N° d'ordre :
N° de série :

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITÉ HAMMA LAKHDAR EL OUED

FACULTÉ DES SCIENCES EXACTES

Mémoire de fin d'étude

MASTER ACADEMIQUE

Domaine : Mathématiques et Informatique
Filière : Mathématiques
Spécialité : Mathématiques fondamentales

Thème

Courbes Elliptiques avec un Point Rationnel d'ordre 6

Présenté par : Berrabah Aicha
kehil Chahinez

Soutenu publiquement devant le jury composé de

Chaia Ahmed	MAA	Président	Univ. El Oued
Youmbai Ahmed El Amine	MCB	Rapporteur	Univ. El Oued
Zelaci Hacene	MCA	Examinateur	Univ. El Oued

Année universitaire 2022 – 2023

Table des matières

Introduction

Dans la théorie des nombres, l'étude des courbes algébriques définis sur un corps K consiste a décrire l'ensemble de tout les points K-rationnels. Autrement dit préciser la taille de cet ensemble. la difficulté varie selon le genre de la courbe à étudier, les plus faciles sont ceux de genre 0 à savoir les droites et les coniques, nous verrons que les points d'une droite rationnelles sont totalement para-métrisables de même pour les cubique singulières et les coniques dont on connaisse un point. Une deuxième catégorie celle de genre supérieur ou égal à 2, il à été prouver que de telles courbes possèdent toujours un nombre fini de points. Finalement, c'est les courbes de genre 1 (les courbes elliptiques) qui pausent le plus de problèmes, car si nous essayons de paramétrer les points d'une courbes elliptique de la manière utiliser pour paramétrer les coniques en générale sela ne marche pas.

L'un des premier résultats est la création par les spécialistes d'une loi de groupe sur l'ensemble des points d'une courbe elliptique, c'est une loi géométrique avec le points à l'infini comme élément neutre, elle repose sur la condition " trois points colinéaires ont une somme nul" est aussi connu par la loi de la corde tangente.

La structure de ce groupe à été bien précisé par un théorème fondamental dù a Mordell, ce dernier stipule que le groupe de points d'une courbe elliptique définie sur le corps de rationnelles est de type fini, c-à-d c'est la somme directe d'un sous groupe de torsion avec une partie libre isomorphe à un $\mathbb{Z}$-module libre de rang fini r où l'entier r s'appelle le rang de la courbe, qui désigne aussi le nombre de générateurs de la partie libre du groupe. Nous entamons ce travail par une introduction aux courbes algébriques (en particulier les cubiques non singulières), cette théorie se trouve dans [][][].....

Après avoir définir les courbes elliptiques, le deuxième chapitre est consacré aux résultats fondamentaux sur l'ensemble des points d'une courbe elliptique notamment la partie contenant les points d'ordre fini.

Dans le troisième chapitre, avons choisi d'étudier les courbes elliptiques ayant un sous groupe de torsion isomorphe à $\frac{\mathbb{Z}}{6\mathbb{Z}}$, le record actuel pour ces courbes est une famille infinie de rang générique 3 (c-à-d la partie libre du groupe contient au moins trois points indépendants d'ordre infini).

Comme résultat, nous avons construit une courbe elliptique paramétrée dans le rang générique égal au record 3, la courbe construite est isomorphe à la courbe obtenu par Eroshkin (voir[]) mais obtenue par une méthode alternative.

Chapitre 1

Préliminaires

La théorie dans cette section se trouve principalement dans .

1.1 Courbes Algébriques

1.1.1 espace Affine, espace projectif

Définition 1 *Le n-espace affine(sur K) est l'ensemble des n-uplets* $\mathbb{A}^n = \mathbb{A}^n(\bar{K}) = (a_1, ..., a_n) : a_i \in \bar{K}$, *où K est un corps local, global ou fini.*

Exemple 2 *Considérons la courbe affine* $C : y^2 = x^4 + ax + b$ *définie sur un corps K. Son corps de fonctions est le corps* $K(x, y)$, *engendré par les éléments transcendants satisfaisant la relation algébrique.*

A partir de ce dernier (espace affine) nous pouvons construire un autre espace comme suite.

Définition 3 *Le n-espace projectif* $\mathbb{P}^n$ *(sur K) est l'ensemble des lignes passantes par l'origine dans* $\mathbb{A}^{n+1}$. *Ainsi :*

$$\mathbb{P}^n = Pn(\bar{K}) = (a_0, ..., a_n) \in \mathbb{A}^{n+1} : \text{ les } a_i = 0 \text{ pour tous sauf un nombre fini}/\sim$$

où nous définissons la relation d'équivalence $\sim$ *par*

$$(x_0, ..., x_n) \sim (y_0, ..., y_n) \Leftrightarrow (x_0, ..., x_n) = \lambda(y_0, ..., y_n) pour quelque \lambda \in \bar{K}^*.$$

Un point $P = (x_0 : ... : x_n) \in P^n$ *représente donc la classe d'équivalence du* $(n+1)$*-tuple* $(x_0, ..., x_n)$, *et les* x_i *sont des coordonnées homogènes ou projectives pour P.*

La courbe affine plane de l'exemple **??** a pour polynôme de définition $f(x, y) = y^2 - x^4 - ax - b$ en deux variables. Ce polynôme peut être complété par la courbe algébrique projective d'équation

$$F(x, y, z) = y^2z^2 - x^4 - axz^3 - bz^4.$$

Les zéros de ce polynôme homogène en trois variables décrivent la courbe projective plane

$$C_0 : y^2z^2 = x^4 + axz^3 + bz^4.$$

1.1.2 Le Genre Algébrique

Les courbes algébriques sont classées en fonction d'un nombre entier non négatif appelé le genre g. Toute courbe de genre 0 définie sur $\mathcal{C}$ est birationnellement équivalente à la droite. Les courbes de genre 0 définies sur $\mathbb{Q}$ sont équivalentes d'un point de vue birationnel à une droite ou à une conique. Nous allons voir que la théorie des courbes de genre 0 est entièrement comprise. Le théorème suivant donne la formule pour le genre d'une courbe non singulière C.

Théorème 4 *Soit une courbe C donnée par l'ensemble des zéros d'un polynôme homogène irréductible $f(X, Y, Z) \in \bar{K}[X, Y, Z]$, où le degré de f est un entier $d \geq 1$.*

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

Nous appelons un point (x, y) dans le plan un point rationnel si ses deux coordonnées sont des rationnels. Nous appelons une droite est rationnelle si son équation peut s'écrire en nombres rationnels, c'est-à-dire s'il a une équation

$$ax + by + c = 0$$

avec des nombres rationnels a, b et c.
Évidemment, si nous avons deux points rationnels, la droite qui les traverse est une droite rationnelle. Et ce n'est pas difficile à deviner ni à prouver que si nous avons deux droites rationnelles, alors leur intersection est un point rationnel. De manière équivalente, si vous avez deux équations linéaires dont les coefficients sont des nombres rationnels et que vous les résolvez, vous obtiendrez des nombres rationnels comme résultat. Le sujet général de ce mémoire est les points rationnels sur les courbes, en particulier les courbes elliptiques, qui sont un cas particulier des courbes cubiques. Mais il serait commode de commencer par des formes quadratiques pour constater les difficultés qui ne se présentent qu'avec les courbes elliptiques.

1.1.3 Les Coniques

sont les courbe algébriques ayant une équation affine de la forme :

$$C : ax^2 + bxy + cy^2 + dx + ey + f = 0 \tag{1.1}$$

La question qui se pose est comment déterminé tous les points rationnels si elles existes ?
Supposons que les coefficients de l'équation **??** sont rationnels. Si une droite rationnelle D intersecte la conique C, les coordonnées des deux points d'intersection (le point d'intersection double dans le cas d'une tangente) dépendent des solutions d'une forme quadratiques $\alpha x^2 + \beta x + \gamma = 0$.

Si l'une d'elle est rationnelle l'autre l'est aussi, cela vient de fait que la somme des racines $\dfrac{-\beta}{\alpha}$ est rationnel. On a alors le théorème suivant :

Théorème 5 *Soit C une conique rationnelle. Si elle possède une solution, alors elle admet une infinité de solutions.*

Cette idée très simple permet de décrire complètement les points rationnels d'une conique. Mais il faut d'abord avoir une solution rationnelle pour en avoir d'autres. Étant donné une conique rationnelle, une question naturelle qui se pose est de savoir s'il existe ou non des points rationnels sur cette conique, une réponse a cette question est donnée par un principe dit de Hasse.
Principe de Hasse :
Théorème (Hasse) : Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$, le cardinal du groupe $E(\mathbb{F}_q)$ est noté $\sharp(E(\mathbb{F}_q))$. Alors :

$$|q + 1 - \sharp(E(\mathbb{F}_q))| \leq 2\sqrt{q}$$

Pour ce qui suit, posons $a = q + 1 - \sharp(E(\mathbb{F}_q))$ Théorème 5 Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$ de cardinalité $q + 1 - a$. Alors la cardinalité de $E(\mathbb{F}_{q^n})$ avec $n \in \mathbb{N}^*$ est égal à $q^n + 1 - \alpha n - \beta n$ où α et β sont les racines complexes du polynôme $x^2 - ax + q$. Supposons $\sharp(E(Fq))$ connu ; alors il existe un moyen simple de calculer $\sharp(E(\mathbb{F}_{q^n}))$. On pose $a = q+1-\sharp(E(\mathbb{F}_H))$; soient α et β les deux racines complexes du polynôme :

$$x^2 - ax + q = (x - \alpha)(x - \beta)$$

La formule est : $\forall n \in \mathbb{N}^* : \sharp(E(\mathbb{F}_{q^n})) = q^n + 1 - (\alpha n + \beta n)$. Illusrons cette théorie par quelques exemple :

Exemple 6 (Conique résoluble) *Soit C_1 une conique rationnelle donnée par l'équation affine*

$$ax^2 + bx + c^2 = y^2,$$

il est facile de voir que $(x, y) = (0, c)$ constitue une solution rationnelle de C, nous allons utilisé cette dernière pour en avoir une infinité de solutions comme le prétend le théorème **??**, *en effet, il suffit de résoudre l'équation $ax^2 + bx + c^2 = (kx + c)^2$ où l'on a posé $y = kx + c$. il en résulte une équation en x de deuxième degré admettant le deux solution 0 et $\frac{-(b-2ck)}{(a-k^2)}$ pour $k \neq a$.*

Exemple 7 (Conique résoluble) *Soit C_2 une conique rationnelle donnée par l'équation affine*

$$x^2 + 7x + 1 = y^2$$

, elle admet la solution $(x, y) = (1, 3)$, en posant $X = x - 1$ et $Y = kx + 3$ on se ramène à résoudre l'équation $(X + 1)^2 + b(X + 1) + c^2 = (kX + 3)^2$ qui possède la solution paramétrée $X = \frac{-(6k-9)}{(k^2-1)}$ pour $k \neq \pm 1$.

Nous sommes maintenant en mesure de commencer notre étude des cubiques.

1.1.4 Les Cubiques

Soit

$$ax^3 + bx^2y + cxy^2 + dy^3 + xc + fxy + gy^2 + hx + iy + j = 0 \tag{1.2}$$

l'équation d'une cubique générale. Nous dirons qu'une cubique est rationnelle si les coefficients de son équation sont des nombres rationnels. Un exemple célèbre est

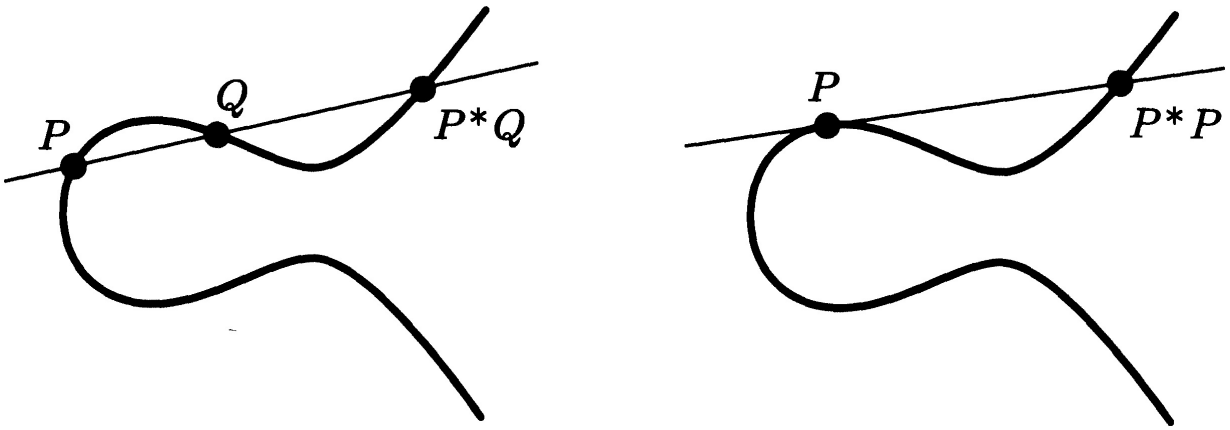
$$x^3 + y^3 = 1,$$

qui en projectif s'écrit sous la forme :

$$x^3 + y^3 = z^3.$$

Trouver les solutions rationnelles de $x^3+y^3 = 1$ revient à trouver les solutions entières de sa forme projective $x^3 + y^3 = z^3$, premier cas non trivial du dernier "théorème" de Fermat. contrairement au conique, nous ne pouvons pas utiliser le principe géométrique pour trouver des solutions sur une cubique, car une ligne rencontre généralement une cubique en trois points. Et si nous avons un seul point rationnel, nous ne pouvons pas projeter la cubique sur une droite, car les deux autres points d'intersections d'une droite qui passe par le premier point rationnel peuvent ne pas être rationnelles sauf si la première solution est un point singulier donc double.
De là, nous pouvons utiliser le principe géométrique si nous pouvons trouver deux points rationnels sur la courbe, nous pouvons généralement en trouver un troisième. En d'autres termes, dessinez la ligne reliant les deux points que vous avez trouvés. Il s'agit d'une rationnelle, et elle rencontre la cubique en un point supplémentaire. Si nous regardons et voyons ce qui se passe lorsque nous essayons de trouver les trois intersections d'une ligne rationnelle avec une cubique rationnelle, nous obtenons une équation cubique à coefficients rationnels. Si deux des racines sont rationnelles, la troisième doit

l'être aussi. Nous donnerons plus loin des exemples explicites, mais le principe est clair. Cela donne donc une sorte de loi de composition :
A partir de deux points P et Q, nous traçons la droite passant par P et Q et nous désignons par $P * Q$ le troisième point d'intersection de la ligne avec la cubique.



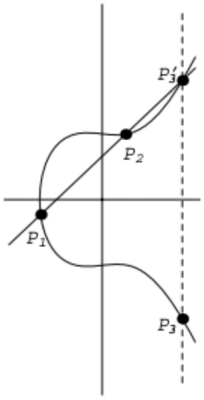
Même si nous n'avons qu'un seul point rationnel P, nous pouvons généralement en obtenir un autre. En traçant la ligne tangente à la cubique en P, nous traçons essentiellement la ligne passant par P et P. La ligne tangente rencontre la cubique deux fois en P, et le même argument montrera que le troisième point d'intersection est rationnel. Nous pouvons alors relier ces nouveaux points et obtenir d'autres points. Ainsi, si nous commençons avec quelques points rationnels, en traçant des lignes, nous en obtenons généralement beaucoup d'autres. mais une autre question se pose :
Si le processus s'arrête en un nombre fini d'opérations ?.
Nous pourrions nous interroger sur la structure algébrique de cet ensemble et de cette loi de composition $P * Q$; par exemple, s'agit-il d'un groupe ?.

Malheureusement, ce n'est pas un groupe ; pour commencer, il est assez clair qu'il n'y a pas d'élément d'identité.

1.1.5 Loi de Groupe

Pour surmonter ce problème, nous définissons un point particulier dans la courbe appelé le point à l'infini, pour l'obtenir, fixez $Z = 0$ dans (**??**) pour trouver $0 = X^3$ et donc $X = 0$, Y étant tout nombre non nul dans K. D'où $O = (0 : Y : 0) = (0 : 1 : 0)$ est le seul point $\bar{K}$-rationnel sur la droite à l'infini $Z = 0$. De plus, O est un point d'inflexion non singulier, la droite tangente étant la droite à l'infini.

Cependant, nous pouvons en faire un groupe de telle sorte que le point rationnel à l'infini O devienne l'élément zéro du groupe. Nous désignerons la loi du groupe par + car il s'agit d'un groupe commutatif. La règle est la suivante :
Pour additionner P et Q, prenez le troisième point d'intersection $P * Q$, le joindre à O, puis prendre le troisième point d'intersection comme étant $P + Q$. Ainsi, par définition, $P + Q = O * (P * Q)$.



Pour des formules explicites de la somme de deux points confère [**?**, **?**, **?**, **?**].
Le problème de trouver des points rationnels dans les droites, les coniques (ayant un point) et les cubique singulière est totalement résolu. Alors seules les cubiques non singulières persistent. Même si la loi + lui donne une structure de groupe, reste a savoir la taille de ce dernier.
Avant de répondre a cette question, discutons les différents formes des cubiques de Weierstrass.

1.1.6 Equations de Weierstrass

Dans notre cas, nous considérons toujours des cubiques rationnelles.
Maintenant que nous avons une idée de la difficulté de trouver des points rationnelles sur les différents types de courbes, à savoir de genre $0, 1$ ou plus, une famille particulière nécessite une étude plus profonde, de ce fait, nous introduisons les courbes elliptiques définies sur le corps des rationnels.

1.1.7 Courbes Elliptiques

Définition 8 *Une courbe elliptique est une cubique non singulière, irréductible de points muni du point à l'infini* $(0 : 1 : 0)$ *d'équation de Weierstrass généralisée :*

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

Pour plus de commodité au calculs, nous utilisons un modèle réduit de courbes elliptiques de la forme :

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

où A et B sont des élément de $\mathbb{Q}$ ou un corps de fonction rationnel s'il s'agit d'une courbe elliptique paramétrée.
A partir de n'importe quel modèle de cubique, on peut être toujours se ramener à un modèle réduit via des changement de variables rationnelles admissibles comme nous pouvons le voir dans cet

Exemple 9 *Considérons l'équation de Weierstrass*

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

où $a_1, ..., a_6$ *sont des constantes rationnelles. Cette forme plus générale (nous l'appellerons l'équation de Weierstrass généralisée) est utile lorsque l'on travaille avec des corps de caractéristique 2 et de caractéristique 3. Si la caractéristique du corps n'est pas 2, alors on peut diviser par 2 et compléter le carré :*

$$(y + \tfrac{a_1x}{2} + \tfrac{a_3}{2})^2 = x^3 + (a_2 + \tfrac{a_1^2}{4})x^2 + (a_4 + \tfrac{a_1a_3}{2})x + (\tfrac{a_3^2}{4} + a_6),$$

qui peut s'écrire comme avec

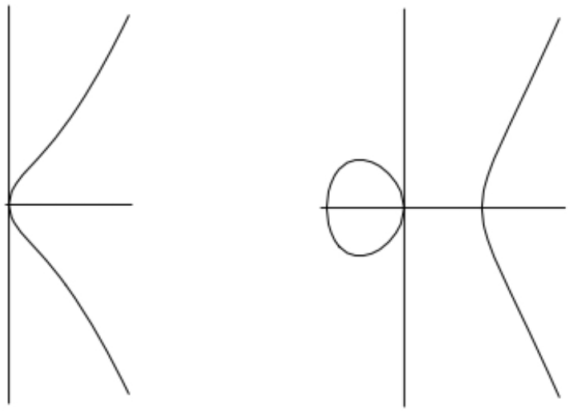
$$y_1^2 = x^3 + a\prime_2x^2 + a\prime_4x + a\prime_6,$$

avec $y_1 = y + a_1x/2 + a_3/2$ *et avec quelques constantes* $a\prime_2, a\prime_4, a\prime_6$*. Si la caractéristique n'est pas non plus 3, alors on peut poser* $x_1 = x + a\prime_2/3$ *et obtenir*

$$y_1^2 = x_1^3 + Ax_1 + B,$$

pour certaines constantes A,B.

Le graphe d'une courbe elliptique est généralement l'un des deux types suivants :



D'après (**??**), nous savons que les points d'une courbe elliptique E, forment un groupe abélien. Une question naturelle qui se pose est "quel groupe peut etre $E(\mathbb{Q})$?"

Théorème 10 (Mordell) *Soit E une courbe elliptique définie sur le corps des rationnels, alors le groupe $E(\mathbb{Q})$ est de type fini.*

$$E(\mathbb{Q}) = T \oplus L$$

où T est le sous groupe de torsion (points d'ordres fini) et L une partie isomorphe à un $\mathbb{Z}$ module libre de rang r.

L'entier non négatif r est le rang algébrique de la courbe elliptique $E(\mathbb{Q})$.
Ce théorème préconise qu'à partir un nombre fini de points d'une courbe elliptique nous pouvons engendrer tout les points de la courbe.

Pour bien comprendre l'arithmétique d'une courbe elliptique E sur K, il faut donc connaître, d'une part le rang sur K et d'autre part la partie de torsion.

Chapitre 2

Points d'ordre fini

Un élément P de tout groupe est dit d'ordre m si

$$mP = \underbrace{P + P + ... + P}_{m \text{ fois}} = 0$$

mais $m'P \neq O$ pour tout entier $1 \leqslant m' < m$. Si un tel m existe, alors P est d'ordre fini ; sinon il a un ordre infini.

Théorème 11 (Nagel-Lutz) *Soit*

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

une courbe cubique non singulière à coefficients entiers a, b, c ; et soit D le discriminant du polynôme cubique $f(x)$, $D = -4a^3c + a^2b^2 + 18abc - 4b^3$–$27c^2$. Soit $P = (x, y)$ un point rationnel d'ordre fini. Alors :

- *x et y sont des entiers ;*
- *Soit $y = 0$, auquel cas P est d'ordre deux, soit y divise D.*

En effet, Comme tout point d'ordre fini a des coordonnées entières. Si P est d'ordre deux, alors nous savons que $y = 0$, nous avons donc terminé. Sinon, $2P \neq O$. Mais $2P$ est aussi un point d'ordre fini, donc il a aussi des coordonnées entières. Dans ([**?**], section 3), les auteurs ont montré que si $P = (x, y)$ et $2P$ ont des coordonnées entières, alors y divise D, Ce qui prouve juste le deuxième point de la théorie

Remarque 12 *À des fins de calcul, la forme plus forte suivante du théorème de $Nagell - Lutz$ est souvent utile. Soit $P = (x, y)$ un point rationnel d'ordre fini avec $y \neq 0$. Alors y^2 divise le discriminant D.*

Nous voulons réitérer que le théorème de $Nagel - Lutz$ n'est pas une déclaration "si et seulement si". Il est tout à fait possible d'avoir des points de coordonnées entières et de y divisant D qui ne soient pas des points d'ordre fini. Le théorème de $Nagel - Lutz$ peut être utilisé pour compiler une liste de points qui comprend tous les points d'ordre fini ; mais il ne peut jamais être utilisé pour prouver qu'un point particulier a effectivement un ordre définit. Pour vérifier qu'un point P est d'ordre fini, il faut trouver un entier $n > 1$ tel que $nP = 0$.

D'autre part, le théorème de $Nagel - Lutz$ peut souvent être utilisé pour prouver qu'un point est d'ordre infini. L'idée est de calculer P, $2P$,... jusqu'à arriver à un multiple nP dont les coordonnées ne sont pas des entiers. Alors on sait que nP, et a priori aussi P, ne peuvent pas être d'ordre fini. Ce calcul peut être accéléré en calculant à la place uniquement les coordonnées x de $2P, 4P, 8P, ...$ en utilisant la formule de duplication jusqu'à ce qu'une certaine coordonnée x ne soit pas un entier.

La question se pose naturellement de savoir quels points d'ordre fini peuvent survenir. Nous avons déjà vu qu'il est facile d'obtenir des points d'ordre deux en prenant le polynôme cubique pour avoir une racine rationnelle. De même, en utilisant notre description des points d'ordre trois, il n'est pas difficile de trouver des courbes cubiques telles que $C(Q)$ ait un point d'ordre trois.
Il est également possible de trouver des points rationnels d'ordre supérieur. Par exemple, le point $P = (1, 1)$ sur la courbe $y^2 = x^3 - x^2 + x$ est d'ordre quatre, puisqu'on vérifie facilement que $2P = (0, 0)$, et on sait que $(0, 0)$ est d'ordre deux. Alors $3P = -P = (1, -1)$ est aussi un point d'ordre 4.
On peut utiliser le théorème de $Nagel - Lutz$ pour vérifier qu'il n'y a pas d'autres points d'ordre fini sur cette courbe. Ici $D = -3$, donc les valeurs possibles pour y sont $+1$ et ± 3. Nous savons déjà que $y = \pm 1$ donne des points d'ordre quatre, nous vérifions donc $y = \pm 3$. Cela conduit à l'équation $x^3 - x^2 + x - 9 = 0$. Les seules racines rationnelles possibles sont des entiers divisant 9, et on vérifie rapidement que $\pm 1, \pm 3 et \pm 9$ ne sont pas des racines. Ainsi les seuls points d'ordre définit sont ceux que nous connaissons ; et le sous-groupe qui se compose de tous les points d'ordre fini est un groupe cyclique d'ordre quatre. En fait, il existe une infinité de courbes avec un point rationnel d'ordre quatre. Pour tout nombre rationnel $t \neq 0, \frac{1}{4}$, le point (t, t) est sur la courbe cubique non singulière

$$y^2 = x^3 - (2t - 1)x^2 + t^2 x$$

De la même manière, on peut écrire une infinité d'exemples de courbes avec des points rationnels d'ordres 5, 6, 7, 8, 9, 10 ou 12. Essentiellement, ces exemples ont été écrits au cours de la seconde moitié du $19^{\text{ième}}$ siècle. Mais personne n'a jamais été capable de trouver ne serait-ce qu'un exemple de courbe cubique avec un point rationnel d'ordre onze. Il y a une bonne raison à cela puisque Billing et Mahler ont prouvé en 1940 qu'une telle courbe n'existe pas ! Beaucoup de gens ont travaillé sur le problème de déterminer quels ordres sont possibles, aboutissant à un très beau et très difficile théorème de Mazur. Dans le cas où le corps de base est $\mathbb{Q}$, Mazur à démontré que le cardinal de la partie de torsion d'une courbe elliptique est majoré par 16 et il a également donné la liste complète de tous les types de sous–groupes de torsion possibles.

Théorème 13 (Mazur) *Soit E une courbe elliptique définie sur $\mathbb{Q}$, alors les seuls sous groupes de torsion possibles de E sur $\mathbb{Q}$ sont donnés par :*

$$\mathbb{T}(\mathbb{Q}) = \begin{cases} \frac{\mathbb{Z}}{n\mathbb{Z}} & 1 \leq n \leq 10 \text{ ou } n = 12, \\ \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{(2n)\mathbb{Z}} & 1 \leq n \leq 4, \end{cases} \tag{2.1}$$

2.1 Points d'ordre deux et trois

Nous commençons notre étude des points d'ordre fini sur les courbes elliptiques en examinant les points d'ordre deux et trois. Comme d'habitude, nous supposerons que notre courbe elliptique est définie sur le corps des rationnels par une équation de Weierstrass

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

et que le point à l'infini O est considéré comme l'élément zéro pour la loi de groupe.

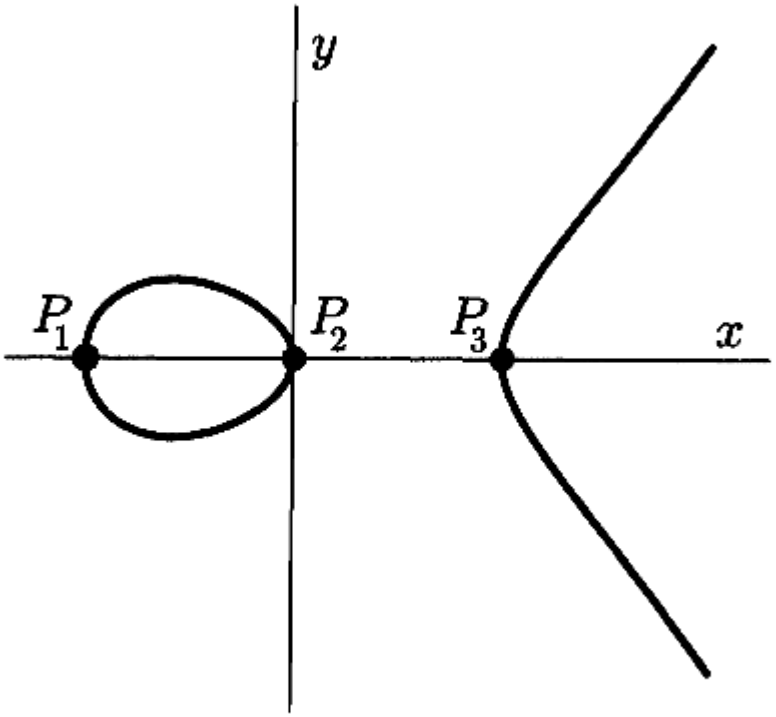
2.1.1 Points d'ordre deux

Quels points de notre groupe satisfont $2P = O$, mais $P \neq O$? Au lieu de $2P = O$, il est plus facile de regarder la condition équivalente $P = -P$ puisque $-(x, y)$ est juste $(x, -y)$, voici les points

avec $y = 0$:

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

où $\alpha_1, \alpha_2, \alpha_3$ sont les racines du polynôme cubique $f(x)$. Donc si on admet des coordonnées complexes, il y a exactement trois points d'ordre deux, car la non-singularité de la courbe assure que $f(x)$ a des racines distinctes. Si les trois racines de $f(x)$ sont réelles, alors l'image ressemble à la figure.



Points of Order Two

Si nous prenons tous les points satisfaisant $2P = O$, y compris $P = 0$, alors nous obtenons l'ensemble $\{O, P_1, P_2, P_3\}$. On voit aisément que dans notre groupe abélien, l'ensemble des solutions de l'équation $2P = O$ forme un sous-groupe. Nous avons donc un groupe d'ordre quatre ; et puisque tout élément est d'ordre un ou deux , il est évident que ce groupe est le produit de deux groupes d'ordre deux $\simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$. Cela signifie que la somme de deux des points P_1, P_2, P_3 doit être égale au troisième, ce qui est évident du fait que les trois points sont colinéaires. Nous savons maintenant exactement à quoi ressemble le groupe de points P tel que $2P = O$. Si nous autorisons des coordonnées complexes, c'est le Groupe des Quatre ; si nous n'autorisons que des coordonnées réelles, il s'agit soit du groupe des quatre, soit d'un cyclique d'ordre deux, selon que $f(x)$ a trois ou une racine réelle ; et si nous restreignons notre attention aux coordonnées rationnelles, il s'agit soit du groupe des quatre, cyclique d'ordre deux, soit trivial, selon que $f(x)$ a trois, une ou zéro racine rationnelle.

2.1.2 Points d'ordre trois

Un tel point vérifie la condition $3P = 0$, Mais nous pouvons également écrit $2P = -P$, donc un point d'ordre trois satisfera la condition équivalente $x(2P) = x(-P) = x(P)$. Inversement, si $P \neq O$ vérifie $x(2P) = x(P)$, alors $2P = \pm P$, donc soit $P = O$ (exclu par hypothèse) soit $3P = 0$.
Autrement dit, les points d'ordre trois sont exactement les points vérifiant $x(2P) = x(P)$.
Pour trouver les points satisfaisant cette condition, on utilise la formule de duplication et on fixe l'abscisse de $2P$ égale à l'abscisse de P. Si on écrit $P = (x, y)$, alors on nous avons l'abscisse de $2P$ est égal

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

En posant cette expression égale à x, avec une multiplication croisée et un peu d'algèbre, on en déduire les abscisse des points d'ordre 3 qui sont exactement les solutions rationnelles de

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

Chapitre 3

Courbe Elliptique avec Groupe de Torsion $\frac{\mathbb{Z}}{6\mathbb{Z}}$

L'un des sujets les plus difficiles de la théorie des nombres est le calcul du rang d'une courbe elliptique (nombre de générateurs de la partie libre du groupe de Mordell-Weil). Ce dernier à fait l'objet de plusieurs conjecture et un large débat sur sa valeur exacte, une question majeur qui se pose

Question 14 *Le rang d'une courbe elliptique est il arbitraire ?*

Même si nous pouvions répondre à cette question, nous aimerions produire des exemples. le plus grand rang connu est dù à N. Elkies avec une courbe elliptique de rang égal à 28 ayant un sous groupe de torsion trivial. La difficulté de construire des courbes de rang élevé varie selon le sous groupe de torsion de la courbe comme en peut le voir sur le tableau record dans [**?**].

Considérons une courbe elliptique sur le corps des rationnelles, d'après le théorème **??** il existe des courbes elliptiques ayant un sous groupe de torsion isomorphe à $\frac{\mathbb{Z}}{6\mathbb{Z}}$, c'est un groupe cyclique engendré par un élément d'ordre 6.

Dans ce mémoire, nous avons choisi d'étudier en particulier les courbes elliptiques avec un sous groupe de torsion isomorphe à $\frac{\mathbb{Z}}{6\mathbb{Z}}$. Les courbes avec ce torsion ont été étudiers par plusieurs spécialistes, on particulier O. Lecacheux [**?**], S. Kihara [**?**], Y. G. Eroshkin, A. Dujella et K. Peral [**?**] et MacLeod [**?**] ont construit des familles infinies de courbes elliptiques avec un rang supérieur ou égal à 3.
Parmis les méthodes enployées, citons la plus simple, il s'agit de la méthode de la 2-descente.

3.1 Descente :

Soit E_t une courbe elliptique sur le corps de fonctions $\mathbb{Q}(t)$ (c-à-d) une courbe avec un paramètre t). supposons que $\forall t \in \mathbb{Q}$ la courbe E_t est de rang r, la méthode de la descente consiste à extraire de la famille infinie E_t une infinité de courbes elliptiques de rang $r+1$.

3.1.1 Description de la 2-descent

Nous imposons un point P d'abscisse x_0 dans une courbe

$$E_t : y^2 = x^3 + a(t)x + b(t)$$

de sort que le membre à droite se réduit

$$H^2 \times (\alpha t^2 + \beta t + \gamma)$$

, nous aurons $P \in E_t$ si la forme quadratique $\square = \alpha t^2 + \beta t + \gamma$ possède une solution, et ainsi on obtient une infinité de courbes contenant le point P d'ordre infini ce qui pourrait augmenter le rang. Cette procédure peut être répéter pour augmenter à chaque fois le rang par 1.

Exemple 15 *Soit $E_t : y^2 = x^3 - x + t^2$, un point P d'abscisse 2 serait dans la courbe si*

$$2^3 - 2 + t^2 = t^2 + 4$$

est un carré dans $\mathbb{Q}$, or $t^2 + 4 = y^2$ possède une solution $(t, y) = (0, 2)$ donc il existe une infinité de solution. en particulier $t = -\frac{k^2+4}{2k}$ est une solution paramétrique.

Retour au courbes avec un sous groupe de torsion $\frac{\mathbb{Z}}{6\mathbb{Z}}$. Pour obtenir une telle courbe E, nous pouvons choisir par exemple une courbe d'équation de Weierstrass qui contient un seul point P d'ordre 2, cela est facile à réaliser car, les courbes elliptiques contenant un seul point d'ordre 2 peuvent toujours s'écrire de la forme

$$E : y^2 = x^3 + Ax^2 + Bx$$

où le polynôme $x^3 + Ax^2 + Bx$ contient une seule racine rationnelle. Maintenant, pour atteindre le torsion $\frac{\mathbb{Z}}{6\mathbb{Z}}$ (point d'ordre 6), il faut que la courbe elliptique E possède de plus un point Q d'ordre 3. En effet, la somme $P + Q$ serait d'ordre égal au PPCM des ordre de P et Q qui est égal exactement à $2 \times 3 = 6$.

Exemple 16 *Soit la courbe elliptique d'équation*

$$E : y^2 = x^3 + Ax^2 + Bx.$$

Le second membre $x^3 + Ax^2 + Bx$ contient la solution 0 qui implique le point $P = (0, 0)$ d'ordre deux dans la courbe E. Pour que 0 soit l'unique solution, il suffit de considérer la condition suivante : Comme nous avons $x^3 + Ax^2 + Bx = x(x^2 + Ax + B)$, le polynôme $x^2 + Ax + B$ doit être irréductible dans $\mathbb{Q}[x]$, autrement dit

Condition 17 *le discriminant $D = A^2 - 4B$ de $x^2 + Ax + B$ n'est pas un carré dans $\mathbb{Q}$.*

Imposant maintenant sur E un point $Q = (x, y)$ d'ordre 3, d'après **??**, *il suffit de résoudre*

$$\frac{x^4 - 2Bx^2 + b^2}{4x^3 + 4Ax^2 + 4Bx} = x.$$

Ceci est équivalent à

$$3x^4 - (-4A)x^3 - (-4B)x^2 - (-2B)x - B^2 = 0.$$

Prenons par exemple $x = 1$ comme abscisse du point Q supposé d'ordre 3. cela implique

$$-4A - 6B + B^2 - 3 = 0,$$

et nous avons $A = (\frac{1}{4})B^2 - (\frac{3}{2})B - (\frac{3}{4})$ comme solution. Finalement, nous obtenons une famille de courbes elliptiques sur $\mathbb{Q}(B)$ avec le point $P = (0, 0)$ d'ordre 2 et le point $Q = (1, \frac{1}{2}(B - 1))$ d'ordre 3, ainsi le point $P + Q = (B, \frac{-1}{2}B^2 + \frac{1}{2}B)$ est d'ordre 6.

Dans ce qui suit, nous verrons différents modèles de courbes elliptiques paramétrées avec un sous groupe de torsion $\frac{\mathbb{Z}}{6\mathbb{Z}}$, ces modèles ont été utiliser pour construire des familles infinis de courbes elliptiques dont le groupe de Mordell-Weil est isomorphe à $\frac{\mathbb{Z}}{6\mathbb{Z}} \oplus \mathbb{Z}^3$.

3.2 Modèle Gènèral

La forme normale de Tate pour une courbe elliptique est donnée par

$$E(b,c): \quad y^2+(1-c)xy-by=x^3-bx^2$$

Il est non singulier si et seulement si $b\neq 0$. En utilisant la loi d'addition pour le point $P=(0,0)$ on trouve

$$3P=(c,b-c), -3P=(c,c^2).$$

Il s'ensuit que P est un point de torsion d'ordre 6 pour $b=c+c^2$. Donc, pour $b=c+c^2$ on écrit la courbe sous la forme $y^2=x^3+A(c)x^2+B(c)x$. Nous avons

$$A(c)=1+6c-3c^2, \quad B(c)=-16c^3$$

Aux nouvelles coordonnées, le point de torsion d'ordre 6 est $(-4c, 4c(1+c))$.

3.3 CONSTRUCTION DE KIHARA POUR LE RANG 3

Kihara dans [**?**] considère la courbe projective

$$\left(x^2-y^2\right)^2+\left(2ax^2+2by^2\right)z^2+cz^4=0$$

puis il utilise les substitutions et arrive à la courbe elliptique

$$\begin{aligned} X&=\frac{x^2}{y^2},\\ Y&=\frac{x\left(cz^2+ax^2+by^2\right)}{y^3}\end{aligned}$$

et arrive à la courbe elliptique

$$E: \quad Y^2=X\left(\left(a^2-c\right)X^2+(2ab+2c)X+\left(b^2-c\right)\right)$$

Le point $P=(1,a+b)$ est sur E. Forcer P à être d'ordre 3 implique $c=\frac{(3a-b)(a+b)}{4}$ auquel cas $P+(0,0)$ est d'ordre 6. Avec cette valeur de c la courbe E est donnée par

$$Y^2=X^3+A(a,b)X^2+B(a,b)X$$

où

$$\begin{aligned} A(a,b)&=2\left(3a^2+6ab-b^2\right),\\ B(a,b)&=-(a-b)^3(3a+5b).\end{aligned}$$

En imposant de nouveaux points sur la courbe, Kihara obtient une famille de groupe de torsion $\mathbb{Z}/6\mathbb{Z}$ et de rang au moins 3 donné comme $y^2=x^3+a_{63K}(t)x^2+b_{63K}(t)x$ où

$$\begin{aligned} a_{63K}(t)=&-2\left(64t^8-1952t^7-4652t^6-10172t^5-28955t^4+35602t^3\right.\\ &\left.-56987t^2+83692t+9604\right)\\ b_{63K}(t)=&(t-7)^3(t+2)^3(2t+1)^3(4t-7)^3\left(2t^2-91t+98\right)\left(4t^2+13t+1\right)\end{aligned}$$

Les abscisses de trois points indépendants d'ordre infini sont :

$$x\left(Q_1\right)=\frac{9(-7+t)^2(2+t)^2(1+2t)^2(-7+4t)^2\left(7+2t^2\right)^2}{\left(-7-4t+2t^2\right)^2}$$
$$x\left(Q_2\right)=\frac{(-7+t)^2(2+t)^2(1+2t)^2(-7+4t)^2\left(7+2t^2\right)^2}{\left(-7+14t+2t^2\right)^2}$$
$$x\left(Q_3\right)=\frac{(-7+t)^2(2+t)^2(1+2t)^2(-7+4t)^2\left(-7+14t+2t^2\right)^2}{\left(-7-4t+2t^2\right)^2}.$$

3.4 CONSTRUCTION D'EROSHKIN POUR LE RANG 3 :

En 2008 Eroshkin à construit un autre exemple de courbe de rang 3 sur $\mathbb{Q}(s,t)$. Le point de départ de sa construction est la famille biparamétrique de rang >2 sur $\mathbb{Q}(u,v)$, donnée par

$$\begin{aligned}A(u,v)&=v^8u^4+2u^7v^5+3u^6v^6+2u^5v^7+3u^4v^2+3v^4u^2-12u^3v^3+u^8v^4-3u^6\\&\quad-6u^5+7u^4-3u^2+6u^3-6v^5+7v^4-3v^6+21u^6v^2+36u^4v^4-9u^2v^2\\&\quad+12v^2u-24u^4v^5-9u^4v^6+36u^5v^3+21u^2v^6-24u^5v^4-10v^4u-6v^7u^2\\&\quad+4u^5v^6-2u^2v^5+2u^4v^7-14u^3v^6+8u^5v-9u^6v^4-18u^5v^5+2v^7u^3+12vu^2\\&\quad+2u^3v-6v^6u-20u^2v^3+8v^5u-6u^6v+36u^3v^5+2u^7v^3-10u^4v+4u^6v^5\\&\quad-6uv+2v^3u-6u^7v^2-14u^6v^3-3v^2+6v^3+2u^7v^4-2u^5v^2-20u^3v^2,\\B(u,v)&=-16(u+v)^3(-1+v)^3(1+v)^3(-1+u)^3(1+u)^3\\&\quad\times\left(u^2+uv+v^2-2vu^2-2v^2u+u^3v+v^3u-2u^3v^2-2u^2v^3+u^4v^2+v^4u^2+u^3v^3\right).\end{aligned}$$

La courbe $y^2=x^3+A(u,v)x^2+B(u,v)x$ contient les points avec les coordonnées en x

$4(v-1)^2(1+v)^3(-1+u)^2(1+u)^3$ et $-4(u-1)(u+1)(v-1)^3(v+1)^2(u+v)^3$.
Forcer le point d'abscisse $3(v-1)^2(v+1)^2(-1+u)^2(1+u)^2(v+u)^2$ à appartenir à la courbe conduit à la condition $v=1/3$. Par substitution $u=(1-t)/(1+t)$ et quelques simplifications, on obtient la courbe de rang 3 d'Eroshkin à coefficients

$$\begin{aligned}a_{63E}(t)&=16+576t-1408t^2-1440t^3+1608t^4+720t^5-352t^6-72t^7+t^8,\\b_{63E}(t)&=27648(-2+t)^3t^3(1+t)^3\left(2+t^2\right)^2,\end{aligned}$$

et les coordonnées x de trois points indépendants $R_1,\ R_2,\ R_3$ sont données par :

$$\begin{aligned}x\left(R_1\right)&=864(-2+t)^3t^3,\\x\left(R_2\right)&=3456t^2(1+t)^3,\\x\left(R_3\right)&=288(-2+t)^3t^3(1+t)^2.\end{aligned}$$

Une autre façon d'obtenir une famille de rang 3 à partir de la famille à deux paramètres d'Eroshkin est de prendre $v=-1/3$. Par substitution $u=(1-t)/(1+t)$, comme ci-dessus, on obtient

$$\begin{aligned}a_{63ER}(t)&=256t^8-2304t^7-3232t^6+1008t^5+2337t^4-504t^3-808t^2+288t+16,\\b_{63ER}(t)&=27648\left(16t^4-11t^2+4\right)(2t-1)^3(t+1)^3t^3\end{aligned}$$

et trois points indépendants d'ordre infini S_1,S_2,S_3 avec des coordonnées x

$$\begin{aligned}x\left(S_1\right)&=1728t^2(t+1)^3,\\x\left(S_2\right)&=864t^3(2t-1)^3,\\x\left(S_3\right)&=864t^3(t+1)^2(2t-1).\end{aligned}$$

3.5 UNE CONSTRUCTION DIRECTE DE DUJELLA ET PERAL (2012) :

L'exemple suivant est basé sur l'utilisation de la 2-descente comme suit. Considérons la courbe générale avec torsion $\mathbb{Z}/6\mathbb{Z}$, c'est-à-dire :

$$y^2 = x^3 + x^2(1 + 6c - 3c^2) + x(-16c^3).$$

On impose d'abord $16c^2$ comme coordonnée d'un nouveau point, cela équivaut à résoudre $1 + 5c + 13c^2 = \square$. La paramétrisation correspondante est $c = -\frac{(-4+u)(-2+u)}{(-13+u^2)}$. Ce nous donne un point d'ordre infini et une courbe de rang au moins 1 sur $\mathbb{Q}(u)$ dont les coefficients sont

$$A_{61}(u) = 601 - 180u - 152u^2 + 72u^2 - 8u^4,$$
$$B_{61}(u) = 16(-4 + u)^3(-2 + u)^3(-13 + u^2).$$

Observez maintenant qu'imposer $4(-4+u)(-2+u)^3$ comme nouveau point revient à résoudre $-103+12u+4u^2 = \square$. Ceci peut être réalisé avec $u = -\frac{103+t^2}{4(-3+t)}$ famille a les coefficients suivants Le nouveau

$$A_{63}(t) = -2(26009437 + 18059772t + 5057576t^2 + 813612t^3 + 89370t^4 + 7860t^5 + 608t^6 + 36t^7 + t^8),$$
$$B_{63}(t) = (5 + t)^3(11 + t)^3(79 + 8t + t^2)^3(8737 + 1248t - 2t^2 + t^4).$$

Dans ce cas, la famille a un rang > 3. Ci-dessous, nous listons les abscisses des trois points indépendants d'ordre infini sur la courbe

$$x(P_1) = 4(5 + t)^2(11 + t)^2(79 + 8t + t^2)^2,$$
$$x(P_2) = (5 + t)(11 + t)(79 + 8t + t^2)^3,$$
$$x(P_3) = \frac{64(4 + t)^2(5 + t)^2(11 + t)^2(79 + 8t + t^2)^2}{(29 + 6t + t^2)^2}.$$

Les deux premiers points sont ceux que nous avons imposés dans la constructions, tandis que le troisième apparaît dans le dernier changement. Donc ce changement produit deux nouveaux points indépendants d'ordre infini et par conséquent cette famille a au moins le rang 3.

3.6 LA CONSTRUCTION PAR MACLEOD (2013) :

Une famille de rang 3 provient du papier de MacLeod [**?**]. La courbe de rang 3 a des coefficients polynomiaux :

$$\begin{aligned}
a_{ML}(t) =& 60637t^{16} - 944657615t^{15} + 31848156014t^{14} + 755909592013t^{13} - 673080292884t^{12} \\
&+ 1307034748065611t^{11} - 226951225t^{10} - 154581659288296019t^9 - 510978585000097818t^8 \\
&+ 496074059556450416t^7 - 489634848796803349 66t_6 + 878594688586562760 05t^5 \\
&+ 127778653981127482476 4t^4 - 861560195308301691408t^3 + 207209922649820722t^2 \\
&- 1499601599678467324208t - 13576669409260628 68067 \\
b_{ML}(t) =& -(t^2 - 14t - 83)^3(17t^2 - 226t - 367)^3(t^2 + 58t - 347)^3 \\
&(t^2 - 290t + 2017)^3 x = x(4451 - 26680t + 2985406 + 7487800 - 1005590264 - 81635904813 \\
&+ 149228674362 - 55316709112t + 68821828189),
\end{aligned}$$

et les $x-$coordonnées de trois points indépendants d'ordre infini Q_1, Q_2 et Q_3 sont

$$
\begin{aligned}
x(Q1) =& -4(13t^2-458t+1021)^2(t^2+4t-149)^2(t^2-290t+2017)(t^2+58t-347)\\
&(17t^2-226t-367)(t^2-14t-83),\\
x(Q_2) =& -9(17t^3-226t-367)^3(t^2-14t-83)^3(t^3-290t+2017)(t^22+58t-347),\\
x(Q_3) =& (4451-26680t+298540t+7487800-10055902648163590483+1492286743662\\
&-55316709112t+68821828189)(17t^2-226t-367)^2(t2-14t-83)^2.
\end{aligned}
$$

3.7 CONSTRUCTION DE LECACHEUX POUR LE RANG 3 :

Dans [**?**] une famille de rang 3 vient de la spécialisation dans la famille de rang 2 donnée par Lecacheux. Dans cet article, Lecacheux construit quatre familles biparamétriques de courbes de groupe de torsion $\mathbb{Z}/6\mathbb{Z}$ et de rang 2 sur $\mathbb{Q}(s,t)$, et par spécialisation de s elle obtient une famille de courbes de cette torsion et de rang 3 sur $\mathbb{Q}(t)$. Le modèle de départ utilisé par Lecacheux pour la torsion $\mathbb{Z}/6\mathbb{Z}$, une fois traduit en $(0,0)$, est $y^2=x^3+a_6(d)x^2+b_6(d)x$ où

$$
\begin{aligned}
a_6(d) &= -3-6d+d^2,\\
b_6(d) &= 16d.
\end{aligned}
$$

Lecacheux montre que l'utilisation de l'une des quatre valeurs

$$
\begin{aligned}
d_1 &= \frac{(-t^2+s)\,(1+ts)\,(t-s^2)}{(-1+t)t(-1+s)s(t+s)},\\
d_2 &= \frac{(-s^2+t(1+t)(1+s))\,(-t^2+(1+t)s(1+s))}{ts(1+t+s)(t+s+ts)},\\
d_3 &= \frac{(t+s+ts(2+t+s))\,((1+t+s)^2+ts(1+ts+2(t+s)))}{t\,(1+t+t^2)\,s\,(1+s+s^2)},\\
d_4 &= -\frac{(t-1)(s-1)\,(t^2+ts+s^2)\,(1+ts+2(t+s))}{(t+s)\,(-t^2+s)\,(t-s^2)},
\end{aligned}
$$

la famille biparamétrique résultante est de rang ≥ 2 sur $\mathbb{Q}(s,t)$ Puis elle se spécialise et obtient une famille de rang 3 sur $\mathbb{Q}(t)$. La valeur de d est une expression rationnelle avec numérateur de degré 10 et dénominateur de degré 9 donnée par :

$$
\frac{(-1+t+t^2)\,(-1+2t+t^3)\,(-1+2t-t^2+t^3+2t^4+t^5)}{t^2(1+t)(-1+2t)\,(-1+2t+t^2)\,(-1+t+t^2+t^3)}.
$$

La courbe de rang 3 a des coefficients polynomiaux en t de degré 20 et 40 respectivement. Les coefficients sont

$$
\begin{aligned}
a_{63L}(t) =& 1-10t+35t^2-36t^3-61t^4+146t^5+5t^6-254t^7+300t^8+58t^9-436t^{10}-294t^{11}\\
&+496t^{12}+710t^{13}+93t^{14}-434t^{15}-489t^{16}-264t^{17}-73t^{18}-6t^{19}+t^{20},\\
b_{63L}(t) =& 16t^6(1+t)^3(-1+2t)^3\left(-1+t+t^2\right)\left(-1+2t+t^2\right)^3\left(-1+2t+t^3\right)\left(-1+t+t^2+t^3\right)^3\\
&\times\left(-1+2t-t^2+t^3+2t^4+t^5\right).
\end{aligned}
$$

et x les coordonnées a de trois points indépendants d'ordre infini P_1, P_2 et P_3 sont

$$
\begin{aligned}
x\left(P_1\right) &= 4t(1+t)(-1+2t)\left(-1+t+t^2\right)\left(-1+2t+t^2\right)^2\left(-1+2t+t^3\right)\left(-1+t+t^2+t^3\right)^2\\
x\left(P_2\right) &= 4t^4(1+t)(-1+2t)\left(-1+2t+t^2\right)^2\left(-1+2t+t^3\right)\left(-1+2t-t^2+t^3+2t^4+t^5\right)\\
x\left(P_3\right) &= 4t^2(-1+2t)\left(-1+2t+t^2\right)^2\left(-1+t+t^2+t^3\right)^2\left(-1+2t-t^2+t^3+2t^4+t^5\right)
\end{aligned}
$$

Dans la section suivante, à partir du modèle utiliser par O. Leucacheux, nous construisons notre propre courbe de rang 3 avec un sous groupe de torsion $\frac{\mathbb{Z}}{6\mathbb{Z}}$.

3.8 Résultats

3.8.1 Familles de rang ≥ 1

Considérons la courbe donné par l'équation :

$$y^2 = x^3 + (-6c + c^2 - 3)x^2 + 16cx \tag{3.1}$$

On appliquant la méthode de la 2-descente nous avons trouver plusieurs familles infinie de rang égal à 1. nous avons omit les détailles et nous donnons dans le tableau (**??**) les abscisses des points à imposer, les formes quadratiques associées et le changement de variable qui mène a une courbe de rang 1.

3.8.2 Familles de rang ≥ 2

De la même manière, nous pouvons imposer deux points indépendants d'ordre infinis, cela en regardons les points dont les forme quadratiques ont une composante commune, dans notre cas plusieurs familles peuvent être obtenues. Puisque les constructions sont similaires, nous citons seulement l'une d'elles. Si dans (**??**)nous imposons les deux points P_1 et P_2 d'abscisses respectivement $x(P_1) = 3$ et $x(P_2) = \frac{16c}{3(3c+1)}$ cela conduit à résoudre simultanément les deux formes quadratiques

$$3c(3c - 2) = \square$$

et

$$3c(3c + 1) = \square.$$

Pour la première $c = (-\frac{k^2}{6k+6})$ est une solution, remplacer dans la deuxième donne

$$c = \frac{(s^2 + 2)^2}{12(s + 1)s(s - 2)}.$$

Avec cette valeur de c, la famille qui en résulte possède à la fois les points P_1 et P_2.

3.8.3 Familles de rang ≥ 3

En utilisant la famille e rang ≥ 2 obtenue précédemment, nous avons calculer avec Magma [**?**] le rang pour $(3 < s < 100)$ et nous avons remarquer que le rang est en réalité ≥ 3 sauf un nombre fini de valeur, delà en constate que le changement de variable $c = \frac{(s^2+2)^2}{12(s+1)s(s-2)}$ produit en faite un autre point additionnel. Nous n'avons pas trouver ce point mais il s'est avéré qu'elle est isomorphe à la courbe d'Eroshkin mentionnée dans [**?**].

TABLE 3.1 – Familles de rang supérieur ou égal à 1

Numéro	Abscisse du point à imposé	Forme quadratique associée	Paramétrisation
1	1	$10c + c^2 - 2$	$\frac{k^2+2}{2k+10}$
2	-4	$-10c + c^2 - 7$	$\frac{k^2+7}{2k-10}$
3	$-4c(c-2)$	$-(3c-2)(c-2)$	$2\frac{k^2+1}{k^2+3}$
4	$4c^2$	$c(5c+4)$	$\frac{4}{k^2-5}$
5	3	$3c(3c-2)$	$\frac{k^2}{6k-6}$
6	$-\frac{16}{27}c(2c-9)$	$-3(10c-9)(2c-9)$	$\frac{9}{2}\frac{k^2+12}{k^2+60}$
7	$-\frac{4}{3}c(c-4)$	$-3c(c-4)$	$\frac{12}{k^2+3}$
8	$16\frac{c}{c+3}$	$c(c+3)$	$\frac{3}{k^2-1}$
9	$\frac{16}{3}\frac{c}{3c+1}$	$3c(3c+1)$	$\frac{k^2}{6k+3}$
10	$48\frac{c}{2c+9}$	$3(6c-5)(2c+9)$	$\frac{k^2+135}{12k+132}$
12	$-c(c-6)$	$-(3c-2)(c-6)$	$\frac{2}{3}\frac{k^2+27}{k^2+3}$
13	$\frac{-16}{c-5}$	$-(c-1)(c-5)$	$\frac{k^2+5}{k^2+1}$
14	$\frac{-16}{c+3}$	$-(c+3)$	$-k^2-3$
15	$\frac{-27}{2c-9}$	$-3(10c-9)(2c-9)$	$\frac{9}{2}\frac{k^2+12}{k^2+60}$
16	$\frac{1}{3}\frac{25c-9}{3c-1}$	$3(25c-9)(3c-1)$	$\frac{k^2-27}{30k-156}$
17	$\frac{c-9}{c-3}$	$(c-9)(c-3)$	$\frac{k^2-27}{2k-12}$
18	$-\frac{1}{2}c$	$2(2c+7)(c-10)$	$\frac{k^2+140}{4k-26}$
19	$\frac{9}{2}c$	$2(3c-2)(6c-5)$	$\frac{k^2-20}{12k-54}$
21	$-c(c-5)$	$-(c-5)$	$-k^2+5$
22	$\frac{c-1}{c+1}$	$(c-1)(c+1)$	$\frac{k^2+1}{2k}$
23	$\frac{c-25}{c-7}$	$(c-25)(c-7)$	$\frac{k^2-175}{2k-32}$
24	$\frac{25}{6}c$	$6(10c-9)(15c-14)$	$\frac{3}{10}\frac{3k^2-2800}{(k-30)(k+30)}$
25	$\frac{25}{4}c$	$(5c+4)(20c-11)$	$\frac{k^2+44}{20k+25}$
26	$\frac{-1}{20}c$	$5(5c+76)(4c-85)$	$\frac{k^2+32300}{20k-605}$
27	$\frac{-1}{12}c$	$3(4c+45)(3c-52)$	$\frac{k^2+7020}{12k-219}$
28	$\frac{-1}{6}c$	$6(3c+22)(2c-27)$	$\frac{k^2+3564}{12k-222}$
29	$\frac{-4}{15}c$	$15(5c+27)(3c-35)$	$\frac{k^2+14175}{30k-1410}$
30	$\frac{-4}{3}c$	$3(3c+5)(c-9)$	$\frac{k^2+135}{6k-66}$
31	$\frac{-9}{4}c$	$(12c+13)(3c-28)$	$\frac{k^2+364}{12k-297}$
32	$\frac{-16}{21}c$	$21(7c+18)(3c-28)$	$\frac{k^2+10584}{42k-2982}$
33	$\frac{-9}{10}c$	$10(15c+34)(6c-55)$	$\frac{k^2+18700}{60k-6210}$
34	$\frac{-25}{24}c$	$6(40c+81)(15c-136)$	$\frac{k^2+66096}{120k-25350}$
35	$\frac{-25}{14}c$	$14(35c+46)(10c-91)$	$\frac{k^2+58604}{140k-38150}$
36	$\frac{-25}{6}c$	$6(30c+19)(5c-54)$	$\frac{k^2+6156}{60k-9150}$
37	$\frac{-c}{c-8}$	$(c-10)(c-8)$	$\frac{k^2-80}{2k-18}$
38	$\frac{-4c}{(c-2)}$	$(c-10)(c-2)$	$\frac{k^2-20}{2k-12}$
39	$\frac{-12c}{(c-6)}$	$3(c-4)(c-28)$	$4\frac{k^2-21}{k^2-3}$
40	$(\frac{-16c}{(c-6)})$	$(c-10)(c-5)$	$\frac{k^2-50}{2k-15}$
41	$\frac{-20c}{c-6}$	$5(5c-54)(c-6)$	$\frac{k^2-1620}{10k-420}$
42	$\frac{-24c}{(c-7)}$	$3(3c-35)(c-7)$	$\frac{k^2-735}{6k-168}$
43	$\frac{-4ac}{(c-a1}$	$a(ac+1)((-a)c+(a+4)(a+1))$	$\frac{4a^3+5a^4+a^5-k^2}{a(a^3+k^2)}$
44	$\frac{24c}{(c+5)}$	$3(3c+5)(c+5)$	$\frac{k^2-75}{6k+60}$
45	$\frac{20c}{(c+4)}$	$5(5c+4)(c+4)$	$\frac{k^2-80}{10k+120}$
46	$\frac{12c}{(c+2)}$	$3(3c-2)(c+2)$	$\frac{k^2+12}{6k+12}$

Conclusion et Perspective

Cette étude a contribué à enrichir les connaissances et à éclairer l'arithmétique des courbes elliptiques (Le thème général de cette thèse) où nous avons mentionné que le comptage des points rationnels sur les courbes algébriques, en particulier les courbes elliptiques pause un grand problème.

Un théorème fondamental de Mordell (1922) affirme que les points d'une courbe elliptique sur le corps des rationnelles muni d'une addition dite la loi de la corde tangente forme un groupe de type fini, c-à-d une somme directe d'un sous groupe de torsion (ensemble des points d'ordre fini) avec une partie libre isomorphe à r copies de $\mathbb{Z}$.
Si le éléments du sous groupe de torsion sans totalement décrites par les théorème de Nagel-Lutz et Mazur, la taille de la partie libre (rang de la courbe) demeure un mystère car il n'existe aucun algorithme qui garanti le calcul exacte de sa valeur.

Notre Principal résultat est la construction d'une famille infinie de courbes elliptiques avec un sous groupe de torsion isomorphe à $\mathbb{Z}/6\mathbb{Z}$ ayant un rang générique supérieur ou égal à 3. Même si nous avons égalé le record actuel pour ce torsion la courbe construite est en faite isomorphe celle d'Eroshkine.
Enfin, comme perspectives il serait intéressant de passer à l'études des courbes elliptiques avec un autre sous groupe de torsion de la liste mentionnée par Mazur.

Résumé

Dans ce mémoire nous avons étudié les courbes elliptiques, en particulier celles avec un sous groupe de torsion $\mathbb{Z}/6\mathbb{Z}$, nous également construit des familles infinies de rang au moins 1, 2 puis via une 2-descente un exemple d'une courbe de rang supérieur ou égal à 3 à été construit ce qui atteint le record pour les courbes elliptiques avec ce torsion, cette dernière est isomorphe à la courbe d'Eroshkin mais obtenue avec une une differente méthode.

Abstract

In this dissertation we studied elliptic curves, in particular those with a torsion subgroup $\mathbb{Z}/6\mathbb{Z}$, we also constructed infinite families of rank at least 1, 2 then via a 2-descent an example of a curve of rank greater than or equal to 3 was constructed which reaches the record for elliptic curves with this torsion, the latter is isomorphic to the Eroshkin curve but obtained with a different method.
. (The calculations were carried out by Magma)

Remercier

Louanges et remerciements à Dieu, qui nous a donné la force de mener à bien notre travail
J'adresse également mes remerciements à tous nos enseignants qui ont travaillé dur avec nous dans notre parcours académique
Je suis très honoré de remercier la présence de mon co-encadrant Mr.Youmbai Ahmed El Amine
Je remercie également les membres de ce jury de thèse pour leur participation et pour tous leurs commentaires intéressants
Sur le plan personnel, je remercie ma famille bien-aimée (KEHIL), en particulier mon père MOHAMMED.KEHIL, ma mère, OUAHIBA .KEHIL, et mes frères ZAINAB, DAREEN et Abdullah.
et mes chers grands-parents pour leurs encouragements et leur amour pour moi
Je remercie mes deux amis adorés Hizia .Fartas et Noura.Saiar Pour m'avoir accompagné dans mon parcours scolaire et m'avoir soutenu Je remercie également mon amie Aicha Berrabah
Je remercie également moi-même et mon groupe bien-aimé BTS

Bibliographie

[1] A. Dujella, https ://web.math.pmf.unizg.hr/∼duje/index.html.

[2] A. Dujella, C. Peral and P. TADIĆ, Elliptic Curves with torsion group $\frac{\mathbb{Z}}{6\mathbb{Z}}$ arXiv :1503.03667v1.

[3] W. Fulton, Algebraic curves : an introduction to algebraic geometry. Addison-Wesley, 1989.

[4] S. Kihara, On the rank of elliptic curves with a rational point of order 6, Proc. Japan Acad. Ser. A Math. Sci. 82 (2006), 81–82.

[5] O. Lecacheux, Rang de courbes elliptiques avec groupe de torsion non trivial, J. Théor. Nombres Bordeaux 15 (2003), 231–247, Les XXIIèmes Journées Arithmetiques (Lille, 2001).

[6] A. MacLeod, A simple method for high-rank families of elliptic curves with specified torsion, arXiv :1410.1662

[7] W. Bosma, J.J. Cannon, C. Fieker and A. Steel (eds.), Handbook of Magma functions, Edition 2.20-9, 2014.

[8] L.J. Mordell, Diophantine Equations, Pure and Applied Mathematics, vol. 30 (Academic, London, 1969).

[9] J.H. Silverman, Advanced topics in the arithmetic of elliptic curves, Vol 151, Springer Science and Business Media, 2013.

[10] Silverman, J. H. and Tate, J. T. (1992). Rational points on elliptic curves (Vol. 9). New York : Springer-Verlag.

[11] Silverman, J. H. (2009). The arithmetic of elliptic curves (Vol. 106). Springer Science and Business Media.

[12] Washington, L. C. (2008). Elliptic curves : number theory and cryptography. CRC press.