N° d'ordre :
N° de série :

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

UNIVERSITÉ D'EL-OUED

FACULTÉ DES SCIENCES ET DE TECHNOLOGIE

Mémoire de fin d'étude

LICENCE ACADEMIQUE

Domaine: Mathématiques et Informatique
Filière: Mathématiques
Spécialité: Modélisation mathématiques & simulation numérique

Présenté par : BEN AMOR Marwa
BOUZENNA Houria
HOUIDI Nacira

Thème

Point d'ordre fini de courbe elliptique

Soutenu le …juin 2014

Devant le jury composé de:

Mr.Ahfouda Belhadi	MC (B) Univ. El Oued	Président
Mr.Rhoma Abd Elhamied	MA (B) Univ. ElOued	examinateur
Mr.Youmbai Ahmed El Amine	MA (B) Univ. ElOued	Rapporteur

Année universitaire 2013 – 2014

Introduction générale

La théorie des équations de Diophantine et une branche de mathématiques qui étudie les solutions d'une équation polynômial.

Dans ce mémoire nous avant étudié les solutions d'une équation spécial dite (courbe elliptique), le premier chapitre traite les notions des courbes algébriques à fin de définir une courbe elliptique, le second chapitre étudi profondément les courbes elliptiques et leur invariants.

Et finalement le dérnier chapitre montre des méthodes classique pour trouver le sous groupe de torsion et quelques points d'ordre donné.

Remerciements

hf:ejlei:gjelgt

l:gjtlg

jgetgetgjelg

Table des matières

Chapitre 1

Courbes algébrique planes

un point P du plan Oxy admet coordonnées(x, y)

Définition 1.0.1 *: on appelle courbe algébrique plane est défnie par une équation algébrique $f(x, y) = 0$, dans un ameau de polynôme $\mathbb{k}[x, y]$sur un corps comuntatif global,local ou nul*

Exemple 1.0.1 *: pour $n = 1$:*

$$f(x, y) = a_1x + a_2y + a_3 = 0$$

est l'équation d'une droite[2]

Exemple 1.0.2 *f est irréductible:pour $n = 2$*

$$f(x, y) = a_1x^2 + a_2xy + a_3y^2 + a_4x + a_5y + a_6 = 0$$

est l'équation d'une conique ou cercle ou :

$$f(x, y) = (a_1x + a_2y + a_3)(a_4x + a_5y + a_6) = 0$$

est l'equation du produit de deux droite .[2]

Exemple 1.0.3 *: f est irréductible:pour $n = 3$*

$$f(x,y) = a_1x^3 + a_2x^2y + a_3xy^2 + a_4y^3 + a_5x^2 + a_6xy + a_7y^2 + a_8x + a_9y + a_{10} = 0$$

est l'équation d'une cubique non dégénérée lorsque f est irréductible,si:

$$f(x,y) = (a_1x^2 + a_2xy + a_3y^2 + a_4x + a_5y + a_6)(a_7x + a_8xy + a_9y) = 0$$

est l'équation du produit d'une conique par une droite.

$$f(x,y) = (a_1x + a_2y + a_3)(a_4x + a_5y + a_6)(a_7x + a_8y + a_9) = 0$$

est l'équation du produit de trois droites.

Exemple 1.0.4 *f irréductible,si pour $n \geq 3$ si $f(x,y) = 0$ est l'équation d'une courbe plane hypérelliptique*

1.1 Singularités et genre d'une courbe algébrique

Définition 1.1.1 *:on appelle courbe algébrique plane C,d'équation $f(x,y) = 0$ .admet un point singulier s si elle satisfait*

$$f(x) = 0, f'_x(s) = 0, f'_y(s) = 0, ..., \frac{\partial f^{n-1}}{\partial x^{n-1}} = 0, \frac{\partial f^{n-1}}{\partial y^{n-1}} = 0, \frac{\partial f^n(s)}{\partial x^n} \neq 0$$

est la dérivé partielle de f qui ne s annule pas en s,$n \geq 2$:

le point singulier s est un point double $n = 2$:

$$f(s) = f^{'}_x(s) = f'_y(s) = 0 est f^{"}_x(s) \neq 0$$

le point singulier s est un point triple $n = 3$:

$$f(s) = f^{'}_x(s) = f^{'}_y(s) = f^{"}_x(s) = f^{"}_y(s) = f^{"}_{xy}(s) = 0 est f^{"'}_x(s) \neq 0$$

Définition 1.1.2

$$f(s) = f^{'}_x(s) = f'_y(s) = ... = f^{(n-1)}_{x^{(n-1)}}(s) = f^{(n-1)}_{y^{(n-1)}}(s) = 0 et f^{(n)}_{x^n}(s) \neq 0$$

pour un point multiple d'ordre n [2]

Exemple 1.1.1 *:* $f(x,y) = 2x^{(2)} - y^{(3)} + 2xy - 3x^{(2)}y - 1 = 0$

$f'_x(s) = 4x + 2y - 6xy et f'_y(s) = -3y^2 + 2x - 3x^2$

$f_x^{"}(s) = 4 - 6y$ *et* $f_y^{"}(s) = -6y$

le point $s = (0,0)$ *n'est pas singulier*

$f(x,y) = y^{(2)} - 2y - x^{(3)} + 3x - 1 = 0$

$f'_x(s) = 3x^2 + 3$ *et* $f'_y(s) = 2y - 2$

$f_x^{"}(s) = 6x et\ f_y^{"}(s) = 2$

$f_x"(s) = 6 \neq 0$

Définition 1.1.3 *: Le genre d'une courbe algébrique est lié à son degré et au nombre de ses point singuliers,soit une courbe algébrique plane de degré n qui possède s point singuliers. Alors son genre est égal à l'entier positif ou nul égal a:*

$$g = \frac{1}{2}(n-1)(n-2) - s$$

[2]

Définition 1.1.4 *:* $g = 0$ *pour les droites,les cercles,les coniques et les coubiques singulières.*$g = 1$ *pour les courbes elliptique ,les quartique ayant 2 points singulier...*[2]

Définition 1.1.5 *:une cubique de weierstrass est une cubique plane d'équation particuliére*

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \in \Bbbk[x,y] \tag{1.1.1}$$

les cinq coeffcients a_i sont des l'elements d'un corps commutatif $\Bbbk$,les deux variable x et y sont des zéros de l'équation algébrique $(1,1)$; donc x et y sont des éléments d'une clôture algébrique $\Bbbk_{al}$ de $\Bbbk$

1.2 Espace affine,espace projectivs

Définition 1.2.1 *: un n−espace affine sur un corps commutatif* $\Bbbk$ *est l'élémemt des n–uples d"élémemt aide k :*

$$A^n(k) = \{a = (a_1, ..., a_n)\,; a_i \in \Bbbk\}$$

[2]

Exemple 1.2.1 *: Les espaces affines $A(C)$ sont représentés par une droite,les espaces affines ne $A^2(C)$ sont représenté par le plan réel $\bigcirc xy$, tout point Pde cet espace a deux coordonnés (x, y)*

Les espace affine$A^3(C)$ est représenté par l'espace $\bigcirc xyz$ tout point Pde cet espace a trois coordonnés (x, y, z)

Définition 1.2.2 *:Un on sont élémemt on dit qu'un $a \in A_n(k)$ est un point $a = (a_1, ..., a_n)$de l'espace affine .les $a_i$sont les coordonnées de ce point*

Définition 1.2.3 *:On appelle n– espace projectif sur un corps $\Bbbk$, L'ensemble des classes d'equivalence de $(n + 1)$uples $(a_1, ..., a_{n+1})$d'élémemt de $\Bbbk$,non tous nuls par la relation d'equivalence et $(b_1, ..., b_{n+1})$ alors :a$\Re$b si et seulememt si*

$$a = (a_1, ..., a_{n+1}) = \lambda b = (b_1, ..., b_{n+1})$$

pour $\lambda \neq 0, \lambda \in k$

Définition 1.2.4 *:l'espace qoutient de*

$$A^{n+1}(k) - \{(0, 0, ..., 0)\} \diagdown R$$

est l'espace projectif $P^n(k)$ alors :

$$P^n(k) = A^{n+1} \diagdown \Re$$

[2]

1.3 Equation de Weierstrass d'une cubique

Une cubique de Weierstrass est le plan E un plan affine A^2qu'est du forme :

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

Dans le plan projectif P^2 cette equation est la forme:

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

Le passage du plan projectif P^2 au plan affine A^2,s'obtient à l'aide de la transformation linéaire

$$(x, y, z) \to (x, y, 1) \in A^2 \tag{1.3.1}$$

Le passage du plan affine A^2au plan projectif P^2 s'obtient avec deux opérations :

La prémiere est

$$(x, y) \to \left(\frac{x}{z}, \frac{y}{z}\right) \tag{1.3.2}$$

Une multiplication par z^d(d=degr du polynôme$f$)

La secound :

$$z^d f\,(x, y, z) = h\,(x, y, z) \tag{1.3.3}$$

[2]

Exemple 1.3.1 *:* $f(x, y, z) = x^3 + 2x^2y + z^2x + xyz$

Ce polynôme homogène est tronsformé en polynôme affine :

$$f(x, y, 1) = x^3 + 2x^2y + x + xy \in A^2$$

Le polynôme affine

$$f(x, y) = x^4 + 2xy^3 + 5$$

de degré deux est transformé en:

$$f\left(\frac{x}{z}; \frac{y}{z}\right) = \frac{x^4}{z^4} + \frac{2xy^3}{z^4} + 5$$

Puis, par multiplication par d^4 ,en un polynôme homogène de degré 4 :

$$z^4 f\left(\frac{x}{z}, \frac{y}{z}\right) = x^4 + 2xy^3 + 5z^4$$

1.4 Transformation d'une cubique Weierstrass

On appelle du cubique Weierstrass E d'équation :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \in \Bbbk[x, y] \tag{1.4.1}$$

Qu'peut être transformée par des changements de variables convenables élminons les monômes men xy et en y par le changement de variable :car$(k) \neq 2$

$$(x, y) \to \left(X, \frac{1}{2}(Y - a_1X - a_3)\right) \tag{1.4.2}$$

Alors :

$$E_1 : Y^2 = 4X^3 + b_2X^2 + 2b_4X + b_6 \in k[x; y] \tag{1.4.3}$$

on pose :$b_2 = a_1^2 + 4a_2$, $b_4 = a_1a_3 + 2a_4$, $b_6 = a_3^2 + 4a_6$

ces 3 coèffcients b_{2i} sont des polynômes homogènes de degré $2i$ dans l'anneau

l'élimintation le monôme en X^2 et du coeffcient 4 dans la formule avec le changement de variables :

$$X = \frac{x - 3b_2}{36}, Y = \frac{y}{108} \tag{1.4.4}$$

Nous obtenons pour car$(k) \neq 2, 3$ l'équation :

$$E_2 : y^2 = x^3 - 27c_4x - 54c_6 \tag{1.4.5}$$

ces 2 coeffcients c_{2i}sont polynôme homogènes de degré $2i$dans l'anneau$\mathbb{Z}[b2; b4; b6]$

$c_4 = b_2^2 - 24b_4; c_6 = 36b_2b_4 - b_2^2 - 216b_6$ [2]

1.4.1 Discriminants

Après notre digression dans l'analyse réelle et complexe , nous retournons sur le terrain

des nombres rationnels . Comme toujours , nous prenons notre courbe dans sa forme normale

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

où a, b, c sont des nombres rationnels . Si nous laissons $X = d^2x$ et $Y = d^3y$, alors notre équation devient

$$Y^2 = X^3 + d^2aX^2 + +d^4bXd^6c$$

En choisissant une grand nombre entier d, on peut effacer les dénominateurs en a, b, c une Donc à partir de maintenant nous supposerons que notre courbe cubique est donnée par un nombre entier d'équations ayant coefficients .

Notre objectif dans ce chapitre est de démontrer le théorème : demontre par Nagell et Lutz , qu'explique comment trouver tous les points rationnels d'ordre fini. Leur théorème dit qu' un point d'ordre fini (x, y) doit rationnelle.

Ont coordonnées entières, et soit $y = 0$ (pour les points d'ordre deux) ou d'autre $y\backslash D$, où D est le discriminant du polynôme $f(x)$. En particulier,une courbe cubique a qu'un nombre fini de points rationnels d'ordre fini .

Le discriminant de $f(x)$ est la quantité

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

Peut-être quand $a = 0$,

$$D = -4b^3 - 27c^2$$

Si l'on tient compte $\diagup$ sur les nombres complexes ,

$$f(x) = (x - \alpha_1)\{x - \alpha_2)(x - \alpha_3)$$

alors on peut vérifier que

$$D = (\alpha_1 - \alpha_2)^2(a_1 - \alpha_3)^2(a_2 - \alpha_3)^2$$

Et ainsi de la non - disparition de$D$ nous dit que les racines de $f(x)$ sont distincts .Ainsi, la question de trouver les points rationnels d'ordre fini peut être réglé en un nombre fini d'étapes . Vous prenez l'entier D , et considérez chacun des un nombre fini de nombres entiers y avec $y\backslash D$. Vous prenez toutes les valeurs de y et les remplacer dans l'équation $y^2 = f(x)$. Le polynôme $f(x)$a coefficients entiers et de coefficient dominant 1 . S'il a une racine entière ,cette racine va diviser le terme constant . Ainsi, il existe un nombre fini de

choses à vérifier , et de cette manière nous serons sûr de trouver tous les points de ordre fini en un nombre fini d'étapes

Le discriminant d'une cubique de WeierstrassE/K est le polynôme" homogène" de degré12de l'anneau $\mathbb{Z}[b2; b4; b6; b8]$ [8]

Définition 1.4.1 *On appelle discriminant, noté* Δ,*la quantité*

$$\Delta(E) = 9b_2b_4b_6 - b_2^2b_8 - 8b_4^3 - 27b_6^2 \in K$$

avec $4b_8 = b_2b_6 - b_4^2$ *et ;Carac(K)* $\neq 2, 3$ [7]

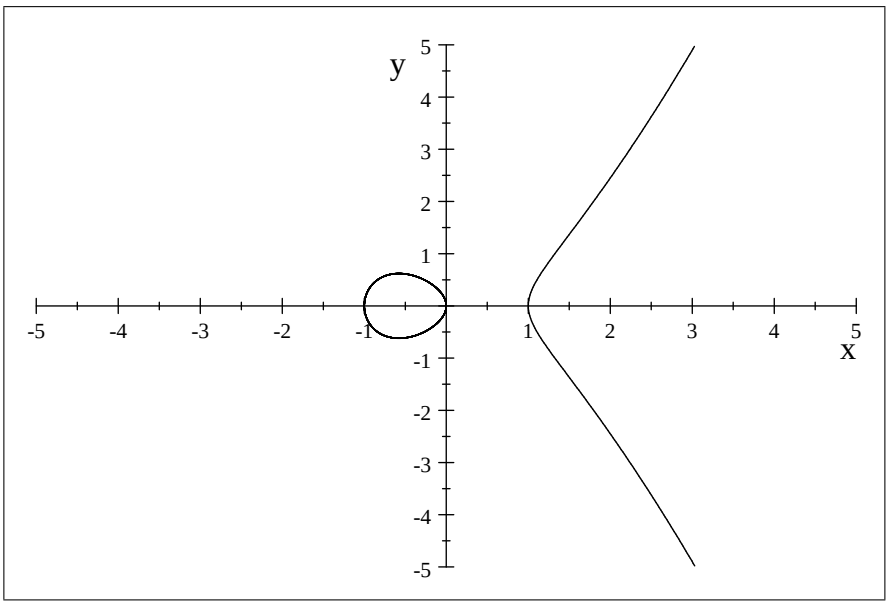
Définition 1.4.2 *l'invariant modulaire d'une cubique de Weierstrass E est l'élément du corps K égal à :*

$$j(E) = \frac{c_4^3(E)}{\Delta(E)} \in K$$

[2]

Exemple 1.4.1 *Soit E la courbe elliptique définie sur* $\mathbb{R}$ *par l'équation de Weierstrass*

$y^2 = x^3 - x$



On a:

$a_1 = a_2 = a_3 = a_6 = 0$ et $a_4 = -1$

On en déduit : $b_2 = b_6 = c_6 = 0, b_4 = -2, b_8 = -1, c_4 = 48$

Le calcul du discriminant donne donc $\Delta = 64$ et l'invariant modulaire vaut alors E : $j = 1728$, la courbe elliptique E n'est donc ni singulière ni supersingulière

Proposition 1.4.1 *Soit une courbe elliptique E sur Q ,d'équation de weierstrass:*

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

avec $A,\ B \in \mathbb{Z}$ *et* $4A^3 + 27B^2 \neq 0$,

Considéons un point $P = (x, y)$ de torsion de E

Exemple 1.4.2 *courbe elliptique E d'équation de weierstrass :*$y^2 = x + 6 \in Q[x, y]$

Alors $4A^3 + 27B^2 = 4 + 6 \times 27 = 166$

Chapitre 2

Généralités sur les courbes elliptiques

2.1 courbe elliptique

Une courbe elliptique E sur le corps $\Bbbk$ (notée$E(K)$) est définie par

une équation de Weierstrass du type

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.1.1}$$

pour $a_i \in \Bbbk$:

Une équation deWeierstrass définit bien une courbe elliptique s'il n'existe pas de point de $E(\Bbbk)$ pour lequel les dérivées partielles $(2y + a_1x + a_3)$ et $(3x^2 + 2a_2x + a_4 - a_1y)$s'annulent simultanément. Les coordonnées$(x; y)$ sont appelées coordonnées a nes sur E.

La courbe elliptique $E(\Bbbk)$ est l'ensemble des points $P = (x; y)$ de $\Bbbk^2$

vérifiant l'équation () plus un point à l'infni noté P_∞.

$$E(\Bbbk) = \{(x; y) \in K \times Ktelsquey^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{P_\infty\} \tag{2.1.2}$$

Le point à l'infini peut symboliquement être vu comme le point d'intersection des droites verticales. Cette idée grossière se formalise en considérant l'espace projectif, ce qui est fait dans[Sil92,ChapIII1].

Définition 2.1.1 *: (Courbe elliptique)*

Une courbe elliptique est une paire (E, O), où E est une courbe lisse sur $\overline{K}$ de genre 1 et $O \in E$. On dit que O est le point à l'infini de E. On dit que E est définie sur K et on note E/K si E est définie sur K en tant que courbe et si $O \in E(K)$.On va souvent écrire seulement E pour une courbe elliptique, le O étant sous-entendu.Nous allons maintenant montrer, en utilisant le théorème de Riemann-Roch, qu'une courbe elliptique peut être décrite par une équation de Weierstrass et réciproquement que toute courbe décrite par une équation de Weierstrass est une courbe elliptique

Définition 2.1.2 *:*

Une courbe elliptique E sur K est la donnée d'une équation

$$E : y^2 = x^3 + Ax + B, \tag{2.1.3}$$

$(A, B \in K)$

telle que

$$\triangle' := 4A^3 + 27B^2 \neq 0$$

et d'un point O dit point à l'infini. Plus precisément, E d´esigne le lieu dans P^2 de l'équation homogène

$$Y^2Z = X^3 + AXZ + BZ^3$$

associée à (3) et $O = [0, 1, 0]$.

Une équation du type (3) est appelée équation de Weierstrass. Une courbe elliptique est une courbe lisse($car\ \triangle' \neq 0$)et de genre1. En fait, on peut montrer que toute courbe lisse de genre 1 est donnée par une équation de Weierstrass (3)

avec $\triangle' \neq 0$.

Lorsque$K$ est de caractéristique 2 ou 3, ce qui précéde est encore valable à condition de remplacer (3) par une équation un peu plus compliquée :

Définition 2.1.3

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

$(ai \in K, i = 1, ..., 6)$.

Pour L/K une extension, l'ensemble des points L-rationnels de E est l'ensemble

2.2 Loi de groupe

soit C une courbe plane projective non singulière de degré trois sur un corps $\Bbbk$ parfait ($\Bbbk \neq \mathbb{Q}$ en ce qui nous concerne)

par le théorème de bézout,une droite passant par deux point P, Q de C à coordonnées dans $\Bbbk$ courpe C en exactement un troisième point (noté PQ) à coordonnées dans $\Bbbk$.si$P = Q$ la droite PQ peut être considérée comme la tangente en P à C .si la droite PQ est tangente en Q à C alors $PQ = Q$ et si P est un point d'inflexion,alors $PP = P$

Théorème 2.2.1 *:*

Soit E un courbe elliptique et D une droite du plan. Si D est tangente en un point à la courbe E ou bien si D coupe E en deux points distincts ; alors D coupe E en un unique autre point.Nous commençons par donner une interprétation géométrique de la loi.

Soient P et Q deux points $\Bbbk$ rationnels de E, nous appelons somme des points P et Q le point $\mathbb{R}$ obtenu par la construction suivante schématisée dans la Figure $I.2$. Tout d'abord nous traçons la droite (PQ). La droite (PQ) coupe la courbe elliptique E en un troisième point, le point $P + Q$ est le symétrique par rapport à l'axe des abscisses de ce troisième point d'intersection.

Pour P un point de la courbe, il est possible de calculer le point$[2]P$ en utilisant la tangente à la courbe au point P. Nous noterons $[r]P$ le point obtenu en additionnant r fois le point P,$[r]P = \underbrace{P + P + ... + P}_{r\ fois}$ Les schémas de résument cette construction.

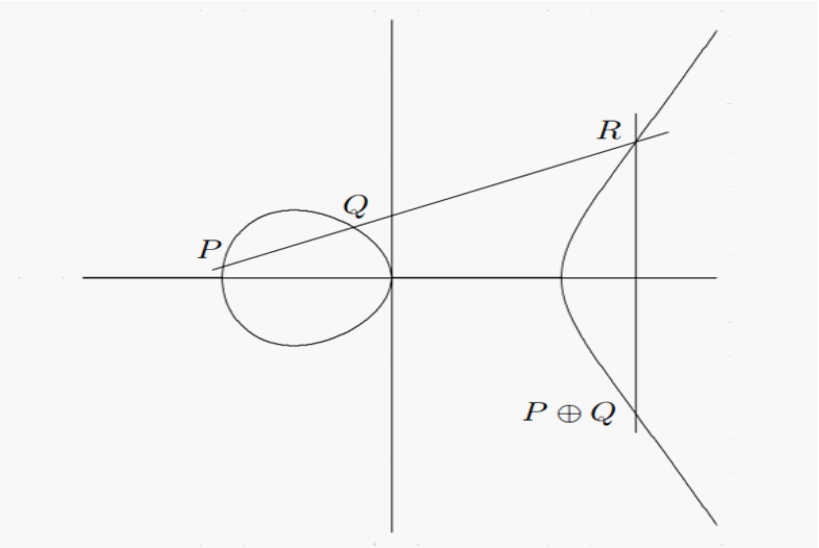
Théorème 2.2.2

Cette construction nous permet d'assurer que le théorème suivant est vrai.

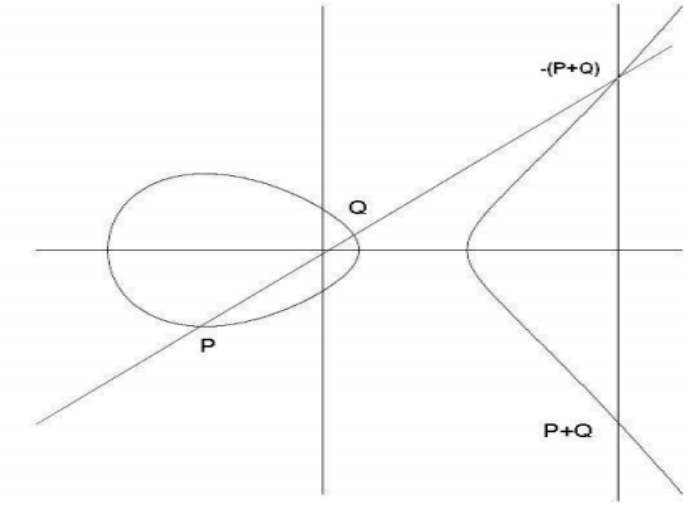
Théorème 2.2.3 *:*

L'ensemble des points d'une courbe elliptique E muni de la loi + véri e les propriétés suivantes :

(i) La loi + est interne : $\forall P; Q \in E, P + Q \in E$.



Tracé de la droite (PQ)



Illustrastion de la constructionde $P + Q$

(ii) Existence d'un élément neutre :

$$\forall P \in E; P + P_\infty = P$$

(iii) Commutativité de la loi + :

$$\forall P; Q \in E; P + Q = Q + P$$

(iv) La loi + est associative :

$$\forall P; Q; R \in E; (P + Q) + R = P + (Q + R)$$

(v) La loi + est symétrique : $\forall P \in E$, il existe un point noté $-P$ tel que

$$P + (-P) = P_\infty$$

$(E(\Bbbk); +)$ est donc un groupe abélien additif d'élément neutre P_∞.

Proposition 2.2.1 *:*

L'opposé du point$P$, noté $-P$, admet pour coordonnées $(x_P; -y_P)$.

Addition de deux points Soient $P = (x_P; y_P)$et $Q = (x_Q; y_Q)$deux points distincts d'une courbe elliptique $E(\Bbbk)$ tels que $P \neq -Q$. Pour trouver les formules donnant les coordonnées du point $R = P + Q$avec $R = (x_R; y_R)$, nous cherchons à résoudre le système de deux équations formé par l'équation de la droite (PQ) et l'équation de la courbe elliptique. Ce système traduit exactement le fait que

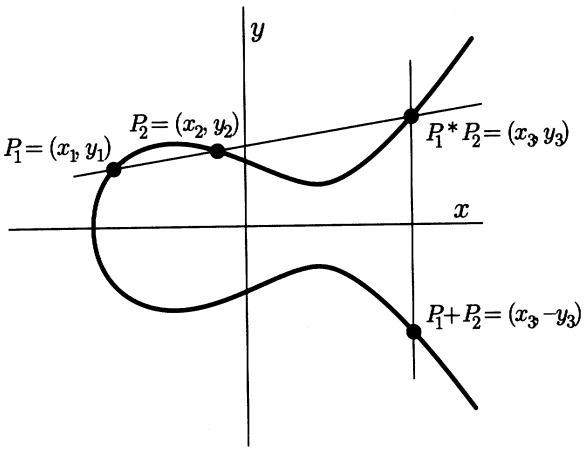
$-(P + Q)$ est le troisième point d'intersection de la courbe elliptique et de la droite (PQ). Nous obtenons les formules $(I.2.2)$, où représente la pente de la droite (PQ) :
$$\begin{cases} \lambda = \frac{y_P - y_Q}{x_P - x_Q} \\ x_R = \lambda^2 - x_P - x_Q \\ y_R = \lambda\,(x_P - x_R) - y_P \end{cases}$$
La complexité de l'addition sur la courbe elliptique est de

$$4A + 1S + 2M + 1I$$

où A (respectivement S,M et I) représente une addition (respectivement un carré, une multiplication et une inversion) dans le corp $\Bbbk$ [1]

Doublement d'un point

Pour trouver les formules donnant les coordonnées du point $R = [2]P$, nous utilisons le fait que $-[2]P$ est le second point d'intersection de la courbe Eet de la tangente en E au point



P. L'équation de la tangente et celle de la courbe elliptique forment un système dont la résolution nous donne les formules pour obtenir les coordonnées de point $R = [2]P$. Nous obtenons les formules (I.2.3), où représente la pente de la tangente au point P de la courbe elliptique :

$$2P = \begin{cases} \lambda = \frac{3x_P^2 + a}{2y_P} \\ x_R = \lambda^2 - 2x_P \\ y_R = \lambda\,(x_P - x_R) - y_P \end{cases}$$

La complexité doublement sur la courbe elliptique est de $5A + 1S + 2M + 1I$ dans $\mathbb{k}$.[1]

Chapitre 3

point d'order fini

Définition 3.0.1 *Un point d'order m d'une courbe elliptique E est un point P du groupe alébien $E(\Bbbk)$ tel que :*

$$mP = O_E\,[2]$$

Définition 3.0.2 *Pour tout entier ratiennal m ,un point P du groupe $E(\Bbbk)$ d'order m satisfait la relation $mP = O_E$ le synbole mP réprésente les sommes:$mP = P + P + P..... = P\,[2]$*

Définition 3.0.3 *:Le sous groupe de n-troison du groupe $E(\Bbbk)$ est l'ensemble $E(\Bbbk)\ [m]$ des points d'order m .*[2]

Définition 3.0.4 *:Le groupe de torsion d'une courbe elliptique E est l'ensemble*

$$T(E(\Bbbk)) = T(E) = \{P \in E(\Bbbk)\,; mP = O_E\}$$

L'ensemble $E(\Bbbk)$ des points K-rationnels d'une Courbe Elliptique $E/\Bbbk$ est un groupe abélien d'élément neutre le point $O_E = (\infty;\infty)$, et la loi basée sur la règle géométrique de 3 points colinéaires de E :

$$P_1 + P_2 + P_3 = O_E$$

Définition 3.0.5 *Soit E/K d´efinie par*

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

.L'ensemple des points K rationnels de E est

$$E(K) = \left\{(x, y) \in K^2, y^2 \cdots = \cdots + a_6\right\} \cup \{O\}$$

[8]

Exemple 3.0.1 *Soit E définie par $E : y^2 + y = x^3 - 6x + 4$. L'ensemble des points Q rationnels de E est*

$E(K) = \{O, (-1, 3), (-1, -3), (2, -3), (2, 0), (1, -1)\}$.

3.1 Points d'ordre 2

On dit qu$P$ et doublle 2 si $2P = 0$ et $P \neq O$. La condition $2P = O$ équivaut à $P = -P$

Puisque $-(x; y) = (x; -y)$, ces points vérifient alors $y = 0$. Ce sont donc les points:

$$P_1 = (\alpha_1, 0)P_2 = (\alpha_2, 0)P_3 = (\alpha_3, 0)$$

où $\alpha_1; \alpha_2; \alpha_3$ sont les racines du polynôme cubique

$$f(x) = x^3 + ax^2 + bx + c$$

Etudions maintenant la nature du sous-groupe $G = \{O; P_1; P_2; P_3\}$ des points d'ordre diviseurs 2:

Si l'on travaille avec des coordonnées complexes, alors il y a trois points distincts(car la courbe est non singulière) d'ordre 2 et ainsi G est le groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Il'on travaille avec des coordonnées réelles, alors les trois racines précédentes sont réelles et G est sera le groupe de Klein. Il n'y a qu'une seule racine réelle et alors G est $\mathbb{Z} = 2\mathbb{Z}$.

Si l'on travaille avec des coordonnées rationelles, alors G est le groupe de Klein, le groupe cyclique d'ordre 2 ou le groupe trivial suivant que f a $3, 1$ ou 0 racines rationnelles .[8]

3.2 Points d'ordre 3

On dit que les points sont d'ordre vérifiant$3P = O$, ce qui équivaut à $2P = -P$. Un point d'ordre 3 satisfait donc

$$x(2P) = x(-P) = x(P)$$

(et réciproquement). Pour trouver ces points, on utilise la formule de duplication démontrée dans le 2.4. On doit avoir:

$$x = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} \tag{3.2.1}$$

Ce qui, après calculs, donne:

x est racine du polynôme

$$g\left(x\right) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + \left(4ac - b^2\right)$$

Mais puisque

$$x\left(2P\right) = \frac{f'\left(x\right)^2}{4f\left(x\right) - a - 2x}$$

Une autre expression de $g(x)$ est

$$g(x) = 2f(x)f"(x) - f\prime(x)^2$$

g a alors 4 racines (complexes) distinctes (sinon f et $f\prime$ auraient des racines communes). Soient $\beta_1; \beta_2; \beta_3; \beta_4$ ses 4 racines et pour chaque β_i soit $\delta_i = \sqrt[1]{f\left(\beta_i\right)}$.

Alors l'ensemble $(1;1); (2;2); (3;3); (4;4)$ est l'ensemble complet des points d'ordre 3 sur la courbe.

De plus, aucun δ_i ne peut être egal a 0 (sinon les points seraient d'ordre 2), donc cet ensemble contient 8 points distincts d'ordre 3.

Ainsi l'ensemble des points complexes d'ordre divisant 3 forme un groupe d'ordre 9 : c'est le groupe $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Si l'on travaille avec des coordonnées réelles, le groupe des points d'ordre divisant 3 est le groupe $\mathbb{Z}/3\mathbb{Z}$.

Si l'on travaille avec des coordonnées rationnelles, c'est soit le groupe cyclique d'ordre 3, soit le groupe trivial.[8]

3.2.1 Points d'ordre deux et trois.

Soit C être la cubique non singulière courbe

$$C : y^2 = f(x) = x^3 + ax^2 + bx + c$$

.

[Rappelons que C est f prévu non singulière $f(x)$ et $f\prime(x)$ n'ont pas de commune racines complexes .]

(a) Un point $P = (x, y) \neq O$ sur C est d'ordre deux si et seulement si $y = 0$.

(b) C a exactement quatre points de l'ordre divisant 2 . Celles-ci forment quatre points un groupe qui est un produit de deux groupes cycliques d'ordre deux .

(c) Un point $P = (x, y) \neq O$ sur C a pour trois si et seulement si x est une racine du polynôme

$$\Psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + \left(4ac - b^2\right)$$

(d) C a exactement neuf points de l'ordre divisant 3 . Ce formulaire neuf points un groupe qui est un produit de deux groupes cycliques d'ordre trois .[6]

3.2.2 Groupe de Torsion $E(Q)$

Soit E une courbe elliptique défini sur Q , l'ensemble des points rationnels d'ordre fini du groupe de Mordell-Weil $E(Q)$ est un sous groupe de $E(Q)$

Définition 3.2.1 *Le groupe de Torsion d'une courbe elliptique E est l'ensemble :*

$E(Q)_{tors} = \{P \in E(Q) ; mP = O_E\}$ [2]

A partir de la loi de groupe d'une courbe elliptique définie sur une clôture algébrique de , on peut définir l'application

Q ,on peut définir l'application

$[m]\{P \quad \mathbf{a}\ P+P+...+P$

Définition 3.2.2 *Les éléments du noyau de cette application sont les points de $m-$torsion de la courbeE/Q .*

On note cet ensemble $E[m]$, sous groupe de $E\left(Q^{a\lg}\right)$. Ce sont les éléments d'ordre m

Proposition 3.2.1 *Le groupe de Torsion d'une courbe elliptique E vérifie la relation:*

$E(k)_{tors} = \overset{n}{\underset{m=1}{\cup}} E[m][2]$

Preuve. :évident ■

Polynômes de m-division

Considérons une courbe elliptique E donnée par une équation de Weierstrass de la forme

$$E = y^2 = x^3 + ax + b$$

On veut calculer les points d'ordre m, c'est-à-dire calculer le point mPen fonction de $P = (x, y)$, en utilisant la loi du groupe.

Définition 3.2.3 *Les coordonnées des points $mP = P + P + ... + P$ $(m > 0)$ d'une courbe elliptique $E : y^2 = x^3 + ax + b$ où$(4a^3 + 27b_1^2)$ sont de la forme :*

$$mP = \left\{ \frac{f_m}{y_m^2}, \frac{w_m}{y_m^3} \right\}$$

Où y_m, f_m, w_m sont des polynômes de l'anneau $\mathbb{Z}[x, y, a, b]$satisfaisant aux relations :

$y_0(x,y) = 0$

$y_1(x,y) = 1$

$y_2(x,y) = 2y$

$y_3(x,y) = 3x^4 + 6ax^2 + 12bx - a^2$

$y_4(x,y) = 4y\,(x^5 + 5ax^5 + 20bx^3 - 4abx - 8b^2 - a^3)$

$y_{2m+1}(x,y) = y_{m+2}(x,y)\,y_m^3(x,y) - y_{m-1}(x,y)\,y_{m+1}^3(x,y)$

$y_{2m}(x,y) = \frac{1}{2y} y_m(x,y)\left(y_{m+2}(x,y)\,y_{m-1}^2(x,y) - y_{m-2}(x,y)\,y_{m+1}^2(x,y)\right)$

$y_m(x,y) = x y_m^2(x,y) - y_{m+1}(x,y)\,y_m(x,y)$

$4yw(x,y) = y_{m+2}(x,y)\,y_{m-1}^2(x,y) - y_{m-2}(x,y)\,y_{m+1}^2(x,y)$

La démonstration se fait par récurrence sur m.

Le deux théorèmes suivants décrivent totalement $E(Q)_{tors}$ [6]

Théorème 3.2.1 *(Lutz-Nagell)*

Soit E/Q une courbe elliptique donnée par une équation de Weierstrass

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

A,B$\in \mathbb{Z}$

Si $P = (x, y, 1)$est un point de torsion de $E(Q)$, alors :

$x, y \in \mathbb{Z}$

ou bien $y = 0$,ou bien y^2divise $V = 4A^2 + 27B^2$ [2]

Preuve. :L'assertion a) découle du corollaire 2 III.1.

Si $2P = 0$, alors $y = 0$et x est solution rationnelle de $x^3 + Ax + b = 0$ donc appartient à . Le théorème est ainsi vérifié. Supposons alors $2P^1O$.

Soit $P=(x_1,y_2,1)\in E(Q)$ tel que $2P^1O$. Prenons les coordonnées homogènes de $2P$ sous la forme $2P=(x_2,y_2,1)$et montrons que b) :

Supposons y_1^1 0, alors $-2P=(x_2,-y_2,1)$est le deuxième point d'intersection de la tangente en P à la courbe affine :

$$y^2=f(x);\qquad f(x)=x^3+Ax+b$$

L'équation de la tangente en P s'écrit :$y=ax+b$ avec $a=\left\{\frac{dy}{dx}\right\}=\frac{f(x_1)}{2y_1}$

Les coordonnées de P et de $-2P$ vérifie le système:

$$\begin{cases} y^2=x^3+Ax+b \\ y=ax+b \end{cases}$$

$x_1$et x_2 sont solutions de :$(ax+b)^2=x^3+Ax+b$ c'est-à-dire de l'équation du troisième degré : $x^3-a^2x^2+...+b-b^2=0$

Puisque x_1,$x_2$sont entiers, on en déduit que $a^2=x_1+x_2+x_3$ et $a=\frac{f(x_1)}{2y_1}$le sont aussi.

Ainsi y divise$f(x_1)$, et comme $y_1^2=f(x_1)$, on voit que y_1 divise aussi $f(x_1)$.

La théorie sur les résultants (Cf Chapitre1) montre que y_1 divise aussi$V$.

Dans notre cas, on peut voir que :

$(6Ax^2-9Bx+4A^2)(3x^2+A)-(18Ax-27B)(x^3+Ax+B)=4A^3+27B^2$ ■

Théorème mazur

Soit C une courbe elliptique est supposososons qu'il existe une point fini d'order m sur C .

Alors $1\leq m\leq 10$ ou $m=12$.Plus précisément ,l'ensemble des points rationnels d'orders fini forme un sous-groupe qui a l'une des deux formes suivants:

$\mathbb{Z}/N\mathbb{Z}$ avec $1\leq N\leq 10$ ou $N=12$

1. $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ avec $1\leq N\leq 4$ [8]

   Preuve. :voir silverman ■

Théorème mazur

Soit E/Q une courbe elliptique. Alors$E(Q)_{tors}\backsimeq\begin{cases} Z/mZ, m=1,2,3,4,5,6,7,8,9,10,12 \\ ou \\ Z/2Z\times\ Z/2mZ, m=1,2,3,4 \end{cases}$

Exemple Considérons l'équationdeWeierstrass

$E : y^2 = x^3 - 43x + 166$ et $V = 4A^2 + 27B^2 = 425984 = 2^{15} \times 13$.

Donc pour tout point de torsion, $y\,(P)$appartient à l'ensemble :

$\{0, \pm 2, \pm 4, \pm 8, \pm 16, \pm 32, \pm 64, \pm 128\}$

En remplaçant les coordonnées dans l'équation de on obtient l'ensemble des points de torsion :

$$E\,(Q)_{tors} = \{(3, \pm 8)\,, (-5, \pm 16)\,, (11, \pm 32)\,, O\}$$

Remarque 3.2.1 *Comme le montre l'exemple précédent ,les conditions a) et b) du théorème 1 ne sont pas suffisantes pour décrire les points de torsion*

Bibliographie

[1] Marc Joye., Introduction élémentaire de la théorie des courbes elliptiques. Université catholique de louvain. Belgique

[2] M. zitouni., Géométrie Arithmetique et algorethmique des courbes elliptiques.OPU

[3] Husemoller, D., Elliptic Curves, Springer-Verlag, New York, 1987.

[4] Mordell, L.J., On the rational solutions of the indeterminate equations of the third and fourth degrees. Proc. Camb. Philos.Soc. 21 A922), 179-192.

[5] Koblitz, N., Introduction to Elliptic Curves and Modular Forms, Springer-Verlag, New York, 1984.

[6] Silverman, J.H., The Arithmetic of Elliptic Curves, Springer-Verlag, New York, 1986.

[7] Silverman, J.H., Integer points and the rank of Thue elliptic curves. Invent Math. 66 A982), 395-404.

[8] Joseph H. Silverman John Tate., Rational Points on Elliptic Curves, Undergraduate texts on mathematics.

Bibliographie

[1] Marc Joye., Introduction élémentaire de la théorie des courbes elliptiques. Université catholique de louvain. Belgique

[2] M. ZITOUNI., Géométrie Arithmetique et algorethmique des courbes elliptiques.OPU

[3] Husemoller, D., Elliptic Curves, Springer-Verlag, New York, 1987.

[4] Mordell, L.J., On the rational solutions of the indeterminate equations of the third and fourth degrees. Proc. Camb. Philos.Soc. 21 A922), 179-192.

[5] Koblitz, N., Introduction to Elliptic Curves and Modular Forms, Springer-Verlag, New York, 1984.

[6] Silverman, J.H., The Arithmetic of Elliptic Curves, Springer-Verlag, New York, 1986.

[7] Silverman, J.H., Integer points and the rank of Thue elliptic curves. Invent Math. 66 A982), 395-404.

[8] Joseph H. Silverman John Tate., Rational Points on Elliptic Curves, Undergraduate texts on mathemat