3 = 3x^4 + 24x^2 - 16 = 0; \tag{1}$$

Ce polynôme bicarré Ψ_3 admet les 4 zéros :

$$x = \pm 2\sqrt{-1 \pm \frac{\sqrt{21}}{3}}; \tag{2}$$

irrationnels ; ils appartiennent à l'extension quartique $K = \mathbb{Q}(\sqrt{-1 \pm \frac{\sqrt{21}}{3}})$ du corps des rationnels $\mathbb{Q}$. Donc ces points n'appartiennent pas au groupe de Mordell-Weil $E(\mathbb{Q})$, ils appartiennent au groupe abélien $E(K)$.

Les points d'ordre 4 de la courbe elliptique E ont pour coordonnées

$$4P = (x_{4P}, y_{4P}). \tag{3}$$

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

$$x_{4P} = \frac{\phi_4}{\Psi_4^2} \quad ; \quad y_{4P} = \frac{\omega_4}{\Psi_4^3}. \tag{4}$$

Un point d'ordre 4 pour la courbe elliptique d'équation :

$$E : y^2 = x^3 + 4x; \tag{5}$$

est déterminé par le système :

$$\begin{cases} \Psi_4 = 4y(x^6 + 20x^4 - 80x^2 - 64) = 0; \\ y^2 = x^3 + 4x. \end{cases} \tag{6}$$

Ces deux polynômes admettent des solutions dans le corps $\mathbb{C}$ des nombres complexes. Il en résulte les solutions :

1) $y = 0$ et $x^3 + 4x = 0$; soit $x = 0, x = \pm 2i$.

2) $y \neq 0$ et $f(x) = x^6 + 20x^4 - 80x^2 - 64 = 0$.

Proposition 7 : *Soit un polynôme* $g(x) = x^n + d_1 x^{n-1} + ... + d_n \in \mathbb{Z}[x]$; *alors toute solution rationnelle* t *divise le coefficient constant* d_n.

Donc toute solution rationnelle r de $f(x)$ divise -64. Les tests donnent deux diviseurs entiers et $f(\pm 2) = 0$. Il en résulte deux solutions $(2, y^2 = 16)$ et $(-2, y^2 = -16)$. Dans le corps des nombres rationnels $\mathbb{Q}$, $y^2 = -16$ n'admet pas de solution. Nous en déduisons les deux solutions $R = (2, 4)$ et $R' = (2, -4)$. Ces deux points sont, d'après la théorie des courbes elliptiques, symétriques sur la courbe E. Par le calcul nous obtenons les points $2R = (12, -44)$ et $3R = -R = (2, -4)$. Cela implique que le groupe de torsion de la courbe elliptique E est cyclique d'ordre 4 : $E_{tor}(\mathbb{Q}) = \{R, 2R, 3R, 4R = O_E\} \cong \mathbb{Z}/4\mathbb{Z}$. Ce résultat est conforme au théorème de Mazur.

L'existence d'un point non nul de torsion sur une courbe elliptique E sur l'anneau $\mathbb{Z}$ peut être étudiée avec la :

Proposition 8 : *Soit une courbe elliptique* E *d'équation :*

$$E : y^2 = x^3 + Ax + B \qquad \text{avec} \qquad A, B \in \mathbb{Z};$$

satisfaisant la condition : $4A^3 + 27B^2 \neq 0$.

Soit un point $P = (x, y)$ *non trivial de torsion de la courbe* E. *Alors :*

1) les coordonnées x *et* y *de ce point sont des entiers rationnels*

2) soit $y = 0$ *soit* y^2 *divise* $4A^3 + 27B^2$.

Preuve :

C'est le théorème de Naguell-Lutz cf [14]. ■

1.6 Morphismes de courbes elliptiques

Une courbe elliptique a une structure de groupe abélien de type fini et une structure de variété abélienne de dimension un. Selon la théorie des morphismes de courbes il existe des homomorphismes, des endomorphismes, des isomorphismes et des automorphismes de courbes elliptiques. Indiquons brièvement la nature et quelques propriétés de

ces homomorphismes.

Définition 10 : *Soit deux courbes elliptiques E et E' sur un corps K de points de base respectifs O_E et $O_{E'}$. Un morphisme de courbes elliptiques $f : E \longrightarrow E'$ est un homomorphisme de groupes abéliens $f : E(K) \longrightarrow E'(K)$.*

Endomorphismes d'une courbe elliptique

La description complète de l'anneau des endomorphismes $End(E)$ d'une courbe elliptique a été indiquée par Deuring cf [5] : L'anneau des endormorphismes d'une courbe elliptique est isomorphe soit à l'anneau $\mathbb{Z}$, soit à un ordre d'un corps quadratique imaginaire ; soit à un ordre de l'algèbre des quaternions. Ce dernier cas se produit lorsque $carac(K) = p > 0$. L'ensemble des endomorphismes $End_K(E)$ d'une courbe elliptique $E(K)$ forme un anneau intègre de caractéristique nulle, isomorphe à l'anneau $\mathbb{Z}$ ou isomorphe à un anneau contenant $\mathbb{Z}$.

Définition 11 : *Les courbes elliptiques dont l'anneau des endomorphismes $End_K(E)$ contient l'anneau $\mathbb{Z}$ sont des courbes elliptiques à multiplication complexe.*

Dans le cas où la courbe elliptique E sur un corps quadratique imaginaire $\mathbb{Q}\left(\sqrt{-d}\right)$ est à multiplication complexe, l'anneau $End_{\mathbb{Q}(\sqrt{-d})}(E)$ est isomorphe à l'anneau des entiers de ce corps.

Isomorphismes de courbes elliptiques

Un isomorphisme de courbes elliptiques est un homomorphisme de courbes elliptiques bijectif.

Proposition 9 : *Soit une courbe elliptique E d'équation de Weierstrass :*

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

et de point à l'infini O_E. Alors les changements de variables qui préservent le point à l'infini et la forme (1) *sont de la forme :*

$$\begin{cases} x = \mu^2 x' + r \quad ; \quad y = \mu^3 y' + \mu^2 s x' + t \\ \text{avec} \qquad \mu \in K^* \text{ et } r, s, t \in K. \end{cases} \tag{2}$$

Preuve :

Pour la première partie de la preuve cf [14] chapitre III proposition 3.1.b), page 63.

Le changement de variables (2) transforme l'équation (1) en l'équation :

$$E' : y'^2 + a'_1 x' y' + a'_3 y' = x'^3 + a'_2 x'^2 + a'_4 x' + a'_6 \quad \text{avec} \quad a'_i \in K. \tag{3}$$

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

$$\begin{aligned} &\mu a'_1 = a_1 + 2s; \\ &\mu^2 a'_2 = a_2 - s a_1 + 3r - s^2; \\ &\mu^3 a'_3 = a_3 + r a_1 + 2t; \\ &\mu^4 a'_4 = a_4 - s a_3 + 2r a_2 - (t + r s) a_1 + 3r^2 - 2st; \\ &\mu^6 a'_6 = a_6 + r a_4 + r^2 a_2 + r^3 - t a_3 - t^2 - r t a_1. \end{aligned} \tag{4}$$

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

$$\begin{aligned} &\mu^2 b'_2 = b_2 + 12r; \\ &\mu^4 b'_4 = b_4 + r b_2 + 6r^2; \\ &\mu^6 b'_6 = b_6 + 2r b_4 + r^2 b_2 + 4r^3; \\ &\mu^8 b'_8 = b_8 + 3r b_6 + 3r^2 b_4 + r^3 b_2 + 3r^4. \end{aligned} \tag{5}$$

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

$$\begin{aligned} &\mu^4 c'_4 = c_4; \\ &\mu^6 c'_6 = c_6. \end{aligned} \tag{6}$$

Les discriminants des deux courbes sont liés par la formule :

$$\mu^{12} \Delta(E') = \Delta(E). \tag{7}$$

Les invariants modulaires des deux courbes sont égaux :

$j(E') = j(E)$. (8) ■

Les courbes elliptiques peuvent être classifiées par leurs invariants modulaires $j(E)$.

Proposition 10 : *1) Deux courbes elliptiques sur un corps algébriquement clos sont isomorphes si et seulement si leurs invariants modulaires sont égaux.*

2) Pour tout nombre t d'une clôture algébrique du corps K, il existe une courbe elliptique sur l'extension $K(t)$ d'invariant modulaire $t = j(E)$.

Preuve de"les deux courbes elliptiques E et E' sont isomorphes" implique "leurs deux invariants modulaires sont égaux"

Soit deux courbes elliptiques E et E' isomorphes, alors l'équation de E est transformée en équation de E' par les changements de variables (2). Cela implique la relation (8) : $j(E) = j(E')$.

Preuve de" $j(E) = j(E')$" implique "les deux courbes E et E'sont isomorphes"

Soit deux courbes elliptiques d'équations de Weierstrass :

$$\begin{aligned} E &: y^2 = x^3 + Ax + B; \\ E' &: y'^2 = x'^3 + A'x' + B'; \end{aligned} \qquad (1)$$

satisfaisant les deux conditions respectives : $4A^3+27B^2 \neq 0$ et $4A'^3+27B'^2 \neq 0$. (2)

L'hypothèse :

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

et la formule de l'invariant modulaire :

$$j = 1728.4.A^3/\Delta(E);$$

impliquent la relation :

$$A^3B'^2 = A'^3B^2; \tag{3}$$

Les relations d'isomorphismes de courbes elliptiques donnent les relations entre les coefficients A, A' et B, B' :

$$\mu^4 A' = A \quad \text{et} \quad \mu^6 B' = B. \tag{4}$$

Examinons les cas possibles : $A = 0$ et $B \neq 0$, $A \neq 0$ et $B = 0$ et $AB \neq 0$.

Lorsque $A = 0$ et $B \neq 0$, les formules (4) et (6) des isomorphismes impliquent : $A' = 0$ et $B' \neq 0$. La formule (4) implique les six valeurs $\mu = (B/B')^{1/6}$ qui déterminent les six isomorphismes λ de E dans E' de valeur : $\lambda(x, y) = (\mu^2 x, \mu^3 y)$.

Lorsque $B = 0$, $A \neq 0$, les formules (4) et (6) des isomorphismes impliquent : $A' \neq 0$ et $B' = 0$.

La formule (4) implique les quatre valeurs : $\mu = (A/A')^{1/4}$ qui détermine les quatre isomorphismes θ des deux courbes de valeur $\theta(x, y) = (\mu^2 x, \mu^3 y)$.

Lorsque $AB \neq 0$, les formules (4) et (6) des isomorphismes impliquent $A' \neq 0$ et $B' \neq 0$.

La formule (4) implique $\mu = (A/A')^{1/4} = (B/B')^{1/6}$. (5)

Il en résulte l'isomorphisme φ de E dans E' de valeur : $\varphi(x, y) = (\mu x, \mu y)$.

Les équations des courbes elliptiques isomorphes :

$$E : y^2 = x^3 + A'\mu^4 x + B'\mu^6 \quad ; \quad E' : y^2 = x^3 + A'x + B'.$$

Preuve de"tout nombre t d'une clôture algébrique K^{alg} est l'invariant modulaire d'une courbe elliptique définie sur l'extension $K(t)$"

Soit un élément $t \in K^{alg}$. Considérons la courbe elliptique E d'équation :

$$E : y^2 = x^3 + Ax + B; \tag{1}$$

Son discriminant vaut :

$$\Delta(E) = -16(4A^3 + 27B^2) \neq 0; \tag{2}$$

Son invariant modulaire vaut :

$$j(E) = \frac{4.1728.A^3}{4A^3 + 27B^2}. \tag{3}$$

L'hypothèse : $j(E) = t$ implique la relation :

$$j(E) = \frac{4.1728.A^3}{4A^3 + 27B^2} = t. \tag{4}$$

Pour déterminer les coefficients A et B à partir de la formule (4), nous examinons les trois cas possibles pour l'élément t : $t = 0, 1728$ et $t \neq 0, 1728$.

Lorsque $t = 0$, la formule (3) implique la valeur : $A = 0$. (6)

L'équation (1) de la courbe devient $E : y^2 = x^3 + B$. (7)

La condition (2) implique $B \neq 0$.

Cette courbe elliptique E est isomorphe à toute courbe elliptique $E' : y^2 = x^3 + \mu^6 B$ avec μ dans K.

Lorsque l'invariant modulaire $t = 1728$, la formule (3) implique la relation :

$$1728 = \frac{1728.4.A^3}{4A^3 + 27B^2}. \tag{8}$$

La relation (8) et la condition (2) impliquent :

$$B = 0 \quad ; \quad A \neq 0. \tag{9}$$

La courbe elliptique E d'équation :

$$E : y^2 = x^3 + Ax; \tag{10}$$

est isomorphe à toute courbe elliptique E' d'équation :

$$E' : y^2 = x^3 + \mu^4 Ax \quad \text{avec} \quad \mu \in K^*.$$

Lorsque $t \neq 0$, 1728, la formule de l'invariant modulaire d'une courbe elliptique implique la relation : $27tB^2 = (1728 - t)A^3$. (11)

On choisit $A = \dfrac{3t}{1728 - t} \in K(t)$. (12)

Les relations (11) et (12) impliquent une valeur $B = \dfrac{t}{1728 - t} \in K(t)$. (13)

Les relations (12) et (13) impliquent une courbe elliptique E sur le corps $K(t)$ d'invariant modulaire $t \neq 0; 1728$:

$$E : y^2 = x^3 + \frac{3t}{1728 - t}x + \frac{t}{1728 - t}. \quad \blacksquare$$

Automorphismes d'une courbe elliptique

Définition 12 : *Un automorphisme d'une courbe elliptique est un endomorphisme bijectif du groupe abélien $E(K)$.*

L'ordre du groupe des automorphismes d'une courbe elliptique E est un diviseur de 24, comme le montre la :

Proposition 11 : *Soit une courbe elliptique E sur un corps K, d'invariant modulaire $j(E)$. Alors, le groupe $Aut\,(E)$ de ses automorphismes est d'ordre :*

1) 2 *si* $j(E) \neq 0$ *et* 1728 *et* $caracK \neq 2$ *et* 3.

2) 4 *si* $j(E) = 1728$ *et* $caracK \neq 2$ *et* 3.

3) 6 *si* $j(E) = 0$ *et* $caracK \neq 2$ *et* 3.

4) 12 *si* $j(E) = 0 = 1728$ *et* $caracK = 3$.

5) 24 *si* $j(E) = 0 = 1728$ *et* $caracK = 2$.

où $caracK$ signifie caractéristique du corps K.

Preuve de 1) :

Soit une courbe elliptique E d'équation :

$$E : y^2 = x^3 + a_4x + a_6 \qquad \text{avec} \quad 4a_4^3 + 27a_6^2 \neq 0; \tag{1}$$

sur un corps K de caractéristique $caracK \neq 2$ et 3.

Les formules donnent les deux invariants de la courbe :

$$\Delta(E) = -16(4a_4^3 + 27a_6^2) \neq 0 \qquad \text{et} \qquad j(E) = \frac{4.1728.a_4^3}{4a_4^3 + 27a_6^2} \neq 0,\ 1728. \tag{2}$$

Les hypothèses $caracK \neq 2, 3$, $j(E) \neq 0, 1728$ et la relation (2) impliquent les conditions :

$$a_4 \neq 0 \qquad \text{et} \qquad a_6 \neq 0. \tag{3}$$

Les formules d'isomorphismes (2) du paragraphe 3 donnent l'automorphisme :

$$\begin{aligned} h_u : E(K) &\to E(K) \\ (x, y) &\longmapsto (u^2x, u^3y); \end{aligned}$$

pour un certain élément u non nul du corps K.

La courbe elliptique E' image de la courbe elliptique E par l'isomorphisme h_u est :

$$E' : y'^2 = x'^3 + a'_4x' + a'_6;$$

avec les relations :

$$a_4 = u^4a'_4 \qquad \text{et} \qquad a_6 = u^6a'_6. \tag{4}$$

Les deux courbes E et E' ont leurs deux invariants modulaires égaux :

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

ce qui implique l'égalité :

$$\frac{a_4^3}{4a_4^3+27a_6^2}=\frac{a_4'^3}{4a_4'^3+27a_6'^2}.$$

Les formules (4) donnent les valeurs de l'élément u : $u^4=u^6=1$ par les propriétés de l'automorphisme h_u. Il en résulte $u^2=1$ et les deux automorphismes :

$$(x,y)\rightarrow(x,y) \quad ; \quad (x,y)\rightarrow(x,-y).$$

d'où $Aut(E)$ est d'ordre deux.

Preuve de 2) :

Soit une courbe elliptique E d'équation :

$$E : y^2=x^3+a_4x+a_6. \tag{1}$$

Les formules donnent les deux invariants de la courbe :

$$\Delta(E)=-16(4a_4^3+27a_6^2)\neq 0 \quad et \quad j(E)=\frac{1728.4.a_4^3}{4a_4^3+27a_6^2}=1728. \tag{2}$$

Les hypothèses $caracK\neq 2,\ 3$ et la formule (2) impliquent la condition :

$$a_6=0. \tag{3}$$

La courbe E étant elliptique et la formule (3) impliquent la condition $a_4\neq 0$.

Les formules d'isomorphismes (2) du paragraphe 3 donnent l'automorphisme :

$$\begin{aligned} h_u : E(K) &\rightarrow E(K) \\ (x,y) &\longmapsto (u^2x,u^3y); \end{aligned}$$

pour un certain élément u non nul du corps. La courbe elliptique E' image de la courbe E par l'isomorphisme h_u est $E' : y'^2=x'^3+a_4'x'+a_6'$;

avec les deux relations : $u^4a_4'=a_4$ et $u^6a_6'=a_6$. (4)

Les formules (3) et (4) impliquent : $u^4 a'_4 = a_4$ et $a'_6 = a_6 = 0$. (5)

La formule (5) implique : $u^4 = 1$ qui donne les quatre valeurs de l'élément u :

$u = \pm 1, \pm i$. Il en résulte quatre automorphismes : $(x, y) \longmapsto (x, y)$;

$(x, y) \longmapsto (x, -y); (x, y) \longmapsto (-x, -iy); (x, y) \longmapsto (-x, iy)$.

Preuve de 3) :

Soit une courbe elliptique E d'équation :

$$E : y^2 = x^3 + a_4 x + a_6. \tag{1}$$

Les formules donnent les deux invariants de la courbe :

$$\Delta(E) = -16(4a_4^3 + 27a_6^2) \neq 0 \qquad \text{et} \qquad j(E) = 0. \tag{2}$$

Les hypothèses $caracK \neq 2$ et 3, $j(E) = 0$ et la relation (2) impliquent les valeurs :

$$a_4 = 0 \quad \text{et} \quad a_6 \neq 0. \tag{3}$$

Les formules d'isomorphismes (2) du paragraphe 3 donnent l'automorphisme :

$$\begin{aligned} h_u : E(K) &\to E(K) \\ (x, y) &\longmapsto (u^2 x, u^3 y); \end{aligned}$$

pour un certain élément u non nul du corps. La courbe elliptique E' image de la courbe E par l'isomorphisme h_u est :

$$E' : y'^2 = x'^3 + a'_6;$$

avec le relation :

$$u^6 a'_6 = a_6. \tag{4}$$

L'équation: $u^6 = 1$ admet six racines : $u = \pm 1, \pm j, \pm j^2$. Il en résulte les six automorphismes : $(x, y) \longmapsto (x, y)$; $(x, y) \longmapsto (x, -y)$; $(x, y) \longmapsto (jx, y)$; $(x, y) \longmapsto (jx, -y)$; $(x, y) \longmapsto (j^2 x, y)$; $(x, y) \longmapsto (j^2 x, -y)$ où $j = exp(\frac{2i\pi}{3})$ et $j^3 = 1$.

Preuve de 4) :

C'est la valeur $j(E) = 0$ et la formule $j(E) = \dfrac{c_4^3}{\Delta(E)}$ qui justifient la forme convenable de l'équation de la courbe E que nous prenons :

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

Nous choisissons l'isomorphisme du groupe abélien $E(K)$ de la forme :

$$\begin{aligned} h_u : E(K) &\to E(K) \\ (x, y) &\longmapsto (u^2x + r, u^3y); \end{aligned}$$

Les relations entre a_i et a'_i impliquent les formules :

$$u^4 = a_4/a'_4 \quad \text{et} \quad r^3 + ra_4 + a_6 - u^6a'_6 = 0.$$

Pour $E = E'$, l'automorphisme implique les valeurs $a'_4 = a_4$ et $a'_6 = a_6$. Il en résulte :

$$\begin{cases} u^4 = 1; \\ r^3 + ra_4 + (1 - u^2)a_6 = 0. \end{cases} \tag{1}$$

Cela implique $4 \times 3 = 12$ paires (u, r) qui déterminent le groupe des douze automorphismes de la courbe E. Les quatre valeurs de u sont $\pm 1, \pm i$, les trois valeurs de r sont les trois racines de l'équation dans le système (1). Les douze automorphismes de la courbe E sont :

$(x, y) \longmapsto (x+r_1, y)$; $(x, y) \longmapsto (x+r_2, y)$; $(x, y) \longmapsto (x+r_3, y)$; $(x, y) \longmapsto (x+r_1, -y)$;

$(x, y) \longmapsto (x + r_2, -y)$; $(x, y) \longmapsto (x + r_3, -y)$; $(x, y) \longmapsto (-x + r_1, -iy)$;

$(x, y) \longmapsto (-x + r_2, -iy)$; $(x, y) \longmapsto (-x + r_3, -iy)$; $(x, y) \longmapsto (-x + r_1, iy)$;

$(x, y) \longmapsto (-x + r_2, iy)$; $(x, y) \longmapsto (-x + r_3, iy)$.

Ce groupe engendré par u et r, $u^3 = 1$, $r^3 = 1$, $ur = 1$ est le sous groupe alterné A_4 du groupe symétrique S_4.

Preuve de 5) :

Les hypothèses $caracK = 2$, $j(E) = 0$ et les formules : c_4 et $j(E) = c_4^3/\Delta(E)$ justifient l'équation de la forme :

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

ses invariants valent :

$$c_4 = -48a_4 \qquad ; \qquad \Delta(E) = a_3^2 \neq 0.$$

Les formules convenables de l'automorphisme :

$$\begin{array}{rl} h_u : E(K) & \to E(K) \\ (x, y) & \longmapsto (u^2 x + s^2, u^3 y + s u^2 x + t); \end{array} \qquad (2)$$

pour certains paramètres u, s et t du corps K.

Les relations entre a_i et a_i' impliquent les trois équations :

$$\begin{cases} u^3 = 1 = \dfrac{a_3}{a_3'}; \\ s^4 + a_3 s + (1-u)a_4 = 0; \\ t^2 + t a_3 + s^6 + a_4 s^2 = 0. \end{cases} \qquad (3)$$

Tout automorphisme (2) de la courbe E est déterminé par un triplet (u, s, t). Les équations (3) donnent trois valeurs de u, quatre valeurs de s et deux valeurs de t. Il en résulte que le groupe $Aut(E)$ est un groupe d'ordre vingt-quatre formé par un groupe cyclique C_3 d'ordre trois twisté par le produit d'un groupe engendré par un élément s d'ordre quatre et un groupe engendré par un élément t d'ordre deux.

Ce groupe d'ordre vingt-quatre est isomorphe au groupe spécial linéaire $SL_2(\mathbb{F}_3)$, produit direct d'un groupe cyclique C_3 d'ordre trois par le groupe des quaternions, engendré

par les deux éléments s et t, d'ordre huit. ■

La théorie des courbes elliptiques introduit des homomorphismes particuliers :

Les isogénies de courbes elliptiques

Une courbe elliptique E sur un corps commutatif K a une structure de groupe abélien de type fini .

Tout morphisme de courbes elliptiques :

$$f : E_1(K) \longmapsto E_2(K);$$

satisfait les relations d'homomorphisme de groupes :

$$\begin{aligned} & f : E_1(K) \ \rightarrow E_2(K) \\ & \text{de valeur} \quad f(O_{E_1}) = O_{E_2} \ \text{ et } \ f(P_1 + P_2) = f(P_1) + f(P_2); \end{aligned}$$

pour les points neutres O_{E_i} de la courbe E_i.

Il existe des morphismes surjectifs de noyaux finis ; on a donné un nom particulier à ces morphismes.

Définition 13 : *Une isogénie de deux courbes elliptiques E_1 et E_2 sur un corps commutatif K est un morphisme de courbes elliptiques :*

$$f : E_1(K) \longmapsto E_2(K);$$

qui satisfait les conditions :

1) f n'est pas nulle ;

2) le noyau de f est un sous groupe fini du groupe $E_1(K)$;

3) l'application f est surjective ;

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

Définition 14 : *Le degré de l'isogénie f est égal à l'ordre du groupe $f^{-1}(O_{E_2})$ noyau de f, qui est un sous groupe du groupe $E_1(K)$.*

Définition 15 : 1) *Si la courbe elliptique E_1 est isogène à E_2, alors la courbe E_2 est isogène à E_1. Les deux courbes elliptiques E_1 et E_2 sont isogènes.*

2) *Il existe une isogénie particulière $\widehat{f} : E_2(K) \longmapsto E_1(K)$ associée à une isogénie*

$$f : E_1(K) \longmapsto E_2(K).$$

La relation "E_1 et E_2 isogènes" est une relation d'équivalence dans une classe de courbes elliptiques isogènes :

1) E_1 et E_1 sont isogènes ;

2)"E_1 isogène à E_2" implique "E_2 isogène à E_1";

3)"E_1 isogène à E_2" et "E_2 isogène à E_3" impliquent "E_1 isogène à E_3".

A une isogénie f de degré m de deux courbes elliptiques E_1 et E_2 sur un corps commutatif K, est associée une isogénie unique de degré m :

$$\widehat{f} : E_2(K) \to E_1(K);$$

dont les composées sont la multiplication par m dans les groupes respectifs $E_1(K)$ et $E_2(K) : \widehat{f} \circ f = m_{E_1} : E_1(K) \to E_1(K)$ *et* $f \circ \widehat{f} = m_{E_2} : E_2(K) \to E_2(K)$ de valeurs : $m_{E_i}(P) = mP$ pour $i = 1, 2$.

Définition 16 : *Cette isogénie $\widehat{f}$ associée à l'isogénie $f : E_1(K) \longmapsto E_2(K)$ est l'isogénie duale de l'isogénie f.*

Les formules d'isomorphismes de courbes elliptiques montrent qu'il y a une infinité de courbes elliptiques isomorphes à une courbe elliptique E sur K lorsque K est un corps infini. Il n'en est pas de même pour les courbes elliptiques isogènes.

Proposition 12 : *Soit une courbe elliptique E sur un corps K. Alors, il existe seulement un nombre fini de courbes elliptiques E' isogènes à la courbe E sur K.*

Preuve :

Elle repose sur la propriété de deux courbes isogènes E et E' d'avoir le même ensemble de nombres premiers de mauvaise réduction. ■

Chapitre 2

Réductions d'une courbe elliptique

Dans l'équation de Weierstrass d'une courbe elliptique E :

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

les cinq coefficients a_i sont des éléments d'un corps commutatif K, les deux variables x et y des éléments d'une clôture algébrique K^{alg} du corps K.

L'arithmétique d'un corps de nombres K comporte le chapitre des idéaux et le chapitre des valeurs absolues. La théorie des réductions d'une courbe elliptique définie sur K necessite l'étude de l'arithmétique de ce corps.

2.1 Anneaux particuliers

Définition 17 : *Un anneau local est un anneau $\mathcal{A}$ qui possède un seul idéal maximal $\mathcal{M}$.*

Cela implique que $\mathcal{M}$ est l'ensemble des éléments non inversibles de l'anneau $\mathcal{A}$; l'ensemble $\mathcal{A} - \mathcal{M}$ est celui des éléments inversibles de l'anneau $\mathcal{A}$.

Exemple 6 :

Soit un anneau $\mathcal{A}$ et un idéal premier $\mathcal{P}$ de $\mathcal{A}$; alors l'ensemble $\mathcal{S} = \mathcal{A} - \mathcal{P}$ est une

partie multiplicative ; l'ensemble $\mathcal{S}^{-1}\mathcal{A} = \{\frac{a}{s};\ a \in \mathcal{A} \text{ et } s \in \mathcal{S}\}$ est un anneau local.

Définition 18 : *Un anneau de Dedekind est un anneau noethérien A intégralement clos dont tout idéal premier est maximal.*

Cela implique que tout idéal I de l'anneau $\mathcal{A}$ est factorisé en un produit de puissances d'idéaux premiers P_i de façon unique :

$$I = P_1^{e_1} P_2^{e_2} ... P_r^{e_r}.$$

Définition 19 : *Un anneau de valuation discrète est un anneau principal $\mathcal{A}$ qui possède un seul idéal maximal $\mathcal{M}$.*

Cela implique qu'un anneau de valuation discrète $\mathcal{A}$ est un anneau local ; il existe un élément π dans l'idéal $\mathcal{M}$ tel que tout élément $\alpha \neq 0$ de l'anneau $\mathcal{A}$ se met sous la forme unique : $\alpha = u\,\pi^r$ pour un certain entier rationnel r et une certaine unité u. Cet élément π est une uniformisante de l'anneau $\mathcal{A}$.

2.2 Valuations sur les corps de nombres

Indiquons un bref aperçu de la théorie des valuations d'un corps de nombres.

Définition 20 : *Une valuation d'un corps de nombres F est une fonction à valeurs réelles :*

$$v : F \longrightarrow \mathbb{R};$$

qui satisfait les trois axiomes :

$(val\ 1)$ $v(0) = +\infty$;

$(val\ 2)$ $v(ab) = v(a) + v(b)$;

$(val\ 3)$ $v(a+b) \geq Min(v(a), v(b)) + \alpha_v$ *pour tous les points* a et b dans F.

où α_v est une constante réelle négative ou nulle qui détermine la nature de la valuation v :

v est non archimédienne si et seulement si $\alpha_v = 0$.

v est archimédienne si et seulement si $\alpha_v = -\log 2$.

Exemples 7 :

1) La valuation triviale $v(0) = +\infty$ et $v(a) = 1$ pour tout élément $a \neq 0$ de F.

2) La valuation p-adiques $v_p(x)$ qui désigne le plus grand exposant du nombre premier p qui divise x,dans la décomposition de x en produit de nombres premiers $x = \pm \prod_p p^{v_p(x)}$.

Dans l'ensemble M_F des valuations de F, nous définissons une relation d'équivalence.

Définition 21 : *Deux valuations v_1 et v_2 sont équivalentes si elles satisfont la relation :*

$$v_1 = \alpha . v_2 \quad ; \qquad \textit{pour un certain nombre réel } \alpha > 0.$$

Définition 22 : *La classe d'équivalence d'une valuation v du corps F est le diviseur premier de F :*

$$P = \{\alpha . v,\ \alpha > 0\}.$$

On convient de désigner la classe d'équivalence de v par diviseur premier archimédien si v est archimédienne, par diviseur premier non archimédien si v est non archimédienne.

A toute valuation v non archimédienne d'un corps de nombres F correspondent quatre sous ensembles de F :

$$A_v = \{a \in F\,;\, v(a) \leq 1\};$$

anneau des $v-$entiers du corps F = anneau de valuation en v.

$$M_v = \{a \in F; v(a) < 1\};$$

$v-$idéal premier = idéal premier en v.

$$U_v = \{a \in F; v(a) = 1\};$$

groupe des $v-$unités.

$A_v/M_v = F_{résid}$ =corps résiduel en v. Ces sous ensembles ne sont pas définis pour

une valuation archimédienne de F.

Un corps local est un corps de nombres K de caractéristique nulle, complet pour un diviseur premier $P = \{\alpha.v, \alpha > 0\}$ discret ayant un corps de classes résiduelles $A_v/M_v = K_{résid}$ fini.

2.3 Réduction d'une courbe elliptique modulo une valuation non archimédienne discrète (*V.N.A.D.*)

Définition 23 : *Une valuation $v : F \longrightarrow \mathbb{R}$ est discrète lorsque l'ensemble de valeurs $v(F) = \mathbb{Z} \cup \{\infty\}$.*

Par définition d'une valuation non archimédienne discrète v, en abrégé V.N.A.D., v prend des valeurs $v_p(x)$ dans l'anneau $\mathbb{Z} \cup \{\infty\}$; $v_p(p) = 1$, $v_p(p^n) = n$ pour tout nombre premier p et $v_p(q) = 0$ pour tout nombre premier $q \neq p$ et $v_p(0) = +\infty$.

Soit l'application :

$$\begin{cases} v_p : & \mathbb{K} \longrightarrow \mathbb{F}_p \\ & x \longmapsto \widetilde{x} \quad , \qquad \text{classe de } x \text{ modulo } p. \end{cases} \tag{1}$$

La réduction modulo p de la courbe elliptique E d'équation :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6; \tag{2}$$

est la courbe $\widetilde{E}$ d'équation :

$$\widetilde{E} : y^2 + \widetilde{a}_1xy + \widetilde{a}_3y = x^3 + \widetilde{a}_2x^2 + \widetilde{a}_4x + \widetilde{a}_6. \tag{3}$$

où les coéfficients $\widetilde{a}_i$ sont les réductions modulo p des coéfficients a_i.

Exemple 8 :

Réductions de la courbe E d'équation :

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

La courbe réduite $\widetilde{E}$ modulo v_3 a pour équation :

$$\widetilde{E} : y^2 + 2xy + y = x^3 + x^2 + x + 2.$$

La courbe réduite $\widetilde{E}$ modulo v_5 a pour équation :

$$\widetilde{E} : y^2 + 2xy = x^3 + 3x^2 + x + 3.$$

La courbe réduite $\widetilde{E}$ modulo v_7 a pour équation :

$$\widetilde{E} : y^2 + 2xy + 2y = x^3 + 5x^2 + x.$$

Les courbes réduites sont classées en trois types de réduction : bonne, multiplicative ou additive grace aux deux invariants $\Delta(E)$ et c_4.

Définition 24 : *Soit une courbe elliptique E sur un corps K muni d'une valuation V.N.A.D. v, et ses deux invariants $\Delta(E)$ et c_4. Alors :*

1) la réduction de la courbe E en v est bonne lorsque $v(\Delta(\widetilde{E})) \neq 0$; la courbe réduite $\widetilde{E}$ est donc une courbe elliptique.

2) la réduction de la courbe E en v est multiplicative lorsque $v(\Delta(\widetilde{E})) = 0$ et $v(c_4) \neq 0$; alors la cubique réduite $\widetilde{E}$ n'est pas elliptique, elle possède un point singulier $\widetilde{S}$ qui est un noeud.

3) la réduction de la courbe E en v est additive lorsque $v(\Delta(\widetilde{E})) = 0$ et $v(c_4) = 0$; alors la cubique réduite $\widetilde{E}$ n'est pas elliptique, elle possède un point singulier $\widetilde{S}$ qui est un point de rebroussement.

Exemple 9 :

Soit la courbe elliptique E d'équation :

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

son discriminant vaut : $\Delta(E) = 3^3.5.11$ et son invariant : $c_4 = 2^4.3^2$.

La réduction est mauvaise pour les diviseurs premiers du discriminant qui sont $p = 3, 5, 11$. La réduction est bonne pour les autres nombres premiers. La réduction modulo 3 est additive. Les réductions modulo 5 et 11 sont multiplicatives.

2.4 Equation minimale d'une courbe elliptique

Définition 25 : *L'équation de Weierstrass d'une courbe elliptique* E :

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

est minimale en une valuation N.A.D. v *si les coefficients* a_i *sont* $v-$*entiers et le discriminant* $\Delta(E)$ *est de valuation* $v(\Delta(E))$ *minimale dans l'anneau* $\mathbb{N}$.

Un critère de minimalité est basé sur les relations entre les invariants de deux courbes elliptiques isomorphes. L'équation de Weierstrass est minimale si l'une des trois conditions est satisfaite :

$$\begin{aligned} &(1) v(a_i) \geq 0 \quad \text{et} \quad v(\Delta(E)) < 12; \\ &(2) v(a_i) \geq 0 \quad \text{et} \quad v(c_4) < 4; \\ &(3) v(a_i) \geq 0 \quad \text{et} \quad v(c_6) < 6. \end{aligned}$$

La nature de la réduction en v est précisée par la :

Proposition 13 : *Soit une cubique E singulière d'équation sur un corps K :*

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

Alors :

1) lorsque la courbe E possède un noeud S, elle admet deux tangentes distinctes en ce point S d'équations : $y = r_ix + s_i$ pour $i = 1, 2$. La partie non singulière $E(K)_{ns}$ est un groupe isomorphe au groupe multiplicatif $K^\times$:

$$\begin{array}{ll} E(K)_{ns} & \longrightarrow K^\times \\ (x,y) & \longmapsto \dfrac{y - r_1x - s_1}{y - r_2x - s_2}. \end{array}$$

2) lorsque la courbe E possède un point de rebroussement T, elle admet une tangente unique en ce point T d'équation : $y = rx + s$. La partie non singulière $E(K)_{ns}$ est un groupe isomorphe au groupe additif K^+ :

$$\begin{array}{ll} E(K)_{ns} & \longrightarrow K^+ \\ (x,y) & \longmapsto \dfrac{x - x_T}{y - rx - s}. \end{array}$$

Preuve :

Cf [14] chapitre III -2 proposition 2-5. ■

Proposition 14 : *Soit une courbe elliptique E sur un corps K muni d'une valuation N.A.D. v, la courbe réduite $\widetilde{E}$ sur le corps résiduel $K_{résid}$. Alors, l'application :*

$$\begin{array}{rll} f : E(K)[m] & \longrightarrow \widetilde{E}(K_{résid}) \\ P & \longmapsto f(P) = \widetilde{P}; \end{array}$$

est injective.

Preuve :

Cf [14] chapitre *VII -§ 3* proposition 3-1. ■

Chapitre 3

Rangs de courbes elliptiques

3.1 Groupe E(K)/mE(K)

Pour toute courbe elliptique E sur un corps K, la structure du groupe abélien $E(K)$ est précisée par l'isomorphisme de groupes :

$$E(K) \simeq E_{tor}(K) \times \mathbb{Z}^r;$$

le sous groupe de torsion $E_{tor}(K)$ est fini et le groupe quotient $E(K)/E_{tor}(K)$ est la partie infinie du groupe $E(K)$; ce groupe de rang $r = r(E)$ admet une partie génératrice formée de r points $P_1, P_2, ..., P_r$. Ce rang peut être nul et peut prendre de grandes valeurs. La détermination de ce rang nécessite plusieurs outils mathématiques: nous décrivons quelques uns dans ce chapitre.

Proposition 15 : *Soit une courbe elliptique E sur un corps K de groupe de Mordell-Weil $E(K)$ et le sous groupe $mE(K) = \{mP;\ P \text{ dans } E(K)\}$ pour un entier naturel $m \geq 2$. Alors, le groupe $E(K)/mE(K)$ est fini.*

Preuve :

Le groupe abélien $E(K)$ est additif; donc tous ses sous groupes le sont. Le groupe

quotient $E(K)/mE(K)$ est formé des classes $mE(K)$, $(m+1)E(K), ..., (2m-1)E(K)$ où $(m+t)E(K) = mE(K) + tE(K)$. ■

Introduisons une application entre groupes liés à la courbe E :

Définition 26 : *L'application Ψ de Kummer est :*

$$\begin{array}{rccl} \Psi : & E(K) \times G_{K^{alg}/K} & \longrightarrow & E(K)[m] \\ & (P, \sigma) & \longmapsto & \sigma(R) - R \quad \text{avec} \quad P = mR \text{ et } R \in E(K^{alg}); \end{array} \tag{1}$$

où $G_{K^{alg}/K}$ est le groupe de Galois d'une clôture algébrique K^{alg} de K et $E(K)[m]$ le sous groupe de $m-$torsion du goupe $E(K)$.

Proposition 16 : *Soit l'application Ψ de Kummer définie ci-dessus. Alors :*

1) cette application Ψ est bilinéaire ;

2) le noyau à gauche de Ψ est le sous groupe $mE(K)$;

3) le noyau à droite de Ψ est le sous groupe du groupe de Galois $G_{K^{alg}/K}$ avec $L = K(m^{-1}E(K)) =$ corps engendré par les points R du groupe $E(K)$ qui satisfont $P = mR$.

Preuve de la linéarité de Ψ par rapport à la premiere variable :

$\Psi(P_1 + P_2, \sigma) = \sigma(R_1 + R_2) - (R_1 + R_2)$ avec $P_i = mR_i$. (1)

La loi du groupe abélien $E(K)$ implique les relations $P_1 + P_2 = mR_1 + mR_2$ et

$\sigma(R_1 + R_2) = \sigma(R_1) + \sigma(R_2)$; (2)

les relations (1) et (2) impliquent la relation :

$\Psi(P_1 + P_2, \sigma) = \sigma(R_1) - R_1 + \sigma(R_2) - R_2 = \Psi(P_1, \sigma) + \Psi(P_2 + \sigma)$. (3)

Calcul de l'image $\Psi(O_E, \sigma)$: $\Psi(O_E, \sigma) = \sigma(R) - R$ avec $O_E = mR$; cela implique que R est un point de $m-$torsion. L'image $\sigma(O_E) = O_E$ implique $\sigma(R) - R = O_E$ et $\Psi(O_E, \sigma) = O_E$. (4)

Preuve de la linéarité de Ψ par rapport à la deuxième variable :

$$\Psi(P,\sigma\tau) = \sigma\tau(R) - R \quad \text{avec} \quad P = mR \tag{5}$$
$$= \tau(\sigma(R) - R) + \tau(R) - R$$
$$= \tau\Psi(P,\sigma) + \Psi(P,\tau). \tag{6}$$

Preuve du noyau à gauche :

$$\Psi^{-1}_{gauche}(O_E) = \{P \in E(K)\,;\, \sigma(R) = R\} = \{P \in E(K)\,;\, P = mR\} = mE(K). \tag{7}$$

Preuve du noyau à droite :

$$\Psi^{-1}_{droite}(O_E) = \left\{\sigma \in G_{K^{\text{alg}}/K}\,;\ \sigma(R) = R\right\}. \tag{8}$$

L'hypothèse $P = mR$ implique $R = m^{-1}P$ et l'automorphisme σ du corps K^{alg} laisse fixes les points $m^{-1}P$. (9)

Donc σ laisse fixe le corps $K(m^{-1}E(K)) = L$. (10)

Cela implique le noyau de Ψ à droite : $\Psi^{-1}_{droite}(O_E) = G_{K^{\text{alg}}/K}$. (11) ■

Corollaire : *Cette application Ψ bilinéaire de Kummer induit une application :*

$$\Psi_m : E(K)/mE(K) \times G_{L/K} \longrightarrow E(K)[m];$$

bijective.

Preuve :

On utilise le théorème : *Soit un morphisme surjectif de groupes : $f : G \longrightarrow H$ de noyau $f^{-1}(e)$. Alors, f induit un isomorphisme : $f_0 : G/f^{-1}(e) \longrightarrow H$.* (1)

Le noyau à gauche $\Psi^{-1}_{gauche}(O_E) = mE(K)$ implique l'isomorphisme $E(K)/mE(K) \longrightarrow E(K)[m]$. (2)

Le noyau à droite $\Psi^{-1}_{droite}(O_E) = G_{K^{\text{alg}}/K}$ implique l'isomorphisme $G_{K^{\text{alg}}/K}/G_{K^{\text{alg}}/L} \longrightarrow G_{L/K}$. (3)

Les applications (2) et (3) impliquent l'application Ψ_m du corollaire. ■

Cette application bilinéaire de Kummer est liée à certains groupes de cohomologie relatifs à la courbe E.

Définition 27 : *La suite de Kummer d'une courbe elliptique E sur un corps K est la suite exacte courte :*

$$0 \longrightarrow E(K)/mE(K) \xrightarrow{\delta} H^1(G_{K^{alg}/K}, E(K)[m]) \longrightarrow H^1(G_{K^{alg}/K}, E(K))[m] \longrightarrow 0;$$

où $A[m]$ désigne le sous groupe de $m-$torsion du groupe abélien A, $H^1(G_{K^{alg}/K}, A)$ désigne le premier groupe de cohomologie du groupe G dans le groupe A; l'homomorphisme δ est l'application bilinéaire Ψ_m du corollaire; le 1-cocycle $\delta(P)$ est déterminé par l'application : $c : G_{K^{alg}/K} \longrightarrow E(K)[m]$ de valeur: $c_\sigma(P) = \sigma(R) - R$ avec $P = mR$.

3.2 Hauteurs sur une courbe elliptique

Pour montrer que la partie infinie du groupe de Mordell-Weil $E(K)$, isomorphe au groupe $\mathbb{Z}^r$, est de type fini, il est utile d'introduire la notion de hauteur.

Proposition 17 : *Soit un groupe abélien G et une application :*

$$h : G \longrightarrow \mathbb{R};$$

à valeurs réelles qui satisfait les trois axiomes :

h1) il existe un point P_0 fixé du groupe G et une constante $c_1 = c_1(G, P_0)$ qui satisfont l'inégalité :

$$h(P + P_0) \leq 2h(P) + c_1 \qquad \text{pour tout point } P \text{ de } G.$$

h2) il existe un entier naturel $m \geq 2$ et une constante $c_2 = c_2(G)$ qui satisfait l'inégalité:

$$h(mP) \geq m^2 h(P) + c_2 \qquad \text{pour tout point } P \text{ de } G.$$

h3) l'ensemble des points $\{P \in G : h(P) \leq c_3\}$ est fini pour toute constante c_3.

On suppose que cette fonction existe et que le groupe G/mG est fini; alors le groupe abélien G est de type fini.

Preuve :

Soit un groupe abélien G, le groupe quotient G/mG et des représentants $R_1, R_2, ..., R_t$ des classes de ce groupe quotient. (1)

Considérons une suite de n points $P_1, P_2, ..., P_n$ du groupe G déterminés par des combinaisons de représentants $R_j : P = mP_1 + R_{i_1}$; $P_1 = mP_2 + R_{i_2}$; $P_j = mP_{j+1} + R_{i_{j+1}}$; $P_{n-1} = mP + R_{i_n}$, avec $1 \leq i_1, i_2, ..., i_n \leq t$. (2)

L'axiome $(h2)$ implique l'inégalité : $h(P_j) \leq \frac{1}{m^2}(h(mP_j) + c_2)$. (3)

Les relations (2) et (3) impliquent l'égalité : $mP_j = P_{j-1} - R_{i_{j-1}}$. (4)

Les relations (3) et (4) impliquent l'inégalité : $h(P_j) \leq \frac{1}{m^2}(h(P_{j-1} - R_{i_{j-1}}) + c_2)$. (5)

L'axiome $(h1)$ et la relation (5) impliquent l'inégalité :

$h(P_j) \leq \frac{1}{m^2}(2h(P_{j-1}) + c_2 + c_1')$. (6)

Pour $j = 1, 2, ..., n$, les relations (2) et (6) impliquent :

$$h(P_n) \leq (\frac{2}{m^2})^n h(P) + \left(\frac{1}{m^2} + \frac{2}{m^4} + \frac{2^{n-1}}{m^{2n}}\right)(c_2 + c_1'); \quad (7)$$

la série en $\frac{1}{m^2}$ du deuxième membre provient du développement limité de

$$\frac{c_1' + c_2}{m^2 - 2} = \frac{\frac{c_1' + c_2}{m^2}}{1 - \frac{2}{m^2}}. \quad (8)$$

Les relations (7) et (8) impliquent les inégalités :

$$h(P_n) < (\frac{1}{m^2})^n h(P) + \frac{c_4}{m^2 - 2} \leq \frac{1}{2^n}h(P) + \frac{c_4}{2} \quad \text{pour } m \geq 2 \quad \text{et } c_4 = \frac{c_1' + c_2}{2}. \quad (9)$$

Pour un entier n assez grand, $\frac{1}{2}h(P) = 1$. (10)

Il en résulte la borne de $h(P_n)$: $h(P_n) \leq 1 + c_5$ avec $c_4 = 2c_5$. (11)

L'axiome $(h3)$ et la relation (11) impliquent l'ensemble :

$$E = \{S_n \in G;\ h(S_n) \leq 1 + c_5\} \text{ est fini.} \quad (12)$$

Il en résulte que tout point P du groupe abélien G est une combinaison linéaire :

$P = m_1 R_1 + ... + m_t R_t + m_1' S_1 + m_u' S_u$; avec $S_i \in E$. ■

Définition 28 : *Cette application à valeurs réelles qui satisfait les trois axiomes* $(h1)$, $(h2)$ *et* $(h3)$ *est une hauteur sur le groupe abélien* G.

Le procédé de construction de la suite de points $P_1, P_2, ..., P_n$ dans le groupe G utilise les hauteurs.

Comme le groupe de Mordell-Weil $E(K)$ est abélien, il existe donc des hauteurs sur ce groupe $E(K)$ ou hauteurs sur la courbe elliptique E sur K.

Toute hauteur $h : E(K) \longrightarrow \mathbb{R}$ est définie par sa valeur $h(P)$ en un point P de $E(K)$. Elle peut être déterminée avec une valuation du corps K. Il y a plusieurs valeurs possibles $h(P)$.

Nous citerons ici trois hauteurs sur les courbes elliptiques :

(a) la hauteur logarithmique ou hauteur de Weil ;

(b) la hauteur canonique ou hauteur de Néron -Tate ;

(c) les hauteurs locales liées aux valuations discrètes.

Définition 29 : *La hauteur de Weil (ou hauteur logarithmique) sur une courbe elliptique E sur le corps des nombres rationnels $\mathbb{Q}$ est la fonction : $h : E(\mathbb{Q}) \longrightarrow \mathbb{R}$ de valeur $h(P) = \log\{\max(|a|, |b|)\}$ pour tout point $P = (x, y)$ du groupe $E(\mathbb{Q})$ d'abscisse $x = a/b$.*

Exemple 10 : Soit la courbe elliptique E d'équation :

$$E : y^2 = x^3 - \frac{7}{5}x^2 + \frac{3}{5}x + \frac{7}{25};$$

son discriminant vaut $\Delta(E) = 64.2413.625^{-1} > 0$. Le point $P = \left(\frac{2}{5}, \frac{3}{5}\right)$ se trouve dans le groupe $E(\mathbb{Q})$, sa hauteur de Weil vaut $h(P) = \log\{\max(|2|, |5|)\} = \log 5$.

La hauteur sur le groupe $E(K)$ peut être associée à une fonction $f \in K^{\text{alg}}(E)$. Alors, on obtient une nouvelle hauteur.

Définition 30 : Soit une courbe elliptique E sur un corps K et une fonction $f \in K^{\text{alg}}(E)$; la hauteur de Weil relative à f sur la courbe E est la fonction : $h_f : E(K^{\text{alg}}) \longrightarrow \mathbb{R}$ de valeur : $h_f(P) = \log\{\max(|c|, |d|)\}$ avec $f(P) = f(x, y) = (\frac{c}{d}, z)$.

Exemple 11 :

Soit la courbe elliptique E d'équation :

$$E : y^2 = x^3 + \frac{5}{3}x^2 - \frac{4}{3}x - \frac{16}{27};$$

son discriminant $\Delta(E) = 2^8.3^{-3}.407$. Soit la fonction $f \in K^{\text{alg}}(E)$: $f(x,y) = (u^2x, u^3y)$ avec $u = \frac{1}{2}$. La courbe elliptique E contient le point $P = \left(\frac{2}{3}, \frac{2}{3}\right)$ son image par la fonction f vaut :
$f(P) = \left(\frac{1}{6}, \frac{1}{12}\right)$, la hauteur de Weil relative à la fonction f vaut :
$h_f(P) = \log\{\max(|1|, |6|)\} = \log 6$.

La valeur $h(P)$ peut prendre la forme d'une limite.

Définition 31 : *La hauteur canonique (ou la hauteur de Neron-Tate) sur une courbe elliptique E sur un corps K est la fonction $\widehat{h} : E(K^{\text{alg}}) \longrightarrow \mathbb{R}$ de valeur :*
$\widehat{h}(P) = \lim_{n\to\infty} 4^{-n} h\left(2^n P\right)$.

En associant à cette hauteur canonique $\widehat{h}$ une fonction f paire, non constante, du corps de fonctions $K(E)$, on obtient la hauteur canonique $\widehat{h}_f$ relative à la fonction f.

Proposition 18 : *La hauteur canonique $\widehat{h}_f$ relative à une fonction f à pour valeur :* $\widehat{h}_f(P) = \frac{1}{\deg(f)}\widehat{h}(P) = \frac{1}{\deg(f)} \lim_{n\to\infty} 4^{-n} h_f\left(2^n P\right)$. *Alors, la limite existe; elle est indépendante de f.*

Preuve :

Cf [14] Chapitre $VIII$.§ 9.proposition 9.1. ■

La hauteur canonique est une forme quadratique :

Proposition 19 : *Soit la hauteur canonique $\widehat{h}$ sur une courbe elliptique E sur un corps K. Alors $\widehat{h}$ satisfait les relations :*

1) $\widehat{h}(P+R) + \widehat{h}(P-R) = 2\widehat{h}(P) + 2\widehat{h}(R)$ pour tous points P et R du groupe de Mordell-Weil $E(K)$; c'est la loi du parallélogramme.

2) $\widehat{h}(mP) = m^2\widehat{h}(P)$ *pour tout entier* $m \in \mathbb{Z}$ *et pour tout point* $P \in E(K^{\text{alg}})$.

3) l'application $< .,. >: E(K^{\text{alg}}) \times E(K^{\text{alg}}) \longrightarrow \mathbb{R}$ *de valeur :*

$< P, R >= \widehat{h}(P+R) - \widehat{h}(P) - \widehat{h}(R)$ *est bilinéaire; donc* $\widehat{h}$ *est une forme quadratique sur le groupe* $E(K^{\text{alg}})$

4) $\widehat{h}$ *prend des valeurs positives* $\widehat{h}(P) > 0$ *aux points* P *qui ne sont pas de torsion;* $\widehat{h}(T) = 0$ *lorsque* T *est un point de* m*-torsion avec* $m \geq 2$.

Preuve :

Cf [14] chapitre $VIII$.§ 6 proposition 6.2;on utilise :

$$h_f(P+R) + h_f(P-R) + 2h_f(P) + 2h_f(R) + O(1). \qquad (1)$$

En un point T de $m-$ torsion, $mT = O_E$ cela implique $h(2^n P) = h(O_E) = 0$. ■

Corollaire : *Avec les hypothèses de la proposition précédente, la hauteur canonique* $\widehat{h}$ *sur une courbe elliptique* $E(K)$ *est une forme quadratique, définie, positive sur l'espace vectoriel* $\mathbb{R} \otimes E(K)$.

Preuve :

Le groupe abélien $E(K)$ est de type fini $r(E) = r$. Alors, le produit tensoriel $\mathbb{R} \otimes E(K)$ est un espace vectoriel réel de base $1 \otimes R_1$, $1 \otimes R_2$, ..., $1 \otimes R_r$. Le groupe quotient $E(K)/E_{tor}(K)$ engendre un réseau dans cet espace $\mathbb{R} \otimes E(K)$. ■

La hauteur d'une courbe elliptique E sur un corps K peut être associée à une valuation archimédienne ou non archimédienne de ce corps.

Proposition 20 : *Soit un corps* K *muni d'une valuation* v, *le complété* K_v *en* v *et une courbe elliptique* E *sur le corps* K *d'équation :*

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

Alors, il existe une fonction unique à valeurs réelles : $h_v : E(K_v) - \{O_E\} \longrightarrow \mathbb{R}$ *qui satisfait les quatre propriétés :*

1) h_v *est une fonction continue pour la topologie* $v-$*adique sur le complété* K_v *et pour la topologie usuelle sur le corps* $\mathbb{R}$ *;*

2) $\lim_{P \to O_E} (h_v(P) + \frac{1}{2} v(x))$ *existe lorsque le point* $P = (x, y)$ *tend vers le point* O_E *à l'infini pour la topologie* $v-$*adique;*

3) soit un point $P = (x, y)$ *de la courbe* E *qui n'est pas d'ordre 2. Alors,* h_v *satisfait la relation :* $h_v(2P) = 4h_v(P) + v(2y + a_1 x + a_3) - \frac{1}{4} v(\Delta(E))$;

4) la fonction h_v satisfait *la formule :*
$h_v(P+R) + h_v(P-R) = 2h_v(P) + 2h_v(R) + v(x_P - x_R) - \frac{1}{6} v(\Delta(E))$ *pour tous points* P *et* R *du groupe* $E(K_v)$ *avec* $P \pm R \neq O_E$.

Définition 32 : *La hauteur locale de la courbe elliptique en une valuation* v *du corps* K *est la fonction* h_v *qui satisfait les quatre propriétés contenues dans la proposition précédente.*

La hauteur peut être associée à des fonctions complexes modulaires.

Proposition 21 : *Soit une courbe elliptique* E *sur un corps* K *muni d'une valuation* v *et une hauteur locale* h_v *en* v *sur le groupe* $E(K)$. *Lorsque* v *est archimédienne, soit un réseau complexe* L *et un isomorphisme analytique complexe :* $C/L \longrightarrow E(K_v^{\text{alg}})$ *la fonction* $\sigma(z, L)$ *de Weierstrass, le discriminant* $\Delta(L)$ *du réseau et la fonction complexe Eta* $\eta : L \longrightarrow C$. *Alors,* $h_v(P) = -\log v \left\{ \left| \Delta(L)^{1/12} . \exp(-z\eta(z)/2) . \sigma(z, L) \right| \right\}$, *pour tout point* P *de la courbe* E *correspondant à un point* z *du tore* $\mathbb{C}/L$.

Preuve :

Cf [14] Appendix C ; §18-Local Height Functions, théorème 18.3.a.. ■

Corollaire : *Soit les hypothèses de la proposition 21 et une valuation* v *non archimédienne. Alors lorsque la courbe* E *a une réduction multiplicative décomposée en* v, *on fixe un isomorphisme* $E(K_v)/E_0(K_v) \longrightarrow \mathbb{Z}/N\mathbb{Z}$ *avec* $N = -ord_v(j(E))$. *A tout point* P *du groupe* $E(K_v)$ *correspond un entier* n *tel que* $1 \leq n \leq N-1$ *et la hauteur de valeur :*

$$h_v(P) = -\frac{1}{2}B_2(\frac{n}{N})v(j(E));$$

où $B_2(t) = t^2 - t + \frac{1}{6}$ *est le second polynôme de Bernoulli ;*

$E_0(K_v)$ *ensemble des points* P *de réduction* $\widetilde{P} = O_E$;

$j(E)$ *l'invariant modulaire de la courbe elliptique* E.

Preuve :

Cf [14] Appendix C; §18-Local Height Functions, théorème 18.3.c. ■

Exemple 12 :

Soit la courbe elliptique E d'équation :

$$E : y^2 = x^3 + \frac{5}{3}x^2 - \frac{4}{3}x - \frac{16}{27};$$

son discriminant $\Delta(E) = 2^8.407.3^{-6}$ et son invariant modulaire $j(E) = 2^{-4}.3^4.61.407^{-1}$. La réduction de la courbe est multiplicative pour la valuation N.A.D.v_{407}; elle est additive pour les valuations N.A.D. v_2 et v_3 ; elle est bonne pour les autres valuations N.A.D.

L'application du corollaire donne la hauteur h_v pour la valuation v_{407} :

$h_v(P) = \frac{1}{2}B_2(n/N)v(j(E))$; avec $N = -ord_v(j(E)) = 1$ et $B_2(n/N) = n^2 - n + \frac{1}{6}$ soit

$h_v(P) = (n^2 - n + \frac{1}{6}) = \frac{1}{2}$ pour $n = 1$.

Une relation entre hauteur canonique $\widehat{h}$ et hauteur locale h_v est précisée dans la :

Proposition 22 : *Soit une courbe elliptique* E *sur un corps* K *et l'ensemble* Val_K *des valuations inéquivalentes de* K. *Alors, la hauteur canonique* $\widehat{h}$ *et les hauteurs* h_v *en* v *satisfont la relation :* $\widehat{h}(P) = \frac{1}{[K:\mathbb{Q}]}\sum_{v \in Val_K} n_v h_v(P)$, *où* $n_v = [K_v : \mathbb{Q}]$ *est le degré local de* K *en* v.

Preuve :

Cf [14] Appendix C; §18-Local Height Functions, théorème 18.2. ■

Formulaire de fonctions modulaires :

$\Delta(L) = g_2^3 + 27g_3^2$ pour la courbe elliptique E d'équation $E : y^2 = 4x^3 - g_2x - g_3$.

Dans la suite $q = \exp(2\pi iz)$.

$\Delta(L) = \frac{(2\pi)^{12}}{1728}(E_4(z)^3 - E_6(z)^2)$ avec $E_4(z) = 1 + 240\sum_{n=0}^{\infty}\sigma_3(n)q^n$ et

$E_6(z) = 1 - 504\sum_{n=0}^{\infty}\sigma_5(n)q^n$ où $\sigma_k(n) = \sum_{d/n} d^k$.

Fonction Eta : $\eta(z) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$.

Fonction invariant modulaire : $j(E) = \frac{1728E_4(z)^3}{E_4(z)^3 - E_6(z)^2}$.

Fonction sigma de Weierstrass : $\sigma(z) = \sigma(z, L) = z\prod_{w\in L^*}(1-\frac{z}{w})\exp\left(\frac{(-z/w)+(z(w))^2}{2}\right)$.

Série $G_{2R}(z)$ d'Eisenstein : $G_{2R}(z) = \sum_{w\in L^*} w^{-2k} = 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n$.

Dans la théorie des fonctions modulaires, une fonction modulaire de poids k est une fonction f sur le demi plan de Poincaré $f : \mathbb{H} \longrightarrow \mathbb{H}$ qui satisfait les deux conditions :

1) $f(z) = (cz+d)^{-k}f(M(z))$, pour un nombre rationnel k et une matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ du groupe spécial linéaire $SL_2(\mathbb{Z})$.

2) $f(z)$ admet un developpement de Fourier en la variable $q = \exp(2i\pi z)$ de la forme : $f(z) = \sum_{n=n(f)}^{\infty} c(n)q^n$, pour un entier relatif $n(f)$ dépendant de f.

Une forme modulaire f de poids k est une fonction holomorphe sur le demi plan de Poincaré avec $n(f) = 0$.

3.3 Espaces homogènes ; twists ; groupes de Châtelet-Weil ; groupes de Selmer ; groupes de Shafarevich-Tate

Pour faire des calculs dans le groupe 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).

1 Espaces homogènes

Définition 33 : Un espace homogène pour une courbe elliptique E sur un corps K est une courbe algébrique C sur le corps K, lisse, projective, munie de deux morphismes λ et Ψ où $\lambda : C \times E \longrightarrow C$ qui satisfait :

1) $\lambda(M, O_E) = M$, pour tout point M de C;

2) $\lambda(\lambda(MP), R) = \lambda(M, P + R)$, pour tous les points M de C, P et R de E;

3) à toute paire $\{M, M'\}$ de points de C correspond un point unique P de E tel que $\lambda(M, P) = M'$.

et $\Psi : C \times C \longrightarrow E$, de valeur $\Psi(M, M') = P$, unique point P de E satisfaisant $\lambda(M, P) = M'$.

Les deux morphismes satisfont d'autres propriétés :

Proposition 23 : *Soit un espace homogène $\{C, \lambda, \Psi\}$ pour une courbe elliptique E sur un corps K. Alors les morphismes $\lambda : C \times E \longrightarrow C$ et $\Psi : C \times C \longrightarrow E$ satisfont les relations :*

1) $\lambda(M, O_E) = M$ et $\Psi(M, M) = O_E$ pour tout point M de C;

2) $\lambda(M, \Psi(M', M)) = M'$ et $\Psi(\lambda(M, P), M) = P$ pour tous les points M, M' de C et P de E;

3) $\lambda(\Psi(M, M'), P - P') = \Psi(\lambda(M, P), \lambda(M', P'))$ pour tous les points M, M' de C et P, P' de E.

Preuve :

On utilise les propriétés des deux morphismes λ et Ψ. Pour plus de détails, consulter [14] chapitre $X.\S 3$ ■

Proposition 24 : *A tout espace homogène $\{C, \lambda, \Psi\}$ pour une courbe elliptique E sur un corps K est associé l'application $\theta : E \longrightarrow C$ de valeur $\theta(P) = M_0 + P$, où M_0 est un point fixé de C qui satisfait les cinq propriétés :*

1) θ est un isomorphisme de E sur le corps $K(M_0)$;

2) C est isomorphe à E sur le corps K;

3) $M + P = \theta(\theta^{-1}(M) + P)$, pour tous les points M de C et P de E;

4) $M - M' = \theta^{-1}(M) - \theta^{-1}(M')$, pour tous les points M et M' de C;

5) l'application $\Psi : C \times C \longrightarrow E$, de valeur $\Psi(M, M') = M - M' = P$, unique point P de E tel que $\lambda(M, P) = M'$ est un morphisme de courbes.

Preuve :

On utilise les définitions de C, λ, Ψ et l'action du groupe de Galois $G_{K^{alg}/K}$. ■

Dans l'ensemble des espaces homogènes pour une courbe elliptique E sur un corps K nous définissons une relation d'équivalence par la :

Proposition 25 : *Deux espaces homogènes $\{C, \lambda, \Psi\}$ et $\{C', \lambda', \Psi'\}$ pour une courbe elliptique E sur un corps K sont équivalents s'il existe un isomorphisme $C \longrightarrow C'$ compatible avec les morphismes $E \longrightarrow C$ et $E \longrightarrow C'$.*

Preuve :

Cette relation est reflexive : à un espace homogène $\{C, \lambda, \Psi\}$ il correspond un isomorphisme $C \longrightarrow C$ compatible avec les morphismes $E \longrightarrow C$; donc $\{C, \lambda, \Psi\}$ est équivalent à lui même.

Cette relation est symétrique : Soit deux espaces homogènes $\{C, \lambda, \Psi\}$ et $\{C', \lambda', \Psi'\}$; alors il existe un isomorphisme $C \longrightarrow C'$ compatible avec les morphismes $E \longrightarrow C$

et $E \longrightarrow C'$; tout isomorphisme admet un isomorphisme réciproque $C' \longrightarrow C$; cet isomorphisme est compatible avec les morphismes $E \longrightarrow C'$ et $E \longrightarrow C$, donc les espaces homogènes $\{C, \lambda, \Psi\}$ et $\{C', \lambda', \Psi'\}$ sont équivalents.

Cette relation est transitive : Soit trois espaces homogènes $\{C, \lambda, \Psi\}$, $\{C', \lambda', \Psi'\}$ et $\{C'', \lambda'', \Psi''\}$ tels que $\{C, \lambda, \Psi\}$ équivalent à $\{C', \lambda', \Psi'\}$ et $\{C', \lambda', \Psi'\}$ équivalent à $\{C'', \lambda'', \Psi''\}$.

Alors il existe un isomorphisme $C \longrightarrow C'$ compatible avec les morphismes $E \longrightarrow C$ et $E \longrightarrow C'$, il existe un isomorphisme $C' \longrightarrow C''$ compatible avec les morphismes $E \longrightarrow C'$ et $E \longrightarrow C''$, il en résulte un isomorphisme composé $C \longrightarrow C''$ compatible avec les morphisme $E \longrightarrow C$ et $E \longrightarrow C''$.

Donc les espaces homogènes $\{C, \lambda, \Psi\}$ et $\{C'', \lambda'', \Psi''\}$ sont équivalents.

Cela implique que c'est une relation d'équivalence dans l'ensemble des espaces homogènes $\{C, \lambda, \Psi\}$ pour une courbe elliptique E sur un corps K. ■

La classe triviale est la classe de C agissant sur E par translation.

Proposition 26 : *Soit un espace homogène $\{C, \lambda, \Psi\}$ pour une courbe elliptique E sur un corps K, alors la courbe C est dans la classe triviale si et seulement si le groupe de Mordell-Weil $C(K)$ n'est pas trivial.*

Preuve :

Soit un espace homogène $\{C, \lambda, \Psi\}$ avec une courbe C dans la classe triviale. Alors il existe un $K-$isomorphisme $f : E \longrightarrow C$; cela implique $f(O_E) \in C(K)$.

Soit une courbe C telle que son groupe de Mordell-Weil $C(K)$ n'est pas trivial. Alors, il existe un $K-$isomorphisme $f : E \longrightarrow C$ et un point $M \in C(K)$ tel que $f(P) = M + P$ pour tout point P de la courbe elliptique E. Cet isomorphisme f satisfait les conditions de compatibilité avec les morphismes λ et Ψ de définition d'un espace homogène $\{C, \lambda, \Psi\}$.

Pour plus de détails, consulter [14] chapitre X. ■

2 Groupes de Châtelet-Weil, groupes de Selmer et groupes de Shafarevich-Tate

Définition 34 : *Le groupe de Châtelet-Weil d'une courbe elliptique E sur un corps K est l'ensemble $WC(E/K)$ des classes d'équivalence des espaces homogènes $\{C, \lambda, \Psi\}$ pour E.*

Le groupe $WC(E/K)$ de Châtelet-Weil est lié à la cohomologie de groupes.

Proposition 27 : *Soit une courbe elliptique E sur un corps K, son groupe de Mordell-Weil $E(K)$, son groupe de Châtelet-Weil $WC(E/K)$, le groupe de Galois $G_{K^{alg}/K}$ et le premier groupe de cohomologie $H^1(G_{K^{alg}/K}, E(K))$.*
Alors, l'application :

$$WC(E/K) \longrightarrow H^1(G_{K^{alg}/K}, E(K))$$
$$cl(C/L) \longmapsto cl\{\sigma \longmapsto \sigma(P) - P\};$$

est une bijection.

Preuve :

La classe $\{\sigma, \sigma(P) - P\}$ est un $1-$cocycle du premier groupe de cohomologie. Pour un élément $\sigma\tau$ du groupe de Galois, on obtient le cocycle .

$\sigma\tau(P) - P = \sigma\tau(P) - \tau(P) + \tau(P) - P = \tau(\sigma(P) - P) + \tau(P) - P$. Pour plus de détails, consulter [14] chapitre $X - 3$-théorème $3 - 6$. $p.291$. ■

Avec une isogénie de courbes elliptiques et une valuation du corps K on obtient les groupes de Selmer et les groupes de Shafarevich-Tate.

Définition 35 : *Soit une isogénie $\gamma : E(K) \longrightarrow E'(K)$ de courbes elliptiques, $E[\gamma]$ le noyau de l'isogénie γ, l'ensemble Val_K des valutions inéquivalentes du corps K et le groupe $WC(E/K)$ de Châtelet-Weil de E.*

a) Le groupe de Selmer pour l'isogénie γ est le sous groupe du premier groupe de cohomologie $H^1(G_{K^{alg}/K}, E[\gamma])$ défini par le noyau $S_\gamma(E/K)$ de l'application :

$$H^1(G_{K^{alg}/K}, E[\gamma]) \longrightarrow \prod_{v \in Val(K)} WC(E/K_v).$$

b) Le groupe de Shafarevich-Tate de E sur K *est le sous groupe du groupe* $WC(E/K)$ *de Châtelet -Weil défini par le noyau* $Ш(E/K)$ *de l'application :*

$$WC(E/K) \longrightarrow \prod_{v \in Val(K)} WC(E/K_v).$$

où K_v *est le complété du corps* K *en la valuation* v.

Citons trois résultats relatifs au rang d'une courbe elliptique et au groupe de Shafarevich-Tate.

Proposition 28 : *Il existe une infinité de courbes elliptiques* E *sur le corps des nombres rationnels* $\mathbb{Q}$ *qui satisfont les relations :* $Rang(E(\mathbb{Q})) = 0$ *et le sous groupe de* $2-$*torsion* $Ш(E/\mathbb{Q})[2] = 0$.

Preuve :

Cf [9]. ■

Proposition 29 : *Soit une isogénie* $\gamma : E(K) \longrightarrow E\prime(K)$ *de courbes elliptiques et les groupes* $S_\gamma(E/K)$ *de Selmer et* $Ш(E/K)$ *de Shafarevich-Tate. Alors :*

1) la suite (1) de groupes est exacte :

$$0 \longrightarrow E(K)/\gamma(E(K)) \longrightarrow S_\gamma(E/K) \longrightarrow Ш(E/K)[\gamma] \longrightarrow 0. \qquad (1)$$

2) le groupe $S_\gamma(E/K)$ *de Selmer est fini.*

Preuve :

Cf [14] chapitre X.4.théorème $4-2$ p 298. ■

Proposition 30 : *Soit un nombre premier* $p \equiv 1 \, mod \, 8$ *tel que* $2 \not\equiv n^4 \bmod p$ *et une courbe elliptique* E *sur le corps des nombres rationnels* $\mathbb{Q}$, *d'équation :*

$E : y^2 = x^3 + px$. Alors, $rang E(\mathbb{Q})) = 0$ et le sous groupe de $2-$torsion du groupe $\text{Ш}(E/K)[2]$ de Shafarevich-Tate est isomorphe au groupe $(\mathbb{Z}/2\mathbb{Z})^2$.

Preuve

Cf [14] chapitre $X - 6-$proposition 6.5 p 316. ■

3 Twists de courbes elliptiques

La notion de twist est utilisée pour les groupes : un groupe G twisté par un groupe H est un groupe G "tordu" par le groupe H. Cette idée de "tordre" une courbe elliptique E pour obtenir une autre courbe elliptique est traduite dans la :

Définition 36 : *Un twist d'une courbe elliptique E sur un corps K est une courbe lisse C isomorphe à E sur une extension du corps K.*

Le groupe $Isom(E) = \{E \longrightarrow E\}$ opère sur les courbes elliptiques E avec leur structure de courbes algébriques projectives lisses. Ce groupe contient le sous groupe $Aut(E)$ et le sous groupe des translations de la courbe E.

Proposition 31 : *Soit une courbe elliptique E sur un corps K avec sa structure de courbe algébrique, projective, lisse, le groupe $Isom(E)$ des isomorphismes de E et l'ensemble $Twist(E)$ des twists de la courbe E. Alors :*

1) à chaque twist C de E correspond un isomorphisme $f : C \longrightarrow E$ et une application : $u : G_{K^{alg}/K} \longrightarrow Isom(E)$ liée à f par $u(\sigma) = \sigma f - f$, u élément du groupe de cohomologie $H^1(G_{K^{alg}/K}, Isom(E))$.

2) la classe de cohomologie $\{u\}$ est déterminée par la classe des $K-$isomorphismes du twist C ; elle ne dépend pas de l'application f.

3) l'application :

$$\begin{array}{lcl} Twist(E) & \longrightarrow & H^1(G_{K^{alg}/K}, Isom(E)) \\ cl\,(twist(E)) & \mapsto & cl\,(1 - cocycle\ u); \end{array}$$

où cl signifie classe, est une bijection.

Déterminons l'équation d'un twist de la courbe elliptique E.

Exemple 13 :

Twist d'une courbe elliptique E sur K d'équation :

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

Soit une extension quadratique $K(\sqrt{d})$ du corps K, avec d entier rationnel sans facteur carré et $carac(K) \neq 2$ (2)

Le groupe de Galois $G_{K(\sqrt{d})/K}$ est d'ordre 2 : $G = G_{K(\sqrt{d})/K} = \{S, S^2 = Id\}$. (3)

Il agit sur le corps $K(\sqrt{d})$ par $S(\sqrt{d}) = -\sqrt{d}$ et $S^2(\sqrt{d}) = \sqrt{d}$. (4)

On définit le $1-$cocycle de $H^1(G_{K^{alg}/K}, Isom(E))$ par $u(S) = \left[\dfrac{S(\sqrt{d})}{\sqrt{d}}\right]$. (5)

Dans le corps $K(\sqrt{d})(x, y)$ les fonctions $x' = x$ et $y' = y/\sqrt{d}$ sont fixes par le groupe G. Elles satisfont l'équation:

$$y'^2 d = f(x') = x'^3 + a_2x'^2 + a_4x' + a_6; \qquad (6)$$

Le changement de variables :

$$x' = dx \quad \text{et} \quad y' = dy; \qquad (7)$$

transforme l'équation (6) en l'équation :

$$E_d : d^3y^2 = d^3x^3 + d^2a_2x^2 + da_4x + a_6; \qquad (8)$$

La multiplication de (8) par d^{-3} implique l'équation:

$$E_d : y^2 = x^3 + d^{-1}a_2x^2 + d^{-2}a_4x + d^{-3}a_6; \qquad (9)$$

En posant $d^{-1} = D$ dans (9) on obtient l'équation :

$$E_D : y^2 = x^3 + Da_2x^2 + D^2a_4x + D^3a_6; \qquad (10)$$

E_D est l'équation de la courbe twist de E par le corps quadratique $K(\sqrt{d})$.

Le terme "quadratique" provient du corps quadratique qui a servi à construire le twist.

4 Rangs de twists de courbes elliptiques

Dans le paragraphe précédent sur les twists, nous avons obtenu, pour une courbe elliptique E sur K d'équation :

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6; \tag{1}$$

le twist quadratique E_D de la courbe E :

$$E_D : y^2 = x^3 + Da_2x^2 + D^2a_4x + D^3a_6. \tag{2}$$

Lorsque $a_2 = a_6 = 0$ et $a_4 = -1$; l'équation du twist E_D devient :

$$E_D : y^2 = x^3 - D^2x. \tag{3}$$

Par définition, un rationnel n est un nombre congruent s'il existe un triangle rectangle de côtés a, b, c rationnels, dont l'aire est égale à n. Par exemple $3^2 + 4^2 = 5^2$ implique que l'aire du triangle rectangle de côtés $3, 4, 5$ est égale à $\frac{1}{2}.(3).(4) = 6$; donc 6 est un nombre congruent. Lorsque $D = n$ est un nombre congruent le groupe de Mordell-Weil $E_n(\mathbb{Q})$ de la courbe elliptique E_n et d'équation : $E_n : y^2 = x^3 - n^2x$ est isomorphe au produit de groupes :

$$E_n(\mathbb{Q}) \simeq E_n(\mathbb{Q})_{tor} \times \mathbb{Z}^r.$$

Proposition 32 : *Le groupe de torsion de la courbe E_n sur $\mathbb{Q}$ est d'ordre 4.*

Preuve :

La réduction modulo un nombre premier p ne divisant pas n donne une courbe réduite $\widetilde{E}_n$ sur le corps fini $\mathbb{F}_p$. L'application : $E_n(\mathbb{Q})_{tor} \longrightarrow \widetilde{E}_n(\mathbb{F}_p)$ est injective. Les seuls points rationnels d'ordre fini sur $E_n(\mathbb{Q})$ sont les quatre points d'ordre 2 qui sont $O_E = (\infty, \infty)$, $(0,0)$ et $(\pm n, 0)$. Il en résulte que le groupe de torsion de la courbe E_n est $E_n(\mathbb{Q})_{tor} = \{O_E, (0,0), (\pm n, 0)\}$. Pour plus de détails cf [7] ■

Une relation "nombres congruents -rang" est précisée par la :

Proposition 33 : *Soit la courbe elliptique twist quadratique E_n sur le corps $\mathbb{Q}$ d'équation :*

$$E_n : y^2 = x^3 - n^2 x;$$

Alors, la courbe E_n a un rang $r(E_n) > 0$, si et seulement si le nombre n est congruent.

Preuve de "n est un nombre congruent" implique "rang $r(E_n) > 0$" :

Soit un nombre congruent n. Par définition, n est l'aire d'un triangle rectangle à côtés rationnels ; $a^2 + b^2 = c^2$ et $ab = 2n$. Cela implique des points $P = (x, y)$ rationnels sur la courbe E_n d'abscisse $x = t^2 =$ carré d'un nombre rationnel t. La courbe elliptique E_n admet seulement trois points d'ordre 2 : les points $(0, 0)$ et $(\pm n, 0)$. Les autres points du groupe $E_n(\mathbb{Q})$ sont d'ordre infini ; cela implique le rang $r(E_n) > 0$.

Pour la réciproque cf [7] ■

La détermination du rang $r(E)$ d'une courbe elliptique E peut être entreprise par plusieurs méthodes : méthode de Tate [17], méthode de Penney-Pomerance [A search for elliptic curves with large rank ; Math. Comp. 28 (1974)851 – 853], méthode A Brumer-K Kramer [3].. .

3.4 Bornes de rang d'une courbe elliptique

Nous utilisons ici une méthode de K.Rubin et A.Silverberg basée sur la procédure développée par F.Grouvêa et B.Mazur dans[6].

Soit une courbe elliptique E d'équation :

$$E : y^2 = f(x) = x^3 + ax^2 + bx + c; \qquad (1)$$

avec a, b, c dans l'anneau des entiers relatifs $\mathbb{Z}$ avec :

$18\,abc + a^2b^2 - 4\,a^3c - 4\,b^3 - 27\,c^2 \neq 0.$ (2)

Les twists quadratiques de E sont de la forme $E_d : dy^2 = f(x)$, avec un entier rationnel d sans facteur carré (3)

Tout nombre rationnel x se met sous la forme :

$x = \frac{s}{t}$, avec s, $t \in \mathbb{Z}$ et $t > 0$. (4)

Alors : $f(x) = f(s/t) = (s^3 + as^2t + bst^2 + ct^3)t^{-3}$ implique :

$F(s,t) = t^4 f(s/t) = t(s^3 + as^2t + bst^2 + ct^3)$. (5)

est un nombre entier rationnel, polynôme homogène de deux variables s et t de degré quatre.

Ce nombre entier admet dans l'anneau $\mathbb{Z}$ une décomposition unique en produit de puissances de nombres premiers p et q, p à une puissance paire, q à une puissance impaire:

$F(s,t) = \varepsilon p_1^{2s_1} p_2^{2s_2} ... q_1^{2t_1+1} q_2^{2t_2+1} ...$avec $0 \leq s_i,\ t_i \quad ; \varepsilon = \pm 1.$ (6)

Ce nombre se met sous la forme $F(s,t) = dN^2$, avec d sans facteur carré,

$d = \varepsilon q_1 q_2 ...$ et $\quad N = p_1^{s_1} p_2^{s_2} ... q_1^{t_1} q_2^{t_2} ...$ (7)

La hauteur h_x de Weil opère sur le groupe de Mordell-Weil $E_d(\mathbb{Q})$ par la formule :

$$h_x(x,y) = \max\{1, \log|s|, \log|t|\} = h_x(s/t). \qquad (8)$$

On associe à (7) la série infinie $C_E(j,k)$ pour deux nombres réels $j, k \geq 0$:

$$C_E(j,k) = \sum_{\substack{s,t \in \mathbb{Z},\ F(s,t) \neq 0 \\ \text{pgcd}(s,t)=1}} |d|^{-k} \, |h_x(s/t)|^{-j} \ . \qquad (9)$$

D'après l'exercice 8.17.p 239 cf[14], la hauteur canonique $\widehat{h}_E : E(\mathbb{Q}^{alg}) \longrightarrow \mathbb{R}$ et la hauteur canonique $\widehat{h}_d$ sur la courbe twist E_d satisfont la relation :

$$\widehat{h}_d(x,y) = \widehat{h}_E(x, \sqrt{d}y). \tag{10}$$

$\widehat{h}_E(P) > 0$ pour tout point $P \in E(\mathbb{Q}) - E(\mathbb{Q})_{tor}$ et $\widehat{h}_E(T) = 0$ pour tout point T de torsion de $E(\mathbb{Q})_{tor}$. Alors, l'application :

$$\begin{aligned} \lambda : E_d(\mathbb{Q}) &\longrightarrow E_d(\mathbb{Q})[2] \\ (s/t, y) &\longmapsto \quad (\frac{s}{t}, \frac{N}{t^2}); \end{aligned} \tag{11}$$

est une surjection.

La différence entre hauteur canonique $\widehat{h}_d$ et hauteur de Weil h_x est bornée :

$$\left|\widehat{h}_d(\lambda(s,t)) - \tfrac{1}{2}h_x(s/t)\right| \leq B; \tag{12}$$

avec une certaine constante $B > 0$ indépendante de s et t, cf [14] GTM 106 théorème $VIII.9.6(e)$. Il en résulte l'encadrement :

$$\frac{1}{4}h_x(s/t) \leq \widehat{h}_d(\lambda(s,t)) \leq \frac{3}{4}h_x(s/t). \tag{13}$$

Proposition 34 : *Soit une courbe elliptique E sur le corps $\mathbb{Q}$, de rang r, un nombre réel j positif et la hauteur canonique $\widehat{h}_E$. Alors, si $r \geq 2j$, la série H_E :*

$$H_E = \sum_{P \in E(\mathbb{Q}) - E(\mathbb{Q})[2]} \widehat{h}_E(P)^{-j};$$

est divergente.

Preuve :

Soit r générateurs R_1, R_2, ..., R_r de la partie infinie du groupe de Mordell-Weil $E(\mathbb{Q})$ avec $r \geq 2j$. La hauteur canonique $\widehat{h}_E$ implique une forme quadratique sur l'espace $E(\mathbb{Q})/E_{tor}(\mathbb{Q}) \simeq \mathbb{R} \otimes E(\mathbb{Q})$.

La série H_E est bornée :

$$H_E = \sum_{P \in E(\mathbb{Q}) - E(\mathbb{Q})[2]} \widehat{h}_E(P)^{-j} \geq \sum_{n,\ldots,\, n_t = -\infty}^{+\infty} \widehat{h}_E(\sum_{i=1}^{r} n_i R_i)^{-j}.$$

La série du deuxième membre de l'inégalité est divergente (par la théorie des fonctions Zéta d'Epstein). ■

Il en résulte, pour le cas $r < 2j$, la :

Proposition 35 : *Soit une courbe elliptique twist E_d sur le corps $\mathbb{Q}$ de rang r, un nombre réel j positif et la série précédente $C_E(j,k)$. Alors, $r < 2j$ implique $C_E(j,k)$ converge pour un certain nombre réel $k \geq 1$.*

Preuve :

Soit une courbe elliptique E_d sur $\mathbb{Q}$ de rang $r < 2j$. Alors il existe une base $R_1, R_2, ..., R_r$ du groupe $E_d(\mathbb{Q}) - E_d(\mathbb{Q})_{tor}$ (1)

Soit la série infinie :

$$C_E(j,k) = \sum_{\substack{s,t\in\mathbb{Z},\, F(s,t)\neq 0 \\ \text{pgcd}(s,t)=1}} |d|^{-k} \, |h_x(s/t)|^{-j} \, . \tag{2}$$

La relation :

$$\frac{1}{4} h_x(s/t) \leq \widehat{h}_d(s/t);$$

et la formule (2) impliquent l'inégalité :

$$C_E(j,k) \leq 4^{-j} \sum_{\substack{s,t\in\mathbb{Z},\, F(s,t)\neq 0 \\ \text{pgcd}(s,t)=1}} |d|^{-k} \left|\widehat{h}_d(s/t)\right|^{-j} \, . \tag{3}$$

La relation $\widehat{h}_d(s/t) > 0$ pour tout point P du groupe $E_d(\mathbb{Q}) - E_d(\mathbb{Q})_{tor}$ et l'hypothèse $r < 2j$ impliquent l'inégalité :

$$C_E(j,k) \leq \sum_{\substack{s,t\in\mathbb{Z},\, F(s,t)\neq 0 \\ \text{pgcd}(s,t)=1}} |d|^{-k} \left|\widehat{h}_d(P)\right|^{-j} \, . \tag{4}$$

Les combinaisons $P = n_1R_1 + n_2R_2 + ... + n_rR_r$ avec $r < 2j$ et la forme quadratique associée à la hauteur canonique $\widehat{h}_d$ impliquent que la série $\sum_P \left|\widehat{h}_d(P)\right|^{-j}$ est bornée. Il en résulte que la série $\sum_{\substack{s,t\in\mathbb{Z},\, F(s,t)\neq 0 \\ \text{pgcd}(s,t)=1}} |d|^{-k} \left|\widehat{h}_d(P)\right|^{-j}$ est bornée pour un certain entier $k \geq 1$. Donc la série $C_E(j,k)$ converge pour un certain entier $k \geq 1$. ■

Cette proposition est utilisée pour la recherche de twists quadratiques de courbes elliptiques de rang élevé, dont l'algorithme est précisé par Grouvêa et Mazur cf [6].

Pour conclure cette étude, nous signalons la méthode de Crémona [4]; elle consiste en une procédure de 2−déscente pour la recherche de courbes modulaires et de 2-rang du groupe $\text{Ш}(E/K)$ de Shafarevich-Tate. La détermination de l'image de l'homomorphisme injectif $E(\mathbb{Q})/2E(\mathbb{Q})$ dans le groupe de Selmer implique que le rang du groupe $E(\mathbb{Q})$ est égal à $r = t, t-1$ ou $t-2$ suivant que le nombre de points d'ordre 2 dans le groupe de Mordell-Weil $E(\mathbb{Q})$ est respectivement $0, 1$ ou 3 (lorsque le 2−groupe de Selmer est d'ordre 2^t). On peut trouver dans cet ouvrage de Cremona [4] des tables de générateurs de groupes $E(\mathbb{Q})$ de Mordell-Weil dans chaque classe d'isogénie de rang $r > 0$.

Bibliographie

[1] **B.J.Birch and W.Kuyk(eds)** : Modular functions of one variable; *lectures notes in Mathmatics 476 (1975), Springer Verlag.*

[2] **B.J.Birch and H.P.F.Swinnerton-Dyer :** Notes on elliptic curves I; *Jour. Reine Anger.Math., 212 (1963) 7-25.*

[3] **A.Brumer and K.Kumer** : The rank of elliptic curves; Duke. Math. Jour. *44 (1977) 715-743.Springer Verlag, New York, Inc.(1997).*

[4] **J.E.Cremona** : Algorithms for modular elliptic curves; *Cambridge University Press (1997).*

[5] **M.Deuring :** Algebren; *Springer Verlag, New York (1968).*

[6] **F.Grouvêa and B.Mazur** : The square-free sieve and the rank of elliptic curves, *J.Amer.Math.Soc.4 (1991) 1-23.*

[7] **N.Koblitz :** Introduction to elliptic curves and modular formes. G.T.M 97.*Springer Verlag.*

[8] **G.Kramaz :** All congruent numbers less than *2000, Math Ann. 273 (1986) 337-340.*

[9] **V.I.Kolyvagin** : Finiteness of $E(\mathbb{Q})$ and $E(\mathbb{Q})$ for a subclass of Weil curves; *Math USSR Izvest. 32 (1989) 523-542.*

[10] **S.Lang** : a)Elliptic fonctions, Addisson Wesley *(1973).*

b) Intoduction to modular forms, *Springer Verlag (1996).*

c) Elliptic curves diophantiene analyse, *Springer Verlag.*

[11] **M.Laska** : An algorithm for finding a minimal Weierstrass equation for an elliptic curves, Math. Comp. *38 (1982) 257-260.*

[12] **B.Mazur** : a) Modular curves and the Eisenstein ideal, *IHES Publ. Math. 47.(1977), 33-186.*

b) Rational isogenies of prime degre, *Invent. Math. 44 (1978), 129-162.*

[13] **G.Shimura** : Introduction to the arithmetic theory of the automorphic functions, *Jap. Math. Soc. n° 11 (1971).*

[14] **J.H.Silverman** : a) The arithmetic of elliptic curves, G T M *106, Springer Verlag (1986).*

b) Computing heighs on elliptic curves, *Math. Comp. 51 (1988) 339-358.*

c) The difference betwen the Weil Height and the canonical height on elliptic curves, *Math. Comp. 55 (1990) 723-743.*

[15] **C.L.Stewart and J.Cop** : On ranks of elliptic curves and power free values of binary forms , *J. Amer. Math. Soc. 8 (1995) 943-973.*

[16] **N.P.Smart, S.Siksek and J.R.Meriman** : Explicit *4*-descents on an elliptic curve, *Acta. Math., LXXVII.4 (1996) 385-404.*

[17] **J.T.Tate** : Algorithm for determining the singular fiber in an elliptic pencil, Modular functions of one variable *IV*, Lecture notes in Mathematics *476, Springer Verlag (1975)*