



UNIVERSITÉ de CAEN BASSE NORMANDIE

U.F.R Sciences

ECOLE DOCTORALE SIMEM

LABORATOIRE DE MATHÉMATIQUES NICOLAS ORESME

THÈSE

Présentée par

Fanomezantsoa Patrick RABARISON

et soutenue le 19 Septembre 2008

en vue de l'obtention du

DOCTORAT de l'UNIVERSITÉ de CAEN

Specialité : Mathématiques et leurs interactions

Arrêté du 07 Août 2006

Torsion et rang des courbes elliptiques définies sur les corps de nombres algébriques

Après avis de

John CREMONA Professeur, University of Warwick, Royaume-Uni (Rapporteur)
Odile LECACHEUX Maître de Conférences, H.D.R, Université Paris VI (Rapporteur)

MEMBRES du JURY

John BOXALL Professeur, Université de Caen Basse-Normandie
Christophe DELAUNAY Maître de Conférences, Université Lyon I
Odile LECACHEUX Maître de Conférences, H.D.R, Université Paris VI
Denis SIMON Professeur, Université de Caen Basse-Normandie (Directeur)

REMERCIEMENTS

A travers ces quelques lignes, je vais tenter de satisfaire au difficile exercice de remerciements. Eh oui, difficile puisque je ne veux oublier personne. C'est pourquoi, je remercie par avance ceux dont le nom n'apparaît pas dans cette page et qui m'ont aidé d'une manière ou d'une autre.

C'est avec joie que j'adresse mes premières remerciements à mon directeur de thèse Denis Simon, qui a su m'initier à la recherche depuis mon mémoire de DEA jusqu'à la thèse. Je lui remercie de m'avoir fait découvrir ses visions sur beaucoup de domaines de la théorie des nombres à travers son regard de mécanicien ainsi que de m'avoir accordé la confiance et la grande liberté nécessaire à l'accomplissement de mes travaux, tout en y gardant un oeil critique et avisé. Plus qu'un encadrant, je crois avoir trouvé en lui le père mathématicien qui m'a aidé aussi bien dans le travail que dans la vie lorsque j'en avais besoin. Je lui remercie d'avoir su supporter mes humeurs dépressives au cours des années de thèse.

Je remercie John Cremona et Odile Lecacheux de m'avoir fait l'honneur d'être les rapporteurs de cette thèse. J'éprouve un profond respect pour leur travail. Je leur remercie aussi pour la rapidité avec laquelle ils ont lu mon manuscrit et l'intérêt qu'ils ont porté à mon travail. Merci également aux autres membres du jury qui ont accepté de juger ce travail : John Boxall et Christophe Delaunay.

Le Laboratoire de Mathématiques Nicolas Oresme m'a permis de réaliser ces quelques travaux de recherches. Je tiens à remercier ses membres. Un grand merci à Patrick Dehornoy et Bernard Leclerc, grâce à qui j'ai fait la connaissance de Denis Simon, et qui ont fait beaucoup de gymnastiques pour faciliter les démarches administratifs, ainsi me permettant entre autres de consacrer plus de mon temps à la recherche. Je ne puis oublier Jean Cougnard qui a été mon directeur officiel pendant un bon moment durant la thèse. Je lui remercie aussi pour sa confiance et je lui adresse toutes mes reconnaissances. Je tiens également à remercier John Boxall et Philippe Satgé pour leurs disponibilités à partager leurs grandes cultures en

mathématiques. Je n'oublierai pas les aides permanentes reçues de Bruno Anglès pour les questions administratifs. Je lui remercie davantage pour son dynamisme et son enthousiasme à enseigner. Je tiens également à remercier les doctorants et ATER du LMNO, merci pour votre amitié et votre accueil.

Maintenant, je vais adresser mes remerciements aux personnes qui ont des influences dans l'accomplissement de ce travail. Je remercie tous particulièrement Christophe Delaunay d'avoir donné des précisions sur la théorie des courbes elliptiques, je remercie aussi Mark van Hoeij pour ses programmes et sa disponibilité à répondre aux courriels, même le dimanche soir ainsi que pour l'aide précieuse en calcul de genre d'une courbe.

J'adresse mes salutations à tous mes anciens professeurs de l'Université d'Antananarivo, qui ont sans doute influencé mon intérêt à l'algèbre, à la combinatoire et bien sur à la théorie des nombres. Mes pensées vont tout d'abord à feu Razafy Andriamampianina Désiré, à qui je dois beaucoup d'estime et qui presque sans le savoir, m'a conforté mon envie de faire de la recherche en théorie des nombres et calculs formels. J'exprime toute ma reconnaissance et remerciements au professeur et ami Randrianarivony Arthur, pour tous ses encouragements et surtout son soutien moral. J'ai découvert en lui un modèle de simplicité, de sagesse et d'humanisme. Je suis désolé de l'avoir trop dérangé pour toutes les démarches entreprises depuis les préparatifs de départ de Madagascar pour les études en France. Mes remerciements vont également au chef du Département des Mathématiques et Informatiques de la Faculté des Sciences d'Antananarivo, Rabiazamaholy Marc. Merci d'avoir été un vrai soutien inconditionnel à tout épreuves. Je lui remercie de la confiance qu'il m'a accordée et je suis heureux de lui témoigner toutes mes respects et reconnaissances d'avoir été le professeur qui m'a éveillé mon désir d'enseigner. Je ne puis également oublier d'exprimer ma gratitude à tous mes professeurs qui m'ont beaucoup appris.

Par ces quelques mots, Je remercie le collègue et ami Oswaldo Velásquez, d'avoir été l'un des premiers à apporter ses remarques et corrections sur ce manuscrit. Je te remercie aussi pour les échanges d'idées tant en mathématiques que dans la vision global de la vie.

J'aimerais adresser maintenant mes remerciements à Herimalala Rahobisoa et Haritiana Deverly pour les aides et corrections apportés à ce document. Mes remerciements vont également à Ludovic Delabarre, Laurent Demonet pour les quelques remarques et suggestions.

Pour leurs amitiés et leurs encouragements, j'adresse mes vifs remerciements à « Tsinjo sy Tony » Razafimanantsoa. Sans votre aide et votre soutien moral, inconditionnel, je n'aurais pu faire cette thèse...

Je passe ensuite un salut spécial à tous les jeunes gens que j'ai eu le plaisir de côtoyer durant mes quelques années d'apprentissage, à savoir Setra, Pascal, Zo, Malalatiana, Paul André, Tsimba, Naivo Régis, Bako, Tahina, Rado, Ando... Ah, la liste est bien trop longue pour tous vous énumérer.

Je remercie les membres de la FPMA Strasbourg, je salue particulièrement les amis Fanilo, Soary, Rindra, Sata Johary, Tahina. Je remercie également ceux de la FPMA Caen ainsi que la communauté malgache de Caen. Enfin, je remercie tous simplement les ami(e)s.

Je remercie aussi Dominique Dumont de m'avoir si bien reçu à Strasbourg. J'adresse également mes remerciements à Didier Pinchon, pour ses exposés à Ankatso et son amitié.

Cela va de soi, je remercie évidemment ma famille pour son soutien et son encouragement. Ils ont été présents pour partager les joies, cette thèse est un peu la leur ; Merci Jeannette, Robert, John, Fabien, Maria.

« Des arts libéraux : géométrie, arithmétique et musique, je t'en ai donné le goût quand tu étais encore jeune, à cinq ou six ans ; achève le cycle ; en astronomie, apprends toutes les règles, mais laisse-moi l'astrologie et l'art de Lulle, comme autant de supercheries et de futilités(...) Quant à la connaissance des faits de la nature, je veux que tu t'y adonnes avec curiosité : qu'il n'y ait mer, rivière, ni source dont tu ignores les poissons ; tous les oiseaux du ciel, tous les arbres, arbustes, et les buissons des forêts, toutes les herbes de la terre, tous les métaux cachés au ventre des abîmes, les pierreries de tous les pays de l'Orient et du Midi, que rien ne te soit inconnu. Puis relis soigneusement les livres des médecins grecs, arabes et latins, sans mépriser les Talmudistes et les Cabalistes et, par de fréquentes dissections, acquiers une connaissance parfaite de cet autre monde qu'est l'homme(...) »

Lettre de Gargantua à son fils Pantagruel,
Rabelais, Pantagruel, chap. VIII, 1532.

PRÉFACE

Pour une courbe elliptique définie sur \mathbb{Q} , la liste des sous-groupes de torsion possibles est connue depuis Mazur [Maz78]. Les cas des corps de nombres ne sont connus que très partiellement. Par exemple, la liste des sous-groupes de torsion possibles des courbes elliptiques définies sur les corps quadratique est connue, depuis les travaux de Kamienny [Kam86a], [Kam86b] et ceux de Kenku et Momose [KM88].

La thèse est organisée de la manière suivante : dans le premier chapitre, nous ferons quelques rappels sur les résultats et méthodes connus sur l'arithmétique des courbes elliptiques. Nous ferons alors des survols rapides sur quelques techniques de descente qui nous permettent de trouver les rangs des courbes obtenues. Il s'agit de rappels seulement, puisque en réalité, ces algorithmes sont implémentés sur machine par Simon ([Sima] sur \mathbb{Q} et [Simb] pour le cas des corps des nombres). Nous soulignons que cela nécessite beaucoup de méthodes du type algorithmique.

Nous décrirons aussi quelques résultats sur le rang analytique des courbes elliptiques définies sur \mathbb{Q} . Ces résultats peuvent présenter, dans certains cas, une alternative aux méthodes algébriques usuelles, pour le calcul du rang. Nous citerons les célèbres travaux de Gross-Zagier, Rubin et Kolyvagin sur la conjecture de Birch et Swinnerton-Dyer, affirmant l'égalité entre le rang analytique et le rang algébrique.

Ensuite, dans le deuxième chapitre, nous nous intéresserons à deux problèmes liés : il s'agit d'une part de décrire la forme générale des courbes elliptiques avec des sous-groupes de torsion donnés pour le cas où le corps de base est une extension quadratique de \mathbb{Q} . Nous utilisons essentiellement la forme normale de Tate pour trouver ces formes. Nous compléterons alors les travaux de Kubert [Kub76] et de Reichert [Rei85], qui utilisent la même forme mais qui ne traitent pas les torsions du type $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. En utilisant les algorithmes de van Hoeij [vH97], [vH95] et [vH02], nous retrouvons ces paramétrisations de Kubert et de Reichert mais

nous donnerons des formules plus simplifiées ainsi que des équations plus simples pour les courbes modulaires.

Dans ce deuxième chapitre, il s'agira d'autre part de donner des exemples explicites de courbes elliptiques de grand rang et dont la partie torsion est non triviale. Par spécialisation, nous montrons par exemple l'existence de courbes elliptiques dont le groupe de Mordell–Weil est isomorphes à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}^3$ ou $\mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}^2$ sur certains corps quadratiques. Nous obtenons des résultats analogues pour les autres types de torsion.

En ce qui concerne les courbes elliptiques définies sur \mathbb{Q} , si l'on se donne un entier naturel n , alors une question naturelle est de savoir si l'on peut toujours trouver des courbes elliptiques avec un rang au moins n . Ceci reste encore un problème ouvert. Il est difficile, en pratique, de trouver des exemples explicites de courbes elliptiques de grand rang. Elkies a donné en 2007 [Elk07] un exemple de courbe elliptique sur \mathbb{Q} dont le rang est au moins 28. La méthode consiste d'abord à trouver une famille infinie de courbes elliptiques dont le rang est au moins 18 (il s'agit en fait d'une seule courbe elliptique de rang au moins 18 sur $\mathbb{Q}(t)$), puis à spécialiser (en choisissant des valeurs pour t).

Déjà, dans [Mes91a] et [Mes91b], Mestre décrivait une méthode de construction de telles familles infinies de courbes elliptiques de grand rangs (rang au moins 11). La méthode de construction de Mestre est devenue une des méthodes les plus utilisées mais s'avère cependant, presque inutilisable si on veut au moins 3 points de torsion (voir par exemple [Fer96] pour la 2-torsion).

Lorsque l'on impose que la courbe elliptique possède un grand sous-groupe de torsion, il est encore plus difficile de trouver de courbes de grand rang. Nous citerons, entre autres, Lecacheux [Lec03a], Kulesz [Kul03], Kihara [Kih06], Nagao [Nag97], Atkin et Morain [AM93], Dujella [Duj07], Campbell [Cam97] qui ont décrit des familles paramétrées par une variable $t \in \mathbb{Q}$ ou par les points d'une courbe elliptique de rang 1 sur \mathbb{Q} .

La troisième chapitre porte sur une nouvelle construction de familles infinies de courbes elliptiques. Nous montrons, entre autre, l'existence de courbes elliptiques (que l'on appellera des *paramétrisantes*) définies sur $\mathbb{Q}(t)$, dont à chaque point correspond une courbe elliptique sur $\mathbb{Q}(t)$, avec un sous-groupe de torsion spécial et de rang non nul. Nous utilisons les intersections de droites avec certaines familles de courbes elliptiques.

Notons que des résultats sur ce sujet ont fait l'objet d'exposés (O. Lecacheux : Casablanca (2003) et Zagreb (preprint 2007)). La thèse de Titem Harrache (en cours) contient aussi des résultats sur ce sujet.

Nous partons pour cela d'un point sur une courbe elliptique (définie sur $\mathbb{Q}(t)$) puis ensuite, nous traçons des droites passant par ce point en choisissant une pente

rationnelle adaptée. Si la pente et la paramètre t vérifient certaines conditions, la droite rencontre la courbe elliptique en deux nouveaux points rationnels. Nous donnerons dans l'annexe B, des exemples courbes elliptiques sur \mathbb{Q} de rang 0, 1 ou 2 et dont les points rationnels paramétrisent des familles de courbes elliptiques de grand rang et de grande torsion. Notons aussi que la méthode décrite par Kulesz [Kul03] est un cas particulier de notre construction.

Nous traiterons aussi le cas où l'on considère la pente de la droite comme une variable. Nous montrerons par exemple qu'il existe une courbe elliptique $\mathcal{S}^{(1,3)}$ sur $\mathbb{Q}(t)$ (de torsion $T \supseteq \mathbb{Z}/3\mathbb{Z}$) avec un point Q d'ordre infini, telle que à tout point P sur $\mathcal{S}^{(1,3)}(\mathbb{Q}(t))$, sauf un nombre fini, correspond une courbe elliptique $\mathcal{S}_P^{(1,7)}$ définie sur $\mathbb{Q}(t)$ de rang au moins 1 et de torsion $T' \supseteq \mathbb{Z}/7\mathbb{Z}$. En particulier, pour $P = nQ$, on obtient une suite de familles infinies

$$\mathcal{S}_n^{(1,7)} = \{\mathcal{S}_{nQ}^{(1,7)}, t \in \mathbb{Q}\}$$

de courbes elliptiques sur \mathbb{Q} de rang au moins 1 et de torsion $T' \supseteq \mathbb{Z}/7\mathbb{Z}$. Notons que nos résultats sont explicites.

Une des principales difficultés pour trouver ces courbes elliptiques est le grand degré des polynômes qui entrent en jeu dans les paramétrisations, en particulier lorsque la partie torsion est grande.

TABLE DES MATIÈRES

Remerciements	i
Préface	v
1. Introduction	1
1.1. Quelques rappels préliminaires	1
1.1.1. Les points K -rationnels	2
1.1.2. Le théorème de Mordell–Weil	3
1.2. Les points de torsion	4
1.2.1. L’application réduction	4
1.2.2. Polynômes de division	5
1.3. Le rang algébrique	6
1.3.1. Méthode de 2–descente : cas sans point de 2–torsion.	6
1.3.2. Les espaces homogènes	8
1.4. Sur le rang analytique	9
1.4.1. Cas des extension quadratiques	10
1.4.2. Torsion sur $\mathbb{Q}(\sqrt{D})$ lorsque E est définie sur \mathbb{Q}	11
2. Paramétrisations des structures	13
2.1. Cadre général	13
2.2. Le cas des corps de nombres quadratiques	14
2.2.1. Torsions possibles	14
2.2.2. Sur le rang	15
2.3. Paramétrisations des structures	15
2.3.1. Les courbes modulaires	15
2.3.2. Forme normale de Tate	16
2.3.3. Description générale	17
2.4. Torsion des courbes elliptiques définies sur \mathbb{Q}	18
2.4.1. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/2\mathbb{Z}$	18
2.4.2. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/3\mathbb{Z}$	18
2.4.3. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/4\mathbb{Z}$	18

2.4.4. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/5\mathbb{Z}$	19
2.4.5. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/6\mathbb{Z}$	19
2.4.6. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/7\mathbb{Z}$	19
2.4.7. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/8\mathbb{Z}$	20
2.4.8. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/9\mathbb{Z}$	20
2.4.9. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/10\mathbb{Z}$	21
2.4.10. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/12\mathbb{Z}$	21
2.4.11. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	22
2.4.12. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	22
2.4.13. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	23
2.4.14. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	24
2.5. Les torsions supplémentaires pour $[K : \mathbb{Q}] = 2$	25
2.5.1. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/11\mathbb{Z}$	25
2.5.2. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/13\mathbb{Z}$	30
2.5.3. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/14\mathbb{Z}$	31
2.5.4. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/15\mathbb{Z}$	34
2.5.5. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/16\mathbb{Z}$	36
2.5.6. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/18\mathbb{Z}$	38
2.5.7. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$	39
2.5.8. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$	42
2.5.9. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	45
2.5.10. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	48
2.5.11. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	50
3. Les familles de courbes elliptiques de grand rang	53
3.1. Description des résultats connus	53
3.2. Intersection d'une courbe elliptique avec des droites	54
3.2.1. Description de la méthode	54
3.2.2. Exemples d'illustration	55
3.2.3. Modèle quartique et modèle cubique.	60
3.3. Courbes avec des structures de torsion données	61
3.3.1. Familles avec $\text{Tors}(E, \mathbb{Q}) \supseteq \mathbb{Z}/7\mathbb{Z}$	61
3.3.2. Familles avec $\text{Tors}(E, \mathbb{Q}) \supseteq \mathbb{Z}/8\mathbb{Z}$	72
3.3.3. Familles avec $\text{Tors}(E, \mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	78
3.3.4. Familles avec $\text{Tors}(E, \mathbb{Q}) \supseteq \mathbb{Z}/9\mathbb{Z}$	85
3.3.5. Familles avec $\text{Tors}(E, \mathbb{Q}) \supseteq \mathbb{Z}/10\mathbb{Z}$	87
3.3.6. Familles avec $\text{Tors}(E, \mathbb{Q}) \supseteq \mathbb{Z}/12\mathbb{Z}$	88
3.3.7. Familles avec $\text{Tors}(E, \mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	90
3.3.8. Familles de courbes avec $\text{Tors}(E, \mathbb{Q}(\sqrt{-3})) \supseteq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	91
3.3.9. Familles de courbes avec $\text{Tors}(E, \mathbb{Q}(\sqrt{-1})) \supseteq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	94
A. Quelques détails complémentaires	97
A.1. Forme normale de Tate	97

B. Quelques exemples de courbes paramétrisantes	99
B.1. Le cas $T \supseteq (1, 12)$ et $r \geq 1$	99
B.2. Le cas $T \supseteq (2, 6)$ et $r \geq 2$	101
B.3. Le cas $T \supseteq (1, 7)$ et $r \geq 2$	102
B.4. le cas $T \supseteq (1, 10)$ et $r \geq 1$	103
B.5. Le cas $T \supseteq (1, 9)$ et $r \geq 1$	107
B.6. Le cas $T \supseteq (2, 8)$ et $r \geq 1$	108
B.7. Le cas $T \supseteq (1, 8)$ et $r \geq 2$	110
Bibliographie	111

CHAPITRE 1

INTRODUCTION

1.1. Quelques rappels préliminaires

La présente thèse concerne l'arithmétique des courbes elliptiques sur les corps de nombres algébriques et sur quelques corps de fonctions. Une courbe elliptique sur un corps K est une variété projective définie sur K , de dimension 1, de genre 1 et possédant au moins un point sur K .

En pratique, une telle courbe peut être représentée dans le plan projectif par une équation de Weierstrass :

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 . \quad (1.1)$$

Les coefficients a_i , sont dans K et il faut en plus que le discriminant Δ associée à la courbe elliptique E soit non nul.

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \quad (1.2)$$

avec

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

Le point $[0, 1, 0]$ est appelé point à l'infini et sera noté \mathcal{O} par la suite. Le modèle affine est souvent obtenu en faisant $x = \frac{X}{Z}$ et $y = \frac{Y}{Z}$ pour $Z \neq 0$. Alors, on obtient :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 . \quad (1.3)$$

Nous disons que la courbe E est définie sur un corps K si tous les coefficients a_i sont dans K , puis nous définissons l'ensemble $E(K)$ des points rationnels sur K

par :

$$E(K) = \{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\} \quad (1.4)$$

Dans tout ce chapitre, sauf mention du contraire, K désignera un corps de nombres algébriques. Dans ce cas, il est toujours possible (comme dans tout autre corps de caractéristique différente de 2 et 3), grâce à un changement de variable rationnel convenable, de se ramener à la forme de Weierstrass réduite

$$E : y^2 = x^3 + Ax + B. \quad (1.5)$$

Il est aussi coutume de faire des changements de variables de telle sorte que les coefficients de l'équation de la courbe elliptique soient entiers algébriques.

1.1.1. Les points K -rationnels. — Soit E une courbe elliptique définie sur un corps de nombres K et $E(K)$ l'ensemble des points K -rationnels de E . Alors, $E(K)$ possède une structure de groupe abélien dont le point \mathcal{O} est l'élément neutre. La loi de groupe sur $E(K)$ est complètement déterminée par les intersections des droites passant par les points de $E(K)$.

L'avantage d'écrire un modèle de Weierstrass pour une courbe elliptique E est que l'on peut écrire explicitement la loi de groupe en termes de fractions rationnelles. Dorénavant, sauf mention du contraire, nous utiliserons donc un modèle de Weierstrass pour une courbe elliptique E .

Loi de groupe. — Soient P, Q deux points sur $E(K)$ et L la droite passant par P et Q (on prend la droite tangente si $P = Q$). On note par $R = P * Q$ le troisième point d'intersection de L avec E . Soit maintenant L' la droite passant par R et \mathcal{O} , alors L' rencontre E en un autre point que l'on notera $P + Q$. On montre alors que la loi $+$ est bien une loi de groupe abélien sur $E(K)$.

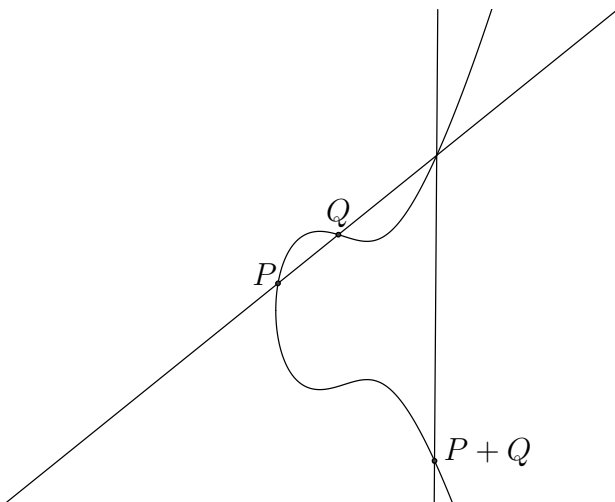
On note

$$[m]P = P + \cdots + P \text{ (m fois) .}$$

et on dit que P est un point de torsion s'il existe un entier $m \geq 1$ tel que $[m]P = \mathcal{O}$. On dit qu'un point est d'ordre infini s'il n'est pas de torsion.

Nous renvoyons le lecteur désireux d'en savoir davantage, au très bon livre de Silverman [Sil86, Chapitre III].

Il est à noter que nous effectuons les calculs des coordonnées des points d'une courbe elliptique sur le système PARI/GP (voir [BBB⁺]).

FIG. 1.1. Loi de groupe pour une courbe elliptique sur \mathbb{R} .

1.1.2. Le théorème de Mordell–Weil. — Soit une courbe elliptique E définie par son modèle de Weierstrass :

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

On suppose que les a_i sont des éléments d'un corps K fixé et l'on note toujours par \mathcal{O} le point à l'infini. Mordell a démontré que lorsque le corps de base est $K = \mathbb{Q}$, l'ensemble des points $E(\mathbb{Q})$ forme un groupe abélien de type fini. Son résultat fut ensuite généralisé par Weil dans le cas des corps de nombres algébriques en général.

Théorème 1.1 (Mordell–Weil, [Sil86]). — Soit E une courbe elliptique définie sur un corps de nombres K , alors il existe $n \in \mathbb{N}$ et $\text{Tors}(E, K)$, un groupe abélien fini tel que :

$$E(K) \simeq \text{Tors}(E, K) \times \mathbb{Z}^n .$$

L'entier n est appelé le rang (algébrique) de la courbe elliptique E sur K et on le notera par la suite $\text{rang}(E, K)$. La partie $\text{Tors}(E, K)$ est le sous-groupe des points d'ordre fini de $E(K)$.

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.

Dans le cas où le corps de base est \mathbb{Q} , Mazur a 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 1.2 (Mazur, [Maz78]). — 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 :

$$\text{Tors}(E, \mathbb{Q}) \simeq \begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{avec } 1 \leq n \leq 10 \text{ ou } n = 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, & \text{avec } 1 \leq n \leq 4. \end{cases} \quad (1.6)$$

Lorsque l'on se donne une courbe elliptique E définie sur un corps de nombres K fixé, la partie de torsion est relativement facile à trouver et cela grâce par exemple aux polynômes de division associés à la courbe. C'est d'autant plus facile encore si, en plus, on dispose d'information sur les sous-groupes de torsion admissible sur K .

Dans [Mer96] Merel a démontré qu'il existe pour tout entier d un entier $B(d)$ tel que, pour tout corps de nombres K de degré d sur \mathbb{Q} et pour toute courbe elliptique E sur K , la partie de torsion $\text{Tors}(E, K)$ est de cardinal majoré par $B(d)$. Ensuite, Parent a donné une borne effective du théorème de Merel (voir [Par99]).

Dans [Kub76], Kubert a donné les paramétrisations des courbes elliptiques définies sur \mathbb{Q} , avec tous les sous-groupes de torsion possible de la liste de Mazur. On peut donc dire que la partie de torsion d'une courbe elliptique sur \mathbb{Q} est bien connue. Le rang de la courbe reste cependant plus difficile à trouver.

1.2. Les points de torsion

1.2.1. L'application réduction. — Soit E une courbe elliptique définie sur un corps de nombres K :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_4 .$$

On peut supposer, via un changement de variable convenable, que les coefficients a_i soit dans \mathbb{Z}_K , l'anneau d'entiers de K . Soit maintenant \mathfrak{p} un idéal maximal de \mathbb{Z}_K . Alors, on considère l'application réduction

$$\begin{aligned} \text{red}_{\mathfrak{p}} : \mathbb{Z}_K &\rightarrow \mathbb{F}_{\mathfrak{p}} = \mathbb{Z}_K/\mathfrak{p}\mathbb{Z}_K \\ x &\mapsto \tilde{x} = \text{Classe}(x) \end{aligned}$$

que l'on applique sur les coefficients a_i . On obtient ainsi la courbe \tilde{E} :

$$\tilde{E} : y^2 + \tilde{a}_1xy + \tilde{a}_3y = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_4 ,$$

définie sur $\mathbb{F}_{\mathfrak{p}}$ qui peut bien sur être singulière (si $\tilde{\Delta} = 0$).

Étant donnée une courbe elliptique E définie sur un corps de nombres K , on peut donc lui associer ses réduites $E/\mathbb{F}_{\mathfrak{p}}$ pour chaque $\mathfrak{p} \in \mathbb{Z}_K$, idéal maximal.

Nous dirons alors que E est de bonne réduction en \mathfrak{p} si il existe un modèle tel que $\tilde{E}/\mathbb{F}_{\mathfrak{p}}$ n'est pas singulière (on obtient une courbe elliptique définie sur $\mathbb{F}_{\mathfrak{p}}$) et de mauvaise réduction dans le cas contraire. Nous avons la proposition suivante

Proposition 1.1. — Soient E un courbe elliptique définie sur un corps de nombres K , \mathfrak{p} un idéal premier de \mathbb{Z}_K et m un entier strictement positif, premier avec $\#\mathbb{F}_{\mathfrak{p}}$. Sous l'hypothèse que E est de bonne réduction en \mathfrak{p} , alors l'application

$$\begin{aligned} \text{red}_{\mathfrak{p}} : E(K)[m] &\rightarrow E(\mathbb{F}_{\mathfrak{p}}) \\ \mathcal{O} &\mapsto \mathcal{O} \\ (x, y) &\mapsto (\tilde{x}, \tilde{y}) \end{aligned}$$

est bien définie et est un morphisme injectif de groupes.

Démonstration. — Voir le livre de Silverman [Sil86, Chapitre VII,§3]. \square

En pratique, cette proposition est utilisée comme l'une des manières rapides pour obtenir une borne sur $\text{Tors}(E, K)$, et cela en choisissant quelques \mathfrak{p} de bonne réduction.

Une fois connue une bonne borne du cardinal de la partie torsion, on peut alors utiliser les polynômes de division de E pour déterminer exactement le sous-groupe $\text{Tors}(E, K)$.

1.2.2. Polynômes de division. — Soit K un corps de caractéristique $\text{car}(K) \neq 2, 3$ et soit E une courbe elliptique définie sur K par :

$$E : y^2 = x^3 + Ax + B. \quad (1.7)$$

On définit les polynômes de division $\psi_m \in \mathbb{Z}[A, B, x, y]$ de E par :

$$\begin{aligned} \psi_1 &= 1, \\ \psi_2 &= 2y, \\ \psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2, \\ \psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3), \\ \psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \text{ pour } m \geq 2, \\ 2y\psi_{2m} &= \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \text{ pour } m \geq 3. \end{aligned}$$

On peut montrer que si $P = (x_0, y_0) \in E \setminus \mathcal{O}$, alors :

$$[m]P = \left(\frac{\phi_m(P)}{\psi_m(P)^2}, \frac{\omega_m(P)}{\psi_m(P)^3} \right) \quad (1.8)$$

avec ϕ_m et $\omega_m \in \mathbb{Z}[A, B, x, y]$. Il est donc clair que si $P \in E(K) \setminus \{\mathcal{O}\}$, alors $[m]P = \mathcal{O} \Leftrightarrow \psi_m(x) = 0$ (voir [Sil86, Chapitre III, Exercice 3.7]).

1.3. Le rang algébrique

La recherche du rang d'une courbe est un peu délicate. La méthode la plus habituelle est celle de la 2-descente. Nous utilisons les programmes de Simon [Sima] et [Simb], sur PARI/gp [BBB⁺] pour calculer le rang des courbes ou, à défaut, trouver une bonne majoration pour celui-ci. Dans certains cas, quelques conjectures fortes permettent d'avoir une estimation du rang (voir 1.2).

Théorème 1.3 (Mordell–Weil : Forme faible). — *Soit $n \geq 2$ un entier naturel, alors $E(K)/nE(K)$ est un groupe d'ordre fini.*

En fait, c'est surtout ce théorème, qui nous est vraiment utile pour trouver le rang de la courbe dans E sur K puisque l'on a

$$E(K)/2E(K) = 2^{r+\varepsilon} \tag{1.9}$$

où r est le rang de la courbe et $\varepsilon = 0, 1$ ou 2 suivant le nombre de points d'ordre 2. Pour trouver une borne supérieure du rang, on plonge donc le groupe $E(K)/nE(K)$ dans un autre groupe, dit de Selmer et on essaie de déterminer le rang de ce dernier. Notons que sous certaines conjectures, il est aussi possible de prédire le rang algébrique.

Nous allons maintenant décrire les méthodes permettant de trouver le rang algébrique d'une courbe elliptique définie sur un corps de nombres K , donné.

1.3.1. Méthode de 2-descente : cas sans point de 2-torsion.— Soit E une courbe elliptique définie sur le corps de nombres K par une équation de Weierstrass de la forme :

$$E : y^2 = F(x) = x^3 + ax^2 + bx + c. \tag{1.10}$$

On supposera que a, b, c sont entiers algébriques et F irréductible sur K , ce qui équivaut à dire que la courbe n'a pas de point de 2-torsion non trivial.

La méthode consiste à déterminer le rang de la courbe en calculant $\#E(K)/2E(K)$ qui est égal à 2^r , où r est exactement le rang. Cela se réalise en faisant des majorations successives pour le rang de la courbe.

Pour cela, on plonge $E(K)/2E(K)$ dans un autre groupe qui est isomorphe au 2-groupe de Selmer. Ensuite, on détermine l'ordre de ce dernier.

Du fait de l'irréductibilité du polynôme F , on peut définir le corps L suivant :

$$L = K[\theta]/(F(\theta)) \quad (1.11)$$

Nous considérons l'application (on peut démontrer que c'est un homomorphisme) :

$$\begin{aligned} \Psi : E(K) &\rightarrow L^*/L^{*2} \\ 0 &\mapsto 1 \\ (x, y) &\mapsto x - \theta. \end{aligned}$$

Regardons maintenant le noyau de cet homomorphisme. Tout d'abord, nous avons $\Psi(2P) = \Psi(P)^2 = 1$, ce qui entraîne $2E(K) \subseteq \ker \Psi$.

Supposons maintenant que $\Psi(P) = 1$, où $P = (a, b)$ appartient à $E(K)$, il s'ensuit que :

$$a - \theta = (a_1 + a_2\theta + a_3\theta^2)^2 \text{ pour certains } a_i \in K. \quad (1.12)$$

En développant cette dernière équation, on obtient les trois équations :

$$Q_1(a_1, a_2, a_3) = 0 \quad (1.13)$$

$$Q_2(a_1, a_2, a_3) = -1 \quad (1.14)$$

$$Q_3(a_1, a_2, a_3) = x \quad (1.15)$$

Les deux premières équations quadratiques sont celles qui nous intéressent pour l'instant, puisque la troisième donne seulement la première coordonnée du point P sur la courbe.

Donc, pour qu'il y ait bien une solution, il est nécessaire que ces deux équations soient vérifiées ensemble.

Considérons aussi l'application Norme N définie par :

$$\begin{aligned} N : L^*/L^{*2} &\rightarrow K^*/K^{*2} \\ x &\mapsto N_{L/K}(x) \bmod K^{*2} \end{aligned} \quad (1.16)$$

Notre but maintenant, est de trouver l'image de cette homomorphisme : $\Im \Psi$, ou de trouver une estimation sur son ordre. Il se trouve que L^*/L^{*2} est trop grand et donc, il nous faut éliminer, dans la mesure du possible, tous les éléments qui ne peuvent pas être dans $\Im \Psi$.

On remarque aussi, au passage, que N est un homomorphisme de groupe. Notons les propositions suivantes :

Proposition 1.2. — *L'image de Ψ est un sous groupe de $\ker N$.*

Démonstration. — Soit $P = (x, y) \in E(K)$, il est facile de voir que l'on a $N_{L/K}(\Psi(P)) = N_{L/K}(x - \theta) = F(x) = y^2$.

□

Soient maintenant E une courbe elliptique sur K et S , un ensemble fini de places. Définissons le groupe :

$$L(S, 2) = \{\delta \in L^*/L^{*2}, \forall \mathfrak{p} \notin S, v_{\mathfrak{p}}(\delta) \equiv 0 \pmod{2}\}. \quad (1.17)$$

Proposition 1.3. — *Soit S l'ensemble fini de places contenant les places infinies de K et les idéaux maximaux η au dessus de \mathfrak{p} tel que \mathfrak{p} divise $F'(\theta)$ et \mathfrak{p}^2 divise le discriminant de F , alors :*

$$\text{Im}(\Psi) \subset L(S, 2) \cap \ker N$$

Démonstration. — Voir l'article de Simon [Simb]. □

Cette proposition permet de trouver une première majoration pour le rang.

Solubilités des équations quadratiques. — L'étape suivante est maintenant de montrer l'existence ou non des solutions rationnelles pour les équations quadratiques.

1.3.2. Les espaces homogènes. — Revenons maintenant dans le cas générale. En considérant les équations du type $Q_2 = -1$ et en paramétrisant les équations quadratiques $Q_1 = 0$ qui sont solubles localement pour toute place v , on obtient des quartiques du type $Y^2 = q(x, z)$, où q est un polynôme homogène de degré 4.

Ceci dit, pour que les deux équations quadratiques soient vérifiées simultanément, il faut donc que la quartique correspondante soit localement soluble pour toute place v .

Dans [Simb], Simon explicite une méthode pour minimiser le discriminant $\text{Disc}(q)$ d'une quartique. Cela permet alors d'avoir un nombre minimal de places pour le test.

Le fait que la quartique est partout soluble localement (ELS), ne nous permet pas de dire qu'elle possède une solution dans K mais néanmoins, cela réduit encore $\text{Im}(\Psi)$ et ainsi donc on obtient plus de raffinements. Les $\eta \in L(S, 2) \cap \ker N$ qui induisent des quartiques "ELS" forment un groupe isomorphe au 2-groupe de Selmer. On dénotera par la suite ce groupe comme le groupe de Selmer. Rappelons la suite exacte :

$$0 \rightarrow E(K)/2E(K) \rightarrow \text{Sel}^2(E/K) \rightarrow \text{III}(E/K)[2] \rightarrow 0 \quad (1.18)$$

Un renseignement sur $\#\text{III}(E/K)[2]$ nous permettra donc d'avoir des renseignements supplémentaires sur le rang de la courbe.

Du point de vue algorithmique, la construction des quartiques ELS issues de cette descente est assez longue. Cela est dû en majeure partie à la recherche des solutions pour les équations de Legendre (voir[Sim02]).

Il est aussi à noter que, pour une quartique de ce genre, on ne connaît pas à ce jour, de moyen efficace pour trouver un point puisque en général, la taille des coefficients de la quartique elle-même peut être très grande. Il peut également arriver que la quartique soit soluble partout mais ne possède pas de point K -rationnel.

Nous donnons aussi des exemples de quartiques définies sur des corps quadratiques dans l'appendice A.

Pour le cas rationnel ($K = \mathbb{Q}$), nous citerons par exemple l'article [Cre99] de Cremona et Stoll pour réduire la taille des coefficients. Le cas des quartiques sur les corps de nombres est encore plus difficile.

1.4. Sur le rang analytique

Soit K un corps de nombres et E une courbe elliptique définie sur K de discriminant Δ_E . La fonction L de E/K est défini comme le produit Eulerien suivant :

$$L(s, E/K) = \prod_{\mathfrak{p} \nmid \Delta_E} \left(1 - \frac{a(\mathfrak{p})}{(N\mathfrak{p})^s} + \frac{1}{N(\mathfrak{p})^{2s-1}} \right)^{-1} \times \prod_{\mathfrak{p} \mid \Delta_E} \left(1 - \frac{a(\mathfrak{p})}{N(\mathfrak{p})^s} \right) \quad (1.19)$$

où pour chaque \mathfrak{p} de bonne réduction :

$$N(\mathfrak{p}) = \#\mathbb{Z}_K/\mathfrak{p} = p^f \quad (1.20)$$

$$\mathfrak{a}(\mathfrak{p}) = N(\mathfrak{p}) + 1 - \#E(\mathbb{F}_\mathfrak{p}) \quad (1.21)$$

Lorsque $\Re(s) > \frac{3}{2}$, cette fonction peut être écrite comme une série de Dirichlet :

$$L(s, E/K) = \sum_{\mathfrak{a}} a(\mathfrak{a}) N(\mathfrak{a})^{-s}$$

où la somme est sur toutes les idéaux entiers de \mathbb{Z}_K .

Conjecture 1.1. — Soit E une courbe elliptique définie sur un corps de nombre K avec une série $L(s) = L(s, E/K)$. Notons par $N_{E/K}$ le conducteur de E , D_K

le discriminant de K/\mathbb{Q} et $n = [K : \mathbb{Q}]$. Si l'on définit la fonction :

$$\Lambda(s) = N_{E/K}^{s/2} |D_K| (2\pi)^{-s} \Gamma(s) L(s) ,$$

alors

$$\Lambda(s) = \varepsilon \Lambda(2 - s) \text{ avec } \varepsilon = \pm 1 .$$

La quantité ε est appelée le signe de l'équation fonctionnelle.

Sous cette conjecture, on peut étendre L sur tout le plan complexe. En particulier, nous avons aussi une des conjectures les plus célèbres sur l'arithmétique de courbes elliptiques

Conjecture 1.2 (Birch–Swinnerton-Dyer). — Soit E une courbe elliptique définie sur un corps de nombres K , alors :

$$\text{ord}_{s=1} L(s, E/K) = \text{rang}(E, K) . \quad (1.22)$$

Il est à noter qu'à l'heure actuelle, on ne dispose pas d'algorithme qui garantit efficacement le rang (algébrique) d'une courbe elliptique sur un corps de nombres donné. Néanmoins, la dernière conjecture propose en quelque sorte à quoi doit-on s'attendre.

Un des résultats à propos de ce conjecture n'est connu que pour le cas rationnel. Nous citerons par exemples les célèbres travaux de Gross–Zagier, Rubin et Kolyvagin :

Théorème 1.4 (Gross–Zagier–Kolyvagin). — Soit E une courbe elliptique définie sur \mathbb{Q} et soit L sa fonction de Dirichlet associée. Alors,

- Si $L(E, 1) \neq 0$ alors $\text{rang}(E/\mathbb{Q}) = 0$.
- Si $L(E, 1) = 0$ et si $L'(E, 1) \neq 0$, alors $\text{rang}(E/\mathbb{Q}) = 1$.

Étant donnée une courbe elliptique définie sur \mathbb{Q} , de rang n , on peut poser la question de savoir quel est son rang sur les extensions finies de \mathbb{Q} . Par la suite, nous serons amenés à étudier le cas des extensions quadratiques.

1.4.1. Cas des extension quadratiques. — Dans cette section, on considère une courbe elliptique E définie sur \mathbb{Q} par une équation de Weierstrass réduite :

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

Notons N_E le conducteur de E et $K = \mathbb{Q}(\sqrt{D})$, pour D entier sans facteur carré. On note par E^D la courbe elliptique tordue par D , c'est-à-dire $E^D : Dy^2 = x^3 + ax + b$. Alors

$$L(s, E/K) = L(s, E/\mathbb{Q}) \times L(s, E^D/\mathbb{Q})$$

De plus, $L(s, E/\mathbb{Q})$ peut être prolongée analytiquement sur tout le plan complexe et vérifie l'équation fonctionnelle :

$$\begin{aligned}\Lambda(s, E) &= \left(\frac{\sqrt{N_E}}{2\pi}\right)^s \Gamma(s) L(s, E) \\ &= w_E \Lambda(2-s, E) \text{ avec } w_E = \pm 1.\end{aligned}$$

Aussi, $L(s, E^D/\mathbb{Q})$ peut être prolongée analytiquement sur tout le plan complexe et vérifie une équation fonctionnelle :

$$\begin{aligned}\Lambda(s, E^D) &= (|D| \frac{\sqrt{N_E}}{2\pi})^s \Gamma(s) L(s, E/\mathbb{Q}) \\ &= w_E \chi_D(-N_E) \Lambda(2-s, E^D)\end{aligned}$$

où

$$\chi_D(n) = \left(\frac{D}{n}\right)$$

est le symbole de Kronecker. En fait, on a également un résultat facile mais très utile pour le cas du rang algébrique :

$$\text{rang}(E/K) = \text{rang}(E/\mathbb{Q}) + \text{rang}(E^D/\mathbb{Q}). \quad (1.23)$$

Il est souvent plus facile de trouver le rang d'une courbe elliptique sur \mathbb{Q} ainsi que sa tordue par D , puis user de cette formule pour trouver le rang sur K . Ceci à cause de l'arithmétique du corps K qui peut-être difficile (du point de vue algorithmique, par exemple, trouver le groupe de classes d'idéaux, les unités, ...est difficile) .

Pour calculer le rang algébrique d'une courbe elliptique E/\mathbb{Q} , on peut commencer par calculer son rang analytique, c'est-à-dire l'ordre d'annulation en $s = 1$ de la fonction L . Si ce rang analytique est 0 ou 1, le théorème 1.4 permet de conclure. Nous utilisons le programme de Womack [**Wom**] pour calculer le rang analytique d'une courbe elliptique définie sur \mathbb{Q} .

Dans certains cas, nous adoptons cette technique pour le calcul du rang algébrique de la courbe elliptique E définie sur \mathbb{Q} ainsi que pour sa tordue E^D . Dans ce cas, il est possible, par la formule (1.23), de déterminer rapidement le rang algébrique de E sur K sans faire de descente.

1.4.2. Torsion sur $\mathbb{Q}(\sqrt{D})$ lorsque E est définie sur \mathbb{Q} . — Pour une courbe elliptique définie sur \mathbb{Q} , on peut se demander quelle peut être la structure du groupe de Mordell–Weil sur les extensions finies de \mathbb{Q} . Nous nous intéresserons au cas où l'extension est quadratique.

On notera par D un entier naturel sans facteur carré, E^D la tordue quadratique d'une courbe elliptique E et par σ un générateur du groupe de Galois

$\text{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q})$. Il est clair que le groupe $\text{Tors}(E, \mathbb{Q})$ est un sous-groupe de $\text{Tors}(E, \mathbb{Q}(\sqrt{D}))$.

Nous avons maintenant la proposition :

Proposition 1.4 ([Kwo97]). — Soit $E : y^2 = x^3 + ax + b$, une courbe elliptique définie sur \mathbb{Q} . Alors, l'application

$$h : \text{Tors}(E, \mathbb{Q}(\sqrt{D})) / \text{Tors}(E, \mathbb{Q}) \rightarrow \text{Tors}(E^D, \mathbb{Q})$$

définie par : $h(\tilde{P}) = P - P^\sigma$ est un homomorphisme injectif.

Démonstration. — Soit $P \in E(\mathbb{Q}(\sqrt{D}))$, si $X = P - P^\sigma$, alors $X^\sigma = -X$ et donc $X = (x_0, y_0\sqrt{D})$ avec x_0 et y_0 dans \mathbb{Q} . Le point $X = (x_0, y_0\sqrt{D})$ peut être vu comme le point (x_0, y_0) de $\text{Tors}(E^D, \mathbb{Q})$. L'application h est donc bien définie puisque $\text{Tors}(E, \mathbb{Q})$ est dans le noyau de h .

Soient maintenant Q et $P \in \text{Tors}(E, \mathbb{Q}(\sqrt{D}))$. Supposons que l'on a $P - P^\sigma = Q - Q^\sigma$, alors on obtient $(P - Q)^\sigma = P - Q$, c'est-à-dire, $P - Q$ est dans $\text{Tors}(E, \mathbb{Q})$, ce qui implique l'injectivité de h . \square

Corollaire 1.1. — Soit E une courbe elliptique définie sur \mathbb{Q} . Alors, pour tout entier sans facteur carré D , sauf un nombre fini,

$$\text{Tors}(E, \mathbb{Q}(\sqrt{D})) = \text{Tors}(E, \mathbb{Q}).$$

Démonstration. — Par la proposition 1.4, $\text{Tors}(E, \mathbb{Q}(\sqrt{D})) / \text{Tors}(E, \mathbb{Q})$ est isomorphe à un sous-groupe de $\text{Tors}(E^D, \mathbb{Q})$. Par le théorème de Mazur, l'ordre d'un point de $\text{Tors}(E^D, \mathbb{Q})$ est 1, 2, 3, ..., 10 ou 12. Il en résulte que $\text{Tors}(E, \mathbb{Q}) \subsetneq \text{Tors}(E, \mathbb{Q}(\sqrt{D}))$ si et seulement si il existe $P \in \text{Tors}(E, \mathbb{Q})$, $Q \in \text{Tors}(E, \overline{\mathbb{Q}})$ et $m \in \{2, 3, \dots, 10, 12\}$ tel que

$$mQ = P, \mathbb{Q}(Q) = \mathbb{Q}(x, y) = \mathbb{Q}(\sqrt{D}) \text{ avec } Q = (x, y).$$

Il est à noter qu'il existe un nombre fini de $P \in \text{Tors}(E, \mathbb{Q})$ et de $m \in \{2, 3, \dots, 10, 12\}$. Alors, il existe un nombre fini de $Q \in \text{Tors}(E, \overline{\mathbb{Q}})$ tel que $mQ = P$ et parmi eux, il existe un nombre fini de Q tel que $\mathbb{Q}(Q) = \mathbb{Q}(\sqrt{D})$. Ce qui achève la preuve. \square

CHAPITRE 2

PARAMÉTRISATIONS DES STRUCTURES

« Ce chapitre est une version plus détaillée d'un article soumis dans une revue ».

Actuellement, nous savons que le sous-groupe de torsion d'une courbe elliptique définie sur un corps de nombres quadratique est isomorphe à l'un des 26 groupes d'une liste explicite. Pour chacune des 15 structures différentes de torsion sur \mathbb{Q} , Kubert a donné (voir [Kub76]) les paramétrisations de toutes les courbes elliptiques définies sur \mathbb{Q} ayant cette torsion. Reichert [Rei85] a traité les 6 structures de torsion cycliques supplémentaires pour les cas des corps de nombres quadratiques. Nous reprenons ces résultats en donnant des preuves plus détaillées pour les structures sur \mathbb{Q} et des formules plus simples pour les autres. Nous complétons ces travaux en donnant les paramétrisations des courbes elliptiques avec des sous-groupes de torsion isomorphes à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Nous donnons aussi des exemples explicites de courbes elliptiques de rang non nul sur des corps quadratiques et dont le groupe des points rationnels est chacun des groupes : $\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}^2$, $\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}^2$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}^3$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}^3$.

2.1. Cadre général

Nous ne répondrons pas aux questions suivantes, mais nous ferons un état des lieux des avancées relatives à ces questions, notamment lorsque l'on travaille sur un corps de nombres.

Soit K un corps de caractéristique nulle (ex : un corps de nombres, $\mathbb{Q}(t)$, ...) et soit E une courbe elliptique définie sur K .

Question 1. Quels sont les nombres premiers p tels que $E(K)$ peut posséder un sous-groupe d'ordre p ?

Question 2. Quelle peut être la structure de la partie torsion ?

Mazur, dans [Maz78], a montré que les seuls nombres premiers qui divisent l'ordre d'un point de torsion pour une courbe elliptique sur \mathbb{Q} sont 2, 3, 5, 7. Ensuite, il a donné la liste complète des sous-groupes de torsion possibles pour une courbe elliptique sur \mathbb{Q} , voir le théorème 1.2 du chapitre précédent.

Pour le cas des corps de nombres en générale, nous avons un théorème précis :

Théorème 2.1 (Merel, [Mer96]). — *Soit d un entier positif. Alors, quels que soient K un corps de nombre de degré d et E une courbe elliptique définie sur K , il existe une borne finie $B(d)$ dépendant seulement de d telle que :*

$$\text{Tors}(E, K) \leq B(d).$$

Nous connaissons actuellement la liste de tous les sous-groupes de torsion possibles pour le cas des courbes elliptiques définies sur les corps quadratiques.

2.2. Le cas des corps de nombres quadratiques

2.2.1. Torsions possibles. — Soit K une extension quadratique de \mathbb{Q} et E une courbe elliptique définie sur K . Kamienny, à la suite de Mazur, a montré dans [Kam86a] et [Kam86b] que le cardinal de $\text{Tors}(E, K)$ est bornée indépendamment de E et de K . Il a donné alors la liste complète des nombres premiers pouvant diviser le cardinal du sous-groupe $\text{Tors}(E, K)$, pour une courbe elliptique E sur un corps de nombres quadratique : 2, 3, 5, 7, 11, 13.

Après Kamienny, Kenku et Momose ont donné la liste de tous les sous-groupes de torsion possibles :

Théorème 2.2 (Mazur–Kamienny–Kenku–Momose, [KM88])

Soit E une courbe elliptique définie sur un corps de nombres quadratique K , alors le sous-groupe $\text{Tors}(E, K)$ est isomorphe à l'un des groupes suivants :

$$\text{Tors}(E, K) \simeq \begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{avec } n \in 1 \leq n \leq 16 \text{ ou } n = 18 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, & \text{avec } 1 \leq n \leq 6 \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z}, & \text{avec } n = 1, 2 \text{ si } K = \mathbb{Q}(\sqrt{-3}) \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \text{si } K = \mathbb{Q}(\sqrt{-1}). \end{cases}$$

Remarque 2.1. — *Notons que pour un corps quadratique fixé, il peut arriver que certains de ces groupes n'apparaissent pas comme la partie torsion.*

2.2.1.1. Paramétrisations connues. — Dans [Rei85], Reichert a donné les paramétrisations des courbes elliptiques dont le sous-groupe de torsion est cyclique : $\mathbb{Z}/11\mathbb{Z}$, $\mathbb{Z}/13\mathbb{Z}$, $\mathbb{Z}/14\mathbb{Z}$, $\mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/18\mathbb{Z}$.

Nous retrouvons ici ces paramétrisations avec plus de détails, en utilisant les algorithmes de van Hoeij [vH95],[vH97] et [vH02], et avec des modèles des courbes modulaires plus simples.

2.2.1.2. Nouvelles paramétrisations. — Dans ce chapitre, nous donnons les paramétrisations des autres structures, c'est-à-dire, le cas où $\text{Tors}(E, K)$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ ou $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Nous donnons également quelques exemples explicites de courbes elliptiques avec des sous-groupes de torsion non triviaux, et de rang non nul. Nous montrons aussi le non existence de courbes elliptiques (définies sur certains corps) possédant des torsions spéciales.

2.2.2. Sur le rang. — Soit K un corps de nombres et G un groupe abélien fini tels qu'il existe une courbe elliptique sur K dont le sous-groupe de torsion défini sur K est isomorphe à G , puis définissons :

$$\text{Br}(G, K) = \sup_{E_G} \text{rang}(E_G(K))$$

où E_G parcourt les courbes elliptiques sur K avec $\text{Tors}(E, K) \simeq G$.

La recherche du rang d'une courbe est un peu délicat. La méthode la plus habituelle est celle de la 2-descente. Dans cet article, nous utilisons le programme de Simon [Simb], sur PARI/gp [BBB⁺] pour calculer le rang des courbes ou, à défaut, trouver une bonne majoration pour celui-ci. Dans la pratique, conjuguer à la fois rang élevé et torsion non trivial est assez difficile. Par exemple, pour $K = \mathbb{Q}$ et pour $G = \mathbb{Z}/9\mathbb{Z}, \mathbb{Z}/12\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, on ne sait pas si $\text{Br}(G, \mathbb{Q}) \geq 4$ (voir la page de Dujella [Dujb] pour des exemples de courbes elliptiques avec $\text{Br}(G, \mathbb{Q}) = 3$ ainsi que la liste des records actuels).

2.3. Paramétrisations des structures

2.3.1. Les courbes modulaires. — Soient deux entiers positifs M et N tels que $M|N$ et soit $\Gamma_1(M, N)$, le sous-groupe de congruence de $SL(2, \mathbb{Z})$ défini par :

$$\Gamma_1(M, N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N}, b \equiv 0 \pmod{M} \right\}$$

Le groupe $\Gamma_1(M, N)$ agit sur le demi-plan de Poincaré :

$$\mathbb{H} = \{z \in \mathfrak{c} \mid \Im(z) > 0\},$$

et on note par

$$Y_1(M, N) = \mathbb{H}/\Gamma_1(M, N).$$

C'est l'espace des modules des classes d'isomorphismes des courbes elliptiques avec des points (P_M, P_N) tel que $\langle P_M \rangle \times \langle P_N \rangle$ est un sous-groupe isomorphe à $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ (voir [KM88]). On note aussi $X_1(M, N)$ le compactifié de $Y_1(M, N)$. Notons que $X_1(N)$ et $X_1(1, N)$ désignent la même variété.

Proposition 2.1 ([JK05]). — Soit $g \in \{0, 1, 2\}$ et soient les ensembles S_g suivants :

$$S_0 = \{(4), (5), (6), (7), (8), (9), (10), (12), (2, 4), (2, 6), (2, 8), (3, 3), (3, 6), (4, 4)\}$$

$$S_1 = \{(11), (14), (15), (2, 10), (2, 12)\}$$

$$S_2 = \{(13), (16), (18)\}$$

alors $X_1(\lambda)$ est de genre g si $\lambda \in S_g$.

La dernière proposition signifie que si l'on se donne un corps de nombres K fixé, alors $Br(G, K)$ est borné pour $G = \mathbb{Z}/13\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$ ou $\mathbb{Z}/18\mathbb{Z}$ puisqu'il n'existe qu'un nombre fini de courbes elliptiques avec ces torsions. Ceci est une conséquence directe du théorème de Faltings (voir [Fal83]).

2.3.2. Forme normale de Tate. — Soit E une courbe elliptique définie sur le corps K de la forme :

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

On suppose aussi que la courbe possède un point rationnel non trivial sur K qui ne soit d'ordre 2 ni 3. Une transformation birationnelle ramène ce point à l'origine et de plus l'équation de E devient :

$$E_{b,c} : y^2 + (1-c)xy + by = x^3 + bx^2.$$

C'est la forme normale de Tate. Le discriminant de $E_{b,c}$ est donné par :

$$\Delta_{E_{b,c}} = b^3(-c^4 + 3c^3 + (-8b-3)c^2 + (-20b+1)c + (-16b^2+b)) \neq 0.$$

Il est clair que le point $P_0 = (0, 0)$ est sur la courbe $E_{b,c}$. Pour une discussion plus détaillée, voir l'annexe A ou [Kna92, Chapitre V]. Voir aussi [Mes81].

Remarque 2.2. — Notons que dans l'équation de la courbe $E_{b,c}$, b doit être nécessairement non nul puisque dans le cas contraire, la courbe serait singulière.

On utilisera par la suite la courbe de Tate pour construire la forme générale des courbes elliptiques avec des sous-groupes de torsions non triviales. Nous verrons cela plus en détail dans le paragraphe suivant l'utilisation de la loi de groupe, donnée par la méthode de la corde et de la tangente.

2.3.3. Description générale. — Décrivons maintenant les méthodes utilisées pour les paramétrisation des structures de torsion.

Les cas $\lambda = (N)$, $N \geq 4$. — Pour trouver une relation entre les coefficients b et c de la forme normale de Tate, on impose que le point $P_0 = (0, 0)$ soit d'ordre N en utilisant les formules de la loi du groupe.

Cas où N est pair : on utilise la relation $[\frac{N}{2}]P_0 = [-\frac{N}{2}]P_0$.

Cas où N est impair : on utilise alors $[\frac{N+1}{2}]P_0 = [-\frac{N-1}{2}]P_0$.

Notons que nous utilisons PARI/gp [BBB⁺] pour les calculs :

1. Initialiser la courbe $E_{b,c} = [1 - c, b, b, 0, 0]$;
2. Initialiser le point $P_0 = [0, 0]$;
3. Prendre le contenu du vecteur $[\frac{N}{2}]P_0 = [-\frac{N}{2}]P_0$ ou $[\frac{N}{2}]P_0 = [-\frac{N}{2}]P_0$.

On obtient ainsi une certaine équation $\mathcal{U}_{b,c} = 0$ en b et c . Cette équation ne définit pas forcément une courbe irréductible sur \mathbb{Q} . On peut simplifier en particulier par les expressions $U_{b,c}$ obtenues de la même manière pour les diviseurs de N . L'équation obtenue est alors celle de $X_1(\lambda)$, que l'on peut réduire en utilisant les algorithmes de van Hoeij [vH97], [vH95] et [vH02].

Les cas $\lambda = (2, 2N)$. — Pour trouver la forme des courbes elliptiques avec une torsion isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$, on commence par regarder la paramétrisation des courbes avec un point d'ordre $2N$. On remarque alors que le point $Q = [N]P_0$ est d'ordre 2, cela suggère un changement de variable convenable, pour se ramener à une forme du type :

$$E : y^2 = x(x^2 + fx + g) .$$

Pour avoir la 2-torsion complète ($E[2] \subset E(K)$), nous imposons à ce que $f^2 - 4g$ soit un carré dans K^* , ce qui donne la relation souhaitée entre les coefficients de E .

Les cas $\lambda = (3, 3N)$ avec $N \in \{1, 2\}$. — Pour obtenir la 3-torsion complète ($E[3] \subset E(K)$) à partir de la paramétrisation des courbes ayant une torsion cyclique d'ordre $3N$, il suffit d'écrire le polynôme de 3-division et d'imposer que ses

racines soient rationnelles.

Le cas $\lambda = (4, 4)$. — Partant du type $(2, 4)$, on résout une équation du type $P = [2]Q$.

Pour la réduction et la minimisation des courbes de genre 1 (resp. 2), on peut par exemple utiliser l'algorithme de Van Hoeij [**vH95**] (resp. [**vH02**]).

2.4. Torsion des courbes elliptiques définies sur \mathbb{Q} .

Dans [**Kub76**], Kubert a donné les paramétrisations des structures de torsion pour le cas $K = \mathbb{Q}$. Nous indiquons ici plus de détails sur ces paramétrisations.

2.4.1. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/2\mathbb{Z}$. — Prenons la forme de Weierstrass réduite :

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

Supposons que $P(x_P, y_P) \in E(K)[2]$, le changement de variable $x \mapsto x - x_P$ ramène à la forme générale :

$$\mathcal{E}^{(2)} : y^2 = x(x^2 + sx + t), \text{ où } s, t \in K \text{ sont tels que :} \quad (2.24)$$

$$\Delta_{\mathcal{E}^{(2)}} = 16t^2(s^2 - 4t) \neq 0 .$$

Le point $P_0 = (0, 0)$ est d'ordre 2.

2.4.2. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/3\mathbb{Z}$. — Nous connaissons par exemple depuis [**Kna92**, p. 146] que les courbes elliptiques avec un point d'ordre 3 ont un modèle de la forme :

$$\mathcal{E}^{(3)} : y^2 + sxy + ty = x^3 \text{ avec } s, t \in K \text{ sont tels que :} \quad (2.25)$$

$$\Delta_{\mathcal{E}^{(3)}} = t^3(s^3 - 27t) \neq 0 .$$

Le point $P_0 = (0, 0)$ est d'ordre 3.

2.4.3. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/4\mathbb{Z}$. — On sait que E peut être donnée par son modèle de Tate $E_{b,c}$, avec $b \neq 0$ (voir remarque 2.2). L'égalité $[2]P_0 = [-2]P_0$ (c'est-à-dire $[4]P_0 = \mathcal{O}$) équivaut alors à :

$$U_{b,c} : c = 0 .$$

On en déduit alors la forme générale des courbes :

$$\mathcal{E}^{(4)} : y^2 + xy + ty = x^3 + tx^2 \text{ avec } t \in K \text{ est tel que :} \quad (2.26)$$

$$\Delta_{\mathcal{E}^{(4)}} = (-16t + 1)t^4 \neq 0 .$$

Le point $P_0 = (0, 0)$ est d'ordre 4.

2.4.4. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/5\mathbb{Z}$. — L'égalité $[3]P_0 = [-2]P_0$ sur la forme normale de Tate $E_{b,c}$ est équivalente à :

$$\mathcal{U}_{b,c} : b + c = 0$$

On en déduit la forme générale des courbes :

$$\mathcal{E}^{(5)} : y^2 + (1-t)xy - ty = x^3 - tx^2 \text{ avec } t \in K \text{ tel que :} \quad (2.27)$$

$$\Delta_{\mathcal{E}^{(5)}} = t^5(t^2 - 11t - 1) \neq 0.$$

Le point $P_0 = (0, 0)$ est d'ordre 5 sur $\mathcal{E}^{(5)}$.

2.4.5. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/6\mathbb{Z}$. — L'égalité $[3]P_0 = [-3]P_0$ sur la forme normale de Tate $E_{b,c}$ équivaut à :

$$\mathcal{U}_{b,c} : b + c + c^2 = 0.$$

On en déduit la forme générale :

$$\mathcal{E}^{(6)} : y^2 + (1-t)xy - t(t+1)y = x^3 - t(t+1)x^2 \text{ avec } t \in K \text{ tel que :} \quad (2.28)$$

$$\Delta_{\mathcal{E}^{(6)}} = t^6(t+1)^3(9t+1) \neq 0.$$

Le point $P_0 = (0, 0) \in \mathcal{E}^{(6)}$ est d'ordre 6.

2.4.6. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/7\mathbb{Z}$. — L'égalité $[4]P_0 = [-3]P_0$ sur la forme normale de Tate $E_{b,c}$ équivaut à :

$$\mathcal{U}_{b,c} : -c^3 + bc + b^2 = 0.$$

Cela définit une courbe de genre 0, donc paramétrisable. L'algorithme [vH97] donne ensuite :

$$(b, c) = (t^2(1-t), t^2 - t)$$

On en déduit la forme générale des courbes :

$$\mathcal{E}^{(7)} : y^2 - (t^2 - t - 1)xy - t^2(t-1)y = x^3 - t^2(t-1)x^2. \quad (2.29)$$

où $t \in K$ est tel que le discriminant de $\mathcal{E}^{(7)}$:

$$\Delta_{\mathcal{E}^{(7)}} = t^7(t-1)^7(t^3 - 8t^2 + 5t + 1) \neq 0.$$

Le point $P_0 = (0, 0)$ est d'ordre 7.

2.4.7. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/8\mathbb{Z}$. — Pour que $P_0 = (0, 0)$ soit d'ordre 8 sur la courbe elliptique $E_{b,c}$, il faut que $bc \neq 0$, puisque sinon $E_{b,c}$ serait singulière ou $[4]P_0 = \mathcal{O}$ d'après 2.3.2 et 2.4.3. L'égalité $[4]P = [-4]P$ ($[4]P_0 \neq \mathcal{O}$) équivaut alors à :

$$U_{b,c} : 2b^2 + bc^2 + 3bc + c^2 = 0 .$$

que l'on peut paramétrer grâce à [vH97] par :

$$(b, c) = \left(-6 - 7u - 2u^2, -\frac{6 + 7u + 2u^2}{1 + u} \right)$$

On obtient alors la forme :

$$\mathcal{E} : y^2 - \frac{2u^2 - 4u + 1}{u}xy - (2u - 1)(t - 1)y = x^3 - (2u - 1)(u - 1)x^2 .$$

Puis en posant $t = u - 1$, et en faisant le changement de variable :

$$(x, y) \mapsto \left(\frac{x}{t^2}, \frac{y}{t^3} \right) ,$$

on obtient la forme générale plus simple :

$$\begin{aligned} \mathcal{E}^{(8)} : y^2 - (2t^2 - 4t + 1)xy - (2t - 1)(t - 1)t^3y \\ = x^3 - (2t - 1)(t - 1)t^2x^2 . \end{aligned} \quad (2.30)$$

où $t \in K$ est tel que le discriminant de $\mathcal{E}^{(8)}$, donné par :

$$\Delta_{\mathcal{E}^{(8)}} = t^8(t - 1)^8(2t - 1)^4(8t^2 - 8t + 1) ,$$

est non nul. Le point $P_0 = (0, 0)$ est d'ordre 8.

2.4.8. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/9\mathbb{Z}$. — Soient $b \neq 0$ et $P_0 = (0, 0)$ tel que $[3]P_0 = \mathcal{O}$. L'égalité $[5]P_0 = [-4]P_0$ sur la forme normale de Tate $E_{b,c}$ équivaut à :

$$\mathcal{U}_{b,c} : b^3 + 3b^2c + bc^3 + 3bc^2 + c^5 + c^4 + c^3 = 0 .$$

En utilisant l'algorithme [vH97], on trouve la paramétrisation suivante :

$$(b, c) = (-t^2(t - 1)(t^2 - t + 1), t^2(t - 1))$$

On obtient alors la forme générale :

$$\begin{aligned} \mathcal{E}^{(9)} : y^2 + (-t^3 + t^2 + 1)xy - t^2(t - 1)(t^2 - t + 1)y \\ = x^3 - t^2(t - 1)(t^2 - t + 1)x^2, \end{aligned} \quad (2.31)$$

où $t \in K$ est tel que le discriminant :

$$\Delta_{\mathcal{E}^{(9)}} = t^9(t - 1)^9(t^2 - t + 1)^3(t^3 - 6t^2 + 3t + 1) \neq 0 .$$

Le point $P_0 = (0, 0)$ est d'ordre 9.

2.4.9. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/10\mathbb{Z}$. — Soient $b \neq 0$ et $P = (0, 0)$ tel que $\text{ord}(P_0) \notin \{2, 5\}$. L'égalité $[5]P = [-5]P$ sur la forme normale de Tate $E_{b,c}$ est équivalente à :

$$\mathcal{U}_{b,c} : b^3 + 3b^2c^2 + 2b^2c + bc^4 + 3bc^3 + bc^2 - c^5 = 0 .$$

Cette équation définit une courbe de genre 0. L'algorithme [vH97] permet de trouver la paramétrisation :

$$(b, c) = \left(\frac{-t^3(t-1)(t-2)}{(t^2-6t+4)^2}, \frac{-t(t-1)(t-2)}{t^2-6t+4} \right)$$

On obtient alors la forme :

$$\mathcal{E}^{(10)} : y^2 + \frac{t^3 - 2t^2 - 4t + 4}{t^2 - 6t + 4}xy - \frac{(t-1)(t-2)t^3}{(t^2 - 6t + 4)^2}y = x^3 - \frac{(t-1)(t-2)t^3}{(t^2 - 6t + 4)^2}x^2 .$$

et le changement de variable :

$$(x, y) \mapsto \left(\frac{x}{(t^2 - 6t + 4)^2}, \frac{y}{(t^2 - 6t + 4)^3} \right)$$

donne la forme générale plus simple :

$$\begin{aligned} \mathcal{E}^{(10)} : y^2 + (t^3 - 2t^2 - 4t + 4)xy \\ - (t-1)(t-2)(t^2 - 6t + 4)t^3y = x^3 - (t-1)(t-2)t^3x^2. \end{aligned} \quad (2.32)$$

où $t \in K$ est tel que le discriminant de $\mathcal{E}^{(10)}$, donné par :

$$\Delta_{\mathcal{E}^{(10)}} = (t-1)^5(t-2)^{10}t^{10}(t^2 - t - 1)(t^2 - 6t + 4)^2 ,$$

soit non nul. Le point $P_0 = (0, 0)$ est d'ordre 10.

2.4.10. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/12\mathbb{Z}$. — On suppose que $b \neq 0$ et soit $P_0 = (0, 0)$ tel que $\text{ord}(P_0) \notin \{2, 3, 4, 6\}$, alors l'égalité $[6]P_0 = [-6]P_0$ sur la forme normale de Tate $E_{b,c}$ équivaut à :

$$\mathcal{U}_{b,c} : 3b^4 + b^3c^2 + 9b^3c + 10b^2c^2 - bc^4 + 5bc^3 + c^6 + c^4 = 0 .$$

Cette équation définit une courbe de genre 0. L'algorithme [vH97] permet de trouver la paramétrisation :

$$(b, c) = \left(\frac{-12t^6 + 30t^5 - 34t^4 + 21t^3 - 7t^2 + t}{(t-1)^4}, \frac{-6t^4 + 9t^3 - 5t^2 + t}{(t-1)^3} \right)$$

On obtient alors la forme :

$$\begin{aligned} \mathcal{E}^{(12)} : y^2 + \frac{6t^4 - 8t^3 + 2t^2 + 2t - 1}{(t-1)^3}xy \\ + \frac{-12t^6 + 30t^5 - 34t^4 + 21t^3 - 7t^2 + t}{(t-1)^4}y \\ = x^3 + \frac{-12t^6 + 30t^5 - 34t^4 + 21t^3 - 7t^2 + t}{(t-1)^4}x^2. \end{aligned}$$

Enfin, le changement de variable suivant :

$$(x, y) \mapsto \left(\frac{x}{(t-1)^6}, \frac{y}{(t-1)^9} \right)$$

donne la forme générale, sans dénominateur :

$$\begin{aligned} \mathcal{E}^{(12)} : y^2 + (6t^4 - 8t^3 + 2t^2 + 2t - 1)xy \\ + (-12t^6 + 30t^5 - 34t^4 + 21t^3 - 7t^2 + t)(t-1)^5y \\ = x^3 + (-12t^6 + 30t^5 - 34t^4 + 21t^3 - 7t^2 + t)((t-1)^2x^2). \quad (2.33) \end{aligned}$$

où $t \in K$ est tel que le discriminant de $\mathcal{E}^{(12)}$, donné par :

$$\Delta_{\mathcal{E}^{(12)}} = t^{12}(t-1)^{12}(2t-1)^6(2t^2-2t+1)^3(3t^2-3t+1)^4(6t^2-6t+1),$$

est non nul. Le point $P_0 = (0, 0)$ est d'ordre 12.

2.4.11. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. — La forme générale pour cette structure est bien connue :

$$\mathcal{E}^{(2,2)} : y^2 = x(x-s)(x-t) \text{ avec } s, t \in K, \quad (2.34)$$

tels que le discriminant de $\mathcal{E}^{(2,2)}$ donné par :

$$\Delta_{\mathcal{E}^{(2,2)}} = 16s^2t^2(s-t)^2,$$

ne soit pas nul. Les points $(0, 0), (s, 0), (t, 0)$ sont d'ordre 2.

2.4.12. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. — Considérons la forme de Tate des courbes avec un point d'ordre 4 (voir 2.4.3) :

$$\mathcal{E}^{(4)} : y^2 + xy + ty = x^3 + tx^2.$$

Cette courbe est birationnellement équivalente à :

$$\mathcal{E}^{(4)} : y^2 = x \left(x^2 + \left(-2t + \frac{1}{4} \right) x + t^2 \right) = x f_t(x)$$

Pour que cette courbe admette une 2-torsion complète, il faut et il suffit que le discriminant de $f_t(x)$ soit un carré dans K^* , soit :

$$\Delta(f_t(x)) = -t + \frac{1}{16} = u^2, \text{ où } u \in K^* .$$

La forme générale des courbes elliptiques dont la partie de torsion contient cette structure s'ensuit :

$$\mathcal{E}^{(2,4)} : y^2 + xy - (t^2 - \frac{1}{16})y = x^3 - (t^2 - \frac{1}{16})x^2, \quad (2.35)$$

où $t \in K$ est tel que le discriminant de $\mathcal{E}^{(2,4)}$ donné par :

$$\Delta_{\mathcal{E}^{(2,4)}} = \frac{1}{2^{12}} t^2 (4t - 1)^4 (4t + 1)^4 \neq 0.$$

Les points

$$P_0 = (0, 0) \text{ et } Q_2 = \left(\frac{1}{8}(4t - 1), \frac{1}{32}(4t - 1)^2 \right)$$

sont d'ordre 4 et 2 respectivement et engendrent un sous-groupe isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

2.4.13. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. — Considérons la forme de Tate des courbes avec un point d'ordre 6 (d'après 2.4.5)

$$\mathcal{E}^{(6)} : y^2 + (1 - t)xy - t(t + 1)y = x^3 - t(t + 1)x^2.$$

Cette courbe est birationnellement équivalente à :

$$\mathcal{E}^{(6)} : y^2 = x f_t(x) = x \left(x^2 + \left(\frac{-3}{4}t^2 + \frac{3}{2}t + \frac{1}{4} \right) x - t^3 \right)$$

Pour avoir la 2-torsion complète, nous imposons que le discriminant de $f_t(x)$

$$\Delta(f_t(x)) = \frac{1}{16}(t + 1)^3(9t + 1)$$

soit un carré. On considère alors la courbe :

$$X_1(2, 6) : (t + 1)(9t + 1) - u^2 = 0$$

Cette courbe est de genre 0. L'algorithme [vH97] permet de trouver la paramétrisation :

$$(t, u) = \left(\frac{z^2 - z}{3z + 1}, \frac{3z^2 + 2z - 1}{3z + 1} \right),$$

puis le changement de variable :

$$(x, y) \mapsto \left(\frac{x}{(3z + 1)^2}, \frac{y}{(3z + 1)^3} \right)$$

donne la forme générale simplifiée :

$$\begin{aligned} \mathcal{E}^{(2,6)} : y^2 + (-t^2 + 4t + 1)xy - t(t-1)(t+1)^2(3t+1)y \\ = x^3 - t(t-1)(t+1)^2x^2. \end{aligned} \quad (2.36)$$

où $t \in K$ est tel que le discriminant de $\mathcal{E}^{(2,6)}$ donné par :

$$\Delta_{\mathcal{E}^{(2,6)}} = t^6(t-1)^6(t+1)^6(3t-1)^2(3t+1)^2 \neq 0.$$

Les points :

$$P_0 = (0, 0) \text{ et } Q = \left(\frac{3}{4}(t-1)(3t+1)(t+1)^2, \frac{3}{8}(t-1)^2(3t+1)(t+1)^3 \right),$$

sont d'ordre 6 et 2 respectivement et on a :

$$\langle Q, P_0 \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}.$$

2.4.14. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. — Considérons la forme de Tate des courbes avec un point d'ordre 8 (voir 2.4.7) :

$$\mathcal{E}^{(8)} : y^2 - \frac{2t^2 - 4t + 1}{t}xy - (2t-1)(t-1)y = x^3 - (2t-1)(t-1)x^2.$$

Cette courbe est birationnellement équivalente à :

$$\mathcal{E}^{(6)} : y^2 = x \left(x^2 + \left(\frac{8t^4 - 16t^3 + 16t^2 - 8t + 1}{4t^2} \right) x + t^4 - 4t^3 + 6t^2 - 4t + 1 \right) = x f_t(x).$$

Pour que la 2-torsion complète soit définie sur K , il faut et il suffit que le discriminant de $f_t(x)$

$$\Delta(f_t(x)) = \frac{(2t-1)^4(8t^2 - 8t + 1)}{16t^4}$$

soit un carré. Nous considérons alors la courbe :

$$X_1(2, 8) : 8t^2 - 8t + 1 - u^2 = 0,$$

Cette courbe est de genre 0. En utilisant l'algorithme [vH97], on obtient la paramétrisation :

$$(t, u) = \left(\frac{2z + z^2}{-8 + z^2}, \frac{-z^2 - 8 - 8z}{-8 + z^2} \right).$$

La forme générale des courbes elliptiques avec cette structure est ainsi donnée par :

$$\begin{aligned} \mathcal{E}^{(2,8)} : y^2 + \frac{z^4 - 24z^2 - 64z - 64}{z(z+2)(z^2-8)}xy - 2 \frac{(z^2 + 4z + 8)(z+4)}{(z^2-8)^2}y \\ = x^3 - 2 \frac{(z^2 + 4z + 8)(z+4)}{(z^2-8)^2}x^2. \end{aligned}$$

Avec le changement de variable

$$(x, y) \mapsto \left(\frac{x}{(z(z+2)(z^2-8))^2}, \frac{y}{(z(z+2)(z^2-8))^3} \right)$$

puis en substituant z par t , on se ramène à la forme plus simple :

$$\begin{aligned} \mathcal{E}^{(2,8)} : y^2 + (t^4 - 24t^2 - 64t - 64)xy \\ - 2(t^2 + 4t + 8)(t + 4)(t^2 - 8)(t + 2)^3 t^3 y \\ = x^3 - 2(t^2 + 4t + 8)(t + 4)(t + 2)^2 t^2 x^2, \end{aligned} \quad (2.37)$$

où $t \in K$ est tel que le discriminant de $\mathcal{E}^{(2,8)}$ donné par :

$$\Delta_{\mathcal{E}^{(2,8)}} = 2^8 t^8 (t + 2)^8 (t + 4)^8 (t^2 - 8)^2 (t^2 + 4t + 8)^4 (t^2 + 8t + 8)^2 \neq 0.$$

Les points

$$P_0 = (0, 0) \text{ et}$$

$$Q = \left(\frac{-z^3(z+4)(z^2-8)(z^2+4z+8)}{4}, \frac{z^4(z+4)^2(z^2-8)(z^2+4z+8)^2}{8} \right),$$

sont d'ordre 8 et 2 respectivement, et on a :

$$\langle Q, P_0 \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}.$$

2.5. Les torsions supplémentaires pour $[K : \mathbb{Q}] = 2$

2.5.1. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/11\mathbb{Z}$. — La paramétrisation des courbes elliptiques avec un point d'ordre 11 est donc un peu différente des cas précédents puisque le genre de $X_1(11)$ est 1 et non plus 0. Nous reprenons ici la forme vue dans [Sil94, p. 190] ou [Rei85] pour plus détails des transformations utilisées. Soit maintenant la courbe modulaire $X_1(11)$ (c'est la courbe 11a3 dans la table de Cremona [Cre97]) définie par :

$$X_1(11) : s^2 - s = t^3 - t^2,$$

les expressions de b et $a = 1 - c$ deviennent :

$$\begin{aligned} b &= \frac{s(s-1)(s-t)}{t}, \\ a = 1 - c &= \frac{st + t - s^2}{t}. \end{aligned}$$

La forme générale des courbes avec un point d'ordre 11 est donnée par :

$$\mathcal{E}^{(11)} : y^2 + (st + t - s^2)xy + s(s-1)(s-t)t^2y = x^3 + s(s-1)(s-t)tx^2. \quad (2.38)$$

où $P = (t, s) \in X_1(11)$ est tel que :

$$t(t-1)(t^5 - 18t^4 + 35t^3 - 16t^2 - 2t + 1) \neq 0.$$

Il est bien connu qu'il n'existe pas de courbe elliptique défini sur \mathbb{Q} , avec un point d'ordre 11. En effet, la courbe modulaire $X_1(11)$ est de rang 0 sur \mathbb{Q} et admet exactement 5 points rationnels sur \mathbb{Q} (voir le rang de 11a3 dans la table de Cremona [Cre97]) :

$$X_1(11)(\mathbb{Q}) = \{\mathcal{O}, (0, 0), (1, 0), (0, 1), (1, 1)\}$$

De plus, ces points induisent des courbes singulières dans la paramétrisation (2.38) ci-dessus.

Lemme 2.1. — *Soit K un corps de nombres quadratique, alors :*

$$\text{Tors}(X_1(11), K) = \text{Tors}(X_1(11), \mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z} .$$

Démonstration. — Nous utilisons le modèle :

$$C : y^2 = f(x) = x^3 - 432x + 8208,$$

pour la courbe modulaire $X_1(11)$. On observe d'abord que :

$$\text{Tors}(X_1(11), K) \supseteq \text{Tors}(X_1(11), \mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z} .$$

Par le théorème 2.2, les seules structures possibles pour $\text{Tors}(X_1(11), K)$ sont : $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$. Pour prouver le lemme, il suffit donc de voir que $X_1(11)$ n'a pas de point d'ordre 2, ni 3.

Le polynôme f est de degré 3 et est irréductible sur \mathbb{Q} , il est donc irréductible sur toutes les extensions quadratiques de \mathbb{Q} , d'où l'on tire que $X_1(11)$ ne possède pas de point de 2-torsion sur K .

Soit Ψ_3 le polynôme de 3-division de C :

$$\Psi_3(x) = x^4 - 864x^2 + 32832x - 62208 .$$

Si $C(K)$ a un point d'ordre 3, alors Ψ_3 a un facteur linéaire sur K , donc Ψ_3 a un facteur quadratique sur \mathbb{Q} . Or Ψ_3 est irréductible sur \mathbb{Q} , il ne peut y avoir de point d'ordre 3 dans $C(K)$. \square

Remarque 2.3. — *Il est clair que si K est tel que $X_1(11)(K) = X_1(11)(\mathbb{Q})$, alors il n'existe pas de courbe elliptique sur K avec un point d'ordre 11. En revanche si le rang de $X_1(11)$ sur K est non nul, cela permet d'affirmer immédiatement qu'il existe une infinité de courbes elliptiques sur K avec un point d'ordre 11.*

Exemple 2.1. — La courbe $C_d : y^2 = x^3 - 4dx^2 + 16d^3$ est isomorphe (sur $\mathbb{Q}(\sqrt{d})$) à la courbe $X_1(11)$, de plus si $P_3 = (a, b)$ est un point non trivial sur $C_d(\mathbb{Q})$, on trouvera que le point

$$P = (t, s) = \left(\frac{a}{4d}, \frac{b\sqrt{d}}{8d^2} + \frac{1}{2} \right)$$

est un point de $X_1(11)(\mathbb{Q}(\sqrt{d}))$. On peut utiliser cette méthode pour obtenir des points d'ordre infini sur $X_1(11)(K)$.

Nous utilisons ici les programmes de Simon [Sima] et [Simb] pour trouver le rang et des points sur $X_1(11)(\mathbb{Q}(\sqrt{d}))$.

La table 2.1 donne une liste de structure du groupe de $X_1(11)(\mathbb{Q}(\sqrt{d}))$ avec $|d| \leq 10$.

d	$\mathbb{Q}(\sqrt{d})$	$X_1(11)(\mathbb{Q}(\sqrt{d}))$	Point d'ordre infini
-10	$\theta^2 + 10 = 0$	$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}$	$(-\frac{241}{250}, -\frac{4961\theta + 1}{12500})$
-7	$\theta^2 + 7 = 0$	$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}$	$(\frac{\theta+5}{8}, \frac{11-\theta}{16})$
-6	$\theta^2 + 6 = 0$	$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}$	$(-\frac{25}{6}, \frac{18-139\theta}{36})$
-5	$\theta^2 + 5 = 0$	$\mathbb{Z}/5\mathbb{Z}$	-
-3	$\theta^2 + 3 = 0$	$\mathbb{Z}/5\mathbb{Z}$	-
-2	$\theta^2 + 2 = 0$	$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}$	$(-\frac{1}{2}, \frac{2-\theta}{4})$
-1	$\theta^2 + 1 = 0$	$\mathbb{Z}/5\mathbb{Z}$	-
2	$\theta^2 - 2 = 0$	$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}$	$(\frac{1}{2}, \frac{2-\theta}{4})$
3	$\theta^2 - 3 = 0$	$\mathbb{Z}/5\mathbb{Z}$	-
5	$\theta^2 - 5 = 0$	$\mathbb{Z}/5\mathbb{Z}$	-
6	$\theta^2 - 6 = 0$	$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}$	$(-7\theta + 18, -42\theta + 103)$
7	$\theta^2 - 7 = 0$	$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}$	$(-2\theta + 5, -6\theta + 16)$
10	$\theta^2 - 10 = 0$	$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}$	$(\frac{9}{10}, \frac{50-13\theta}{50})$

TAB. 2.1. $X_1(11)(\mathbb{Q}(\sqrt{d}))$, $-10 \leq d \leq 10$.

Nous avons maintenant le théorème suivant :

Théorème 2.3. — Soit $d \in \{-3239, -599, -47, 6, 7, 22, 73, 193\}$, alors il existe au moins une courbe elliptique définie sur $\mathbb{Q}(\sqrt{d})$, de rang 1 et dont le sous-groupe de torsion est isomorphe à $\mathbb{Z}/11\mathbb{Z}$:

$$\text{Br}(\mathbb{Z}/11\mathbb{Z}, \mathbb{Q}(\sqrt{d})) \geq 1.$$

Démonstration. — Nous donnons explicitement les équations des courbes elliptiques sur chacun des corps cités dans le théorème.

- Pour $K = \mathbb{Q}(\sqrt{-3239})$, soit θ avec $\theta^2 - \theta + 810 = 0$. On considère la courbe :

$$E_{-3239} : y^2 = x^3 + \left(3310\theta + \frac{823041}{4}\right)x^2 - (22996305\theta + 502211745)x + 20447192475\theta - 784526490225.$$

A noter que cette courbe est obtenue en faisant $t = -9$ dans l'expression de $\mathcal{E}^{(11)}$ ci-dessus. Par un calcul de 2-descente et en utilisant le programme [**Simb**], on montre que $\text{rang}(E_{-3239}, K) \leq 1$. Du fait que le point $P_{-3239} = (-162\theta + 162, -100602\theta - 96228)$ n'est pas un point de 11-torsion, il s'ensuit qu'il est donc d'ordre infini, d'après la liste des torsions possibles du théorème 2.2. Le rang vaut donc exactement 1.

- Pour $K = \mathbb{Q}(\sqrt{-599})$, soit θ avec $\theta^2 - \theta + 150 = 0$, et soit la courbe :

$$E_{-599} : y^2 = x^3 + \left(324\theta + \frac{30625}{4}\right)x^2 - (204375\theta + 3046875)x + 38671875\theta - 439453125.$$

Le rang de E_{-599} sur $\mathbb{Q}(\sqrt{-599})$ est 1 ([**Simb**]). On peut vérifier facilement, que $Q_{-599} = (0, -1875\theta - 9375)$ est d'ordre 11. Le point :

$$P_{-599} = (-60\theta - 750, -7395\theta - 68250)$$

est d'ordre infini.

- Pour $K = \mathbb{Q}(\sqrt{-47})$, soit θ avec $\theta^2 - \theta + 12 = 0$ et E_{-47} la courbe elliptique :

$$E_{-47} : y^2 = x^3 + \left(\frac{45}{4}\theta + 46\right)x^2 - (24\theta + 1344)x + 2880\theta - 4608.$$

Par un calcul de 2-descente ([**Simb**]), on montre que le rang de E_{-47} sur $\mathbb{Q}(\sqrt{-47})$ est 1. Le point $Q_{-47} = (0, -24\theta - 48)$ est d'ordre 11 et le point :

$$P_{-47} = (-3\theta + 15, -30\theta - 18)$$

est d'ordre infini.

• Soit maintenant le corps $K = \mathbb{Q}(\sqrt{6})$, et soit θ avec $\theta^2 - 6 = 0$. Considérons alors la courbe :

$$E_6 : y^2 = x^3 + (2725751520\theta - 6998236812)x - 125187864624576\theta + 308865461210640.$$

Par un calcul de 2-descente [**Simb**], on montre que le rang de E_6 sur $\mathbb{Q}(\sqrt{6})$ est 1. Le point $Q_6 = (8328\theta - 3390, -6480000\theta + 14580000)$ est d'ordre 11 et le point :

$$P_6 = (19128\theta - 46590, 6998400\theta - 15681600)$$

est d'ordre infini.

• Pour $K = \mathbb{Q}(\sqrt{7})$, soit θ avec $\theta^2 - 7 = 0$ et soit la courbe :

$$E_7 : Y^2 = x^3 - (405889920\theta + 1039492656)x + 7062737158656\theta + 18719722947456.$$

Le rang de E_7 sur $\mathbb{Q}(\sqrt{7})$ est 1 (calcul de 2-descente [**Simb**]). Le point $Q_7 = (8880\theta + 27420, -1575936\theta - 3691008)$ est d'ordre 11 et le point

$$P_7 = \left(\frac{27600}{7}\theta + \frac{115908}{7}, \frac{4852224}{49}\theta - \frac{2985984}{7} \right)$$

est d'ordre infini.

• Pour $K = \mathbb{Q}(\sqrt{22})$, soit θ avec $\theta^2 - 4\theta - 18 = 0$ et soit la courbe :

$$E_{22} : y^2 = x^3 + \left(\frac{59}{128}\theta - \frac{621}{256} \right) x^2 + \frac{81}{2048}\theta x - \frac{6561}{8192}\theta + \frac{177147}{32768}.$$

Par un calcul de 2-descente [**Simb**], on montre que le rang de E_{22} sur $\mathbb{Q}(\sqrt{22})$ est 1. Le point $Q_{22} = (0, -\frac{81}{256}\theta + \frac{243}{128})$ est d'ordre 11 et le point :

$$P_{22} = \left(\frac{81}{4}, -\frac{4779}{256}\theta + \frac{4131}{128} \right)$$

est d'ordre infini.

• Pour $K = \mathbb{Q}(\sqrt{73})$, soit θ avec $\theta^2 - \theta - 18 = 0$ et soit la courbe :

$$E_{73} : y^2 = x^3 + \left(40\theta - \frac{351}{4} \right) x^2 + (-1539\theta + 6561)x - 32805\theta + 177147.$$

Par un calcul de 2-descente [**Simb**], on montre que le rang de E_{73} sur $\mathbb{Q}(\sqrt{73})$ est 1. Le point $Q_{73} = (0, -81\theta + 243)$ est d'ordre 11 et le point :

$$P_{73} = (-22\theta + 90, -54\theta + 486)$$

est d'ordre infini.

- Pour $K = \mathbb{Q}(\sqrt{193})$, soit θ avec $\theta^2 - \theta - 48 = 0$ et soit la courbe :

$$E_{193} : y^2 = x^3 + \left(\frac{513}{4}\theta - 176\right)x^2 + (-20352\theta + 122880)x - 1032192\theta + 9437184 .$$

Le rang de E_{193} sur $\mathbb{Q}(\sqrt{193})$ est 1. Le point $Q_{193} = (0, -384\theta + 1536)$ est d'ordre 11 et le point :

$$P_{193} = (8\theta, -156\theta - 576)$$

est d'ordre infini.

□

2.5.2. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/13\mathbb{Z}$. — Commençons par donner la paramétrisation des courbes elliptiques avec un point d'ordre 13. La condition $[7]P_0 = [-6]P_0$ sur la forme normale de Tate $E_{b,c}$ équivaut à :

$$\begin{aligned} \mathcal{U}_{b,c} : & b^7 + 6cb^6 + (4c^3 + 15c^2)b^5 + (9c^5 + 15c^4 + 20c^3)b^4 \\ & + (5c^7 + 24c^6 + 21c^5 + 15c^4)b^3 + (c^9 + 6c^8 + 21c^7 + 13c^6 + 6c^5)b^2 \\ & + (6c^8 + 3c^7 + c^6)b - c^{10} = 0. \end{aligned} \quad (2.39)$$

Cette équation définit une courbe de genre 2. En utilisant l'algorithme de van Hoeij [**vH02**], on montre qu'une transformation birationnelle permet de réécrire la courbe $\mathcal{U}_{b,c}$ par :

$$X_1(13) : s^2 = t^6 - 2t^5 + t^4 - 2t^3 + 6t^2 - 4t + 1 .$$

et où b et c dans $E_{b,c}$ sont des fonctions de s et t :

$$\begin{cases} a = 1 - c = \frac{(t-1)^2(t^2+t-1)s-t^7+2t^6+3t^5-2t^4-5t^3+9t^2-5t+1}{2t^5}, \\ b = \frac{(t-1)^2((t^5+2t^4-5t^2+4t-1)s-t^8-t^7+4t^6+2t^5+t^4-13t^3+14t^2-6t+1)}{2t^9} \end{cases} . \quad (2.40)$$

La forme générale des courbes elliptiques avec un point d'ordre 13 est ainsi donnée par :

$$\mathcal{E}^{(13)} : y^2 + axy + by = x^3 + bx^2 , \quad (2.41)$$

avec a, b donnés par (2.40), $P = (t, s) \in X_1(13)$ et

$$t(t-1)(t^3 - 4t^2 + t + 1) \neq 0.$$

Le point $P_0 = (0, 0)$ est un point d'ordre 13. Pour une forme sans dénominateur, on pourra faire le changement de variable $(x, y) \mapsto (4t^{10}x, 8t^{15}y)$.

Théorème 2.4. — Soit $K = \mathbb{Q}(\sqrt{193})$, alors il existe une courbe elliptique définie sur K , de rang 2 et dont le sous-groupe de torsion est isomorphe à $\mathbb{Z}/13\mathbb{Z}$:

$$\text{Br}(\mathbb{Z}/13\mathbb{Z}, K) \geq 2.$$

Démonstration. — Soit θ tel que $\theta^2 - 193 = 0$ et soit la courbe :

$$C : y^2 + \left(-\frac{9}{64}\theta - \frac{215}{64}\right)xy + \left(\frac{261}{1024}\theta - \frac{2277}{1024}\right)y = x^3 + \left(\frac{261}{1024}\theta - \frac{2277}{1024}\right)x^2.$$

Le point $P_0 = (0, 0)$ est sur la courbe C et il est d'ordre 13 (voir 2.2). Un calcul de 2-descente [Simb] montre que l'ordre du 2-groupe de Selmer de la courbe C est 4 ($\text{Sel}^2(C/K) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$), ce qui permet de majorer le rang :

$$\text{rang}(C, K) \leq 2.$$

On vérifie facilement alors que les points :

$$P = \left(-\frac{69}{196}\theta - \frac{87}{49}, -\frac{5361}{10976}\theta - \frac{17547}{10976}\right),$$

$$Q = \left(-\frac{21}{64}\theta - \frac{267}{64}, -\frac{1623}{2048}\theta - \frac{22281}{2048}\right),$$

sont des points d'ordre infini puisqu'ils ne sont pas de 13-torsion. De plus, comme P et Q sont indépendants. On conclut donc que $\text{rang}(C, K) = 2$. \square

2.5.3. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/14\mathbb{Z}$. — Soient $P = (0, 0)$ tel que l'ordre de P n'est ni 2 ni 7 (voir 2.4.1 et 2.4.6), et $b \neq 0$. L'égalité $[7]P_0 = [-7]P_0$, sur la forme normale de Tate $E_{b,c}$ est équivalente à :

$$\begin{aligned} \mathcal{U}_{b,c} : & b^6 + 6b^5c^2 + 5b^5c + 5b^4c^4 + 25b^4c^3 + 10b^4c^2 + b^3c^6 + 16b^3c^5 \\ & + 40b^3c^4 + 10b^3c^3 + 4b^2c^7 + 17b^2c^6 + 30b^2c^5 + 5b^2c^4 + bc^9 \\ & + 3bc^8 + 6bc^7 + 10bc^6 + bc^5 + c^7 = 0. \end{aligned} \quad (2.42)$$

En utilisant l'algorithme de van Hoeij [vH95], on montre qu'une transformation birationnelle permet de réécrire la courbe $\mathcal{U}_{b,c}$ définie par (2.42) par :

$$X_1(14) : s^2 + st + s = t^3 - t,$$

avec :

$$\begin{cases} a = 1 - c = \frac{t^4 - st^3 + (2s-4)t^2 - st + 1}{(t+1)(t^3 - 2t^2 - t + 1)}, \\ b = \frac{-t^7 + 2t^6 + (2s-1)t^5 + (-2s-1)t^4 + (-2s+2)t^3 + (3s-1)t^2 - st}{(t+1)^2(t^3 - 2t^2 - t + 1)^2}. \end{cases} \quad (2.43)$$

A noter que cette courbe est la courbe 14a4 dans la table de Cremona [Cre97].

La forme générale des courbes elliptiques avec un point d'ordre 14 est ainsi donnée par :

$$\mathcal{E}_P^{(14)} : y^2 + axy + by = x^3 + bx^2. \quad (2.44)$$

avec a, b donnés par (2.43), $P = (s, t) \in X_1(14)$ et

$$t(t-1)(t+1)(t^3 - 9t^2 - t + 1)(t^3 - 2t^2 - t + 1) \neq 0.$$

Le point $P_0 = (0, 0)$ est un point d'ordre 14.

La courbe modulaire $X_1(14)$ est de rang 0 sur \mathbb{Q} et admet exactement 6 points rationnels sur \mathbb{Q} (voir la table de Cremona [Cre97] pour 14a4). Clairement $X_1(14)(\mathbb{Q}) = \text{Tors}(X_1(14), \mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$ et de plus, ces points induisent des courbes singulières dans la paramétrisation (2.44) ci-dessus :

$$X_1(14)(\mathbb{Q}) = \{\mathcal{O}, (1, 0), (0, 0), (-1, 0), (0, -1), (1, -2)\}$$

Lemme 2.2. — Soit K une extension quadratique de \mathbb{Q} , alors :

$$\text{Tors}(X_1(14), K) \simeq \begin{cases} \mathbb{Z}/6\mathbb{Z}, & \text{si } K \neq \mathbb{Q}(\sqrt{-7}) \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, & \text{si } K = \mathbb{Q}(\sqrt{-7}) \end{cases}$$

Démonstration. — Soit K un corps quadratique, nous utilisons alors le modèle de Weierstrass réduit de $X_1(14)$:

$$C : y^2 = f(x) = x^3 - 675x + 13662$$

On observe d'abord que :

$$\text{Tors}(X_1(14), K) \supseteq \text{Tors}(X_1(14), \mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}.$$

Par le théorème 2.2, les seules structures possibles pour $\text{Tors}(X_1(14), K)$ sont : $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/18\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$. IL suffit donc de montrer que $X_1(14)(K)$ n'a pas de 2-torsion complète sur K (sauf si $K = \mathbb{Q}(\sqrt{-7})$), pas de 4-torsion, ni de 9-torsion.

Il est clair que $C(K)$ possède une 2-torsion complète si et seulement si $\Psi_2 = f$ se scinde sur K . Or $f(x) = (x+3)(x^2 - 33x + 414)$ ne se scinde complètement que

si $K = \mathbb{Q}(\sqrt{-7})$. C'est donc le seul corps quadratique tel qu'on ait la 2-torsion complète.

La factorisation du polynôme de 4-division de C en facteurs irréductibles sur \mathbb{Q} est donnée par :

$$\Psi_4(x) = (x^2 + 66x - 1503)(x^4 - 66x^3 + 2484x^2 + 10098x + 788859).$$

Il en résulte que Ψ_4 n'a de zéros sur K que lorsque $K = \mathbb{Q}(\sqrt{-7})$. Soit alors $K = \mathbb{Q}(\sqrt{-7})$, un calcul simple montre que si $x(P) = \theta$ est la première coordonnée d'un point P , tel que $\theta^2 + 66\theta - 1503 = 0$, alors la deuxième coordonnée $y(P)$ n'est pas dans K puisque $f(\theta)$ n'est pas un carré dans $\mathbb{Q}(\sqrt{-7})$.

Dans la factorisation sur \mathbb{Q} du polynôme de 9-division, il n'y apparaît pas de facteur de degré ≤ 2 , il résulte donc que C ne possède pas de point de 9-torsion sur K . \square

Exemple 2.2. — La table 2.2 montre la structure de groupe $X_1(14)$ sur $\mathbb{Q}(\sqrt{d})$ avec $|d| \leq 10$.

d	$\mathbb{Q}(\sqrt{d})$	$X_1(14)(\mathbb{Q}(\sqrt{d}))$	Point d'ordre infini
-10	$\theta^2 + 10 = 0$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}$	$\left(-\frac{2717}{405}, \frac{97648}{18225}\theta + \frac{1156}{405}\right)$
-7	$\theta^2 + 7 = 0$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	-
-6	$\theta^2 + 6 = 0$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}$	$\left(-\frac{35}{27}, \frac{92}{243}\theta + \frac{4}{27}\right)$
-5	$\theta^2 + 5 = 0$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}$	$\left(-\frac{22}{81}\theta + \frac{35}{81}, \frac{308}{729}\theta - \frac{490}{729}\right)$
-3	$\theta^2 + 3 = 0$	$\mathbb{Z}/6\mathbb{Z}$	-
-2	$\theta^2 + 5 = 0$	$\mathbb{Z}/6\mathbb{Z}$	-
-1	$\theta^2 + 1 = 0$	$\mathbb{Z}/6\mathbb{Z}$	-
2	$\theta^2 - 2 = 0$	$\mathbb{Z}/6\mathbb{Z}$	-
3	$\theta^2 - 3 = 0$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}$	$(-2\theta + 3, 6\theta - 10)$
5	$\theta^2 - 5 = 0$	$\mathbb{Z}/6\mathbb{Z}$	-
6	$\theta^2 - 6 = 0$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}$	$\left(\frac{8}{25}\theta - \frac{3}{25}, -\frac{16}{125}\theta + \frac{6}{125}\right)$
7	$\theta^2 - 7 = 0$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}$	$\left(-\frac{1}{2}, -\frac{1}{4}\theta - \frac{1}{4}\right)$
10	$\theta^2 - 10 = 0$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}$	$\left(\frac{4}{9}\theta + \frac{5}{9}, -\frac{20}{27}\theta - \frac{52}{27}\right)$

TAB. 2.2. $X_1(14)(\mathbb{Q}(\sqrt{d}))$, $-10 \leq d \leq 10$.

Théorème 2.5. — Soit $K \in \left\{\mathbb{Q}(\sqrt{-23}), \mathbb{Q}(\sqrt{265})\right\}$, alors il existe au moins une courbe elliptique définie sur K de rang 1 et dont le sous-groupe de torsion est

isomorphe à $\mathbb{Z}/14\mathbb{Z}$:

$$\mathrm{Br}(\mathbb{Z}/14\mathbb{Z}, K) \geq 1 .$$

Démonstration. — Nous donnons explicitement les équations des courbes elliptiques.

• Pour $K = Q(\sqrt{-23})$ et θ tel que $\theta^2 + 368 = 0$, alors un calcul de 2-descente [Simb] montre que la courbe d'équation :

$$E_{-23} : y^2 + \left(\frac{5}{1872}\theta + \frac{539}{468} \right) xy + \left(\frac{47}{18252}\theta + \frac{527}{4563} \right) y = x^3 + \left(\frac{47}{18252}\theta + \frac{527}{4563} \right) x^2 .$$

est au plus de rang 1 et puisque le point

$$P = \left(\frac{1}{312}\theta - \frac{17}{78}, -\frac{17}{6084}\theta + \frac{133}{1521} \right)$$

n'est pas de 14-torsion, il est d'ordre infini et donc le rang de la courbe vaut exactement 1.

• Soient maintenant $K = Q(\sqrt{265})$ et θ tel que $\theta^2 + 5\theta - 60 = 0$, alors un calcul de 2-descente [Simb] montre que la courbe d'équation

$$E_{265} : y^2 + \left(-\frac{36}{145}\theta + \frac{193}{145} \right) xy + \left(\frac{1452}{21025}\theta - \frac{1872}{4205} \right) y = x^3 + \left(\frac{1452}{21025}\theta - \frac{1872}{4205} \right) x^2$$

est au plus de rang 1. On vérifie facilement que le point

$$P = \left(\frac{10}{29}\theta + \frac{6}{29}, -\frac{202}{841}\theta + \frac{3846}{841} \right)$$

est d'ordre infini puisqu'il n'est pas de torsion (un calcul simple montre qu'il n'est pas d'ordre 14). Le point $P_0 = (0, 0)$ est d'ordre 14 et le rang vaut 1. \square

2.5.4. Le cas $\mathrm{Tors}(E, K) \supseteq \mathbb{Z}/15\mathbb{Z}$. — Soient $b \neq 0$ et $P_0 = (0, 0)$ tel que $\mathrm{ord}(P_0) \notin \{3, 5\}$ (voir 2.4.2 et 2.4.4). La condition $[8]P_0 = [-7]P_0$ sur $E_{b,c}$ équivaut alors à :

$$\begin{aligned} \mathcal{U}_{b,c} : & -c^{13} + (b-1)c^{12} + (-b^2 + 3b - 1)c^{11} + (-3b^2 - 2b - 1)c^{10} \\ & + (-7b^3 - 19b^2 - 8b - 1)c^9 + (-36b^3 - 37b^2 - 9b)c^8 + (-18b^4 - 73b^3 - 36b^2)c^7 \\ & + (-62b^4 - 74b^3)c^6 + (-19b^5 - 81b^4 + b^3)c^5 + (-45b^5 + 5b^4)c^4 \\ & + (-10b^6 + 10b^5)c^3 + 10b^6c^2 + 5b^7c + b^8 = 0 . \end{aligned} \quad (2.45)$$

En utilisant l'algorithme de van Hoeij [vH95], on montre qu'une transformation birationnelle permet de réécrire la courbe $\mathcal{U}_{b,c}$ sous la forme :

$$X_1(15) : s^2 + st + s = t^3 + t^2 ,$$

avec :

$$\begin{cases} a = 1 - c = \frac{(t^2-t)s+(t^5+5t^4+9t^3+7t^2+4t+1)}{(t+1)^3(t^2+t+1)}, \\ b = \frac{t(t^4-2t^2-t-1)s+t^3(t+1)(t^3+3t^2+t+1)}{(t+1)^6(t^2+t+1)}. \end{cases} \quad (2.46)$$

La courbe $X_1(15)$ est notée 15a8 dans la table de Cremona [Cre97].

La forme générale des courbes elliptiques avec un point d'ordre 15 est :

$$\mathcal{E}_P^{(15)} : y^2 + axy + by = x^3 + bx^2. \quad (2.47)$$

avec a, b donnés par (2.46), $P = (t, s) \in X_1(15)$ et

$$t(t+1)(t^2+t+1)(t^4+3t^3+4t^2+2t+1)(t^4-7t^3-6t^2+2t+1) \neq 0 .$$

Le point $P_0 = (0, 0)$ est un point d'ordre 15.

La courbe modulaire $X_1(15)$ est de rang 0 sur \mathbb{Q} et admet exactement 4 points rationnels. Clairement $X_1(15)(\mathbb{Q}) = \text{Tors}(X_1(15), \mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$ et de plus ces points induisent des courbes singulières dans la paramétrisation (2.47) ci-dessus :

$$X_1(15)(\mathbb{Q}) = \{\mathcal{O}, (0, 0), (-1, 0), (0, -1)\}$$

Lemme 2.3. — Soit K une extension quadratique de \mathbb{Q} , alors :

$$\text{Tors}(X_1(15), K) \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, & \text{si } K = \mathbb{Q}(\sqrt{-15}) \\ \mathbb{Z}/8\mathbb{Z}, & \text{si } K \in \{\mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{5})\} \\ \mathbb{Z}/4\mathbb{Z}, & \text{sinon} \end{cases}$$

Démonstration. — Soit K un corps quadratique, nous utilisons alors le modèle de Weierstrass réduit de $X_1(15)$:

$$C : y^2 = f(x) = x^3 - 27x + 8694$$

On observe d'abord que :

$$\text{Tors}(X_1(15), K) \supseteq \text{Tors}(X_1(15), \mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z} .$$

Par le théorème 2.2, les seuls sous-groupes de torsion possibles sur K sont : $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Le polynôme de 3-division de C :

$$\Psi_3(x) = 3x^4 - 162x^2 + 104328x - 729,$$

est irréductible sur \mathbb{Q} et donc, n'a pas de zéro sur K . Il en résulte que les cas $\mathbb{Z}/12\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ sont à écarter puisque $C(K)$ ne peut avoir de point 3-torsion.

La factorisation du polynôme de 8-division en facteurs irréductibles sur \mathbb{Q} est donnée par :

$$\Psi_8(x) = 8(x - 15)(x + 57)(x^2 - 66x - 531)(x^2 + 6x + 981)f_4^{(1)}f_4^{(2)}h_{16},$$

où $f_4^{(1)}, f_4^{(2)}$ et h_{16} sont des polynômes de degré $\deg(f_4^{(1)}) = \deg(f_4^{(2)}) = 4$ et $\deg(h_{16}) = 16$. Un calcul simple montre que les points d'abscisse $x(P) = 15$ sont d'ordre 4 sur $C(\mathbb{Q})$ et les points d'abscisse $x(P) = -57$ sont d'ordre 4 sur $C(\mathbb{Q}(\sqrt{-15}))$. Si $K = \mathbb{Q}(\sqrt{5})$, $\theta_1 \in K$ est tel que $\theta_1^2 - 66\theta_1 - 531 = 0$, alors les points tels que $x(P) = \theta_1$ sont d'ordre 8 sur $C(K)$. Si $K = \mathbb{Q}(\sqrt{-3})$ et θ_2 est tel que $\theta_2^2 + 6\theta_2 + 981 = 0$, alors les points tels que $x(P) = \theta_2$ sont d'ordre 8 sur $C(K)$.

La factorisation sur \mathbb{Q} en facteurs irréductibles du polynôme :

$$\frac{\Psi_{16}(x)}{\Psi_8(x)} = 2f_4^{(3)}f_4^{(4)}g_{16}^{(1)}g_{16}^{(2)}h_{64}^{(1)},$$

avec $f_i^{(j)}, g_i^{(k)}$ et $h_i^{(l)}$ de degré i , implique qu'on ne peut pas obtenir des points d'ordre 16 si l'on se restreint à des extensions quadratiques. Maintenant, pour obtenir la 2-torsion complète, il faut et il suffit que f se scinde complètement dans K . Comme on a :

$$\Psi_2(x) = f(x) = (x + 21)(x^2 - 21x + 414),$$

il en résulte que $C(K) \supset C[2]$ si et seulement si $K = \mathbb{Q}(\sqrt{-15})$. On montre de plus que si $K = \mathbb{Q}(\sqrt{-15})$ alors $\text{Tors}(X_1(15), K) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ puisque le polynôme de 4-division ne se scinde pas complètement sur K . \square

Exemple 2.3. — La table 2.3 montre les structures de groupe de la courbe elliptique $X_1(15)$ sur $K = \mathbb{Q}(\sqrt{d})$ avec $|d| \leq 10$.

2.5.5. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/16\mathbb{Z}$. — Soit $P = (0, 0)$ tel que $\text{ord}(P) \notin \{2, 4, 8\}$ (voir 2.4.3 et 2.4.7). L'égalité $[8]P_0 = [-8]P_0$, sur la forme normale de Tate $E_{b,c}$

d	$\mathbb{Q}(\sqrt{d})$	$X_1(15)(\mathbb{Q}(\sqrt{d}))$	Point d'ordre infini
-10	$\theta^2 + 10 = 0$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}$	$(-\frac{13}{4}, -\frac{3}{2}\theta + \frac{9}{8})$
-7	$\theta^2 + 7 = 0$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}$	$(-\frac{1}{8}\theta - \frac{5}{8}, \frac{1}{16}\theta + \frac{5}{16})$
-6	$\theta^2 + 6 = 0$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}$	$(-\frac{5}{4}, -\frac{1}{4}\theta + \frac{1}{8})$
-5	$\theta^2 + 5 = 0$	$\mathbb{Z}/4\mathbb{Z}$	-
-3	$\theta^2 + 3 = 0$	$\mathbb{Z}/8\mathbb{Z}$	-
-2	$\theta^2 + 5 = 0$	$\mathbb{Z}/4\mathbb{Z}$	-
-1	$\theta^2 + 1 = 0$	$\mathbb{Z}/4\mathbb{Z}$	-
2	$\theta^2 - 2 = 0$	$\mathbb{Z}/4\mathbb{Z}$	-
3	$\theta^2 - 3 = 0$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}$	$(-\frac{1}{2}, -\frac{1}{4}\theta - \frac{1}{4})$
5	$\theta^2 - 5 = 0$	$\mathbb{Z}/8\mathbb{Z}$	-
6	$\theta^2 - 6 = 0$	$\mathbb{Z}/4\mathbb{Z}$	-
7	$\theta^2 - 7 = 0$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}$	$(\frac{3}{4}, \frac{1}{2}\theta - \frac{7}{8})$
10	$\theta^2 - 10 = 0$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}$	$(-\frac{3}{4}, \frac{1}{8}\theta - \frac{1}{8})$

TAB. 2.3. $X_1(15)(\mathbb{Q}(\sqrt{d}))$, $-10 \leq d \leq 10$.

équivalent alors à :

$$\begin{aligned}
\mathcal{U}_{b,c} : & (b-1)c^{12} + 3bc^{11} + (4b^2 + 10b)c^{10} \\
& + (20b^2 + 6b)c^9 + (10b^3 + 15b^2 + 3b)c^8 + (10b^3 + 14b^2 + b)c^7 \\
& + (30b^3 + 7b^2)c^6 + (40b^4 + 22b^3)c^5 + (b^6 + 35b^5 + 40b^4)c^4 \\
& + (18b^6 + 45b^5)c^3 + (4b^7 + 31b^6)c^2 + 12b^7c + 2b^8 = 0. \quad (2.48)
\end{aligned}$$

En utilisant l'algorithme de van Hoeij [vH95], une transformation birationnelle ramène à la forme minimale :

$$X_1(16) : s^2 = t(t^2 + 1)(t^2 + 2t - 1).$$

avec a et b, fonctions de s et de t :

$$\begin{cases} a = 1 - c = \frac{(t-1)(t^4+2t^3+6t-1)}{(t+1)^5(t^2+2t-1)}s + \frac{t^5+t^4+14t^3+6t^2+9t+1}{(t+1)^5}, \\ b = \frac{(t-1)^3(3t^4+8t^3-2t^2+8t-1)}{(t+1)^8(t^2+2t-1)}s + \frac{t(t-1)^3(t^2+1)(t^4+8t^3+10t^2-8t+5)}{(t+1)^8(t^2+2t-1)} \end{cases} \quad (2.49)$$

La forme générale des courbes elliptiques avec un point d'ordre 16 est :

$$\mathcal{E}_P^{(16)} : y^2 + axy + by = x^3 + bx^2.$$

avec a, b donnés par (2.49), $P = (t, s) \in X_1(16)$ et

$$t(t-1)(t+1)(t^2+1)(t^2-2t-1)(t^2+2t-1) \neq 0.$$

Le point $P_0 = (0, 0)$ est un point d'ordre 16.

Pour une forme sans dénominateur, on pourra faire le changement de variable

$$(x, y) \mapsto \left(\frac{x}{(t+1)^{10}(t^2+2t-1)^2}, \frac{y}{(t+1)^{15}(t^2+2t-1)^3} \right)$$

Théorème 2.6. — Soit $K = \mathbb{Q}(\sqrt{10})$, alors il existe une courbe elliptique définie sur K , de rang 1 et dont le sous-groupe de torsion est isomorphe à $\mathbb{Z}/16\mathbb{Z}$:

$$\text{Br}(\mathbb{Z}/16\mathbb{Z}, K) \geq 1.$$

Démonstration. — Soit θ tel que $\theta^2 - 10 = 0$ et soit la courbe elliptique :

$$E : y^2 + (39\theta + 121)xy - (1107\theta + 3510)y = x^3 - (1107\theta + 3510)x^2$$

Un calcul de 2-descente [S**imb**] permet d'obtenir que $\text{rang}(E, \mathbb{Q}(\sqrt{10})) \leq 1$, et puisque le point

$$P = (-9\theta - 24, 2970\theta + 9402),$$

n'étant pas de 16-torsion, il est d'ordre infini. Le rang vaut donc exactement 1. On vérifie facilement que le point $(0, 0)$ est d'ordre 16. \square

2.5.6. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/18\mathbb{Z}$. — Soient $b \neq 0$ et $P = (0, 0)$, supposons que $\text{ord}(P) \notin \{2, 3, 6, 9\}$ sur $E_{b,c}$ (voir 2.4.5 et 2.4.8. L'égalité $[9]P_0 = [-9]P_0$ dans la forme normale de Tate $E_{b,c}$ équivaut alors à :

$$\begin{aligned} \mathcal{U}_{b,c} : & -c^{13} + c^{12} + (-b^3 + 7b - 1)c^{11} + (-8b^3 - 11b)c^{10} \\ & + (-7b^4 - 37b^3 - 55b^2)c^9 + (-50b^4 - 128b^3)c^8 + (-18b^5 - 143b^4 + 8b^3)c^7 \\ & + (b^6 - 67b^5 + 41b^4 + b^3)c^6 + (-b^6 + 84b^5 + 6b^4)c^5 \\ & + (6b^7 + 86b^6 + 15b^5)c^4 + (44b^7 + 20b^6)c^3 + (9b^8 + 15b^7)c^2 + 6b^8c + b^9 = 0. \end{aligned} \tag{2.50}$$

Il s'agit d'une courbe de genre 2. En utilisant l'algorithme de van Hoeij [v**H02**], on montre qu'une transformation birationnelle permet de réécrire $\mathcal{U}_{b,c}$ donné par (2.50) par la forme plus simple :

$$X_1(18) : s^2 = t^6 + 2t^5 + 5t^4 + 10t^3 + 10t^2 + 4t + 1$$

avec :

$$\begin{cases} a = 1 - c = \frac{-t^2 - 3t - 2}{2t^3(t^3 - 3t - 1)}s - \frac{(-2t^5 + t^4 + 10t^3 + 11t^2 + 11t + 5)}{2t^2(t^3 - 3t - 1)}, \\ b = -\frac{(t+1)(t^2+t+1)(t^4+2t^3-t+1)}{2t^5(t^3-3t-1)^2}s - \frac{(t+1)(t^2+t+1)(t^7+3t^6+4t^5+6t^4+4t^3-t^2-t-1)}{2t^5(t^3-3t-1)^2} \end{cases} \quad (2.51)$$

La forme générale des courbes elliptiques avec un point d'ordre 18 est finalement donnée par :

$$\mathcal{E}_P^{(18)} : y^2 + axy + by = x^3 + bx^2,$$

avec a, b donnés par (2.51), $P = (t, s) \in X_1(18)(K)$ et

$$t(t+1)(t^2+t+1)(t^3-3t-1) \neq 0.$$

Le point $P_0 = (0, 0)$ est un point d'ordre 18. Pour une forme sans dénominateur, on pourra faire le changement de variable :

$$(x, y) \mapsto \left(\frac{x}{4t^6(t^3 - 3t - 1)^4}, \frac{y}{8t^9(t^3 - 3t - 1)^6} \right)$$

2.5.7. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$. — D'après la proposition 2.1, le genre de la courbe modulaire $X_1(2, 10)$ est 1. Notre premier résultat est le suivant :

Proposition 2.2. — *La courbe modulaire $X_1(2, 10)$ est donnée par l'équation :*

$$X_1(2, 10) : s^2 = t^3 + t^2 - t.$$

Démonstration. — Considérons la forme des courbes avec un point d'ordre 10 (voir 2.4.9) :

$$\mathcal{E}^{(10)} : y^2 + \frac{t^3 - 2t^2 - 4t + 4}{t^2 - 6t + 4}xy - \frac{(t-1)(t-2)t^3}{(t^2 - 6t + 4)^2}y = x^3 - \frac{(t-1)(t-2)t^3}{(t^2 - 6t + 4)^2}x^2.$$

Cette courbe est birationnellement équivalente à :

$$\begin{aligned} \mathcal{E}^{(10)} : y^2 = x f_t(x) = x^3 \\ + \left(\frac{-t^6 + 8t^5 - 20t^4 + 20t^3 - 16t + 8}{2(t^2 - 6t + 4)^2} \right) x^2 + \left(\frac{t^5(t-2)^5}{16(t^2 - 6t + 4)^3} \right) x. \end{aligned} \quad (2.52)$$

Le discriminant de $f_t(x)$ est donné par :

$$\Delta(f_t(x)) = \frac{2^4(t-1)^5(t^2-t-1)}{(t^2-6t+4)^4}$$

et doit être un carré pour que $E[2] \subset E(K)$. Nous considérons la courbe :

$$U_{s,t} : s^2 - (t-1)(t^2-t-1) = 0.$$

Le genre de $U_{s,t}$ est 1 et le changement de variable :

$$(s, t) \mapsto (s, t + 1)$$

donne la forme minimale de la courbe $X_1(2, 10) : s^2 = t^3 + t^2 - t$. \square

La courbe $X_1(2, 10)$ est appelée 20a2 dans la table de Cremona [Cre97].

La forme des courbes elliptiques avec un sous-groupe de torsion isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ est donnée par :

$$\mathcal{E}_P^{(2,10)} : y^2 + \frac{t^3 + t^2 - 4t + 1}{t^2 - 4t - 1}xy - \frac{t(t-1)(t+1)^3}{(t^2 - 4t - 1)^2}y = x^3 - \frac{t(t-1)(t+1)^3}{(t^2 - 4t - 1)^2}x^2,$$

où $P = (t, s) \in X_1(2, 10)$. Pour obtenir une forme plus simple, faisons le changement de variable :

$$(x, y) \mapsto \left(\frac{x}{(t^2 - 4t - 1)^2}, \frac{y}{(t^2 - 4t - 1)^3} \right)$$

où $P = (t, s) \in X_1(2, 10)$. On obtient alors la forme :

$$\begin{aligned} \mathcal{E}_P^{(2,10)} : y^2 + (t^3 + t^2 - 4t + 1)xy \\ - t(t-1)(t+1)^3(t^2 - 4t - 1)y = x^3 - t(t-1)(t+1)^3x^2. \end{aligned} \quad (2.53)$$

où $P = (t, s) \in X_1(2, 10)$ est tel que le discriminant :

$$\Delta_{\mathcal{E}(2,10)} = t^5(t^2 - 1)^{10}(t^2 - 4t - 1)^2(t^2 + t - 1)^2 \neq 0.$$

Les points

$$P_0 = (0, 0) \text{ et } Q = \left((-2t + s - 1)(s + 1)t, (s + 1)^2((s + 1)t^2 - 2t - 2s^2) \right),$$

sont d'ordre 10 et 2 respectivement, et on a :

$$\langle Q, P_0 \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}.$$

La courbe modulaire $X_1(2, 10)$ est de rang 0 sur \mathbb{Q} et admet exactement 6 points rationnels sur \mathbb{Q} (voir table de Cremona pour la courbe 20a2) :

$$X_1(2, 10)(\mathbb{Q}) = \{\mathcal{O}, (-1, 1), (1, -1), (0, 0), (1, 1), (-1, -1)\}$$

Ces points induisent des courbes singulières dans la paramétrisation (2.53) ci-dessus.

Lemme 2.4. — Soit K une extension quadratique de \mathbb{Q} , alors :

$$\text{Tors}(X_1(2, 10), K) \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, & \text{si } K = \mathbb{Q}(\sqrt{5}) \\ \mathbb{Z}/6\mathbb{Z}, & \text{sinon} \end{cases}$$

Démonstration. — Soit K un corps de nombres quadratique. Nous utilisons le modèle de Weierstrass réduite de $X_1(2, 10)$:

$$C : y^2 = f(x) = x^3 - 1728x + 19008$$

On observe d'abord que :

$$\text{Tors}(X_1(2, 10), K) \supseteq \text{Tors}(X_1(2, 10), \mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}.$$

Par le théorème 2.2, les seules structures possibles pour $\text{Tors}(X_1(2, 10), K)$ sont : $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/18\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

Pour obtenir la 2-torsion complète, il faut que f se scinde complètement sur K . Comme on a :

$$\Psi_2(x) = f(x) = (x - 12)(x^2 + 12x - 1584),$$

il faut donc que $K \supseteq \mathbb{Q}(\sqrt{5})$. On a ensuite la factorisation sur \mathbb{Q} du polynôme :

$$\frac{\Psi_4(x)}{\Psi_2(x)} = (x^2 - 24x + 1440)f_4^{(1)},$$

où $f_4^{(1)}$ est un polynôme irréductible de degré 4. Les points dont l'abscisse $x(P) = \theta$ avec $\theta^2 - 24\theta + 1440 = 0$ n'ont pas leurs coordonnées dans $K = \mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{-1})$. Il ne peut donc y avoir de point d'ordre 4.

La factorisation du polynôme de 3-division de C en facteurs irréductibles sur \mathbb{Q} est donnée par

$$\Psi_3(x) = (x - 48)(x^3 + 48x^2 - 1152x + 20736).$$

Cela implique que quel que soit K , on ne peut avoir la 3-torsion complète. Enfin, la factorisation du polynôme de 9-division est donnée par

$$\Psi_9(x) = f_9 f_{27} \Psi_3(x),$$

où f_9 et f_{27} sont de polynômes irréductibles sur \mathbb{Q} , de degré 9 et 27 respectivement. Il ne peut donc y avoir de point d'ordre 9 sur K . \square

Exemple 2.4. — La table 2.4 montre les structures de groupe de la courbe elliptique $X_1(2, 10)$ sur $K = \mathbb{Q}(\sqrt{d})$ avec $|d| \leq 10$.

d	$\mathbb{Q}(\sqrt{d})$	$X_1(2, 10)(\mathbb{Q}(\sqrt{d}))$	Point d'ordre infini
-10	$\theta^2 + 10 = 0$	$\mathbb{Z}/6\mathbb{Z}$	-
-7	$\theta^2 + 7 = 0$	$\mathbb{Z}/6\mathbb{Z}$	-
-6	$\theta^2 + 6 = 0$	$\mathbb{Z}/6\mathbb{Z}$	-
-5	$\theta^2 + 5 = 0$	$\mathbb{Z}/6\mathbb{Z}$	-
-3	$\theta^2 + 3 = 0$	$\mathbb{Z}/6\mathbb{Z}$	-
-2	$\theta^2 + 5 = 0$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}$	$(-2, -\theta)$
-1	$\theta^2 + 1 = 0$	$\mathbb{Z}/6\mathbb{Z}$	-
2	$\theta^2 - 2 = 0$	$\mathbb{Z}/6\mathbb{Z}$	-
3	$\theta^2 - 3 = 0$	$\mathbb{Z}/6\mathbb{Z}$	-
5	$\theta^2 - 5 = 0$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	-
6	$\theta^2 - 6 = 0$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}$	$(-2\theta + 7, 8\theta - 23)$
7	$\theta^2 - 7 = 0$	$\mathbb{Z}/6\mathbb{Z}$	-
10	$\theta^2 - 10 = 0$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}$	$(2, -\theta)$

TAB. 2.4. $X_1(2, 10)(\mathbb{Q}(\sqrt{d}))$, $-10 \leq d \leq 10$.

2.5.8. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$. — Considérons la forme des courbes avec un point d'ordre 12 :

$$\begin{aligned}
\mathcal{E}^{(12)} : y^2 + \frac{6t^4 - 8t^3 + 2t^2 + 2t - 1}{(t-1)^3}xy \\
+ \frac{-12t^6 + 30t^5 - 34t^4 + 21t^3 - 7t^2 + t}{(t-1)^4}y \\
= x^3 + \frac{-12t^6 + 30t^5 - 34t^4 + 21t^3 - 7t^2 + t}{(t-1)^4}x^2. \quad (2.54)
\end{aligned}$$

Par une transformation birationnelle, on obtient la forme équivalente :

$$\begin{aligned}
\mathcal{E}^{(12)} : y^2 = x f_t(x) \\
= x^3 + \frac{24t^8 - 96t^7 + 216t^6 - 312t^5 + 288t^4 - 168t^3 + 60t^2 - 12t + 1}{4t^6 - 24t^5 + 60t^4 - 80t^3 + 60t^2 - 24t + 4}x^2 \\
+ \frac{9t^{10} - 18t^9 + 15t^8 - 6t^7 + t^6}{t^6 - 6t^5 + 15t^4 - 20t^3 + 15t^2 - 6t + 1}x. \quad (2.55)
\end{aligned}$$

Le discriminant de $f_t(x)$ est donné par :

$$\Delta(f_t(x)) = \frac{(2t-1)^6(2t^2-2t+1)^3(6t^2-6t+1)}{16(t-1)^{12}}.$$

Pour que $E[2] \subset E(K)$, nous imposons que ce discriminant soit un carré dans K , ce qui nous amène à considérer la courbe :

$$\Gamma : s^2 = (2t^2 - 2t + 1)(6t^2 - 6t + 1). \quad (2.56)$$

La courbe modulaire $X_1(2, 12)$ est appelée $24a4$ dans la table [Cre97].

Nous trouvons la forme simplifiée en utilisant la même méthode que dans [AM93] :

$$\Gamma : s^2 = 12t^4 - 24t^3 + 20t^2 - 8t + 1.$$

Le point $(0, 1)$ est sur Γ . En posant

$$t = \left(T + \frac{1}{2}\right)^{-1} \text{ et } s = St^2,$$

on trouve que Γ est birationnellement équivalente à :

$$\Gamma' : S^2 = T^4 - 4T^2 - 8T - 4,$$

qui ensuite est birationnellement équivalente à :

$$y^2 = x^3 + \frac{2}{3}x + \frac{7}{27},$$

par le changement de variable :

$$T = \frac{y+1}{x-\frac{1}{3}} \text{ et } S = -T^2 + 2x + \frac{2}{3}.$$

En faisant le changement de variable :

$$(x, y) \mapsto \left(x - \frac{1}{3}, y\right),$$

On obtient enfin la forme minimale $\Gamma'' : y^2 = x^3 - x^2 + x$.

Proposition 2.3. — *La courbe modulaire $X_1(2, 12)$ est donnée par l'équation :*

$$X_1(2, 12) : s^2 = t^3 - t^2 + t.$$

Démonstration. — voir la discussion ci-dessus. □

Bien qu'il y ait une correspondance entre les points rationnels de $X_1(2, 12)$ et ceux de la courbe Γ , par souci de commodité, nous allons utiliser la paramétrisation des courbes elliptiques avec 2-torsion complète et un point d'ordre 12 par la courbe Γ .

La forme des courbes elliptiques avec un sous-groupe de torsion isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ est donnée par :

$$\begin{aligned}
\mathcal{E}^{(2,12)} : y^2 + (6t^4 - 8t^3 + 2t^2 + 2t - 1)xy \\
+ (-12t^6 + 30t^5 - 34t^4 + 21t^3 - 7t^2 + t)(t-1)^5y \\
= x^3 + (-12t^6 + 30t^5 - 34t^4 + 21t^3 - 7t^2 + t)((t-1)^2x^2). \quad (2.57)
\end{aligned}$$

avec $P = (t, s) \in \Gamma(K)$ est tel que le discriminant de $\mathcal{E}^{(2,12)}$ donné par :

$$\Delta_{\mathcal{E}^{(12)}} = t^{12}(t-1)^{12}(2t-1)^6(2t^2-2t+1)^3(3t^2-3t+1)^4(6t^2-6t+1) \neq 0.$$

Les points $P_0 = (0, 0)$ et

$$\begin{aligned}
Q = \left(\frac{1}{72}((-36s^2 - 12s + 12)t^3 + (42s^2 + 18s - 22)t^2 \right. \\
\left. + (-12s^3 - 12s^2 - 12s + 16)t + (6s^3 - 4s^2 + 3s - 5)), \right. \\
\left. \frac{1}{864}((144s^4 - 108s^3 + 72s^2 - 12s + 16)t^3 + (-180s^4 + 210s^3 - 120s^2 + 26s - 28)t^2 \right. \\
\left. + (36s^5 + 96s^4 - 132s^3 + 88s^2 - 20s + 20)t + (6s^5 - 21s^4 + 41s^3 - 27s^2 + 7s - 6)) \right),
\end{aligned}$$

sont d'ordre 12 et 2 respectivement, et on a :

$$\langle Q, P_0 \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}.$$

La courbe modulaire $X_1(2, 12)$ est de rang 0 sur \mathbb{Q} et admet exactement 4 points rationnels sur \mathbb{Q} . Clairement $X_1(2, 12)(\mathbb{Q}) = \text{Tors}(X_1(2, 12), \mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$ et de plus ces points induisent des courbes singulières dans la paramétrisation (2.57) ci-dessus :

$$X_1(2, 12)(\mathbb{Q}) = \{\mathcal{O}, (1, 1), (0, 0), (1, -1)\}$$

Lemme 2.5. — Soit K une extension quadratique de \mathbb{Q} , alors :

$$\text{Tors}(X_1(2, 12), K) \simeq \begin{cases} \mathbb{Z}/8\mathbb{Z}, & \text{si } K \in \{\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{3})\} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, & \text{si } K = \mathbb{Q}(\sqrt{-3}) \\ \mathbb{Z}/4\mathbb{Z}, & \text{sinon} \end{cases}$$

Démonstration. — Preuve : Soit K un corps de nombres quadratique. Nous utilisons le modèle de Weierstrass simplifié de $X_1(2, 12)$:

$$C : y^2 = f(x) = x^3 + 864x + 12096$$

On observe d'abord que

$$\text{Tors}(X_1(2, 12), K) \supseteq \text{Tors}(X_1(2, 12), \mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}.$$

Par le théorème 2.2, les seuls sous-groupes de torsion possibles sont : $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Pour obtenir la 2-torsion complète, il faut et il suffit que

$$\Psi_2(x) = f(x) = (x + 12)(x^2 - 12x + 1008)$$

se scinde complètement dans K , c'est-à-dire $K = \mathbb{Q}(\sqrt{-3})$.

La courbe C ne peut avoir un point d'ordre 3 puisque le polynôme de 3-division

$$\Psi_3(x) = x^4 + 1728x^2 + 48384x - 248832,$$

est irréductible sur \mathbb{Q} et donc ne peut posséder de racines sur K .

La factorisation du polynôme de 4-division en facteurs irréductibles sur \mathbb{Q} est donnée par :

$$\Psi_4(x) = (x - 24)(x + 48)f_4\Psi_2(x)$$

où f_4 est un polynôme irréductible de degré 4 sur \mathbb{Q} . Les points d'abscisse $x(P) = 24$ sont dans $C(\mathbb{Q})$ et les points d'abscisse $x(P) = -48$ sont dans $C(\mathbb{Q}(\sqrt{-3}))[4] \setminus C(\mathbb{Q})[4]$. Comme $\Psi_4(x)$ possède un facteur irréductible de degré 4, on ne peut donc avoir la 4-torsion complète sur K .

La factorisation du polynôme de 8-division est :

$$\Psi_8(x) = (x^2 - 120x - 288)(x^2 + 24x + 1440)f_4^{(2)}f_16^{(2)}\Psi_4(C),$$

où les $f_i^{(j)}$ sont de degré i et sont irréductibles sur \mathbb{Q} . Soit $K = \mathbb{Q}(\sqrt{3})$ et θ_1 tel que $\theta_1^2 - 120\theta_1 - 288 = 0$, alors les points d'abscisse $x(P) = \theta_1$ sont d'ordre 8 sur $C(K)$. De même, si $K = \mathbb{Q}(\sqrt{-1})$ et θ_2 est tel que $\theta_2^2 + 24\theta_2 + 1440 = 0$, alors les points d'abscisse $x(P) = \theta_2$ sont d'ordre 8 sur $C(K)$.

La factorisation sur \mathbb{Q} du polynôme de 16-division est donnée par :

$$\Psi_{16}(x) = f_8^{(3)}f_8^{(4)}f_8^{(5)}f_8^{(6)}f_{64}^{(1)}\Psi_8(x)$$

où les $f_i^{(j)}$ sont des polynômes irréductibles de degré i . Ceci montre qu'il ne peut y avoir de point d'ordre 16 sur K . \square

Exemple 2.5. — La table 2.5 montre les structures de groupe de la courbe elliptique $X_1(2, 12)$ sur $K = \mathbb{Q}(\sqrt{d})$ avec $|d| \leq 10$.

2.5.9. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. — Dans [Kub76], Kubert a proposé une paramétrisation pour cette structure comme suit :

$$C : y^2 = x^3 + ax^2 + bx + c, \text{ avec}$$

$$a = \frac{3}{4}(r + s), b = \frac{1}{2}(rs + t), c = \frac{1}{4}rt, r = \frac{2t}{s - v}, t = \frac{v^2 + 3s^2}{12}$$

d	$\mathbb{Q}(\sqrt{d})$	$X_1(2, 12)/\mathbb{Q}(\sqrt{d})$	Point d'ordre infini
-10	$\theta^2 + 10 = 0$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}$	$(\frac{1608\theta+3049}{5929}, \frac{20904\theta+39637}{456533})$
-7	$\theta^2 + 7 = 0$	$\mathbb{Z}/4\mathbb{Z}$	-
-6	$\theta^2 + 6 = 0$	$\mathbb{Z}/4\mathbb{Z}$	-
-5	$\theta^2 + 5 = 0$	$\mathbb{Z}/4\mathbb{Z}$	-
-3	$\theta^2 + 3 = 0$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	-
-2	$\theta^2 + 5 = 0$	$\mathbb{Z}/4\mathbb{Z}$	-
-1	$\theta^2 + 1 = 0$	$\mathbb{Z}/8\mathbb{Z}$	-
2	$\theta^2 - 2 = 0$	$\mathbb{Z}/4\mathbb{Z}$	-
3	$\theta^2 - 3 = 0$	$\mathbb{Z}/8\mathbb{Z}$	-
5	$\theta^2 - 5 = 0$	$\mathbb{Z}/4\mathbb{Z}$	-
6	$\theta^2 - 6 = 0$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}$	$(2, -\theta)$
7	$\theta^2 - 7 = 0$	$\mathbb{Z}/4\mathbb{Z}$	-
10	$\theta^2 - 10 = 0$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}$	$(\frac{5}{8}, \frac{7}{32}\theta)$

TAB. 2.5. $X_1(2, 12)(\mathbb{Q}(\sqrt{d}))$, $-10 \leq d \leq 10$.

Nous proposons ici une autre approche. Rappelons que la forme d'une courbe avec 3-torsion est donnée par :

$$\mathcal{E}^{(3)} : y^2 + sxy + ty = x^3 .$$

Grâce au changement de variable

$$(x, y) \mapsto \left(x - \frac{s^2}{12}, y - \frac{sx + t}{2} \right),$$

on obtient

$$C^{(3)} : y^2 = x^3 + \left(-\frac{1}{48}s^4 + 12ts\right)x + \frac{1}{864}s^6 - \frac{1}{24}ts^3 + \frac{1}{4}t^2 .$$

On impose maintenant $E[3] \in E[K]$. En factorisant complètement le polynôme de 3-division associé

$$\Psi_3(x) = \frac{3}{576} \left(x - \frac{s^2}{12}\right) \Phi_{3,s}(x, t) = 0 ,$$

on est ramené à résoudre :

$$C_3 : \Phi_{3,s}(x, t) = 576x^3 + 48s^2x^2 + (576st - 20s^4)x + (576t^2 - 48s^3t + s^6) .$$

En considérant s comme un paramètre, l'algorithme de van Hoeij [**vH97**] permet de trouver :

$$t = \frac{4v(144s^2 - 24vs^4 + 432vs + 432v^2 + v^2s^6 - 36v^2s^3)}{(vs^2 - 12)^3},$$

$$x = -\frac{-48v^2s^3 + 576v^2 + v^2s^6 - 24vs^4 + 576vs + 144s^2}{4(vs^2 - 12)^2},$$

où $v \in K$ est tel que $vs^2 - 12 \neq 0$. Avec le changement de variable :

$$(x, y) \mapsto \left(\frac{x}{(vs^2 - 12)^2}, \frac{y}{(vs^2 - 12)^3} \right),$$

on obtient la forme générale :

$$\begin{aligned} \mathcal{E}^{(3,3)} : y^2 + s(vs^2 - 12)xy \\ + 4v(144s^2 - 24vs^4 + 432vs + 432v^2 + v^2s^6 - 36v^2s^3)y = x^3, \end{aligned} \quad (2.58)$$

où $v, s \in K$ sont tels que le discriminant de $\mathcal{E}^{(3,3)}$:

$$\begin{aligned} \Delta_{\mathcal{E}^{(3,3)}} = 2^6 v^3 (vs^3 - 36v - 12s)^3 \\ (144s^2 - 24vs^4 + 432vs + 432v^2 + v^2s^6 - 36v^2s^3)^3 \end{aligned}$$

est non nul. Les points

$$P_0 = (0, 0) \text{ et}$$

$$Q = \left(-\frac{-48v^2s^3 + 576v^2 + v^2s^6 - 24vs^4 + 576vs + 144s^2}{4}, \right. \\ \left. \frac{(\sqrt{-3} + 3)(vs^3 + (-6\sqrt{-3} - 18)v - 12s)^2 (vs^3 + (6\sqrt{-3} - 18)v - 12s)}{18v^3} \right)$$

sont d'ordre 3, et engendrent un sous-groupe isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Théorème 2.7. — Soit $K = \mathbb{Q}(\sqrt{-3})$, alors il existe une courbe elliptique définie sur K , de rang 2 et avec un sous-groupe de torsion isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$:

$$\text{Br}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, K) \geq 2$$

Démonstration. — Preuve : En substituant v par -3 et s par 1 dans l'équation (2.58), nous obtenons la courbe elliptique :

$$E : y^2 - 15xy - 29916y = x^3.$$

En utilisant le programme [Sima], nous trouvons que le rang vaut 2. Les points

$$P_1 = (-180, -13392) \\ \text{et } P_2 = \left(-\frac{14958}{49}, \frac{3941433}{343} \right),$$

sont d'ordre infini et indépendants. De plus, les points :

$$(0, 0) \text{ et } \left(-831, \frac{25761}{2}\sqrt{-3} + \frac{17451}{2} \right),$$

sont d'ordre 3 et engendrent un sous-groupe isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. □

2.5.10. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. — Le principe pour le cas $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ est le même que précédemment. Rappelons que la forme des courbes elliptiques avec un point d'ordre 6 est

$$\mathcal{E}^{(6)} : y^2 + (1-t)xy - t(t+1)y = x^3 - t(t+1)x^2.$$

Cherchons d'abord une forme du type $y^2 = x^3 + A(s, t)x + B(s, t)$. Cela s'obtient en faisant le changement de variable :

$$(x, y) \mapsto \left(x + \frac{3}{4}t^2 + \frac{3}{2}t - \frac{1}{4}, y - \frac{(1-t)x - t(t+1)}{2} \right).$$

On obtient alors l'équation :

$$\begin{aligned} C^{(6)} : y^2 = x^3 + & \left(-\frac{3}{16}t^4 - \frac{1}{4}t^3 - \frac{5}{8}t^2 - \frac{1}{4}t - \frac{1}{48} \right)x \\ & + \left(-\frac{1}{32}t^6 - \frac{1}{16}t^5 + \frac{5}{32}t^4 + \frac{5}{24}t^3 + \frac{11}{96}t^2 + \frac{1}{48}t + \frac{1}{864} \right). \end{aligned} \quad (2.59)$$

Le polynôme de 3-division de cette courbe est donné par :

$$\Psi_3(x, t) = \frac{3}{576} \left(x - \frac{3}{4}t^2 - \frac{1}{2}t - \frac{1}{12} \right) \Phi_3(x, t), \text{ avec :}$$

$$\begin{aligned} \Phi_3(x, t) = & 576x^3 + (432t^2 + 288t + 48)x^2 \\ & + (108t^4 + 144t^3 - 504t^2 - 240t - 20)x \\ & + (9t^6 + 18t^5 + 63t^4 + 60t^3 + 87t^2 + 18t + 1). \end{aligned} \quad (2.60)$$

La courbe $C : \Phi_3(x, t) = 0$ est de genre 0 et la paramétrisation de cette courbe, donnée par l'algorithme [vH97], induit que t doit être de la forme :

$$t = -\frac{(3v-2)(3v^2+4)}{9(v-2)^3} \text{ où } v \in K \setminus \{2\}.$$

On obtient alors la forme générale

$$\begin{aligned} \mathcal{E}^{(3,6)} : y^2 + \frac{2(9v^3 - 30v^2 + 60v - 40)}{9(v-2)^3}xy \\ - \frac{16(3v-2)(3v^2+4)(3v^2-6v+4)}{81(v-2)^6}y \\ = x^3 - \frac{16(3v-2)(3v^2+4)(3v^2-6v+4)}{81(v-2)^6}x^2. \end{aligned}$$

Le changement de variable suivant :

$$(x, y) \mapsto \left(\frac{x}{81(v-2)^6}, \frac{y}{729(v-2)^9} \right),$$

nous ramène à la forme plus simple

$$\begin{aligned} \mathcal{E}^{(3,6)} : y^2 + 2(9v^3 - 30v^2 + 60v - 40)xy \\ - 144(3v-2)(3v^2+4)(3v^2-6v+4)(v-2)^3y \\ = x^3 - 16(3v-2)(3v^2+4)(3v^2-6v+4)x^2, \quad (2.61) \end{aligned}$$

où $v \in K$ est tel que le discriminant de $\mathcal{E}^{(3,6)}$ donné par :

$$\Delta_{\mathcal{E}^{(3,6)}} = 2^{15}3^6v^3(v-2)^6(3v-2)^6(3v^2+4)^6(3v^2-6v+4)^3.$$

est non nul. Les points

$$P_0 = (0, 0) \text{ et}$$

$$\begin{aligned} Q = \left(-12(v-2)^2(3v^2-16v+4)(3v^2+4), \right. \\ \left. \left(324\sqrt{-3} + 972 \right) (v-2)^2 \left(v - \frac{2}{3}\sqrt{-3} \right)^2 \left(v - \frac{1}{3}\sqrt{-3} - 1 \right) \right. \\ \left. \left(v + \frac{1}{3}\sqrt{-3} - 1 \right)^2 \left(v + \frac{2}{3}\sqrt{-3} \right)^2 \right), \end{aligned}$$

sont d'ordre 6 et 3 respectivement, et engendrent un sous-groupe isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

Théorème 2.8. — Soit $K = \mathbb{Q}(\sqrt{-3})$, alors il existe une courbe elliptique définie sur K , de rang 3 et avec un sous-groupe de torsion isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$:

$$\text{Br}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, K) \geq 3.$$

Démonstration. — Substituons v par $-\frac{3}{2}$ dans l'équation (2.61), nous obtenons la courbe elliptique :

$$E : y^2 - \frac{1823}{4}xy - \frac{136325007}{16}y = x^3 + \frac{44161}{2}x^2.$$

En utilisant le programme de Simon [**Sima**], on trouve :

$$\text{rang}(E, \mathbb{Q}) = 1 \text{ et } \text{rang}(E^{(-3)}, \mathbb{Q}) = 2 .$$

Les points suivants :

$$\begin{aligned} & \left(\frac{7927256701}{6400}, \frac{873716268258379}{512000} \right) \\ & \left(-\frac{112359}{4}, \frac{3677661}{16}\theta - \frac{34252725}{16} \right) \\ & \left(-\frac{2570841}{16}, \frac{3718175643}{128}\theta - \frac{4141343115}{128} \right) \end{aligned}$$

sont d'ordre infini et indépendants. De plus, les points

$$P_0 = (0, 0) \text{ et}$$

$$Q = \left(-\frac{499359}{16}, -\frac{64417311}{128}\sqrt{-3} - \frac{365031429}{128} \right)$$

sont d'ordre 6 et 3 respectivement :

$$\langle Q, P_0 \rangle \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} .$$

□

2.5.11. Le cas $\text{Tors}(E, K) \supseteq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. — On commence par considérer la forme générale des courbes elliptiques dont le sous-groupe de torsion est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$:

$$\mathcal{E}^{(2,4)} : y^2 + xy - \left(t^2 - \frac{1}{16}\right)y = x^3 - \left(t^2 - \frac{1}{16}\right)x^2. \quad (2.62)$$

Notons

$$P_4 = (0, 0) \text{ et } P_2 = \left(\frac{1}{4}(4t - 1), \frac{1}{32}(4t - 1)^2 \right) .$$

Nous avons vu (section 2.4.12) que les points P_4 et P_2 sont d'ordre 4 et 2 respectivement, et de plus :

$$\langle P_2, P_4 \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} .$$

Pour obtenir la 4-torsion complète, il nous faut alors résoudre l'équation :

$$P_2 = [2]Q .$$

Lemme 2.6. — Soit E une courbe elliptique sur un corps K , définie par l'équation :

$$E : y^2 = (x - \alpha)(x - \beta)(x - \gamma),$$

où $\alpha, \beta, \gamma \in K$ et soit $P = (x_P, y_P) \in E(K)$, alors il existe un point $Q \in E(K)$ tel que $P = [2]Q$ si et seulement si il existe $u, v, z \in K$ avec

$$x_P - \alpha = u^2, x_P - \beta = v^2, x_P - \gamma = z^2.$$

Démonstration. — Voir par exemple [Kna92, p.85] ou [Cas91, Chapitre 15]. \square

Nous utilisons maintenant le modèle :

$$C : y^2 = \left(x - t^2 + \frac{1}{16}\right) \left(x - \frac{1}{2}t + \frac{1}{8}\right) \left(x + \frac{1}{2}t + \frac{1}{8}\right),$$

pour la surface elliptique $\mathcal{E}^{(2,4)}$. Le point $P_2 = \left(\frac{1}{2}t - \frac{1}{8}, 0\right)$ est d'ordre 2 sur la courbe C . Grâce au lemme 2.6, une condition nécessaire et suffisante pour que ce point soit le double d'un autre point Q est que $t = z^2$ et $(t - \frac{1}{4})^2 = -v^2$ avec $v, z \in K$.

Remarque 2.4. — La dernière condition signifie que -1 doit nécessairement être un carré dans le corps K , cela veut dire que le seul corps quadratique tel qu'il existe une courbe elliptique dont le sous-groupe de torsion est isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ est $\mathbb{Q}(\sqrt{-1})$ (voir le théorème 2.2).

La discussion ci-dessus permet de trouver la forme générale des courbes elliptiques avec une torsion isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$:

$$\mathcal{E}^{(4,4)} : y^2 + xy - \left(t^4 - \frac{1}{16}\right)y = x^3 - \left(t^4 - \frac{1}{16}\right)x^2, \quad (2.63)$$

où $t \in K$ est tel que le discriminant de $\mathcal{E}^{(4,4)}$:

$$\Delta_{\mathcal{E}^{(4,4)}} = \frac{1}{2^{12}} t^4 (2t - 1)^4 (2t + 1)^4 (4t^2 + 1)^4.$$

est non nulle. Les points

$$P = (0, 0) \text{ et}$$

$$Q = \left(-\frac{1}{8}(2t + 1)(4t^2 + 1), \sqrt{-1} \left(t + \frac{1}{2}\right)^2 \left(t - \frac{\sqrt{-1}}{2}\right)^2 \left(t + \frac{\sqrt{-1}}{2}\right)\right)$$

sont générateurs de la 4-torsion complète :

$$\langle P, Q \rangle \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

Théorème 2.9. — Soit $K = \mathbb{Q}(\sqrt{-1})$, alors il existe une courbe elliptique E définie sur K de rang 3 et telle que $\text{Tors}(E, K) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$:

$$\text{Br}(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, K) \geq 3.$$

Démonstration. — Substituons t par 11 dans l'équation (3.184), nous obtenons la courbe elliptique :

$$E : y^2 + xy - \frac{234255}{16}y = x^3 - \frac{234255}{16}x^2 .$$

En utilisant le programme de Simon [**Sima**], nous obtenons que $\text{rang}(E, \mathbb{Q}) = 1$ et $\text{rang}(E^{(-1)}, \mathbb{Q}) = 2$. Les points

$$\begin{aligned} P_1 &= \left(\frac{1699800809}{73984}, \frac{42124907328091}{20123648} \right), \\ P_2 &= \left(-\frac{424005}{784}, \frac{726647625\sqrt{-1}}{10976} + \frac{2975625}{392} \right), \\ P_3 &= \left(-\frac{203021}{72}, \frac{10057348\sqrt{-1}}{27} + \frac{2514337}{288} \right), \end{aligned}$$

sont indépendants sur $E(K)$ et de plus

$$\langle (0, 0) \rangle \times \left\langle \left(-\frac{11155}{8}, \frac{2822215\sqrt{-1}}{16} + \frac{256565}{32} \right) \right\rangle \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} .$$

□

CHAPITRE 3

LES FAMILLES DE COURBES ELLIPTIQUES DE GRAND RANG

Dans ce chapitre, nous cherchons à construire des familles de courbes elliptiques de grand rang, possédant une grande torsion. Dans un premier temps, nous ferons un survol rapide sur les résultats connus.

Ensuite nous développerons une nouvelle méthode pour obtenir de telles familles de courbes elliptiques. Nous donnerons ainsi explicitement de nombreux exemples de familles infinies de courbes elliptiques avec des structures de torsion non triviales.

3.1. Description des résultats connus

Une conjecture pour le cas rationnel. — Soit E une courbe elliptique définie sur \mathbb{Q} . Bien que toutes les structures des sous-groupes de torsion possibles de $E(\mathbb{Q})$ soient connues (Théorème de Mazur 1.2), le rang reste cependant mystérieux.

Conjecture 3.1. — *Quel que soit l'entier $n \in \mathbb{N}$, alors on peut trouver une courbe elliptique E/\mathbb{Q} telle que $\text{rang}(E/\mathbb{Q}) \geq n$.*

Nous connaissons à l'heure actuelle le résultat donné par Elkies [Elk07] :

Théorème 3.1 (Elkies). — *Il existe une courbe elliptique définie sur \mathbb{Q} telle que le rang vaut au moins 28.*

Pour les coefficients explicites d'une telle courbe, on renvoie le lecteur à la page de Dujella [Duja]. Il s'avère que dans la pratique, trouver des exemples de courbes elliptiques de grand rang est un problème assez difficile. Cela l'est d'autant difficile si l'on impose que la courbe possède une torsion non triviale, voir [Duja] pour des exemples explicites.

La méthode usuelle consiste à trouver de courbes elliptiques de rang élevé sur $\mathbb{Q}(t)$, on obtient ainsi, par spécialisation, des courbes elliptiques définies sur \mathbb{Q}

avec de grand rang. On peut aussi chercher les familles de courbes elliptiques paramétrées par les points d'une courbe elliptique de rang au moins 1.

Dans l'article [Nér56], Néron a montré (construction géométrique) l'existence de courbes elliptiques sur \mathbb{Q} de rang au moins 11. Ensuite, Shioda [Shi91] a donné une description plus effective de cette construction ainsi qu'un exemple de famille de courbes elliptiques de rang au moins 9.

Une autre approche plus algébrique est décrite par Mestre dans [Mes91a] et dans [Mes91b]. Mestre donne alors des exemples de familles infinies de courbes elliptiques de rang au moins 11 et 12. Cette construction fût reprise par beaucoup d'autres auteurs et qui est devenu la méthode la plus utilisée en pratique, voir par exemple [Fer96].

Le meilleur résultat connu à l'heure actuelle est celui de Elkies [Elk07] où l'auteur construit des familles de courbes elliptiques sur \mathbb{Q} de rang au moins 18.

En pratique, fournir des exemples des familles de courbes elliptiques de grand rang et de sous-groupes de torsion donnée est un problème difficile, notamment lorsque la partie torsion est grande.

Nous citerons par exemple : Lecacheux [Lec03a], Fermigier [Fer96], Kulesz [Kul03], Kihara [Kih06], Elkies [Elk07], Dujella, Nagao [Nag97],... Dans la section suivante, on décrira une autre méthode de construction.

3.2. Intersection d'une courbe elliptique avec des droites

Dans cette section, on supposera que l'on dispose d'une certaine famille de cubiques planes que l'on notera \mathcal{E}_t et avec des propriétés spéciales. Nous décrirons alors, par les intersections de droites, comment trouver des sous-familles avec un grand rang. Nous nous intéresserons particulièrement aux familles de courbes avec une grande torsion.

3.2.1. Description de la méthode. — Soit \mathcal{E}_t une cubique plane non singulière sur $\mathbb{Q}(t)$ et possédant un point rationnel qui n'est pas un point d'inflexion. Nous savons que la loi de groupe sur les cubiques est basée sur les intersections avec des droites. Il est donc naturel d'exploiter ces intersections.

Supposons donné un point P sur la courbe. On considère alors la droite $L_{P,\lambda}$ qui passe par P et de pente λ (on peut choisir λ de telle sorte que $L_{P,\lambda}$ ne soit pas tangent en P). Le théorème de Bézout affirme alors que $L_{P,\lambda}$ intersecte \mathcal{E}_t en 2 autres points P_1 et P_2 (qui peuvent être non rationnels). Cette intersection fournit

un trinôme P_λ sur $\mathbb{Q}(t)$ dont les solutions sont les abscisses des points P_1 et P_2 . Les points P_1 et P_2 sont rationnels si le discriminant $\text{Disc}(P_\lambda)$ est un carré. Les points rationnels sur la courbe

$$\Lambda : v^2 = \text{Disc } P_\lambda \quad (3.64)$$

peuvent alors paramétrer des familles de courbes elliptiques ayant davantage de points que sur la famille initiale.

En général, deux pentes différentes λ_1 et λ_2 fournissent différentes paramétrisations de sous-familles de \mathcal{E}_t . En choisissant de bonnes valeurs pour λ , on peut trouver des sous-familles de rang strictement plus grand.

Dans [Kul03], Kulesz a donné une astuce similaire pour produire des familles de courbes elliptiques avec des torsions non triviales et de grand rang : nous allons décrire cette méthode dans la section suivante.

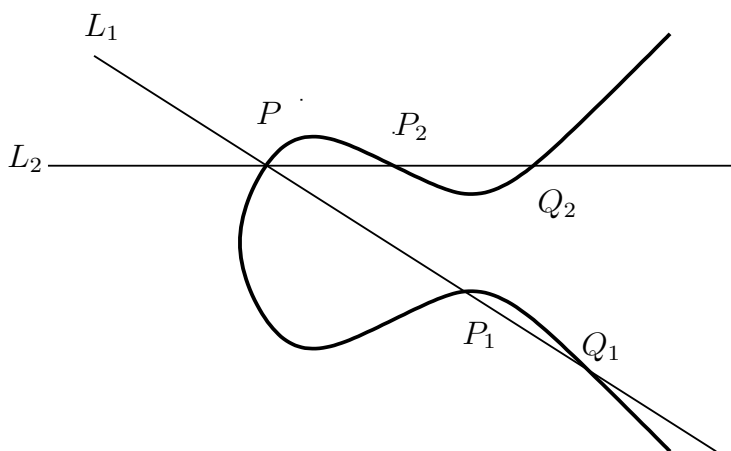


FIG. 3.1. Intersection de droites avec une cubique plane.

3.2.2. Exemples d'illustration. — Nous partons de la famille de cubiques planes Γ_t construite par Shioda dans [Shi91] :

$$\begin{aligned} \Gamma_t : 9z^3 - 2272xz^2 - 102949x^2z + 23898yz^2 + 201390xyz \\ - 79128x^2y - 128788y^2z + 87840xy^2 + t(x^3 - y^2z); \quad (3.65) \end{aligned}$$

Cette courbe passe par le point $\mathcal{O} = (0, 1, 0)$ et possède 9 autres points rationnels,

qui sont les points $Q_i = (u_i^{-2}, u_i^{-3}, 1)$ avec

$$\begin{array}{cccccc} u_0 = 0 & u_1 = 1 & u_2 = 2 & u_3 = -\frac{2}{3} & & \\ u_4 = 3 & u_5 = 4 & u_6 = 5 & u_7 = 6 & u_8 = -\frac{61}{3} & \end{array}$$

Shioda a ensuite montré que les 8 points Q_i pour $i = 1, \dots, 9$ sont indépendants donnant ainsi un nouvel exemple de courbe elliptique de rang au moins 8 sur $\mathbb{Q}(t)$.

Montrons qu'il existe une spécialisation $t = f(v)$ avec $f \in \mathbb{Q}[v]$, telle que $\Gamma_{f(v)}$ possède un autre point d'ordre infini et ainsi, on montre qu'à partir de la famille de cubique Γ_t , on peut construire une sous-famille de cubiques planes dont les rangs sont au moins 9.

Pour cela, nous allons travailler dans le plan affine. Nous partons de la courbe Γ_t de (3.65) et faisons $z = 1$. On considère le point $P = Q_1 = (1, 1)$ qui est sur $\Gamma_t(\mathbb{Q})$, on considérera aussi la droite $L_{P,-1}$ passant par P et de pente -1 . Cette droite coupe Γ_t en deux autres points $N_1(x_1, y_1)$ et $N_2(x_2, y_2)$ (remarquons que $N_1 + N_2 + P = \mathcal{O}$) dont les abscisses x_i sont les solutions de l'équation :

$$g(x) = (t + 166968)x^2 - 775775x + 4t + 467347 = 0 \quad (3.66)$$

Nous voulons imposer que x_1 et x_2 soient rationnels. Ainsi, on considère la courbe :

$$\mathcal{C}_{-1} : k^2 = \text{Disc}_x(g(x)) = -16t^2 - 4540876t + 289698875041 \quad (3.67)$$

On peut par exemple utiliser l'algorithme de van Hoeij [vH97] pour obtenir la paramétrisation :

$$(t_{-1}, k_{-1}) = \left(\frac{-1288947l^2 + 2420600l + 2459648}{4l^2 + 64}, \frac{325(931l^2 + 17756l - 14896)}{l^2 + 16} \right) \quad (3.68)$$

Cette construction permet alors d'obtenir un nouveau point :

$$N_{-1} = \left(\frac{-32l + 168}{21l + 64}, \frac{74l - 40}{21l + 64} \right)$$

sur la courbe $\Gamma_{t_{-1}}$. Afin de montrer que N_{-1} est bien d'ordre infini, il suffit de spécialiser une valeur pour l . Pour $l = 2$, on a $t = \frac{107253}{4}$, $N_{-1} = \left(\frac{52}{53}, \frac{54}{53} \right)$ et on

obtient la courbe elliptique :

$$\Gamma_{\frac{107253}{4}} : \frac{107253}{4}x^3 + (-79128y - 102949)x^2 + (87840y^2 + 201390y - 2272)x + \left(-\frac{622405}{4}y^2 + 23898y + 9\right). \quad (3.69)$$

En utilisant l'algorithme de van Hoeij [**vH97**], on obtient que $\Gamma_{\frac{107253}{4}}$ est équivalente à la courbe $\Gamma'_{\frac{107253}{4}}$ suivante :

$$\Gamma'_{\frac{107253}{4}} : y^2 = x^3 - \frac{2617622784729000703216}{3}x + \frac{96133075771647363172200828546028}{27} \quad (3.70)$$

et que le point N_{-1} correspond au point

$$N'_{-1} = \left(\frac{123192886904}{3}, 6080785909877250 \right)$$

Par un calcul direct, on peut montrer que N'_{-1} est d'ordre infini puisqu'il n'est pas de torsion. Aussi, les points $Q_i, i = 1, \dots, 8$ correspondent respectivement aux points :

$$\begin{aligned} Q'_1 &= \left(\frac{103910570279}{3}, 3859100479216125 \right) \\ Q'_2 &= \left(-\frac{375839726629}{12}, \frac{3253525894212165}{8} \right) \\ Q'_3 &= \left(\frac{23428144773491}{12}, -\frac{21821035542989574375}{8} \right) \\ Q'_4 &= \left(-\frac{258267862163}{9}, \frac{60181618922264125}{27} \right) \\ Q'_5 &= \left(-\frac{1289209178581}{48}, \frac{176672862176169645}{64} \right) \\ Q'_6 &= \left(-\frac{77391669025}{3}, 2983563311035617 \right) \\ Q'_7 &= \left(-\frac{905395749527}{36}, \frac{669149341350563125}{216} \right) \\ Q'_8 &= \left(-\frac{905395749527}{36}, \frac{669149341350563125}{216} \right). \end{aligned}$$

Ces points sont tous d'ordre infini. Un calcul sur PARI/gp [**BBB+**] montre que la matrice des hauteurs de points $Q_i, i = 1, \dots, 8$ et N'_{-1} est de déterminant non nul. Ce qui prouve que ces points sont indépendants. Nous avons donc obtenu une sous-famille infinie de courbes elliptiques de rang au moins 9.

En général, on peut obtenir une autre sous-famille en utilisant un autre point Q_i avec $i \neq 1$ ou en choisissant une autre pente. C'est ce que nous allons faire ici.

Un autre exemple. — Nous partons toujours du point $P = (1, 1)$ et choisissons la droite $L_{P,1}$ qui passe par P et de pente 1. Comme avant, $L_{P,1}$ intersecte la courbe Γ_t en deux autres points dont les abscisses sont les solutions de l'équation :

$$g(x) = (t + 8712)x^2 - 21635x - 9 = 0 .$$

Afin d'imposer que ces deux points soient rationnels, on considère la courbe :

$$\mathcal{C}_1 : m^2 = \text{Disc}_x(g(x)) = 36t + 468386857. \quad (3.71)$$

On trouve alors que t doit être de la forme

$$t = h(m) = \frac{1}{36}(m^2 - 468386857) ,$$

où $m \in \mathbb{Q}$. Ceci fournit de la même manière une nouvelle sous-famille de courbes de rang au moins 9.

La méthode de Kulesz [Kul03]. — Soit $E(t)$ une courbe elliptique définie sur $\mathbb{Q}(t)$ (en général de rang nul) :

$$E(t) : P(x, y) = y^2 + a_1(t)xy + a_3(t)y - (x^3 + a_2(t)x^2 + a_4(t)x + a_6(t)) = 0 \quad (3.72)$$

et un point de torsion $P(x(t), y(t))$ sur $E(t)$.

Considérons le polynôme

$$\mathcal{Q}_t(x) = \frac{P(x, y(t))}{(x - x(t))}. \quad (3.73)$$

Ce polynôme est de degré 2 en x . Définissons le polynôme $\mathcal{F}(t)$ comme la partie sans facteur carré du discriminant de \mathcal{Q}_t par rapport à x :

$$\text{Disc}_x(\mathcal{Q}_t(x)) = \mathcal{F}(t)\mathcal{R}(t)^2. \quad (3.74)$$

Si l'on spécialise la valeur $t \in \mathbb{Q}$, la droite horizontale $y = y(t)$ rencontre $E(t)$ en deux points rationnels si $\mathcal{F}(t)$ est un carré. L'équation $s^2 = \mathcal{F}(t)$ définit en général une courbe hyperelliptique, et dans certains cas, une courbe de genre 1 ou même 0, dont on cherchera les points rationnels.

Les points rationnels sur $E(t)$ que l'on construit ainsi sont généralement d'ordre infinis.

Lorsque $\deg(\mathcal{F}) = 3$ ou 4, on obtient la courbe elliptique

$$\Gamma_{\lambda, P} : s^2 = \mathcal{F}(t). \quad (3.75)$$

Il est nécessaire de bien vérifier que le rang $\Gamma_{\lambda,P}$ sur \mathbb{Q} soit au moins 1 pour obtenir une famille infinie de courbes elliptiques (paramétrée par Γ), qui soient de rang non nul.

Variation de la pente. — Nous avons vu que la méthode de Kulesz consiste à faire passer des droites horizontales par un point de la courbe. Nous nous autorisons ici à faire varier la pente de la droite, ce qui donne plus de liberté et nous permet de construire un grand nombre de nouvelles familles.

Soit maintenant $E(t)$ une courbe elliptique définie sur $\mathbb{Q}(t)$ par sa forme de Weierstrass

$$E(t) : P(x, y) = y^2 + a_1(t)xy + a_3(t)y - (x^3 + a_2(t)x^2 + a_4(t)x + a_6(t)) = 0 \quad (3.76)$$

et un point $P(x(t), y(t))$ sur $E(t)$, pas nécessairement de torsion. Nous considérons maintenant la droite $L_{\lambda,P}$ de pente λ , et passant par P :

$$L_{\lambda,P} : y - y(t) - \lambda(x - x(t)) = 0. \quad (3.77)$$

Soit $\lambda = \lambda(t)$ une fonction rationnelle; en considérant l'intersection de $L_{\lambda,P}$ avec la courbe $E(t)$, on est ramené à l'équation :

$$Q_t(x) = \frac{P(x, \lambda(x - x(t)) + y(t))}{(x - x(t))} = 0. \quad (3.78)$$

Pour obtenir de nouveaux points rationnels, il faut donc que le discriminant de Q par rapport à y soit un carré dans $\mathbb{Q}(t)$. Pour cela, nous regardons la partie sans facteur carré de ce discriminant que l'on notera $\mathcal{F}(\lambda, t)$ comme dans la section précédente.

Remarque 3.1. — *Dans tous les cas considérés dans cette thèse, lorsque $\deg(\mathcal{F}(t)) = 1$ ou 2 , nous remarquons que les coniques que nous avons obtenues possèdent toujours des points rationnels et par conséquent, on peut écrire s et t de l'équation $\Gamma : s^2 = \mathcal{F}(t)$ par des fonctions rationnelles en v sans changer de corps de base :*

$$s = f(v) \text{ et } t = g(v),$$

permettant ainsi d'obtenir deux autres points

$$N_1(x_1(v), y_1(v)) \text{ et } N_2(x_2(v), y_2(v)).$$

Ces points sont liés puisqu'ils sont alignés avec P et sont généralement d'ordre infini.

La suite de ce chapitre consiste à appliquer la méthode décrite précédemment aux familles de courbes avec des structures de torsion non triviales vues au chapitre 2 (voir aussi [Kub76]). Nous utilisons cette méthode en prenant comme point de départ, sauf mention du contraire, un point P de torsion et comme pente λ une fonction rationnelle en t .

Lorsque $\deg(\mathcal{F}(t)) = 1$ ou 2 , on obtient une famille de courbes elliptiques sur $\mathbb{Q}(v)$, de rang au moins 1 puis il est possible de recommencer le même processus en utilisant un autre droite passant par un point P' (on peut par exemple choisir le même point qu'avant).

Lorsque $\deg(\mathcal{F}(t)) > 4$, la situation n'est plus pareille puisque il ne peut y avoir de famille infinie (Théorème de Faltings) et si $\deg(\mathcal{F}(t)) = 3$ ou 4 , on obtient une famille de courbes elliptiques paramétrée par les points rationnels d'une courbe elliptique :

$$\Gamma_{\lambda, P} : s^2 = \mathcal{F}(t). \quad (3.79)$$

Dans la section suivante, nous nous intéresserons aussi aux cas où l'on considère la pente comme une variable.

Quelques notations supplémentaires. — Dans toute la suite, K désignera un corps de caractéristique nulle (presque toujours $\mathbb{Q}(t)$ dans la suite) et \mathcal{S} désignera une courbe elliptique sur K sous forme cubique (la plupart du temps, sous une forme de Weierstrass). La notation Λ désignera une courbe de genre 1 sous une forme quartique.

Soit \mathcal{C} une variété algébrique définie sur K et \mathcal{S} une courbe elliptique définie sur $K(\mathcal{C})$. On dit que \mathcal{C} paramétrise \mathcal{S} et on est amené à considérer la famille $\mathcal{S}_P, P \in \mathcal{C}(K)$ obtenue par spécialisation des coefficients. On dira aussi que \mathcal{C} est une paramétrisante.

Prenons maintenant deux entiers naturels non nuls m et n tels que $m|n$ et soit T le couple (m, n) . Si \mathcal{S} est une courbe elliptique définie sur K , la notation \mathcal{S}^T indiquera que $\text{Tors}(\mathcal{S}^T, K) \supseteq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

3.2.3. Modèle quartique et modèle cubique. — Nous rappelons une méthode connue sur le passage d'une forme cubique à une forme cubique (nous reprenons la méthode utilisée dans [AM93]). Soit l'équation de la forme :

$$H : y^2 = f(x) = ax^4 + bx^3 + cx^2 + dx + e, \quad (3.80)$$

avec a, b, c, d, e dans K , alors H définit une courbe de genre 1 si g n'a pas de facteur carré. On suppose que H possède un point K -rationnel $P = (x_0, y_0)$ qui n'est pas un point à l'infini. Avec la transformation :

$$x = x_0 + y_0 \left(X - \frac{f'(x_0)}{4y_0} \right)^{-1} \quad (3.81)$$

$$y = \frac{Y}{y_0} (x - x_0), \quad (3.82)$$

on montre que la courbe H est équivalente à la courbe H' définie par :

$$H' : X^4 - 6A_2X^2 + 4A_1X + A_0 = F(X). \quad (3.83)$$

qui, grâce à la transformation

$$X = \frac{T - A_1/2}{S - A_2} \quad Y = -X^2 + 2S + A_2 \quad (3.84)$$

est équivalente à la cubique

$$H'' : T^2 = S^3 - \frac{3A_2^2 + A_0}{4} + \frac{A_1^2 - A_2(A_2^2 - A_0)}{4} \quad (3.85)$$

Par la suite, nous utilisons par la suite des modèles de Weierstrass pour les courbes de genre 1 sous forme quartique via la transformation ci-dessus. Notons qu'il existe d'autres méthode pour passer d'un modèle quartique à un modèle de Weierstrass, voir par exemple [Cre97].

Lorsque $K = \mathbb{Q}$, nous utilisons la classification des courbes elliptiques sur \mathbb{Q} suivant leurs conducteurs, voir [Cre97].

3.3. Courbes avec des structures de torsion données

3.3.1. Familles avec $\text{Tors}(E, \mathbb{Q}) \supseteq \mathbb{Z}/7\mathbb{Z}$. — Soit $\mathcal{E}^7(t)$ la courbe elliptique définie sur $\mathbb{Q}(t)$ (voir 2.4.6) :

$$\mathcal{E}^{(7)} : y^2 - (t^2 - t - 1)xy - t^2(t - 1)y = x^3 - t^2(t - 1)x^2. \quad (3.86)$$

Nous avons $P_0 = (0, 0)$ qui est d'ordre 7 et nous partons de la courbe $\mathcal{E}^{(7)}$ pour obtenir une nouvelle courbe elliptique définie sur $\mathbb{Q}(t)$ de rang au moins 1 et un point d'ordre 7. Nous allons, pour cela reprendre la démarche de Kulesz [Kul03].

Soit $Q_1 = [4]P_0 = (t(t - 1), t^2(t - 1)^2)$ et soit la pente $\lambda = 0$. On considère l'intersection de la droite horizontale :

$$L_{\lambda, Q} : y = t^2(t - 1)^2 \quad (3.87)$$

avec la courbe $\mathcal{E}^{(7)}$, ainsi on obtient le polynôme :

$$\begin{aligned}\mathcal{Q}(x, t, \lambda) &= \frac{P(x, y_1)}{(x - x_1)} \\ &= -x^2 - t(t-1)^2x - t^3(t-2)(t-1)^2\end{aligned}$$

de discriminant

$$\Delta(\mathcal{Q}(x, t, \lambda)) = -t^2(t-1)^2(3t^2 - 6t - 1).$$

Nous considérons alors la courbe :

$$\Gamma_{\lambda, \mathcal{Q}} : s^2 = \mathcal{F}(t) = -(3t^2 - 6t - 1). \quad (3.88)$$

La courbe $\Gamma_{\lambda, \mathcal{Q}}$ est de genre 0 et on peut la paramétrer par :

$$(s, t) = \left(\frac{2v^2 - 6}{v^2 + 3}, \frac{v^2 - 4v + 3}{v^2 + 3} \right).$$

En substituant dans (3.86), on obtient la courbe elliptique :

$$\begin{aligned}\mathcal{E}_1^{(7)} : y^2 + \frac{v^4 + 4v^3 - 10v^2 + 12v + 9}{(v^2 + 3)^2}xy + \frac{4v(v-1)^2(v-3)^2}{(v^2 + 3)^3}y \\ = x^3 + 2\frac{v(v-1)^2(v-3)^2}{(v^2 + 3)^3}x^2.\end{aligned} \quad (3.89)$$

qui admet le modèle plus simple suivant :

$$\begin{aligned}\mathcal{E}_1^{(7)} : y^2 + (v^4 + 4v^3 - 10v^2 + 12v + 9)xy + 4v(v-1)^2(v-3)^2(v^2 + 3)^3y \\ = x^3 + 2v(v-1)^2(v-3)^2(v^2 + 3)x^2.\end{aligned} \quad (3.90)$$

On obtient aussi le point d'ordre infini :

$$N_1 = \left(4v(v-3)(v-1)^2(v+3)(v^2+3), 16v^2(v-3)^2(v-1)^2(v^2+3)^2 \right). \quad (3.91)$$

Pour la dernière assertion, il suffit de spécialiser la valeur de v . Par exemple, si on remplace v par 2 dans (3.90), on obtient la courbe elliptique :

$$E : y^2 + 41xy + 2744y = x^3 + 56x^2 \quad (3.92)$$

et le point $N_1 = (-280, 3136)$ qui est d'ordre infini puisqu'il n'est pas d'ordre 7 (voir le théorème de Mazur(1.2)).

À partir de cette famille (3.90), nous pouvons réitérer la méthode pour trouver encore des sous-familles de courbes elliptiques de rang plus grand. Nous avons maintenant la proposition suivante :

Théorème 3.2. — Il existe une courbe elliptique F définie sur \mathbb{Q} , telle que $F(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^2$ et une courbe elliptique $E_2^{(7)}$ définie sur $\mathbb{Q}(F)$ telle que $\text{Tors}(E_2^{(7)}, \mathbb{Q}(F)) \supseteq \mathbb{Z}/7\mathbb{Z}$ et $\text{rang}(E_2^{(7)}, \mathbb{Q}(F)) \geq 2$.

Remarque 3.2. — Elkies [Elk07] et Lecacheux [Lec03b], [Lec04] ont des résultats du même genre, sauf que leurs courbes elliptiques paramétrisantes sont de rang 1.

Démonstration. — Nous partons de la courbe elliptique obtenue ci-dessus :

$$\mathcal{E}_1^{(7)} : P(x, y) = y^2 + (v^4 + 4v^3 - 10v^2 + 12v + 9)xy + 4v(v-1)^2(v-3)^2(v^2+3)^3y - (x^3 + 2v(v-1)^2(v-3)^2(v^2+3)x^2) = 0. \quad (3.93)$$

On peut alors voir $\mathcal{E}_1^{(7)}$ comme une courbe elliptique définie sur $\mathbb{Q}(v)$. Posons maintenant $Q = [5]P_0$ où $P_0 = (0, 0)$. Nous allons ensuite tracer la droite $L_{\lambda, Q}$ passant par Q avec la pente $\lambda = -(v^2 - 2v + 3)^2$.

Mis à part le point P_0 , les abscisses des points d'intersection N_1 et N_2 de $L_{\lambda, Q}$ avec $\mathcal{E}_1^{(7)}$, sont solutions de l'équation quadratique

$$\mathcal{Q}(x, v) = \frac{P(x, \lambda(x - x(Q)) + y(Q))}{(x - x(Q))} = 0. \quad (3.94)$$

On montre alors que le discriminant de $\mathcal{Q}(x, v)$ est donné par :

$$\text{Disc}_x \mathcal{Q} = 2^4 v^4 (v^2 - 2v + 3)^2 (25v^4 - 116v^3 + 250v^2 - 348v + 225). \quad (3.95)$$

Pour que les deux points d'intersection soient rationnels, il faut que ce discriminant soit un carré. Il est donc naturel de considérer la courbe :

$$F : s^2 = 25v^4 - 116v^3 + 250v^2 - 348v + 225. \quad (3.96)$$

La courbe F est de genre 1. Aussi, nous pouvons utiliser le modèle de Weierstrass suivant pour F :

$$4416bb1 : y^2 = x^3 + x^2 - 185x + 1479.$$

Cette courbe est de rang 2 sur \mathbb{Q} (voir table de Cremona [Cre97]) et de sous-groupe de torsion isomorphe à $\mathbb{Z}/2\mathbb{Z}$. \square

Il est facile de vérifier que le sous-groupe de torsion de la courbe 4416bb1 est engendré par $(-17, 0)$ et que les points $(-14, 39)$ et $(-5, 48)$ sont d'ordre infini et indépendants.

Jusqu'à maintenant, c'est la seule courbe elliptique définie sur \mathbb{Q} que nous connaissons, qui soit de rang 2 et qui paramétrise en même temps des courbes elliptiques de rang 2 et de partie torsion isomorphe à $\mathbb{Z}/7\mathbb{Z}$.

Dans l'annexe B, nous montrons l'existence d'autres courbes paramétrisantes en faisant d'autres choix de points de départ et d'autres pentes. Les courbes elliptiques paramétrisantes que nous obtenons sont alors de rang 1. Elles sont au nombre de 4 :

$$\{1221a1, 243a2, 444b1, 504f2\}$$

Nous renvoyons le lecteur à l'annexe B pour les équations de ces courbes.

Théorème 3.3. — Soit $K = \mathbb{Q}(a)$, alors il existe une courbe elliptique $\mathcal{S}^{(1,2)}$ définie sur K , telle que

$$\text{Tors}(\mathcal{S}^{(1,2)}, K) \supseteq \mathbb{Z}/2\mathbb{Z}, \text{rang}(\mathcal{S}^{(1,2)}, K) \geq 1,$$

et une courbe elliptique $\mathcal{S}^{(1,7)}$ définie sur $K(\mathcal{S}^{(1,2)})$ telle que

$$\text{Tors}(\mathcal{S}^{(1,7)}, K(\mathcal{S}^{(1,2)})) \supseteq \mathbb{Z}/7\mathbb{Z} \text{ et } \text{rang}(\mathcal{S}^{(1,7)}, K(\mathcal{S}^{(1,2)})) \geq 1.$$

Démonstration. — On part de la famille de courbes elliptiques :

$$\mathcal{E}^{(7)} : y^2 - (t^2 - t - 1)xy - t^2(t - 1)y = x^3 - t^2(t - 1)x^2. \quad (3.97)$$

Le point $P_0 = (0, 0)$ est d'ordre 7 dans $\mathcal{E}^{(7)}(\mathbb{Q}(t))$. Nous considérons ensuite la droite passant par P_0 et de pente $\lambda = at^2$ où a sera une variable. Nous considérons maintenant l'intersection de la droite d'équation $y = \lambda x$ et la courbe elliptique $\mathcal{E}^{(7)}/\mathbb{Q}(t)$. Mis à part le point $P_0 = (0, 0)$, les abscisses des deux autres points de cette intersection sont les racines de l'équation quadratique :

$$Q_{a,t}(x) = -x^2 + (a(a - 1)t^4 + (a + 1)t^3 + (a - 1)t^2)x + at^4(-t + 1) = 0.$$

Le discriminant de $Q_{a,t}$ est :

$$\begin{aligned} \text{Disc}_x(Q_{a,t}) &= (a^2(a - 1)^2t^4 + 2a(a^2 - 1)t^3 + (2a^3 - 3a^2 + 4a + 1)t^2 \\ &\quad + (2a^2 - 4a - 2)t + (a + 1)^2)t^4. \end{aligned} \quad (3.98)$$

Pour que les racines soient rationnelles, nous imposons ensuite que $\text{Disc}_x(Q_{a,t}(x))$ soit un carré dans le corps $\mathbb{Q}(a)$. On considère alors la courbe définie sur $\mathbb{Q}(a)$ par :

$$\Lambda^{(1,2)} : Y^2 = \mathcal{F}_a(t) = t^{-4} \text{Disc}_x(Q_{a,t}(x))$$

La courbe $\Lambda^{(1,2)}/\mathbb{Q}(a)$ de genre 1 dont $(Y, t) = (a + 1, 0)$ est un point particulier. On utilise ensuite son modèle de Weierstrass :

$$\begin{aligned} \mathcal{S}^{(1,2)} : s^2 = x^3 - 2^{-4}3^{-1}(16a^6 - 24a^5 + 25a^4 + 4a^3 - 2a^2 - 4a + 1)x \\ - 2^{-5}3^{-3}(4a^3 + 3a^2 + 2a - 1)(16a^6 - 48a^5 + 25a^4 + 4a^3 - 2a^2 - 4a + 1). \end{aligned} \quad (3.99)$$

Les points

$$P_2 = \left(-\frac{4a^3 + 3a^2 + 2a - 1}{12}, 0 \right) \text{ et}$$

$$P_G = \left(-\frac{1}{12} \frac{4a^5 - a^4 + 12a^3 + 6a^2 - 1}{(a + 1)^2}, \frac{a^4(3a^2 + 2a + 1)}{2(a + 1)^3} \right)$$

sont sur $\mathcal{S}^{(1,2)}$ et il est immédiat de voir que l'ordre de P_2 est 2. Pour montrer que P_G est bien d'ordre infini, il suffit de spécialiser la valeur de a dans les expressions ci-dessus. Si l'on remplace a par 3 dans (3.99), on obtient la courbe elliptique :

$$E : y^2 = x^3 - \frac{496}{3}x - \frac{9205}{27}, \quad (3.100)$$

et le point P_G devient alors

$$P_g = \left(-\frac{317}{48}, -\frac{1377}{64} \right).$$

Ce point est d'ordre infini puisqu'il n'est pas de torsion. Le rang de $\mathcal{S}^{(1,2)}$ sur $\mathbb{Q}(a)$ est donc au moins 1. \square

Soit $P = (x_P, y_P) \in \mathcal{S}^{(1,2)}$, puis en suivant la méthode vue au paragraphe 3.2.3, nous obtenons le point (t_P, Y_P) correspondant sur la quartique $\Lambda^{(1,2)}$ avec :

$$t_P = \frac{-24(a + 1)^2 x_P - 8a^5 + 2a^4 - 24a^3 - 12a^2 + 2}{12(a^2 - 2a - 1)x_P + 4a^5 + 19a^4 - 8a^3 - 8a^2 - 24ay_P - 24y_P + 1} \quad (3.101)$$

Pour trouver la courbe elliptique $\mathcal{S}_P^{(1,7)}$, il suffit de remplacer t par t_P dans l'expression de $\mathcal{E}^{(7)}$ (voir (3.97)). On obtient aussi les abscisses des deux autres points d'intersection :

$$\frac{-t_P^2(-a^2 + a)t^2 + (-a - 1)t + (-a + 1) \pm Y_P}{2} \quad (3.102)$$

Nous allons maintenant illustrer cela en donnant quelques exemples.

Exemple. — Prenons le point $P_2 = [2]P_G \in \mathcal{S}^{(1,2)}(\mathbb{Q}(a))$, on obtient le point $(t_{P_2}, Y_{P_2}) \in \Lambda^{(1,2)}(\mathbb{Q}(a))$ avec :

$$t_{P_2} = -\frac{(a+1)(3a^2+2a+1)}{(a^2+a+1)(a^3-a^2-2a-1)}. \quad (3.103)$$

Nous obtenons ensuite l'expression de la courbe elliptique $\mathcal{S}_{P_2}^{(1,7)}$ en remplaçant t par t_{P_2} dans l'expression de $\mathcal{E}^{(7)}$.

$$\begin{aligned} \mathcal{S}_{P_2}^{(1,7)} : y^2 + \frac{a(a+1)^4(3a^2+2a+1)^2(a^4+3a^3+6a^2+4a+1)}{(a^2+a+1)^3(a^3-a^2-2a-1)^3}y \\ + \frac{(a^{10}-3a^9-21a^8-58a^7-90a^6-82a^5-39a^4-2a^3+9a^2+5a+1)}{(a^2+a+1)^2(a^3-a^2-2a-1)^2}xy \\ = x^3 + \frac{a(a+1)^4(3a^2+2a+1)^2(a^4+3a^3+6a^2+4a+1)}{(a^2+a+1)^3(a^3-a^2-2a-1)^3}x^2. \end{aligned} \quad (3.104)$$

On trouve alors le point d'ordre infini :

$$R_2 = \left(-\frac{a(a+1)^4(3a^2+2a+1)^2}{(a^2+a+1)^4(a^3-a^2-2a-1)}, \frac{a^2(a+1)^5(2a+1)(3a^2+2a+1)^3}{(a^2+a+1)^6(a^3-a^2-2a-1)^2} \right). \quad (3.105)$$

Pour voir la dernière assertion, il suffit de spécialiser a . Remplaçons A par 3 dans (3.104) et dans (3.105). On obtient alors la courbe elliptique

$$E : y^2 - \frac{353279}{20449}xy + \frac{203308032}{2924207}y = x^3 + \frac{203308032}{2924207}x^2. \quad (3.106)$$

ainsi que le point

$$N = \left(\frac{-887808}{314171}, \frac{2535579648}{584043889} \right)$$

qui est d'ordre infini puisqu'il n'est pas de torsion.

Théorème 3.4. — Soit $K = \mathbb{Q}(a)$, alors il existe une courbe elliptique $\mathcal{S}^{(1,3)}$ définie sur K , telle que

$$\text{Tors}(\mathcal{S}^{(1,3)}, K) \supseteq \mathbb{Z}/3\mathbb{Z}, \text{rang}(\mathcal{S}^{(1,3)}, K) \geq 1,$$

et une courbe elliptique $\mathcal{S}^{(1,7)}$ définie sur $K(\mathcal{S}^{(1,3)})$ telle que

$$\text{Tors}(\mathcal{S}^{(1,7)}, K(\mathcal{S}^{(1,3)})) \supseteq \mathbb{Z}/7\mathbb{Z} \text{ et } \text{rang}(\mathcal{S}^{(1,7)}, K(\mathcal{S}^{(1,3)})) \geq 1.$$

Démonstration. — Comme précédemment, la construction de la paramétrisation est explicite. Soient la courbe elliptique définie sur $\mathbb{Q}(t)$ (voir 2.4.6) définie par :

$$\mathcal{E}^{(7)} : y^2 - (t^2 - t - 1)xy - t^2(t-1)y = x^3 - t^2(t-1)x^2, \quad (3.107)$$

et le point $P_0 = (0, 0)$ qui est d'ordre 7 sur $\mathcal{E}^{(7)}(\mathbb{Q}(t))$. Nous considérons alors la droite passant par P_0 et de pente $\lambda = at$ où a est une nouvelle indéterminée.

Considérons l'intersection de la droite d'équation $y = \lambda x$ et la courbe elliptique $\mathcal{E}^{(7)}$. Mis à part le point P_0 , les deux autres points de cette intersection ont leurs abscisses solutions de l'équation quadratique :

$$Q_{a,t}(x) = -x^2 + ((-a + 1)t^3 + (a^2 + a - 1)t^2 + at)x + at^3(-t + 1) = 0. \quad (3.108)$$

Le discriminant de $Q_{a,t}$ est :

$$\begin{aligned} \text{Disc}_x(Q_{a,t}) = & ((a - 1)^2 t^4 + (-2a^3 + 4a - 2)t^3 + (a^4 + 2a^3 - 3a^2 - 4a + 1)t^2 \\ & + (2a^3 + 2a^2 + 2a)t + a^2)t^2. \end{aligned}$$

Ainsi, pour ne pas changer de corps de base, nous imposons que $\text{Disc}_x(Q_{a,t}(x))$ soit un carré. On considère alors la courbe (de genre 1) sur $\mathbb{Q}(a)$:

$$\Lambda^{(1,3)} : Y^2 = \mathcal{F}_a(t) = t^{-2} \text{Disc}_x(Q_{a,t}(x))$$

Cela définit une courbe de genre 1 dont $(Y, t) = (a, 0)$ est un point particulier. On utilise ensuite son modèle de Weierstrass :

$$\begin{aligned} \mathcal{S}^{(1,3)} : s^2 = & x^3 - 2^{-4}3^{-1}(a^2 + a + 1)(a^6 + 3a^5 + 6a^4 - 17a^3 + 6a^2 + 3a + 1)x \\ & + 2^{-5}3^{-3}(a^{12} + 6a^{11} + 21a^{10} + 14a^9 - 18a^8 - 90a^7 \\ & + 105a^6 - 90a^5 - 18a^4 + 14a^3 + 21a^2 + 6a + 1). \end{aligned} \quad (3.109)$$

Il est facile de vérifier que les points

$$P_3 = \left(\frac{1}{12}(a^2 + a + 1), \frac{1}{2}a^3 \right) \quad (3.110)$$

et

$$P_G = \left(\frac{1}{12}(a^4 + 2a^3 + 15a^2 + 14a + 1), -\frac{1}{2}a(a^3 + 3a^2 + 4a + 1) \right), \quad (3.111)$$

sont sur $\mathcal{S}^{(1,3)}$ et que P_3 est d'ordre 3. Pour montrer que P_G est bien d'ordre infini, il suffit de spécialiser la valeur de a dans les expressions ci-dessus. Si l'on remplace a par 3 dans (3.109), on obtient la courbe elliptique :

$$E : y^2 = x^3 - \frac{-20137}{48}x + \frac{2848789}{864}, \quad (3.112)$$

et le point P_G devient alors

$$P_g = \left(-\frac{313}{12}, -\frac{-201}{2} \right).$$

Ce point est d'ordre infini puisqu'il n'est pas de torsion. Cela prouve donc que le rang de $\mathcal{S}^{(1,3)}$ sur $(\mathbb{Q}(a))$ est au moins 1. \square

Soit $P = (x_P, y_P) \in \mathcal{S}^{(1,3)}$, puis en suivant la méthode vue au paragraphe 3.2.3, nous obtenons le point (t_P, Y_P) correspondant sur la quartique $\Lambda^{(1,3)}$ avec :

$$t_P = \frac{a(24x_P - 2a^4 - 4a^3 - 30a^2 - 28a - 2)}{-12(a^2 + a + 1) + a^6 + 3a^5 + 6a^4 - 5a^3 - 18a^2 + 3a + 1}, \quad (3.113)$$

Pour trouver la courbe elliptique $\mathcal{S}_P^{(1,7)}$, il suffit de remplacer t par t_P dans l'expression de $\mathcal{E}^{(7)}$ (voir (3.107)). Les abscisses des deux autres points d'intersection sont :

$$\frac{-t_P \left((-a+1)t_P^2 + (a^2+a-1)t_P + a \pm Y_P \right)}{2}. \quad (3.114)$$

Nous allons maintenant donner des exemples pour illustrer le théorème.

Exemples. — En général, deux points distincts P et P' sur $\mathcal{S}^{(1,3)}(Q(a))$ donnent deux courbes elliptiques $\mathcal{S}_P^{(1,3)}$ et $\mathcal{S}_{P'}^{(1,3)}$ qui ne sont pas isomorphes sur $\mathbb{Q}(a)$.

Avec le point $P_2 = [2]P_G \in \mathcal{S}^{(1,3)}(\mathbb{Q}(a))$, nous obtenons le point $(t_{P_2}, Y_{P_2}) \in \Lambda^{(1,3)}(\mathbb{Q}(a))$ avec

$$t_{P_2} = \frac{a^3 + 3a^2 + 4a + 1}{(a+2)(2a+1)}, \quad (3.115)$$

Si l'on remplace t par t_{P_2} dans l'expression de $\mathcal{E}^{(7)}$, cela nous donne la courbe elliptique :

$$\begin{aligned} \mathcal{S}_{P_2}^{(1,7)} : y^2 - \frac{(a^6 + 4a^5 + 2a^4 - 19a^3 - 39a^2 - 25a - 5)}{(a+2)^2(2a+1)^2}xy \\ - \frac{(a-1)(a+1)^2(a^3 + 3a^2 + 4a + 1)^2}{(a+2)^3(2a+1)^3}y \\ = x^3 - \frac{(a-1)(a+1)^2(a^3 + 3a^2 + 4a + 1)^2}{(a+2)^3(2a+1)^3}x^2. \end{aligned} \quad (3.116)$$

On obtient de même un point d'ordre infini sur $\mathcal{S}_{P_2}^{(1,7)}(\mathbb{Q}(a))$:

$$R_2 = \left(\frac{(a^2-1)(a^3+3a^2+4a+1)}{(a+2)^3(2a+1)}, \frac{a(a^2-1)(a^3+3a^2+4a+1)^2}{(a+2)^4(2a+1)^2} \right) \quad (3.117)$$

Pour voir la dernière assertion, il suffit de spécialiser a . Remplaçons a par 3 dans (3.116) et dans (3.117). On obtient alors la courbe elliptique

$$E : y^2 - \frac{919}{1225}xy - \frac{143648}{42875}y = x^3 - \frac{143648}{42875}x^2. \quad (3.118)$$

et le point

$$R_2 = \left(\frac{536}{875}, \frac{107736}{30625} \right).$$

Ce point est d'ordre infini puisqu'il n'est pas de torsion. Nous obtenons bien que la courbe $\mathcal{S}_{P_2}^{(1,7)}$ est de rang au moins 1 sur $\mathbb{Q}(a)$.

Lorsque l'on prend le point $P_3 = [3]P_G$, on obtient le point correspondant (t_{P_3}, Y_{P_3}) dans $\Lambda^{(1,3)}(\mathbb{Q}(a))$ avec :

$$\begin{aligned} t_{P_3} &= (a+1)(a^2+a+1)(a^3+3a^2+4a+1)(a^4+6a^3+13a^2+6a+1) \\ &\quad \times (a^4+7a^3+11a^2+7a+1)^{-1}(a^5+3a^4+7a^3+10a^2+5a+1)^{-1}. \end{aligned} \quad (3.119)$$

Ainsi, si l'on remplace t par t_{P_3} dans l'expression de $\mathcal{E}^{(7)}$, nous obtenons la courbe elliptique $\mathcal{S}_{P_3}^{(1,7)}$. Les points d'abscisses

$$\begin{aligned} x_3 &= \left(a^2(a+1)(a+2)(a^2+a+1)(a^3+3a^2+4a+1)^2 \right. \\ &\quad \times (a^4+4a^3+10a^2+9a+3)(a^4+6a^3+13a^2+6a+1) \\ &\quad \left. \times (a^4+7a^3+11a^2+7a+1)^{-3}(a^5+3a^4+7a^3+10a^2+5a+1)^{-1} \right) \end{aligned}$$

sont d'ordre infini. Cela peut être prouvé en spécialisant a . En faisant $a = 2$, on obtient la courbe elliptique

$$E : y^2 - \frac{3647218895}{600103009}xy - \frac{333673856100144}{14700723411473}y = x^3 - \frac{333673856100144}{14700723411473}x^2, \quad (3.120)$$

et le point

$$R_3 = \left(\frac{3973301136}{420393017}, \frac{624293021090592}{10298367737449} \right).$$

Ce point est d'ordre infini puisqu'il n'est pas de torsion. Nous obtenons alors que la courbe $\mathcal{S}_{P_3}^{(1,7)}$ est de rang au moins 1 sur $\mathbb{Q}(a)$.

Théorème 3.5. — Soit $K = \mathbb{Q}(a)$, alors il existe une courbe elliptique $\mathcal{S}^{(1,4)}$ définie sur K , telle que

$$\text{Tors}(\mathcal{S}^{(1,4)}, K) \supseteq \mathbb{Z}/4\mathbb{Z}, \text{rang}(\mathcal{S}^{(1,4)}) \geq 1,$$

et une courbe elliptique $\mathcal{S}^{(1,7)}$ définie sur $K(\mathcal{S}^{(1,4)})$ telle que

$$\text{Tors}(\mathcal{S}^{(1,7)}, K(\mathcal{S}^{(1,4)})) \supseteq \mathbb{Z}/7\mathbb{Z} \text{ et } \text{rang}(\mathcal{S}^{(1,7)}, K(\mathcal{S}^{(1,4)})) \geq 1.$$

Démonstration. — Soient la courbe elliptique sur $\mathbb{Q}(t)$ définie par :

$$\mathcal{E}^{(7)} : y^2 - (t^2 - t - 1)xy - t^2(t - 1)y = x^3 - t^2(t - 1)x^2 = 0, \quad (3.121)$$

ainsi que le point $P_0 = (0, 0)$ qui est d'ordre 7 sur $\mathcal{E}^{(7)}(\mathbb{Q}(t))$ (voir 2.4.6). Considérons la droite passant par P_0 et de pente $\lambda = a(t - 1)$ où a est une nouvelle indéterminée.

Nous considérons ensuite l'intersection de la droite d'équation $y = \lambda x$ et de la courbe elliptique $\mathcal{E}^{(7)}$. Mis à part le point P_0 , les deux autres points de cette intersection ont leurs abscisses solutions de l'équation quadratique :

$$Q_{a,t}(x) = -x^2 + ((-a + 1)t^3 + (a^2 + 2a - 1)t^2 - 2a^2t + (a^2 - a))x - at^2(t - 1)^2 = 0.$$

Le discriminant de $Q_{a,t}$ est :

$$\begin{aligned} \text{Disc}_x(Q) &= ((a - 1)^2t^4 - 2a(a^2 - 1)t^3 + a(a - 1)(a^2 + 5a + 2) \\ &\quad - 2a^2(a - 1)^2t + a^2(a - 1)^2)(t - 1)^2. \end{aligned}$$

Ainsi, pour que les deux autres points de l'intersection soient rationnels, il faut que $\text{Disc}_x(Q_{a,t}(x))$ soit un carré. On considère alors la courbe définie sur $\mathbb{Q}(a)$ par :

$$\Lambda^{(1,4)} : Y^2 = \mathcal{F}_a(t) = (t - 1)^{-2} \text{Disc}_x(Q_{a,t}(x)).$$

La courbe $\Lambda^{(1,4)}/\mathbb{Q}(a)$ de genre 1 dont $(Y, t) = (a(a - 1), 0)$ est un point particulier. On utilise ensuite le modèle de Weierstrass :

$$\begin{aligned} \mathcal{S}^{(1,4)} : s^2 &= x^3 - 2^{-4}3^{-1}a^2(a - 1)^2(a^4 - 2a^3 + 17a^2 - 16a + 16)x \\ &\quad + 2^{-5}3^{-3}a^3(a - 1)^3(a^2 - a + 8)(a^4 - 2a^3 + 17a^2 - 16a - 8). \end{aligned} \quad (3.122)$$

Le point

$$P_T = \left(\frac{1}{12}a(a - 1)(a^2 - a - 4), \frac{1}{2}a^2(a - 1)^2 \right)$$

est d'ordre 4 et le point

$$P_G = \left(\frac{1}{12}a(a^3 - 2a^2 + 9a + 4), \frac{1}{2}a^2(a + 1) \right), \quad (3.123)$$

est d'ordre infini. En effet, il suffit de spécialiser a . En faisant $a = 2$ dans (3.122) et dans (3.123), on obtient la courbe elliptique :

$$E : y^2 = x^3 - 111x + 434,$$

et le point $Pg = (10, 18)$. Il est facile de voir que Pg est d'ordre infini puisqu'il n'est pas de torsion. Il s'ensuit donc que le rang de $\mathcal{S}^{(1,4)}$ sur $\mathbb{Q}(a)$ est non nul. \square

Comme avant, on obtient une famille infinie de courbes elliptiques par spécialisation du point sur $\Lambda^{(1,4)}$. Soit $P = (x_P, y_P) \in \mathcal{S}^{(1,4)}$, puis en suivant la méthode vue au paragraphe 3.2.3, nous obtenons le point (t_P, Y_P) correspondant sur la quartique $\Lambda^{(1,4)}$ avec :

$$t_P = \frac{24a(a-1)x_P - 2a^2(a-1)(a^3 - 2A^2 + 9a + 4)}{12a(a+1)x_P - a^6 + a^5 - 7a^4 - a^3 + 8a^2} \quad (3.124)$$

Pour trouver la courbe elliptique $\mathcal{S}_P^{(1,7)}$, il suffit maintenant de remplacer t par t_P dans l'expression de $\mathcal{E}^{(7)}$ (voir (3.121)). On obtient aussi les abscisses des deux autres points d'intersection :

$$\frac{(-a+1)t_P^3 + (a^2+2a-1)t_P^2 - 2a^2t_P + (a^2-a)}{2} \pm Y_P(t_P-1). \quad (3.125)$$

Nous allons illustrer cela par quelques exemples.

Exemples. — Avec le point $P_2 = [2]P_G \in \mathcal{S}^{(1,4)}(\mathbb{Q}(a))$, on trouve le point correspondant $(t_{P_2}, Y_{P_2}) \in \Lambda^{(1,4)}(\mathbb{Q}(a))$ avec :

$$t_{P_2} = \frac{a^2 - 1}{a - 2} \quad (3.126)$$

Nous obtenons la courbe elliptique $\mathcal{S}_{P_2}^{(1,7)}$ en remplaçant t par t_{P_2} dans l'équation de $\mathcal{E}^{(7)}$ (voir (3.97)).

$$\begin{aligned} \mathcal{S}_{P_2}^{(1,7)} : y^2 - (a^4 - a^3 - a^2 + 5a - 5)(a-2)^{-2}xy - (a^2-1)(a-2)^{-3}(a^2-a+1)y \\ = x^3 - (a^2-1)(a-2)^{-3}(a^2-a+1)x^2, \end{aligned} \quad (3.127)$$

Nous obtenons également le point d'ordre infini sur $\mathcal{S}_{P_1}^{(1,7)}$:

$$R_2 = \left(-\frac{a(a-1)(a^2-a+1)}{a-2}, -\frac{a^2(a-1)(a^2-a+1)^2}{(a-2)^2} \right). \quad (3.128)$$

En effet, il suffit de spécialiser a . Remplaçons a par 3 dans (3.127). On obtient la courbe elliptique :

$$E : y^2 - 55xy - 448y = x^3 - 448x^2.$$

ainsi que le point

$$R_2 = (-42, -882). \quad (3.129)$$

Ce point est d'ordre infini puisqu'il n'est pas de torsion.

Prenons maintenant un autre point sur $\mathcal{S}^{(1,4)}(\mathbb{Q}(a))$. Le point $P_3 = [3]P_G$ correspond au point $(t_{P_3}, Y_{P_3}) \in \Lambda^{(1,4)}(\mathbb{Q}(a))$ avec :

$$t_{P_3} = \frac{(a-1)(a+1)(a^3 - 5a^2 + 2a - 1)}{(a-2)(a^4 - a^3 + 2a^2 - 4a + 1)}.$$

Avec le point P_3 , nous obtenons alors la courbe elliptique :

$$\begin{aligned} \mathcal{S}_{P_3}^{(1,7)} : & y^2 + (a^{10} - 4a^9 + 10a^8 - 65a^7 + 164a^6 - 184a^5 + 122a^4 \\ & - 92a^3 + 67a^2 - 19a + 1)xy + (a^2 - 1)^2(a^3 - 5a^2 + 2a - 1)^2 \\ & \times (a^3 + 2a^2 - 5a + 3)(a-2)^{-3}(a^4 - a^3 + 2a^2 - 4a + 1)^{-3}y \\ & = x^3 + (a^2 - 1)^2(a^3 - 5a^2 + 2a - 1)^2(a^3 + 2a^2 - 5a + 3) \\ & \quad \times (a-2)^{-3}(a^4 - a^3 + 2a^2 - 4a + 1)^{-3}x^2, \end{aligned} \quad (3.130)$$

ainsi qu'un point d'ordre infini sur $\mathcal{S}_{P_3}^{(1,7)}(\mathbb{Q}(a))$:

$$\begin{aligned} R_3 = & \left(\frac{(a-1)(a+1)^2(2a-1)(a^3 + 2a^2 - 5a + 3)}{(a-2)^3(a^4 - a^3 + 2a^2 - 4a + 1)}, \right. \\ & \left. - \frac{a(a-1)(a+1)^2(2a-1)^2(a^3 + 2a^2 - 5a + 3)^2}{(a-2)^4(a^4 - a^3 + 2a^2 - 4a + 1)^2} \right) \end{aligned} \quad (3.131)$$

Pour prouver la dernière assertion, nous allons spécialiser a . Remplaçons a par 3 dans (3.130). On obtient la courbe elliptique :

$$E : y^2 - \frac{13439}{3721}xy + \frac{1784640}{226981}y = x^3 + \frac{1784640}{226981}x^2.$$

ainsi que le point

$$R_3 = \left(\frac{5280}{61}, -\frac{2613600}{3721} \right). \quad (3.132)$$

Ce point est d'ordre infini puisqu'il n'est pas de torsion. On en conclut donc que le rang de $\mathcal{S}_{P_3}^{(1,7)}$ sur $\mathbb{Q}(a)$ est au moins 1.

3.3.2. Familles avec $\text{Tors}(E, \mathbb{Q}) \supseteq \mathbb{Z}/8\mathbb{Z}$. — Soit $\mathcal{E}^8(t)$ la courbe elliptique définie sur $\mathbb{Q}(t)$:

$$\begin{aligned} \mathcal{E}^{(8)} : & y^2 - (2t^2 - 4t + 1)xy - (2t - 1)(t - 1)t^3y \\ & - (x^3 - (2t - 1)(t - 1)t^2x^2) = 0. \end{aligned} \quad (3.133)$$

Le $P_0 = (0, 0)$ est d'ordre 8 (voir 2.4.7). Nous partons de cette courbe pour obtenir des familles infinies de courbes elliptiques de rang au moins 2 et possédant un point d'ordre 8.

Dans [Kul03], [Lec03b], [Lec04], Kulesz et Lecacheux ont chacun montré de façons différentes le théorème suivant

Théorème 3.6. — *Il existe une courbe elliptique E définie sur $\mathbb{Q}(t)$ telle que $\text{Tors}(E, \mathbb{Q}) \supseteq \mathbb{Z}/8\mathbb{Z}$ et $\text{rang}(E, \mathbb{Q}(t)) \geq 1$.*

Nous allons reprendre ici la démarche de Kulesz [Kul03].

Soit $Q_1 = [2]P_0 = (x_1, y_1) = (2(t^2(t-1)(2t-1), t^2(t-1)^2(2t-1)^2)$ et soit $\lambda = 0$. On considère l'intersection de la droite horizontale d'équation :

$$L : y = y_1 \quad (3.134)$$

passant par P_0 avec la courbe $\mathcal{E}^{(8)}$, ainsi on obtient l'équation :

$$\mathcal{Q}(y, t, \lambda) = -x^2 - t^2(t-1)^2(2t-1)^2(2t^2 - 4t + 1) = 0.$$

L'intersection est constituée de deux nouveaux points rationnels si $-2t^2 + 4t - 1$ est un carré. Nous considérons donc la courbe d'équation :

$$\Gamma : s^2 = \mathcal{F}(t) = -2t^2 + 4t - 1, \quad (3.135)$$

qui est de genre 0 et que l'on peut paramétrer par :

$$(s, t) = \left(\frac{v^2 - 2}{v^2 + 2}, \frac{v^2 - 2v + 2}{v^2 + 2} \right).$$

En remplaçant « s » dans l'expression de $\mathcal{E}^{(8)}$, on obtient alors la courbe elliptique :

$$\begin{aligned} \mathcal{E}_1^{(8)} : y^2 + \frac{(v^2 - 2)^2}{(v^2 + 2)^2}xy + \frac{2v(v^2 - 4v + 2)(v^2 - 2v + 2)^3}{(v^2 + 2)^5}y \\ = x^3 + 2\frac{v(v^2 - 4v + 2)(v^2 - 2v + 2)^2}{(v^2 + 2)^4}x^2, \end{aligned} \quad (3.136)$$

définie sur $\mathbb{Q}(v)$ et un nouveau point :

$$N = \left(\frac{2v(v-1)(v^2 - 2v + 2)^2}{(v^2 + 2)^3}, -\frac{4v^2(v-1)^2(v^2 - 2v + 2)^2(v^2 - 2)}{(v^2 + 2)^5} \right)$$

Le rang de la courbe $\mathcal{E}_1^{(8)}$ sur $\mathbb{Q}(t)$ est donc au moins 1.

Nous optons pour le modèle sans dénominateur suivant pour la courbe $\mathcal{E}_1^{(8)}$:

$$\begin{aligned} \mathcal{E}_1^{(8)} : y^2 + (v^2 - 2)^2xy + 2v(v^2 + 2)(v^2 - 4v + 2)(v^2 - 2v + 2)^3y \\ = x^3 + 2v(v^2 - 4v + 2)(v^2 - 2v + 2)^2x^2. \end{aligned} \quad (3.137)$$

Le point $P_0 = (0, 0)$ est d'ordre 8 et le point

$$N = \left(2v(v-1)(v^2+2)(v^2-2v+2)^2, -4v^2(v-1)^2(v^2+2)(v^2-2v+2)^2(v^2-2) \right)$$

est d'ordre infini. Pour la dernière assertion, il suffit de spécialiser la valeur de v . Par exemple, si l'on remplace v par 2 dans 2.4.7, on obtient la courbe elliptique :

$$E : y^2 + 49xy - 8250y = x^3 - 150x^2, \quad (3.138)$$

et le point $N = (3300, -277200)$. Il est facile de voir que N est d'ordre infini puisque $[8]N \neq \mathcal{O}$; le théorème de Mazur [Maz78] permet de conclure. Ce qui achève donc la preuve.

Théorème 3.7. — *Il existe une courbe elliptique F définie sur \mathbb{Q} , telle que $F(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ et une courbe elliptique $E_2^{(8)}$ définie sur $\mathbb{Q}(F)$ telle que*

$$\text{Tors}(E_2^{(8)}, \mathbb{Q}(F)) \supseteq \mathbb{Z}/8\mathbb{Z} \text{ et } \text{rang}(E_2^{(8)}, \mathbb{Q}(F)) \geq 2.$$

Remarque 3.3. — *Dans [Lec04], Lecacheux a obtenu un résultat analogue en utilisant une méthode différente.*

Démonstration. — Nous partons de la courbe $\mathcal{E}_1^{(8)}$ obtenue au (3.137).

$$\begin{aligned} \mathcal{E}_1^{(8)} : P(x, y) = & y^2 + (v^2 - 2)^2 xy + 2v(v^2 + 2)(v^2 - 4v + 2)(v^2 - 2v + 2)^3 y \\ & - (x^3 + 2v(v^2 - 4v + 2)(v^2 - 2v + 2)^2 x^2) = 0. \end{aligned}$$

Posons maintenant $Q = [4]P_0$ où $P_0 = (0, 0)$. Nous allons ensuite tracer la droite $L_{\lambda, Q}$ passant par Q avec la pente $\lambda = 4v^2$.

Mis à part le point P_0 , les abscisses des points d'intersection de $L_{\lambda, Q}$ avec la courbe elliptique $\mathcal{E}_1^{(8)}$ sont les solutions de l'équation quadratique

$$\mathcal{Q}(x, v) = \frac{P(x, \lambda(x - x(Q)) + y(Q))}{(x - x(Q))} = 0. \quad (3.139)$$

On montre alors que le discriminant de $\mathcal{Q}(x, v)$ est donné par :

$$\text{Disc}_x \mathcal{Q} = 2^4 v^2 (v^2 - 2v + 2)^2 (v^2 + 2)^2 (v^4 - 4v^3 + 12v^2 - 8v + 4). \quad (3.140)$$

Pour que les deux points d'intersection soient rationnels, il faut et il suffit que ce discriminant soit un carré. Il est donc naturel de considérer la courbe :

$$\Gamma : s^2 = v^4 - 4v^3 + 12v^2 - 8v + 4. \quad (3.141)$$

La courbe Γ est de genre 1 et possède de nombreux points dont $(v, s) = (0, 2)$. Aussi, nous pouvons utiliser le modèle de Weierstrass suivant pour Γ :

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

La courbe E est appelée 256b1 dans la table de Cremona [Cre97] et d'après la même table, le rang de E sur \mathbb{Q} est 1. De plus, $\text{Tors}(E, \mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$. \square

Nous obtenons d'autres résultats en utilisant d'autres droites. Nous citons par exemple les courbes :

$$\{1088m1, 1904d1, 2624a1, 640b2, 2624a1, 640g1\} \quad (3.142)$$

dont le groupe de Mordell–Weil est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. Ces courbes elliptiques paramétrisent d'autres familles courbes elliptiques sur \mathbb{Q} avec une partie torsion contenant $\mathbb{Z}/8\mathbb{Z}$ et dont le rang est au moins 2. Notons aussi que la courbe elliptique

$$192a2 : y^2 = x^3 - x^2 - 9x + 9$$

de groupe de Mordell–Weil à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}$ paramétrise une famille de courbes elliptiques sur \mathbb{Q} , de rang au moins 2 et de sous-groupe de torsion isomorphe à $\mathbb{Z}/8\mathbb{Z}$.

Nous renvoyons le lecteur à l'annexe B pour les points et les pentes choisies et les familles correspondantes.

Théorème 3.8. — Soit $K = \mathbb{Q}(a)$, alors il existe une courbe elliptique $\mathcal{S}^{(1,1)}$ définie sur K , telle que

$$\text{rang}(\mathcal{S}^{(1,1)}, K) \geq 1 ,$$

et une courbe elliptique $\mathcal{S}^{(1,8)}$ définie sur $K(F)$ telle que

$$\text{Tors}(\mathcal{S}^{(1,8)}, K(F)) \supseteq \mathbb{Z}/8\mathbb{Z} \text{ et } \text{rang}(\mathcal{S}^{(1,8)}, K(\mathcal{S}^{(1,1)})) \geq 1 .$$

Démonstration. — Considérons la courbe elliptique sur $\mathbb{Q}(t)$:

$$\mathcal{E}^{(8)} : y^2 + (2t^2 + 4t + 1)xy - t^3(t+1)(2t+1)y = x^3 - t^2(t+1)(2t+1)x^2 \quad (3.143)$$

Le point $P_0 = (0, 0)$ est un point d'ordre 8 (voir 2.4.7). Nous considérons aussi la droite passant par P_0 et de pente $\lambda = at^2$ où a est une indéterminée. Considérons l'intersection de la droite avec la courbe elliptique $\mathcal{E}^{(8)}$. Mis à part le point P_0 , les abscisses des deux autres points de cette intersection sont les solutions de l'équation quadratique :

$$Q(x) = -x^2 + ((a^2 + 2a + 2)t^4 + (4a + 3)t^3 + (a + 1)t^2)x - at^5(t+1)(2t+1) = 0 \quad (3.144)$$

Le discriminant de $Q_{a,t}$ est :

$$\begin{aligned} \text{Disc}_x(Q) &= ((a^2 + 2a + 2)^2 t^4 + (8a^3 + 22a^2 + 20a + 12)t^3 \\ &\quad + (8a^3 + 22a^2 + 20a + 12)t^2 + (8a^2 + 10a + 6)t + (a + 1)^2)t^4 . \end{aligned}$$

La courbe $\Lambda^{(1,2)}/\mathbb{Q}(a)$ de genre 1 dont $(Y, t) = (a + 1, 0)$ est un point particulier. On utilise ensuite son modèle de Weierstrass :

$$\Lambda^{(1,1)} : Y^2 = \mathcal{F}_a(t) = t^{-4} \text{Disc}_x(Q)$$

Cela définit une courbe elliptique dont un modèle de Weierstrass est :

$$\begin{aligned} \mathcal{S}^{(1,1)} : s^2 = x^3 - 2^{-4}3^{-1}(16a^6 - 32a^5 - 16a^3 + 24a^2 - 8a + 1)x \\ - 2^{-5}3^{-3}(64a^9 - 192a^8 + 96a^7 - 280a^6 + 48a^5 - 120a^4 + 136a^3 - 60a^2 + 12a - 1). \end{aligned} \quad (3.145)$$

On trouve que le point

$$P_G = \left(-\frac{4a^5 + 4a^4 + 12a^3 + 3a^2 + 2a - 1}{12(a+1)^2}, -\frac{a^3(a^3 - a^2 - 2a - 2)}{2(a+1)^3} \right). \quad (3.146)$$

est d'ordre infini sur $\mathcal{S}^{(1,1)}(\mathbb{Q}(a))$. En effet, si l'on fait $a = 3$ dans (3.145) et dans (3.146), on obtient la courbe elliptique :

$$E : y^2 = x^3 - \frac{3649}{48}x - \frac{10943}{864},$$

ainsi que le point

$$P_g = \left(-\frac{413}{48}, -\frac{135}{64} \right),$$

qui est d'ordre infini ($P_g \notin \text{Tors}(E, \mathbb{Q})$). Par conséquent, le rang de $\mathcal{S}^{(1,1)}$ sur $\mathbb{Q}(a)$ est au moins 1. \square

Si l'on prend maintenant un point $P = (x_P, y_P)$ sur $\mathcal{S}^{(1,1)}$, alors, en suivant la méthode vue au paragraphe 3.2.3, on obtient le point (t_P, Y_P) correspondant sur la quartique $\Lambda^{(1,1)}$ avec :

$$t_P = \frac{-24(a+1)^2 x_P - 8a^5 - 8a^4 - 24a^3 - 6a^2 - 4a + 2}{(48a^2 + 60a + 36)x_P + 16a^5 + 16a^4 + 20a^3 + 4a^2 + (-24y_P + 7)a + (-24y_P - 3)} \quad (3.147)$$

L'équation de la courbe elliptique $\mathcal{S}_P^{(1,8)}$ s'obtient en remplaçant t par t_P dans l'expression de $\mathcal{E}^{(8)}$ (voir (3.143)). On obtient aussi les abscisses des deux autres points d'intersection :

$$\frac{((a^2 + 2a + 2)t_P^2 + (4a + 3)t_P + (a + 1) \pm Y_P)t_P^2}{2}. \quad (3.148)$$

Illustrons maintenant ce théorème par des exemples.

Exemples. — Le point $P_2 = [2]P_G$ correspond à un point (t_{P_2}, Y_{P_2}) sur $\Lambda^{(1,1)}(\mathbb{Q}(a))$ où :

$$t_{P_2} = \frac{(a+1)^2(a^3 - a^2 - 2a - 2)}{a^5 + 5a^4 + 12a^3 + 13a^2 + 8a + 2}. \quad (3.149)$$

Nous obtenons l'équation de la courbe elliptique $\mathcal{S}_{P_2}^{(1,8)}$ en remplaçant t par t_{P_2} dans l'expression de $\mathcal{E}^{(8)}$ (voir 3.143). Le rang de $\mathcal{S}_{P_2}^{(1,8)}$ sur $\mathbb{Q}(a)$ est au moins 1 et voici un point d'ordre infini :

$$R_2 = \frac{a(a+1)^5(a^2 + 2a + 2)(a^3 - a^2 - 2a - 2)^2(a^3 + a^2 - 1)}{(a^5 + 5a^4 + 12a^3 + 13a^2 + 8a + 2)^3} \cdot \frac{a^2(a+1)^9(a^2 + 2a + 2)(a^3 - a^2 - 2a - 2)^4(a^3 + a^2 - 1)}{(a^5 + 5a^4 + 12a^3 + 13a^2 + 8a + 2)^5} \quad (3.150)$$

En effet, si l'on remplace la valeur de a par 3 dans (3.149), on obtient $t = \frac{32}{223}$ puis en substituant dans (3.143), on obtient la courbe elliptique :

$$E : y^2 + \frac{80321}{49729}xy - \frac{2398126080}{551473077343}y = x^3 - \frac{74941440}{2472973441}.$$

Le point R_2 obtenu devient

$$N = \left(\frac{1462272}{11089567}, \frac{4492099584}{551473077343} \right). \quad (3.151)$$

Ce point est d'ordre infini puisqu'il n'est pas de torsion.

Prenons maintenant un autre point de $\mathcal{S}^{(1,1)}(\mathbb{Q}(a))$. Choisissons par exemple le point $P_{-2} = [-2]P_G$. Le point P_{-2} correspond au point $(t_{P_{-2}}, Y_{P_{-2}})$ sur $\Lambda^{(1,1)}$ où :

$$t_{P_{-2}} = -(a+1)^2(a^3 - a^2 - 2a - 2)(a+2)^{-1}(a^2 + a + 1)^{-1} \\ \times (5a^{10} + 32a^9 + 90a^8 + 136a^7 + 94a^6 - 48a^5 - 184a^4 - 208a^3 - 132a^2 - 48a - 8)^{-1} \\ \times (a^8 + 8a^7 + 31a^6 + 64a^5 + 90a^4 + 89a^3 + 64a^2 + 30a + 8).$$

Lorsque l'on remplace t par $t_{P_{-2}}$ dans l'expression de $\mathcal{E}^{(8)}$, nous obtenons la courbe elliptique $\mathcal{S}_{P_{-2}}^{(1,8)}$ de rang au moins 1. Les points d'abscisse

$$\begin{aligned}
x_{-2} &= a(a+1)^5(a^3 - a^2 - 2a - 2)^3(a+2)^{-4}(a^2 + a + 1)^{-4} \\
&\times (5a^{10} + 32a^9 + 90a^8 + 136a^7 + 94a^6 - 48a^5 - 184a^4 - 208a^3 - 132a^2 - 48a - 8)^{-3} \\
&\times (3a^6 + 8a^5 + 10a^4 + 8a^3 + 6a^2 + 4a + 2)(4a^4 + 14a^3 + 21a^2 + 16a + 6) \\
&\times (a^8 + 8a^7 + 31a^6 + 64a^5 + 90a^4 + 89a^3 + 64a^2 + 30a + 8)^2.
\end{aligned}$$

sont d'ordre infini. En effet, il suffit de spécialiser la valeur de a . Faisons $a = 3$ dans les expressions précédentes, on obtient alors $t = -\frac{92896}{960973}$. En remplaçant t dans l'équation de $\mathcal{E}^{(8)}$ (voir (3.143)), on obtient la courbe elliptique :

$$\begin{aligned}
E : y^2 + \frac{583646249129}{923469106729}xy + \frac{539451508012174809969426432}{819513153160466525405129656093} \\
= x^3 - \frac{5807047752456239342592}{852795191082857193079441}.
\end{aligned}$$

On obtient aussi le point d'ordre infini.

$$N = \left(-\frac{8181131253571584}{11536575412708935121}, -\frac{211801310688861539776069632}{10653670991086064830266685529209} \right) \quad (3.152)$$

3.3.3. Familles avec $\text{Tors}(E, \mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. — Soit $\mathcal{E}^{(2,6)}$ la courbe elliptique définie sur $\mathbb{Q}(t)$:

$$\begin{aligned}
\mathcal{E}^{(2,6)} : y^2 + (-t^2 + 4t + 1)xy - t(t-1)(t+1)^2(3t+1)y \\
= x^3 - t(t-1)(t+1)^2x^2. \quad (3.153)
\end{aligned}$$

Le point $P_0 = (0, 0)$ est d'ordre 6 (voir 2.4.13).

Nous commençons par le théorème suivant :

Théorème 3.9. — *Il existe une courbe elliptique E définie sur $\mathbb{Q}(t)$ telle que $\text{Tors}(E, \mathbb{Q}(t)) \supseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ et $\text{rang}(E, \mathbb{Q}(t)) \geq 1$.*

Dans [Kul03],[Lec03a],[Cam97] et [Duj07], les auteurs ont donné chacun une construction différente et explicite d'une courbe ayant cette structure. Nous reprenons ici la démarche de Kulesz [Kul03]. Choisissons la pente $\lambda = 0$ et $Q = [2]P_0 = (x_1, y_1)$.

$$Q = (t^2(t-1)(t+1)^2, t^2(t-1)^2(t+1)^2).$$

On considère l'intersection de la droite horizontale :

$$L_Q : y = y_1 = t^2(t-1)^2(t+1)^2 \quad (3.154)$$

qui passe par Q , avec la courbe $\mathcal{E}^{(2,6)}$. Sauf le point P_0 , les abscisses des points intersection de la droite et de la courbe elliptique, sont solutions de l'équation quadratique

$$\begin{aligned}\mathcal{Q}(x, t) &= \frac{P(x, y_1)}{(x - x_1)} \\ &= -x^2 - t^2(t - 1)^2(t + 1)^2(t^2 - 4t + 1) = 0.\end{aligned}$$

Pour obtenir de nouveaux points rationnels, nous considérons maintenant la courbe d'équation :

$$\Gamma_Q : s^2 = \mathcal{F}(t) = -t^2 + 4t + 1. \quad (3.155)$$

C'est une courbe de genre 0 que l'on peut paramétrer par :

$$(s, t) = \left(\frac{-2v^2 + 2v + 2}{v^2 + 1}, \frac{3v^2 + 4v + 1}{v^2 + 1} \right).$$

On obtient alors la courbe elliptique :

$$\begin{aligned}\mathcal{S}_1^{(2,6)} : y^2 + \frac{4(v^2 - v - 1)^2}{(v^2 + 1)^2}xy \\ - 16 \frac{v(v + 1)(v + 2)(3v + 1)(2v^2 + 2v + 1)^2(5v^2 + 6v + 2)}{(v^2 + 1)^5}y \\ = x^3 - 8 \frac{v(v + 1)(v + 2)(3v + 1)(2v^2 + 2v + 1)^2}{(v^2 + 1)^4}x^2.\end{aligned}$$

On peut utiliser le modèle plus simple :

$$\begin{aligned}\mathcal{S}_1^{(2,6)} : y^2 + 4(v^2 - v - 1)^2xy \\ - 16v(v + 1)(v + 2)(3v + 1)(2v^2 + 2v + 1)^2(5v^2 + 6v + 2)(v^2 + 1)y \\ = x^3 - 8v(v + 1)(v + 2)(3v + 1)(2v^2 + 2v + 1)^2x^2.\end{aligned}$$

Le point N suivant est d'ordre infini

$$\begin{aligned}N = \left(8v(v + 1)(v + 2)(3v + 1)(v^2 - v - 1)(2v^2 + 2v + 1), \right. \\ \left. 16v^2(v + 1)^2(v + 2)^2(3v + 1)^2(2v^2 + 2v + 1)^2 \right) \quad (3.156)\end{aligned}$$

Pour prouver la dernière assertion, il suffit de spécialiser la valeur de v . Prenons par exemple $v = 2$ dans 3.156. On obtient alors la courbe elliptique :

$$E : y^2 + 4xy - 77226240y = x^3 - 227136x^2. \quad (3.157)$$

et le point $N = (17472, 76317696)$. Par un calcul direct, on montre que $[6]N \neq \mathcal{O}$. Le théorème de Mazur [**Maz78**] permet de conclure que N est d'ordre infini.

Poursuivons notre but de trouver des courbes de rang élevé. Nous pouvons maintenant partir de la courbe elliptique $\mathcal{S}_{(1)}^{(2,6)}$ (3.156). Nous avons alors :

Théorème 3.10. — *Il existe une courbe elliptique F définie sur \mathbb{Q} , telle que $F(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^2$ et une courbe elliptique $E_2^{(2,6)}$ définie sur $\mathbb{Q}(F)$ telle que $\text{Tors}(E_2^{(2,6)}, \mathbb{Q}(F)) \supseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ et $\text{rang}(E_2^{(2,6)}, \mathbb{Q}(F)) \geq 2$.*

Remarque 3.4. — *Dans [Lec03a] et par une méthode différente, Lecacheux obtient un résultat du même genre, sauf que la courbe elliptique paramétrisante est de rang 1.*

Démonstration. — Nous partons de la courbe elliptique obtenue ci-dessus

$$\begin{aligned} \mathcal{S}_{(1)}^{(2,6)} : P(x, y) = & y^2 + 4(v^2 - v - 1)^2 xy \\ & - 16v(v+1)(v+2)(3v+1)(2v^2 + 2v + 1)^2(5v^2 + 6v + 2)(v^2 + 1)y \\ & - (x^3 - 8v(v+1)(v+2)(3v+1)(2v^2 + 2v + 1)^2 x^2) = 0 . \end{aligned}$$

Nous utilisons la même méthode et nous choisissons alors la pente

$$\lambda_2 = 2v^4 + 4v^3 + 2v^2 + 4v .$$

Prenons aussi comme point de départ, le point $Q_2 = [4]P_0$

$$Q_2 = \left(8v(v+1)(v+2)(3v+1)(2v^2 + 2v + 1)^2, 0 \right)$$

Mis à part le point P_0 , les abscisses des points N_1 et N_2 , intersection de $L_{\lambda, Q}$ avec $\mathcal{E}_{\lambda, Q_1}^{(7)}$, sont solutions de l'équation quadratique

$$\mathcal{Q}(x, v) = \frac{P(x, \lambda(x - x(Q_2)) + y(Q_2))}{(x - x(Q_2))} = 0 . \quad (3.158)$$

Pour que les deux points d'intersection soient rationnels, il faut que ce discriminant soit un carré. On obtient ainsi la courbe paramétrisante

$$\Gamma_{Q_2} : s^2 = \mathcal{F}(t) = -3(7v^2 + 10v + 2)(3v^2 + 2v + 2). \quad (3.159)$$

Cette courbe possède le point trivial $(v, s) = (-1, 3)$. Nous utilisons alors le modèle de Weierstrass :

$$(39600bu1) : y^2 = x^3 + 105x - 650. \quad (3.160)$$

dont le rang sur \mathbb{Q} est 2, d'après la table [Cre97]. Les deux points

$$N_1 = (6, 14) \text{ et } N_2 = (9, 32)$$

sont d'ordre infini et indépendants. □

Nous obtenons d'autres résultats en utilisant d'autres droites. Nous citons par exemples les courbes :

$$\{360e2, 800a1, 1160c2\} \quad (3.161)$$

dont les groupes de Mordell–Weil sont tous isomorphes à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}$. Ces courbes elliptiques paramétrisent, des familles de courbes elliptiques sur \mathbb{Q} avec une partie de torsion contenant $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ et dont le rang est au moins 2.

Notons aussi la courbe elliptique 190a1 d'équation

$$190a1 : y^2 + xy + y = x^3 - x^2 - 48x + 147 ,$$

de groupe de Mordell–Weil isomorphe à \mathbb{Z} (torsion triviale) qui est aussi une paramétrisante pour la structure $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ et rang au moins 2.

Voir l'annexe B pour les points et les pentes choisies.

Théorème 3.11. — *Soit $K = \mathbb{Q}(a)$, alors il existe une courbe elliptique \mathcal{S} définie sur K , telle que*

$$\text{rang}(\mathcal{S}, K) \geq 1 ,$$

et une courbe elliptique $\mathcal{S}^{(2,6)}$ définie sur $K(\mathcal{S})$ telle que

$$\text{Tors}(\mathcal{S}^{(2,6)}, K(\mathcal{S})) \supseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \text{ et } \text{rang}(\mathcal{S}^{(2,6)}, K(\mathcal{S})) \geq 1 .$$

Démonstration. — Considérons la courbe elliptique sur $\mathbb{Q}(t)$:

$$\mathcal{E}^{(2,6)} : y^2 + (-t^2 + 4t + 1)xy - t(t-1)(t+1)^2(3t+1)y = x^3 - t(t-1)(t+1)^2x^2$$

On a vu au paragraphe (2.4.13) que les points

$$P_0 = (0, 0) \text{ et } Q = \left(\frac{3}{4}(t-1)(3t+1)(t+1)^2, \frac{3}{8}(t-1)^2(3t+1)(t+1)^3 \right),$$

sont respectivement d'ordre 6 et d'ordre 2. De plus :

$$\langle Q, P_0 \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} .$$

Soit maintenant la droite passant par P_0 et de pente $\lambda = a(t+1)(t-1)$ où a est une indéterminée. Considérons l'intersection de cette droite avec la courbe elliptique $\mathcal{E}^{(2,6)}$. Mis à part le point $P_0 = (0, 0)$, les abscisses des deux autres points de cette intersection sont les solutions de l'équation quadratique :

$$\begin{aligned} Q_{a,t}(x) = & -x^2 + -x^2 + ((a^2 - a + 1)t^4 + (4a + 1)t^3 + (-2a^2 + 2a - 1)t^2 \\ & + (-4a - 1)t + (a^2 - a))x - 3at(t-1)^2(t+1)^3(3t+1) = 0 \end{aligned}$$

Le discriminant de $Q_{a,t}$ est :

$$\begin{aligned} \text{Disc}_x(Q) &= ((a^2 - a + 1)^2 t^4 + (8a^3 - 6a^2 - 6a + 2)t^3 \\ &+ (-2a^4 + 4a^3 + 12a^2 - 6a + 1)t^2 - 2a(4a^2 - 3a + 1)t + a^2(a - 1)^2)t^2(t - 1)^2. \end{aligned}$$

Pour que les racines soient rationnelles, nous imposons ensuite que $\text{Disc}_x(Q_{a,t}(x))$ soit un carré dans le corps $\mathbb{Q}(a)$. On considère alors la courbe définie sur $\mathbb{Q}(a)$ par :

$$\Lambda^{(1,1)} : Y^2 = \mathcal{F}_a(t) = (t + 1)^{-2}(t - 1)^{-2} \text{Disc}_x(Q_{a,t}(x))$$

Comme la courbe $\Lambda^{(1,1)}$ est de genre 1 avec point trivial $(Y, t) = (a(a - 1), 0)$, on peut donc utiliser sa forme de Weierstrass réduite :

$$\begin{aligned} \mathcal{S}^{(1,1)} : s^2 &= x^3 - 2^{-4}3^{-1}(16a^8 - 64a^7 + 256a^6 - 288a^5 + 200a^4 - 64a^3 + 1)x \\ &+ 2^{-5}3^{-3}(64a^{12} - 384a^{11} + 1920a^{10} - 4544a^9 + 8112a^8 \\ &- 6240a^7 + 1920a^6 - 432a^5 + 300a^4 - 96a^3 + 1) \end{aligned}$$

Il est facile de vérifier que le point

$$P_G = \left(\frac{(4a^6 - 16a^5 + 44a^4 - 20a^3 + a^2 - 2a + 1)}{12(a - 1)^2}, \frac{a^3(a + 1)(2a - 1)^2}{2(a - 1)^3} \right)$$

est d'ordre infini. □

Illustrons maintenant le théorème par des exemples explicites.

Exemple. — Le point $P_2 = [2]P_G$ correspond au point (t_{P_2}, Y_{P_2}) sur $\Lambda^{(1,1)}$ avec :

$$t_{P_2} = -\frac{(a - 1)^2(a + 1)}{a^3 - 4a^2 + 7a - 3}. \quad (3.162)$$

En remplaçant t par t_{P_2} dans $\mathcal{E}^{(2,6)}$, on obtient la courbe elliptique :

$$\begin{aligned} \mathcal{S}_{P_1}^{(2,6)} : y^2 &- \frac{4a^6 - 14a^5 + 9a^4 + 46a^3 - 106a^2 + 80a - 20}{(a^3 - 4a^2 + 7a - 3)^3}xy \\ &+ \frac{(a - 2)^2(a - 1)^2(a + 1)(2a - 3)(2a - 1)(3a - 2)^2(a^2 - 2a + 2)(a^2 + 2a - 2)}{(a^3 - 4a^2 + 7a - 3)^5}y \\ &= x^3 - \frac{(a - 2)^2(a - 1)^2(a + 1)(2a - 1)(3a - 2)^2(a^2 - 2a + 2)}{(a^3 - 4a^2 + 7a - 3)^4}x^2. \end{aligned}$$

Nous trouvons aussi le point d'ordre infini

$$R_1 = \left(\frac{a(a-2)^2(a-1)(2a-1)(2a-3)(3a-2)(a^2-2a+2)}{(a^3-4a^2+7a-3)^3}, \frac{a^2(a-2)^3(a-1)(2a-1)^2(2a-3)(3a-2)^2(a^2-2a+2)^2}{(a^3-4a^2+7a-3)^5} \right). \quad (3.163)$$

Théorème 3.12. — Soit $K = \mathbb{Q}(a)$, alors il existe une courbe elliptique $\mathcal{S}^{(1,2)}$ définie sur K , telle que

$$\text{Tors}(\mathcal{S}^{(1,2)}, K) \supseteq \mathbb{Z}/2\mathbb{Z}, \text{rang}(\mathcal{S}^{(1,2)}, K) \geq 1,$$

et une courbe elliptique $\mathcal{S}^{(2,6)}$ définie sur K ($\mathcal{S}^{(1,2)}$) telle que

$$\text{Tors}(\mathcal{S}^{(2,6)}, K(\mathcal{S}^{(1,2)})) \supseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \text{ et } \text{rang}(\mathcal{S}^{(2,6)}, K(\mathcal{S}^{(1,2)})) \geq 1.$$

Démonstration. — Considérons la courbe elliptique sur $\mathbb{Q}(t)$:

$$\mathcal{E}^{(2,6)} : y^2 + (-t^2 + 4t + 1)xy - t(t-1)(t+1)^2(3t+1)y = x^3 - t(t-1)(t+1)^2x^2$$

Nous avons vu au paragraphe (2.4.13) que les points

$$P_0 = (0, 0) \text{ et } Q = \left(\frac{3}{4}(t-1)(3t+1)(t+1)^2, \frac{3}{8}(t-1)^2(3t+1)(t+1)^3 \right),$$

sont d'ordre 6 et 2 respectivement et de plus $\langle Q, P_0 \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

Soit maintenant la droite passant par P_0 et de pente $\lambda = at(t-1)$ où a est une nouvelle indéterminée. Considérons l'intersection de cette droite avec la courbe elliptique $\mathcal{E}^{(2,6)}$. Mis à part le point $P_0 = (0, 0)$, les deux autres points de cette intersection ont leurs abscisses racines de la forme quadratique :

$$Q_{a,t}(x) = -x^2 + ((a^2 - a + 1)t^4 + (-2a^2 + 5a + 1)t^3 + (a^2 - 3a - 1)t^2 + (-a - 1)t)x - at^2(t+1)^2(t-1)^2(3t+1) \quad (3.164)$$

Le discriminant de $Q_{a,t}$ est :

$$\text{Disc}_x(Q) = ((a^2 - a + 1)^2t^4 + (-2a^4 + 10a^3 - 6a^2 - 8a + 4)t^3 + (a^4 - 6a^3 + 12a^2 - 12a + 6)t^2 - 2(a-1)(a^2 - 2a + 2)t + (a-1)^2)t^2(t-1)^2.$$

Pour que les deux autres points d'intersection soient rationnels, il faut et il suffit que $\text{Disc}_x(Q_{a,t})$ soit un carré dans $\mathbb{Q}(a)$. On considère alors la courbe définie sur $\mathbb{Q}(a)$:

$$\Lambda^{(2)} : Y^2 = \mathcal{F}_a(t) = t^{-2}(t-1)^{-2} \text{Disc}_x(Q_{a,t}(x)).$$

C'est une courbe de genre 1 avec point trivial $(Y, t) = (a-1, 0)$. Nous utilisons ensuite le modèle de Weierstrass :

$$\mathcal{S}^{(1,2)} : s^2 = x^3 - 2^{-4}3^{-1}a^2(a^6 - 24a^5 + 168a^4 - 480a^3 + 720a^2 - 576a + 192)x + 2^{-5}3^{-3}a^4(a^2 - 12a + 12)(a^6 - 24a^5 + 168a^4 - 576a^3 + 1008a^2 - 864a + 288)$$

Le point

$$P_2 = \left(\frac{a^2(a^2 - 12 + 12)}{12}, 0 \right)$$

est d'ordre 2 et le point

$$P_G = \left(\frac{1}{12}a^4, \frac{1}{2}a^2(a-2)^2(a-1) \right) \quad (3.165)$$

est d'ordre infini. Pour cela, nous spécialisons la valeur de a . Faisons alors $a = 3$ dans (3.3.3). Nous obtenons alors la courbe elliptique :

$$E : y^2 = x^3 - \frac{1467}{16}x + \frac{12555}{32},$$

et le point

$$N = \left(\frac{27}{4}, 9 \right)$$

qui est d'ordre infini ($N \notin \text{Tors}(E, \mathbb{Q})$). Il en résulte que le rang de la courbe paramétrisante $\mathcal{S}_a^{(1,2)}$ sur $\mathbb{Q}(a)$ est au moins 1. \square

Illustrons maintenant ce théorème par des exemples.

Exemples. — Prenons le point $P_3 = [3]P_G$ qui correspond au point (t_{P_3}, Y_{P_3}) dans $\Lambda^{(1)}(\mathbb{Q}(a))$ avec :

$$t_{P_3} = \frac{a^2 - a + 1}{a^2 + 2a - 2}. \quad (3.166)$$

En remplaçant t par t_{P_3} dans l'équation de $\mathcal{E}^{(2,6)}$, on obtient l'expression suivante pour la courbe elliptique sur $\mathbb{Q}(a)$:

$$\begin{aligned} \mathcal{S}_{P_3}^{(2,6)} : y^2 + \frac{4a^4 + 10a^3 - 15a^2 + 10a - 5}{(a^2 + 2a - 2)^2}xy \\ + 3 \frac{(a-1)(a+1)^2(2a-1)^2(a^2-a+1)(4a^2-a+1)}{(a^2+2a-2)^5}y \\ = x^3 + 3 \frac{(a-1)(a+1)^2(2a-1)^2(a^2-a+1)}{a^2+2a-2}x^2. \end{aligned} \quad (3.167)$$

Le point R_3 suivant est dans $\mathcal{S}_{P_3}^{(1,2)}(\mathbb{Q}(a))$ et est d'ordre infini :

$$R_3 = \left(-3 \frac{a(a-1)(a+1)^2(a^2-a+1)}{(a^2+2a-2)^3}, 9 \frac{a^2(a-1)^2(a+1)^2(a^2-a+1)^2}{(a^2+2a-2)^5} \right) \quad (3.168)$$

En effet, il suffit de spécialiser la valeur de a . Faisons alors $a = 3$ dans (3.167) et dans (3.168). On obtient alors la courbe elliptique :

$$E : y^2 + \frac{484}{169}xy + \frac{571200}{371293}y = x^3 + \frac{16800}{28561}x^2,$$

et le point

$$N = \left(-\frac{2016}{2197}, \frac{254016}{371293} \right).$$

Ce point est d'ordre infini ($N \notin \text{Tors}(E, \mathbb{Q})$).

3.3.4. Familles avec $\text{Tors}(E, \mathbb{Q}) \supseteq \mathbb{Z}/9\mathbb{Z}$. — La forme des courbes elliptiques ayant cette structure a déjà été donnée par Kubert ([**Kub76**]). Mais on ne connaît pas à l'heure actuelle de courbe elliptique sur $\mathbb{Q}(t)$ de rang au moins 1 qui possède cette structure de torsion. Il existe des courbes elliptiques de rang 1 qui paramétrisent une telle structure et de rang au moins 1 (voir [**AM93**] ou [**Kul03**]).

Nous donnons plusieurs nouvelles courbes elliptiques de rang 1 et 2 qui paramétrisent de telles familles de courbes elliptiques avec un point d'ordre 9 (voir l'annexe B pour les points et les pentes utilisés).

Théorème 3.13. — *Il existe une courbe elliptique F définie sur \mathbb{Q} , telle que $F(\mathbb{Q}) \simeq \mathbb{Z}^2$ et une courbe elliptique $E_2^{(9)}$ définie sur $\mathbb{Q}(F)$ telle que*

$$\text{Tors}(E_2^{(9)}, \mathbb{Q}(F)) \supseteq \mathbb{Z}/9\mathbb{Z} \text{ et } \text{rang}(E_2^{(9)}, \mathbb{Q}(F)) \geq 1.$$

Démonstration. — Nous partons de la forme générale des courbes elliptiques avec un point d'ordre 9, donnée par l'équation :

$$\begin{aligned} \mathcal{E}^{(9)} : P(x, y) = y^2 + (-t^3 + t^2 + 1)xy - t^2(t-1)(t^2 - t + 1)y \\ - (x^3 - t^2(t-1)(t^2 - t + 1)x^2) = 0. \end{aligned}$$

Le point $P_0 = (0, 0)$ est d'ordre 9 (voir paragraphe (2.4.8)).

Choisissons la pente $\lambda = 4t(t-1)$ et le point de départ $Q_1 = [7]P_0 = (x_1, y_1) = (t^2(t-1)(t^2 - t + 1))$. Ensuite, on considère l'intersection de la droite $L_{\lambda, Q}$ qui passe par Q et de pente λ , avec la courbe $\mathcal{E}^{(9)}$.

$$L_{\lambda, Q} : y = \lambda(x - x_1) + y_1.$$

Mis à part le point Q , les abscisses des deux autres points de l'intersection ont leurs abscisses solutions de l'équation quadratique :

$$\mathcal{Q}_t(x) = \frac{P(x, y_1)}{(x - x_1)} = -x^2 - 4t(t-1)(t^3 - 5t^2 + 4t - 1)x - 16t^3(t-1)^2(2t-1)^2(t^2 - t - 1) = 0$$

Le discriminant de $\mathcal{Q}_{t,\lambda}$ est :

$$\text{Disc}_x(\mathcal{Q}_t) = 16t^2(t-1)^4(t^4 - 12t^3 + 16t^2 - 7t + 1).$$

Pour que les deux autres points d'intersection soient rationnels, il faut et il suffit que le discriminant $\text{Disc}_x(\mathcal{Q}_t)$ soit un carré. Nous considérons alors la courbe paramétrisante d'équation :

$$\Gamma_Q : s^2 = \mathcal{F}(t) = (t^4 - 12t^3 + 16t^2 - 7t + 1).$$

Cette quartique est une courbe de genre 1 avec le point trivial $(t, s) = (0, 1)$. Nous utilisons sa forme de Weierstrass :

$$F : y^2 = x^3 + x^2 - 5x + 4$$

La courbe E est connue sous le nom (1132a1) dans la table de Cremona [Cre97]. Dans cette table, on trouve que le rang de 1132a1 sur \mathbb{Q} est 2, puis on a 2 points d'ordre infini et indépendants :

$$N_1 = (-1, 3) \text{ et } N_2 = (0, 2).$$

Ce qui achève la preuve. □

En choisissant d'autres droites, nous obtenons que les 9 courbes elliptiques suivants sont de rang 1 et paramétrisent chacune, une famille de courbes elliptiques de rang (sur \mathbb{Q}) au moins 1 et dont la partie de torsion est au moins $\mathbb{Z}/9\mathbb{Z}$:

$$141d1, 324c1, 408d1, 43a1, 53a1, 58a1, 606e1, 92b1, 99a1$$

Nous remarquons que la partie torsion de 324c1 et 54b1 est isomorphe à $\mathbb{Z}/3\mathbb{Z}$, celle de 99a1 est $\mathbb{Z}/2\mathbb{Z}$ et les autres courbes paramétrisantes n'ont pas de points de torsion non trivial.

Nous renvoyons le lecteur aux tableaux de l'annexe B pour les droites utilisées ainsi que les équations des paramétrisantes obtenues.

3.3.5. Familles avec $\text{Tors}(E, \mathbb{Q}) \supseteq \mathbb{Z}/10\mathbb{Z}$. — Comme pour le cas où l'on a un point d'ordre 9, la forme des courbes elliptiques ayant un point d'ordre 10 est connue depuis Kubert ([**Kub76**]). A l'heure actuelle, on ne connaît pas de courbe elliptique sur $\mathbb{Q}(t)$ de rang au moins 1 qui possède un point d'ordre 10. Néanmoins, on sait qu'il existe des courbes elliptiques de rang 1 qui paramétrisent des familles de courbes elliptiques ayant une telle structure et de rang au moins 1 ([**AM93**] ou [**Kul03**]).

Nous donnons plusieurs nouvelles courbes elliptiques de rang 1 et 2 qui paramétrisent des courbes elliptiques avec un point d'ordre 10 et un point d'ordre infini (voir l'annexe B pour les points et les pentes utilisées).

Théorème 3.14. — *Il existe une courbe elliptique F définie sur \mathbb{Q} avec $F(\mathbb{Q}) \simeq \mathbb{Z}^2$ et une courbe elliptique $E_2^{(10)}$ définie sur $\mathbb{Q}(F)$ telle que $\text{Tors}(E_2^{(10)}, \mathbb{Q}(F)) \supseteq \mathbb{Z}/10\mathbb{Z}$ et $\text{rang}(E_2^{(10)}, \mathbb{Q}(F)) \geq 1$.*

Démonstration. — Nous partons de la forme générale des courbes elliptiques avec un point d'ordre 10, donnée par l'équation :

$$\begin{aligned} \mathcal{E}^{(10)} : P(x, y) = y^2 + \frac{2t^3 + 2t^2 + 2t + 1}{(t+1)^2}xy \\ + \frac{t^2(2t+1)}{(t+1)^2}y - \left(x^3 + \frac{t^2(2t+1)}{(t+1)^2}x^2\right) = 0. \end{aligned}$$

Pour plus de détail sur cette courbe, voir [**Kul03**]. Le point $P_0 = (0, 0)$ est d'ordre 5.

Choisissons maintenant la pente $\lambda = -4t + 3$ et le point de départ $Q_1 = [2]P_0$

$$Q_1 = \left(\frac{-t^2(2t+1)}{(t+1)^2}, \frac{t^4(2t+1)^2}{(t+1)^4} \right)$$

En procédant comme avant, nous considérons l'intersection passant par Q_1 et de pente λ avec la courbe $\mathcal{E}^{(10)}$, ainsi on obtient l'équation :

$$\mathcal{Q}(x, t) = \frac{P(x, \lambda(x - x(Q_1)) + y(Q_1))}{(x - x(Q_1))} = 0. \quad (3.169)$$

Pour que les deux autres points d'intersection soient rationnels, il faut et il suffit que le discriminant de \mathcal{Q} soit un carré dans le corps considéré.

Nous obtenons ainsi la courbe elliptique paramétrisante :

$$\Gamma_{\mathcal{Q}} : s^2 = \mathcal{F}(t) = 16t^4 + 96t^3 + 193t^2 + 140t + 36.$$

Cette courbe est de genre 1 avec le point $(t, s) = (0, 6)$ et est isomorphe sur \mathbb{Q} à la courbe

$$F : y^2 + xy = x^3 - 80x + 256.$$

La courbe elliptique E est connue sous le nom 2918b1 dans la table de Cremona [Cre97]. Dans cette même table, on trouve que le rang de la courbe 2918b1 sur \mathbb{Q} est 2 puis ensuite les points :

$$P_1 = \left(-\frac{80}{49}, \frac{6992}{343} \right) \text{ et } P_2 = (-6, 26).$$

sont d'ordre infini et indépendants. □

Parmi les courbes elliptiques de rang 2 qui paramétrisent une famille de courbes elliptiques avec une torsion $\mathbb{Z}/10\mathbb{Z}$ et de rang au moins 1, nous citerons :

$$1324a1, 1576a1, 2918b1, 5830f1.$$

Nous remarquons alors que les sous-groupes de torsion de ces courbes elliptiques sont triviaux. Notons aussi les courbes paramétrisantes de rang 1 suivantes :

$$102a1, 123b1, 128a1, 148a1, 158a1, 163a1, 176c1, 214a1, 219b1, \\ 248c1, 366g1, 430d1, 43a1, 528a2, 65a1, 79a1, 88a1, 912i1$$

Nous renvoyons le lecteur à l'annexe B pour les équations des courbes paramétrisantes ainsi que les droites utilisées.

3.3.6. Familles avec $\text{Tors}(E, \mathbb{Q}) \supseteq \mathbb{Z}/12\mathbb{Z}$. — Dans cette section, Nous donnons 6 courbes elliptiques de rang 1 sur \mathbb{Q} qui paramétrisent des courbes elliptiques avec un point d'ordre 12 (voir l'annexe B pour les points et les pentes utilisées).

Théorème 3.15. — *Il existe une courbe elliptique F définie sur \mathbb{Q} , telle que $F(\mathbb{Q}) \simeq \mathbb{Z}^2$ et une courbe elliptique $E_2^{(12)}$ définie sur $\mathbb{Q}(F)$ telle que*

$$\text{Tors}(E_2^{(12)}, \mathbb{Q}(F)) \supseteq \mathbb{Z}/12\mathbb{Z} \text{ et } \text{rang}(E_2^{(12)}, \mathbb{Q}(F)) \geq 1.$$

Remarque 3.5. — *Kulesz [Kul03] obtient un résultat du même genre, sauf que sa courbe elliptique paramétrisante est de rang 1.*

Démonstration. — Nous partons de la forme générale des courbes elliptiques avec un point d'ordre 12, donnée par l'équation :

$$\begin{aligned} \mathcal{E}^{(12)} : P(x, y) = & y^2 + \frac{6t^4 - 8t^3 + 2t^2 + 2t - 1}{(t-1)^3}xy \\ & + \frac{-12t^6 + 30t^5 - 34t^4 + 21t^3 - 7t^2 + t}{(t-1)^4}y \\ & - \left(x^3 + \frac{-12t^6 + 30t^5 - 34t^4 + 21t^3 - 7t^2 + t}{(t-1)^4}x^2\right) = 0. \end{aligned}$$

Le point $P_0 = (0, 0)$ est d'ordre 12 (voir paragraphe (2.4.10)).

Prenons maintenant comme pente $\lambda = \frac{2t(3t^2-3t+1)}{(t-1)^2}$ et comme point de départ, le point $Q = [2]P_0 = (x_1, y_1)$:

$$Q = \left(\frac{t(2t-1)(2t^2-2t+1)(3t^2-3t+1)}{(t-1)^4}, -\frac{t^2(2t-1)^2(2t^2-2t+1)(3t^2-3t+1)^2}{(t-1)^7} \right).$$

Nous considérons alors l'intersection de la droite $L_{\lambda, Q}$ passant par Q et de pente λ , avec la courbe $\mathcal{E}^{(12)}$. Mis à part le point Q , pour que les points d'intersection soient rationnels, il faut et il suffit que le discriminant de la forme quadratique :

$$\mathcal{Q}(x, t) = \frac{P(x, \lambda(x - x(Q)) + y(Q))}{(x - x(Q))} = 0. \quad (3.170)$$

soit un carré. Procédant comme avant, nous considérons alors la courbe elliptique paramétrisante :

$$\Gamma_{\lambda, Q} : s^2 = \mathcal{F}(t) = -192t^4 + 320t^3 - 160t^2 + 16. \quad (3.171)$$

Cette quartique est une courbe est de genre 1 avec le point trivial $(t, s) = (0, 4)$ et est isomorphe sur \mathbb{Q} à la courbe

$$F : y^2 = x^3 - x^2 + 15x + 1. \quad (3.172)$$

La courbe E est connue sous le nom 1696e1 dans la table de Cremona [Cre97]. Dans cette même table, on trouve que le rang de la courbe 1696e1 sur \mathbb{Q} est 2. Les points

$$P_1 = (0, 1) \text{ et } P_2 = (1, 4),$$

sont d'ordre infini et indépendants. \square

En choisissant d'autres droites, nous obtenons que les 7 courbes elliptiques suivantes sont de rang 1 et paramétrisent chacune une famille de courbes elliptiques de rang sur \mathbb{Q} au moins 1 et dont la partie de torsion est $\mathbb{Z}/12\mathbb{Z}$:

128a1, 148a1, 226a1, 288a2, 344a1, 368d1, 58a1

On renvoie le lecteur à l'annexe B pour les équations des courbes paramétrisantes, ainsi que les droites et points de départ utilisés.

3.3.7. Familles avec $\text{Tors}(E, \mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. — Comme pour le cas où l'on a un point d'ordre 10, la forme des courbes elliptiques ayant un sous-groupe du type $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ est connue depuis Kubert ([**Kub76**]). On ne sait cependant pas s'il est possible de trouver des courbes elliptiques sur $\mathbb{Q}(t)$ de rang au moins 1 qui possèdent cette structure de torsion.

En revanche, le théorème suivant a été démontré par des méthodes différentes (voir [**AM93**], [**Lec03a**] ou Kulesz[**Kul03**]).

Théorème 3.16. — *Il existe une courbe elliptique F définie sur \mathbb{Q} , telle que $F(\mathbb{Q}) \simeq \mathbb{Z}^2$ et une courbe elliptique $E_2^{(2,8)}$ définie sur $\mathbb{Q}(F)$ telle que*

$$\text{Tors}(E_2^{(2,8)}, \mathbb{Q}(F)) \supseteq \mathbb{Z}/2 \times \mathbb{Z}/8\mathbb{Z} \text{ et } \text{rang}(E_2^{(2,8)}, \mathbb{Q}(F)) \geq 1 .$$

Démonstration. — Nous partons de la famille de courbes elliptiques

$$\begin{aligned} \mathcal{E}^{(2,8)} : y^2 + (t^4 - 24t^2 - 64t - 64)xy \\ - 2(t^2 + 4t + 8)(t + 4)(t^2 - 8)(t + 2)^3 t^3 y \\ = x^3 - 2(t^2 + 4t + 8)(t + 4)(t + 2)^2 t^2 x^2, \end{aligned}$$

Le point $P_0 = (0, 0)$ est d'ordre 8 (voir paragraphe(2.4.14)).

Prenons maintenant comme pente $\lambda = 4(t - 1)(t - 4)(t + 4)$ et comme point de départ, le point $Q = [2]P_0 = (x_1, y_1) :$

$$Q = (2t^3(t + 2)^3(t + 4), 4t^4(t + 2)^4(t + 4)^2)$$

Nous considérons alors l'intersection de la droite $L_{\lambda, Q}$ passant par Q et de pente λ , avec la courbe $\mathcal{E}^{(2,8)}$. Mis à part le point Q , pour que les points d'intersection soient rationnels, il faut et il suffit que le discriminant de la forme quadratique :

$$Q(x, v) = \frac{P(x, \lambda(x - x(Q)) + y(Q))}{(x - x(Q))} = 0 . \quad (3.173)$$

soit un carré. Nous considérons alors la courbe elliptique paramétrisante :

$$\Gamma_{\lambda, Q} : s^2 = \mathcal{F}(t) = 2(t - 4)(t + 8)(t^2 + 4t - 4) .$$

Cette quartique est une courbe de genre 1 avec le point $(t, s) = (0, 16)$, et est isomorphe sur \mathbb{Q} à la courbe

$$F : y^2 = x^3 - x^2 - 449x + 3585.$$

La courbe E est connue sous le nom 1344n3 dans la table de Cremona [Cre97]. Dans cette table, on trouve que le rang de la courbe 1344n3 sur \mathbb{Q} est 1 et que le point $(-13, 84)$ est d'ordre infini.

□

En choisissant d'autres droites, nous obtenons que les 5 courbes elliptiques suivantes sont de rang 1 et paramétrisent chacune, une famille de courbes elliptiques de rang au moins 1 et dont la partie torsion est $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$:

$$160a2, 192a2, 448b1, 480f1, 640a2$$

Nous renvoyons le lecteur à l'annexe B pour les équations des courbes paramétrisantes ainsi que les droites utilisées.

3.3.8. Familles de courbes avec $\text{Tors}(E, \mathbb{Q}(\sqrt{-3})) \supseteq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. — Soit $K = \mathbb{Q}(\zeta)$ où $\zeta^2 + \zeta + 1 = 0$. Nous nous intéressons maintenant à la courbe :

$$\mathcal{S}_t : F(x, y, z) = x^3 + y^3 + z^3 + txyz = 0 \quad (3.174)$$

La courbe définie par (3.174) est bien connue (voir par exemple [Bea82] ou [Fri02]). Une courbe elliptique de la forme \mathcal{S}_{t_0} pour une certaine valeur $t_0 \in K$ est dit sous la forme de Hesse. Lorsque l'on fixe un point de base, il est possible de donner explicitement la loi de groupe sur \mathcal{S}_{t_0} (voir par exemple [Cas91] ou [Fri02]).

Soit une courbe projective plane dans \mathbb{P}^2 définie par une équation de la forme $\mathcal{S} : F(x, y, z) = 0$, on définit son Hessien par :

$$\text{Hes}(F) = \begin{vmatrix} \frac{\partial^2 F}{\partial x^2} & \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial x \partial z} \\ \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial y^2} & \frac{\partial^2 F}{\partial y \partial z} \\ \frac{\partial^2 F}{\partial x \partial z} & \frac{\partial^2 F}{\partial y \partial z} & \frac{\partial^2 F}{\partial z^2} \end{vmatrix} \quad (3.175)$$

Remarque 3.6. — La courbe hessienne $\text{Hes}(F) = 0$ d'une cubique plane $F = 0$ de Hesse est aussi une cubique plane de Hesse (voir [Fri02]).

Nous avons maintenant le théorème suivant

Théorème 3.17. — Soit F une courbe de degré $d > 1$ sur k un corps de caractéristique nulle, alors un point P est dans $H(F) \cap F$ si et seulement si P est un point d'inflexion ou un point singulier de F .

En ce qui concerne le cas d'une cubique plane lisse dans $\mathbb{P}^2(K)$, ce théorème caractérise les points d'inflexion de F . Pour le cas d'une courbe sous la forme de Hesse, F et $H(F)$ s'intersectent en exactement 9 points :

$$\begin{array}{lll} Q_1 = (0, 1, -1) & Q_2 = (0, 1, -\zeta) & Q_3 = (0, 1, -\zeta^2) \\ Q_4 = (1, 0, -1) & Q_5 = (1, 0, -\zeta) & Q_6 = (1, 0, -\zeta^2) \\ Q_7 = (1, -1, 0) & Q_8 = (1, -\zeta, 0) & Q_9 = (1, -\zeta^2, 0) \end{array}$$

Supposons que l'on a fixé un point \mathcal{O} de F comme l'élément neutre pour la loi du groupe (\mathcal{O} doit être un point d'inflexion), alors trois points P, Q et R sont tels que $P + Q + R = \mathcal{O}$ si et seulement si ils sont les trois points d'intersection de E avec une droite, en comptant la multiplicité.

Les points Q_i définis plus haut sont d'ordre 3 et donc forment un sous-groupe isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Nous allons maintenant utiliser la famille de cubiques du type Hesse pour construire des familles infinies de courbes elliptiques de partie torsion contenant un sous-groupe isomorphe $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ et dont les rangs sont grands.

Une famille de rang 1. — Considérons \mathcal{S}_t la courbe elliptique définie sur $\mathbb{Q}(t)$ par 3.174. On a le théorème suivant

Théorème 3.18. — Soit K un corps de nombres tel que $K \supseteq \mathbb{Q}(\sqrt{-3})$, alors il existe au moins une famille infinie de courbes elliptiques définies sur K de rang au moins 1 et avec un sous-groupe de torsion :

$$\text{Tors}(E, K) \supseteq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

Démonstration. — Il suffit que l'on impose que t soit un carré : $t = T^2$, on obtient alors la nouvelle courbe elliptique :

$$\mathcal{S} : F(x, y, 1) = x^3 + y^3 + T^2xy + 1 = 0 \quad (3.176)$$

En faisant cela, nous obtenons un point d'ordre infini sur $\mathcal{S}(K(T))$:

$$N_1 = (x_{N_1}, y_{N_1}) = (T, -1) . \quad (3.177)$$

Pour la dernière assertion, il suffit de spécialiser T . Remplaçons T par 2 dans 3.176. On obtient la courbe elliptique

$$E : x^3 + y^3 + 4xy + 1 = 0 . \quad (3.178)$$

et le point $N_1 = (2, 1)$. L'algorithme de van Hoeij [vH97] permet de trouver un modèle de Weierstrass suivant pour E :

$$E' : y^2 = x^3 + \frac{38}{3}x + \frac{4103}{108} , \quad (3.179)$$

ainsi que le point $N'_1 = \left(\frac{43}{12}, \frac{91}{8}\right)$ de E' correspondant à $N_1 \in E$. Il est maintenant facile de montrer que N'_1 n'est pas de torsion donc N'_1 est d'ordre infini. Ce qui achève la preuve. \square

Avec la nouvelle courbe obtenue (voir 3.176), nous obtenons le théorème suivant :

Théorème 3.19. — *Soit $K = \mathbb{Q}(\zeta_3)$, alors il existe une courbe elliptique $\mathcal{S}^{(1,2)}$ définie sur $K(a)$, telle que*

$$\text{Tors}(\mathcal{S}^{(1,2)}, K(a)) \supseteq \mathbb{Z}/2\mathbb{Z}, \text{rang}(E^{(1,2)}, K(a)) \geq 1 ,$$

et une courbe elliptique $\mathcal{S}^{(3,3)}$ définie sur $K(a)(F)$ telle que

$$\text{Tors}(\mathcal{S}^{(3,3)}, K(a)(F)) \supseteq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \text{ et } \text{rang}(\mathcal{S}^{(3,3)}, K(a)(F)) \geq 2 .$$

Comme pour les cas précédents, la preuve est explicite.

Démonstration. — On part de la cubique :

$$\mathcal{S} : F(x, y, 1) = x^3 + y^3 + t^2xy + 1 = 0$$

Le point $P_0 = (0, -1)$ est sur $\mathcal{S}^{(7)}(K(t))$. Nous considérons la droite passant par P_0 et de pente $\lambda = a$ où a est une nouvelle indéterminée.

Regardons maintenant l'intersection de la droite d'équation $y = \lambda x$ et la courbe elliptique $\mathcal{S}^{(7)}/K(t)$. Il est facile de voir que, mis à part le point P_0 , les abscisses des deux autres points de cette intersection sont les racines de l'équation quadratique :

$$Q_{a,t}(x) = (a^3 + 1)x^2 + (a(t^2 - 3a))x + (3a - t^2) = 0 ,$$

dont le discriminant de $Q_{a,t}$ est :

$$\text{Disc}_x(Q_{a,t}) = a^2t^4 + (-2a^3 + 4)t^2 + (-3a^4 - 12a) . \quad (3.180)$$

Pour que les deux autres points d'intersections soient rationnels, il faut et il suffit que $\text{Disc}_x(Q_{a,t})$ soit un carré dans le corps $K(a)$. On considère alors la courbe définie sur $K(a)$:

$$\Lambda^{(1,2)} : Y^2 = a^2 t^4 + (-2a^3 + 4)t^2 + (-3a^4 - 12a).$$

La courbe $\Lambda^{(1,2)}/\mathbb{Q}(a)$ est une quartique de genre 1 avec un point $(t, Y) = (a + 1, (a + 2)(a^2 - a + 1))$. Nous utilisons alors le modèle de Weierstrass :

$$\mathcal{S}_a^{(1,1)} : s^2 = x^3 + 423(2a^6 + 10a^3 - 1)x - 1728(a^3 - 2)(7a^6 + 26a^3 + 1). \quad (3.181)$$

Le point P_2 suivant est d'ordre 2 :

$$P_2 = (12a^3 - 24, 0). \quad (3.182)$$

Nous avons aussi le point

$$P_G = \left(12 \frac{a^5 + 16a^4 + 52a^3 + 70a^2 + 40a + 4}{(a + 2)^2}, -432 \frac{a(a + 1)^3(a^3 + 5a^2 + 13a + 12)}{(a + 2)^3} \right). \quad (3.183)$$

□

3.3.9. Familles de courbes avec $\text{Tors}(E, \mathbb{Q}(\sqrt{-1})) \supseteq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. — Nous avons vu à la section 2.5.11 que la courbe elliptique d'équation

$$\mathcal{E}^{(4,4)} : y^2 + xy - (t^4 - \frac{1}{16})y = x^3 - (t^4 - \frac{1}{16})x^2, \quad (3.184)$$

est telle que

$$\text{Tors}(\mathcal{E}^{(4,4)}, \mathbb{Q}(\sqrt{-1})) \supseteq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}. \quad (3.185)$$

Les points

$$P = (0, 0) \text{ et}$$

$$Q = \left(-\frac{1}{8}(2t + 1)(4t^2 + 1), \sqrt{-1} \left(t + \frac{1}{2} \right)^2 \left(t - \frac{\sqrt{-1}}{2} \right)^2 \left(t + \frac{\sqrt{-1}}{2} \right) \right)$$

sont tels que $\langle Q, P \rangle \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ (voir paragraphe 2.5.11). Nous partons de cette courbe pour prouver le théorème suivant :

Théorème 3.20. — *Soit $K = \mathbb{Q}(\sqrt{-1})$, alors il existe une courbe elliptique $\mathcal{S}^{(1,2)}$ définie sur $K(a)$, telle que*

$$\text{Tors}(\mathcal{S}^{(1,2)}, K(a)) \supseteq \mathbb{Z}/2\mathbb{Z}, \text{ rang}(E^{(1,2)}, K(a)) \geq 1,$$

et une courbe elliptique $\mathcal{S}^{(4,4)}$ définie sur $K(a)(F)$ telle que

$$\text{Tors}(\mathcal{S}^{(4,4)}, K(a)(F)) \supseteq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \text{ et } \text{rang}(\mathcal{S}^{(4,4)}, K(a)(F)) \geq 2.$$

Démonstration. — Considérons la courbe elliptique $\mathcal{E}^{(4,4)}$ définie sur $\mathbb{Q}(t)$ ci-dessus. avec le point $P_0 = (0, 0)$, nous menons la droite passant par ce point et de pente $\lambda = a(2t - 1)(2t + 1)$ où a est une indéterminée. Considérons l'intersection de la droite d'équation $y = \lambda x$ avec la courbe elliptique $\mathcal{E}^{(4,4)}$. Mis à part le point P_0 , les abscisses des deux autres points de cette intersection sont les racines de l'équation quadratique :

$$Q_{a,t}(x) = -x^2 + \left((16a^2 + 1)t^4 + (-8a^2 + 4a)t^2 + \left(a^2 - a - \frac{1}{16} \right) \right) x - \frac{a}{16}(2t - 1)(2t + 1)(4t^2 + 1) \quad (3.186)$$

Le discriminant de $Q_{a,t}$ est :

$$\begin{aligned} \text{Disc}_x(Q) &= \left(\frac{1}{16}(16a^2 + 1)^2 t^4 - \frac{1}{32}(4a - 1)(4a + 1)(16a^2 - 16a + 1)t^2 \right. \\ &\quad \left. + \frac{1}{256}(4a - 1)(16a^2 - 24a + 1)(2t - 1)^2(2t + 1)^2 \right). \end{aligned}$$

Pour que les deux autres points d'intersection soient rationnels, il faut et il suffit $\text{Disc}_x(Q_{a,t}(x))$ soit un carré. On considère alors la courbe définie sur $K(a)$:

$$\Lambda^{(1,2)} : Y^2 = (2t - 1)^{-2}(2t + 1)^{-2} \text{Disc}_x(Q_{a,t}(x)).$$

C'est une quartique de genre 1 avec un point $(t, Y) = (\frac{1}{2}, a - \frac{1}{8})$. Nous utilisons le modèle de Weierstrass suivant :

$$\begin{aligned} \mathcal{S}_a^{(1,2)} : s^2 &= x^3 - 2^{-12}3^{-1}(4096a^6 - 6144a^5 + 768a^4 - 256a^3 + 48a^2 - 24a + 1) \\ &\quad \times (4a - 1)^2 x + 2^{-17}3^{-3}(4a - 1)^3(4a + 1)(16a^2 - 16a + 1) \\ &\quad \times (4096a^6 - 6144a^5 + 768a^4 - 1024a^3 + 48a^2 - 24a + 1) \end{aligned}$$

Le point

$$P_2 = \left(2^{-6}3^{-1}(4a - 1)(4a + 1)(16a^2 - 16a + 1), 0 \right)$$

et le point

$$P_G = \left(2^{-6}3^{-1} \frac{(4a - 1)(4096a^5 + 2048a^4 - 1472a^3 + 208a^2 - 28a + 1)}{(8a - 1)^2}, \frac{-2^3 a^4 (4a - 1)^2 (16a^2 - 6a + 1)}{(8a - 1)^3} \right)$$

sont sur $\mathcal{S}^{(1,1)}(\mathbb{Q}(a))$ et sont respectivement d'ordre 2 et d'ordre infini. \square

Nous allons maintenant illustrer ce théorème par des exemples.

Exemple. — Prenons maintenant le point $P_2 = [2]P_G$, on obtient un point sur $(t_{P_2}, Y_{P_2}) \in \Lambda^{(1)}(\mathbb{Q}(a))$ correspondant avec :

$$t_{P_2} = \left(-\frac{1}{2} \frac{24576a^5 - 18432a^4 + 5376a^3 - 736a^2 + 48a - 1}{(32a^2 - 1)(256a^3 - 64a^2 + 16a - 1)} \right). \quad (3.187)$$

Nous obtenons enfin la courbe elliptique $\mathcal{S}_{P_2}^{(4,4)}(\mathbb{Q}(a))$, en remplaçant t par t_{P_2} dans l'expression de $\mathcal{E}^{(4,4)}$.

Si l'on pose

$$\begin{aligned} x_2 = & 8a(8a - 1)^2(16a^2 - 6a + 1)(32a^2 - 1)^4(256a^3 - 64a^2 + 16a - 1)^{-2} \\ & \times (65536a^6 - 65536a^5 + 28672a^4 - 6144a^3 + 640a^2 - 32a + 1) \\ & \times (8192a^5 - 8192a^4 + 2560a^3 - 384a^2 + 32a - 1). \end{aligned} \quad (3.188)$$

alors les points d'abscisses x_2 sont d'ordre infini.

ANNEXE A

QUELQUES DÉTAILS COMPLÉMENTAIRES

A.1. Forme normale de Tate

Soit E une courbe elliptique définie sur un corps K et possédant un modèle de Weierstrass de la forme :

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

Supposons aussi que la courbe possède un point rationnel non trivial $P_0 = (x_0, y_0)$ sur K qui ne soit pas un point d'ordre 2 ni d'ordre 3. Une translation ramène ce point à l'origine et de plus l'équation de E devient :

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

Le point $P_0 = (0, 0)$ est donc sur la courbe E . Comme P n'est pas d'ordre 2, cela équivaut à dire que le coefficient a_3 est non nul. Cela permet donc le changement de variable :

$$x = X \text{ et } y = Y + \frac{a_4}{a_3}x .$$

et nous ramène à la forme :

$$E : y^2 + A_1xy + A_3y = x^3 + A_2x^2 .$$

Le coefficient A_2 ne peut pas être nul puisque sinon, P_0 serait d'ordre 3. En faisant le changement de variable $(x, y) \mapsto \left(\frac{A_2^2}{A_3^2}x, \frac{A_2^2}{A_3^2}y\right)$ on obtient ainsi la nouvelle équation :

$$y^2 + \frac{A_1A_2}{A_3}xy + \frac{A_2^3}{A_3^2}y = x^3 + \frac{A_2^3}{A_3^2}x^2 ,$$

que l'on écrira par la suite :

$$E_{b,c} : y^2 + (1 - c)xy + by = x^3 + bx^2 .$$

C'est la forme normale de Tate. Le discriminant de la courbe $E_{b,c}$ est :

$$\Delta(E_{b,c}) = b^3(-c^4 + 3c^3 + (-8b - 3)c^2 + (-20b + 1)c + (-16b^2 + b))$$

Cas où $\text{Tors}(E, K) \supseteq \mathbb{Z}/2\mathbb{Z}$. — On suppose que le corps de base K est de caractéristique différente de 2 et de 3. Dans ce cas, on peut utiliser le modèle de Weierstrass réduit :

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

Si $P = (x_0, y_0)$ est un point de $E(K)$, alors $-P = (x_0, -y_0)$. Le point P est d'ordre 2 si et seulement si $P = -P$. Ce qui équivaut à dire $y_0 = 0$. Les points de 2-torsion sont donc les points dont les abscisses sont les racines du polynôme f .

Cas où $\text{Tors}(E, K) \supseteq \mathbb{Z}/3\mathbb{Z}$. — On va reprendre la méthode décrite dans [Kna92, chapitre V] pour trouver la forme générale des courbes elliptiques ayant un point de 3-torsion. On part de la courbe elliptique :

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

La loi du groupe donne

$$-P = (0, -a_3) \text{ et } [2]P = (-a_2, a_1a_2 - a_3) .$$

Au lieu de faire $[3]P = \mathcal{O}$, on écrit $[2]P = -P$, ce qui nous donne $a_2 = 0$. La forme générale des courbes elliptiques sur K admettant un point de 3-torsion est donc :

$$E : y^2 + sxy + ty = x^3$$

où s et t sont des éléments de K avec $t(s^3 - 27t) \neq 0$. Il est alors facile de vérifier que le point $(0, 0)$ est d'ordre 3.

ANNEXE B

QUELQUES EXEMPLES DE COURBES PARAMÉTRISANTES

Dans cet appendice, nous donnerons essentiellement des courbes elliptiques paramétrisantes, les pentes des droites considérées ainsi que les points de départ.

Dans la première colonne, nous donnons le nom de la courbe paramétrisante selon la table de Cremona [Cre97]. Dans la deuxième colonne, nous donnons son équation ; la notation $[a_1, a_2, a_3, a_4, a_6]$ signifie que la paramétrisante a pour équation de Weierstrass :

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

Dans la quatrième colonne, nous donnons le rang de la courbe paramétrisante.

Il est à noter que dans tous les tableaux de l'annexe, nous partons des familles de courbes elliptiques contenant le point $P = (0, 0)$. Ainsi, nous obtenons des courbes elliptiques de rang supérieur en choisissant la pente de la colonne 5 et le point $[n]P$.

Nous remarquons qu'il peut s'avérer que différentes pentes ou deux points de torsion différents induisent la même paramétrisante.

B.1. Le cas $T \supseteq (1, 12)$ et $r \geq 1$

Nous partons de la famille de courbes elliptiques :

$$\begin{aligned} \mathcal{E}^{(12)} : y^2 + (6t^4 - 8t^3 + 2t^2 + 2t - 1)xy - t(t-1)^5(2t-1)(2t^2 - 2t + 1) \\ \times (3t^2 - 3t + 1)y = x^3 - t(t-1)^2(2t-1)(2t^2 - 2t + 1)(3t^2 - 3t + 1)x^2 . \end{aligned}$$

Le point $P = (0, 0)$ est d'ordre 12. Nous utilisons le point $[n]P$ comme point de départ et avec des pentes bien choisies, nous obtenons des familles de courbes elliptiques de rang au moins 1 et de partie torsion isomorphe à $\mathbb{Z}/12\mathbb{Z}$.

TAB. 2.1: Paramétrisantes pour le cas (1, 12)

Cremona	Modèle minimale	Points	r	Pente	n
150a2	[1, 0, 1, -8, -7]		0	$(t-1)^2(3t^2-2t+1)$	4
128a1	[0, 1, 0, 1, 1]	(0, 1)	1	$-2t(t-1)^2(2t-1)$ $-(2t-1)(3t^2-3t+1)$ $-2t(t-1)^3$ $-2t^4-2t^3+6t^2+4t+1$ $-(2t-1)(2t^3-2t+1)$	4 2 8 8 4
148a1	[0, -1, 0, -5, 1]	(-1, 2)	1	$-2t(2t-1)(3t^2-3t+1)$ $-2(t-1)^2(2t^2-1)$ $-2(t-1)(2t^3+2t^2-3t+1)$ $(t-1)^2(3t^2-4t+2)$ $3t^4-6t^3+7t^2-4t+1$ $-t(2t-1)(2t^2-3t+2)$ $-2t^2(2t-1)^2$	2 8 8 6 6 4 4
160b2	[0, -1, 0, -1, -15]		0	$-2(t-1)^2(2t^2+2t-1)$ $-t(4t^3-6t^2+5t-2)$	4 8
162d1	[1, -1, 1, 4, -1]		0	$-2t(2t-1)(3t^2-3t+1)$ $-6t^4+8t^3-2t^2-2t+1$ $6(1-2t)(2t^2-2t+1)$ 0	8 8 4 4
1696e1	[0, -1, 0, 15, 1]	(0, 1), (1, 4)	2	$2t(t-1)(3t^2-3t+1)$ $-4t(t-1)(3t^2-3t+1)$	2 10
226a1	[1, 0, 0, -5, 1]	(-2, 3)	1	$-t^3$ $-t(3t^2-3t+1)$	10 10
24a4	[0, -1, 0, 1, 0]		0	$-\frac{1}{2}6t^4-8t^3+2t^2+2t-1$ $(1-t)(2t-1)$	6 10
288a2	[0, 0, 0, -12, 0]	(-2, 4)	1	$(t-1)^2(4t^2-2t+1)$	8
344a1	[0, 0, 0, 4, 4]	(0, 2)	1	$-2t(t-1)^2(2t-1)$ $-t^2(t-1)^2$ $-t^4-2t^3+5t^2-4t+1$ $-t(2t^3-8t^2+7t-2)$ $-2t(t-1)^3$ $2t^4+2t^3-6t^2+4t-1$	2 6 6 8 10 10
368d1	[0, 1, 0, 0, -1]	(1, 1)	1	$-2t(t-1)^2(2t-1)$ $t(t-1)(2t-1)$ $-(2t-1)(3t^2-3t+1)$	8 10 10

Cremona	Modèle minimale	Points	r	Pente	n
				$-2t(t-1)^3$	4
				$-2t^4 + 2t^3 - 6t^2 + 4t - 1$	4
				$-(2t-1)(2t^3 - 2t + 1)$	8
45a1	$[1, -1, 0, 0, -5]$		0	$-(t-1)^2(2t-1)$	2
				$-(t-1)^2(2t-1)$	6
58a1	$[1, -1, 0, -1, 1]$	$(0, 1)$	1	$-2t^2(t-1)^2$	8
				$-2t^4 - 4t^2 + 4t - 1$	8
				$t^2(3t^2 - 3t + 1)$	6
				$(t-1)(3t^3 - 4t^2 + 3t - 1)$	6
				$-4t^4 + 8t^3 - 6t^2 + 2t$	4
				$(1 - 2t^2)(2t^2 - 2t + 1)$	4

B.2. Le cas $T \supseteq (2, 6)$ et $r \geq 2$

Nous partons de la famille de courbes elliptiques :

$$\begin{aligned} \mathcal{S}_{(1)}^{(2,6)} : y^2 + 4(t^2 - t - 1)^2 xy \\ - 16t(t+1)(t+2)(3t+1)(2t^2 + 2t + 1)^2(5t^2 + 6t + 2)(t^2 + 1)y \\ = x^3 - 8t(t+1)(t+2)(3t+1)(2t^2 + 2t + 1)^2 x^2. \end{aligned}$$

Le point

$$\begin{aligned} N_\lambda = \left(8t(t+1)(t+2)(3t+1)(t^2 - t - 1)(2t^2 + 2t + 1), \right. \\ \left. 16t^2(t+1)^2(t+2)^2(3t+1)^2(2t^2 + 2t + 1)^2 \right) \quad (2.189) \end{aligned}$$

est d'ordre infini et le point $P = (0, 0)$ est d'ordre 6. Nous utilisons le point $[n]P$ comme point de départ et avec des pentes bien choisies, nous obtenons des familles de courbes elliptiques de rang au moins 2 et de partie torsion isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

TAB. 2.2: Paramétrisantes pour le cas $(2, 6)$

Cremona	Modèle minimale	Points	r	Pente	n
190a1	$[1, -1, 1, -48, 147]$	$(13, -47)$	1	$-2t(t-3)(2t^2 + 2t + 1)$	2

Cremona	Modèle minimale	Points	r	Pente	n
				$2(t-1)(t+2)(2t^2+2t+1)$	2
360e2	[0, 0, 0, -63, 162]	(-3, 18)	1	$-2t(t+2)(2t^2+2t+1)$	1
39600bu1	[0, 0, 0, 105, -650]	(6, 14), (9, 32)	2	$2t(t+2)(t^2+1)$	4
				$-2(t+1)(3t+1)(t^2-2t+2)$	2
800a1	[0, 0, 0, -25, 0]	(-4, 6)	1	$2(t+1)(t+2)(t^2-t-1)$	3
				$-2t(3t+1)(t^2-t-1)$	3
1160c2	[0, 0, 0, -247, 1386]	(2, 30)	1	$(2t-1)(2t+1)(4t+1)$	5

B.3. Le cas $T \supseteq (1, 7)$ et $r \geq 2$

Nous partons de la famille de courbes elliptiques :

$$\begin{aligned} \mathcal{E}_1^{(7)} : y^2 + (t^4 + 4t^3 - 10t^2 + 12t + 9)xy + 4t(t-1)^2(t-3)^2(t^2+3)^3y \\ = x^3 + 2t(t-1)^2(t-3)^2(t^2+3)x^2. \end{aligned}$$

Le point

$$N_1 = \left(4t(t-3)(t-1)^2(t+3)(t^2+3), 16t^2(t-3)^2(t-1)^2(t^2+3)^2 \right)$$

est d'ordre infini et le point $P = (0, 0)$ est d'ordre 7. Nous utilisons le point $[n]P$ comme point de départ et avec des pentes bien choisies, nous obtenons des familles de courbes elliptiques de rang au moins 2 et de partie torsion isomorphe à $\mathbb{Z}/7\mathbb{Z}$.

TAB. 2.3: Paramétrisantes pour le cas (1, 7)

Cremona	Modèle minimale	Points	r	Pente	n
1221a1	[1, 0, 1, 5, -7]	(13, 41)	1	$-t^4 + 4t^3 + 10t^2 + 12t - 9$	4
				$-(t-1)(t-3)(t^2+3)$	6
				$(1-t^2)(t^2-9)$	2
243a2	[0, 0, 1, 0, 20]	(-2, 3)	1	$(1-t)(t^3+3t^2-9t-3)$	4
				$-3(t-1)^2(t^2+3)$	5
4416bb1	[0, 1, 0, -1851479]	(-14, 39), (-5, 48)	2	$-(t^2-2t+3)^2$	5
444b1	[0, 1, 0, -9, 0]	(-3, 3)	1	$-2(t^2+3)(t^2-2t+3)$	6
				$-(t+1)(t+3)(t^2+3)$	3

504f2	$[0, 0, 0, -111, -110]$	$(-7, 18)$	1	$-(t^2 - 2t + 3)(t^2 + 2t + 3)$	6
-------	-------------------------	------------	---	---------------------------------	---

B.4. le cas $T \supseteq (1, 10)$ et $r \geq 1$

Nous partons de la famille de courbes elliptiques (voir [Kul03]) :

$$\mathcal{E}^{(10)} : P(x, y) = y^2 + \frac{2t^3 + 2t^2 + 2t + 1}{(t + 1)^2}xy + \frac{t^2(2t + 1)}{(t + 1)^2}y - \left(x^3 + \frac{t^2(2t + 1)}{(t + 1)^2}x^2\right) = 0 .$$

Le point

$$P = \left(-\frac{t^2(2t + 1)}{(t + 1)^3}, -\frac{t^3(2t + 1)^2}{(t + 1)^5} \right) ,$$

est d'ordre 10. Nous utilisons le point $[n]P$ comme point de départ et avec des pentes bien choisies, nous obtenons des familles de courbes elliptiques de rang au moins 1 et de partie torsion isomorphe à $\mathbb{Z}/10\mathbb{Z}$.

TAB. 2.4: Paramétrisantes pour le cas (1, 10)

Cremona	Modèle minimale	Points	r	Pente	n
102a1	$[1, 1, 0, -2, 0]$	$(-1, 2)$	1	$\frac{-2t-1}{(t+1)^2}$	6
				$\frac{-2t^2}{t+1}$	4
				$\frac{3t(t+2)}{(t+1)^2}$	8
				$-2t - 1$	2
				$-3t - 2$	4
				$(t - 1)(t + 1)$	8
123b1	$[0, -1, 1, 1, -1]$	$(1, 0)$	1	$-\frac{(2t+1)t^2+t+1}{(t+1)^2}$	6
				$\frac{t(2t+1)}{(t+1)^2}$	8
				$\frac{t}{t+1}$	4
				$-\frac{2t^2+2t+1}{t+1}$	2
128a1	$[0, 1, 0, 1, 1]$	$(0, 1)$	1	$-2t - 2$	4
				$-\frac{t(t-1)}{t+1}$	4
				$-t^2$	6
				$-\frac{-t^2}{(t+1)^2}$	8
				$-\frac{t(t-1)}{t+1}$	4

1324a1	$[0, 1, 0, 3, 4]$	$(-1, 1), (0, 2)$	2	$\frac{3t-1}{t+1}$ $\frac{4t(t+2)}{t+1}$ $\frac{t+1}{t(t-1)}$ $-\frac{t+1}{t+1}$	4 8 4
148a1	$[0, -1, 0, -5, 1]$	$(-1, 2)$	1	$\frac{-2t-1}{(t+1)^2}$ $\frac{-2t^2}{t+1}$ $\frac{t+1}{t(3t+2)}$ $\frac{t+1}{(t+1)^2}$ $-2t - 1$ $-4t - 2$ $\frac{(t-1)^2}{(t+1)^2}$ $-\frac{t(t-1)}{t+1}$	2 8 6 4 2 6 4
150a1	$[1, 0, 0, -3, -3]$		0	0 $-\frac{2t^3+2t^2+2t+1}{(t+1)^2}$ $-\frac{t^2(2t+1)}{(t+1)^2}$ -1	4 6 3 2
1576a1	$[0, 1, 0, -9, -5]$	$(-2, 3), -1, 2)$	2	$-\frac{(t-1)^2}{(t+1)^2}$	8
158a1	$[1, -1, 1, -9, 9]$	$(-1, 4)$	1	$-2t$ $\frac{-2t-1}{2t+2}$ $\frac{(1-t)(2t+1)}{t+1}$ $\frac{2t^2-1}{(t+1)^2}$ $\frac{(1-t)(2t+1)}{t+1}$	6 6 8 4 8
163a1	$[0, 0, 1, -2, 1]$	$(1, 0)$	1	0 $-\frac{2t^3+2t^2+2t+1}{(t+1)^2}$ $-\frac{t^2(2t+1)}{(t+1)^2}$ -1 $\frac{2t+1}{t+1}$ $\frac{(1-t)(2t+1)}{t+1}$	5 8 5 5 3 8
176c1	$[0, -1, 0, 3, 1]$	$(1, 2)$	1	0 $-\frac{2t^3+2t^2+2t+1}{(t+1)^2}$ $-\frac{t^2(2t+1)}{(t+1)^2}$ $-2\frac{t^2(2t+1)}{t+1}$ 1 -1	2 8 4 2 6 6
20a2	$[0, 1, 0, -1, 0]$		0	$-\frac{2t^3+2t^2+2t+1}{2(t+1)^2}$ $\frac{-2t-1}{t+1}$ $\frac{t+1}{(t^2-t+1)}$ $\frac{t+1}{(t+1)^2}$	5 7 1

				$\frac{-t(2t+1)}{t+1}$	9
214a1	[1, 0, 0, -12, 16]	(0, 4)	1	$-t + 1$	5
				$\frac{t(2t+1)}{t+1}$	3
219b1	[0, 1, 1, 3, 2]	(2, 4)	1	$-\frac{2t^2+1}{t+1}$	2
248c1	[0, 0, 0, 1, -1]	(1, 1)	1	$-\frac{t(t+2)}{(t+1)^2}$	4
				$\frac{-2t^2-t+1}{t+1}$	6
				$\frac{t(2t+1)}{t+1}$	3
2918b1	[1, 0, 0, -80, 256]	$(-\frac{80}{49}, \frac{6992}{343}), (-6, 26)$	2	$\frac{3t(2t+1)}{(t+1)^2}$	1
				$-4t - 3$	7
				$\frac{4t+1}{2t+2}$	3
				$\frac{-2t^2}{(t+1)^2}$	9
				$\frac{t(2t+1)}{t+1}$	3
34a1	[1, 0, 0, -3, 1]		0	$\frac{t+1}{-2t^2}$	6
				$\frac{t+1}{t(3t+2)}$	2
				$\frac{-2t-1}{(t+1)^2}$	8
				$-2t$	4
				$\frac{(t-1)(2t+1)}{t+1}$	2
				$\frac{(t-1)(2t+1)}{(t+1)^2}$	4
				$\frac{2t^2-1}{(t+1)^2}$	6
366g1	[1, 1, 1, -32, 65]	(-3, 13)	1	$\frac{4t+1}{t+1}$	4
38b1	[1, 1, 1, 0, 1]		0	0	9
				$\frac{-2t^3-2t^2-2t-1}{(t+1)^2}$	1
				$\frac{-t^2(2t+1)}{(t+1)^2}$	3
				-1	7
				2t	4
				$\frac{2t+1}{t+1}$	9
				$\frac{t+1}{t^2}$	8
				$\frac{-t^2-1}{t+1}$	5
				$\frac{(t-1)(2t+1)}{2(t+1)^2}$	1
				$\frac{-2t^2-t-1}{t+1}$	2
430d1	[1, 0, 0, -1415, 20617]	(-26, 213)	1	$-\frac{4t(2t+1)}{(t+1)^2}$	6
43a1	[0, 1, 1, 0, 0]	(0, 0)	1	$\frac{-2t-1}{t+1}$	8
				$\frac{t^2-t-1}{(t+1)^2}$	4
				$-4t^2$	8

				$-\frac{t(2t+1)}{t+1}$	6
				$\frac{t+1}{t(2t+1)}$	6
528a2	[0, -1, 0, 32, -32]	(4, 12)	1	3	4
				$-4\frac{t^2(2t+1)}{(t+1)^2}$	8
				$\frac{t(2t+1)}{t+1}$	3
5830f1	[1, -1, 1, -708, 7527]	(-27, 93), (125, -1427)	2	$4\frac{2t+1}{t+1}$	6
65a1	[1, 0, 0, -1, 0]	(-1, 1)	1	$\frac{2t}{t+1}$	3
				$-2(t+1)$	7
				$-t$	6
				t	5
				$-\frac{(2t+1)}{t+1}$	6
				$\frac{t^2-t-1}{t+1}$	8
				$(t-1)(t+1)$	4
				$-\frac{t^2}{(t+1)^2}$	9
				$-\frac{t^2-t-1}{t+1}$	5
				$-\frac{t+1}{t(2t+1)}$	2
79a1	[1, 1, 1, -2, 0]	(0, 0)	1	0	3
				$-\frac{2t^3-2t^2-2t-1}{(t+1)^2}$	7
				$-\frac{t^2(2t+1)}{(t+1)^2}$	1
				-1	9
				$-2t$	7
				$-t$	5
				$\frac{t^2-t-1}{t+1}$	5
				$\frac{(t-1)(2t+1)}{t+1}$	1
				$\frac{t+1}{2t^2-1}$	1
				$\frac{2t^2-1}{(t+1)^2}$	3
88a1	[0, 0, 0, -4, 4]	(2, -2)	1	$\frac{2t^2}{t+1}$	2
				$\frac{2t(2t+1)}{(t+1)^2}$	2
				$-2t-2$	8
				$2t$	8
				$2t-1$	6
				$\frac{3t+1}{t+1}$	6
				$-\frac{t^2}{(t+1)^2}$	6
				$\frac{t^2}{(t+1)^2}$	6
				$-\frac{2t^2-t-1}{t+1}$	4

912i1	$[0, 1, 0, 3, -9]$	$(3, 6)$	1	$\frac{8}{-9\frac{t^2(2t+1)}{(t+1)^2}}$	2 4
-------	--------------------	----------	---	---	--------

B.5. Le cas $T \supseteq (1, 9)$ et $r \geq 1$

Nous partons de la famille de courbes elliptiques :

$$\mathcal{E}^{(9)} : P(x, y) = y^2 + (-t^3 + t^2 + 1)xy - t^2(t - 1)(t^2 - t + 1)y - (x^3 - t^2(t - 1)(t^2 - t + 1)x^2) = 0 .$$

Le point $P = (0, 0)$ est d'ordre 9. Le bon choix de la pente et du point de départ $[n]P$ permet d'obtenir des familles de courbes elliptiques de rang au moins 1.

TAB. 2.5: Paramétrisantes pour le cas $(1, 9)$

Cremona	Modèle minimale	Points	r	Pente	n
1132a1	$[0, 1, 0, -5, 4]$	$(-1, 3), (0, 2)$	2	$4t(t - 1)$ $-\frac{4t^2}{(t+1)^2}$	7 7
141d1	$[0, -1, 1, -1, 0]$	$(0, 0)$	1	$-3t(t - 1)$ $2t^2 - 2t - 1$ $-2t(2t - 1)$	4 1 2
324c1	$[0, 0, 0, 9, 9]$	$(-3, 3)$	1	$t^2 - 2$ $-2t^2$	3 6
408d1	$[0, 1, 0, -17, 51]$	$(7, -18)$	1	$3(t^2 - t + 1)$	4
43a1	$[0, 1, 1, 0, 0]$	$(0, 0)$	1	$t^2 - t - 1$ $-2t(t - 1)$ $-t^2$ $-t - 1$	3 3 6 8
53a1	$[1, -1, 1, 0, 0]$	$(0, 0)$	1	$t^2 - t - 1$ $2t(t - 1)$ $t - 1$ $t - 1$ $t - 1$	8 5 1 4 7

				$-t^2$	7
54b1	[1, -1, 1, 1, -1]		0	$t(t-2)$	2
				$-t^2 + t - 1$	1
				t^2	3
58a1	[1, -1, 0, -1, 1]	(0, 1)	1	$t(t-2)$	3
				$-t^2 + t - 1$	6
				$t^2 - t + 1$	1
606e1	[1, 0, 0, -120, 576]	(0, 24)	1	$-3t(t-1)$	1
92b1	[0, 0, 0, -1, 1]	(1, -1)	1	$(t-1)^2$	6
				$t^2 - t - 1$	5
				$2t(t-1)$	2
				$-t^2$	1
				t^2	1
				$-t^2 - 1$	6
99a1	[1, -1, 1, -2, 0]	(0, 0)	1	$(t-1)(t+1)$	1
				$(t-1)(t+1)$	2
				$(t-1)(t+1)$	4
				$(t-1)(t+1)$	5
				$(t-1)(t+1)$	7
				$(t-1)(t+1)$	8

B.6. Le cas $T \supseteq (2, 8)$ et $r \geq 1$

Nous partons de la famille de courbes elliptiques :

$$\begin{aligned}
 \mathcal{E}^{(2,8)} : y^2 + (t^4 - 24t^2 - 64t - 64)xy \\
 - 2(t^2 + 4t + 8)(t + 4)(t^2 - 8)(t + 2)^3 t^3 y \\
 = x^3 - 2(t^2 + 4t + 8)(t + 4)(t + 2)^2 t^2 x^2,
 \end{aligned}$$

Le point $P = (0, 0)$ est d'ordre 8. Le bon choix de la pente et du point de départ $[n]P$ permet d'obtenir des familles de courbes elliptiques de rang au moins 1 et de partie torsion isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.

TAB. 2.6: Paramétrisantes pour le cas (2, 8)

Cremona	Modèle minimale	Points	rang	Pente	n
1344n3	[0, -1, 0, -449, 3585]	(-13, 84)	1	$4(t-4)(t+4)(t-1)$	4
14a1	[1, 0, 1, 4, -6]		0	$-4(3t+4)(t^2-t-4)$	4
				$-t^3(t+4)$	4
				$4t(t+2)(t+4)$	4
15a8	[1, 1, 1, 0, 0]		0	$4t(t+2)^2$	4
				$2t^2(t+4)$	4
				$-4t^2(t+2)(t+4)$	4
160a2	[0, 1, 0, -1, 15]	(-1, 4)	1	$4t^2$	4
				$4t^2(t+2)$	6
				$4t^2(t+4)$	2
				$-2t(t+2)^2(t+4)$	6
				$4t(t^2+5t+8)$	4
192a2	[0, -1, 0, -9, 9]	(-1, 4)	1	$-2t^2(t+2)$	6
				$4(t+4)^2$	4
				$4(t^3+8t^2+16t+16)$	2
21a1	[1, 0, 0, -4, -1]		0	$4(t^3+4t^2+4t+4)$	2
				$4(t+4)(t^2+3t+4)$	2
				$4(t+4)(t^2+3t+4)$	6
40a1	[0, 0, 0, -7, -6]		0	$4(3t^2+8t+8)$	4
				$4(t+2)^3$	4
				$4(t+4)(t^2+2t+4)$	2
448b1	[0, 0, 0, 4, -16]	(4, 8)	1	$t^2(t+2)$	4
				$-t^3(t+4)$	4
				0	2
				$4t(t+2)(t+4)$	6
				$4(t+2)(t^2+4t+8)$	6
480f1	[0, -1, 0, -30, 72]	(-1, 10)	1	$-4(t+4)(t^2+t-4)$	4
56a2	[0, 0, 0, -19, 30]		0	$4(t^2+4t+8)$	2
				$4(t+2)(t^2-8)$	4
				$4t^2(t+2)$	2
				$4t^2(t+2)$	4
				$4(t^3+4t^2+8t+16)$	2
48a1	[0, 1, 0, -4, -4]		0	$-\frac{1}{2}t^3(t+4)$	4
				$-\frac{1}{2}t^3(t+4)$	6

48a3	[0, 1, 0, -24, 36]		0	$\frac{4t^2(t+2)^2(t+4)}{t^2-8}$	4
640a2	[0, 0, 0, -8, -32]	(9, 25)	1	$-4t(t+2)(t+4)$ $8t(t+2)(t+4)$	2 6

B.7. Le cas $T \supseteq (1, 8)$ et $r \geq 2$

Nous partons de la famille de courbes elliptiques :

$$\begin{aligned} \mathcal{E}_{\lambda, Q}^{(8)} : y^2 + (t^2 - 2)^2 xy + 2t(t^2 + 2)(t^2 - 4t + 2)(t^2 - 2t + 2)^3 y \\ = x^3 + 2t(t^2 - 4t + 2)(t^2 - 2t + 2)^2 x^2. \end{aligned}$$

Le point

$$N_{\lambda, Q} = \left(2t(t-1)(t^2+2)(t^2-2t+2)^2, 4t^2(t-1)^2(t^2+2)(t^2-2t+2)^2(t^2-2) \right)$$

est d'ordre infini et le point $P = (0, 0)$ est d'ordre 8. Nous utilisons le point $[n]P$ comme point de départ et avec des pentes bien choisies, nous obtenons des familles de courbes elliptiques de rang au moins 2 et de partie torsion isomorphe à $\mathbb{Z}/8\mathbb{Z}$.

TAB. 2.7: Paramétrisantes pour le cas (1, 8)

Cremona	Modèle minimale	Points	rang	Pente	n
256b1	[0, 0, 0, -2, 0]	(-1, 1)	1	$4t^2$ $-4t(t^2 - 4t + 2)$	4 2
1088m1	[0, 1, 0, -17, -17]	(-3, 4)	1	$-2t(t^2 - 4t + 2)$	6
1904d1	[0, 0, 0, 29, -30]	(2, 6)	1	$-2t(t^2 + 2)$ $-4t(t^2 - 2t + 2)$	6 4
32a1	[0, 0, 0, 4, 0]		0	$4t(t^2 - 2t + 2)$	6
192a2	[0, -1, 0, -9, 9]	(-1, 4)	1	$4t(t^2 - 2t + 2)$	6
2624a1	[0, 0, 0, -44, -80]	(-3, 5)	1	$2t(t^2 + 2)$	6
448e1	[0, -1, 0, -1, 33]		0	$-2t(3t^2 - 8t + 6)$	6
448b1	[0, 0, 0, 4, -16]	(4, 8)	1	$-2t(3t^2 - 8t + 6)$	2
640b2	[0, 0, 0, -8, 32]	(1, 5)	1	$4t(t^2 - t + 2)$	4
640g1	[0, 0, 0, -2, 4]	(0, 2)	1	$4t(t^2 - 2t + 2)$	2

BIBLIOGRAPHIE

- [AM93] A. O. L. ATKIN & F. MORAIN – « Finding suitable curves for the elliptic curve method of factorization », *Math. Comp.* **60** (1993), no. 201, p. 399–405.
- [BBB⁺] C. BATUT, K. BELABAS, D. BERNARDI, H. COHEN & M. OLIVIER – « The computer algebra system pari-gp », <http://pari.math.u-bordeaux.fr/>.
- [BCP97] W. BOSMA, J. CANNON & C. PLAYOUST – « The Magma algebra system. I. The user language », *J. Symbolic Comput.* **24** (1997), no. 3-4, p. 235–265, Computational algebra and number theory (London, 1993).
- [Bea82] A. BEAUVILLE – « Les familles stables de courbes elliptiques sur \mathbf{P}^1 admettant quatre fibres singulières », *C. R. Acad. Sci. Paris Sér. I Math.* **294** (1982), no. 19, p. 657–660.
- [BM40] G. BILLING & K. MAHLER – « On exceptional points on cubic curves », *J. London Math. Soc.* **15** (1940), p. 32–43.
- [Cam97] G. CAMPBELL – « Finding elliptic curves defined over \mathbf{Q} of high rank », African Americans in mathematics (Piscataway, NJ, 1996), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 34, Amer. Math. Soc., Providence, RI, 1997, p. 107–109.
- [Cas91] J. W. S. CASSELS – *Lectures on elliptic curves*, London Mathematical Society Student Texts, vol. 24, Cambridge University Press, Cambridge, 1991.
- [Coh93] H. COHEN – *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993.

- [CP80] D. A. COX & W. R. PARRY – « Torsion in elliptic curves over $k(t)$ », *Compositio Math.* **41** (1980), no. 3, p. 337–354.
- [Cre97] J. E. CREMONA – *Algorithms for modular elliptic curves*, seconde éd., Cambridge University Press, Cambridge, 1997.
- [Cre99] ———, « Reduction of binary cubic and quartic forms », *LMS J. Comput. Math.* **2** (1999), p. 64–94 (electronic).
- [CS99] J. E. CREMONA & P. SERF – « Computing the rank of elliptic curves over real quadratic number fields of class number 1 », *Math. Comp.* **68** (1999), no. 227, p. 1187–1200.
- [Duja] A. DUJELLA – « High rank elliptic curves with prescribed torsion », <http://web.math.hr/~duje/tors/generic.html>.
- [Dujb] ———, « Infinite families of elliptic curves with high rank and prescribed torsion », <http://web.math.hr/~duje/tors/tors.html>.
- [Duj07] A. DUJELLA – « On Mordell-Weil groups of elliptic curves induced by Diophantine triples », *Glas. Mat. Ser. III* **42(62)** (2007), no. 1, p. 3–18.
- [Elk07] N. D. ELKIES – « Three lectures on elliptic surfaces and curves of high rank », 2007.
- [Fal83] G. FALTINGS – « Endlichkeitssätze für abelsche Varietäten über Zahlkörpern », *Invent. Math.* **73** (1983), no. 3, p. 349–366.
- [Fer96] S. FERMIGIER – « Exemples de courbes elliptiques de grand rang sur $\mathbf{Q}(t)$ et sur \mathbf{Q} possédant des points d'ordre 2 », *C. R. Acad. Sci. Paris Sér. I Math.* **322** (1996), no. 10, p. 949–957.
- [FG08] E. V. FLYNN & C. GRATTONI – « Descent via isogeny on elliptic curves with large rational torsion subgroups », *J. Symb. Comput.* **43** (2008), no. 4, p. 293–303.
- [Fis00] T. FISCHER – « On 5 and 7 descents for elliptic curves », Thèse, University of Cambridge, 2000.
- [Fri02] H. R. FRIUM – « The group law on elliptic curves on Hesse form », *Finite fields with applications to coding theory, cryptography and related areas* (Oaxaca, 2001), Springer, Berlin, 2002, p. 123–151.

- [Hus87] D. HUSEMOLLER – *Elliptic curves*, Graduate Texts in Mathematics, vol. 111, Springer-Verlag, New York, 1987, With an appendix by Ruth Lawrence.
- [JK05] D. JEON & C. H. KIM – « Bielliptic modular curves $X_1(M, N)$ », *Manuscripta Math.* **118** (2005), no. 4, p. 455–466.
- [Kam86a] S. KAMIENNY – « Torsion points on elliptic curves over all quadratic fields », *Duke Math. J.* **53** (1986), no. 1, p. 157–162.
- [Kam86b] S. KAMIENNY – « Torsion points on elliptic curves over all quadratic fields. II », *Bull. Soc. Math. France* **114** (1986), no. 1, p. 119–122.
- [Kih06] S. KIHARA – « On the rank of the elliptic curves with a rational point of order 6 », *Proc. Japan Acad. Ser. A Math. Sci.* **82** (2006), no. 7, p. 81–82.
- [KM88] M. A. KENKU & F. MOMOSE – « Torsion points on elliptic curves defined over quadratic fields », *Nagoya Math. J.* **109** (1988), p. 125–149.
- [Kna92] A. W. KNAPP – *Elliptic curves*, Mathematical Notes, vol. 40, Princeton University Press, Princeton, NJ, 1992.
- [Kob93] N. KOBLITZ – *Introduction to elliptic curves and modular forms*, second éd., Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1993.
- [Kub76] D. S. KUBERT – « Universal bounds on the torsion of elliptic curves », *Proc. London Math. Soc. (3)* **33** (1976), no. 2, p. 193–237.
- [Kul03] L. KULESZ – « Families of elliptic curves of high rank with nontrivial torsion group over \mathbb{Q} », *Acta Arith.* **108** (2003), no. 4, p. 339–356.
- [Kwo97] S. KWON – « Torsion subgroups of elliptic curves over quadratic extensions », *J. Number Theory* **62** (1997), no. 1, p. 144–162.
- [Lec03a] O. LECACHEUX – « Rang de courbes elliptiques avec groupe de torsion non trivial », *J. Théor. Nombres Bordeaux* **15** (2003), no. 1, p. 231–247, Les XXIIèmes Journées Arithmétiques (Lille, 2001).

- [Lec03b] ———, « Rang de familles de courbes elliptiques », *Acta Arith.* **109** (2003), no. 2, p. 131–142.
- [Lec04] ———, « Rang de courbes elliptiques dont le groupe de torsion est non trivial », *Ann. Sci. Math. Québec* **28** (2004), no. 1-2, p. 145–151 (2005).
- [Maz78] B. MAZUR – « Rational isogenies of prime degree (with an appendix by D. Goldfeld) », *Invent. Math.* **44** (1978), no. 2, p. 129–162.
- [Mer96] L. MEREL – « Bornes pour la torsion des courbes elliptiques sur les corps de nombres », *Invent. Math.* **124** (1996), no. 1-3, p. 437–449.
- [Mes81] J.-F. MESTRE – « Corps euclidiens, unités exceptionnelles et courbes elliptiques », *J. Number Theory* **13** (1981), no. 2, p. 123–137.
- [Mes91a] ———, « Courbes elliptiques de rang ≥ 11 sur $\mathbf{Q}(t)$ », *C. R. Acad. Sci. Paris Sér. I Math.* **313** (1991), no. 3, p. 139–142.
- [Mes91b] ———, « Courbes elliptiques de rang ≥ 12 sur $\mathbf{Q}(t)$ », *C. R. Acad. Sci. Paris Sér. I Math.* **313** (1991), no. 4, p. 171–174.
- [Nag97] K.-I. NAGAO – « Construction of high-rank elliptic curves with a non-trivial torsion point », *Math. Comp.* **66** (1997), no. 217, p. 411–415.
- [Nér56] A. NÉRON – « Propriétés arithmétiques de certaines familles de courbes algébriques », *Proceedings of the International Congress of Mathematicians, 1954, Amsterdam, vol. III*, Erven P. Noordhoff N.V., Groningen, 1956, p. 481–488.
- [Par99] P. PARENT – « Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres », *J. Reine Angew. Math.* **506** (1999), p. 85–116.
- [Rab08] F. P. RABARISON – « Structure de torsion des courbes elliptiques définies sur les corps de nombres quadratiques », preprint, 2008.
- [Rei85] M. A. REICHERT – « Explicit determination of non-trivial torsion structures of elliptic curves over quadratic number fields », *EUROCAL '85 : Research Contributions from the European Conference on Computer Algebra-Volume 2* (London, UK), Springer-Verlag, 1985, p. 489–490.

- [SC03] M. STOLL & J. E. CREMONA – « On the reduction theory of binary forms », *J. Reine Angew. Math.* **565** (2003), p. 79–99.
- [Sch96] E. F. SCHAEFER – « Class groups and Selmer groups », *J. Number Theory* **56** (1996), no. 1, p. 79–114.
- [Ser95] P. SERF – « The rank of elliptic curves over real quadratic number fields of class number 1 », Thèse, Universität des Saarlandes, Saarbrüucken, 1995.
- [Shi] G. SHIMURA – *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11.
- [Shi91] T. SHIODA – « An infinite family of elliptic curves over \mathbf{Q} with large rank via Néron’s method », *Invent. Math.* **106** (1991), no. 1, p. 109–119.
- [Sil86] J. H. SILVERMAN – *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.
- [Sil94] ———, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.
- [Sima] D. SIMON – « Le fichier gp », <http://www.math.unicaen.fr/~simon/ellQ.gp>.
- [Simb] ———, « Le fichier gp », <http://www.math.unicaen.fr/~simon/ell.gp>.
- [Sim02] D. SIMON – « Computing the rank of elliptic curves over number fields », *LMS J. Comput. Math.* **5** (2002), p. 7–17 (electronic).
- [SZ91] U. SCHNEIDERS & H. G. ZIMMER – « The rank of elliptic curves upon quadratic extension », Computational number theory (Debrecen, 1989), de Gruyter, Berlin, 1991, p. 239–260.
- [Vél71] J. VÉLU – « Isogénies entre courbes elliptiques », *C. R. Acad. Sci. Paris Sér. A-B* **273** (1971), p. A238–A241.
- [vH95] M. VAN HOEIJ – « An algorithm for computing the Weierstrass normal form », *International Symposium on Symbolic and Algebraic Computation*, 1995, p. 90–95.

- [vH97] M. VAN HOEIJ – « Rational parametrizations of algebraic curves using a canonical divisor », *J. Symbolic Comput.* **23** (1997), no. 2-3, p. 209–227, Parametric algebraic curves and applications (Albuquerque, NM, 1995).
- [vH02] ———, « An algorithm for computing the Weierstrass normal form of hyperelliptic curves », <http://www.citebase.org/abstract?id=oai:arXiv.org:math/0203130>, 2002.
- [Wom] T. WOMACK – « Buhler-Gross algorithm for computing L-series derivatives », <http://http://www.warwick.ac.uk/~masgaj/ftp/progs/pari/bgc.gp>.
- [Zim89] H. G. ZIMMER – « Computational aspects of the theory of elliptic curves », Number theory and applications (Banff, AB, 1988), NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., vol. 265, Kluwer Acad. Publ., Dordrecht, 1989, p. 279–324.