N^0 d'ordre : 04/2004- M/MT

Université des Sciences et de la Technologie
Houari Boumediene

Faculté des Sciences Mathématiques

MEMOIRE

Présenté

Par : Melle AIT IKHLEF NABILA

Pour l'obtention du diplôme de

MAGISTER en **MATHEMATIQUES**

Spécialité **ALGEBRE ET THEORIE DES NOMBRES**

Sur le sujet

Rangs d'une Famille de Courbes Elliptiques

$$Y^2 = x^3 + 2\,t^3\,x^2 + t^2\,x$$

Soutenu Publiquement le 19/01/2004 , devant le jury composé de :

- BETINA Kamel , Professeur à l'USTHB : Président
- ZITOUNI Mohamed, Professeur à l'USTHB : Dteur de Thèse
- KESSI Arezki , Professeur à l'USTHB : Examinateur
- HACHAICHI M. Salah , Maître de conférence : Examinateur
- BENSEBAA Boualem , Chargé de recherche : Examinateur
- AIDER Abdelkader , Chargé de recherche : Examinateur

Remerciements

J'adresse mes vifs remerciements,

à Monsieur BETINA Kamel qui a bien voulu accepter de présider le jury.

à Monsieur ZITOUNI Mohamed qui m'a fourni le sujet , a suivi mon travail et aidé de ses conseils.

à Messieurs M. S.HACHAICHI ,A. KESSI , B. BENSEBAA. et AEK. AIDER qui ont bien voulu être membres du jury.

Sommaire

Introduction :

Dans cette thèse, nous nous proposons d'étudier des rangs d'une famille de courbes elliptiques $E_t : y^2 = x^3 + 2t^3 x^2 + t^2 x$. Elle est formée de 4 chapitres.

La détermination du rang d'une courbe elliptique a donné lieu à plusieurs méthodes particulières. Les méthodes de calculs du rang r (E) = r sont variées ; elles utilisent toutes les propriétés des courbes elliptiques. Comme dans la théorie des groupes abstraits, le nombre de générateurs du groupe E(K) est le rang de la courbe elliptique. Ce rang r (E) = r est donc un entier naturel positif ou nul . Cet invariant est l'objet de nombreux articles. Il existe des courbes elliptiques E(K) de rang nul et des courbes elliptiques de rang r (E)>0. Cependant il n'existe pas un algorithme effectif pour calculer le rang du groupe de Mordell- Weil E(K) .

Dans le Ier chapitre, nous exposerons l'arithmétique des courbes elliptiques dont nous aurons besoin par la suite. Nous énoncerons toutes les propriétés que nous appliquerons à la famille de courbes elliptiques $E_t : y^2 = x^3 + 2t^3 x^2 + t^2 x$.

Dans le chapitre II, nous traiterons les homomorphismes de courbes elliptiques ; nous exposerons les isomorphismes, les isogénies et les automorphismes de courbes elliptiques .Puis nous appliquerons à la famille de courbes elliptiques $E_t : y^2 = x^3 + 2t^3 x^2 + t^2 x$.

Dans le chapitre III, nous étudierons la théorie des valuations et les réductions .Nous commencerons par les valuations d'un corps , leur classification , la topologie induite par une valuation et les valuations équivalentes. Nous traiterons ensuite les réductions des courbes elliptiques. Puis nous appliquerons des réductions à la famille de courbes elliptiques $E_t : y^2 = x^3 + 2t^3 x^2 + t^2 x$

Dans le IVéme et dernier chapitre, nous introduirons la notion de « hauteur sur un groupe abélien » ; cette notion s'applique au groupe abélien E(K) de

Mordell- Weil, nous examinerons quelques aspects des rangs ;il s'agit des méthodes particulières utilisées par des spécialistes pour déterminer le rang d'une courbe elliptique .

Ainsi Brumer et Kramer , utilisent la théorie de la réduction , des suites exactes de groupes , des twists , des isogénies .

La méthode de Wada et Taira , est basée sur des équations diophantiennes, des nombres congruents , la fonction $L_E(s)$ de Hasse – Weil .

La méthode de Shiode , est basée sur des réseaux complexes , des représentations galoisiennes de groupes .

La méthode de Penny et pomérance, repose sur des ensembles particuliers d'entiers naturels.

La méthode de Rubin et Silverberg, est basée sur une fonction homogène de degré 4 associée à l'équation de Weierstrass de degré 4 ,sur la fonction Zeta et la fonction d'Epstein , une fonction hauteur .

D'autres auteurs évaluent le rang à partir de la conjecture de BSD .Ce rang est le rang analytique de la courbe elliptique.

Le rang, r(E) = r, d'une courbe elliptique E, peut être théoriquement, calculer avec « le théorème de descente infinie ».

Chapitre I

Arithmétique des courbes elliptiques

Dans les ouvrages nombreux qui traitent des courbes elliptiques on trouve les définitions suivantes d'une courbe elliptique :

" Variété algébrique abélienne " dans " Diophantine equations with special reference to elliptic curves " , [2] .

" Variété abélienne de dimension un ou courbe projective non singulière de genre un " dans " Introduction to the Arithmetic Theory of Automorphic Function " , [16].

" Courbes de genre un " dans " The Arithmetic of Elliptic Curves ", [18] .

"Courbes algébriques de genre un " dans " Algebraic Geometry p.56" , [4]

"Courbes de genre un " dans " The Arithmetic of Elliptic Curves ", [17].

"Courbe cubique ayant un point d'inflexion et d'équation
$y^2 w + a_1 x y w + a_3 y w - x^3 - a_2 x^2 w - a_4 x w^2 - a_6 w^3 = 0$ dans" Elliptic Curves" [7].

1-Stuctures d'une courbe elliptique :

Définition 1 :
Une courbe elliptique est une cubique plane E , non singulière, irréductible , d'équation algébrique de la forme:
$E : y^2+a_1xy+a_3y=x^3+a_2x^2 + a_4x + a_6$. **(1)**

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

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

Une courbe elliptique possède d'autres structures algébriques :
une structure de variété abélienne de dimension un ;
une structure de courbe algébrique projective de genre un ;
une structure de groupe abélien de type fini ;
une structure de schéma irréductible de dimension un ;

2 - Influence du corps de base sur la courbe elliptique :

Le groupe de Galois $G_{K_{alg}/K}$ de la clôture algébrique K_{alg} du corps K opère sur une courbe elliptique E par les K- automorphismes :
$\sigma(P) = (\sigma(x), \sigma(y))$ pour tout automorphisme σ et pour tout point P = (x , y)
de la courbe .

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

a) lorsque K est un corps de nombres algébriques ,ce corps intervient par les entiers, les discriminants , les classes d'idéaux ,la ramification , les valuations et la réduction , l'analyse p- adique , les nombres premiers , les fonctions arithmétiques ,…

b) lorsque K est le corps des nombres complexes C, ce corps intervient par les réseaux complexes ,les tores complexes , les groupes de Lie ,les fonctions elliptiques ,les fonctions modulaires ,les formes modulaires, le demi plan de Poincaré ; et la géométrie algébrique intervient par les variétés algébriques , les variétés abéliennes ,les courbes algébrique projectives , les diviseurs , les schémas , l'homologie ,la cohomologie ,…

c) Lorsque K est un corps fini $|F_q$, ce corps intervient par le théorème de Hasse, l'invariant de Hasse ,les courbes supersingulières , les tests de primalité , le codage,la cryptographie,…

3 - Transformations linéaires d'équations :

L'équation (1) peut être transformée par des changements linéaires de variables.
Lorsque la caractéristique du corps K est différente de 2 ,le changement de variables:

$$(x , y) \rightarrow \quad (x, \frac{1}{2}(y - a_1 x - a_3)) \qquad \textbf{(2)}$$

élimine les monômes x y et y ; l'équation (1) devient :

E_1 : $y^2=4x^3+b_2x^2+2b_4x+ b_6$ ***(3)***

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

Les calculs donnent les formules b_{2i} :

$$\begin{cases} b_2 = a_1^2 + 4\, a_2 ; \\ b_4=a_1a_3+2a_4; \\ b_6 = a_3^2 + 4\, a_6 ; \end{cases} \qquad \textbf{(4)}$$

L'élimination du monôme x^2 et du coefficient 4 dans l'équation (3) s'obtient par le changement de variables , pour carac(K) $\neq$ 2,3 :
(x , y) $\rightarrow$ ((x - 3 b_2) / 36 , y /108) ,

l'équation de E_1 devient :
E_2 : $y^2 = x^3 - 27\, c_4\, x - 54\, c_6$
Les coefficients c_{2i} sont des polynômes " homogènes de degré 2i " dans l'anneau $Z[b_2 ,b_4 ,b_6]$; les calculs donnent les formules c_{2i} :

$$\begin{cases} c_4 = b_2^2 - 24\, b_4 \ ; \\ c_6 = b_2^3 + 36\, b_2\, b_4 - 216\, b_6 \ ; \end{cases} \qquad \textbf{(5)}$$

L'équation de Weierstrass peut avoir des coefficients a_i nuls et prendre d'autres formes.

E_3 : $y^2 = x^3 + A\ x + B$;

E_4 : $y^2 = x\,(x - 1)\,(x - \lambda)$ avec $\lambda \neq 0,1$,équation de Legendre ***(6)***

L'équation de Weierstrass

E : $y^2= 4x^3-g_2x-g_3$

est transformée en équation de Tate par le changement

$X = x - \frac{1}{12}$; $Y = \frac{y}{2}+\frac{1}{2}(x-\frac{1}{12})$

Le calcul donne l'équation :

E' : $Y^2- XY = X^3- h_2X - h_3$ ***(7)***

avec $h_2 = \frac{1}{4}(g_2-\frac{1}{12})$ et $h_3 = \frac{1}{4}(g_3+\frac{g_2}{12} - \frac{4}{12^3})$ ***(8)***

4 - Cinq invariants d'une courbe elliptique E :

Toute courbe elliptique possède de nombreux invariants: arithmétiques, algébriques, géométriques,...

Nous nous intéressons aux 5 invariants : discriminant, invariant modulaire, invariant différentiel, rang et régulateur.

Définition 3 :

Le discriminant d'une courbe elliptique E est le polynôme " homogène de degré 12 " de l'anneau Z [b_2 ,b_4 ,b_6, b_8] , lorsque carac (K) $\neq$ 2,3

$\Delta (E) = 9\, b_2\, b_4\, b_6 - 8\, b_4^3 - 27\, b_6^2 - b_2^2\, b_8$;où l'on a posé $4\, b_8 = b_2\, b_6 - b_4^2$ **(1)**

C'est aussi un polynôme " homogène de degré 12 " en c_{2i} ,

$$\Delta(E)=(c_4^3-c_6^2) \,/\, 1728 \; ; \qquad \textbf{(2)}$$

L'hypothèse" courbe non singulière" équivaut à la condition $\Delta(\mathrm{E}) \neq 0$ pour une courbe elliptique E .

Donc l'invariant discriminant caractérise les courbes elliptiques.

Définition 4 :

L'invariant modulaire d'une courbe elliptique E est l'élément du corps K :

$$j(E)=c_4^3 \,/\, \Delta(E) \; ; \qquad \textbf{(3)}$$

L'invariant modulaire caractérise les courbes elliptiques isomorphes.

Définition 5 :

L'invariant différentiel d'une courbe elliptique E est l'élément différentiel :

$$\omega (E)=d x \,/\, (2 y + a_1 x + a_3) = - d y \,/\, (3 x^2 + 2a_2 x + a_4 - a_1 y) \; ; \qquad \textbf{(4)}$$

où les polynômes dénominateurs sont les dérivées partielles F'_y et F'_x du polynôme F(x ,y) :

$E : F(x ,y) = y^2 + a_1 x y + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6$.

Cet invariant est utilisé dans les intégrales elliptiques $\int \omega$.

Définition 6 :

Le rang d'une courbe elliptique E est l'entier naturel $r = r(E) \geq 0$ qui apparaît dans l'isomorphisme de groupes :

$$E(K) \cong E(K)_{tors} \times Z^r \; . \qquad \textbf{(5)}$$

Définition 7 :

Le régulateur d'une courbe elliptique E sur un corps K de rang r (E) = r > 0 est le déterminant d'ordre r .

$$R(E / K) = det (< R_i , R_j >)$$

où les points R_i sont des générateurs du groupe abélien E (K) et $<.\ ,\ .>$ la forme quadratique de valeur :
$<R_i , R_j> = \hat{h}(R_i + R_j) - \hat{h}(R_i) - \hat{h}(R_j)$ *, pour la hauteur canonique* $\hat{h}$.
Le régulateur vaut R(E /K) = 1 pour le rang r = 0 , par convention .

Ce régulateur apparaît dans la conjecture de Birch et Swinnerton – Dyer :
la série $L_E(s)$ d'une courbe elliptique E sur le corps Q satisfait les 2 relations :

(1) $L_E(s)$ admet un zéro d'ordre $r_{an}(E)$ en s = 1 ;

$$L_E(s)=\prod_{P\not\in\Delta}\frac{1}{(1-t_p p^{-s})}\prod_{p\in\Delta}\frac{1}{(1-t_p p^{-s}+p^{1-2s})}$$

où $t_p = 1 + p - A_p$

et A_p *= le nombre de points rationnels de la courbe réduite* $\widetilde{E}$ *mod p et p premier.*

(2) $\lim_{s\to 1}(s-1)^{-r_{an}} L_E(s) = \{\int_{E(\Re)}|\omega|\}\, R(E)\, \text{card}\, Ш(E) \prod_p c_p (\#(E(Q)_{tors}))^{-2}$

Cf : [21] conjecture 16.5 , p 362 .

La structure de groupe abélien de l'ensemble E(K) des points K rationnels d'une courbe elliptique permet d'introduire l'invariant qui caractérise ce type fini . Comme dans la théorie des groupes abstraits , le nombre de générateurs du groupe E(K) est le rang de la courbe elliptique . Ce rang r (E) = r est donc un entier naturel positif ou nul . Cet invariant est l'objet de nombreux articles. Il existe des courbes elliptiques E(Q) de rang nul et des courbes elliptiques de rang r (E)>0.

Exemple : *Courbe elliptique E (Q) de rang r (E) = r >2 :*

E : $y^2 - 246\,x\,y + 36599029\,y = x^3 - 89199\,x^2 - 19339780\,x - 36239244$;
Cf : [2]

Les méthodes de calculs du rang r (E) = r sont variées, elles utilisent toutes les propriétés des courbes elliptiques.

Nous commençons donc par un exposé sur les connaissances relatives à une partie de la théorie arithmétique et géométrique des courbes elliptiques.

5- Classification des cubiques planes par leur discriminant :

C'est l'invariant discriminant $\Delta(E)$ qui permet de savoir si une cubique plane E :

E : $y^2 + a_1xy + a_3y = x^3+a_2x^2+ a_4x +a_6$, ***(1)***

est non singulière, donc elliptique , ou singulière , donc non elliptique .

Dans la théorie des singularités d'une courbe algébrique C : $F(x , y) = 0$,

c'est le système de dérivées partielles :

$F_x'(x,y)=0, F_y'(x,y) =0$, $F(x , y) = 0$ ***(2)***

qui donne les coordonnées du point singulier éventuel .

Lorsque le système (2) n'admet pas de solution dans le corps K , alors la courbe C est non singulière .

Lorsque le système (2) admet une solution $S = (x_0 , y_0)$, alors ce point est singulier sur la courbe C .

Le nombre maximal de points singuliers de la courbe C dépend du degré de l'équation projective $F(X , Y ,Z) = 0$. Donc une cubique, qui est de degré 3, admet 1 ou 0 point singulier . ***(3)***

Pour savoir si une équation cubique détermine une courbe elliptique, nous disposons de la

Proposition 1:

Soit une cubique plane E de discriminant $\Delta (E)$ et le point à l'infini $O_E = (\infty,\infty) = (0,1,0)$ associé à E . Alors :

1) le point à l'infini O_E n'est pas singulier sur la cubique E ;

2) *la relation "$\Delta (E) \neq 0$ "équivaut à " la cubique E est une courbe elliptique ".*

Preuve de (1) :

Soit une cubique plane E d'équation projective :

E:$f (X,Y,Z)= Y^2 Z + a_1 XYZ +a_3Y Z^2- X^3 - a_2 X^2Z - a_4 XZ^2 - a_6Z^3 = 0$ ***(1)***

Ses 3 dérivées partielles valent :

$f'_X=a_1YZ-3X^2-2a_2 X Z - a_4 Z^2$; ***(2)***

$f'_Y = 2 YZ + a_1 X Z + a_3 Z^2$;

$f'_Z = Y^2 + a_1 X Y +2 a_3Y Z - a_2 X^2 - 2 a_4 X Z - 3 a_6 Z^2$;

Valeurs des polynômes (1) et (2) au point $O_E = (0,1,0)$.

$f(0,1,0)=0 ; f'_X(0,1,0)=0 = f'_Y(0,1,0) ; f'_Z(0,1,0) = 1$ ***(3)***

(3) implique que le point O_E n'est pas singulier sur la cubique E

□

Preuve de "Δ (E) ≠ 0 " implique " la cubique E est elliptique ":

Soit une cubique E de discriminant Δ (E) et d'équation :

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

Alors le résultant de f vaut $Res(f, f') = c_0 \Delta(f(x))$ ***(2)***

La relation entre les discriminants de f(x) et de E est :

$\Delta(f(x)) = 16\Delta(E)$ ***(3)***

Les relations (2) , (3) et l'hypothèse "Δ (E) ≠ 0 "impliquent le résultant

$Res(f, f') \neq 0$ ***(4)***

(4) implique que les polynômes f(x) et f '(x) n'ont pas de racines communes ; donc les racines de f(x) sont simples , il en résulte que la cubique E est non singulière , donc c' est une courbe elliptique .

□

Preuve de " la cubique E est elliptique " implique "Δ (E) ≠ 0 " :

Soit une cubique elliptique E d'invariant Δ (E) et d'équation :

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

Par définition elle n'est pas singulière . Cela implique que f(x) admet

3 racines simples donc le résultant $Res(f, f') \neq 0$ ***(2)***

Les relations $Res(f, f') = 16 \Delta(E)$ et (2) impliquent l'invariant $\Delta(E) \neq 0$

□

8 – 1 Résultant de deux polynômes :

Dans la théorie des courbes elliptiques ,on peut utiliser la définition du résultant de 2 polynômes de l'anneau K [x] pour étudier ces singularités .

Définition 8 :

Le résultant de 2 polynômes $f(x) = c_0 x^n + \ldots + c_{n-1} x + c_n$ *et* $g(x) = d_0 x^t + \ldots + d_{t-1} x + d_t$ *est le déterminant d'ordre n + t des coefficients* $c_0, \ldots, c_n, d_0, \ldots, d_t$ *:*

$$Res(f,g)=\begin{vmatrix} c_0\ c_1 \cdots c_n\ 0 \cdots\cdots\ 0 \\ 0\ c_1 \cdots c_{n-1}\ c_n\ 0 \cdots\cdots 0 \\ 0 \cdots\cdots 0\ c_0 \cdots\cdots\cdots\ c_n \\ d_0\ d_1 \cdots\cdots\cdots d_t\ 0 \cdots\ 0 \\ 0\ d_0 \cdots d_{t-1}\ d_t\ 0 \cdots\ 0 \\ 0 \cdots\cdots 0\ d_0 \cdots\cdots\cdots d_t \end{vmatrix} \quad \begin{matrix} \} \text{ t lignes} \\ \\ \\ \} \text{ n lignes} \\ \\ \end{matrix} \qquad \textbf{(4)}$$

Les termes manquants sont remplacés par des zéros .

Le résultant *Res (f , g)* est fonction de leur zéros

Proposition 2:
Soit un corps K et 2 polynômes $f(x) = c_0 (x - \lambda_1)(x - \lambda_2) \ldots (x - \lambda_n)$ *et* $g(x) = d_0 (x - \psi_1)(x - \psi_2) \ldots (x - \psi_t)$ *dans l'anneau K[x] .*
Alors leur résultant R (f , g) a pour valeur :

$$Res(f,g) = c_0^{\,t}\, d_0^{\,n} \prod_{i=1}^{n} \prod_{j=1}^{t} (\lambda_i - \psi_j) .$$

Preuve :

Cf :S.Lang,Algebra chapitre V , Polynomials , paragraphe10 , The resultant..

□

Corollaire 1 :
Soit les hypothèses de la proposition 3; alors :
Le résultant Res (f , g) est nul si les deux polynômes f et g admettent une racine commune ; lorsque f et g n'ont pas de racine commune leur résultant n'est pas nul.

Preuve :

Cf : S.Lang, Algebra chapitre V p138 .

□

Corollaire 2 :
Le résultant d'un polynôme $f(x) = c_0 x^n + \ldots + c_{n-1} x + c_n$ *et de sa dérivée* $f'(x) = n\, c_0 x^{n-1} + \ldots + a_{n-1}$ *a pour valeur :*

$$Res(f, f') = c_0^{\,2n-1} \prod_{\substack{1 \le i, j \le n \\ i \ne j}} (\lambda_i - \lambda_j) = c_0\ \Delta(f(x))$$

où les λ_i *sont les racines de f(x) et* $\Delta(f(x))$ *le discriminant de f(x) .*

Preuve :

Cf : S.Lang, Algebra chapitre V p 139 .

□

Il en résulte que le résultant Res (f , f ') du polynôme f(x) de l'équation d'une courbe cubique E : $y^2 = f(x)$ permet de déterminer les points singuliers de la cubique E s'ils existent .

Proposition 3 :
Soit une cubique plane E d'équation :
E : $y^2 = 4x^3 + b_2 x^2 + 2 b_4 x + b_6 = f(x)$.
Alors les discriminants $\Delta(E)$ de E et $\Delta(f(x))$ de f(x) sont liés par la relation :

$$\Delta(f(x))=16\Delta(E) \qquad \textbf{(5)}$$

Preuve :

La formule du discriminant d'une courbe elliptique donne :

$$\Delta(E)=9b_2b_4b_6-8b_4^3-27\, b_6^2 - b_2^2\, b_8 \quad ; \qquad \textbf{(1)}$$

La dérivée du polynôme f(x) vaut

$$f'(x)=12x^2+2b_2x+2b_4 \quad . \qquad \textbf{(2)}$$

Le résultant des polynômes f(x) et f '(x) est le déterminant :

$$Res\,(f, f') = \begin{vmatrix} 4 & b_2 & 2b_4 & b_6 & 0 \\ 0 & 4 & b_2 & 2b_4 & b_6 \\ 12 & 2b_2 & 2b_4 & 0 & 0 \\ 0 & 12 & 2b_2 & 2b_4 & 0 \\ 0 & 0 & 12 & 2b_2 & 2b_4 \end{vmatrix}$$

Le calcul de ce déterminant donne la relation :

$$Res\,(f, f') = 16\,\Delta(E)$$

□

5– 2 Cubiques singulières : nœud, point de rebroussement

Proposition 4 :
Soit une cubique E de discriminant $\Delta(E)$ et $c_4(E) = b_2^2 - 24\, b_4$.
Alors : 1) " $\Delta(E) = 0$ et $c_4(E) \neq 0$ " si et seulement si " la cubique E admet un nœud " .
2)" $\Delta(E) = c_4(E) = 0$ " si et seulement si " la cubique E admet un point de rebroussement "

Preuve de "Δ (E) = 0 et c_4 (E) ≠ 0 "implique " la cubique admet un nœud ":

Soit une cubique E d'équation

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

de discriminant Δ (E) = 0 ;

par le théorème 1, la cubique E admet un point singulier S . ***(1)***

Les pentes des tangentes à la courbe E au point S valent :

$y' = (6 x^2 + b_2 x + b_4) \,/\, y = N(x) \,/\, y$;

Le discriminant du polynôme N(x) vaut :

$\Delta(N(x)) = b_2^2 - 24 b_4 = c_4(E)$ ***(2)***

L'hypothèse " c_4 (E) ≠ 0 " implique que le polynôme N (x) admet 2 racines distinctes ;

Il en résulte 2 tangentes distinctes à la cubique E au point singulier S ;

donc ce point S est un nœud de la cubique.

□

Preuve de " Δ (E) = c_4 (E) = 0 " implique " la cubique E admet un point de rebroussement " :

Nous reprenons les relations (1) , (2) et (3) dans la preuve précédente .

L'hypothèse " c_4 (E) = 0 " implique que le polynôme N (x) admet une racine double ; il en résulte 2 tangentes confondues à la cubique E au point singulier S ;

donc ce point S est un point de rebroussement de la cubique E .

□

Nous ne ferons pas les 2 autres preuves : " E admet un nœud " implique "Δ (E) = 0 et c_4 (E) ≠ 0 " et " E admet un point de rebroussement " implique " Δ (E) = c_4 (E) = 0 ". Ces preuves ne comportent pas de difficultés particulières par rapport au précédentes .

□

5 - 3 Cubiques non singulières : courbes elliptiques

Proposition 5 :
Soit une courbe elliptique E de discriminant $\Delta(E)$. Alors :
1) *$\Delta(E) > 0$ implique trois points simples d'intersection de E avec l'axe Ox ;*
2) *$\Delta(E) < 0$ implique un point simple d'intersection de E avec l'axe Ox ;*

Preuve de (1) :

Soit une courbe elliptique E *de discriminant* $\Delta(E) > 0$ et d'équation :

$E : y^2 = f(x) = (x - e_1)(x - e_2)(x - e_3)$; avec $e_i \neq e_j$ ***(1)***

Son discriminant vaut :

$\Delta(f(x)) = (e_1 - e_2)^2 (e_2 - e_3)^2 (e_3 - e_1)^2$; ***(2)***

L'hypothèse $\Delta(E) > 0$ implique $\Delta(f(x)) > 0$; il en résulte 3 racines réelles

e_1, e_2, e_3 de (1) .

Cela implique trois points d'intersection T_i de E avec l'axe Ox :

$T_i = (e_i, 0)$ avec $i = 1,2,3$.

□

Preuve de (2) :

Soit une courbe elliptique E de discriminant $\Delta(E) < 0$ et d'équation :

$E : y^2 = f(x) = (x - e_1)(x - e_2)(x - e_3)$; avec $e_i \neq e_j$ ***(1)***

L'hypothèse $\Delta(E) < 0$, implique la relation :

$(e_1 - e_2)^2 (e_2 - e_3)^2 (e_3 - e_1)^2 < 0$; ***(2)***

Il en résulte une racine réelle, e_1 par exemple et 2 racines complexes conjuguées

$e_2 = s + i\,t$ et $e_3 = s - i\,t$; ***(3)***

Cela implique $\Delta(f(x)) = (e_1 - s - i\,t)^2 (2\,i\,t)^2 (e_1 - s + i\,t)^2$

$= -4\,t^2 ((e_1 - s)^2 + t^2)^2 < 0$ ***(4)***

La racine réelle e_1 donne le point d'intersection $T_1 = (e_1, 0)$; les deux racines complexes conjuguées e_2 et e_3 ne donnent pas de points d'intersection de la courbe E avec l'axe Ox

□

5 – 4 Classification des cubiques C par Δ (E) en 4 classes :

Cette classification est précisée dans la proposition 6 qui rassemble les résultats obtenus en §5-2 et §5-3

Proposition 6 :
Les cubiques planes E sont classifiées par leur discriminant $\Delta(E)$ et leur coefficient $c_4(E) = b_2^2 - 24\, b_4$ en 4 classes .

1) Classe des cubiques pourvues d'un nœud lorsque $\Delta(E) = 0$ et $c_4(E) \neq 0$;
2) Classe des cubiques pourvues d'un point de rebroussement lorsque $\Delta(E) = c_4(E) = 0$;
3) Classe des courbes elliptiques qui coupent l'axe Ox en trois points simples lorsque $\Delta(E) > 0$;
4) Classe des courbes elliptiques qui coupent l'axe Ox en un seul point , qui est simple lorsque $\Delta(E) < 0$

9 - Structure de groupe abélien de type fini sur une courbe elliptique :

6 – 1 Loi de groupe :

Considérons une courbe elliptique E sur un corps commutatif K et l'ensemble E(K)des points K- rationnels de la courbe E ; une structure de groupe abélien est déterminée par une loi de composition et un élément neutre.

Le point à l'infini, $O_E = (\infty, \infty)$ dans le plan affine et, $O_E = (0,1 , 0)$ dans le plan projectif $|P^2(K)$ joue le rôle d'élément neutre .
Ce point est caractérisé par sa direction $P O_E$ parallèle à l'axe Oy **(*1*)**

La loi de composition est déterminée par la règle géométrique :
« 3 points P, Q et R colinéaires de la courbe elliptique E ont une somme nulle ».

$$P + Q + R = O_E \quad .$$

Cette loi additive est commutative.

Déterminons les points P du groupe E(K) qui sont d'ordre 2 : Ces points P sont définis par les intersections de la tangente en P à la courbe E avec la courbe ; cette tangente coupe la courbe E en un point double P et un point simple M = -2P.

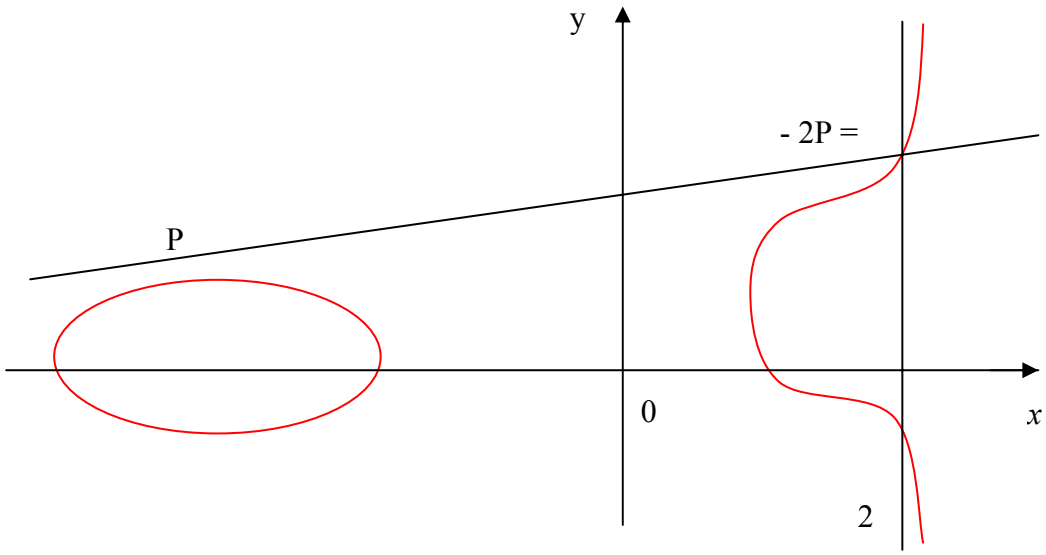


Figure 1

Les calculs donnent les formules des coordonnées des points 2P pour un point P = (x , y) :

$$x(2P) = y'^2 + a_1 y' - a_2 - 2x \;;$$

$$y(2P) = -y'^3 - 2a_1 y'^2 + (a_2 - a_1^2 + 3x)\, y' + a_1 a_2 - a_3 + 2a_1 x - y \;;$$

$$\text{avec } y' = \frac{3x^2 + 2a_2 x + a_4 - a_1 y}{2y + a_1 x + a_3}; \qquad \textbf{(11)}$$

6 – 2 Coordonnées des points $-P$ et $P_1 + P_2$:

Soit l'application $f : E(K) \times E(K) \rightarrow E(K)$ **(2)**

de valeur $f(P_1 , P_2) = P_1 + P_2$

Ce point $P_1 + P_2$ est déterminé par la règle géométrique :

" Trois points colinéaires d'une courbe elliptique E ont une somme nulle

$$P_1 + P_2 + P_3 = O_E \text{ "}$$

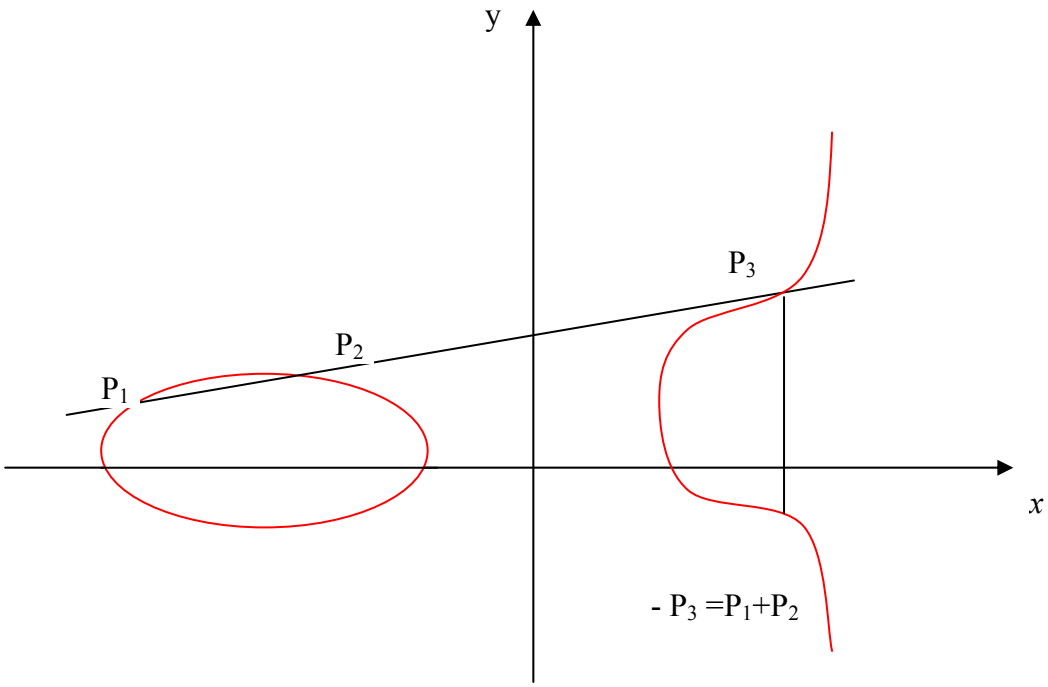


Figure 2

Par convention la droite P O_E est parallèle l'axe Oy **(5)**

Vérifions les 4 axiomes d'un groupe abélien :

L'axiome de l'élément neutre est satisfait par le point O_E ;

L'axiome du symétrique d'un point P de la courbe est satisfait par la parallèle à l'axe Oy passant par le point P qui recoupe la courbe au point –P ;

L' axiome d'associativité est vérifié par le calcul des points ($P_1 + P_2$) + P_3 et $P_1 + (P_2 + P_3)$;

L'axiome de commutativité est vérifié par la coïncidence des sécantes $P_1 P_2$ et $P_2 P_1$

Il en résulte la

Proposition 7 :

L'ensemble E(K) des points K rationnels d'une courbe elliptique E sur un corps K, muni de l'application $(P_1 , P_2) \rightarrow P_1 + P_2$ *définie par la règle géométrique des trois points colinéaires de la courbe E , est un groupe abélien d'élément neutre le point* 0_E *à l'infini .*

La définition de l'intersection d'une courbe algébrique par une sécante permet les calculs des coordonnées des points - P et $P_1 + P_2$:

Le symétrique - P du point P est le point d'intersection de la courbe elliptique E par la parallèle à Oy passant par le point P :

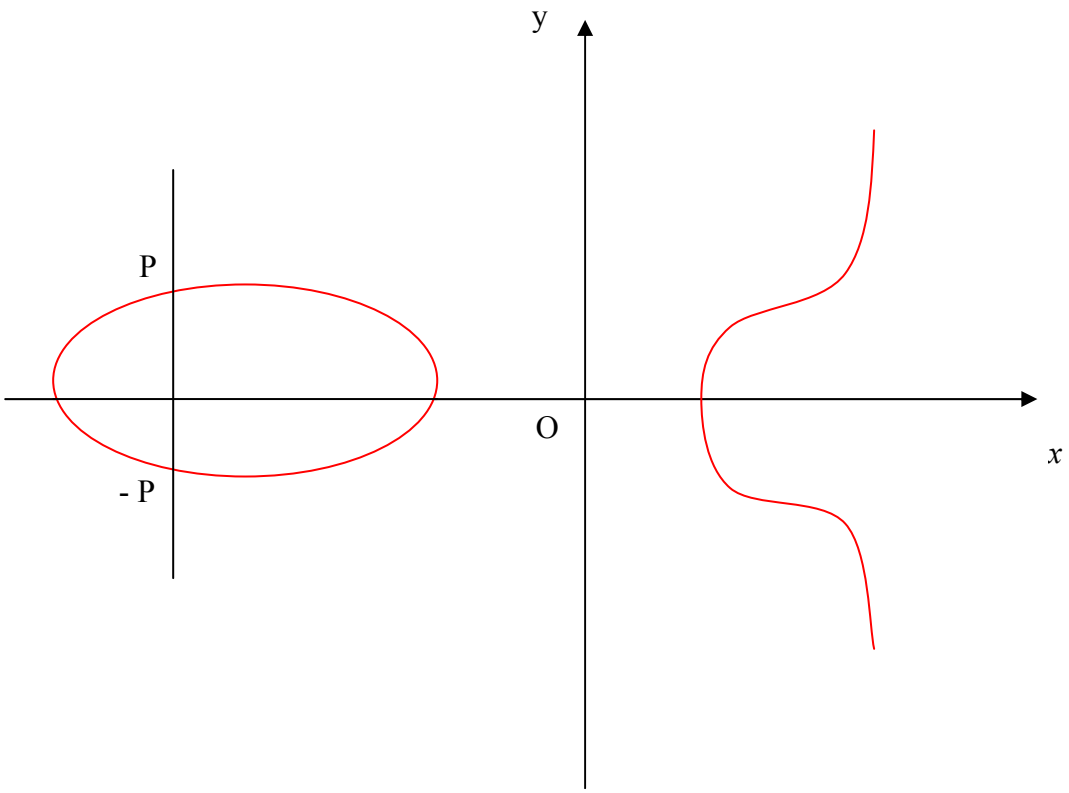


Figure 3

Les calculs donnent les coordonnées du symétrique - P du point P :

$P = (x , y)$ implique $-P = -(x , y) = (x , - y - a_1 x - a_3)$; ***(6)***

Avec la sécante P_1P_2 et la formule du symétrique , les calculs donnent les coordonnées de la « somme » $P_1 + P_2$ de deux points $P_1 \neq \pm P_2$, $P_i = (x_i , y_j)$

$x (P_1 + P_2) = \lambda^2 + a_1 \lambda - a_2 - x_1 - x_2$;

$y (P_1 + P_2) = -\lambda^3 - 2 a_1 \lambda^2 + (a_2 - a_1^2 + 2x_1 + x_2) \lambda + a_1 a_2 - a_3 + a_1 (x_1 + x_2) - y_1$;

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2} \qquad \textbf{(7)}$$

Définition 9 :
Le groupe abélien E (K) des points K - rationnels d'une courbe elliptique E sur un corps K est le groupe de Mordell - Weil de la courbe elliptique E .

6– 3 Points d'ordre fini du groupe de Mordell – Weil E (K) :

Selon la théorie des groupes , un point P d'ordre m est un point P du groupe abélien E(K) qui satisfait la relation $m P = 0_E$ .Ce symbole m P désigne les sommes :

m P = P + … + P , m fois P si m > 0 ;

m P = (- P) + … + (-P) , (- m) fois - P si m < 0 ;

et 0P = O_E si m=0

Proposition 8 :
Pour un entier m , l'ensemble E (K) [m] des points P de la courbe elliptique E qui sont d'ordre m est un sous groupe du groupe E (K) .

Preuve :
Par hypothèse , l'ensemble E (K)[m] est une partie du groupe abélien E (K) .

Soit 2 points P_1 et P_2 d'ordre m . Alors ils satisfont m P_1 = m P_2 = O_E

Cela implique la relation m (P_1 - P_2) = O_E . Il en résulte que la somme

P_1 - P_2 est un point de l'ensemble E (K) [m]= E [m] .

Il en résulte que cet ensemble est un sous groupe du groupe E (K) .

□

Définition 10 :
l'ensemble E (K) [m] = E[m] des points P du groupe abélien E (K) qui sont d'ordre m est le sous groupe de m –torsion de E .

Proposition 9 :
La réunion infinie $\bigcup_{m>0} E(K)[m] = T(E)$ *des sous groupes de m torsion du groupe E(K) , pour les entiers* $m \geq 0$ *est un sous groupe du groupe abélien de Mordell – Weil de la courbe elliptique E .*

Preuve :
La réunion infinie $T(E)$ des sous groupes E (K) [m] du groupe E(K) est un sous groupe du groupe E (K) . (théorème relatif aux sous groupes d'un groupe)

□

Définition 11 :
Le groupe de torsion de la courbe elliptique E est le groupe $T(E)$*, réunion infinie des sous groupes de m –torsion de E .*

6 - 4 Points mP et formules de Cassels :

Des formules ont été déterminer par J.W.S Cassels [17] pour une équation

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

Ces formules sont de la forme :

$$m(x, y) = \left(\Phi_m \,/\, \Psi_m^2 \,,\ \omega_m \,/\, \Psi_m^3 \right)$$

Les Φ_m , ω_m *et* Ψ_m sont des polynômes en x , y , A , B . Ces polynômes sont de la forme :

$\Psi_1 = 1$, $\Psi_2 = 2y$.

$\Psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$,

$\Psi_4 = 4y\,(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4Abx - A^3 - 8B^2)$

Une relation de récurrence permet de calculer les autres polynômes :

$\Psi_{2m+1} = \Psi_{m+2}\,\Psi_m^3 - \Psi_{m-1}\,\Psi_{m+1}^3$; $(m \geq 2)$.

$2y\,\Psi_{2m} = \Psi_m\,(\Psi_{m+2}\,\Psi_{m-1}^2 - \Psi_{m-2}\,\Psi_{m+1}^2)$; $(m \geq 3)$.

On introduit deux autres familles de polynômes Φ_m *et* ω_m par les deux récurrences :

$\Phi_m = x\,\Psi_m^2 - \Psi_{m+1}\,\Psi_{m-1}$; $(m \geq 2)$.

$4y\,\omega_m = \Psi_{m+2}\,\Psi_{m-1}^2 - \Psi_{m-2}\,\Psi_{m+1}^2$; $(m > 2)$.

7– Application à la famille de cubiques :

$$E_t : y^2 = x^3 + 2t^3x^2 + t^2x \qquad 1\text{-}1$$

Calcul des invariants :

Les coefficients a_i et b_i de cette équation sont égaux à :

$a_1 = a_3 = a_6 = 0$; $a_2 = 2t^3$; $a_4 = t^2$;

$b_2 = 8t^3$; $b_4 = 2t^2$; $b_6 = 0$; $b_8 = -t^4$ ***(8)***

Les coefficients c_4 et c_6 sont égaux à :

$c_4 = 16t^2(4t^4 - 3)$; et

$c_6 = 64t^5(-8t^4 + 9)$; ***(9)***

La formule 1-1 donne le discriminant :

$\Delta(E_t) = 64t^6(t^4 - 1)$; ***(10)***

et l'invariant modulaire :

$$j(E_t) = \frac{64(4t^4-3)^3}{(t^4-1)} \qquad (11)$$

Coordonnées des points P_1+P_2 pour $P_1 \neq \pm P_2$ et du symétrique $-P$ du point P :

Les formules (6) et (7) précédentes impliquent les coordonnées de la somme P_1+P_2 de deux points $P_1 \neq \pm P_2$:

$x(P_1 + P_2) = \lambda^2 - 2t^3 - x_1 - x_2$;

$y(P_1 + P_2) = -\lambda^3 + (2t^3 + 2x_1 + x_2)\lambda - y_1$; **(12)**

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

Le symétrique - P du point P est calculé avec les formules (7) :

$-P = -(x, y) = (x, -y)$ **(13)**

Coordonnées des points 2P pour la famille 1-1 :

L'équation 1-1 donne la dérivée y' de y :

$$y' = \frac{3x^2+4t^3x+t^2}{2y}$$

Les calculs donnent les coordonnées du point 2P :

$x(2P) = y'^2 - 2t^3 - 2x$;

$$x(2P) = \frac{1}{(2y)^2}\left[x^4 + 8t^3x^3 + 2t^2(8t^4-1)x^2 + 8t^5x + t^4\right]$$

$y(2P) = -y'^3 + (2t^3 + 3x)y' - y$; **(12)**

t est un nombre rationnel .

Les points $P = (x, y)$ de 2 torsion de la courbe elliptique E_t ont pour coordonnées les solutions du système des 2 équations algébriques :

$$\begin{cases} 2y = 0 \\ y^2 = x^3 + 2t^3x^2 + t^2x \end{cases} \qquad (1)$$

La factorisation du deuxième membre dans (1) implique :

$x^3 + 2t^3x^2 + t^2x = x(x^2 + 2t^3x + t^2)$ **(2)**

Le calcul du discriminant δ ' du polynôme $x^2 + 2\,t^3\,x + t^2$ donne

$\delta' = t^6 - t^2 \geq 0$ ***(3)***

(2) et (3) impliquent $x\,(\,x^2 + 2\,t^3\,x + t^2\,) = x(x+t(t^2+\sqrt{t^4-1}))(x+t(t^2-\sqrt{t^4-1}))$

Les deux racines $x = -\,t(t^2 \pm \sqrt{t^4-1})$ du polynôme $x^2 + 2\,t^3\,x + t^2$ sont positives à la condition $-\,t(t^2 \pm \sqrt{t^4-1}) \succ 0$ et $\Delta(E_t) = 64\,t^6\,(t^4-1) \neq 0$, cela implique les valeurs $t \prec -1$

.

Tableau des coordonnées des 3 points de 2 – torsion de E_t :

x	*0*	x_1	x_2
y	*0*	*0*	*0*

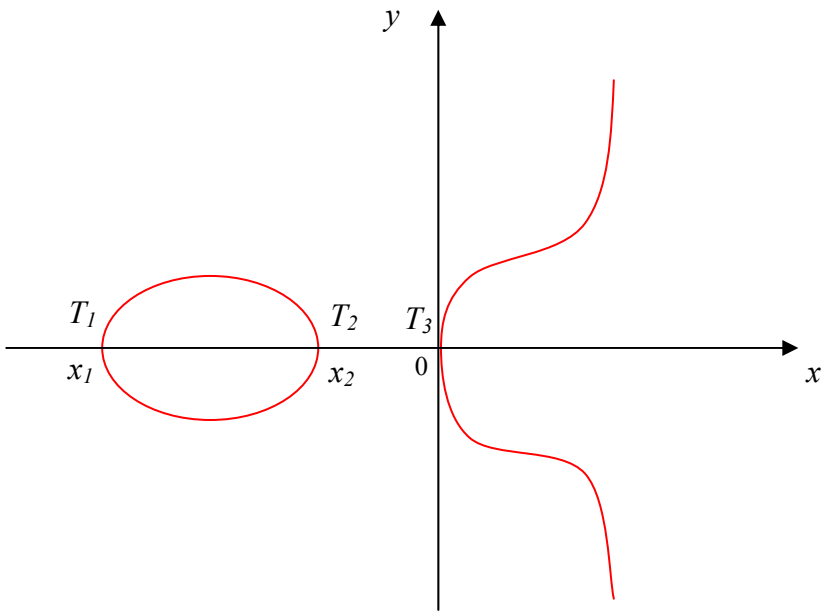


Figure 4

Il y a 3 points de 2 – torsion
(0,0) , T_1 , T_2

Coordonnées du point 3P = 2P+P pour une courbe elliptique

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

Le point 3P est calculé avec la décomposition 3P = 2P + P:

$x(3P) = x(2P+P) = \lambda^2 + a_1\lambda - a_2 - x_{2P} - x_P$; **(13)**

$$\lambda = \frac{y_{2P} - y_P}{x_{2p} - x_P}$$

avec $x(2P) = y'^2 + a_1 y' - a_2 - 2x$ et $y' = \dfrac{3x^2 + 2a_2 x + a_4 - a_1 y}{2y + a_1 x + a_3}$;

Le point 3P est un point d'ordonnée :

$y(3P) = -\lambda^3 - 2a_1\lambda^2 + (a_2 - a_1^2 + 2x_{2P} + x_P)\lambda + a_1 a_2 - a_3 + a_1(x_1 + x_2) - y_{2P}$ **(14)**

avec $y(2P) = -y'^3 - 2a_1 y'^2 + (a_2 - a_1^2 + 3x) y' + a_1 a_2 - a_3 + 2a_1 x - y$;

x et y sont les coordonnées du point P= (x ,y)

Coordonnées du point 4P = 2(2P) :

Le point 4P est un point d'abscisse :

$x(4P) = y'^2 + a_1 y' - a_2 - 2x_{2P}$; **(15)**

Le point 4P est un point d'ordonnée :

$y(4P) = -y'^3 - 2a_1 y'^2 + (a_2 - a_1^2 + 3x_{2P}) y' + a_1 a_2 - a_3 + 2a_1 x_{2P} - y_{2p}$; **(16)**

Coordonnées des points 3P = 2P+P et 4P = 2(2P) pour la famille de courbes elliptiques :

E_t : $y^2 = x^3 + 2t^3 x^2 + t^2 x$:

Les formules (13) et (14) impliquent :

$y' = \dfrac{3x^2 + 4t^3 x + t^2}{2y}$, $x(2P) = y'^2 - 2t^3 - 2x$ et $y(2P) = -y'^3 + (2t^3 + 3x) y' - y$

t est un nombre rationnel .

$x(3P) = \lambda^2 - 2t^3\lambda - a_2 - x_{2P} - x_P$;

$y(3P) = -\lambda^3 + (2t^3 + 2x_{2P} + x_P)\lambda - y_{2P}$

avec $\lambda = \dfrac{y_{2P} - y_P}{x_{2p} - x_P}$

Les formules (15) et (16) impliquent :

$x(4P) = y'^2 + a_1 y' - a_2 - 2 x_{2P}$;

$y(4P) = - y'^3 + (2 t^3 + 3x_{2P}) y' - y_{2p}$

Proposition10 :

Soit la famille de cubiques d'équation de Weierstrass $E_t : y^2 = x^3 + 2t^3 x^2 + t^2 x$

1) les cubiques sont singulières pour les valeurs de t qui satisfont $t^6 (t^4-1) = 0$.

2) les cubiques sont des courbes elliptiques pour les valeurs de t qui satisfont $t^6 (t^4-1) \neq 0$.

Corollaire :

Soit l'hypothèse de la proposition :

1) La Cubique E_t *est une courbe elliptique qui coupe l'axe Ox en 3 points distincts si et seulement si* $t^4 \succ 1$.

2) La Cubique E_t *est une courbe elliptique qui coupe l'axe Ox en un seul point si et seulement si* $t^4 \prec 1$.

Exemples :

1) La courbe $E_2 : y^2 = x^3 + 16 x^2 + 4 x$ coupe Ox en 3 points .

2) La courbe $E_{\frac{1}{4}} : y^2 = x^3 + \dfrac{1}{32} x^2 + \dfrac{1}{16} x$ coupe l'axe Ox en un seul point.

Calcul du discriminant $\Delta(E_t)$ et de l'invariant $c_4(E_t)$ de E_t *:*

$\Delta(E_t) = 64\, t^6 (t^4-1)$

$\Delta(E_t) = 0$ si $t = 0, \pm 1, \pm i$ dans le corps C des nombres complexes . ***(2)***

et $\Delta(E_t) = 0$ si $t = 0, \pm 1$ dans le corps Q des nombres rationnels .

$\Delta(E_t) \succ 0$ si $|t| \succ 1$ alors $t = \pm 2, \pm 3, \pm 4, \ldots$ ***(3)***

$\Delta(E_t) \prec 0$ si $|t| \prec 1$ alors $t = \pm \dfrac{1}{2}, \pm \dfrac{2}{3}, \pm \dfrac{3}{5}, \pm \dfrac{1}{10}, \ldots$ ***(4)***

L'invariant $c_4(E_t) = 16\, t^2\, (4\, t^4 - 3)$

$c_4(E_t) = 0$ si $t=0$,ou $|t| = \sqrt[4]{\frac{3}{4}}$ dans le corps R des nombres réels .

$c_4(E_t) \neq 0$ si non , $t = \pm 1, \pm 2, \pm \frac{3}{4}, \pm \sqrt{2}, \pm \frac{2}{7}, \ldots$ dans le corps R des nombres réels .

Exemple de cubique E_t possédant un nœud :

Pour t=-1 la cubique est singulière et elle a pour équation :

$E_{-1} : y^2 = x^3 - 2x^2 + x$

Calcul des invariants :

$\Delta(E_{-1}) = 0$ et $c_4 = 67 \times 4 \neq 0$.

D'après le corollaire 1 , cette cubique E_{-1} n'est pas elliptique ; elle admet un nœud S .

Le calcul donne les cordonnées du nœud

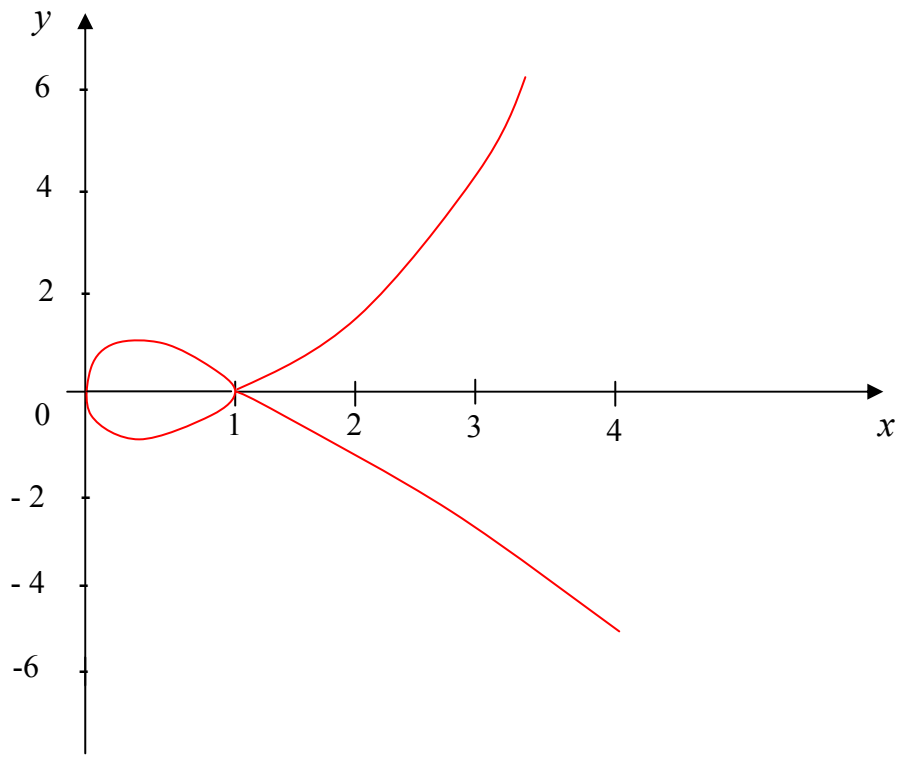
S = (1 , 0) .

Tableau de quelques coordonnées de points (x , y) de la courbe E_{-1} :

x	0	1	2	3	4	5
y^2	0	0	2	12	36	80
y	0	0	$\pm\sqrt{2}$	$\pm 2\sqrt{3}$	± 6	$\pm\sqrt{80}$

Ces points ont des coordonnées dans le corps $K = Q(\sqrt{2}, \sqrt{3}, \sqrt{5})$

Figure 1 :



Exemple de cubique E_t possédant un point de rebroussement :

Pour t=0 la cubique a pour équation $E_0 : y^2=x^3$

Les Calculs donnent les invariants :

$\Delta(E_0) = 0$ et $c_4 = 0$

Il en résulte que la cubique E_0 n'est pas elliptique .

Elle possède un point de rebroussement S .

Les coordonnées de ce point S sont les solutions du système $F(x,y) = F'_x = F'_y = 0$.

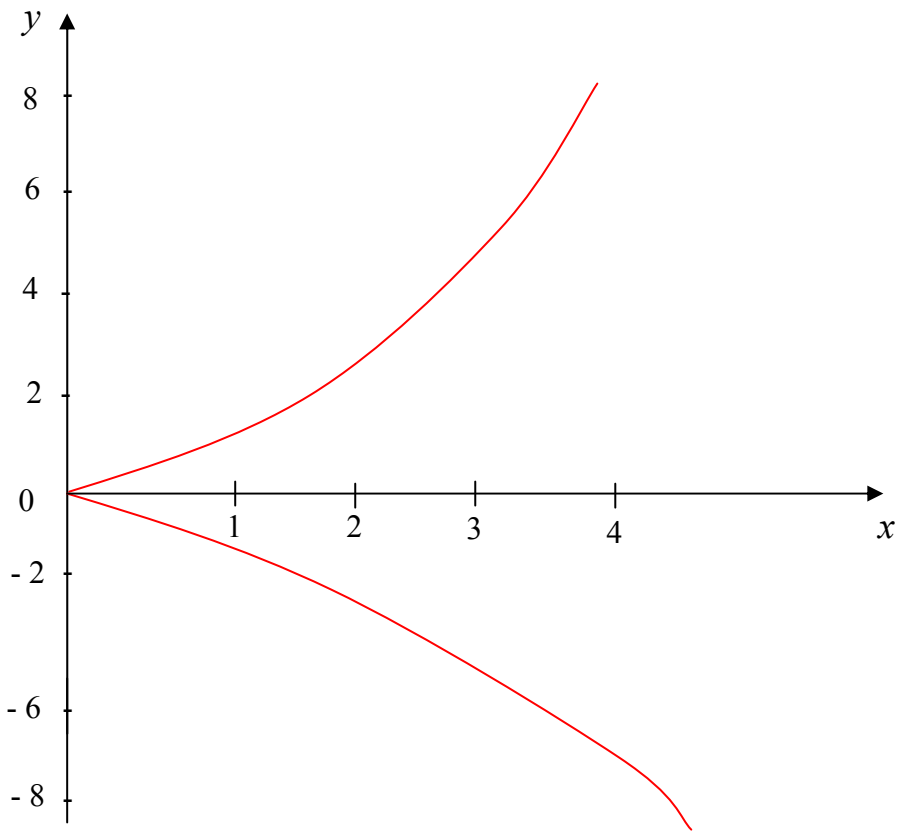
On trouve le point S = (0, 0).

Tableau de quelques coordonnées de points (x , y) de la courbe E_0 :

x	0	1	2	3	4	5	6
y^2	0	1	8	27	64	125	216
y	0	± 1	$\pm 2\sqrt{2}$	$\pm 3\sqrt{3}$	± 8	$\pm \sqrt{125}$	$\pm \sqrt{216}$

Ces points ont des coordonnées dans le corps K = Q ($\sqrt{2},\sqrt{3},\sqrt{5}$)

Figure 2 :



Exemple de courbe elliptique de $\Delta(E_t) > 0$

(1) et la formule (3) impliquent :

Pour t=2 la courbe elliptique E_2 a pour équation :

$E_2 : y^2 = x^3 + 16\,x^2 + 4\,x$

Calcul du discriminant :

$\Delta(E_2) = 2^{12}(2^4-1) \succ 0$ pour car $K \neq 2, 3$ et 5

Résolution de l'équation diophantienne: $x^3+16x^2+4x=0$ ***(1)***

(1) implique $x(x^2+16x+4)=0$

Les calculs donnent trois points d'intersection de la courbe E_2 avec l'axe Ox :

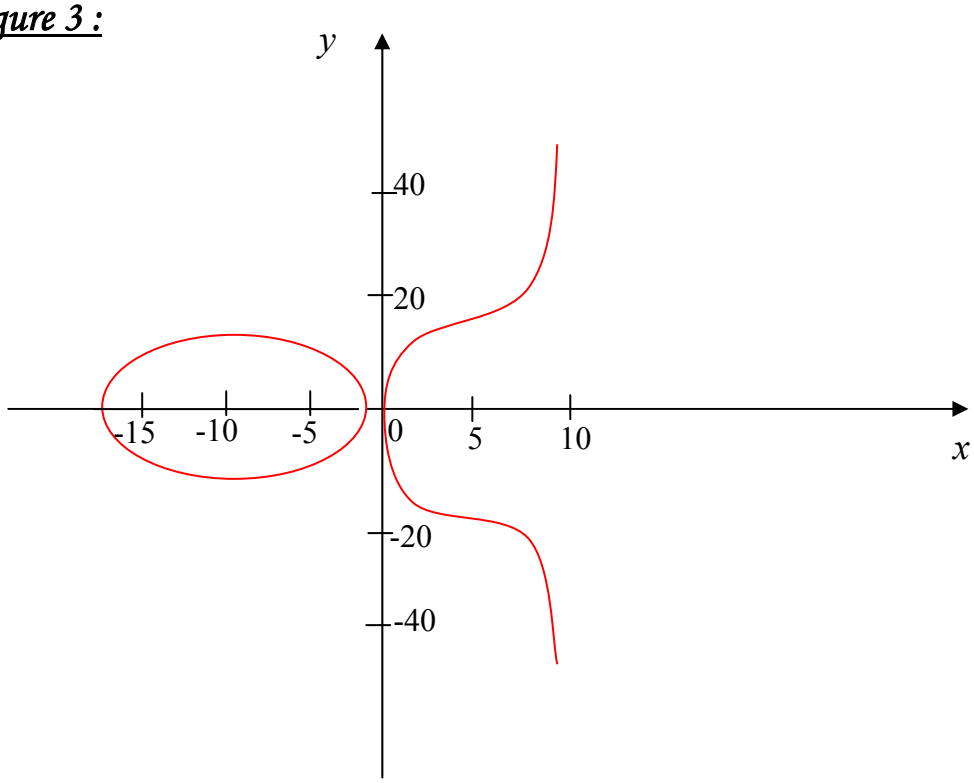
$T_1=(0,0)$,$T_2=(-8-2\sqrt{15},0)$ et $T_3=(-8+2\sqrt{15},0)$ dans le corps $K = Q(\sqrt{21},\sqrt{5},\sqrt{61})$

Tableau de quelques coordonnées de points (x , y) de la courbe E_2 :

x	$-8-2\sqrt{15}$	$-8+2\sqrt{15}$	0	1	2	3
y^2	0	0	0	21	80	183
y	0	0	0	$\pm\sqrt{21}$	$\pm4\sqrt{5}$	$\pm3\sqrt{61}$

Ces points ont des coordonnées dans le corps $K = Q(\sqrt{21},\sqrt{5},\sqrt{61})$

Figure 3 :



Pour t=3 la courbe elliptique E_3 a pour équation :

$E_3 : y^2 = x^3+54x^2+9x$

Calcul du discriminant :

$\Delta(E_3) = 2^6 \times 3^6(3^4-1) > 0$ pour car $K \neq 2, 3$ et 5 .

Résolution de l'équation diophantienne: $x^3+54x^2+9x=0$ ***(1)***

(1) implique $x(x^2+54x+9)=0$

Les calculs donnent trois points d'intersection de la courbe E_2 avec l'axe Ox :

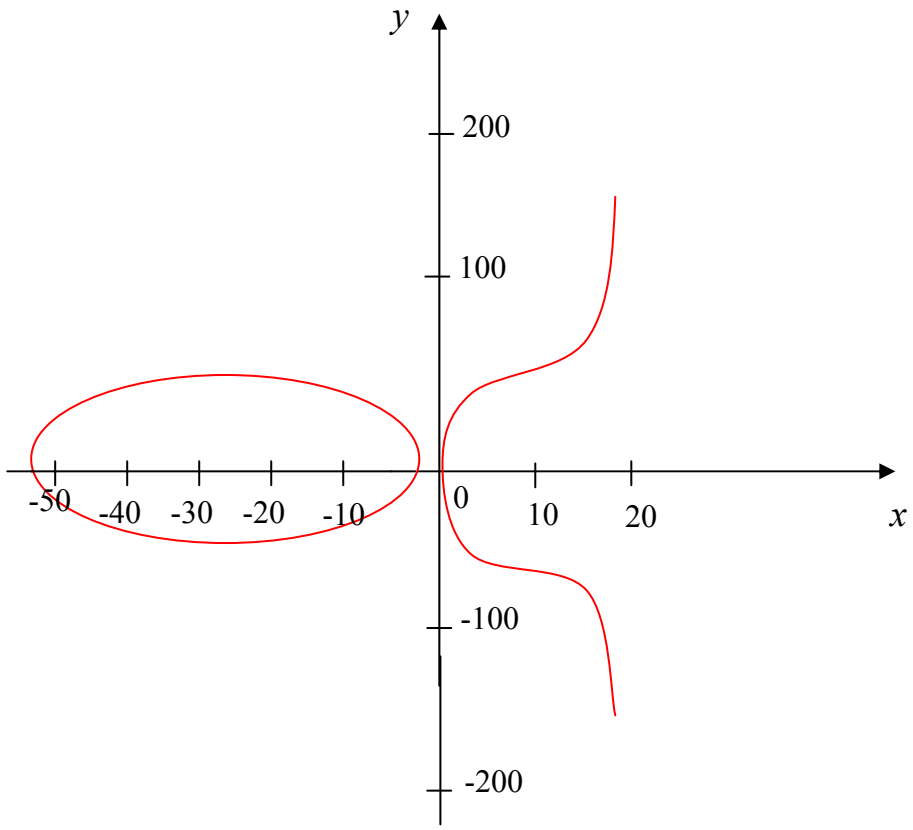
$T_1=(0,0)$,$T_2=(-27-12\sqrt{5},0)$ et $T_3=(-27+12\sqrt{5},0)$ dans le corps $K = Q(\sqrt{2},\sqrt{3},\sqrt{11})$

Tableau de quelques coordonnées de points (x , y) de la courbe E_3 :

x	-4	-3	-2	-1	$-27+12\sqrt{5}$	0	1
y^2	764	432	82	44	0	0	64
y	$\pm\sqrt{764}$	$\pm\sqrt{432}$	$\pm\sqrt{82}$	$\pm2\sqrt{11}$	0	0	±8

Ces points ont des coordonnées dans le corps K = Q ($\sqrt{2},\sqrt{3},\sqrt{11}$)

Figure 4 :



Exemples de courbes elliptiques de discriminant $\Delta(E_t) < 0$:

Pour $t=\frac{1}{4}$ *la courbe elliptique* $E_{\frac{1}{4}}$ *a pour équation :*

$E_{\frac{1}{4}}$: $y^2=x^3+\frac{1}{32}x^2+\frac{1}{16}x$.

Calcul du discriminant :

$\Delta(E_{\frac{1}{4}})= 64\,(\frac{1}{4})^6\,((\frac{1}{4})^4-1) \prec 0$ pour car $K \neq 2,3,5,17$

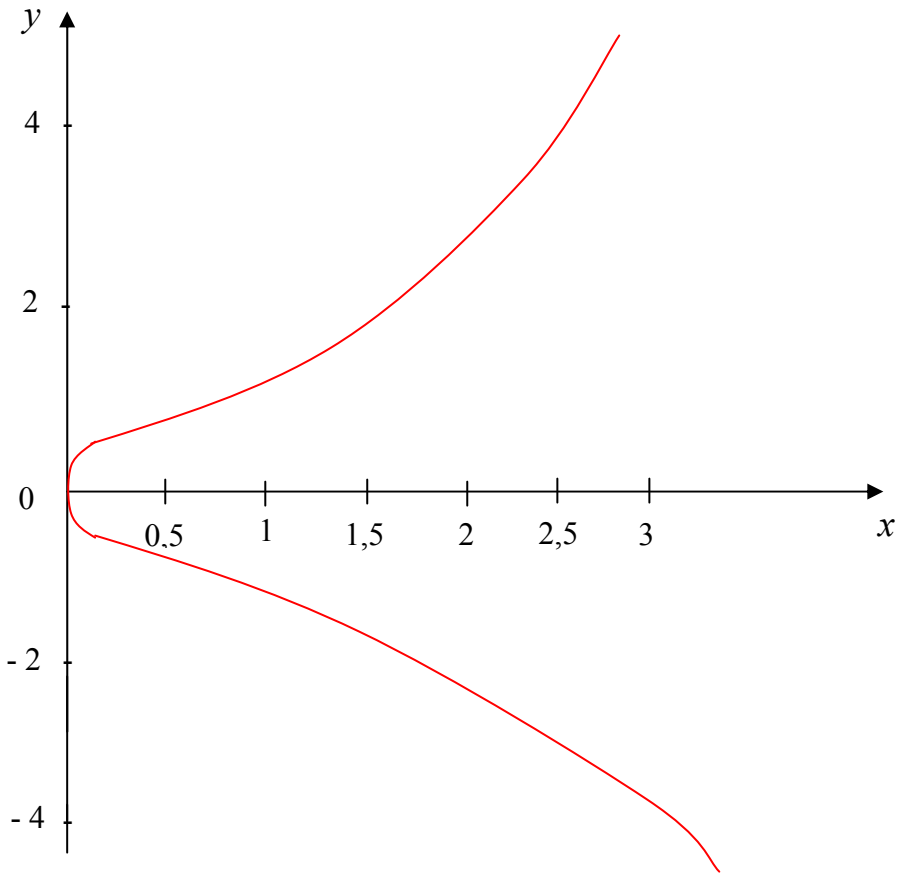
D'après le corollaire 2 , la courbe $E_{\frac{1}{4}}$ coupe l'axe en un seul point T=(0,0) .

Tableau de quelques coordonnées de points de la courbe $E_{\frac{1}{4}}$ *:*

x	0	1	2	3
y^2	0	35/32	33/4	879/32
y	0	$\pm\sqrt{35/32}$	$\pm\sqrt{33/4}$	$\pm\sqrt{879/32}$

Ces points ont des coordonnées dans le corps K = Q ($\sqrt{35},\sqrt{33},\sqrt{3}$) .

Figure 5 :



Pour $t = \frac{1}{2}$ *la courbe elliptique* $E_{\frac{1}{2}}$ *a pour équation :*

$E_{\frac{1}{2}} : y^2 = x^3 + \frac{1}{4}\ x^2 + \frac{1}{4}\ x$.

Calcul du discriminant :

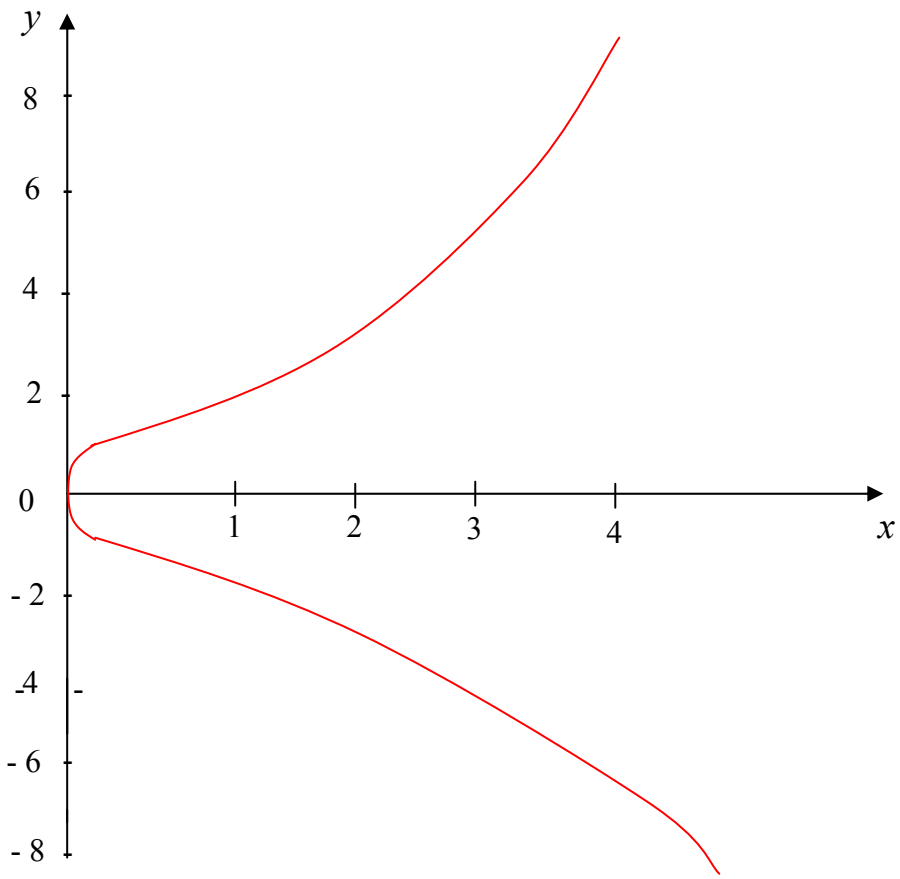
$\Delta\,(E_{\frac{1}{2}}) = 64\,(\frac{1}{2})^6\,((\frac{1}{2})^4 - 1) \prec 0$ pour car $K \neq 2$

D'après le corollaire 2 , la courbe $E_{\frac{1}{2}}$ coupe l'axe en un seul point T=(0,0) .

Tableau de quelques coordonnées de points de la courbe $E_{\frac{1}{2}}$ *:*

X	0	1	2	3	4
Y^2	0	3/2	19/2	30	69
Y	0	$\pm\sqrt{3/2}$	$\pm\sqrt{19/2}$	$\pm\sqrt{30}$	$\pm\sqrt{69}$

Figure 6 :



Chapitre II

Homomorphismes de courbes elliptiques :

Un homomorphisme de 2 courbes elliptiques E et E ' sur un corps K ,est
un homomorphisme de groupes abéliens E(K) et E '(K) :
u : E(K) $\rightarrow$ E '(K)
qui satisfait les formules d'homomorphisme de groupe
u (P + R) = u (P) + u (R) et u (O_E) = $O_{E'}$
pour les points à l'infini O_E de E et $O_{E'}$ de E ' ,

Les homomorphismes de courbes elliptiques se répartissent dans la classe des isomorphismes { E(K) $\rightarrow$ E '(K) } , la classe des automorphismes {E(K) $\rightarrow$ E (K) }et la classe des isogenies {E(K) $\rightarrow$ E'(K) }

II -1 Isomorphismes de courbes elliptiques :

Proposition 11 :
Soit une courbe elliptique E sur un corps K et sa transformée E ' par le changement linéaire de variables :
$x = u^2 x' + r \quad ; \quad y = u^3 y' + s u^2 x' + t$ **(1)**
avec des éléments $u \neq 0$, r , s et t dans le corps K

Alors les courbes elliptiques E et E ' sont isomorphes .

Preuve :

Soit une application
$\lambda : E(K) \rightarrow E'$(K) de valeur λ (x ,y)=(u^2 x ' + r, u^3 y ' + s u^2 x ' + t)
Les calculs permettent de vérifier les relations d'isomorphisme de groupes :

$\lambda\ (P_1+P_2) = \lambda(P_1) + \lambda\ (P_2)$, $\lambda(O_E) = O_{E'}$.

□

Le changement de variables (1) indiqué dans la proposition (11) donne l'équation de Weierstrass d'une courbe elliptique E'

$E' : y^2 + a'_1 x y + a'_3 y = x^3 + a'_2 x^2 + a'_4 x + a'_6$ ***(2)***

Relations entre les coefficients a_i et a'_i :

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

Relations entre les coefficients b_{2i} et b'_{2i} et entre c_{2i} et c'_{2i} :

$$\begin{aligned} u^2 b'_2 &= b_2 + 12 r ; \\ u^4 b'_4 &= b_4 + r b_2 + 6 r^2 ; \\ u^6 b'_6 &= b_6 + 2 r b_4 + r^2 b_2 + 4 r^3 ; \\ u^8 b'_8 &= b_8 + 3 r b_6 + 3 r^2 b_4 + r^3 b_2 + 3 r^4 ; \end{aligned}$$ ***(4)***

$u^4\ c'_4 = c_4$ et $u^6\, c'_6 = c_6$; ***(5)***

Relations entre les invariants $\Delta(E')$ et $\Delta(E)$, j (E ') et j (E) :

$u^{12}\ \Delta(E') = \Delta(E)$ et j (E) = j (E ') ; ***(6)***

La relation (6) implique la

Proposition12 :
1) Deux courbes elliptiques E et E' sur un corps K, qui sont isomorphes admettent des invariants modulaires égaux j (E) = j (E').
2) Deux courbes elliptiques E et E' sur un corps K, qui admettent des invariants modulaires égaux j (E) = j (E') sont isomorphes sur une clôture algébrique K_{alg} *du corps K* .

Preuve de (1) :

Soit deux courbes elliptiques E et E ' sur un corps K qui sont isomorphes. Alors

la $2^{iéme}$ formule (5) précédente implique j (E) = j (E ') .

□

Preuve de (2) :

Soit deux courbes elliptiques E et E ' sur un corps K qui ont même invariant modulaire j (E) = j (E ') et car(K) $\neq 2,3$. ***(1)***

Considérons les 3 cas : j (E) = 0 , j (E) = 1728 et j (E) $\neq 0, 1728$.

(1) Lorsque j (E) = j (E ') = 0 , la formule de l'invariant $j(E) = 1728\, c_4^3 \,/\, (c_4^3 - c_6^2)$

est valable pour des courbes elliptiques d'équations de Weierstrass ***(2)***

E : $y^2 = x^3 - 27\, c_4\, x - 54\, c_6$ et

E' : $y^2 = x^3 - 27\, c'_4\, x - 54\, c'_6$. ***(3)***

L'hypothèse j (E) = j (E ') = 0 implique les valeurs

$c_4 = c'_4 = 0$ et $c_6 \neq 0$, $c'_6 \neq 0$. ***(4)***

Les formules d'isomorphismes impliquent la relation :

$u^6\, c'_6 = c_6$. ***(5)***

Il en résulte 6 valeurs $u = (c_6/c'_6)^{1/6}$ dans une clôture algébrique du corps K . ***(6)***

Cela implique les 6 isomorphismes $x = u^2\, x'$; $y = u^3\, y'$. ***(7)***

(2) Lorsque j (E) = j (E ') = 1728 , les formules (2) impliquent les valeurs

$c_6 = c_6' = 0$ et $c_4 \neq 0, c_4' \neq 0$; ***(8)***

Les formules d'isomorphismes E (K) $\rightarrow$ E ' (K) et (8) impliquent

l'équation $u^4\, c'_4 = c_4$ ***(9)***

(9) admet 4 valeurs $u = (c_4/c'_4)^{1/4}$ dans une clôture algébrique de K . ***(10)***

Il en résulte 4 isomorphismes :

$x = u^2\, x'$, $y = u^3\, y'$. ***(11)***

(3) Lorsque j (E) = j (E ') $\neq$ 0, 1728, on pose t = j (E) ; ***(12)***

Alors la formule de l'invariant modulaire j (E) et (12) impliquent l'équation :

$$\frac{1728\, c_4^3}{c_4^3 - c_6^2} = \frac{1728\, c'^3_4}{c'^3_4 - c'^2_6} = t\,. \qquad \textbf{(13)}$$

L'hypothèse (12) implique $c_4 \neq 0$, $c'_4 \neq 0$, $c_6 \neq 0$ et $c'_6 \neq 0$ ***(14)***

La 1$^{\text{ére}}$ équation (13) implique l'équation :

$1728\ c_4^3 = t\ (c_4^3 - c_6^2)$ ***(15)***

(15)donne la relation $c_4^3(t-1728)= t\, c_6^2$ ***(16)***

Cette équation (16) admet la solution

$$c_4 = \frac{t}{t-1728} \quad , \quad c_6^2 = \frac{t^2}{(t-1728)^2} \qquad \textbf{(17)}$$

Cette solution satisfait la condition $\Delta(E) = c_4^3 - c_6^2 = \frac{t^2(1728)}{(t-1728)^3} \neq 0, \infty$

la 2éme équation (13) implique l'équation :

$$1728\, c'^3_4 = t\, (c'^3_4 - c'^2_6) \qquad \textbf{(18)}$$

On en déduit la solution :

$$u^4 c'_4 = c_4 \quad \text{et } u^6 c'_6 = c_6 \qquad \textbf{(19)}$$

Donc l'isomorphisme a pour valeurs :

$$x = u^2 x' \ , \ y = u^3 y' \text{ et } u = (c_4/c'_4)^{1/4} = (c_6/c'_6)^{1/6} \qquad \textbf{(20)}$$

L'équation de la courbe elliptique E est de la forme

$$E : y^2 = x^3 - 27\,\frac{tx}{t-1728} - 54\,\frac{t}{t-1728} \qquad \textbf{(21)}$$

□

(4) cas de car (K)= 3 :

On choisit une équation de Weierstrass avec des coefficients nuls

$a_1 = a_3 = a_4 = 0$

$$E : \ y^2 = x^3 + a_2 x^2 + a_6 \qquad \textbf{(1)}$$

Alors on obtient les valeurs $b_2 = a_2$, $b_4 = 0$, $b_6 = a_6$, $c_4 = a_2^2$, $b_8 = a_2 a_6$ et les

invariants $\Delta(E) = -a_2^3 a_6$ *et* $j(E) = \frac{a_2^3}{2a_6}$

L'hypothèse j (E) = j (E') ≠ 0 implique les valeurs

$$a_2^3 a_6' = a'^3_2 a_6 \neq 0 \qquad \textbf{(3)}$$

Le changement de variable qui préserve les équations (1) et (2) est :

$$x = u^2 x' \quad \text{et } y = u^3 y' \qquad \textbf{(4)}$$

Par les formules d'isomorphismes : $u^2 a'_2 = a_2$ ***(5)***

Il en résulte 2 valeurs $u = \pm(\frac{a_2}{a'_2})^{\frac{1}{2}}$ dans une clôture algébrique du corps K. ***(6)***

(6) implique 2 isomorphismes :

$$x = u^2 x' \quad \text{et } y = u^3 y'$$

L'hypothèse j (E) = j (E ') = 0

On choisit les courbes elliptiques d'équations de Weierstrass :

E : $y^2 = x^3 + a_2 x^2 + a_6$ ***(1)***

E' : $y^2 = x^3 + a'_2 x^2 + a'_6$ ***(2)***

Le changement de variable qui préserve les équations (1) et (2) est :

$x = u^2 x' + r$ *et* $y = u^3 y'$

On suppose $a_2 \; a'_2 \neq 0$ .Alors l'isomorphisme de E dans E' satisfait les deux relations :

$u^2 \; a'_2 = a_2$ et $u^6 \, a'_6 = a_6 + r^2 a_2 + r^3$

Ce système admet les solutions :

$$u = \left(\frac{a_2}{a'_2}\right)^{\frac{1}{2}} = \left(\frac{a_6 + r^2 a_2 + r^3}{a'_6}\right)^{\frac{1}{6}}$$

Il en résulte que les coefficients a'_i , a_i et r satisfont la relation :

$$a_2^{\,3} a'_6 = a'^{\,3}_2 \, (a_6 + r^2 a_2 + r^3)$$

Cas de carac(K)=2 : On choisit une équation de Weierstrass de la forme :

$E : y^2 + a_1 x y + a_3 y = x^3$

Alors on obtient les valeurs $c_4 = a_1^{\,4}$, $b_8 = 0$, $\Delta(E) = a_3^{\,4}$, $j(E) = \dfrac{a_1^{\,12}}{a_3^{\,4}}$

L'hypothèse j(E) = 0 implique $a_1 = a'_1 = 0$ et $a_3 \neq 0$

Alors une seule valeur $a_3 = 1$.

On prend une équation de Weierstrass de la forme :

E : $y^2 + y = x^3$ et E' : $y^2 + y = x^3$

L'hypothèse j(E) $\neq 0$ implique $a_1 = 1 = a_3$.

Il en résulte les équations :

E : $y^2 + x y + y = x^3$ et E' : $y^2 + x y + y = x^3$

□

II – 2 Isogénies de courbes elliptiques et endomorphismes :

Les isogénies de courbes elliptiques sont des homomorphismes de groupes abéliens $E(K) \rightarrow E'(K)$ qui sont surjectifs mais ne sont pas injectifs .

Définition12 :
Une isogénie de 2 courbes elliptiques E et E ' sur un corps K est un homomorphisme de groupes
$\lambda : E(K) \rightarrow E'(K)$ *qui satisfait les conditions :*
1) λ *est surjective*
2) Son noyau est un sous groupe fini du groupe E(K).
3) L'image de la somme $P_1 + P_2$ *est égale à* $\lambda(P_1 + P_2) = \lambda(P_1) + \lambda(P_2)$.
4) L'image de l'élément neutre O_E *de E est égale à l'élément neutre* $O_{E'}$ *de E' :* $\lambda(O_E) = O_{E'}$

Les formules d'addition $P_1 + P_2$ montrent que les coordonnées du point $P_1 + P_2$ sont des fractions rationnelles de la forme :

$$x(P_1 + P_2) = \frac{f(x,y)}{g(x,y)^2} \quad , \quad y(P_1 + P_2) = \frac{h(x,y)}{g(x,y)^3} \ .$$

Cela implique des formules d'isogénies de même nature.

On peut trouver un exemple dans [19]

A toute isogénie $\lambda : E \rightarrow E'$ sont associées les notions d'isogénie duale et de degré de l'isogénie .

Définition13 :
Soit une isogénie de courbes elliptiques
$\lambda : E(K) \rightarrow E'(K)$

Alors l'isogénie duale de λ *est l'homomorphisme*
$\hat{\lambda} : E'(K) \rightarrow E(K)$
de composées
$\lambda \circ \hat{\lambda}$ = *multiplication sur* $E'(K)$ *par le degré de* λ.
et $\hat{\lambda} \circ \lambda$ = multiplication sur E (K) par le degré de λ.

Définition14 :
Soit une isogénie
$\lambda : E(K) \rightarrow E'(K)$
de noyau un sous groupe F de E (K) . Le degré de l'isogénie λ *est égal à l'ordre du sous groupe F .*

Proposition 13 :
Soit une courbe elliptique E sur un corps K et un sous groupe fini F du groupe E (K) . Alors il existe une isogénie unique
$\lambda : E(K) \rightarrow E' = E(K)/F$ *de noyau F*
□

La multiplication par un entier rationnel m sur une courbe elliptique E est une isogénie .

Proposition 14 :
Soit une courbe elliptique E sur un corps K .
La multiplication

$$m_E : E(K) \rightarrow E(K)$$

par un entier naturel m est une isogénie dont le noyau est le sous groupe de m - torsion
$E(K)[m] = m_E^{-1}(O_E)$.

Preuve :

Cette multiplication m_E est un endomorphisme du groupe abélien E(K) qui satisfait les 4 conditions d'une isogénie .

□

Le degré de cette multiplication est déterminé par le

Corollaire :
La multiplication
$m_E : E(K) \rightarrow E(K)$
sur une courbe elliptique E par un entier m est une isogénie de degré m^2 .

Preuve :

Soit une courbe elliptique E sur un corps K et un entier rationnel m premier à la caractéristique de K .

La multiplication

$$m_E : E \rightarrow E$$

sur la courbe E par m est une isogénie qui admet une isogénie duale .

La théorie des morphismes de variétés implique la valeur du degré de l'isogénie m_E ; il est égal à m^2 .

□

Les isogénies de E(K) forment un anneau End (E) .

La structure de cet anneau sur K a été complètement déterminée par Deuring [4]

Proposition15 :
L'ensemble End (E) des endomorphismes d'une courbe elliptique E sur un corps K est l'un des 3 types suivants :
1) End (E) est isomorphe à Z ;
2)End (E) est un ordre d'une extension quadratique imaginaire du corps $\mathbb{Q}$ des nombres rationnels ;

3) End (E) est un ordre de l'algèbre des quaternions imaginaires sur le corps $\mathbb{Q}$ lorsque le corps K est de caractéristique non nulle.

Preuve de 1) :

La multiplication par un entier rationnel m est une isogénie .Il en résulte une bijection

$Z \to End(E)$,

$m \to t_m$

de valeur m+n $\to$ $t_{m+n} = t_m + t_n$ et mn $\to t_{mn} = t_m t_n$

donc cet end (E) est isomorphe à l'anneau $\mathbb{Z}$.

Dans les deux autre cas on utilise l'isomorphisme analytique complexe d'un tore

$\mathbb{C} / L$ sur une courbe elliptique E_L .

□

II – 3 Automorphismes d'une courbe elliptique :

Un automorphisme d'une courbe elliptique E est un endomorphisme bijectif du groupe E(K) de Mordell – Weil .

Proposition 16 :
L'ensemble Aut (E) des automorphismes d'une courbe elliptique E sur un corps K est un groupe d'ordre *un diviseur de 24. Cet ordre dépend de la caractéristique de K et de l'invariant modulaire j(E) .*
1) Lorsque j(E) $\neq 0$, 1728 alors le groupe Aut *(E) est d'ordre 2 .*
2) Lorsque j(E)=1728 et car (K) $\neq 2,3$ *alors* le groupe Aut *(E) est d'ordre 4 .*
5) Lorsque j(E) =0 et car (K) $\neq 2,3$ *alors* le groupe Aut *(E) est d'ordre 6 .*
6) Lorsque j(E) =0=1728 et car (K) =3 alors le groupe Aut *(E) est d'ordre 12 .*
7) Lorsque j(E) = 0 =1728 et car (K) =2 alors le groupe Aut *(E) est d'ordre 24 .*

Preuve de 1) :

Soit une courbe elliptique E sur un corps K de carac (K) $\neq 2,3$,

d'invariant modulaire j(E) , on choisit une équation de Weierstrass

$y^2 = x^3 + a_4 x + a_6$

L'invariant modulaire est égal à $\dfrac{4 \times 1728\, a_4^{\,3}}{4\, a_4^{\,3} + 27 a_6^{\,2}} =$ j(E)

L'hypothèse j(E) $\neq$ 0,1728 implique l'inégalité

$$\frac{4\times 1728\, a_4^{\,3}}{4\, a_4^{\,3}+27 a_6^{\,2}} \neq 0$$

Cette inégalité implique :

$a_4 \neq 0$ et $a_6 \neq 0$ ***(1)***

Nous choisissons un automorphisme :

$h_u : E(K) \to E(K)$

de valeur $h_u(x, y) = (u^2 x, u^3 y)$;

Relation d'isomorphisme entre a_i et a'_i :

$u^4 a'_4 = a_4$ et $u^6 a'_6 = a_6$ ***(2)***

L'hypothèse $a_4 = a'_4$ et $a'_6 = a'_6$ implique les valeurs

$u^4 = 1$ et $u^6 = 1$ ***(3)***

(2) et (3) impliquent $u^2 = 1$ ***(4)***

(4) implique $u = \pm 1$, soit deux automorphismes de E :

h_1 est l'automorphisme identique $h_1(x, y) = (x, y)$

h_{-1} est l'automorphisme symétrique $h_{-1}(x, y) = (x, -y)$

□

Preuve de (2) :

Les hypothèses j(E)=1728 et car(K) $\neq 2,3$ impliquent $a_6=0$ et $a_4 \neq 0$ dans la formule de $j(E)$.

Nous choisissons un automorphisme:

$h_u : E(K) \to E(K)$

de valeur $h_u(x, y) = (u^2 x, u^3 y)$;

Relation d'isomorphisme entre a_i et a'_i : $u^4 a'_4 = a_4$;

L'hypothèse $a_4 = a'_4$ implique $u^4 = 1$ ***(5)***

L'équation (5) admet 4 solutions $u = \sqrt[4]{1}$; il en résulte 4 automorphismes :

h_1, h_{-1}, h_i et h_{-i}

$h_i(x,y) = (-x, -i y)$ et

$h_{-i}(x, y) = (-x, i y)$ sont des multiplications complexes

h_1 est le morphisme identique

$h_{-1}(x,y) = (x, -y)$

Ces courbes elliptiques ont pour équation

E : $y^2 = x^3 - x$.

□

Preuve de (3) :

Soit un corps K de car(K) $\neq 2,3$ et une courbe elliptique E sur K.

d'invariant modulaire j(E)=0

Nous choisissons une équation de Weierstrass de la courbe E de la forme :

$y^2 = x^3 + a_4 x + a_6$ et

un automorphisme : $h_u : E(K) \to E(K)$

de valeur $h_u(x, y) = (u^2 x, u^3 y)$;

L'invariant modulaire $j(E) = \dfrac{4 \times 1728\, a_4^{\,3}}{4\, a_4^{\,3} + 27 a_6^{\,2}}$ et l'hypothèse j(E) =0

impliquent $a_4=0$ et $a_6 \neq 0$;

Relation d'isomorphisme entre a_i et a'_i :

$u^6 a'_6 = a_6$;

L'hypothèse $a_6 = a'_6$ implique $u^6 = 1$ ***(6)***

(6) implique 6 solutions $u = \sqrt[6]{1}$: $u = \pm 1$ *et* $u = \pm j, \pm j^2$

Il en résulte 6 automorphismes de *E*, h_1 est le morphisme identique ;

$h_{-1}(x,y) = (x, -y)$

$h_{\pm j}$ *et* $h_{\pm j^2}$ sont des multiplications complexes

□

Preuve de (4) :

Soit car (K) = 3 et j (E) = 0 = 1728

On choisit une courbe elliptique d'équation de Weierstrass :

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

Soit un automorphisme :

h: $E(K) \to E(K)$

de valeur $h_{u,r}(x, y) = (u^2 x + r, u^3 y)$;

Les formules d'isomorphisme impliquent les relations :

$u^4 a'_4 = a_4$

$u^6 a'_6 = a_6 + r a_4 + r^3$

Les relations $a_4 = a'_4$ et $a'_6 = a_6$ impliquent les deux équations :

$u^4 = 1$ et $u^6 = 1 + r\, a_4 + r^3$

L'équation $u^4 = 1$ admet 4 racines i , $i^2=-1$, $i^3=-i$ et $i^4 = 1$, ***(7)***

L'équation $r^3 + r\,a_4 + 1 - u^6 = 0$ admet 3 racines r_1 , r_2 ,r_3 , ***(8)***

Les K automorphismes $h_{u,r}$ dépendent des racines u , r_i (7) et (8)

Le groupe Aut(E) est donc le produit semi direct de 2 groupes

cycliques $\{i, i^2, i^3, i^4 = 1\} = C_4$

par le groupe de permutations $\{r_1, r_2, r_3\} = C_3$ des 3 racines .

Alors Aut (E) $\cong c_4 \times c_3$ est d'ordre 12 .

□

Preuve de (5) :

Soit les hypothèses j(E) = 0 =1728 et car (K) = 2 ***(1)***

Nous choisissons une équation de E de la forme :

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

et un automorphisme :

h: $E(K) \to E(K)$

de valeur $h_{u,s,t}(x, y) = \left(u^2 x + s^2, u^3 y + s u^2 x + t\right)$ ***(3)***

Il dépend de 3 paramètres u,s et t

Les relations d'isomorphisme entre coefficients a_i et a'_i de 2 courbes elliptiques isomorphes sont

$u^3 a'_3 = a_3 + s^2\, a_1 + 2t$ ***(4)***

$u^4 a'_4 = a_4 - s a_3 + 2s^2 a_2 - (t + s^3) a_2 + 3s^4 - 2st$ ***(5)***

$u^6 a'_6 = a_6 + s^2 a_4 + t a_3 + s^6 + t^2$ ***(6)***

Dans un corps de caractéristique 2 : ces relations se simplifient avec $2 \equiv 0$

L'hypothèse « h est un automorphisme » implique les relations $a'_i = a_i$ ***(7)***

Les formules (4) ,(5),(6) et (7) impliquent le système :

$$\begin{cases} a_3\left(u^3 + 1\right) = 0 \quad ; a_4\left(1 + u^4\right) + s a_3 + s^4 = 0, \\ a_6\left(1 + u^6\right) + s^2 a_4 + s^6 + t a_3 + t^2 = 0, \end{cases} \qquad \textbf{(8)}$$

La première équation admet trois racines $u = \sqrt[3]{1}$ qui sont permutées par un groupe C_3 d'ordre 3 ; ***(9)***

La deuxième équation admet 4 racines s_1, s_2, s_3, s_4 qui sont permutées par un

groupe C_4 d'ordre 4 ; ***(10)***

La troisième équation admet 2 racines t_1 et t_2 qui sont permutées par un

groupe C_2 d'ordre 2 ; ***(11)***

Les K automorphismes $h_{u,s,t}$ dépendent de ces racines u, s et t

Le groupe C_4C_2 est un groupe d'ordre 8 isomorphe au groupe des quaternions .Il est twisté par C_2 d'après les formules (8) .

Il en résulte que le groupe Aut(E) est d'ordre 24 , le groupe Aut (E) est donc le produit semi direct de ces 3 groupes isomorphes au produit du groupe H_8 des quaternions par un groupe C_3 d'ordre 3 .

$Aut(E) \cong H_8 \times C_3$.

□

II – 4 Application à la famille $E_t : y^2=x^3+2t^3 x^2+t^2x$,

Les coefficients a_i , b_i et c_i de cette équation sont égaux à :

$a_1 = a_3 = a_6 = 0$; $a_2 = 2t^3$; $a_4 = t^2$; ***(1)***

$b_2 = 8t^3$; $b_4 = 2t^2$; $b_6 = 0$; $b_8 = -t^4$ ***(2)***

$c_4 = 16t^2(4t^4 - 3)$; $c_6 = 64t^5(-8t^4 + 9)$ ***(3)***

L'invariant discriminant et l'invariant modulaire sont égaux à :

$$\Delta(E_t) = 64t^6(t^4-1) \quad ; \quad j(E_t) = \frac{64(4t^4-3)^3}{(t^4-1)} \qquad \textbf{(4)}$$

Pour obtenir les formules d'isomorphismes de la famille E_t avec une famille E'_t, on met l'équation de E_t sous la forme :

$$E_t : \; y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 . \qquad \textbf{(5)}$$

où les a_i sont donnés par les formules (1).

Les formules d'isomorphisme :

$$x = u^2 x' + r$$

$$y = u^3 y' + s u^2 x' + v$$

Transforment (5) en l'équation :

$$E'_t : \; y'^2 + a'_1 x' y' + a'_3 y' = x'^3 + a'_2 x'^2 + a'_4 x' + a'_6$$

Les formules (1) ,(2) , (3) et (4) impliquent :

(a) Les relations entre les coefficients a_i et a'_i sont :

$$
\begin{aligned}
& u\, a'_1 = a_1 + 2s = 2s \ ; \\
& u^2 a'_2 = a_2 - s\, a_1 + 3r - s^2 = 2t^3 + 3r - s^2 \ ; \\
& u^3 a'_3 = a_3 + r\, a_1 + 2v = 2v \ ; \\
& u^4 a'_4 = a_4 - s\, a_3 + 2r\, a_2 - (v + r s)\, a_1 + 3r^2 - 2sv = t^2 + 4r t^3 + 3r^2 - 2sv \ ; \\
& u^6 a'_6 = a_6 + r\, a_4 + r^2 a_2 - v\, a_3 - r v\, a_1 + r^3 - v^2 = r t^2 + 2 r^2 t^3 + r^3 - v^2 \ ;
\end{aligned}
\qquad \textbf{(6)}
$$

(b) Les relations entre les coefficients b_{2i} *et* b'_{2i} *et entre* c_{2i} *et* c'_{2i} *:*

$$
\begin{aligned}
& u^2 b'_2 = b_2 + 12r = 8t^3 + 12r \ ; \\
& u^4 b'_4 = b_4 + r\, b_2 + 6r^2 = 2t^2 + r\, 8t^3 + 6r^2 \ ; \\
& u^6 b'_6 = b_6 + 2r\, b_4 + r^2 b_2 + 4r^3 = 4r t^2 + 8 r^2 t^3 + 4r^3 \ ; \\
& u^8 b'_8 = b_8 + 3r\, b_6 + 3r^2 b_4 + r^3 b_2 + 3r^4 = -t^4 + 6 r^2 t^2 + 8 t^3 r^3 + 3r^4 \ ;
\end{aligned}
\qquad \textbf{(7)}
$$

$$u^4 c'_4 = 16 t^2 (4t^4 - 3) \quad \text{et} \quad u^6 c'_6 = 64 t^5 (-8t^4 + 9)$$

(c) Les relations entre les invariants $\Delta(E')$ *et* $\Delta(E)$ *,* $j(E')$ *et* $j(E)$ *:*

$$u^{12}\, \Delta(E') = 64 t^6 (t^4 - 1) \quad \text{et} \quad j(E') = \frac{64(4t^4 - 3)^3}{(t^4 - 1)} \ ;$$

Chapitre III

Valuations et Réductions

1 – Introduction :

La théorie des valuations a des applications dans plusieurs domaines comme la décomposition des idéaux, la ramification modérée, la ramification sauvage, les corps locaux, les corps p – adiques, les réductions des Courbes Elliptiques, les hauteurs, etc.

Cette théorie prend un chapitre dans les ouvrages de Théorie des Nombres (Hasse ,Weiss ,Lang ,Artin ,Iyanaga ,etc.)

2 - Valuations d'un corps :

Les auteurs ne font pas de différence entre « valuation » et « valeur absolue » .
Pour les démonstrations des propositions, nous renvoyons aux ouvrages cités ci-dessus .

Définition 1:
Une valuation d'un corps K est une fonction réelle du corps K, à valeurs dans l'ensemble $\mathbb{R}_+$ *des nombres réels* ≥ 0 .

$$v : K \to \mathbb{R}_+ \qquad \textbf{(1)}$$

qui satisfait les trois axiomes :

(v1) $v(x) \geq 0$ *pour tout élément* $x \neq 0$ *de K et* $v(x)=0$ *si et seulement si* $x=0$;

(v 2) $v(xy) = v(x)\, v(y)$ *pour tous éléments x et y de K ;*

(v 3) il existe une constante réelle $c \succ 0$ *telle que la relation*

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

Exemple1 :

1) K = $\mathbb{R}$ = corps des nombres réels et $v(x) = |x| = \max\{x,-x\}$

C'est la « valeur absolue » usuelle d'un nombre réel x .

Pour l'axiome (v3) , $v(x) \le 1$ implique $-1 \le x \le 1$ et $v(x+1) = |x+1| \le 2$.

Exemple2 :

K= $\mathbb{C}$ = corps des nombres complexes $z = a + ib$.

Alors $v(a+ib) = \sqrt{a^2+b^2}$ = module de z .

Pour l'axiome (*v3*) , $v(a+ib) \le 1$ *implique* $\sqrt{a^2+b^2} \le 1$,

$a^2+b^2 \le 1$ *et* $v(a+ib+1) = \sqrt{(a+1)^2+b^2} \le 2$.

Exemple3 :

K= corps et $v(x) = 1$ pour $x \neq 0$, $v(0) = 0$.

Pour l'axiome (*v3*) , $v(x)=1$ implique $v(x+1)=1$ pour $x+1 \neq 0$ *et*

$v(x+1)=0$ pour $x+1 = 0$.

C'est la valuation triviale d'un corps .

Exemple4 :

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

On choisit un nombre premier p et on pose $v(p) = p^{-1}$ *et* $v(q)=1$ pour tout nombre premier $q \neq p$; $v(0) = 0$

Tout nombre rationnel $\frac{a}{b}$ se met sous la forme : $\frac{a}{b} = p^r \frac{a'}{b'}$

avec p premier *à* *a'b'* .

Pour l'axiome (*v3*) , $v(x) \le 1$ implique $v(x+1) \le 1$

C'est la valuation p – adique du corps $\mathbb{Q}$.

Dans cette définition d'une valuation , l'axiome *v(3)* peut être remplacer par l'axiome de « l'inégalité triangulaire »

v(3') $v(x+y) \le v(x) + v(y)$.

Proposition 1:

Soit une valuation $v : K \to \mathbb{R}_+$ *d'un corps K. Alors, il existe une constante réelle* $c \succ 0$ *qui satisfait l'inégalité* $v(x+y) \le c \max\{v(x), v(y)\}$ *pour tous éléments x et y de K .*

Proposition2 :

Soit une valuation $v : K \to \mathbb{R}_+$ *d'un corps K. Alors ,*

1) v est un homomorphisme du groupe multiplicatif K dans le groupe multiplicatif des nombres réels positifs $\mathbb{R}_+^*$.*

2) v (-1) = v(1) =1 , v(-x) = v(x) , $v(x^{-1})=v(x)^{-1}$ et $v(x/y) = v(x)/v(y)$ pour tous éléments non nuls x et y de K .

∎

Proposition 3:

Toute valuation d'un corps fini est triviale.

Preuve :

Tout corps fini $\mathbb{F}_q$ à $q = p^s$ éléments est l'ensemble des zéros du polynôme $F(x) = x^q - x$.

Les éléments non nuls de $\mathbb{F}_q$ forment un groupe multiplicatif cyclique $\mathbb{F}_q^*$ à q -1 éléments : $\mathbb{F}_q^* = \{ a, a^2, \ldots, a^{q-1}=1 \}$.

Soit une valuation $v : \mathbb{F}_q \to \mathbb{R}_+$. Alors, la valuation $v(a^{q-1})$ s'obtient avec $a^{q-1} = 1$: $v(a^{q-1}) = v(1) = 1$;

Il en résulte la valeur $v(a) = \sqrt[q-1]{1}$; par définition des valuations , *v(a) est un nombre réel positif ; il en résulte v(a) =1*

Alors pour *v(a)* satisfait $v(p^{q-1}) = v(1)=1$; il en résulte *v(a)* =1 pour un générateur a de $\mathbb{F}_q^*$ et $v(x) = v(a^r)= 1$ pour tout élément x de $\mathbb{F}_q^*$.

∎

3 – Classification des valuations $v : K \to \mathbb{R}_+$:

Soit un corps K et l'ensemble *V(K)* des valuations de K . Ces valuations peuvent être classifier par l'axiome *(v3)*

Définition2 :

Une valuation $v : K \to \mathbb{R}_+$ est archimédienne lorsqu'elle satisfait l'axiome de l'inégalité triangulaire $v(x+y) \le v(x) + v(y)$, pour tous éléments x et y de K

Il en résulte que : $v(x) \le 1$ implique $v(x+1) \le 2$.

Définition3 :

Une valuation $v : K \to \mathbb{R}_+$ est non archimédienne lorsqu'elle satisfait « l'axiome du maximum » :

$v(x+y) \le \max\{v(x), v(y)\}$.

Il en résulte que $v(x) \leq 1$ *implique* $v(x+1) \leq 2.$

Les valuations non archimédiennes satisfont la :

Proposition 4 :

Soit une valuation $v : K \to \mathbb{R}_+$ *d'un corps K . Alors v est non archimédienne, si et seulement si , l'ensemble des valuations v(ne) des éléments ne=e+e+...+e de l'élément unité e du corps K , est borné pour tout entier rationnel n= 1,2,3...*

Pour une valuation non archimédienne , la valuation d'une somme se réduit à la valuation d'un seul élément.

Proposition 5:

Soit une valuation non archimédienne $v : K \to \mathbb{R}_+$ *d'un corps K . Alors :*

1) $v(x) \prec v(y)$ *implique* $v(x+y) = v(y);$

2) Soient n éléments $x_1, \ldots, x_n$ *de K de valuations satisfaisant :*

$v(x_t) \leq v(x_1)$ *pour* $t \succ 1$ *et* $v(x_1 + \ldots + x_n) \prec v(x_1).$

Alors $v(x_1) = v(x_r)$ *pour un certain entier* r , $1 \prec r \leq n$

4 – Topologie induite par une valuation sur un corps :

Définition 4 :

Un corps topologique est un corps K muni de la structure topologique de Hausdorff et sur lequel l'adition et la multiplication sont continues .

Les axiomes (v_2) *et* (v_3) *des valuations impliquent une distance*

$d : K^2 \to \mathbb{R}_+$ *de valeur*

$$d(x,y) = v(x-y)$$

Avec cette distance , le corps K devient un espace métrique .

Par définition, une topologie est de Hausdorff lorsque deux points distincts admettent deux voisinages séparés.

Valuations équivalentes :

Définition 5:

Deux valuations v_1 , v_2 , d'un corps K sont équivalentes lorsque la relation

$v_1(x) \prec 1$ *implique* $v_2(x) \prec 1$ *pour tout élément x de K .*

Il en résulte que des valuations équivalentes induisent la même topologie.

Cette équivalence est déterminée par la

Proposition 6:

Soient deux valuations v_1 et v_2 d'un corps K , équivalentes .

Alors 1) $v_1(x) = 1$ implique $v_2(x) = 1$ pour tout élément x de K .

2) il existe une constante réelle $c \succ 0$ telle que $v_2 = v_1^c$.

ſ

Définition 6 :

(1) Dans l'ensemble V(K) des valuations d'un corps K , les classes d'équivalence sont des diviseurs premiers (en anglais prime spot de K)

(2) La classe d'une valuation archimédienne est le diviseur premier infini ; il lui correspond une place infinie de K .

(3) La classe d'une valuation non archimédienne est un diviseur premier fini ; il lui correspond une place finie de K .

Ainsi l'ensemble $V(K)$ est la réunion de deux sous ensembles disjoints ; l'ensemble $V_\infty(K)$ des classes des valuations archimédiennes et l'ensemble $V_0(K)$ des classes des valuations non archimédiennes *de K :*

$$V(K) = V_\infty(K) \cup V_0(K)$$

Des formules d'approximations relient les classes de valuations inéquivalentes par le moyen des propositions suivantes

Proposition 7 :

Soit un nombre fini v_1 , ... ,v_n de valuations , non triviales , et inéquivalentes, d'un corps K . Alors il existe un élément x dans K qui satisfait les inégalités :

$v_1(x) \succ 1$ et $v_t(x) \prec 1$ pour t=2,3,...,n.

Tout élément y qui satisfait cette proposition est lié à *x* par $x = \dfrac{y}{(1+y)}$

Proposition 8 :

Soit un nombre fini v_1 , ... ,v_n de valuations , non triviales, et inéquivalentes, d'un corps K . A tout nombre réel $\varepsilon \succ 0$ et à tout système x_1 , .. , x_n de n éléments de K , on peut associer un élément a de K qui satisfait les inégalités :

$$v_t(a - x_t) \prec \varepsilon$$

ſ

Les valuations inéquivalentes du corps $\mathbb{Q}$ des nombres rationnels satisfont la

Formule du produit de Hasse : $\prod_p v_p(a) = 1,$

Pour tout nombre rationnel non nul a et pour tous les nombres premiers p , finis (valuations p – adiques) et infinis (valeur absolue usuelle)

Cette formule du produit se prolonge aux extensions finies de $\mathbb{Q}$.

Définition 7 :

Une valuation v d'un corps K est discrète lorsque le groupe des valeurs v(K) est discret .

5 – Parties d'un corps associées à une valuation non archimédienne de ce corps :

Nous indiquerons dans ce paragraphe quelques applications :
sous ensembles du corps K déterminés par v , application canonique , prolongement de v à une extension finie L de K , valuation additive , valuation discrète et uniformisante .

Les sous ensembles de K déterminés par v sont :

L'anneau de la valuation v :

$$O_v = \{a \in K; v(a) \leq 1\}.$$

C'est aussi l'anneau des v – entiers du corps K .

L'ideal maximal en v dans K :

$$\mu_v = \{ a \in K \; ; v(a) \prec 1 \}.$$

Le groupe des v – unités :

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

Le corps résiduel de K en v :

$$K_{res} = O_v / \mu_v$$

C'est l'anneau quotient d'un anneau de valuation par un idéal maximal.
Alors, selon Dedekind, l'application canonique
$O_v \to K_{res}$, $a \to classe\,de\,a$,
est la *place du corps en v* .

Ces 4 objets mathématiques liés à une valuation non archimédienne v ne sont pas définis pour une valuation archimédienne.

Toute valuation v d'un corps K se prolonge à une extension L de K , de degré fini [L : K] = n , par une valuation $v_L : L \to \mathbb{R}$, de valeur $v_L(\alpha) = [v(N_{l/K}\alpha)]^{\frac{1}{n}}$ pour tout élément α de L

Une valuation non archimédienne $v : K \to \mathbb{R}_+$ est discrète lorsque son groupe de valeurs *v(K)* est isomorphe à l'anneau $\mathbb{Z}$. Alors il existe un élément π dans K de valuation $v(\pi) = 1$

Définition 8 :
Cet élément π *, de valuation* $v(\pi) = 1$, est une uniformisante de v .

Alors tout élément a , non nul , de K , se met sous la forme unique : $a = u\pi^r$, où u est une v – unité

L'idéal maximal en v est de la forme $\mu_v = \pi O_v$.

Toute valuation v non archimédienne est un homomorphisme de groupes multiplicatifs K* et $\mathbb{R}^*_+$.

On peut lui associer une valuation non archimédienne additive

$\lambda : K \to \mathbb{R}$ par la formule :

$\lambda(a) = -\log(v(a))$ pour $a \neq 0$ et

$\lambda(0) = +\infty$.

Cette valuation additive est une valuation exponentielle. Elle satisfait les trois axiomes :

$(v_A.1)$ $\lambda(x) = -\log(v(a))$ pour $a \neq 0$ et $\lambda(0) = +\infty$;

$(v_A.2)$ $\lambda(xy) = \lambda(x) + \lambda(y)$ *pour tous éléments* x *et* y *non nuls du corps* K;

$(v_A.3)$ $\lambda(x+y) \geq \min(\lambda(x), \lambda(y))$

Lorsque $\lambda(x) \prec \lambda(y)$, l'axiome $(v_A.3)$ implique $\lambda(x+y) = \lambda(x)$

Les 4 objets associés à une valuation λ , non archimédienne , additive ,sont :

L'anneau de la valuation λ :

$$O_\lambda = \{x \in K ; \lambda(x) \geq 0\}.$$

C'est l'anneau des λ – entiers de K .

L'ideal maximal en λ :

$$\mu_\lambda = \{ x \in K \ ; \ \lambda(x) \succ 0 \ \}.$$

Le groupe des λ – unités :

$$U_\lambda = \{ x \in K \ ; \ \lambda(x) = 0 \}$$

Le corps résiduel en λ :

$$K_{res} = O_\lambda / \mu_\lambda$$

Toute valuation non archimédienne discrète $v : K \to \mathbb{R}_+$ permet de construire un corps local L , qui est le complété de K en *v*.

6 – Quelques anneaux de la théorie des nombres :

Définition 9 :

Un corps local est un corps complet pour un diviseur premier discret et qui possède un corps de classes résiduelles fini .

Définition 10 :

(1) *Un anneau local est un anneau A ,unitaire, commutatif, qui admet un seul idéal maximal M ; il satisfait les deux conditions :*

(a.l -1) tout élément x de l'ensemble A –M est inversible ;

(a.l -2) l'idéal maximal M est l'ensemble des éléments non inversibles de l'anneau .

Exemple : l'anneau $\mathbb{Z}_p$ est un anneau local engendré par un nombre premier p .

(2) *Un anneau semi - local est un anneau commutatif qui admet un nombre fini d'idéaux maximaux .*

(3) *Un anneau de valuation d'un corps K est un sous anneau A de K tel que ,pour chaque élément x de K , alors x dans A ou x^{-1} dans A .*

(4) *Un anneau de valuation discrète est un anneau principal qui admet un seul idéal premier ; cet idéal est l'idéal d'une valuation discrète non archimédienne ; Il en résulte que cet anneau est local .*

Proposition 9 :

Un anneau de valuation discrète satisfait les conditions équivalentes suivantes .

(1) c'est un anneau noethérien dont l'idéal maximal est engendré par un élément non nilpotent.

(2) c'est un anneau noethérien, intègre, intégralement clos ; qui possède un seul idéal premier .

(5) *Un anneau de Noether (anneau noethérien) est un anneau commutatif A qui satisfait les trois conditions équivalentes suivantes :*

(a.N-1) « condition de chaîne ascendante » : toute chaîne d'idéaux de A , strictement croissante, est finie :

$$I_1 \subset I_2 \subset I_3 \subset \cdots \subset I_n = I_{n+1} = \cdots$$

C'est donc une chaîne croissante, stationnaire, de longueur n ;

(a.N-2) « condition de la base finie » : Tout idéal I de A admet une base finie :

$$I = \omega_1 A + \cdots + \omega_t A + \omega_1 J + \cdots + \omega_t J,$$

où $\omega_1, \cdots, \omega_t$ est une base de I , J est une partie de lN ,

(a.N-3) « condition du maximum » : toute famille non vide d'idéaux de A

admet un élément maximal .

Exemple :

1) tout anneau principal est noethérien ;

2) tout anneau A[x] de polynômes en x sur un anneau noethérien A est un anneau noethérien . (C'est le théorème de Hilbert)

3) l'image homomorphe f(A) d'un anneau noethérien est un anneau noethérien .

Définition 11:

Un anneau d'Artin (anneau artinien) est un anneau qui satisfait la condition de « chaîne décroissante , stationnaire , d'idéaux ».

Indiquons quelques idéaux particuliers d'anneaux :

Définition 12 :

(1) *le transporteur d'un idéal I_1 dans un idéal I_2 est l'idéal $I_3 = [I_2 : I_1]$ formé des éléments x de l'anneau A tels que $x I_1 \subset I_2$;*

(2) *Un idéal M de A est maximal si l'inclusion d'idéaux $M \subset I$ implique $M = I$ ou $I = A$;*

(3) *Un idéal P de M est premier si la relation « $xy \in P$ » , pour deux éléments x et y de A , implique $x \in P$ ou $y \in P$;*

(4) *Le radical d'un anneau A est l'ensemble des éléments $x \in A$ tels que $1 + x y$ soit inversible pour tout élément $y \in A$;*

(5) *Le radical de Jacobson de A est l'intersection des idéaux maximaux de A ;*

(6) *Le nilradical de A est l'intersection des idéaux premiers de A ;*

(7) *Le spectre de A est l'ensemble des idéaux premiers de A ;*

(8) *<u>La racine d'un idéal I de A</u> est l'intersection des idéaux premiers de A qui contiennent l'idéal I ;*

7 – Réductions des courbes elliptiques :

Les valuations d'un corps commutatif , K , global , local , ou fini ,

permettent de réduire les coefficients de l'équation de Weierstrass d'une courbe elliptique :

$E : \; y^2 + a_1 x\, y + a_3\, y = x^3 + a_2 x^2 + a_4\, x + a_6$. ***(1)*** *où* les cinq coefficients a_1 , … , a_6 sont des éléments d'un corps K .

Pour la valuation p –adique sur le corps $\mathbb{Q}$ des nombres rationnels , la réduction modulo p est l'application :

$$\mathbb{Z} \quad \rightarrow \quad \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$$

$$n \quad \rightarrow \; n \text{ modulo } p.$$

Cette réduction modulo p induit une réduction modulo p sur les courbes elliptiques

E , de groupe de Mordell – Weil E ($\mathbb{Q}$*)*

$$E(\mathbb{Q}) \;\rightarrow\; \widetilde{E}(\mathbb{F}_p)$$

$$P=(x,y) \;\rightarrow\; \widetilde{P} = (\widetilde{x}, \widetilde{y}) \;,$$

Où $\widetilde{P}$ est le symbole de la réduction .

Exemple :

Courbe elliptique E d'équation de Weierstrass

$y^2 - 32\, x\, y + 104\, y = x^3 + 2857\, x^2 + 3514\, x - 8953$ ***(1)***

La réduction modulo 7 : $E(\mathbb{Q}) \;\rightarrow\; E(\mathbb{F}_7)$, réduit cette équation , dans le corps fini $\mathbb{F}_7$, à la forme

$\widetilde{E} : y^2 + 3xy + 6y = x^3 + x^2 \in \mathbb{F}_7[x\,,\,y]$ ***(2)***

Cette forme (2) est donc plus simple que la forme (1) .

Les invariants d'une courbe elliptique $E(\mathbb{Q})$ sont liés aux invariants de la courbe réduite $\widetilde{E}(\mathbb{F}_p)$ par cette réduction .

Dans le cas général d'un corps K , une valuation , v , non archimédienne et discrète , détermine un anneau A_v , des v –entiers de K , un idéal maximal M_v en v , un corps résiduel $A_v / M_v = K_{res}$ et une uniformisante π de valuation

$v(\pi) = 1$; alors $K_{rés} = A_v / \pi A_v$.

La réduction d'une courbe elliptique E modulo *v* est l'application :

$$E(K) \rightarrow \widetilde{E}(K_{rés})$$

$$P = (x,y) \rightarrow \widetilde{P} = (\widetilde{x}, \widetilde{y}) = \text{ point réduit .}$$

Puisque toute courbe elliptique E possède une structure de variété projective, abélienne, la théorie de la réduction modulo une valuation *v* s'étend à l'espace projectif $\mathbb{P}^2$; le point à l'infini O_E admet un point réduit .

Dans l'ensemble des valeurs prises par une valuation multiplicative, l'une des valeurs peut donc être minimale ; cette possibilité implique la notion « d'équation minimale »

Définition13 :

L'équation de Weierstrass d'une courbe elliptique E, définie sur un corps local K muni d'une valuation non archimédienne discrète v est de la forme :

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

Cette équation est minimale en la valuation v si elle satisfait les deux conditions

Les 5 coefficients a_i sont v- entiers et la valuation $v(\Delta)$ du discriminant est minimale .

Proposition 10:

Soit une courbe elliptique E sur un corps K muni d'une valuation discrète non archimédienne v ,d'invariants usuels $\Delta(E)$, $c_4(E)$, $c_6(E)$.

Son équation de Weierstrass est minimale en v si elle satisfait les conditions :

$v(a_i) \geq 0$, $v(\Delta(E)) \prec 12$ *et* { $v(c_4(E)) \prec 4$ *ou* $v(c_6(E)) \prec 6$ }.

Preuve :

Si les invariants $\Delta(E)$, $c_4(E)$, $c_6(E)$ ne satisfont pas ces conditions ,on fait le changement de coordonnées $(x,y) \rightarrow (u^2 x', u^3 y')$. On obtient une courbe elliptique isomorphe E' d'invariants :

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

Il en résulte les bornes 12,4 et 6 de la proposition.

∎

Toute réduction modulo une valuation *v* détermine 2 sous groupes particuliers dans le groupe E(K) de Mordell- Weil d'une courbe elliptique E :

$$E_0(K) = \left\{P \in E(K);\quad \widetilde{P}\ non\ \sin gulier\right\}$$
$$E_1(K) = \left\{P \in E(K); \widetilde{P} = \widetilde{O}_E\right\} = noyau\ de\ la\ réduction.$$

Proposition 11 :

Les groupes E(K) , E_0 (K) et E_1 (K) ,ci-dessus , forment une suite exacte de groupes abéliens.

$$0 \to E_1(K) \to E_0(K) \to \widetilde{E}_{ns}(K) \to 0$$

où $\widetilde{E}_{ns}(K)$ est l'ensemble des points non singuliers de E .

Preuve :

L'application $d_1 : E_1(K) \to E_0(K)$ est un homomorphisme de groupe de noyau $E_1(K)$ et d'image $E_0(K)$.

L'application $d_2 : E_0(K) \to E_{ns}(K)$ est un homomorphisme de noyau $E_1(K)$.

Les deux morphismes satisfont l'exactitude de cette suite . Pour les applications du début et de la fin de la suite , on prend les applications nulles :

$$0 \to O_E \quad et \quad O_E \to 0$$

∫

8 – Classification des réductions d'une courbe elliptique :

Cette classification repose sur la nature de la courbe réduite $\widetilde{E}$: courbe elliptique, cubique avec un nœud , cubique avec un point de rebroussement .

Définition14 :

Soit une courbe elliptique E sur un corps K , muni d' une valuation v non archimédienne discrète , et sa courbe réduite $\widetilde{E}$ avec une équation minimale de Weierstrass

(1) E a une <u>bonne</u> réduction en v si $\widetilde{E}$ est une courbe elliptique ; (sur le corps résiduel $\widetilde{E}(K_{res})$)

(2) E a une réduction <u>multiplicative</u> en v si $\widetilde{E}$ possède un nœud ;

(3) E a une réduction <u>additive</u> si $\widetilde{E}$ possède un point de rebroussement ;

(4) Les deux réductions multiplicatives et additives sont des réductions mauvaises .

(5) Une bonne réduction est une réduction <u>stable</u> ;

(6) Une mauvaise réduction multiplicative est une réduction semi stable ;
(7) Une mauvaise réduction additive est une réduction instable ;
(8) Une réduction multiplicative est décomposée lorsque les pentes des tangentes à la courbe au nœud sont des éléments du corps $K_{rés}$, si non, la réduction multiplicative est non décomposée .

La nature de la réduction d'une courbe elliptique peut être déterminer avec les trois invariants $\Delta(E)$, $c_4(E)$, $c_6(E)$.

Proposition12 :

Soit une courbe elliptique E, sur un corps K muni d'une valuation non archimédienne discrète v , et trois invariants usuels $\Delta(E)$, $c_4(E)$, $c_6(E)$ d'une équation de Weierstrass minimale :

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

Alors

1) E a une bonne réduction en v si et seulement si $\nu(\Delta) = 0$, alors la courbe réduite $\widetilde{E}$ ($K_{rés}$) est elliptique.

2) E a une réduction multiplicative en v si et seulement si $\nu(\Delta) \succ 0$ et $\nu(c_4) = 0$; alors la courbe réduite $\widetilde{E}$ ($K_{rés}$) a un nœud ;

3) E a une réduction additive en v si et seulement si $\nu(\Delta) \succ 0$ et $\nu(c_4) \succ 0$; alors la courbe réduite $\widetilde{E}$ ($K_{rés}$) a un point de rebroussement .

Preuve :
Dans la classification des cubiques planes C par leurs discriminants, nous avons montré (Chapitre I proposition 4)
que 1) C est une courbe elliptique si et seulement si $\Delta(C) \neq 0$

2) la cubique C a un nœud si et seulement si $\Delta(C) = 0$ et $c_4(C) \neq 0$;

3) la cubique C a un point de rebroussement si et seulement si $\Delta(C) = c_4(C) = 0$;

En prenant les valuations des invariants, on obtient les résultats de la proposition .

Γ

Corollaire :

Soit les hypothèses de la proposition.

1) Lorsque la courbe elliptique a une réduction multiplicative en v, la partie $\widetilde{E}_{ns}$ ($K_{rés}$) non singulière de la courbe réduite est isomorphe au groupe

multiplicatif $K_{rés}^{*}$ *;*

$$\widetilde{E}_{ns}(K_{rés}) \xrightarrow{\approx} K_{rés}^{*}$$

2) Lorsque la courbe elliptique a une réduction additive en v, la partie $\widetilde{E}_{ns}$ *(*$K_{rés}$*) est isomorphe au groupe additif* K^{+} *;*

$$\widetilde{E}_{ns}(K_{rés}) \xrightarrow{\approx} K_{rés}^{+}$$

Preuve de 1 :

Soit une courbe elliptique E avec un nœud S ; les deux tangentes à la courbe elliptique en S ont pour équations $y = \alpha_i x + \beta_i$, i=1,2

Considérons l'application de groupes abéliens .

$$E_{ns}(K) \xrightarrow{\lambda} K^{*}$$

de valeur $\lambda(x,y) = \dfrac{y - \alpha_1 x - \beta_1}{y - \alpha_2 x - \beta_2}$

Alors on peut vérifier que cette application est un isomorphisme de groupe.

∎

Preuve de 2 :

Soit une courbe elliptique E avec un point de rebroussement R ; la courbe elliptique admet une tangente unique en R , soit $y = \alpha x + \beta$ son équation

Considérons l'application de groupes abéliens :

$$\theta : E_{ns}(K\ ) \longrightarrow K^{+}$$

de valeur $\theta(x,y) = \dfrac{x - x_R}{y - \alpha x - \beta}$, où $R = (x_R\ ,\ y_R)$

Alors on peut vérifier que cette application θ est un isomorphisme de groupe.

∎

Les qualificatifs « multiplicative » et « additive » d'une mauvaise réduction proviennent de ce corollaire.

Exemples de réduction modulo le nombre premier p =11 :

1) Courbe elliptique d'équation de Weierstrass

$E : y^2 = x^3 + 11\,x^2 + 1,$

Les calculs donnent l'invariant discriminant $\Delta(E) = -16 \times 5351$;

Dans le corps $\mathbb{F}_{11}$, $\Delta(E) \not\equiv 0 \bmod 11$, la valuation v_{11} prend la valeur

$v_{11}(\Delta(E)) = v_{11}(-16 \times 5351) = 0$

Il en résulte que la courbe E a une bonne réduction en p =11 .

2) Courbe elliptique d'équation de Weierstrass :

$E : y^2 = x^3 + x^2 + 11$,

Les calculs donnent les deux invariants, le discriminant et le coefficient $c_4(E)$:

$\Delta(E) = -16 \times 11 \times 7 \times 43$ et $c_4(E) = 16.$

Dans le corps $\mathbb{F}_{11}$, ces 2 invariants satisfont les congruences :

$$\Delta(E) \equiv 0 \bmod 11 \qquad et \quad c_4(E) \not\equiv 0 \bmod 11.$$

La valuation v_{11} prend les valeurs

$$v_{11}(\Delta(E)) = v_{11}(-16 \times 11 \times 7 \times 43) = 1 \quad et \quad v_{11}(16) = 0$$

Par la proposition 12 , cette courbe elliptique a une réduction multiplicative .

3) Soit la courbe E d'équation de Weierstrass :

$E : y^2 = x^3 + 11$,

Les calculs donnent les deux invariants, le discriminant et le coefficient $c_4(E)$:

$\Delta(E) = -3^3 \times 2^4 \times 11^2$ et $c_4(E) = 0$

Dans le corps $\mathbb{F}_{11}$,ces deux invariants satisfont les congruences :

$$\Delta(E) \equiv 0 \bmod 11 \qquad et \quad c_4(E) \equiv 0 \bmod 11.$$

La valuation v_{11} prend les valeurs :

$$v_{11}(\Delta(E)) = 2 \quad et \quad v_{11}(c_4(E)) \succ 0 \ .$$

Par la proposition 12 , cette courbe elliptique a une réduction additive.

Définition15 :

Une courbe elliptique E sur un corps K a une bonne réduction potentielle en une valuation v s'il y a une extension finie L de K telle que E a une bonne réduction sur L .

La reconnaissance d'une bonne réduction potentielle peut être obtenue avec la :

Proposition13 :

Une courbe elliptique E sur un corps K a une bonne réduction potentielle en une valuation v de K si et seulement si son invariant modulaire j (E) est v entier

Une autre application des réductions est exprimé dans la

Proposition 14:

Soit une courbe elliptique E sur un corps K qui a une réduction multiplicative en une valuation v sur K ; soit le sous groupe

$E_0(K) = \left\{P \in E(K);\quad \widetilde{P} \text{ non sin gulier}\right\}$ *. Alors le groupe quotient*

$E(K)/E_0(K)$ *est cyclique d'ordre* $v(\Delta) = -\, v\,(j\,(E))$

Dans les autres cas , c'est un groupe fini d'ordre 4 au plus .

Preuve :

C'est un théorème de Kodaira – Néron .

∫

Corollaire :

Le sous groupe $E_0(K)$ *du groupe E(K) est d'indice fini .*

∫

9 – Application à la famille $E_t : y^2 = x^3+2t^3\,x^2+t^2x$ *1 - 1*

1) Pour t =2 , la courbe elliptique E_2 a pour équation de Weierstrass :

$E_2 : y^2= x^3 +16\, x^2+4\, x$

Les calculs donnent l'invariant discriminant :

$\Delta\,(E_2) = 2^{12}(2^4-1) = 2^{12} \times 15$

Dans le corps $\mathbb{F}_7$, $\Delta(E_2) \not\equiv 0 \bmod 7$, la valuation v_7 prend la valeur

$v_7\,(\Delta(E_2)) = v_7\,(\,2^{12} \times 15\,) = 0$

Il en résulte que la courbe E_2 a une bonne réduction en p =7 .

2) Pour t =3 , la courbe elliptique E_3 a pour équation de Weierstrass :

$E_3 : y^2= x^3 +54\, x^2+9\, x$

Les calculs donnent les deux invariants, le discriminant et le coefficient $c_4(E)$:

$\Delta(E_3) = 2^6 \times 3^6 \times (3^4-1)=2^{10} \times 3^6 \times 5$ et $c_4(E_3) = (2 \times 3)^4 \times 107$.

Dans le corps $\mathbb{F}_5$, ces 2 invariants satisfont les congruences :

$$\Delta(E_3) \equiv 0 \bmod 5 \qquad et \quad c_4(E_3) \not\equiv 0 \bmod 5.$$

La valuation v_5 prend les valeurs

$$v_5(\Delta(E_3))=v_5\ (2^{10} \times 3^6 \times 5\ ) =1 \ \ et \ \ v_5((2 \times 3)^4 \times 107)=0$$

Par la proposition 12 , cette courbe elliptique a une réduction multiplicative.

3) Pour t =5 , la courbe elliptique E_5 a pour équation de Weierstrass :

$E_5 : y^2= x^3 +250\ x^2+25\ x$

Les calculs donnent les deux invariants, le discriminant et le coefficient $c_4(E)$:

$\Delta(E_5) = 2^{10} \times 5^6 \times 3 \times 13$ et $c_4(E_5) =2^4 \times 5^2 \times 11 \times 227$.

Dans le corps $\mathbb{F}_2$, ces deux invariants satisfont les congruences :

$$\Delta(E_5) \equiv 0 \bmod 2 \qquad et \quad c_4(E_5) \equiv 0 \bmod 2.$$

La valuation v_2 prend les valeurs :

$$v_2(\Delta(E_5))=10 \succ 0 \ \ et \ \ v_2(c_4(E_5))=4 \succ 0 \ .$$

Par la proposition 12 , cette courbe elliptique a une réduction additive.

Chapitre IV

Quelques aspects du rang d'une Courbe elliptique

1 – Hauteurs sur le groupe de Mordell - Weil :

Selon S . Lang (Elliptic Curves , Diophantine Analysis) , Mordell a prouvé , en1922 , la conjecture de Poincaré selon laquelle , le groupe des points rationnels d'une courbe elliptique est de type fini .Weil a étendu , en 1929-1930 , ce résultat aux variétés abéliennes (Sur un théorème de Mordell , Bulletin Scientifique 54 (1930) 182- 191) .

C'est ce qui explique le nom de « groupe de Mordell- Weil » donné au groupe E(K).

La preuve de cette conjecture est formée de deux parties ; l'une est consacrée à la preuve que le groupe quotient , $E(K)/mE(K)$, est fini pour un certain entier rationnel m , « classiquement m=2 »

L'autre partie est une « descente infinie » construite avec une fonction hauteur .

La notion de « hauteur » est utilisée pour des polynômes, des corps de nombres, des espaces projectifs, des groupes abéliens. C'est donc la notion de « hauteur sur un groupe abélien » qui s'applique aux courbes elliptiques.

Définition 16 :

Une hauteur sur un groupe abélien , A , est une fonction h sur A , à valeurs réelles non négatives.

$$h : A \to [0, \infty[$$

qui satisfait les 3 axiomes :

(h_1) à tout élément P_0 de A , on peut associer une constante c_0

qui satisfait l'inégalité :
$h(P + P_0) \leq 2\, h(P) + c_0$ *pour tout point P de A ;*

(h_2 *) Il existe un entier rationnel* $m \geq 2$ *et une constante* c_1 *qui satisfont l'inégalité :*
$h(mP) \geq m^2\, h(P) - c_1$ *pour tout point P de A ;*

(h_3*) le nombre de points de A de hauteur bornée est fini.*

Dans cette définition, la valeur h(P) de la hauteur peut être fixer de plusieurs façons ; il en résulte l'existence de plusieurs hauteurs .

Définition 17 :

la fonction $h_{\mathbb{Q}} : \mathbb{Q} \to \mathbb{R}_+$ *, de valeur*

$h(\frac{a}{b}) = max \left\{ |a|, |b| \right\}$ *,où* $|\,.\,|$ *est le symbole de la valeur absolue sur le corps* $\mathbb{Q}$ *des nombres rationnels, satisfait les axiomes des hauteurs .*

Donc $h_{\mathbb{Q}}$ *est une hauteur sur le corps* $\mathbb{Q}$ **.**

Définition 18 :

la fonction $h_x : E(\mathbb{Q}) \to \mathbb{R}_+$ *, de valeur*

$h((x_p, y_p)) = \log h_{\mathbb{Q}}(x_p)$ *et* $h(O_E) = 0$ *,*

pour tout point $P=(x_p, y_p)$ *du groupe de Mordell- Weil* $E(\mathbb{Q})$ *et le point* O_E *à l'infini de E , satisfait les axiomes des hauteurs .*

C'est la <u>hauteur logarithmique</u> - <u>hauteur de Weil</u> - sur une courbe elliptique E .

Définition 19 :

<u>La hauteur canonique – hauteur de Neron Tate</u> sur une courbe elliptique E sur un corps K , est la fonction : $\hat{h} : E(K) \to \mathbb{R}_+$ *,*

de valeur $\hat{h}(P) = \frac{1}{\deg f} \lim_{n \to \infty} 4^{-n}\, h_f\left(2^n\, P\right)$ *,*

où f est une fonction paire , non constante , du corps K (E) et h_f *est la composée* $h \circ f$ *, avec* $h(P) = \log max \left\{ |a|, |b| \right\}$ *pour* $x_p = \frac{a}{b}$

Il existe des hauteurs liées à des valuations du corps K de base de la courbe elliptique .

Proposition 15 :

Soit une courbe elliptique E sur un corps K , une valuation v sur K et le groupe de Mordell – Weil $E(K_v)$ *de E , sur le complété* K_v *de K en v .*

Alors , il existe une fonction unique

$h_v : E(K_v) \to \mathbb{R}$

qui satisfait les propriétés :

1) h_v *est continue pour la topologie définie par v sur le groupe E(* K_v*) .*

2) $\lim_{P \to O_E} \left\{ h_v(P) + \frac{1}{2} v(x_P) \right\}$ *, existe ;*

où P= (x_P , y_P) *et* O_E *est le point à l'infini de E .*

3) Pour tout point P de E(K_v*) , qui n'est pas de 2 – torsion ,* h_v *satisfait la relation .*

$$h_v(2P) = 4\,h_v(P) + v\{(2y_P + a_1 x_P) + a_3\} - \frac{1}{2} v(\Delta(E))$$

où $\Delta(E)$ *est le discriminant de E ,*

a_1 *et* a_3 *sont 2 – coefficients de l'équation de Weierstrass de E ;*

4) h_v *satisfait la « loi du quasi – parallélogramme » .*

$$h_v(P+Q) + h_v(P-Q) = 2h_v(P) + 2h_v(Q) + v(x_P - x_Q) - \frac{1}{6} v(\Delta(E)).$$

Cette fonction h_v satisfait les axiomes d'une hauteur

Définition 20 :

h_v *est la* <u>*hauteur locale de E en v*</u> *.*

Définition 21 :

La <u>*hauteur canonique d'une courbe elliptique E*</u> *, sur un corps K , est la fonction.*

$\lambda : E(K) - \{O_E\} \to \mathbb{R}$ *de valeur*

$$\lambda(P) = \frac{1}{[K : \mathrm{Q}]} \sum_{v \in M_K} n_v\, h_v\,(P)$$

où M_K *est l'ensemble des valuations non équivalentes de K .*

et $n_v = [K_v : \mathrm{Q}_v]$ *désigne le degré local de K en v*

Dans cette définition, la valuation v peut être archimédienne, ou non archimédienne.

Plusieurs auteurs ont utilisé les hauteurs avec des formules propres. Citons les formules de Silvermann :

(1) <u>hauteur associée à une valuation archimédienne v</u> $\in M_K$

$h_v(P) = -\log v\left\{\Delta(L)^{1/2}\, e^{z\,\eta(z)/2}\ \sigma(z)\right\}$

où E est une courbe elliptique sur K ,

le groupe $E(K_v)$ est isomorphe analytiquement à un tore complexe $\mathbb{C}/L$, $\Delta(L)$

est le discriminant du réseau L .

Le point $P \in E(K_v)$ correspond à $z \in \mathbb{C}/L$,

$\eta(z)$ est la fonction Eta de Dedekind ,

$\sigma(z)$ est la fonction Sigma de Weierstrass ,

$$\eta(z) = q^{1/24}\prod_{1\le n}(1-q^n) \quad , \quad q = \exp(2\pi i z), u = \exp(2\pi i \tau)$$

$$\sigma(z) = \frac{1}{2\pi i}(q^{1/2} - q^{-1/2})\prod_{1\le n}\frac{(1-qu^n)(1-q^{-1}u^n)}{(1-u^n)^2} \quad ;$$

(2) <u>hauteur associée à une valuation non archimédienne v</u> $\in M_K$

$$h_v(P) = \max\left\{-\frac{1}{2}v(x_P), 0\right\} + \frac{1}{12}v(\Delta(E))$$

où $P = (x_P, y_P) \in E(K_v)$.

(3) <u>hauteur associée à une valuation non archimédienne v</u> $\in M_K$

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

où $N = -\mathrm{ord}_v(j(E))$, $1 \le n \le N-1$, j(E) est l'invariant modulaire de E et la courbe elliptique E admet une réduction multiplicative décomposée en *v* et P est un point de réduction non singulière .

$B_2(X) = X^2 - X + 16 = 2^{\text{ème}}$ polynôme de Bernoulli.

2 – Descente infinie sur le groupe abélien E(K) :

Le rang, r(E) = r, d'une courbe elliptique E, peut être théoriquement, calculer avec « le théorème de descente infinie », exposé dans la

Proposition 16 :

Soit un groupe abélien A. On suppose qu'il existe un entier rationnel $m \geq 2$ *tel que le groupe quotient A/mA soit fini . Alors ce groupe A est de type fini.*

Preuve :

Dans le groupe quotient $A/m\,A$ nous choisissons des représentants *:*

$T_1, \ldots, T_s$ ***(1)***

Nous construisons une suite infinie récurrente de points $P_1, \ldots, P_n, \ldots$ de A par les formules ci – dessous :

Nous commençons par la relation :

$P = m\,P_1 + T_{i,1}$

Nous poursuivons l'opération avec deux points P_i *et* P_{i+1} *pour* $i = 1,2,\ldots$

$$P_1 = m\,P_2 + T_{i,2}$$

$$P_2 = m\,P_3 + T_{i,3}$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$P_j = m\,P_{j+1} + T_{i,j+1} \qquad \textbf{(2)}$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$P_{n-1} = m\,P_n + T_{i,n}$$

où les points $T_{i,1}$, $T_{i,2}$,… sont des représentants $T_1, \ldots, T_s$

Nous utilisons les axiomes d'une hauteur $h : A \to \mathbb{R}$ ***(3)***

Par l'axiome *(h2)* des hauteurs , nous obtenons avec (2) , l'inégalité ***:***

$$h(P_j) \leq \frac{1}{m^2}\left\{ h(mP_j) + c_1 \right\} \qquad \textbf{(4)}$$

Dans la formule (2) de P_{j-1} , nous calculons le point mP_j :

$$mP_j = P_{j-1} - T_{i,j} \qquad \textbf{(5)}$$

La hauteur des deux membres implique la relation :

$h(mP_j) = h(P_{j-1} - T_{i,j})$ ***(6)***

(4) ,(5) et (6) impliquent l'inégalité :

$$h(P_j) \leq \frac{1}{m^2}\left(h(P_{j-1} - T_{i,j}) + c_1\right) \qquad \textbf{(7)}$$

L'axiome *(h1)* des hauteurs transforme (7) en l'inégalité :

$$h(P_j) \leq \frac{1}{m^2}\left(2h(P_{j-1}) + c_3\right) \qquad \textbf{(8)}$$

où c_3 est une constante dépendant de c_1 .

Les formules de récurrence (3) ,appliquées à (8), impliquent l'inégalité :

$$h(P_j) \leq \left(\frac{2}{m^2}\right)^n h(P) + \left[\frac{1}{m^2} + \frac{2}{m^4} + \frac{4}{m^6} + \cdots + \frac{2^{n-1}}{m^{2n}}\right] c_4 \ , \qquad \textbf{(9)}$$

où c_4 est une constante dépendant de c_3 .

La somme du 2^{éme} membre de (9) est le développement en série de la

fonction $$\frac{1}{m^2-2} = \frac{1}{m^2} \cdot \frac{1}{1-\frac{2}{m^2}} \qquad \textbf{(10)}$$

Il en résulte l'inégalité

$$h(P_n) \leq \left(\frac{2}{m^2}\right)^n h(P) + \frac{c_4}{m^2-2} \ ; \qquad \textbf{(11)}$$

L'hypothèse $m \geq 2$ transforme (11) en l'inégalité

$$h(P_n) \leq 2^{-n} h(P) + \frac{c_4}{2} \qquad \textbf{(12)}$$

Pour « n assez grand » ,(12) devient :

$$h(P_n) \leq 1 + \frac{c_4}{2} \qquad \textbf{(13)}$$

Donc, par (13) , la suite $P_1 , ..., P_n$ est de hauteur bornée .

Par l'axiome (*h3*) des hauteurs, cette suite de points est finie.Nous en déduisons que tout point P du groupe abélien A est une combinaison $\mathbb{Z}$ − linéaire finie de points de A de la forme

$$P = n_1 T_1 + ... + n_s T_s + \sum_j u_j N_j$$

où les points N_j sont de hauteur bornée par (13)

Donc, le groupe abélien A est de type fini.

□

Corollaire 1 :

Le groupe E(ℚ) , de Mordell – Weil , d'une courbe elliptique E sur le corps ℚ ,

qui est abélien , est de type fini .

□

Il en résulte que ce groupe $E(\mathbb{Q})$ admet r générateurs $\mathbb{Z}$ − linéairement indépendants.

Définition22 :

Cet entier r = r(E) est le rang de la courbe elliptique ; cet entier r est nul ou positif .

Corollaire 2 :

Le groupe de Mordell – Weil $E(\mathbb{Q})$ est isomorphe à un produit de groupes abéliens de la forme :

$$E(\mathbb{Q}) \cong T(E) \times \mathbb{Z}^r \qquad \textbf{(1)}$$

où T(E) est le groupe de torsion de la courbe elliptique E .

et $\mathbb{Z}$ est le groupe abélien additif des nombres rationnels en r copies .

Dans la littérature des courbes elliptiques, il y a beaucoup d'exemples de calcul de ce rang r (E) = r ; les méthodes utilisées sont différentes ; aucune n'est générale .Dans de nombreux cas , c'est une borne de r qui est déterminée . Voici quelques exemples.

Penny et Pomérance , (1975) , ont étudié les groupes $E(\mathbb{Q})$ de courbes elliptiques d'équation de Weierstrass :

$E : y^2 = x^3 + a\,x^2 + b\,x + c = f(x) \in \mathbb{Z}[x]$

En utilisant un sous ensemble A de l'anneau $\mathbb{Z}$

$$A = \left\{ n \in \mathbb{Z} \ ; \ |n| \le |b|^{1/2} \quad et \quad n + \frac{b}{n} + a \quad est\,un\,carré \ \right\} \cup \{b\}$$

avec la condition $a^2 - 4b$ non carré et l'homomorphisme $\mathbb{Q}^* \to \mathbb{Q}^* / \mathbb{Q}^{*2}$, ils ont trouvé des programmes, exécutés par l'ordinateur , qui ont permis à ces 2 auteurs d'obtenir 3 courbes elliptiques de rang r ≥ 7.

Ce sont des courbes avec les valeurs :

a=1692602 , 2843738 et 2877338

$b = -530052723915$

Ces valeurs sont grandes.

Brumer et Kramer ,(1977) , ont utilisé une méthode basée sur la « descente », les 2-isogénies, la K – algèbre $A_K = K[x] / (f(x))$, un homomorphisme de groupe :

$$E(K)/2E(K) \to A_K^*/A_K^{*2}$$

Ces 2 auteurs considèrent des courbes elliptiques qui ont une bonne réduction ou une réduction multiplicative . Ils ont utilisé la formule :

$$\mathbf{r + card\ Ш[2] + card\ E(\mathbb{Q})[2] = card\ S[2]\ .}$$

où $Ш[2]$ *est le groupe de 2 – torsion du groupe de Shafarévich – Tate ,*

$E(\mathbb{Q})[2]$ *est le groupe de 2 – torsion du groupe de Mordell – Weil*

et $S[2]$ *est le groupe de 2 – torsion du groupe de Selmer .*

Ils ont ainsi obtenu une longue liste de résultats. Citons -en quelques uns :

Courbes $y^2 + xy + y = x^3 - x^2 - 9x - 8$ *, avec* $\Delta(E) = -431$ *et* $r = 0$ *;*

2 courbes de rang 1 :

$y^2 + 9xy + y = x^3 - 7x^2$ *, avec* $\Delta(E) = 18097$

et $y^2 + xy = x^3 - 1$ *, avec* $\Delta(E) = -431$ *;*

Une courbe de rang 3 :

$y^2 + 15xy + y = x^3 - 49x^2$, *avec* $\Delta(E) = 18097$

Une courbe de rang $r \geq 4$ *:*

$y^2 + 8xy + 11y = x^3 + 2x^2 - 3x$, *avec* $\Delta(E) = -953243$

Une courbe de rang $r \geq 5$ *:*

$y^2 + 14xy + 29y = x^3 + 2x^2 - 15x$, *avec* $\Delta(E) = -177858971$, *etc.*

Wada ,(1996) , a étudié le rang de la famille de courbes elliptiques E d'équation de Weierstrass :

$E : y^2 = x^3 - n^2 x$.

Avec une méthode basée sur des équations diophantiennes, cet auteur a montré que, pour n= 1513 et 7361 , les rangs des 2 courbes est égal à 2 .

Citons, enfin, Rubin et Silverberg , (1999) , qui ont étudié les rangs de twists quadratiques E_D , de courbes elliptiques E , sur le corps $\mathbb{Q}$, d'équation de Weierstrass :

$$E : y^2 = x^3 + a\,x^2 + b\,x + c = f(x) \in \mathbb{Z}[x] ,$$
$$E_D : D\,y^2 = f(x)$$

Ils ont utilisé une méthode basée sur l'ensemble :

$$A = \{u, v \in \mathbb{Z} \ , \ p \gcd(u,v) = 1, v^4 f(u/v) \neq 0\}$$

et la hauteur canonique $\hat{h}$.
Ils ont obtenu une borne du rang :

$$r(E_D(\mathbb{Q})) \prec 2j \quad , \quad \textit{pour un certain entier } j$$

D'autres auteurs ont utilisé la série $L_E(s)$ de la conjecture de Birch et Swinnerton –Dyer pour obtenir le rang analytique $r_{an}(E)$ de courbes elliptiques. Ce rang r_{an} est calculé soit avec les zéros de la série $L_E(1)$, soit avec une formule faisant intervenir les coefficients a_n de la série $L_E(s) = \sum_{n \geq 1} a_n n^{-s}$, les groupes de Shafarévich – Tate , le groupe de torsion .

Plusieurs conjectures sur ce rang analytique ont été émises : sur la parité de r_{an} , sur l'égalité $r = r_{an}$.
Dans le chapitre 1 § 4 , nous avons indiqué les définitions du $R(E)$ et de série $L_E(s)$ de Dirichlet – Hasse d'une courbe elliptique E .

La série $L_E(s)$ de Dirichlet – Hasse d'une courbe elliptique E sur le corps $\mathbb{Q}$ des nombres rationnels satisfait une équation fonctionnelle :

$$F_E(s) = uF_E(2-s)$$

avec $u = \pm 1$

Définition 23 :

Le coefficient $u = \pm 1$ *est le signe de l'équation fonctionnelle de la courbe elliptique E sur* $\mathbb{Q}$.

Cette fonction $F_E(s)$ *est égal à :*

$$F_E(s) = N(E)^{s/2} \frac{\Gamma(s) L_E(s)}{2\pi^s} ,$$

où N(E) est le conducteur de la courbe elliptique et $\Gamma(s)$ *est la fonction analytique complexe Gamma.*

Conjecture de parité :

Le rang r(E) et le rang analytique r_{an} *d'une courbe elliptique E sur le corps* $\mathbb{Q}$ *ont même parité .*

Martin et Mc Millen ,(2000) , ont trouvé une courbe elliptique de rang ≥ 24 ;

E /$\mathbb{Q}$: $y^2 + x\,y + y = x^3$ - 120039822036992245303534619191166796374x

+504224992484910670010801799168082726759443756222911415116 .

N. D. Eckies , (2002) , a étudié des courbes elliptiques d'équation de Weierstrass

$$E_D : D\,y^2 = x^3 - x$$

de rang analytique impair en admettant la conjecture que le rang analytique r_{an} est de même parité que le signe de l'équation fonctionnelle de la série $L_E(s)$.

L'auteur a prouvé que les courbes elliptiques E_D ont un rang $r(E_D) \succ 0$

lorsque $|D|$ est congru à 5,6 ou 7 mod 8 .

3 – Application à la famille $E_t : y^2 = x^3+2t^3\,x^2+t^2x$:

Dans le chapitre I § 7 nous avons calculé le discriminant :

$$\Delta(E_t) = 64\,t^6\,(t^4-1)$$

La courbe E_2 est donc elliptique :

$$E_2 : y^2 = x^3 + 16\,x^2 + 4\,x$$

Déterminons quelques points :

x	*0*	$-8-\sqrt{60}$	$-8+\sqrt{60}$	1	-1	1/2	- 2	2
y	*0*	0	0	$\pm\sqrt{21}$	$\pm\sqrt{11}$	$\pm\frac{7}{\sqrt{8}}$	$\pm\sqrt{48}$	$\pm\sqrt{80}$

Les points $P_1=(0,0)$,$P_2=(-8-2\sqrt{15},0)$, $P_3=(-8+2\sqrt{15},0)$ et $P_4=(1,\sqrt{21})$

ont des coordonnées dans le corps quadratique K= $\mathbb{Q}(\sqrt{60},\sqrt{21}) = \mathbb{Q}(\sqrt{15},\sqrt{21})$.

Les 3 points d'intersections P_1, P_2 et P_3 avec l'axe Ox sont d'ordre 2 .

Déterminons les points mP_4 , où $P_4=(1,\sqrt{21})$, avec les formules de Cassels,

0 $P_4=O_E$ par définition. Nous testons un algorithme de calcul

(1) $y' = \dfrac{3x^2 + 2\times 16x + 4}{2y}$

(2) $x_{2P_4} = y'^2 - 2x - 16 = x_4$

(3) $y_{2P_4} = -y'^3 + (16+3x)y' - y = y_4$

Nous obtenons successivement :

$$y' = \frac{39\times\sqrt{21}}{42};\quad x_4 = \frac{3}{28};\quad y_4 = \frac{1763}{8\times 7\times 49}\sqrt{21}$$

Donc le point P_4 est d'ordre $m \succ 2$.

La poursuite des calculs de 3 P_4 , 4 P_4 … exige un logiciel de calcul .

Pour appliquer la « descente infinie »,il faut choisir une valuation non archimédienne $v \in M_K$.

Ensuite on peut appliquer la hauteur associée à v, de valeur :

$$h_v(P) = \max\left\{ -\frac{1}{2}\ v(x_P), 0 \right\} + \frac{1}{12} v(\Delta(E)).$$

Ces calculs demandent un logiciel spécial que je n'ai pas trouvé.

Je ne peux pas évaluer le rang de cette courbe elliptique E_2 .

C'est un objectif que je poursuivrai à l'avenir.

Bibliographie

[1] A.BRUMER et K. KRAMER ,The rank of elliptic curves. Duke. Math . J. 44. (1977) pp715 – 743 .

[2] J.W.S CASSELS , Diophantine equations with special reference to elliptic curves . J.London.Math.Soc.41(1966) pp193-291.

[3] J.W.S CASSELS et A. FRöLICH , eds ,Algebraic Number Theory ,Academic Press (1967) pp85-93.

[4] DEURING ,Die Typen der Multiplikatorenrige Elliptisher Funktionnen körper , Abh..Math. Sem. Hamburg 14 (1941) pp197 – 272 .

[5] R-HARSTHORNE , Algebraic Geometry , Springer –verlag (1983).

[6] S.KIHARA ,On the rank of the elliptic curves $y^2= x^3+k$,Proc.Jap.Acad.(1996) pp 228-229.

[7] A.W .KNAPP , Elliptic Curves ,Princeton Univ .Press (1992) .

[8] N. KOBLITZ , Introduction in elliptic curves and modular forms ,GTM 97 (1984)

[9] S.LANG , Complex multiplication .Springer – verlag 1983.

[10] S.LANG , Fundamentals of Diophantine Geometry Springer – Verlag (1983) New-York , chapitre 9.

[11] J.F. MESTRE , Construction of an elliptic curves of rank $\geq$ 12 . CRAS , Paris (1982) pp 643 – 644 .

[12] NERON ,Problèmes arithmétique et géométrique rattaché à la notion de rang d'une courbe algébrique dans un corps. Bull.Soc.Math.France 80(1952) pp 101-166.

[13] D.E.PENNY and C.POMERANCE,Three elliptic curves with rank at least seven .Math.of Comp.Vol 29 n^0 131 .(july 1975) pp965-967.

[14] K.RUBIN and A.SILVERBERG , Ranks of elliptic curves ,Bull.of the Amer. Math. Soc. Vol.39 , N^0 4,pp455-474 (July 2002).

[15] I.R.SHAFAREVICH and J.TATE , The rank of elliptic curves ,AMS Transl.8 (1967) pp.917-920 .

[16] G.SHIMURA , Introduction to the Arithmetic Theory of Automorphic Functions Princeton Univ .Press N^0 11, (1971).

[17] J.H.SILVERMAN , The Arithmetic of Elliptic Curves ,G.T.M 106, Springer –verlag 1986

[18] J.TATE , The Arithmetic of Elliptic Curves .Invention .Math. Vol.23 (1974) pp179-206.

[19] J.VELU , Isogénies entre courbes elliptiques .C.R.Acad.Sci.Paris A273 (1971) pp238-241.

[20] H.WADA , On the rank of the elliptic curves $y^2 = x^3-1513^2$ x ,Proc.Jap.Acad.72 (1996) pp 34-35.

[21] H.WADA et M.TAIRA, Computations of the rank of elliptic curves $y^2= x^3-n^2x$. Proc.Japan. Acad.70.(1994) pp154-157.