N° d'ordre : 16 / 2006 – M / MT.

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE D'ENSEIGNEMENT SUPERIEURE ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE
« HOUARI BOUMEDIENE »

Faculté de Mathématiques

MEMOIRE

Présenté pour l'obtention du diplôme de MAGISTER

EN : MATHEMATIQUE

Spécialité : Algèbre et Théorie des Nombres

Par : **MOUHOUB Rachida**

SUJET

Isomorphismes et p-Descentes sur les Courbes Elliptiques

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

M. BEBBOUCHI Rachid	Professeur à l'U.S.T.H.B	Président.
M. ZITOUNI Mohamed	Professeur à l'U.S.T.H.B	Directeur de thèse.
M. HACHAICHI M. S	Professeur à l'U.S.T.H.B.	Examinateur.
M. HERNANE Mohand Ouamar	Maître de conférences à l'U.S.T.H.B	Examinateur.

REMERCIEMENTS

Je remercie Monsieur Mohamed **Zitouni**, professeur à l'USTHB de m'avoir proposée ce sujet et je tiens à lui exprimer toute ma reconnaissance et gratitude pour son entière disponibilité et pour tout le temps consacré à m'assister à la réalisation de cette thèse.

Je remercie tout particulièrement Monsieur Rachid **BEBBOUCHI** maître de conférences à l'USTHB pour son acceptation à présider le jury et à apprécier ce présent travail.

Je remercie également Messieurs Mohand Ouamar **HERNANE** et M.S. **HACHAICHI** maîtres de conférences à l'USTHB pour leur participation au jury.

CHAPITRE I
GEOMETRIE DES COURBES ELLIPTIQUES

Les Courbes Elliptiques sont des courbes algébriques planes particulières ; c'est pourquoi nous commençons par une étude des courbes algébriques planes.
La théorie de ces courbes se trouve dans les ouvrages de géométrie analytique (géométrie dans le plan et géométrie dans l'espace).

1. Courbes algébriques planes : équations et classifications

Définition 1 : *une courbe algébrique plane est l'ensemble des points* $P=(x,y)$ *qui satisfont l'équation* $f(x,y)=0$*, où* $f(x,y)$ *est un polynôme de degré* n *de l'anneau* $IR[x,y]$.

Pour n = 1, les courbes algébriques sont des droites :

$$f(x,y)=(d_1x+d_2y)+d_3, \qquad (1)$$

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

$$f(x,y)=(d_1x^2+d_2xy+d_3y^2)+(d_4x+d_5y)+d_6, \qquad (2)$$

Les courbes sont des cercles lorsque :

$$f(x,y)=(x-d_1)^2+(y-d_2)^2=r^2, \qquad (2-1)$$

des ellipses lorsque :

$$f(x,y)=\frac{x^2}{a^2}+\frac{y^2}{b^2}=1, \quad a\neq b, \qquad (2-2)$$

des hyperboles lorsque :

$$f(x,y)=\frac{x^2}{a^2}-\frac{y^2}{b^2}=1, \quad a\neq b, \qquad (2-3)$$

ou des paraboles lorsque :

$$f(x,y)=y^2=2px \qquad (2-4)$$

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

$$f(x,y)=g_3+g_2+g_1+g_0, \quad g_t=\text{polynôme homogène de degré } t,$$
$$=g_t(x,y) \qquad (3)$$

Les courbes algébriques associées sont des cubiques.

Dans la théorie des courbes algébriques, les courbes sont des quartiques pour n = 4, des quintiques pour n = 5, des sextiques pour n = 6, etc.…

Un polynôme $f(x,y)\in \mathrm{IR}[x,y]$ de degré n peut être factorisé ou non. Cela implique une classification des courbes algébriques en deux classes : la classe des courbes irréductibles et la classe des courbes réductibles.
Pour n = 1, les droites sont irréductibles.
Pour n = 2, il y a les courbes irréductibles (cercles et coniques)
et les courbes réductibles qui sont produit de deux droites.
Pour n = 3, il y a la classe des cubiques irréductibles et la classe des cubiques dégénérées en produit de trois droites ou dégénérées en produit d'une quadratique par une droite.

Dans la classe des courbes algébriques, de degré n, irréductibles, il y a possibilité de points singuliers.

Cela implique une classification en deux classes :
Classe des courbes non singulières et classe des courbes singulières.

Le nombre s de points singuliers d'une courbe algébrique intervient dans l'invariant genre :
Définition 2 : *le genre d'une courbe algébrique plane C de degré n, ayant s points singuliers, est l'entier naturel positif ou nul :*

$$g(C) = \frac{1}{2}(n-1)(n-2) - s \ , \qquad (4)$$

Exemples :
Les droites, les cercles, les coniques et les cubiques singulières ont un genre égal à $g(C) = 0$.
Les cubiques non singulières ont un genre $g(C) = 1$.

2. Equations de Weierstrass des cubiques irréductibles :

Une Courbe Elliptique est munie de plusieurs structures algébriques.
Nous choisissons la :
Définition 3 : *une Courbe Elliptique est une cubique plane, irréductible, non singulière, d'équation spécifique de Weierstrass :*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \in K[x, y] \ ; \qquad (5)$$

où K est un corps commutatif global, local ou fini.

Les deux variables sont des éléments d'une clôture algébrique K_{alg} du corps K.
Les propriétés de la Courbe Elliptique dépendent du corps de base K.

Lorsque K est le corps $\mathbb{Q}$ des nombres rationnels ou un corps de nombres algébriques nous étudions la Courbe Elliptique au moyen de la Théorie des Nombres (entiers algébriques, idéaux, équations diophantiennes, nombres premiers, fonctions arithmétiques, valuations, etc.…).
Lorsque K est le corps $\mathbb{C}$ des nombres complexes, nous étudions la Courbe Elliptique au moyen de l'Analyse Complexe (réseaux et tores complexes, fonctions elliptiques, formes modulaires, etc.…) et la Géométrie Algébrique (variétés abéliennes, diviseurs, schémas, cohomologie, etc.…).

Lorsque K est un corps fini IF_q, à $q = p^n$ éléments, p premier, nous étudions la Courbe Elliptique au moyen de la théorie des corps finis.

Lorsque K est un corps local, nous étudions la Courbe Elliptique au moyen de la théorie des corps locaux.

L'équation affine de Weierstrass se met sous la forme d'équation projective :

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \in \mathrm{IP}^2(K) \qquad (6)$$

L'équation (5) de Weierstrass peut être transformée au moyen de substitutions convenables.

Nous éliminons les monômes en xy et en y avec le changement de variables linéaire :

$$(x,y)\to\left[X,\frac{1}{2}(Y-a_1X-a_3)\right] \qquad (7)$$

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

$$E_1 : Y^2=4X^3+b_2X^2+2b_4X+b_6\in K[X,Y] \qquad (7-1)$$

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

$$b_2=a_1^{\,2}+4a_2\ ;\ b_4=a_1a_3+2a_4\ ;\ b_6=a_3^{\,2}+4a_6\ ; \qquad (7-2)$$

L'élimination du coefficient 4 et du monôme en X^2 dans l'équation E_1 s'obtient avec le changement de variables linéaire :

$$(X,Y)\to\left[\frac{x-3b_2}{36},\frac{y}{108}\right] \qquad (8)$$

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

$$E_2 :\ y^2=x^3-27c_4x-54c_6\in K[x,y] \qquad (8-1)$$

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

$$c_4=b_2^2-24b_4\ ;\ c_6=-b_2^3+36b_2b_4-216b_6 \qquad (8-2)$$

D'autres transformations permettent d'obtenir d'autres équations de Weierstrass :

(1) L'équation de Weierstrass **:**

E : $y^2=x^3+Ax+B\in K[x,y]$ (9)

(2) L'équation de Legendre :

E : $y^2=x(x-1)(x-t)$; $t\neq 0,1$ (9-1)

(3) L'équation de Tate :

E : $y^2+xy=x^3+ax+b\in\mathbb{C}[x,y]$ (9-2)

Les coefficients a et b admettent des développements en séries :

$$a=-5\sum_{n\geq 1}n^3q^n(1-q^n)^{-1}\ ; \qquad (9-3)$$

$$b=-\frac{1}{12}\sum_{n\geq 1}q^n(7n^5+5n^3)(1-q^n)^{-1}\ ;$$

avec $q=\exp(2i\pi z)$ et z dans le demi-plan supérieur ***IH*** $=\{z\in\mathbb{C},\ \mathrm{Im}\ z>0\ \}$.

(4) L'équation de Deuring **:**

E : $y^2+axy+y=x^3$; $a^3\neq 27$, sur un corps K de caractéristique $\neq 3$. (9-4)

3. Invariants des cubiques de Weierstrass :

Les Courbes Elliptiques possèdent plusieurs invariants : arithmétique, algébrique, géométrique, différentiel, analytique : le discriminant, l'invariant modulaire, l'invariant différentiel, l'invariant de Hasse, le conducteur, le régulateur, le rang, la série L de Dirichlet, la fonction Zêta, etc.…

Ces invariants sont des objets mathématiques associés aux cubiques de Weierstrass qui permettent de classifier l'ensemble des cubiques.

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

$$\Delta(E) = 9b_2b_4b_6 - 8{b_4}^3 - 27{b_6}^2 - {b_2}^2b_8; \qquad (10)$$

Où l'on a posé $4b_8 = b_2b_6 - {b_4}^2$ *et pour* $caract(K) \neq 2,3$.

Définition 5 : *l'invariant modulaire d'une cubique de Weierstrass E est l'élément du corps K égal à :*

$$j(E) = \frac{{c_4}^3}{\Delta(E)}; \qquad (11)$$

Définition 6 : *l'invariant différentiel d'une cubique de Weierstrass E est l'élément différentiel :*

$$\omega(E) = \frac{dx}{2y + a_1x + a_3} = \frac{-dy}{3x^2 + 2a_2x + a_4 - a_1y} = \frac{dx}{F_y'} = \frac{-dy}{F_x'}\ . \qquad (12)$$

Les dénominateurs sont les dérivées partielles dans l'équation différentielle :

$dF = F_x'dx + F_y'dy = 0$;

où $F(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$ est l'équation de Weierstrass de la cubique E.

Avec les formules (10), (11) et (12) nous obtenons les invariants :

1) Cubique de Weierstrass $E : y^2 = x^3 + Ax + B$

$$\Delta(E) = -16\left(4A^3 + 27B^2\right),\ j(E) = 1728\left(4A^3\right)/\left(4A^3 + 27B^2\right),\ \omega(E) = \frac{dx}{2y} = \frac{-dy}{3x^2 + A} \qquad (13)$$

2) Cubique de Legendre : $E : y^2 = x(x-1)(x-t),\quad t \neq 0,1$

$$\Delta(E) = 16t^2(t-1)^2,\ j(E) = 2^8\left(t^2 - t + 1\right)^3 / t^2(t-1)^2\ ,\ \omega(E) = \frac{dx}{2y} = \frac{-dy}{3x^2 - 2(t+1)x + t} \qquad (13-1)$$

4. Variétés algébriques abéliennes :

Une Courbe Elliptique admet une structure de Variété abélienne de dimension un.

Nous indiquons quelques notions de Variétés algébriques en nous inspirant d'ouvrages de Géométrie Algébrique, **(HARTSHORNE)**, (**SHAFAREVITCH)**, **(LANG)**....

Nous décrivons successivement les espaces et les Variétés affines, les espaces et les Variétés projectifs, les Variétés abéliennes, les Diviseurs.

4-1. Espaces affines, Variétés affines :

Considérons un corps K algébriquement clos et le K-espace vectoriel K^n des points $a = (a_1,...,a_n)$ à n coordonnées $a_1,...,a_n$ dans K.

Définition 7 : *un n-espace affine sur un corps K est l'ensemble des $n-uples$ $(a_1,...,a_n)$ d'éléments de K :*

$$IA^n(K) = \{a = (a_1,...,a_n); a_1,...,a_n \in K\} \qquad (14)$$

C'est un espace de dimension n.

Cet espace est muni d'une topologie spéciale : la topologie de Zariski qui repose sur les ensembles algébriques.

Définition 8 : *un ensemble algébrique affine est l'ensemble des zéros d'une famille de polynômes $f_1,..., f_d$ de l'anneau $K[X_1,..., X_n]$ associé au n-espace affine $IA^n(K)$.*

Ce sont les ensembles algébriques de l'espace $IA^n(K)$ qui jouent le rôle de fermés.

Définition 9 : *la topologie de Zariski est formée par les ensembles algébriques comme des fermés et leurs complémentaires comme des ouverts.*

Pour cette topologie, l'ensemble vide et l'espace $IA^n(K)$ sont les seules parties ouvertes et fermées à la fois.
Cette topologie n'est pas de Hausdorff.
Avec cette topologie, l'espace affine devient une Variété affine.

Définition 10 : *(1) une Variété affine est une partie d'un espace affine, irréductible et fermée pour la topologie de Zariski.*

(2) une Variété quasi affine est une partie ouverte d'une Variété affine.

(3) une sous Variété d'une Variété affine V est une partie Y de V irréductible et fermée.

Exemple :

L'ensemble $V = \{a = (a_1, a_2, a_3) \in IA^3(IR); f(a) = 0; f(x, y, z) = x^2 y - xz^2\}$
muni de la topologie de Zariski est une Variété affine.

Pour obtenir une Variété projective, nous considérons une relation d'équivalence Eq dans l'espace affine $IA^{n+1}(K)$:

"Deux points $a=(a_1,a_2,...,a_n,a_{n+1})$ et $b=(b_1,b_2,...,b_n,b_{n+1})$ sont équivalents si et seulement si il existe un élément $\lambda \neq 0$ dans K tel que :

$$b=\lambda a=(\lambda a_1,...,\lambda a_{n+1})\ ; \qquad (15)$$

Cette relation Eq satisfait les propriétés d'une relation d'équivalence : réflexivité, symétrie et transitivité.

Définition 11 : *le n-espace projectif est l'ensemble des classes :*

$$IP^n(K)=IA^{n+1}(K)-\{0\}/Eq \qquad (16)$$

Il en résulte que les notions d'ensembles algébriques et de topologie de Zariski valables sur l'espace affine $IA^{n+1}(K)$, le sont aussi sur l'espace projectif $IP^n(K)$.

Définition 12 : *(1) une Variété projective est une partie de l'espace projectif $IP^n(K)$ irréductible et fermée.*

(2) une Variété quasi projective est une partie ouverte d'une Variété projective.

(3) une sous Variété projective est une partie irréductible et fermée d'une Variété projective.

Exemple :

La Variété projective $IP^2(IR)$ est l'ensemble des classes : $cl(r_1,r_2,r_3)$

$$cl(0,1,0)=\{(0,1,0),(0,2,0),(0,\sqrt{2},0),.....\}$$
$$cl(1,1,1)=\{(1,1,1),(5,5,5),(-\tfrac{3}{4},-\tfrac{3}{4},-\tfrac{3}{4}),.....\} \qquad (17)$$

Signalons que la réunion $Y_1 \cup Y_2$ de deux sous Variétés de la Variété projective $IP^n(K)$ n'est pas une Variété ; la réunion $Y_1 \cup Y_2$ est réductible.

Les polynômes $f(x_1,x_2,...,x_n,x_{n+1})$ d'une Variété projective $IP^n(K)$ sont homogènes de degré $d=1,2,.....$

Le passage des coordonnées affines aux coordonnées projectives s'obtient avec l'application :

$$IA^n(K)\to IA^n(K)$$
$$(x_1,...,x_n)\to\left(\frac{x_1}{x_{n+1}},...,\frac{x_n}{x_{n+1}}\right) \qquad \text{(tr 1)}$$

suivie de l'application multiplication par x_{n+1}^d, où d = degré du polynôme $f \in K[x_1,...,x_n]$.

$$\left(\frac{x_1}{x_{n+1}},...,\frac{x_n}{x_{n+1}}\right)\to x_{n+1}^d\left(\frac{x_1}{x_{n+1}},...,\frac{x_n}{x_{n+1}}\right) \qquad \text{(tr 2)}$$

Exemple de passage du plan affine $IA^2(K)$ au plan projectif $IP^2(K)$:
Soit le polynôme affine : $f(x,y) = x^3 - 3yx + 2y^2 - 4y - 7 \in IA^2(K)$;
La transformation (tr 1) transforme le polynôme f en polynôme :

$$f\left(\frac{x}{z},\frac{y}{z}\right) = \frac{x^3}{z^3} - \frac{3xy}{z^2} + 2\frac{y^2}{z^2} - 4\frac{y}{z} - 7 \in IA^2(K).$$

Pour $d = 3$, la multiplication par z^3 transforme le polynôme $f\left(\frac{x}{z},\frac{y}{z}\right)$ en le polynôme homogène de degré 3 :

$$g(x,y,z) = x^3 - 3xyz + 2y^2z - 4yz^2 - 7z^3 \in IP^2(K).$$

Le passage du polynôme homogène $g(x,y,z)$ au polynôme affine s'obtient avec l'application :

$$(x,y,z) \to (x,y,1)$$

Une Variété abélienne se construit avec une Variété de groupe abélien.

Définition 13 : *une Variété abélienne est une Variété projective X munie de 2 applications :*

$X \times X \to X$, $(a,b) \to a+b$ *: loi de groupe abélien.*

$X \to X$, $a \to a^{-1}$ *: application inverse*

Exemple : Courbe Elliptique E d'équation de Weierstrass :

$$E : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \in IP^2(K).$$

La loi de groupe abélien sur le groupe de Mordell-Weil $E(K)$:

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

$f(O_E) = O_E$ = point à l'infini

et $E(K) \to E(K)$, $P \to -P$

la dimension de cette Variété abélienne est égale à :

dim $IP^2(K)$-nombre de relations = 2-1 = 1.

Donc une Courbe Elliptique a une structure de Variété abélienne de dimension un.

5. Diviseurs des courbes algébriques :

[**HARTSHORNE**] : II-6- Divisors ; [**SHAFAREVICH**] : III- Divisors and Differentials Forms .

Hartshorne distingue les Diviseurs de Weil sur les courbes algébriques, les Variétés et les Diviseurs de Cartier sur les schémas.
Shafarevich traite les Diviseurs sur les Variétés, sur les schémas et sur les fonctions $f \in K[X]$
Nous suivons la description de [**HARTSHORNE**].
Soit une courbe algébrique C, projective, non singulière dans $IP^2(K)$, de degré d et une famille $\{L\}$ de lignes de $IP^2(K)$.
L'intersection $L \cap C$ contient d points $P_1,...,P_d$, simples ou multiples de multiplicités n_i.
Définition 14 : *un Diviseur sur une courbe algébrique C est une somme formelle :*

$$D = \sum_i n_i P_i \quad , \quad n_i \in \mathbb{Z} \ , \qquad (18)$$

Lorsque la ligne L varie, l'intersection $L \cap C$ varie et les Diviseurs varient.
Nous obtenons une famille de Diviseurs $\mathrm{Div}(C)$; cet ensemble possède une structure de groupe abélien avec le Diviseur : $D = 0 = \sum_i 0.P_i$, comme élément neutre.
la loi : $D + D' = \sum_i n_i P_i + \sum_i n_i' P_i = \sum_i (n_i + n_i') P_i$,
et le symétrique $-D = \sum_i (-n_i) P_i$. $\qquad (18-1)$

Définition 15 : *un Diviseur de Weil est un élément du groupe abélien libre $\mathrm{Div}(X)$ engendré par les Diviseurs premiers.*

Les entiers $n_i > 0$ correspondent aux zéros de la courbe C, les entiers $n_j < 0$ correspondent aux pôles de C.

Exemple : Diviseurs de la courbe C d'équation :

$$y^2 = f(x) = 4(x-2)^2(x-3)^3(x-4)^{-1}(x-5)^{-4} .$$

Alors son Diviseur de Weil est égal à :

$$D = 2P_1 + 3P_2 - P_3 - 4P_4 ,$$

avec les points :

$P_1 = (2,0)$ zéro d'ordre 2 , $P_2 = (3,0)$ zéro d'ordre 3 , $P_3 = (4,0)$ pôle d'ordre 1 et $P_4 = (5,0)$ pôle d'ordre 4.

Il y a des Diviseurs particuliers.
Définition 16 : *(1) un Diviseur effectif est un Diviseur* $D = \sum_i n_i P_i$ *à coefficients* $n_i \geq 0$.

(2) un Diviseur principal est le Diviseur $(f) = \sum_i n_i P_i$ *d'une fonction rationnelle non nulle* $f \in K(\mathbb{C})$, *les* P_i *sont les zéros et les pôles de* f *avec leurs ordres de multiplicités* n_i.

Alors pour deux fonctions rationnelles f , $g \in K(\mathbb{C})$, les Diviseurs principaux associés sont (f), (g)et $(f/g) = (f) - (g)$.
Le groupe $Div(X)$des Diviseurs d'une courbe *X* contient un sous groupe particulier : le sous groupe $P(X)$des Diviseurs principaux.

Définition 17 : *(1) deux Diviseurs* D *et* D' *du groupe* $Div(X)$*sont linéairement équivalents si* $D - D'$ *est un Diviseur principal.*
(2) le groupe quotient $Div(X)/P(X)$*est le groupe des classes des Diviseurs de X.*

$$cl(X) = Div(X)/P(X) \qquad (18-2)$$

Le degré d'un Diviseur $D = \sum_i n_i P_i$ est l'entier rationnel :

$$\deg D = \sum_i n_i \text{ , pour des points } P_i .$$

Le degré d'un Diviseur $D = \sum_i n_i X_i$, où les X_i sont des sous schémas de codimension un, est l'entier rationnel :

$$\deg D = \sum_i n_i \deg X_i .$$

Exemple : 6.6.1, [HARTSHORNE].

Soit une surface quadrique non singulière H d'équation : *xy = zu* dans l'espace projectif $IP^3(K)$; alors son groupe de classes de Diviseurs est le groupe infini :

$$cl(H) \cong \mathbb{Z} \oplus \mathbb{Z}$$

Exemple 3 : [SHAFAREVICH].

Groupe de classes de Diviseurs particuliers :

(1) $cl(IA^n(K)) = 0$;
(2) $cl(IP^n(K)) = \mathbb{Z}$;
(3) $cl(IP^{n_1} \times ... \times IP^{n_l}) = \mathbb{Z}^l$.

6. Discriminants – Résultants :

L'équation de Weierstrass d'une cubique irréductible :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \in K[x, y] \qquad (19)$$

peut être singulière ou non singulière.

C'est avec le discriminant $\Delta(E)$ de la formule précédente que nous pouvons le savoir.

Pour cela, nous considérons une équation cubique :

$$y^2 = f(x) \in K[x]$$

L'irréductibilité d'un polynôme $f(X) = a_0X^n + a_1X^{n-1} + ... + a_{n-1}X + a_n \in \mathbb{Q}[X]$ peut être déterminée au moyen du :

Critère d'irréductibilité (Eisenstein) :

Soit un polynôme $f(X) = a_0X^n + ... + a_n \in \mathbb{Q}[X]$ de degré n et un nombre premier p .

Supposons que p satisfait les congruences :

a_0 *non congru à 0 modulo* p^2, $a_0 \equiv a_1 \equiv ... \equiv a_{n-1} \equiv 0 \bmod p$ *et* a_n *non congru à 0 modulo p*

Alors $f(x)$ est irréductible sur $\mathbb{Q}$.

Preuve : [LANG-1]. Chapitre V § 7
[KOSTRIKIN]. Chapitre V § 3.

□

Il y a un lien entre le discriminant $\Delta(E)$ d'une cubique de Weierstrass E et le discriminant $dis(f(x))$ d'un polynôme $f(x)$ de la cubique de Weierstrass : $y^2 = f(x)$

Commençons par le discriminant de $f(x)$.

Définition 18 : *le discriminant d'un polynôme :*

$f(x) = a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n = a_0(x - t_1)(x - t_2)...(x - t_n)$ *de degré n > 1, est la fonction symétrique des racines t_i égale à :*

$$dis(f(x)) = a_0^{2n-2} \prod_{1 \le i < j \le n} (t_i - t_j)^2 . \qquad (20)$$

[KOSTRIKIN] page 245 , [LANG] page 139.

Avec le calcul nous obtenons les discriminants $dis(f)$ des polynômes cubiques :

(1) pour $f(X) = X^3 + aX + b$, alors : $dis(f) = -(4a^3 + 27b^2)$; (21)

(2) pour $f(X) = d_0X^3 + d_1X^2 + d_2X + d_3$, alors :

$$dis(f) = 18d_0d_1d_2d_3 + d_1^2d_2^2 - 4d_0d_2^3 - 4d_1^3d_3 - 27d_0^2d_3^2 \ ; \qquad (21-1)$$

(3) pour $f(X) = 4X^3 + b_2X^2 + 2b_4X + b_6$, alors :

$$dis(f) = 16(9b_2b_4b_6 - 8b_4^3 - 27b_6^2 - b_2^2b_8) \ ; \qquad (21-2)$$

(4) pour $f(X) = X^3 - 27c_4X - 54c_6$, alors :

$$dis(f) = 4 \times 27^3 (c_4^3 - c_6^2) \ ; \qquad (21-3)$$

En comparant les discriminants $\Delta(E)$ et $dis(f)$, nous obtenons la :

Proposition 1 :

Soit une cubique plane E, irréductible, d'équation de Weierstrass :

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

Les discriminants $\Delta(E)$ de E et $dis(f)$ satisfont les relations :

1) $dis(f) = 16\Delta(E)$ *lorsque* $f(x) = 4x^3 + b_2x^2 + 2b_4x + b_6$;

2) $\Delta(E) = 16dis(f)$ *lorsque* $f(x) = x^3 + Ax + B$ *et lorsque* $f(x) = x^3 + a_2x^2 + a_4x + a_6$

□

Les zéros de deux polynômes $f(x)$ et $g(x)$ d'un anneau $K[x]$ sont liés par le résultant $\mathrm{Re}\,s(f,g)$:

Définition 19 : *soient 2 polynômes* $f(x) = u_0x^n + u_1x^{n-1} + ... + u_n$ *de degré* $n > 1$ *et* $g(x) = v_0x^p + v_1x^{p-1} + ... + v_p$ *de degré* $p > 1$ *; le résultant de ces 2 polynômes est égal au déterminant d'ordre* $n + p$ *:*

$$\mathrm{Re}\,s(f,g) = \begin{vmatrix} u_0 & u_1 & . & . & . & u_n & 0 & . & . & . \\ 0 & u_0 & u_1 & . & . & . & u_n & 0 & . & . \\ . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & 0 & u_n & . \\ 0 & . & . & . & . & 0 & u_0 & . & . & u_n \\ v_0 & v_1 & . & . & . & v_p & 0 & . & . & 0 \\ 0 & v_0 & v_1 & . & . & . & v_p & . & . & 0 \\ . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . \\ 0 & . & . & . & . & . & v_0 & v_1 & . & v_p \end{vmatrix}$$

formé de p lignes $(u_0,...,u_n)$ et n lignes $(v_0,...,v_p)$, les termes manquants sont remplacés par des zéros.

La diagonale principale est formée de p termes u_0 et n termes v_p.

Les résultants possèdent de nombreuses propriétés que l'on peut trouver dans (LANG-1) et (KOSTRIKIN).

Proposition 2 :

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

□

Le résultant est une fonction des zéros des 2 polynômes.

Proposition 3 :

Soit deux polynômes :

$$f(x) = u_0(x-\theta_1)(x-\theta_2)...(x-\theta_n) \text{ de degré } n > 1$$

$$et \quad g(x) = v_0(x-\lambda_1)(x-\lambda_2)....(x-\lambda_p) \text{ de degré } p > 1.$$

Alors leur résultant est égal à :

$$\begin{aligned} \mathrm{Re}\,s(f,g) &= u_0^p v_0^n \prod_{1\le i\le n}\prod_{j=1}^{p}(\theta_i - \lambda_j) \\ &= u_0^p \prod_{1\le i\le n} g(\theta_i) = (-1)^{np} v_0^n \prod_{1\le j\le p} f(\lambda_j). \end{aligned}$$

□

Le discriminant $dis(f)$ est lié au résultant $\mathrm{Re}\,s(f, f')$ de $f(x)$ et sa dérivée $f'(x)$ par la :

Proposition 4 :

Soit un polynôme $f(x) = u_0(x-\theta_1)...(x-\theta_n)$ *de degré* $n > 1$, *sa dérivée* $f'(x)$.

Alors le discriminant $dis(f)$ *et le résultant* $\mathrm{Re}\,s(f, f')$ *satisfont les relations :*

$$\begin{aligned} \mathrm{Re}\,s(f, f') &= (-1)^{\frac{n(n-1)}{2}} u_0 dis(f) \\ &= u_0^{n-1} \prod_{1\le i\le n} f'(\theta_i) \end{aligned}$$

□

Proposition 5 :

Soit les hypothèses de la proposition 4.

Alors : $\mathrm{Re}\,s(f, f') = u_0^{n-1}(nu_0)^n \prod_{1\le i\le n}\prod_{j\ne i}(\theta_i - \theta_j).$

□

7. Classification des cubiques irréductibles par leurs discriminants :

Soit une cubique plane C, algébrique, irréductible, d'équation de Weierstrass :

$$C : y^2 = f(x) \in K[x].$$

Le résultant $\mathrm{Re}\,s(f, f')$ est nul lorsque $f(x)$ admet 2 racines égales ; (proposition 4) ; il en résulte que la cubique C est singulière ; son discriminant $\Delta(C)$ est nul ;(proposition 1).

Cela implique une classification des cubiques irréductibles par leurs discriminants.

Proposition 6 :

Soit une cubique algébrique plane C, *irréductible, d'équation de Weierstrass :*

$$C : \ y^2 = f(x) \in K[x]$$

de discriminant $\Delta(C)$ *:*

1) la cubique C *est une Courbe Elliptique si et seulement si* $\Delta(C) \ne 0$.

2) la cubique C *est singulière si et seulement si* $\Delta(C) = 0$.

Preuve de " C est une Courbe Elliptique " implique " $\Delta(C) \neq 0$ "
Prenons une équation de Weierstrass de la forme :

$$C : y^2 = f(x) \in IR[x] \qquad (1)$$

Par définition, une Courbe Elliptique est une cubique non singulière ; donc elle coupe l'axe Ox en trois points simples :

$$P_i = (e_i, 0) \; ; \;\; e_i \neq e_j \; ; \;\; i = 1,2,3. \qquad (2)$$

(1) et (2) impliquent le polynôme $f(x)$:

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

Cela implique le résultant $\mathrm{Re}\, s(f, f') \neq 0$ (4)
La proposition (1) implique le discriminant :

$$\Delta(C) \neq 0 \qquad (5)$$

Preuve de " $\Delta(C) \neq 0$ " implique " la cubique C est une Courbe Elliptique"
La relation $\Delta(C) = d.dis(f)$ et l'hypothèse $\Delta(C) \neq 0$ impliquent :

$$dis(f) \neq 0 \qquad (6)$$

Il en résulte que $f(x)$ admet 3 zéros simples : e_1, e_2, e_3 ; (7)
Donc la cubique C est non singulière ; c'est une Courbe Elliptique. (8)

Preuve de " la cubique C est singulière " implique " $\Delta(C) = 0$ "
L'hypothèse " C est singulière " implique " $f(x)$ admet un zéro multiple". (9)
D'après la théorie des discriminants des polynômes,
$dis(f) = 0$ si et seulement si f a une racine multiple (10)
(9) et (10) impliquent : $dis(f) = 0$ (11)
Les relations $\Delta(C) = d.dis(f)$ et (4) impliquent la valeur :

$$\Delta(C) = 0 \, . \qquad (12)$$

□

Une cubique irréductible C, singulière, admet 2 types de point singulier :
un nœud , où la cubique admet 2 tangentes distinctes,
un point de rebroussement , où la cubique admet 2 tangentes confondues.

Figure 1 : un nœud au point $(0,0)$

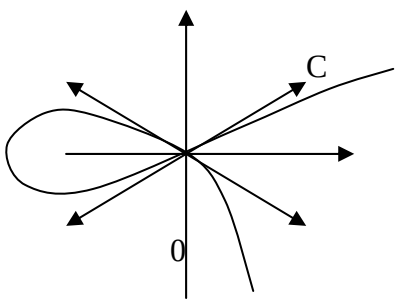
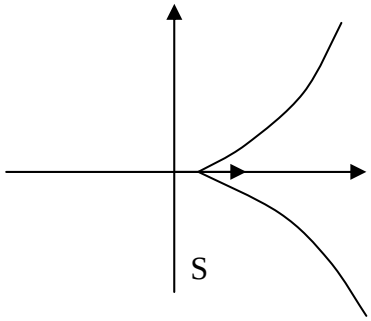


Figure 2 : un point de rebroussement S



Proposition 7 :
Soit une cubique de Weierstrass C *, son discriminant* $\Delta(C)$ *et son invariant usuel* $c_4(C) = c_4$.
1) la cubique admet un nœud si et seulement si $\Delta(C) = 0$ *et* $c_4(C) \neq 0$
2) la cubique admet un point de rebroussement si et seulement si $\Delta(C) = 0$ *et* $c_4(C) = 0$
Preuve de " la cubique C admet un nœud " implique " $\Delta(C) = 0$ et $c_4 \neq 0$ "
Soit une cubique C qui admet un nœud ; donc la cubique C est singulière ; par la proposition 6, son discriminant est nul :

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

L'hypothèse d'un nœud S sur la cubique C implique que la cubique admet 2 tangentes distinctes en S ; (2)
La pente d'une tangente est égale à la dérivée y' de y .
Prenons une équation de Weierstrass :

$$C : y^2 = x^3 - 27c_4 x - 54c_6 \ ; \qquad (3)$$

La dérivée de y est égale à :

$$y' = \frac{\left(3x^2 - 27c_4\right)}{2y} = \frac{3\left(x^2 - 9c_4\right)}{2y} = \frac{N(x)}{2y} \qquad (4)$$

Les tangentes au nœud S sont distinctes ; cela implique que le polynôme $N(x) = 3\left(x^2 - 9c_4\right)$ admet 2 zéros simples.
Donc $c_4 \neq 0$ sur un corps K de carat $(K) \neq 3$. (5)
Preuve de " la cubique C admet un point de rebroussement " implique " $\Delta(C) = 0$ et $c_4 = 0$ ".
Soit une cubique C qui admet un point de rebroussement, cela implique que la cubique est singulière ; donc $\Delta(C) = 0$.
Les formules (1), (3) et (4) sont valables.
L'hypothèse d'un point de rebroussement S sur C implique 2 tangentes confondues à la cubique en S.
Cela implique que $N(x)$ admet un zéro double ; il en résulte :

$$c_4 = 0 \qquad (6)$$

□

Les Courbes Elliptiques sont classifiées en 2 classes par leurs discriminants :
classe des Courbes Elliptiques qui coupent l'axe Ox en 3 points simples,
classe des Courbes Elliptiques qui coupent l'axe Ox en un seul point, qui est simple.

Proposition 8 :
Soit une Courbe Elliptique E *et son discriminant* $\Delta(E)$.
1) E coupe l'axe Ox en trois points simples si et seulement si $\Delta(E) > 0$.
2) E coupe l'axe Ox en un seul point, qui est simple, si et seulement si $\Delta(E) < 0$.

Preuve de " E coupe l'axe Ox en trois points simples " implique " $\Delta(E) > 0$ ".
Nous choisissons une équation de Weierstrass :

$$E : y^2 = (x-e_1)(x-e_2)(x-e_3) = f(x) \in IR[x], \quad e_i \neq e_j . \tag{1}$$

Par définition, le discriminant de $f(x)$ est égal à :

$$dis(f) = (e_1-e_2)^2 (e_1-e_3)^2 (e_2-e_3)^2 \tag{2}$$

Les trois zéros e_1, e_2, e_3 sont des nombres réels ; les carrés $(e_i - e_j)^2$ sont positifs. (3)

Il en résulte :

$$dis(f) > 0 \tag{4}$$

La formule (4) et la relation entre les discriminants de f et de E impliquent :

$$\Delta(E) > 0. \tag{5}$$

Preuve de " $\Delta(E) > 0$ " implique " la Courbe Elliptique E coupe l'axe Ox en 3 trois points simples "

Soit une Courbe Elliptique d'équation de Weierstrass :

$$y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6 = f(x) \in IR[x] \tag{6}$$

La relation $dis(f(x)) = 16\Delta(E)$ et l'hypothèse $\Delta(E) > 0$ impliquent : $dis(f(x)) > 0$ (7)

(6) et (7) impliquent que le polynôme $f(x)$ admet 3 racines simples : e_1, e_2, e_3.

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

Preuve de " E coupe l'axe Ox en seul point simple " implique " $\Delta(E) < 0$ "

Considérons une Courbe Elliptique qui coupe l'axe Ox en un seul point simple $P = (e, 0)$.

Cela implique l'équation de Weierstrass :

$$y^2 = (x-e)\, g(x) = f(x) \in IR[x] . \tag{8}$$

Les deux racines e_1 et e_2 du polynôme $g(x)$ sont conjuguées complexes.

$$e_1 = r + is , \quad e_2 = r - is , \quad r \text{ et } s \text{ réels.} \tag{9}$$

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

$$dis(f) = ((e-e_1)(e-e_2)(e-e_3))^2 \tag{10}$$

Avec le calcul nous obtenons la valeur :

$$dis(f) = -4s^2 \left((e-r)^2 + s^2 \right) \tag{11}$$

Les carrés des nombres réels sont positifs, il en résulte :

$$dis(f) < 0 \tag{12}$$

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

$$\Delta(E) < 0 \tag{13}$$

Preuve de " $\Delta(E) < 0$ " implique " la Courbe Elliptique E coupe l'axe Ox en un seul point, simple "

Un polynôme cubique admet trois racines e_i, simples ou multiples :

$$E : y^2 = 4(x-e_1)(x-e_2)(x-e_3) = f(x) \in IR[x] \tag{14}$$

La relation entre $dis(f(x))$ et $\Delta(E)$ et l'hypothèse $\Delta(E)<0$ impliquent : $dis(f(x))<0.$ (15)
Par définition $dis(f)$ est lié aux racines e_i par :

$$dis(f)=4^4(e_1-e_2)^2(e_1-e_3)^2(e_2-e_3)^2 \in IR \qquad (16)$$

Les relations (14) et (15) impliquent un carré négatif.
Cela implique $e_1=e$ réel, $e_2=r+it$ et $e_3=r-it$; conjuguées complexes.
Alors : $dis(f)=(e-r-it)^2(e-r+it)^2(2it)^2$

$$=-4t^2\left[(e-r)^2+t^2\right]^2<0.$$

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

Les résultats précédents sont rassemblés dans la :
Proposition 9 : (classification des cubiques de Weierstrass).
Soit une cubique C de Weierstrass, son discriminant $\Delta(C)$, son invariant usuel c_4 et son équation :

$$y^2=f(x)\in IR[x].$$

L'ensemble de ces cubiques se répartit en quatre classes selon les valeurs $\Delta(C)$ et c_4 :
I) la classe des cubiques qui ont un nœud, lorsque $\Delta(C)=0$ et $c_4\neq 0$.
II) la classe des cubiques qui ont un point de rebroussement, lorsque $\Delta(C)=0$ et $c_4=0$.
III) la classe des Courbes Elliptiques E qui coupent l'axe Ox en trois points simples, lorsque $\Delta(E)>0$.
IV) la classe des Courbes Elliptiques E qui coupent l'axe Ox en un seul point, qui est simple, lorsque $\Delta(E)<0$.
□

Illustrons cette classification avec un exemple de chaque classe.
Exemple 1 : cubique ayant un nœud :
Soit la cubique E_1 d'équation de Weierstrass :

$$E_1 : y^2=x^3-5x^2+3x+9 \qquad (1)$$

Nous obtenons avec le calcul les invariants de E_1 :

$$b_2=-20,\quad b_4=6,\quad b_6=36,\quad b_8=-189,\quad c_4(E_1)=256\neq 0,\quad \Delta(E_1)=0. \qquad (2)$$

$\Delta(E_1)=0$ implique que la cubique E_1 est singulière.
Cette cubique E_1 a un point singulier.
Le coefficient $c_4\neq 0$ implique que ce point est un nœud.
Les coordonnées de ce nœud sont les solutions du système de 3 équations algébriques :

$$\begin{cases} f(x,y)=y^2-x^3+5x^2-3x-9=0 \\ \dfrac{df}{dx}(x,y)=-3x^2+10x-3=0 \\ \dfrac{df}{dy}(x,y)=2y=0 \end{cases} \qquad (3)$$

Nous obtenons la solution $(3,0)$.
Pour trouver les abscisses entières, nous utilisons le :

Théorème :

Soit une équation diophantienne :

$$f(x) = x^n + r_1 x^{n-1} + \ldots\ldots\ldots + r_n = 0$$

Toute solution de $f(x)$ *est un diviseur du coefficient* r_n.

Ici $r_n = 9$, le test des diviseurs de 9 implique $f(-1) = 0 = f(3)$.
Donc $f(x)$ admet 2 racines : $x_1 = -1$ et $x_2 = 3$.
Il en résulte la factorisation $x^3 - 5x^2 + 3x + 9 = (x-3)(x-3)(x+1)$

$$y^2 = x^3 - 5x^2 + 3x + 9 = (x-3)^2(x+1) \qquad (4)$$

La relation (4) implique la condition $x \geq -1$.

Tableau de coordonnées de quelques points de la cubique E_1 :

x	-1	$-\frac{1}{2}$	0	1	2	3	4	5
y	0	$\pm\frac{7\sqrt{2}}{4}$	± 3	$\pm 2\sqrt{2}$	$\pm\sqrt{3}$	0	$\pm\sqrt{5}$	$\pm 2\sqrt{6}$

La cubique E_1 coupe l'axe Ox en un seul point simple $(-1,0)$ et un point double $(3,0)$.

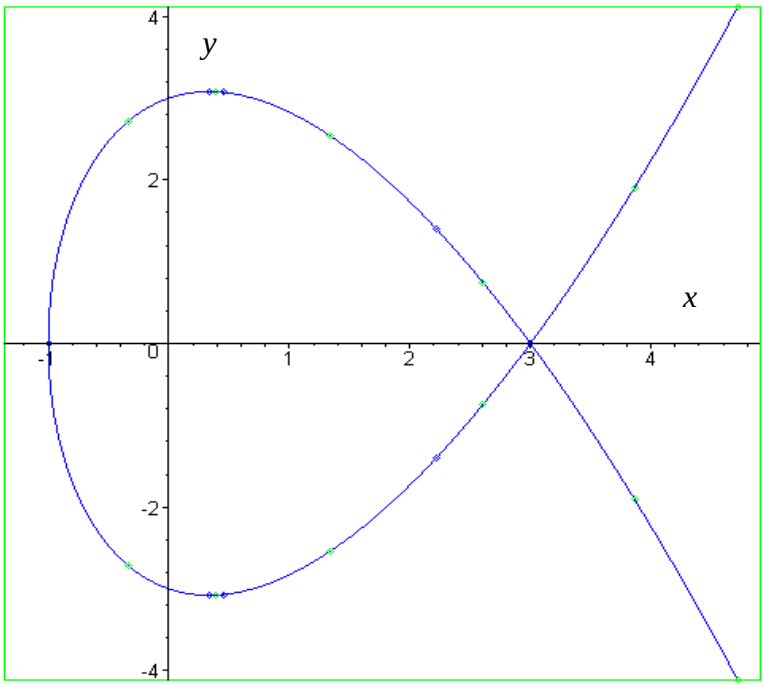


Figure 3 (Courbe tracée avec le logiciel Maple)

Exemple 2 : cubique ayant un point de rebroussement
.Soit la cubique E_2 d'équation de Weierstrass :

$$E_2 : y^2 + 2xy = x^3 + 2x^2 + 3x + 1. \qquad (1)$$

Nous obtenons par le calcul les invariants de E_2 :

$$b_2 = 12,\quad b_4 = 6,\quad b_6 = 4,\quad b_8 = 3,\quad c_4(E_2) = 0,\quad \Delta(E_2) = 0. \qquad (2)$$

$\Delta(E_2) = 0$ implique que la cubique plane E_2 n'est pas une Courbe Elliptique.
Cette cubique E_2 a un point singulier.
Le coefficient $c_4 = 0$ implique que ce point singulier est un point de rebroussement.
Les coordonnées de ce point de rebroussement sont les solutions du système de trois équations algébriques :

$$\begin{cases} f(x,y) = y^2 + 2xy - x^3 - 2x^2 - 3x - 1 = 0 \\ \dfrac{df}{dx}(x,y) = 2y - 3x^2 - 4x - 3 = 0 \\ \dfrac{df}{dy}(x,y) = 2y + 2x = 0 \end{cases} \qquad (3)$$

Nous obtenons la solution $(-1,1)$.

Tableau de coordonnées de quelques points de E_2

x	-2	-1	$-\frac{1}{2}$	0	$\frac{1}{2}$	1
y	Pas de racines y réelles.	1 Racine double.	$\frac{1}{2} \pm \frac{\sqrt{2}}{4}$	± 1	$-\frac{1}{2} \pm \frac{3\sqrt{6}}{4}$	$-1 \pm 2\sqrt{2}$

La cubique E_2 coupe l'axe Oy en deux points d'ordonnées $y_1 = -1$ et $y_2 = 1$.

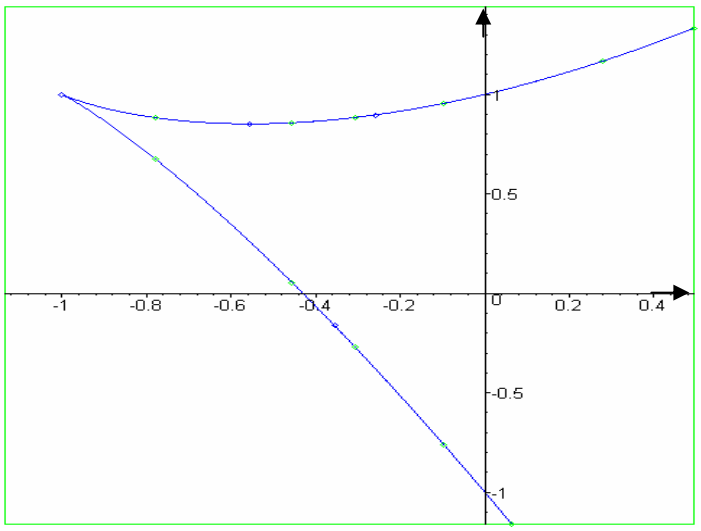


Figure 4 (Courbe tracée avec le logiciel Maple)

Exemple 3 : Courbe Elliptique qui coupe l'axe Ox en trois points simples.
Soit la cubique E_3 d'équation de Weierstrass :

$$E_3 : y^2 + xy - 5y = x^3 + 5x^2 + 2x - 8 . \quad (1)$$

Nous obtenons avec le calcul les invariants de E_3 :

$$b_2 = 21, \quad b_4 = -1, \quad b_6 = -7, \quad b_8 = -37, \quad \Delta(E_3) = 16325 > 0. \quad (2)$$

$\Delta(E_3) > 0$ implique que la cubique E_3 est une Courbe Elliptique qui coupe l'axe Ox en trois points simples.
Avec le logiciel Maple j'obtiens les abscisses x_1, x_2 et x_3 de ces points :

$$x_1 = -4, \quad x_2 = -2, \quad x_3 = 1. \quad (3)$$

Tableau de coordonnées de quelques points de E_3.

x	-5	-4	-3	-2	0	1	3	6
y	$5 \pm \sqrt{7}$	0 et 9	$4 \pm 2\sqrt{5}$	0 et 7	Pas de racines réelles	0 et 4	$1 \pm \sqrt{71}$	$-\frac{1}{2} \pm \frac{\sqrt{1601}}{2}$

La Courbe Elliptique E_3 coupe l'axe Ox en trois points simples :

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

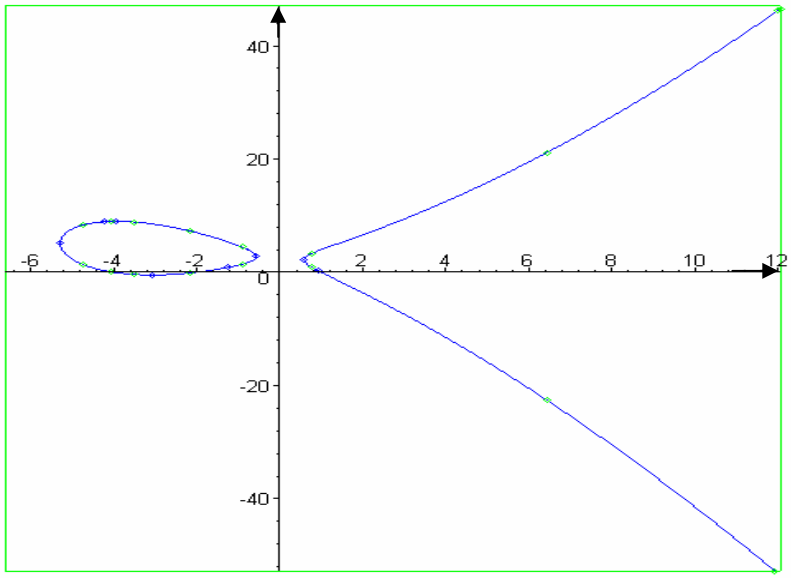


Figure 5 (Courbe tracée avec le logiciel Maple)

Exemple 4 : Courbe Elliptique qui coupe l'axe Ox en un seul point simple.
Soit la cubique E_4 d'équation de Weierstrass :

$$E_4 : y^2 + 6y = x^3 + 4x^2 + 3x + 12 . \quad (1)$$

Nous obtenons par le calcul les invariants de E_4 :

$$b_2 = 16 , \quad b_4 = 6 , \quad b_6 = 84 , \quad b_8 = 327 , \quad \Delta(E_4) = -203376 < 0. \quad (2)$$

Donc la cubique E_4 est une Courbe Elliptique qui coupe l'axe Ox en un seul point, simple.
Avec le logiciel Maple j'obtiens l'abscisse x_4 de ce point :

$$x_4 = -4 . \quad (3)$$

Tableau de coordonnées de quelques points de E_4.

x	-5	-4	-3	-2	0	2	5	8
y	Pas de racines réelles	0 et -6	$-3 \pm \sqrt{21}$	$-3 \pm \sqrt{23}$	$-3 \pm \sqrt{21}$	$-3 \pm \sqrt{51}$	$-3 \pm 3\sqrt{29}$	$-3 \pm \sqrt{813}$

La Courbe Elliptique E_4 coupe l'axe Ox en un seul point $P = (-4,0)$

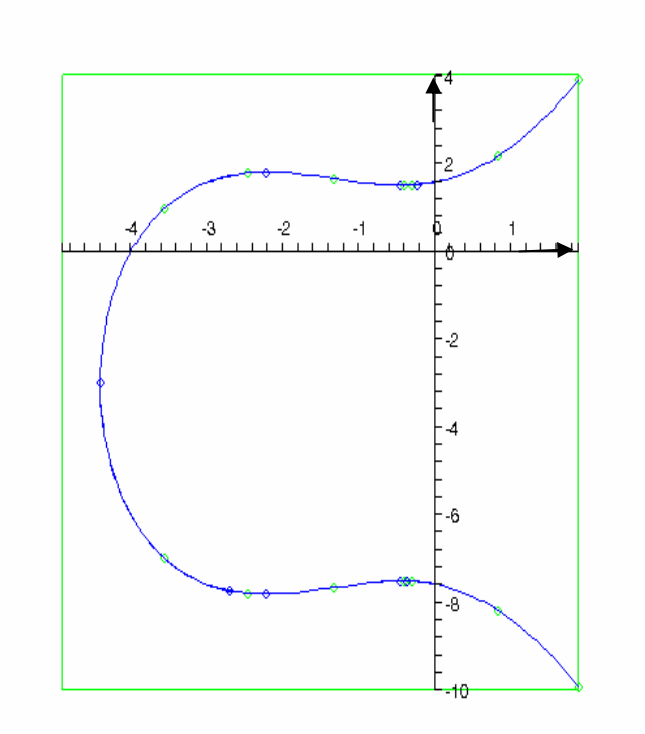


Figure 6 (Courbe tracée avec le logiciel Maple)

CHAPITRE II
GROUPES DE MORDELL-WEIL DES COURBES ELLIPTIQUES

1. Introduction :

D'après Lang [Elliptic curves Diophantine Analysis], Poincaré a conjecturé que l'ensemble $E(K)$ des points K-rationnels d'une Courbe Elliptique E est un groupe abélien de type fini.

En 1922 Mordell a prouvé cette conjecture [On the rational solutions of the indeterminate equations of the third and fourth degrees] Proc. Camb. Philos. Soc 21 (1922) 179-192; Weil a étendu ce résultat aux Variétés Abéliennes [Sur un théorème de Mordell-Weil, Bull-Sci.Math-54(1930) p 182-191].

L'élément neutre d'une Courbe Elliptique E, d'équation de Weierstrass :

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

est le point à l'infini. Ce point est ordinaire.

Proposition 1 :

Le point à l'infini $O_E = (0,1,0)$ *est un point non singulier sur les Courbes Elliptiques* E.

Preuve :

Considérons l'équation projective de E dans le plan $IP^2(K)$:

$$f(x, y, z) = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3 \in K[x, y, z] \quad (1)$$

Au point O_E, la fonction polynôme f prend la valeur :

$$f(O_E) = f(0,1,0) = 0 \ ; \quad (2)$$

il en résulte que le point à l'infini O_E est sur la courbe E.

Pour savoir si ce point est simple ou multiple nous prenons la dérivée partielle :

$$f_z^{'} = y^2 + a_1xy + 2a_3yz - a_2x^2 - 2a_4xz - 3a_6z^2 \quad (3)$$

Cette dérivée prend la valeur $f'(0,1,0) = 1$.

Il en résulte que le point O_E n'est pas singulier.

□

Une loi de groupe sur une Courbe Elliptique peut être déterminée par la théorie des Diviseurs sur une Variété Abélienne.

Cette loi peut être aussi déterminée par «une propriété géométrique de trois points colinéaires d'une Courbe Elliptique».

C'est cette loi que nous choisissons d'exposer.

2. Structure de groupe abélien sur l'ensemble E (K) des points K-rationnels d'une Courbe Elliptique E :

Soit une Courbe Elliptique E d'équation de Weierstrass :

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

Pour obtenir une structure de groupe abélien, nous considérons :

1) L'ensemble $E(K)$ des points K-rationnels de la Courbe Elliptique E.

2) Le point à l'infini O_E qui joue le rôle d'élément neutre ;

$O_E = (\infty, \infty)$ dans le plan affine, et $(0,1,0)$ dans le plan projectif $IP^2(K)$.

Ce point est unique. Il est déterminé par la direction de l'axe Oy dans le plan IR^2.

3) Une loi de composition interne :

$$u : E(K) \times E(K) \to E(K)$$

de valeur :

$$u(P_1, P_2) = P_1 + P_2 \qquad (1-1)$$

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

$$P_1 + P_2 + P_3 = O_E \qquad (1-2)$$

Cette construction du point $P_1 + P_2$ est représentée dans la figure 1 :

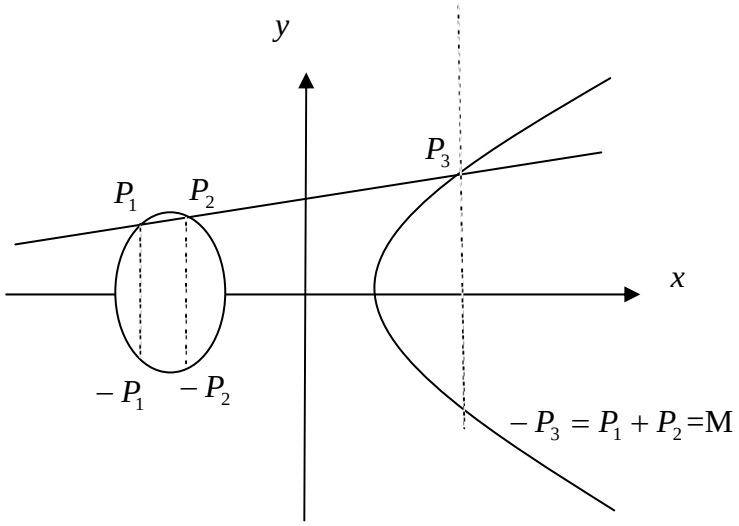


Figure 1

Vérifions les 4 axiomes d'un groupe abélien :

Axiome de l'élément neutre O_E :

C'est le point O_E à l'infini qui joue le rôle d'élément neutre ; il est déterminé par la direction de l'axe Oy.

Pour tout point P de $E(K)$, la sécante PO_E est parallèle à l'axe Oy.

La règle des 3 points colinéaires implique :

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

Donc : $P + O_E = O_E + P = P$

Axiome du symétrique :

Soit un point P sur le groupe $E(K)$;

la parallèle à l'axe Oy passant par le point P coupe la courbe E en trois points P, S, O_E ; il en résulte la relation :

$$P + S + O_E = O_E$$

Nous en déduisons le symétrique :

$$S = -P\ .$$

Cette construction du symétrique d'un point P de la courbe E est représentée dans la figure 2 :

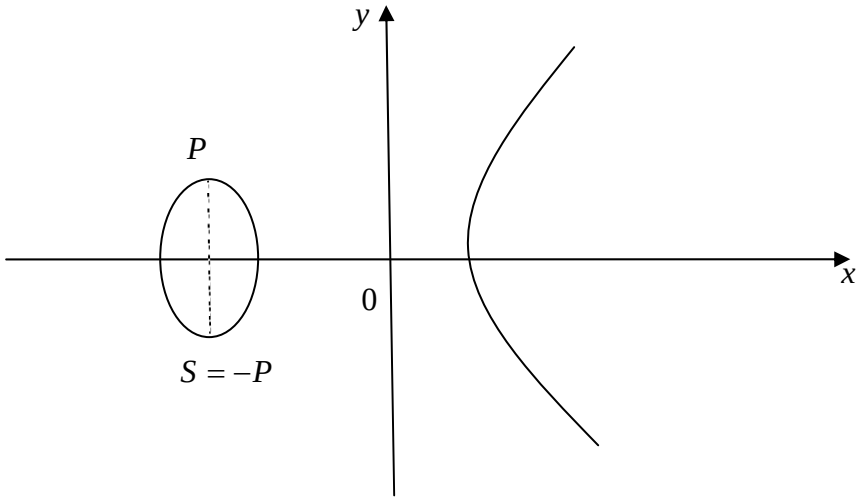


Figure 2

Axiome de commutativité :

Les sécantes P_1P_2 et P_2P_1 sont confondues ; il en résulte la relation :

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

cela implique la relation :

$$P_1 + P_2 = P_2 + P_1 = -P_3\ .$$

Axiome d'associativité :

Soient 3 points P, Q, R colinéaires de la Courbe Elliptique E **.**

Pour vérifier l'associativité de la loi, il faut comparer les points :

$$(P + Q) + R \quad \text{et} \quad P + (Q + R)$$

Il faut donc calculer les coordonnées des sommes :

$$P + Q = A\ ,\ \ A + R = B\ ,\ \ Q + R = C \ \text{ et } \ P + C = D$$

Avec le calcul nous obtenons l'égalité $B = D$ et l'associativité de la loi :

$$(P + Q) + R = P + (Q + R)$$

Nous avons démontré la :

Proposition 2 :

Soit une Courbe Elliptique E d'équation de Weierstrass :

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

Alors l'application $u : E(K) \times E(K) \to E(K)$

de valeur $u(P_1, P_2) = P_1 + P_2$ *, est une loi de groupe abélien d'élément neutre le point à l'infini* O_E *avec la règle géométrique de" 3 points colinéaires de la courbe* E *" :*

$$P_1 + P_2 + P_3 = O_E$$

□

Définition 1 : *le groupe* $E(K)$ *des points K -rationnels d'une Courbe Elliptique E est le groupe de Mordell-Weil de la Courbe Elliptique* E *.*

3. Formules du symétrique $-P$ **, de la somme** $P_1 + P_2$ **et de la somme** $P + P = 2P$ **dans le groupe** $E(K)$ **:**

3-1. Calcul des coordonnées du symétrique $-P$ **d'un point** P **de la courbe** E **, (figure 2) :**

Soit un point $P = (x_p, y_p)$ sur une Courbe Elliptique E .

Son symétrique est l'intersection P' de la courbe E par la parallèle à Oy passant par P .

Equation de la parallèle : $x = x_p$. (1)

Cette parallèle coupe la courbe E en deux points de même abscisse $x = x_p$, et d'ordonnées y_p et $y_{p'}$ racines de l'équation du $2^{ème}$ degré en y :

$$y^2 + y(a_1x_p + a_3) = x_p^3 + a_2x_p^2 + a_4x_p + a_6 \quad (2)$$

La somme des deux racines est une fonction symétrique de ces racines :

$$y_p + y_{-p} = -(a_1x_p + a_3) \quad (3)$$

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

Pour $P = (x_p, y_p)$, alors $-P = (x_p, -y_p - a_1x_p - a_3)$ (4)

3-2. Calcul de la somme $P_1 + P_2$ **de deux points** $P_i = (x_i, y_i)$ **,** $P_1 \neq \pm P_2$ **(figure 1) :**

La sécante P_1P_2 coupe la courbe E en un $3^{ième}$ point P_3 .

La règle géométrique de trois points colinéaires implique la relation :

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

Il en résulte la somme T de deux points :

$$T = P_1 + P_2 = -P_3 \quad (2)$$

Donc le point $P_1 + P_2 = T$ est l'intersection de la parallèle à Oy passant par P_3 avec la courbe.

L'équation de la sécante P_1P_2 est égale à :

$$y - y_1 = t(x - x_1) \ , \ t = (y_1 - y_2)/(x_1 - x_2), x_1 \neq x_2 \qquad (3)$$

Les abscisses des trois points P_1, P_2, P_3 sont solutions de l'équation cubique en x :

$$[y_1 + t(x - x_1)]^2 + (a_1x + a_3)[t(x - x_1) + y_1] = x^3 + a_2x^2 + a_4x + a_6 \qquad (4)$$

La fonction symétrique somme des racines vaut :

$$x_1 + x_2 + x_3 = t^2 + a_1t - a_2 \qquad (5)$$

Cela implique l'abscisse x_3 du point P_3 :

$$x_3 = t^2 + a_1t - a_2 - x_1 - x_2 \qquad (6)$$

Les formules (3) et (6) impliquent l'ordonnée y_3 du point P_3 :

$$y_3 = t(x_3 - x_1) + y_1 \qquad (7)$$

Avec le calcul nous obtenons les coordonnées du symétrique $-P_3 = P_1 + P_2$:

$$P_1 + P_2 = T = \begin{cases} x_T = t^2 + a_1t - a_2 - x_1 - x_2 \\ y_T = -t^3 - 2a_1t^2 + t(a_2 + 2x_1 + x_2 - a_1^2) + a_1a_2 - a_3 - y_1 + a_1(x_1 + x_2) \end{cases} \qquad (8)$$

$$t = (y_1 - y_2)/(x_1 - x_2), \ x_1 \neq x_2 .$$

Rassemblons les résultats précédents dans la :

Proposition 3 :

Soit une Courbe Elliptique E d'équation de Weierstrass :

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

1) Le symétrique d'un point $P = (x_p, y_p)$ de E est le point $-P = (x_p, -y_p - a_1x_p - a_3)$.

2) La somme $P_1 + P_2 = T$ de deux points $P_1 \neq \pm P_2$ de la courbe E , est le point T de coordonnées :

$$P_1 + P_2 = T = \begin{cases} x_T = t^2 + a_1t - a_2 - x_1 - x_2 \quad \text{et} \quad t = \dfrac{y_1 - y_2}{x_1 - x_2} \ , \ x_1 \neq x_2 \\ y_T = -t^3 - 2a_1t^2 + t(a_2 + 2x_1 + x_2 - a_1^2) + a_1a_2 - a_3 - y_1 + a_1(x_1 + x_2) \end{cases}$$

□

D'après la théorie des groupes abéliens, le groupe abélien de Mordell-Weil $E(K)$ possède des sous groupes abéliens et des sous groupes cycliques. Ces sous groupes cycliques sont engendrés par un point P du groupe de Mordell-Weil d'ordre fini.

$\{P, 2P = O_E\}$, $\{T, 2T, 3T = O_E\}$, etc…

3-3. Coordonnées du point $P+P=2P$ de la courbe E (Figure 3) :

Soit un point $P=(x_p,y_p)$ de la Courbe Elliptique .
La tangente à la Courbe Elliptique E au point P a pour équation :

$$y=y_P^{'}(x-x_p)+y_p\,,$$

où $y_P^{'}$ est la pente de la tangente à la Courbe Elliptique E au point $P=(x_p,y_p)$:

$$y_p^{'}=\frac{3x_p{}^2+2a_2x_p+a_4-a_1y_p}{2y_p+a_1x_p+a_3}$$

Cette tangente coupe la courbe E en un point double $P=(x_p,y_p)$et un point simple $M=(x_M,y_M)$.
La règle de trois points colinéaires implique la relation :

$$2P+M=O_E \text{ et } 2P=-M \qquad (1)$$

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

$$\left[y_p+y_p'(x-x_p)\right]^2+a_1x\left[y_p'(x-x_p)+y_p\right]=x^3+a_2x^2+a_4x+a_6 \qquad (2)$$

La fonction symétrique élémentaire somme des racines de l'équation (2) implique la relation :

$$2x_p+x_M=y_p'{}^2+a_1y_p'-a_2 \qquad (3)$$

La relation (3) implique l'abscisse du point M :

$$x_M=y_p'{}^2+a_1y_p'-a_2-2x_p \qquad (4)$$

$(1),(4)$ et la formule du symétrique d'un point impliquent les coordonnées du point $2P$:

$$\begin{cases} x_{2p}=y_p'{}^2+a_1y_p'-a_2-2x_p \quad \text{et} \quad y_P^{'}=\dfrac{3x_P^2+2a_2x_P+a_4-a_1y_p}{2y_P+a_1x_P+a_3} \\ y_{2p}=-y_p'{}^3-2a_1y_p'{}^2+y_p'(a_2-a_1^2+3x_p)+a_1a_2-a_3+2a_1x_p-y_p \end{cases}$$

Nous avons obtenu la :

Proposition 4 :

Soit une Courbe Elliptique E d'équation de Weierstrass :

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

Soit un point $P=(x_p,y_p)$ de E.

Alors les coordonnées du point $P+P=2P=(x_{2p},y_{2p})$ sont égales à :

$$\begin{cases} x_{2p}=y_p'{}^2+a_1y_p'-a_2-2x_p \quad \text{et} \quad y_P^{'}=\dfrac{3x_P^2+2a_2x_P+a_4-a_1y_P}{2y_P+a_1x_P+a_3} \\ y_{2p}=-y_p'{}^3-2a_1y_p'{}^2+y_p'(a_2-a_1^2+3x_p)+a_1a_2-a_3+2a_1x_p-y_p \end{cases}$$

□

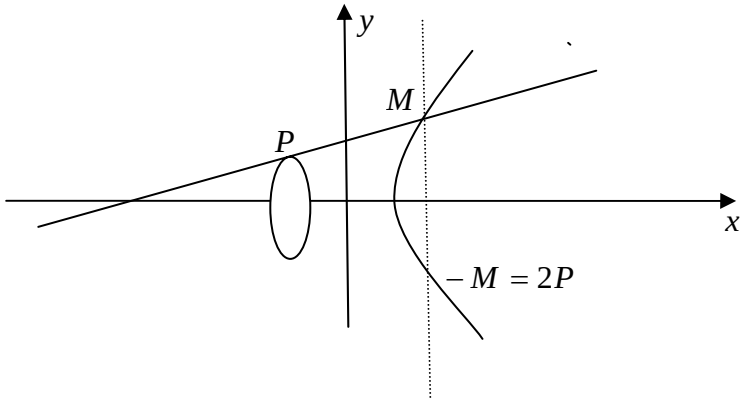


Figure 3

Exemple 1 : (Figure 4)
Soit la Courbe Elliptique E d'équation de Weierstrass :

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

Le groupe de Mordell-Weil $E(\mathbb{Q})$ contient les deux points $M = (-2,-3)$ et $R = (-1,-2)$.
Calcul des coordonnées des points $M + R$, $-M$, $-R$, $2M$, $2R$:
Nous obtenons les résultats :

$$M + R = (1,0),\ -M = (-2,0),\ -R = (-1,0),\ 2M = (2,4),\ 2R = (2,-3).$$

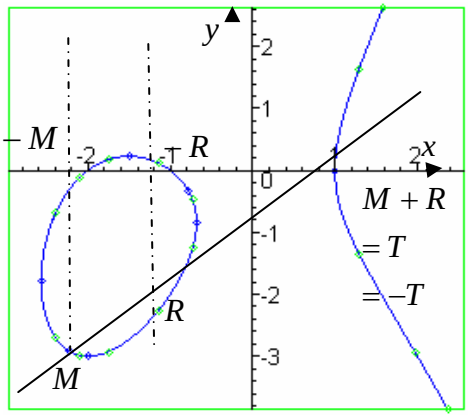


Figure 4

Avec les propositions 3 et 4, nous pouvons calculer les coordonnées de tout point mP, $m > 2$.
Ainsi $3P = 2P + P$, $4P = 2(2P)$, $5P = 4P + P$, etc…

Les coordonnées de ces points sont des fractions rationnelles du corps $K(x, y, a_1, ..., a_6)$.

Il existe des formules de récurrence que l'on trouve dans l'article de « Cassels » [Diophantine Equations with special references to elliptic curves] et dans [S.Lang, Elliptic curves. Diophantine analysis].

4. Formules de Cassels des coordonnées des points mP , $m>2$:
Cassels a obtenu les formules des coordonnées de points mP en prenant une Courbe Elliptique d'équation de Weierstrass :

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

Soit un point P du groupe $E(\mathbb{Q})$ de Mordell-Weil de E.
Posons :

$$mP = \begin{cases} P + P + \Lambda\ \Lambda\ + P\ ; & m \text{ fois } P & \text{si } m \phi\ 0 \\ (-P) + (-P) + \Lambda\ \Lambda\ + (-P); & (-\text{m}) \text{ fois } (-P) & \text{si } m\ \pi\ 0 \\ O_E & & \text{si } m = 0. \end{cases} \quad (1)$$

Selon Cassels les points mP ont pour coordonnées :

$$x(mP) = \frac{\phi_m(P)}{\psi_m^2(P)} \qquad \text{et} \qquad y(mP) = \frac{\omega_m(P)}{\psi_m^3(P)} \quad (2)$$

Les polynômes ψ_m sont égaux à :

$$\begin{aligned} &\psi_{-1} = -1\ ,\ \psi_0 = 0 \\ &\psi_1 = 1\ ,\ \psi_2 = 2y \\ &\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2 \\ &\psi_4 = 4y\left(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2\right) \end{aligned} \quad (3)$$

Les polynômes ψ_m, sont déterminés par des relations de récurrence :

$$\begin{aligned} &\psi_{2m+1} = \psi_{m+2}\psi_m^{\ 3} - \psi_{m-1}\psi_{m+1}^{\ 3} && ; \quad m \geq 2 \\ &2y\psi_{2m} = \psi_m\left(\psi_{m+2}\psi_{m-1}^{\ 2} - \psi_{m-2}\psi_{m+1}^{\ 2}\right) && ; \quad m \geq 3 \end{aligned} \quad (4)$$

Les polynômes ϕ_m et ω_m sont déterminés par les formules :

$$\begin{aligned} &\phi_m = x\psi_m^{\ 2} - \psi_{m+1}\psi_{m-1} && ; \quad m \geq 2 \\ &4y\omega_m = \psi_{m+2}\psi_{m-1}^{\ 2} - \psi_{m-2}\psi_{m+1}^{\ 2} && ; \quad m\ \phi\ 2 \end{aligned} \quad (5)$$

Proposition 5 :

Soit un point $P=(x,y)$ *du groupe de Mordell-Weil* $E(Q)$ *d'une Courbe Elliptique E d'équation de Weierstrass :*

$y^2 = x^3 + Ax + B \in Q[x,y]$ avec $4A^3 + 27B^2 \neq 0$ *et* A , $B \in IZ$

Alors un point $mP=(x_m, y_m)$ *a des coordonnées égales à :*

$$x(mP) = \frac{\phi_m(P)}{\psi_m(P)^2} \quad , \quad y(mP) = \frac{\omega_m(P)}{\psi_m(P)^3}$$

Les numérateurs et les dénominateurs ϕ_m , ψ_m et ω_m *sont des polynômes de l'anneau* $IZ[A,B,x,y]$.

Les polynômes ψ_m , ϕ_m et ω_m *satisfont les relations :*

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

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

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

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

$$\phi_m = x\psi_m{}^2 - \psi_{m+1}\psi_{m-1} \quad ; \quad (\mathrm{m} \geq 2)$$
$$4y\omega_m = \psi_{m+2}\psi_{m-1}{}^2 - \psi_{m-2}\psi_{m+1}{}^2 \quad ; \quad (m \phi\ 2)$$

Preuve :

C'est le lemme 7-2 dans «Diophantine Equations with special references to elliptic curves» de Cassels.

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

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

Les formules se démontrent par récurrence sur l'entier naturel m .

□

En appliquant ces formules pour $m = 2$, nous obtenons les polynômes :

$$\begin{cases} \psi_2 = 2y \\ \phi_2 = x^4 - 2Ax^2 - 8Bx + A^2 \\ \omega_2 = x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2 \end{cases} \quad (6)$$

Les coordonnées du point $2P$ sont donc égales à

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

Pour $m = 3$, nous obtenons les polynômes :

$$\phi_3 = x^9 - 12Ax^7 - 96Bx^6 + 30A^2x^5 - 24ABx^4 + 12(3A^3 + 4B^2)x^3 + 48A^2Bx^2 + 3A(3A^3 + 32B^2)x + 8B(A^3 + 8B^2) \quad (8)$$

C'est un polynôme de l'anneau $IZ[x, A, B]$ de degré 9 en x,

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

donc $\dfrac{\omega_3}{y}$ est un polynôme de l'anneau $IZ[x, A, B]$ de degré 12 en x.

Avec le calcul, nous obtenons le carré du polynôme ψ_3 :

$$\psi_3{}^2 = 9x^8 + 36Ax^6 + 72Bx^5 + 30A^2x^4 + 144ABx^3 + 12(12B^2 - A^3)x^2 - 24A^2Bx + A^4 \quad (10)$$

$\psi_3{}^2$ est un polynôme de l'anneau $IZ[x, A, B]$ de degré 8 en x. Nous en déduisons le polynôme :

$$\psi_3{}^3 = 27x^{12} + 162Ax^{10} + 324Bx^9 + 297A^2x^8 + 1296ABx^7 + 108(A^3 + 12B^2)x^6 + 1080A^2Bx^5 + 9A(288B^2 - 11A^3)x^4 + 432B(4B^2 - A^3)x^3 + 18A^2(A^3 + 24B^2)x^2 - 12A^4Bx - A^6; \quad (11)$$

$\psi_3{}^3$ est un polynôme de l'anneau $IZ[x, A, B]$ de degré 12 en x.

Les formules (2), (8), (9), (10) et (11) impliquent les coordonnées du point $3P$:

$$x_{3P} = \frac{\phi_3}{\psi_3^{\,2}} \quad , \quad y_{3P} = \frac{\omega_3}{\psi_3^{\,3}} \qquad (12)$$

5. Sous groupes de m-torsion, groupe de torsion d'une Courbe Elliptique :

Le groupe $E(K)$ de Mordell-Weil d'une Courbe Elliptique E, qui est abélien, admet des sous groupes cycliques et des sous groupes abéliens.

Définition 2 : *1) Le sous groupe de m-torsion d'une Courbe Elliptique E , pour tout entier m>1, est l'ensemble des points $P \in E(K)$ d'ordre m :*

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

Ces sous groupes sont cycliques ou abéliens d'ordre m.

2) Le groupe de torsion de la Courbe Elliptique, est l'ensemble des points P d'ordre fini ; c'est la réunion infinie des sous groupes de m-torsion de E :

$T(E) = \{P \in E(K);\ mP = O_E\ ,\ m \in IZ\ \} = \bigcup_m E(K)[m]$.

Ce groupe de torsion $T(E)$ est cyclique ou abélien, selon les invariants de la Courbe Elliptique. La détermination du groupe de torsion $T(E)$ a été réalisée pour les Courbes Elliptiques sur le corps $\mathbb{Q}$ des nombres rationnels. La structure de ce groupe a été conjecturée par Ogg.

Cette conjecture a été démontré par Mazur $[13-2]$.

Proposition 6 :

Le groupe de torsion d'une Courbe Elliptique E , sur le corps $\mathbb{Q}$, est isomorphe à l'un des 15 groupes additifs abéliens finis :

1) IZ/mIZ pour $m = 1, 2, 3, \ldots\ldots, 10$ et $m = 12$

2) $IZ/2IZ \oplus IZ/2dIZ$ pour $d = 1, 2, 3, 4$

Preuve : Mazur a obtenu la preuve en utilisant les travaux de Ogg sur les équations diophantiennes, les propriétés des points rationnels sur les courbes modulaires et les travaux de Kubert sur les bornes de torsion de Courbes Elliptiques.

□

Citons quelques résultats publiés sur les groupes $T(E)(K)$.

(1) Kenku a montré qu'il n'y a pas de Courbe Elliptique E, sur un corps quadratique, qui contient un point d'ordre 32 ; il a utilisé les courbes modulaires $X_1(16)$ et $X_1(32)$.

" Certain torsion points on Elliptic Curves defined over quadratic Fields "; J. Lond. Math. 19 (1979)-233- 240.

(2) Kamienny a montré qu'il n'y a pas de Courbe Elliptique, sur un corps quadratique, qui contient un point d'ordre premier $p = 17, 19, 23, 29, 31$; il a utilisé des courbes modulaires $X_1(p)$.
" Torsion points on Elliptic curves over all quadratic Fields "; Duke Math. J-53 (1986)-157- 162.

(3) Fung, Stroker, Williams et Zimmer ont montré que le groupe de torsion $T(E)(K)$ est isomorphe à l'un des 8 groupes abéliens finis : IZ/nIZ pour $n = 2, 3, 4, 5, 12$.
$IZ/2IZ \oplus IZ/dIZ$ pour $d = 2, 3, 6$.
K est un corps cubique pur $K = Q(\sqrt[3]{a})$ et a non puissance $3^{ème}$ dans le corps K.
Ils ont utilisé les formes normales de Kubert $E(b,c)$, les propriétés de l'invariant modulaire $j(E)$ et des valuations p-adiques v_p.
" Torsion Groups of Elliptic Curves with integral $j-$invariant over pure Cubic Fields "; Journal N. T. 36 (1990)-12- 45.

(4) Kishi a montré que le groupe de torsion $T(E)(K)$ est isomorphe à l'un des groupes abéliens finis :
$IZ/11IZ$; $IZ/13IZ$; $IZ/6IZ \oplus IZ/5IZ$; $IZ/8IZ \oplus IZ/7IZ$; $IZ/3IZ \oplus IZ/7IZ$;
$IZ/16IZ \oplus IZ/5IZ$; $IZ/64IZ \oplus IZ/9IZ$; $IZ/2IZ \oplus IZ/32IZ \oplus IZ/9IZ$.

K est un corps quartique cyclique imaginaire.
Il a utilisé la forme normale de Kubert $E(b,c)$, des valuations additives normalisées v_p et les réductions d'une Courbe Elliptique.
" On Torsion Subgroups of Elliptic Curves with Integral $j-$Invariant over Imaginary Cyclic quartic Fields "; Tokyo J. Math vol 20 (1997) 315-327.

Exemple 2 :

Considérons la Courbe Elliptique E d'équation de Weierstrass :

$$E : y^2 = x^3 + 1 \in Q[x, y] \qquad (1)$$

Calcul des invariants de E :
$b_2 = b_4 = 0$, $b_6 = 4$, $b_8 = 0$, $\Delta(E) = -27 \times 16$.

En utilisant les formules ψ_i, nous obtenons les coordonnées d'un point $2P$:

$$x_{2P} = \frac{x^4}{(2y)^2} \quad \text{et} \quad y_{2P} = \frac{x^6 + 20x^3 - 8}{(2y)^3} \qquad (2)$$

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

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

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

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

Les équations (1) et (4) impliquent trois solutions qui sont les abscisses de 3 points :

$P_1 = (-1,0)$ dans le plan IR^2, $P_2 = \left(\frac{1+\sqrt{-3}}{2},0\right)$ et $P_3 = \left(\frac{1-\sqrt{-3}}{2},0\right)$ d'abscisses complexes.

Ces trois points P_i, satisfont la relation $2P_i = O_E$; ce sont donc des points d'ordre 2 .
Le point $P_1 = (-1,0)$ est le seul point de 2-torsion du groupe abélien $E(Q)$.

Exemple 3 :

Certains points de 2-torsion d'une Courbe Elliptique E d'équation :

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

peuvent être obtenus avec la règle géométrique de 3 points colinéaires d'une cubique de Weierstrass.

Aux 3 points d'intersection $T_i = (e_i,0)$ avec l'axe Ox, 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 ($\mathbb{Q}$).

Exemple 4 :

Courbe Elliptique d'équation de Weierstrass :

$$E(n) : y^2 = x^3 - n^2 x \in Q[x,y]$$

Cette courbe $E(n)$ coupe l'axe Ox en 3 points :

$$P_1 = (0,0) \ ; \ P_2 = (n,0) \text{ et } P_3 = (-n,0)$$

Ces trois points engendrent un groupe abélien d'ordre 4.

$$\{P_1, P_2, P_1 + P_2, O_E\} \cong IZ/2IZ \times IZ/2IZ$$

Ces 3 points sont d'ordre 2 ; ce groupe est le groupe de torsion $T(E(n))$ de la Courbe Elliptique.
C'est un groupe de Klein : $\{a, b,\ ab = ba, a^2 = b^2 = (ab)^2 = e\}$.

Les coordonnées de points de torsion des Courbes Elliptiques $E(Q)$ peuvent être calculées avec la :

Proposition 7 :

Soit une Courbe Elliptique E d'équation de Weierstrass :

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

Soit un point $P \in E(Q)$ de torsion. Alors :

1) Les coordonnées x et y de P sont des entiers rationnels.

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

Preuve :

Elle a été obtenue par (Lut) et (Nag).

□

Exemple 5 :

Courbe Elliptique E d'équation de Weierstrass :

$$E: y^2 = x^3 - 3x + 10 \in \mathrm{Q[x, y]} \qquad (1)$$

Alors $4A^3 + 27B^2 = 3^4 \times 2^5$

Les valeurs possibles y^2 sont égales à :

$$y^2 = 4,\ 16,\ 9,\ 81,\ 36.$$

Pour $y^2 = 4$, on obtient l'équation diophantienne cubique $x^3 - 3x + 6 = 0$, pas de solutions rationnelles.

Pour $y^2 = 16$, on obtient l'équation diophantienne cubique $x^3 - 3x - 6 = 0$, pas de solutions rationnelles.

Pour $y^2 = 9$, on obtient l'équation diophantienne cubique $x^3 - 3x + 1 = 0$, pas de solutions rationnelles.

Pour $y^2 = 81$, on obtient l'équation diophantienne cubique $x^3 - 3x - 71 = 0$, pas de solutions rationnelles.

Pour $y^2 = 36$, on obtient l'équation diophantienne cubique $x^3 - 3x - 26 = 0$, pas de solutions rationnelles.

6. Théorème de Mordell-Weil d'une Courbe Elliptique :

Selon Lang, la preuve de ce théorème comporte 2 parties ; l'une est consacrée à l'ordre fini du groupe quotient $E(K)/mE(K)$, l'autre partie concerne le type fini du groupe abélien $E(K)$.

Proposition 8 : *(Théorème faible de Mordell-Weil)*

Soit le groupe de Mordell-Weil $E(K)$ d'une Courbe Elliptique E. Alors le groupe quotient $E(K)/mE(K)$ est fini pour un entier $m \geq 2$.

Preuve :

Selon Lang , il faut prendre une équation de Weierstrass :

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

Soit 3 homomorphismes de groupes :

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

tels que les noyaux satisfont :

$$\bigcap_{i=1,2,3} \ker\theta_i \subset 2\,E(K)\ ,\ \text{pour carac}(K)\neq 2,3\,.$$

Ces 3 homomorphismes θ_i sont choisis tels que :

$\theta_i(O_E)=1$, $\theta_i(x,y)=x-e_i$ si $x\neq e_i$ et $\theta_i(e_i,0)=(e_i-e_j)(e_i-e_k)$.

Alors en utilisant certaines propriétés des groupes abéliens, les auteurs obtiennent le résultat annoncé.

□

Pour le type fini du groupe $E(K)$ de Mordell-Weil, commençons par les fonctions hauteurs.

Définition 3 : (selon Silverman)

Une hauteur sur un groupe abélien A est une fonction h à valeurs réèlles :

$$h : A \to IR$$

qui satisfait les 3 axiomes :

(h_1) *à tout point* P_1 *de A correspond une constante* $c_1(P_1,A)=c_1$ *telle que :*

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

(h_2) *à une constante* c_2 *correspond un entier* $m\ge 2$ *tel que :*

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

(h_3) *l'ensemble des points P de A de hauteur* $h(P)$ *bornée est fini.*

$\{P\in A\,;\,h(P)\le c_3\}$ *est un ensemble fini.*

Les fonctions hauteurs sont déterminées par leur valeur aux points du groupe abélien A. Elles permettent de démontrer la finitude du groupe $A/2A$.

Proposition 9 :

Soit un groupe abélien A tel que le groupe quotient A/mA *soit fini. Alors le groupe abélien A est de type fini.*

Preuve :

Le groupe quotient A/mA étant fini, considérons des représentants des classes de A/mA :

$$T_1\ ,\ T_2\ ,.....,T_s \qquad (1)$$

Construisons une suite infinie de points de A avec des combinaisons linéaires :

$P=mP_1+T_{i1}$; $P_1=mP_2+T_{i2}\ ,.....,P_{n-1}=mP_n+T_{in}$. avec $ij=1,....,s$ $\qquad (2)$

Toute combinaison linéaire $P_{j-1}=mP_j+T_{ij}$ implique :

$$mP_j=P_{j-1}-T_{ij} \qquad (3)$$

Appliquons au 1^{er} membre de (3) l'axiome (h_2) et au $2^{ème}$ membre de (3) l'axiome (h_1).

Nous obtenons l'inégalité :

$$h(P_j)\le \frac{1}{m^2}\left(2\,h(P_{j-1})+c'\right)\ ; \qquad (4)$$

En appliquant cette procédure à chaque point $P, P_1,..., P_{n-1}$ et en ajoutant les inégalités obtenues membre à membre, nous obtenons l'inégalité :

$$h(P_n) \le \left(\frac{2}{m^2}\right)^n h(P) + \left(\frac{1}{m^2} + \frac{2}{m^4} + \frac{4}{m^6} + ... + \frac{2^{n-1}}{m^{2n}}\right) c' \ ; \qquad (5)$$

L'hypothèse $m \ge 2$ et le développement limité égal à la somme $\left(\frac{1}{m^2} + \frac{2}{m^4} + \Lambda + \frac{2^{n-1}}{m^{2n}}\right)$ impliquent l'inégalité :

$$h(P_n) \le 1 + \frac{c'}{2} \ ; \qquad (6)$$

Donc l'ensemble $\{P_n, n \to \infty\}$ est un ensemble de points de hauteur bornée.
Par l'axiome (h_3), cet ensemble est fini

$$\{P_1,..., P_r\} \ ; \qquad (7)$$

Il en résulte que tout point P du groupe abélien A est une IZ -combinaison linéaire de la forme :

$$P = n_1 T_1 + ... + n_s T_s + n_{s+1} P_1 + ... + n_{s+r} P_r \ , \ n_i \in IZ \ ; \qquad (8)$$

Donc le groupe abélien A, admettant un nombre fini de générateurs, est de type fini.
□

Cette proposition s'applique aux groupes de Mordell-Weil des Courbes Elliptiques.

Il existe plusieurs types de hauteurs. Indiquons quelques unes :

1- La hauteur logarithmique sur une Courbe Elliptique $E(Q)$ est la fonction :

$$h_{\log} : E(Q) \to IR$$

de valeur $h_{\log}(P) = \log\{\max(|a|, |b|)\}$, pour $x_P = a/b$ et $h_{\log}(O_E) = 0$.

Pour certains auteurs c'est aussi la hauteur de Weil.

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

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

de valeur $h_f(P) = h_{\log}(f(P))$

3- La hauteur canonique (ou de Néron-Tate) sur une Courbe Elliptique E est la fonction :

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

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

Cette hauteur canonique satisfait la :

Proposition 10 :

1) La hauteur canonique $\hat{h} : E(K) \to IR$ *satisfait la loi du parallélogramme :*

$\hat{h}(P+M) + \hat{h}(P - M) = 2\,\hat{h}(P) + 2\,\hat{h}(M)$ *pour tous points P et M de* $E(K)$.

2) Pour tout point $P \in E(K)$ *et tout entier* $m \in IZ$

$$\hat{h}(mP) = m^2 \hat{h}(P)$$

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

$$< , > : E(K) \times E(K) \to IR$$

de valeur $<M,P> = \hat{h}(P+M) - \hat{h}(P) - \hat{h}(M)$.

Cette forme < , > est bilinéaire.

4) $\hat{h}(P) \geq 0$ et $\hat{h}(P) = 0$ *si et seulement si le point P est d'ordre fini .*

Preuve :

On utilise la définition de $\hat{h}$ et les propriétés des formes quadratiques bilinéaires.
C'est un théorème de Néron-Tate.

□

Cette forme quadratique $\hat{h}$ de Néron-Tate, bilinéaire, permet d'introduire un invariant des Courbes Elliptiques.

Définition 4 : *Soit une Courbe Elliptique E et un système de générateurs* $P_1,....,P_r$ *de la partie infinie* $E(K)/T(E(K))$ *; le régulateur de E est le déterminant d'ordre r :*

$$R(E) = \det\left(< P_i, P_j >\right) , \quad 1 \leq i , j \leq r , \quad pour\ r \neq 0$$

et $R(E) = 1$ *pour r=0 , < , > = Forme quadratique de la proposition 10 .*

C'est le régulateur elliptique de la Courbe Elliptique E.

La proposition 9 s'applique au groupe abélien $E(K)$.

Proposition 11 :

Le groupe de Mordell-Weil $E(K)$ *d'une Courbe Elliptique E est de type fini.*

□

La structure de ce groupe de Mordell-Weil d'une Courbe Elliptique est précisée par le :

Corollaire 1 :

Le groupe de Mordell-Weil $E(K)$ *d'une Courbe Elliptique E est isomorphe au produit de groupes abéliens :*

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

où $T(E)$ *est le groupe de torsion de la Courbe Elliptique E , qui est fini.*

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

IZ^r *= r copies du groupe abélien additif infini IZ.*

□

Définition 5 : *L'entier naturel* $r = r(E) \geq 0$ *de cette formule d'isomorphisme est le rang de la Courbe Elliptique* E *. C'est aussi le nombre de générateurs* $P_1,...,P_r$ *de la partie infinie du groupe* $E(K)$.

Le rang d'une Courbe Elliptique ne peut être obtenu à l'aide d'une formule.

7. Morphismes de Courbes Elliptiques :

Une Courbe Elliptique a une structure de groupe abélien de type fini ; selon la théorie des groupes de courbes il existe des homomorphismes, des endomorphismes, des isomorphismes, des automorphismes et des isogénies de courbes elliptiques.

Définition 6 : *Soit deux Courbes Elliptiques* E *et* E' *, sur le même corps* K *, d'éléments neutres respectifs* O_E *et* $O_{E'}$ *. Un morphisme de Courbes Elliptiques est un homomorphisme de groupes abéliens* $f : E(K) \to E'(K)$.

7-1. Endomorphismes de courbes elliptiques :

La description de l'anneau des endomorphismes $End(\mathrm{E})$ d'une Courbe Elliptique a été indiquée par Deuring.
Selon Deuring, l'anneau des endomorphismes d'une Courbe Elliptique est isomorphe soit à l'anneau IZ , soit à un ordre d'un corps quadratique imaginaire, soit à un ordre de l'algèbre des quaternions.
Ce dernier cas se produit lorsque $\mathrm{carac}(K) = p \neq 0$.

L'ensemble des endomorphismes $End_K(E)$ d'une Courbe Elliptique forme un anneau intègre de caractéristique nulle, isomorphe à l'anneau IZ ou isomorphe à un anneau contenant IZ .

Définition 7 : *Les Courbes Elliptiques dont l'anneau des endomorphismes* $End_K(E)$ *contient l'anneau IZ sont des Courbes Elliptiques à Multiplication Complexe.*

Dans le cas où la Courbe Elliptique E est à Multiplication Complexe, l'anneau $End(E)$ est isomorphe à l'anneau des entiers d'un corps quadratique imaginaire

7-2. Isomorphismes de Courbes Elliptiques :

Définition 8 : *Un isomorphisme de 2 Courbes Elliptiques est un isomorphisme* $f : E(K) \to E'(K)$ *de leurs groupes de Mordell-Weil.*

Donc il satisfait les formules d'isomorphisme de groupes abéliens :

1) $f(O_E) = O_{E'}$
2) $f(P_1 + P_2) = f(P_1) + f(P_2)$
3) f est bijective

Examinons les propriétés de ces isomorphismes :

Soit deux Courbes Elliptiques E et E', d'équations deWeierstrass :
$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \in K[x, y]$ et
$E' : Y^2 + a_1'XY + a_3'Y = X^3 + a_2'X^2 + a_4'X + a_6' \in K[X, Y]$

Proposition 12 :
Un isomorphisme de 2 Courbes Elliptiques E *et* E' *est une application :*

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

de valeur $f(x, y) = (X, Y)$

pour $x = u^2X + r$, $y = u^3Y + su^2X + t$ *et* $u \neq 0,\ r,\ s,\ t \in K$. (1)

Preuve :
Les formules d'homomorphismes :
$f(P_1 + P_2) = f(P_1) + f(P_2)$ et $f(O_E) = O_{E'}$, se vérifient par le calcul.
Pour vérifier que f est bijective, nous calculons les valeurs de X et Y.
$X = (x - r)/u^2$ et $Y = (y - su^2X - t)/u^3$
L'hypothèse $u \neq 0$ implique la bijection.

□

La relation (1) et les calculs impliquent des relations entre les coefficients et les invariants des deux courbes que nous résumons dans le :

Corollaire 2 :

Soit 2 Courbes Elliptiques E et E' isomorphes. Alors :

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

$$\begin{aligned} &ua_1' = a_1 + 2s; \\ &u^2a_2' = a_2 - sa_1 + 3r - s^2; \\ &u^3a_3' = a_3 + ra_1 + 2t; \\ &u^4a_4' = a_4 - sa_3 - (t + rs)a_1 + 2ra_2 + 3r^2 - 2st; \\ &u^6a_6' = a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1. \end{aligned} \qquad (2)$$

Les invariants b_{2i} et b_{2i}' sont liés par les relations :

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

Les relations entre les invariants c_{2i} et c_{2i}' sont : $u^4c_4' = c_4$ *et* $u^6c_6' = c_6$ (4)

Les discriminants satisfont la relation :

$$u^{12}\Delta(E') = \Delta(E) \qquad (5)$$

Les invariants modulaires sont égaux :

$$j(E) = j(E') \qquad (6)$$

Les invariants différentiels satisfont la relation :

$$u^{-1}\omega(E') = \omega(E) \qquad (7)$$

Preuve :

En remplaçant x et y dans l'équation de E par les fonctions $x = u^2X + r$ et $y = u^3Y + su^2X + t$, nous obtenons toutes les relations du corollaire 2.

□

Les Courbes Elliptiques peuvent être classifiées par leurs invariants modulaires $j(E)$.

Proposition 13 :

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 d'invariant modulaire $t = j(E)$.

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

Soit deux Courbes Elliptiques E et E' isomorphes, la relation (6) du corollaire 2 implique l'égalité : $j(E) = j(E')$.

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

Soit deux Courbes Elliptiques d'équations de Weierstrass :

$$E : y^2 = x^3 + Ax + B \qquad \text{et} \qquad E' : y^2 = x^3 + A'x + B' ; \tag{1}$$

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

L'hypothèse : « $j(E) = j(E')$ » et les valeurs :

$j(E) = 1728(4A)^3 / \Delta(\mathrm{E}) = j(E') = 1728(4A')^3 / \Delta(E')$;

implique l'égalité :

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

Les relations d'isomorphismes de Courbes Elliptiques impliquent les relations :

$$u^4 A' = A \ , \quad u^6 B' = B \quad \text{et} \quad u^{12} \Delta(E') = \Delta(E) \tag{4}$$

Examinons les trois cas :

1^{er} cas : $A = 0$ et $B \neq 0$, les formules (2) et (4) des isomorphismes impliquent :

$A' = 0$ et $B' \neq 0$.

La formule (4) implique les six valeurs $u = (B/B')^{1/6}$ qui déterminent les six isomorphismes $f : E \to E'$ de valeurs : $f(x, y) = (u^2 x, u^3 y)$.

$2^{ème}$ cas : $B = 0$, $A \neq 0$, les formules (2) et (4) des isomorphismes impliquent :

$A' \neq 0$ et $B' = 0$.

La formule (4) implique les quatre valeurs : $u = (A/A')^{1/4}$ qui déterminent les quatre isomorphismes f des deux Courbes Elliptiques de valeurs : $f(x, y) = (u^2 x, u^3 y)$.

$3^{ème}$ cas : $AB \neq 0$, les formules (2) et (4) des isomorphismes impliquent :

$A' \neq 0$ et $B' \neq 0$.

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

Il en résulte les isomorphismes $f : E \to E'$ de valeur : $x = u^2 X$, $y = u^3 Y$.

Les équations de Courbes Elliptiques isomorphes sont :

$$E : y^2 = x^3 + A'u^4 x + B'u^6 \qquad \text{et} \qquad E' : y^2 = x^3 + A'x + B' \ ;$$

Preuve de « tout nombre t d'une clôture algébrique K^{alg} est l'invariant modulaire d'une Courbe Elliptique »

Soit un élément $t \in K^{alg}$.

Considérons la Courbe Elliptique E d'équation de Weierstrass :

$$E : y^2 = x^3 + Ax + B \qquad (1)$$

Son discriminant vaut :

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

Son invariant modulaire vaut :

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

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

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

Pour déterminer les valeurs de A et B, nous examinons les trois cas possibles : $t = 0, 1728$ et $t \neq 0, 1728$.

Lorsque $t = 0$, la formule (3) implique la valeur : $A = 0$ (5)

L'équation (1) devient :

$$E : y^2 = x^3 + B \qquad (6)$$

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

Cette Courbe Elliptique E est isomorphe à toute Courbe Elliptique $E' : y^2 = x^3 + u^6 B$ avec $u \in K^*$.

Lorsque $t = 1728$, la formule (3) implique la relation :

$$1728 = \frac{1728.4.A^3}{4A^3 + 27B^2} \qquad (7)$$

La relation (7) et la condition (2) impliquent :

$$B = 0 \quad ; \quad A \neq 0 \qquad (8)$$

La Courbe Elliptique E d'équation de Weierstrass :

$$E : y^2 = x^3 + Ax \qquad (9)$$

est isomorphe à toute Courbe Elliptique E' d'équation de Weierstrass :

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

Lorsque $t \neq 0, 1728$, la formule de l'invariant modulaire d'une Courbe Elliptique implique la relation :

$$27tB^2 = (1728 - t)A^3 . \qquad (10)$$

Cette équation admet les solutions :

$$A = \frac{3t}{1728 - t} \in K(t) \qquad \text{et} \qquad B = \frac{t}{1728 - t} \qquad (11)$$

Il en résulte la Courbe Elliptique d'équation de Weierstrass :

$$E : y^2 = x^3 + \frac{3t}{1728 - t}x + \frac{t}{1728 - t} \ , \quad j(E) = t \neq 0, 1728 .$$

□

Exemple 6 : Courbes Elliptiques isomorphes :
Soit une Courbe Elliptique E_1 d'équation de Weierstrass :

$$E_1 : y^2 + 2xy + y = x^3 + 3x^2 + 4x + 1 \in K[x, y], carac(K) \neq 2, 3..$$

Courbe Elliptique isomorphe E_2 pour les valeurs $u = 2$, $r = 1$, $s = 0$, $t = 0$:

$$E_2 : y^2 + xy + \frac{3}{8}y = x^3 + \frac{3}{2}x^2 + \frac{13}{16}x + \frac{9}{64}$$

Les formules d'isomorphismes liant les invariants b_{2i} et les discriminants impliquent :

$$b_2' = 7 , \quad b_4' = 2 , \quad b_6' = \frac{45}{64} , \quad b_8' = \frac{59}{256} , \quad \Delta(E_2) = \frac{-195}{4096} = 2^{-12}\Delta(E_1) .$$

Tableau de valeurs des coordonnées de quelques points de la Courbe E_1 :

x	-1	$-\frac{1}{4}$	0	$\frac{1}{6}$	2
y	Pas de racines réelles	$-\frac{1}{4} \pm \frac{\sqrt{15}}{8}$	$-\frac{1}{2} \pm \frac{\sqrt{5}}{2}$	$-\frac{2}{3} \pm \frac{5\sqrt{114}}{36}$	$-\frac{5}{2} \pm \frac{\sqrt{141}}{2}$

La Courbe Elliptique E_1 coupe l'axe Ox en un seul point d'abscisse x_1 obtenue avec le logiciel Maple : $x_1 \approx -0,31$. Elle coupe l'axe Oy en deux points d'ordonnées $-\frac{1}{2} + \frac{\sqrt{5}}{2}$ et $-\frac{1}{2} - \frac{\sqrt{5}}{2}$.

Tableau de valeurs des coordonnées de quelques points de la Courbe E_2 :

x	-1	$\frac{-1}{4}$	0	$\frac{1}{6}$	2
y	Pas de racines y réelles	$-\frac{1}{16} \pm \frac{\sqrt{5}}{16}$	$-\frac{3}{16} \pm \frac{3\sqrt{5}}{16}$	$-\frac{13}{48} \pm \frac{\sqrt{8205}}{144}$	$-\frac{19}{16} \pm \frac{\sqrt{4397}}{16}$

La Courbe Elliptique E_2 coupe l'axe Ox en un seul point d'abscisse x_2 obtenue avec le logiciel Maple : $x_2 \approx -0{,}33$. Elle coupe l'axe Oy en deux points d'ordonnées $-\frac{3}{16}+\frac{3\sqrt{5}}{16}$ et $-\frac{3}{16}-\frac{3\sqrt{5}}{16}$.

La Courbe Elliptique E_1 :

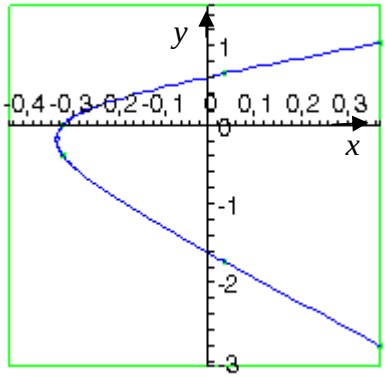


Figure 5

La Courbe Elliptique E_2 isomorphe à E_1 :

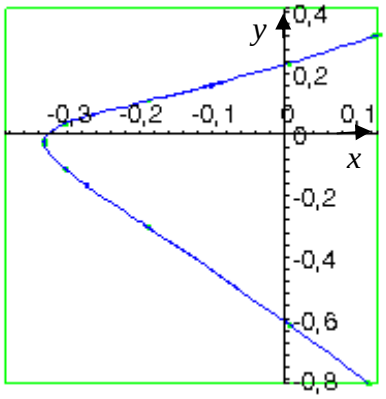


Figure 6

La relation $j(E) = j(E')$ implique une relation d'équivalence dans l'ensemble des Courbes Elliptiques.
Il en résulte que les Courbes Elliptiques se répartissent en classes d'équivalences de Courbes Elliptiques isomorphes :

$cl(E') = \{E', E'_1, E'_2, \text{K K K }, E'_n\}$, d'invariants modulaires égaux :

$$j(E') = j(E'_1) = j(E'_2) = \text{K K K } = j(E'_n).$$

7-3. Automorphismes d'une Courbe Elliptique :

Définition 9 : *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 14 :

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 $j(E) \neq 0$, 1728 et $carac(K) \neq 2$ et 3.
2) 4 si $j(E) = 1728$ et $carac(K) \neq 2$ et 3.
3) 6 si $j(E) = 0$ et $carac(K) \neq 2$ et 3.
4) 12 si $j(E) = 0 = 1728$ et $carac(K) = 3$.
5) 24 si $j(E) = 0 = 1728$ et $carac(K) = 2$.
Où $carac(K)$ est la caractéristique du corps K.

Preuve de 1) :

Soit une Courbe Elliptique E d'équation de Weierstrass :

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

sur un corps K de caractéristique $carac(K) \neq 2 \text{ et } 3$.

Les formules impliquent les deux invariants de la Courbe :

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

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

$$a_4 \neq 0 \quad \text{et} \quad a_6 \neq 0 \qquad (3)$$

Les formules d'isomorphismes (1) impliquent l'automorphisme :

$$g_u : E(K) \to E(K)$$
$$(x, y) \to \left(u^2 x, u^3 y\right);$$

pour un certain élément u non nul du corps K.

La Courbe Elliptique E' image de la Courbe Elliptique E par l'isomorphisme g_u est :

$$E' : y'^2 = x'^3 + a'_4 x' + a'_6;$$

avec les relations :

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

Les invariants modulaires des deux courbes E et E' sont égaux :

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

ce qui implique l'égalité :

$$\frac{a_4^3}{4a_4^3 + 27a_6^2} = \frac{a'^3_4}{4a'^3_4 + 27a'^2_6}.$$

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

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

Donc le groupe $Aut(E)$ est d'ordre deux .

Preuve de 2) :

Soit une Courbe Elliptique E d'équation de Weierstrass :

$$E : y^2 = x^3 + a_4 x + a_6 \in K[x, y]. \tag{1}$$

Les formules impliquent les valeurs des invariants de E :

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

Les hypothèses $carac(K) \neq 2, 3$ 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 (1) impliquent l'automorphisme :

$$g_u : E(K) \to E(K)$$
$$(x, y) \to (u^2 x, u^3 y);$$

pour un certain élément u non nul du corps K. La Courbe Elliptique E' image de la Courbe E par l'isomorphisme g_u a pour équation de Weierstrass :

$$E' : y^2 = x^3 + a'_4 x + a'_6 \ ;$$

avec les relations :

$$u^4 a'_4 = a_4 \text{ et } u^6 a'_6 = a_6 . \quad (4)$$

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

La formule (5) implique : $u^4 = 1$.

Il en résulte les quatre automorphismes : $(x, y) \to (x, y)$; $(x, y) \to (x, -y)$;
$(x, y) \to (-x, -iy)$; $(x, y) \to (-x, iy)$.

Preuve de 3) :

Soit une Courbe Elliptique E d'équation de Weierstrass :

$$E : y^2 = x^3 + a_4 x + a_6 . \quad (1)$$

Il en résulte les invariants :

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

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

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

Les formules d'isomorphismes(1)impliquent l'automorphisme :

$$g_u : E(K) \to E(K)$$
$$(x, y) \to (u^2 x, u^3 y);$$

pour un certain élément u non nul du corps K. La Courbe Elliptique E' image de la Courbe E par l'isomorphisme g_u a pour équation :

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

avec la relation :

$$u^6 a'_6 = a_6 . \quad (4)$$

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

Preuve de 4) :

C'est la valeur $j(E) = 0$ et la formule $j(E) = \frac{c_4^3}{\Delta(E)}$ qui justifient la forme convenable de l'équation de Weierstrass de la Courbe E :

$$E : y^2 = x^3 + a_4 x + a_6 .$$

Nous considérons l'automorphisme du groupe abélien $E(K)$de la forme :

$$g_u : E(K) \to E(K)$$
$$(\mathrm{x}, \mathrm{y}) \to (u^2 x + r, u^3 y);$$

Les relations entre a_i et a_i' impliquent les formules :

$$u^4 = a_4 / a_4' \qquad \text{et} \qquad r^3 + r a_4 + a_6 - u^6 a_6' = 0 .$$

Pour $E = E'$, l'automorphisme implique les valeurs $a_4' = a_4$ et $a_6' = a_6$.

Il en résulte le système :

$$\begin{cases} u^4 = 1; \\ r^3 + r a_4 + (1 - u^2) a_6 = 0 . \end{cases} \qquad (1)$$

Cela implique $4 \times 3 = 12$ paires (u, r) qui déterminent un groupe de douze automorphismes de la courbe E. Les quatre valeurs de u sont ± 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 :
$(x, y) \to (x + r_1, y)$; $(x, y) \to (x + r_2, y)$; $(x, y) \to (x + r_3, y)$; $(x, y) \to (x + r_1, -y)$;
$(x, y) \to (x + r_2, -y)$; $(x, y) \to (x + r_3, -y)$; $(x, y) \to (-x + r_1, -iy)$; $(x, y) \to (-x + r_2, -iy)$;
$(x, y) \to (-x + r_3, -iy)$; $(x, y) \to (-x + r_1, iy)$; $(x, y) \to (-x + r_2, iy)$; $(x, y) \to (-x + r_3, iy)$.
Ce groupe est le sous groupe alterné A_4 du groupe symétrique S_4. Ce sous groupe alterné est d'ordre 12.

Preuve de 5) :

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

$$E : y^2 + a_3 y = x^3 + a_4 x + a_6 \in IF_q[x, y] ; \quad q = 2^n \qquad (1)$$

ses invariants valent :

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

Les automorphismes du groupe $E(IF_q)$sont :

$$g_u : E(K) \to E(K)$$
$$(x, y) \to (u^2 x + s^2, u^3 y + s u^2 x + t); \qquad (2)$$

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) admettent 3 solutions u, 4 solutions s et 2 solutions t. Il en résulte que le groupe $Aut(E)$ est un groupe produit d'un groupe cyclique C_3 d'ordre 3 twisté par le
produit d'un groupe engendré par un élément s d'ordre 4 et un groupe engendré par un élément t d'ordre 2 qui forment le groupe des quaternions d'ordre 8.
Ce groupe $Aut(E)$ est donc d'ordre $3 \times 8 = 24$.
Il est isomorphe au groupe spécial linéaire $SL(2, IF_3)$.

□

La théorie des Courbes Elliptiques introduit des homomorphismes particuliers : les isogénies.

7-4. Isogénies de Courbes Elliptiques :
Signalons que le terme d'isogénie est utilisé pour les Variétés Abéliennes et pour les Tores Complexes.

Une Courbe Elliptique E, a une structure de groupe abélien de type fini.
Tout morphisme de Courbes Elliptiques :

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

satisfait les relations d'homomorphisme de groupes :

$$f : E_1(K) \to E_2(K)$$
$$\text{de valeur} \quad f(O_{E_1}) = O_{E_2} \text{ et } f(P_1 + P_2) = f(P_1) + f(P_2) ;$$

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

Il existe des morphismes surjectifs de noyaux finis ; ce sont des isogénies .

Définition 10 (selon Shimura) **:** *Une isogénie de deux Courbes Elliptiques E_1 et E_2, est un morphisme de Courbes Elliptiques :*

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

qui satisfait les relations :
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 $f(O_{E_1}) = O_{E_2}$.

Exemple 7 :
La multiplication par un entier m sur le groupe de Mordell-Weil $E(K)$ est une isogénie.

$t_m : E(K) \to E(K)$; de valeur $t_m(P) = mP$.

Le symbole mP signifie :

$mP = P + \text{K K K} + \text{P}$, m fois P si $m \phi\ 0$.

$mP = (-m)(-P)$, si $m \pi\ 0$.

$mP = O_E = (\infty, \infty)$, si $m = 0$.

Une isogénie possède des invariants : un degré et une isogénie duale ;

Définition 11 : *1) Le degré d'une isogénie $f : E_1(K) \to E_2(K)$ est égal à l'ordre de son noyau*

$$\deg f = card\left\{f^{-1}(O_{E_2})\right\}$$

2) l'isogénie duale de l'isogénie f de degré d est l'isogénie $\hat{f} : E_2(K) \to E_1(K)$ qui satisfait les relations de composition des applications :

$\hat{f} \circ f : E_1(K) \to E_2(K)$ *est la multiplication par d sur la courbe* E_1.

$f \circ \hat{f} : E_2(K) \to E_1(K)$ *est la multiplication par d sur la courbe* E_2.

La multiplication par un entier rationnel possède des propriétés liées à la caractéristique du corps de base de la Courbe Elliptique.

Proposition 15 :
Soit la multiplication $t_m : E(K) \to E(K)$ par un entier rationnel m . Alors :

1) Le degré de cette multiplication est égal à m^2 .

2) Si la caractéristique du corps K est nulle, alors le noyau de l'isogénie t_m est isomorphe au groupe abélien produit $IZ/mIZ \times IZ/mIZ$.

3) Si la caractéristique du corps K est un entier premier p , premier à m, alors le noyau de la multiplication par p^e est isomorphe au groupe trivial $\{O_E\}$ ou bien isomorphe au groupe abélien $IZ/p^e IZ$ pour e=1, 2, 3, ⌧

Preuve : Elle a été indiquée par Deuring [6].
□

Le noyau d'une isogénie et les sous groupes du groupe $E(K)$ sont liés par la :

Proposition 16 :
Soit une Courbe Elliptique E_1, et un sous groupe fini F du groupe de Mordell-Weil $E_1(K)$. Alors il existe une unique isogénie $f : E_1(K) \to E_2(K)$ de noyau $f^{-1}(O_{E_2}) = F$ pour $E_2(K)$.

Preuve : (Silverman [20-1])

□

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 en est de même pour les Courbes Elliptiques isogènes.
Les isogénies de Courbes Elliptiques sur le corps des nombres rationnels Q, qui sont de degré premier N sont en nombre fini d'après Mazur.

Proposition 17 :

L'ensemble $M(E)$ des multiplications par un entier rationnel sur une Courbe Elliptique E est un anneau isomorphe à l'anneau IZ.

Preuve :

Considérons l'application $f : IZ \to M(E)$, de valeur $f(n)$ = multiplication par l'entier n :

$$t_n : E(K) \to E(K),\ t_n(P) = nP \qquad (1)$$

Soient deux entiers rationnels $n, n' \in IZ$.
Calculons les valeurs $f(n+n')$, $f(0)$ et $f(nn')$ pour déterminer la structure de l'ensemble $M(E)$.
$f(n+n') = t_{n+n'}$ de valeur $t_{n+n'}(P) = (n+n')P = nP + n'P$.
Cela implique $f(n+n') = f(n) + f(n')$ (2)

$f(nn') = t_{nn'}$ de valeur $t_{nn'}(P) = (nn')P = n(n'P)$.
Cela implique la relation $f(nn') = f(n) \circ f(n')$ (3)
$f(0) = 0$, $0P = O_E$ = élément neutre du groupe $E(K)$. (4)
Les relations (2), (3) et (4) impliquent que f est un isomorphisme de l'anneau IZ sur l'ensemble $M(E)$.
Un isomorphisme conserve la structure algébrique ;
cela implique que l'ensemble :

$M(E)$ = { multiplication par IZ sur la Courbe Elliptique } est un anneau isomorphe à IZ.

□

CHAPITRE III
p-DESCENTES SUR LES COURBES ELLIPTIQUES

La notion de descente est utilisée en mathématiques pour des procédures de calculs qui comportent une " infinité " de calculs : descente de Fermat, descente sur un groupe abélien, descente sur un espace homogène, descentes sur des Courbes Elliptiques, descentes galoisiennes,…

La p-descente sur une Courbe Elliptique a pour but de déterminer la structure du groupe abélien E(K).

Le point de départ de cette "descente" est varié : valuations, groupe K(S,p), isogénies, espaces homogènes, cohomologie…

1. Descente infinie de Fermat : (1632)

Elle a été utilisée par Fermat dans des problèmes d'arithmétique : prenons un exemple : Démontrer que le nombre $\sqrt{7}$ n'est pas rationnel.

Faisons un raisonnement par l'absurde :

Dans la suite des carrés n^2, entre $2^2 = 4$ et $3^2 = 9$ il n'y a pas d'autre carré n^2 ; donc 7 n'est pas un carré n^2.

Supposons que $\sqrt{7}$ est un nombre rationnel.

Alors $\sqrt{7} = a/b$, a et b entiers rationnels premiers entre eux ; (1)

En élevant les deux membres de (1) au carré, nous obtenons l'égalité :

$$7b^2 = a^2; \qquad (2)$$

Par un théorème de Gauss appliqué à (2), 7 divise $7b^2$ et a^2 ; il en résulte :

$$a = 7a_1 \ ; \qquad (3)$$

(2) et (3) impliquent l'égalité :

$$b^2 = 7{a_1}^2 \ ; \qquad (4)$$

Par le théorème de Gauss appliqué à (4), 7 divise $7{a_1}^2$ et b^2 ; il en résulte l'égalité :

$$b = 7b_1 \ ; \qquad (5)$$

(4) et (5) impliquent l'égalité :

$$7{b_1}^2 = {a_1}^2 \ ; \qquad (6)$$

Par le théorème de Gauss appliqué à (6), 7 divise $7{b_1}^2$ et ${a_1}^2$; il en résulte l'égalité :

$$a_1 = 7a_2 \ ; \qquad (7)$$

En poursuivant cette procédure, nous obtenons 2 suites infinies d'entiers :

$$a \ \phi \ a_1 \ \phi \ a_2 \ \phi \ \mathrm{K} \ \phi \ a_n \ \phi \ \mathrm{K} \quad \text{et} \quad b \ \phi \ b_1 \ \phi \ b_2 \ \phi \ \mathrm{K} \ \phi \ b_n \ \phi \ \mathrm{K} \qquad (8)$$

Ces deux suites impliquent que les entiers a et b sont divisibles par 7, cela est en contradiction avec la supposition " a et b sont premiers entre eux ".
Donc le nombre $\sqrt{7}$ n'est pas rationnel. C'est un nombre irrationnel quadratique.

Cette descente infinie est utilisée avec les hauteurs sur les groupes abéliens A pour montrer que le groupe A est de type fini lorsque le groupe quotient $A/2A$ est fini.

Pour déterminer les points du groupe de Mordell-Weil $E(K)$ d'une Courbe Elliptique il y a d'autres descentes qui sont finies.

2. 2-Descente sur le groupe *E(K)* :

Cette descente est basée sur certaines valuations du corps K, et sur le groupe quotient $E(K)/2E(K)$.

Proposition 1 :

Soit une Courbe Elliptique E *d'équation de Weierstrass :*

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

Soit l' ensemble de valuations v *du corps K.*

$S = \{ v \text{ archimédiennes, } v \text{ divisant } 2, \text{ et } v \text{ pour lesquelles E a mauvaise réduction} \}.$

Soit le groupe $K(S;2) = \left\{ d \in K^* / K^{*2};\ ord_v(d) \equiv 0 \bmod 2 \ \text{ pour } v \notin S \right\}.$

Soit l'homomorphisme injectif :

$$f : E(K)/2E(K) \to K(S,2) \times K(S,2),$$

de valeur

$$f(x,y) = (x-e_1, x-e_2), \ si \ x \neq e_1, e_2,$$

$$f(x,y) = \left(\frac{e_1-e_3}{e_1-e_2}, e_1-e_2 \right), \ si \ x = e_1,$$

$$f(x,y) = \left(e_2-e_1, \frac{e_2-e_3}{e_2-e_1} \right), \ si \ x = e_2.$$

et $f(O_E) = (1,1)$.

Soit une paire $(d_1,d_2) \in K(S;2) \times K(S;2)$ *différente des images* $f(e_1,y)$, $f(e_2,y)$ *et* $f(O_E)$.

Alors $(d_1,d_2) = f(x,y)$ *si et seulement si* d_1, d_2 *est solution du système :*

$$\begin{cases} d_1 z_1^2 - d_2 z_2^2 = e_2 - e_1 \\ d_1 z_1^2 - d_1 d_2 z_3^2 = e_3 - e_1 \end{cases}$$

Preuve :

(Selon Silverman – Proposition 1-4 – X p 281).

On utilise plusieurs homomorphismes :

La forme bilinéaire de Kummer :

$$Kum : E(K) \times G(K_{a\lg}/K) \longrightarrow E[m]$$

de valeur $Kum(P,\sigma) = \sigma(R) - R$ et $mR = P$.

La forme bilinéaire de Weil :

$$e_m : E[m] \times E[m] \longrightarrow C(m) = \textit{groupe des racines d'ordre m de } 1.$$

L'isomorphisme de groupes :

$$\delta : K^*/K^{*m} \longrightarrow Hom(G(K_{a\lg}/K), C(m))$$

de valeur $\delta(d) = (\sigma) = \sigma(\beta)/\beta$ et $\beta^m = d$.

On obtient l'abscisse x pour $m = 2$.

$$x = e_1 + d_1 z_1^2 = e_2 + d_2 z_2^2 = e_3 + d_1 d_2 z_3^2.$$

□

Cette 2-descente a été utilisée par plusieurs chercheurs (Cremona, etc…).

Exemple : (Silverman)

Courbe Elliptique d'équation de Weierstrass :

$$E : y^2 = x(x-2)(x-10) \in Q[x,y]$$

Calcul du discriminant : $\Delta(E) = 409600 = 2^{14}5^2$.

Il en résulte que la courbe E a bonne réduction pour les valuations p-adiques v_p , $p \neq 2,5$.

L'ensemble de valuations est :

$$S = \{2,5,\infty\}.$$

Le groupe $Q(S,2) = \left\{ d \in Q^*/Q^{*2}; ord_v(d) \equiv 0 \bmod 2; v \notin S \right\}$.

La paire (d_1, d_2) de $Q(S,2)$ satisfait les 2 équations :

$$d_1 z_1^2 - d_2 z_2^2 = 2 \;\; ; \;\; d_1 z_1^2 - d_1 d_2 z_3^2 = 10.$$

Il existe une autre 2-descente particulière basée sur une isogénie de Courbe Elliptique de degré 2.

Proposition 2 :

Soit une Courbe Elliptique E d'équation de Weierstrass :

$$E : y^2 = x^3 + ax^2 + bx \in Q[x, y] \quad et \quad b^2(a^2 - 4b) \neq 0.$$

Soit la courbe isogène :

$$E' : Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X .$$

Par la 2-isogénie $f : E \longrightarrow E'$, $f(x,y) = (y^2/x^2, y(b - x^2)/x^2)$,

de noyau $E[f] = \{(0,0), O_E\}$ *d'ordre 2.*

Soit l'ensemble de valuations du corps Q :

$$S = \{\infty \ ; \ v \text{ divise } 2b(a^2 - 4b)\}.$$

Alors il y a une suite exacte de groupes :

$$0 \longrightarrow E(K)/f(E(K)) \xrightarrow{g} K(S;2) \xrightarrow{h} WC(E/K)[f].$$

$g(O_E) = 1$; $g(0,0) = a^2 - 4b$; $g(X,Y) = X$ et $h(d) = \{C_d/K\}$.

Où C_d/K *=espace homogène de la Courbe Elliptique E :*

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

$A[f]$ *= sous groupe de torsion de A = ensemble des points P d'image* $f(P) = O_E$.

$K(S,2) = \{d \in K^*/K^{*2}, ord_v(d) \equiv 0 \bmod 2 \text{ pour } v \notin S\}$.

Alors le f-groupe de Selmer est égal à :

$$S_f(E/K) \cong \{d \in K(S,2); C_d(K_v) \text{ non vide pour toute v hors de } S\}.$$

Preuve :

(Silverman Proposition 4-9-X [20]).

On utilise la théorie des espaces homogènes pour une Courbe Elliptique E et les groupes associés à ces espaces :

Les groupes $WC(E/K)$de Châtelet-Weil, $S_f(E)$de Selmer et $III(E/K)$de Shafarevich-Tate.

Ces groupes sont liés par la suite exacte :

$$0 \longrightarrow E(K)/f(E(K)) \longrightarrow S_f(E/K) \longrightarrow III(E/K)[f] \longrightarrow 0 .$$

□

Ces notions d'espaces homogènes, de groupes de Châtelet-Weil, de Selmer, de Shafarevich-Tate se trouvent dans [20-1].

Exemple : (Silverman 4-10-X [20])

Courbe Elliptique E d'équation de Weierstrass :

$$E : y^2 = x^3 - 6x^2 + 17x \in Q[x, y]$$

Calcul du discriminant : $\Delta(E) = -2^9.17^2$.
Ensemble de valuations $S = \{\infty, 2, 17\}$ associé à la 2-isogénie.
La courbe 2-isogène a pour équation :

$$E' : Y^2 = X^3 + 12X^2 - 32X \in Q[x, y] \qquad (1)$$

Il en résulte l'espace homogène correspondant à tout nombre $d \in Q(S,2)$:

$$C_d : dw^2 = d^2 + 12dz^2 - 32z^4 \qquad (2)$$

Les valeurs possibles de d sont :

$$d = 2 \quad \text{et} \quad d = 17 .$$

En étudiant les espaces homogènes C_2 et C_{17}, Silverman obtient le groupe quotient :

$$E(Q)/2E(Q) \cong (IZ/2IZ)^2$$

et le groupe de Mordell-Weil :

$$E(Q) \cong IZ \times T(E), \text{ avec } T(E) \cong IZ/2IZ .$$

Donc cette Courbe Elliptique E, a un rang égal à $r(E(Q)) = 1$ et un groupe de torsion $T(E)$ d'ordre 2.

3. Notion de p-descente :

Dans ce qui précède, la notion de 2-descente est liée à un ensemble de valuations S contenant les valuations qui divisent 2 et au corps $K(S,2)$.
La p-descente sur une Courbe Elliptique E est obtenue par le corps :

$$K(S, p) = \left\{ d \in K^* / K^{*p} ; ord_v(d) \equiv 0 \bmod p \text{ pour toute valuation } v \text{ hors de } S \right\}$$

et

$$S = \{\infty, \text{ valuation } v \text{ où } E \text{ a mauvaise réduction, valuations qui divisent} p\}.$$

Alors on lui associe l'application bilinéaire :

$$\psi : E(K)/pE(K) \times E[p] \longrightarrow K^*/K^{*p},$$

liée à l'application de Weil :

$$e_p : E[p] \times [p] \longrightarrow B_p = \{\text{racines p}^{\text{èmes}} \text{ de } 1\},$$

à l'homomorphisme de groupes :

$$\delta_E : E(K)/pE(K) \longrightarrow Hom(G, E[p]),$$

et à l'homomorphisme de groupes :

$$\delta_K : K^*/K^{*p} \longrightarrow Hom(G, B_p),$$

où G = groupe de galois K_{alg}/K.

Ces applications permettent de construire des nombres d et des espaces homogènes C_d.
Il existe une autre méthode de p-descente sur les Courbes Elliptiques qui est décrite dans [16].
Cette p-descente est en relation avec la suite exacte de groupes abéliens :

$$0 \longrightarrow E(K)/pE(K) \longrightarrow S^{(p)}(E) \longrightarrow III(E)[p] \longrightarrow 0,$$

où $S^{(p)} = p$ - groupe de Selmer de la courbe E ,
et *III (E)[p]* = sous groupe de p-torsion du groupe de Shafarevich-Tate.

L'algorithme de calcul du groupe de Selmer utilise la théorie de la cohomologie des groupes et une extension cubique L du corps de base K de la Courbe Elliptique.

Les deux auteurs étudient la 3-descente sur la Courbe Elliptique E :

$$E : y^2 = x^3 - 22x^2 + 21x + 1 \in Q[x, y].$$

Ils trouvent une borne $r(E) \geq 2$.

Ils étudient la 5-descente sur la Courbe Elliptique :

$$E : y^2 = x^3 - 1483\, x \in Q[x, y].$$

L'anneau $End\,(E)$ est isomorphe à l'anneau $IZ[i]$,
le nombre 5 admet la décomposition $5 = (2+i)(2-i)$.
Il en résulte le groupe de Mordell-Weil :

$$E(Q) \cong IZ/2IZ\,,$$

ce groupe est réduit au groupe de torsion $T(E)$.

Le 5-groupe de Selmer $S^{(5)}(E)$ est isomorphe au 5-groupe de Shafarevich-Tate $III(E)[5]$.
Pour mener à son terme cette étude, il est nécessaire d'utiliser des outils de Théorie des Nombres et de Géométrie Algébrique.

En conclusion, la suite de mon programme de recherche concerne l'acquisition de notions sur la cohomologie, les espaces homogènes, les groupes de Châtelet-Weil, les groupes de Selmer, les groupes de Shafarevich-Tate, les extensions de degré p du corps Q, les valuations d'un corps, les réductions des Courbes Elliptiques, les twists de Courbes Elliptiques.

References

[1] ANDRIANOV : « Modular Descent and the Saits-Kurokawa Conjecture-Inv. Math 53 (1979), 267-280.

[2] APOSTOL : « Modular Functions and Dirichlet Series in Number Theory » - GTM 41-Springer-(2000) 2 ^{ème} édition. Classification :11-01 , 11F xx.

[3] BIRCH-KUYK : « Modular Functions of One Variable IV- Lecture Notes in Mathematics n ^{0} 476-Springer (1975).

[4] CASSELS : « Diophantine Equations with Special Reference to Elliptic Curves », Journal London Mathematical Society 41(1966) 193-291.

[5] CREMONA : « Higher Descents on Elliptic Curves (1977) 1-9.

[6] DEURING: « Algebren » ; Springer Verlag, New York (1968).

[7] FULTON : « Algebraic Curves », Benjamin, New York (1969).

[8] HARTSHORNE : « Algebraic Geometry »-GTM 52-Springer (1983).
Classification: 14 A 10 - 14 A 15 - 14 Fxx – 14 H xx – 14 Ixx.

[9] HUSEMOLLER : « Elliptic Curves »- G.T.M. 111 (1987).

[10] KOBLITZ : (1) « Introduction to Elliptic Curves and Modular Forms. 2 ^{ème} édition Springer (1984) GTM 97.

(2) « A course in Number Theory and Cryptographiy 2 ^{ème} édition GTM 114-Springer.

[11] KOSTRIKIN : « Introduction à l'algèbre » Ed . Mir – Moscou- 2 ^{ème} édition (1986).

[12] LANG : (1) « Algebra » 2 ^{ème} édition, Addison Wesley Publishing Company, Inc, Reading; Massachusetts; New York (1984).

(2) « Elliptic Curves – Diophantine Analysis » Springer Verlag (1978) – Classification AMS = 10 B 45 – 10 F 99 – 14 G 25 – 14 H 25.

(3) « Algebraic Number Theory », Addison – Wesley (1970).

(4) « Cyclotomic Fields – GTM 59 – Springer.

[13] MAZUR : (1) « Modular curves and the Eisenstein ideal », IHES publ. Math. 47. (1977). 33-186.

(2) « Rational isogenies of prime degree », Invent. Math. 44 (1978), 129-162.

[14] NERON : « Quasi Fonctions et Hauteurs sur les variétés Abéliennes ». Annals of Mathématics 82 (1965), 249-331.

[15] RUBIN : « Elliptic Curves with Complex Multiplication and the Conjecture of Birch and Swinnerton – Dyer – Inv. Math. 64 (1981) 455 - 470.

[16] SCHAEFER and STOLL : « How to do a p-descente on an Elliptic Curves ». Trans. Amer. Math. Soc- Vol 356 (oct 2003) 1209/1231.

[17] SERRE : (1) « Géométrie Algébrique et Géométrie Analytique – Ann . Inst . Fourier 6 (1956) -1- 42.

(2) « Propriétés galoisiennes des points d'ordre fini des Courbes Elliptiques », Inventions Mathématiques15 (1972), 259 – 331.

[18] SHAFAREVICH : (1) « Basic Algebraic Geometry » - Springer Verlag (1977).

(2) « Algebra I » - Moscou (1986) – Springer (1987).

Classification AMS = 12 – xx , 20 – xx.

[19] SHIMURA : « Introduction to the Arithmetic Theory of Automorphic Function; Princeton University Press (1971).

[20] SILVERMAN : (1) « The Arithmetic of Elliptic Curves » - GTM 106 – Springer (1986). Classification AMS = 1401, 14 G 99, 14 H 05, 14 K 15.

(2) « Lower Bound for the canonical height on Elliptic Curves » - Duke Math . J. 48 (1981) . 633-648.

(3) « The Difference between the Weil Height and the Canonical Height on Elliptic Curves » Math. comp. 35 (1990) 723-743. Classification = 11G 05, 11Y50.
[21] TATE : « The arithmetic of Elliptic Curves ; Inv Math 23 (1974) 179-206.
[22] VELU : « Isogénies entre Courbes Elliptiques ;C.R.A.S. Paris (1971) 238-241.
[23] WEIL : (1) « Sur un théorème de Mordell ; Bull. Sci. Math. 54 (1930).
(2) « L'arithmétique sur les Courbes Elliptiques ». Acta Math 52 (1928) 281-315.
[24] WEISS : « Algebraic Number Theory » - Mc Graw-Hill. New York (1964).
[25] ZIMMER : « On the Difference of the Weil Height and the Neron-Tate Height. Math. Zeit 147 (1976) 35-51.