Sommes de trois carrés en deux variables et représentation de bas degré pour le niveau des courbes réelles

Olivier Macé

N^0 d'ordre : 2340

THESE

Présentée

DEVANT L'UNIVERSITE DE RENNES 1

pour obtenir

le grade de Docteur de l'Université de Rennes 1

Mention : Mathématiques et Applications

par

Olivier Macé

Equipe d'accueil : Institut de Recherche Mathématique de Rennes

Ecole Doctorale : Mathématiques de l'Ouest

Composante universitaire : Institut Mathématique de Rennes

Titre de la Thèse :

Sommes de trois carrés en deux variables et représentation de bas degré pour le niveau des courbes réelles

Soutenue le 31 mars 2000 devant la Commission d'Examen

D. LEEP	Rapporteurs
J. VAN GEEL	
M. COSTE	Examinateurs
D. HOFFMANN	
J. HUISMAN	
L. MAHE	

Table des matières

Introduction

Hilbert a montré [Hi2] que toute fonction non négative de $\mathbb{R}(x,y)$ est une somme de carrés de fractions rationnelles dans $\mathbb{R}(x,y)$, il a aussi prouvé dans [Hi1] qu'un polynôme non négatif de $\mathbb{R}[x,y]$ de degré inférieur ou égal à 4 peut s'écrire comme somme de 3 carrés dans $\mathbb{R}[x,y]$. Plus généralement, Pfister a montré dans dans [Pf1] que toute fraction rationnelle non négative de $\mathbb{R}(x_1,...,x_n)$ est somme de 2^n carrés d'éléments de $\mathbb{R}(x_1,...,x_n)$. Le nombre de Pythagore (nombre minimal de carrés nécessaires pour représenter tout élément non négatif) de $\mathbb{R}(x_1,...,x_n)$ est donc inférieur ou égal à 2^n.

En deux variables, le nombre de Pythagore de $\mathbb{R}(x,y)$ est donc inférieur ou égal à 4. Cassels, Ellison et Pfister ont montré que ce nombre est exactement 4 : dans [CEP], ils démontrent, par le biais de l'étude d'une certaine courbe elliptique, que le polynôme de Motzkin $(1+x^2y^4+x^4y^2-3x^2y^2)$, bien que non négatif, ne peut pas s'écrire comme somme de 3 carrés de fractions rationnelles. Par une méthode similaire, Christie dans [Chr] a donné d'autres exemples de polynômes positifs de $\mathbb{R}[x,y]$ qui ne sont pas sommes de 3 carrés dans $\mathbb{R}(x,y)$. En 1992, Colliot-Thélène a prouvé (voir [CT]) qu'en tout degré pair supérieur ou égal à 6, on peut trouver des polynômes positifs de $\mathbb{R}[x,y]$ non sommes de 3 carrés de fractions rationnelles.

Dans un premier temps, on reviendra sur la méthode utilisée par Christie, méthode elle-même inspirée de celle de Cassels, Ellison et Pfister. L'argument central de ces deux démonstrations est que si un polynôme non négatif de la forme $F(x,y)=1+A(x)y^2+B(x)y^4$ est somme de 3 carrés dans $\mathbb{R}(x,y)$, alors il existe un point défini sur $\mathbb{R}(x)$ et possédant certaines propriétés (ce point sera dit spécial) sur la $\mathbb{R}(x)$-courbe elliptique $\mathcal{C}^{-1}_{\mathbb{R}(x)} : -\beta^2 = \alpha(\alpha^2 - 2A(x)\alpha + A^2(x) - 4B(x))$. L'équation de cette courbe est en fait une forme de Weierstrass de l'équation de la jacobienne de la quartique $Z^2 + F = 0$ définie sur le corps $\mathbb{R}(x)$ et un point spécial sur $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ correspond à un point qui reste toujours sur la composante non-neutre de cette jacobienne pour tout ordre de $\mathbb{R}(x)$ [HM].

Pour démontrer que le polynôme $F(x,y)$ n'est pas sommes de 3 carrés, on

étudie donc la courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ afin de vérifier qu'elle ne possède pas de point spécial. pour cela, Cassels, Ellison et Pfister, ainsi que Christie, ont effectué une étude complète de la courbe $\mathcal{C}^{-1}_{\mathbb{C}(x)}$ définie par la même équation sur le corps $\mathbb{C}(x)$. Une telle étude débute par le traitement des points d'ordre fini pour s'assurer qu'aucun d'entre eux n'est spécial, mais la principale difficulté reste le cas des points d'ordre infini. Cassels, Ellison et Pfister ont donné une méthode utilisant, entre autre, l'analogue du théorème de Mordell-Weil pour les corps de fonctions et des éléments de théorie de Galois, et permettant de déterminer précisément le groupe $\mathcal{C}^{-1}_{\mathbb{C}(x)}$ (pour la courbe associée au polynôme de Motzkin) et de montrer que $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ ne contient pas de point qui ne soit pas de torsion. Christie a proposé une variante de cette méthode dans le cas où $\mathcal{C}^{-1}_{\mathbb{C}(x)}$ est de rang nul, permettant ainsi de la généraliser à certaines familles de courbes elliptiques. Toutefois, sa démonstration est incomplète, c'est pourquoi on la reprendra dans le chapitre 1, et on fera aussi une étude plus appronfondie de la famille de courbes qu'il avait traitée.

Il est intéressant de noter que, aussi bien dans l'exemple de Cassels, Ellison et Pfister que dans ceux de Christie, les courbes elliptiques $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ présentent des singularités en certaines valeurs réelles de x. En effet dans le cas de Cassels, Ellison et Pfister, la courbe $\mathcal{C}^{-1}$ a pour équation $-\beta^2 = \alpha(\alpha - x(x+1)^2(x-2))(\alpha - x(x-1)^2(x+2))$ et donc présente des singularités pour $x = -2, -1, 0, 1, 2$ ainsi qu'à l'infini. L'exemple donné par Christie étant $F(x,y) = 1 + x((x+\mu)^3 - \frac{\nu^3}{2})y^2 + \frac{\nu^6}{16}x^2y^4$ (pour certaines valeurs de μ et ν), la courbe $\mathcal{C}^{-1}$ associée a pour équation $-\beta^2 = \alpha(\alpha - x(x+\mu)^3)(\alpha - x(x+\mu)^3 + x\nu^3)$ et sa fibre est singulière pour $x = -\mu$, $x = 0$ et $x = \nu - \mu$ ainsi qu'à l'infini.

Dans le second chapitre, on traitera certains polynômes factorisés sous la forme $F(x,y) = (y^2 + a(x))(y^2 + b(x))$, a et b étant des polynômes non négatifs de $\mathbb{R}[x]$. On montrera que certains polynômes de ce type ne sont pas somme de 3 carrés bien qu'étant produit de deux sommes de 3 carrés de polynômes. En fait dans les exemples traités, $a(x)$ est un carré de polynôme et on a alors des polynômes qui ne sont pas sommes de 3 carrés dans $\mathbb{R}(x,y)$, mais qui se présentent comme produit d'une somme de 2 carrés par une somme de 3 carrés dans $\mathbb{R}[x,y]$. On étudiera en particulier le cas où $F(x,y) = (y^2 + (x^2+1)^2)(y^2 + (x^2+1)^2 - r^2)$ pour certaines valeurs de $r \in [0,1]$. Pour cette famille de polynômes, on a à étudier les courbes d'équation $-\beta^2 = \alpha(\alpha^2 - 2(2(x^2+1)^2 - r^2)\alpha + r^4)$ et on remarque que, si $0 < r < 1$, ces courbes ne dégénèrent en aucune valeur réelle en dehors de l'infini.

Contrairement à ce que l'on aurait à priori pu penser, le rôle joué par les singularités réelles de la fibration de $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ sur $\mathbb{P}^1(\mathbb{R})$ dans la non existence d'un point spécial (ou même d'un point d'ordre infini) ne semble donc pas être primordial. Grâce à l'étude de l'exemple $F(x,y) = (y^2+(x^2+2)^2)(y^2+(x^2+2)^2-r^2(x^2+1)^2)$, pour $0 < r < 1$, on montrera qu'une telle courbe elliptique peut ne pas avoir de point d'ordre infini, et pas de point spécial, bien que sa projection sur $\mathbb{P}^1(\mathbb{R})$ n'ait aucune valeur singulière réelle : on ne peut donc pas espérer traiter ce problème par une méthode se ramenant uniquement à l'étude des valeurs réelles de x pour lesquelles la courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ dégénère.

Pour traiter ces exemples, on donnera une étude générale des points d'ordre fini des courbes elliptiques associées à un polynôme factorisé du type ci-dessus et, comme les exemples étudiés ne dépendent que de x^2, la symétrie $x \mapsto -x$ sera largement utilisée pour obtenir des simplifications. Cette amélioration de la méthode de Christie ne fonctionne cependant que dans certains cas de figure favorables et ne permet toujours pas de se contenter de l'étude des seuls points spéciaux sans avoir à prouver la non existence de points d'ordre infini : en effet, il n'y a, pour l'instant, aucun moyen de déterminer si un point d'ordre infini dont on ne connait pas les coordonnées est spécial ou non.

Enfin dans le troisième chapitre, on montrera qu'il est possible d'obtenir des polynômes positifs de $\mathbb{R}[x,y]$ de degré aussi grand que souhaité et qui ne sont pas sommes de 3 carrés dans $\mathbb{R}(x,y)$, et cela uniquement par substitution : Si $F(x,y)$ n'est pas somme de 3 carrés alors le polynôme $F(P(x,y),y)$ n'est pas non plus somme de 3 carrés de fractions rationnelles dès que $P(x,y)$ est un polynôme à coefficients réels de degré impair en la variable x.

On terminera ce chapitre par une étude paramétrée du cas où $F(x,y) = (y^2+a(x))(y^2+b(x))$ avec a et b polynômes positifs de degré inférieur ou égal à 2 : d'apres Hilbert, on sait que ces polynômes F de degré inférieur ou égal à 4 et positifs sont sommes de 3 carrés dans $\mathbb{R}[x,y]$. Une courbe elliptique associée à un tel polynôme a donc, au moins, un point spécial. On s'intéressera à déterminer la forme d'un de ces points spéciaux suivant les différents cas de figure observés. Ce travail permettra, lorsqu'on se donne un polynôme de cette forme, de le représenter de manière non triviale comme somme de trois carrés dans $\mathbb{R}[x,y]$ et pour chaque cas de figure, on donnera un exemple numérique.

Tout ce travail constituant un prolongement de celui de Cassels, Ellison et Pfister et de celui de Christie, utilise bien évidemment bon nombre de résultats

qui y sont démontrés. Pour la clarté de l'exposé, nous avons préféré en reprendre ici la démonstration.

D'après le théorème de Pfister, Si K est un corps de degré de transcendance d sur $\mathbb{R}$, alors toute somme de carrés de K peut s'écrire comme une somme d'au plus 2^d carrés. En particulier lorsque $\mathcal{C}$ est une courbe plane définie sur $\mathbb{R}$ sans point réel alors -1 est une somme de carrés dans le corps de fonctions $\mathbb{R}(\mathcal{C})$ et donc le niveau de $\mathbb{R}(\mathcal{C})$, c'est-à-dire le nombre minimal n tel que -1 soit une somme de n carrés dans $\mathbb{R}(\mathcal{C})$, est inférieur ou égal à 2. On s'intéressera dans le chapitre 4 au cas où le niveau de ce corps est 2 et on cherchera une borne explicite pour la "hauteur" des solutions (u, v) dans $\mathbb{R}(\mathcal{C}) \times \mathbb{R}(\mathcal{C})$ de $u^2 + v^2 = -1$: lorsque tous les points singuliers de la courbe $\mathcal{C}$ sont ordinaires, on déterminera un entier N tel qu'il existe un couple de solutions (u, v) ayant des représentants dans $\mathbb{R}(X, Y)$ de degré total inférieur ou égal à N. Pour obtenir cette borne, on utilisera certaines propriétés des idèles sur les corps de fonctions $\mathbb{R}(\mathcal{C})$ et $\mathbb{C}(\mathcal{C})$, notamment des propriétés relatives au comportement des idèles par rapport à une extension quadratique, en particulier sur la norme et la conjugaison. Ces propriétés permettront de se placer dans de conditions favorables pour que l'application du théorème de Riemann-Roch et du théorème fondamental de Nœther fournissent la borne recherchée.

Chapitre 1

Sommes de trois carrés et courbes elliptiques

On reprend dans ce chapitre la démonstration effectuée par Christie dans [Chr], tout d'abord dans sa partie théorique en y ajoutant une correction de l'erreur figurant dans cet article (sections 1.1 à 1.5), puis dans la section 1.6, on propose une généralisation de l'étude de son exemple (sous certaines conditions sur μ et ν, le polynôme $F(x,y) = 1 + x((x+\mu)^3 - \frac{\nu^3}{2})y^2 + \frac{\nu^6}{16}x^2y^4$ n'est pas une somme de trois carrés de fractions rationnelles) à une plus large famille de paramètres.

Avant cela, il est intéressant de rappeler que l'on sait que tout polynôme non négatif de degré inférieur ou égal à 4 de $\mathbb{R}[x,y]$ est somme de 3 carrés dans $\mathbb{R}[x,y]$ (voir [Hi1]) et que tout polynôme non négatif de degré 2 en y peut s'écrire comme somme de 3 carrés dans $\mathbb{R}(x,y)$ (voir [CEP]), ainsi le cas le plus simple à étudier et permettant de trouver un polynôme non négatif qui ne soit pas somme de 3 carrés dans $\mathbb{R}(x,y)$ est donc de la forme $F(x,y) = y^4 + A(x)y^2 + B(x)$, ou de manière équivalente $F(x,y) = B(x)y^4 + A(x)y^2 + 1$, où $A(x)$ et $B(x)$ sont des éléments de $\mathbb{R}[x]$.

Il faut bien sûr s'assurer que le polynôme $F(x,y)$ est positif, ce qui est le cas quand pour tout $x \in \mathbb{R}$, $B(x)$ est positif et que l'on a soit $A^2(x) - 4B(x) < 0$, soit $A(x) \geq 0$. Par la suite, on se placera implicitement sous ces hypothèses.

1.1 Lien avec les courbes elliptiques

L'argument essentiel de la démonstration de Christie, de même que celle de Cassels, Ellison et Pfister réside en un lien entre le fait que $F(x,y) = y^4 + A(x)y^2 +$

$B(x)$ soit une somme de 3 carrés dans $\mathbb{R}(x,y)$ et l'existence d'un $\mathbb{R}(x)$-point ayant certaines propriétés sur une $\mathbb{R}(x)$-courbe elliptique $\mathcal{C}^{-1}$ associée à $F(x,y)$:

Théorème 1.1.1 ([CEP] théorème 2.1) *Le polynôme* $F(x,y) = y^4 + A(x)y^2 + B(x)$ *est une somme de* 3 *carrés dans* $\mathbb{R}(x,y)$ *si et seulement si il existe un point* (α, β), *défini sur* $\mathbb{R}(x)$, *sur la courbe* $\mathcal{C}^{-1}_{\mathbb{R}(x)} : -\beta^2 = \alpha(\alpha^2 - 2A(x)\alpha + A^2(x) - 4B(x))$ *avec* α *et* $-(\alpha^2 - 2A(x)\alpha + A^2(x) - 4B(x))$ *tous deux sommes de deux carrés dans* $\mathbb{R}(x)$. *Un tel point est dit spécial.*

Preuve. On rappelle ici celle donnée par Cassels, Ellison et Pfister :

Si $F(x,y)$ est somme de 3 carrés dans $\mathbb{R}(x,y)$, il l'est aussi dans $\mathbb{R}(x)[y]$ [Ca1], de plus F étant de degré 4 en y, on aurait alors : $F(x,y) = \sum_{i=1}^{3}(a_i y^2 + b_i y + c_i)^2$ avec $a_i, b_i, c_i \in \mathbb{R}(x)$, on obtient donc le système :

$$\begin{cases} \sum_{i=1}^3 a_i^2 = 1 \\ \sum_{i=1}^3 a_i b_i = 0 \\ \sum_{i=1}^3 b_i^2 + 2\sum_{i=1}^3 a_i c_i = A \\ \sum_{i=1}^3 b_i c_i = 0 \\ \sum_{i=1}^3 c_i^2 = B \end{cases}$$

Comme $a_1^2 + a_2^2 + a_3^2 = 1$, le vecteur $(a_1, a_2, a_3) \in \mathbb{R}(x)^3$ est unitaire et on peut donc trouver une transformation orthogonale h sur $\mathbb{R}(x)^3$ telle que l'image du vecteur (a_1, a_2, a_3) par h soit le vecteur $(1,0,0)$. On peut par exemple choisir la symétrie orthogonale transformant (a_1, a_2, a_3) en $(1,0,0)$ et qui est définie par la formule :

pour tout $(u,v,w) \in \mathbb{R}(x)^3$,

$$h(u,v,w) = \left(u - 2(a_1 - 1)\frac{(a_1-1)u + a_2 v + a_3 w}{(a_1-1)^2 + a_2^2 + a_3^2}, v - 2a_2\frac{(a_1-1)u + a_2 v + a_3 w}{(a_1-1)^2 + a_2^2 + a_3^2}, \right.$$

$$\left. w - 2a_3\frac{(a_1-1)u + a_2 v + a_3 w}{(a_1-1)^2 + a_2^2 + a_3^2} \right).$$

Grâce à cette transformation, on peut supposer que $a_1 = 1$ et $a_2 = a_3 = 0$ et on est ramené au système :

$$\begin{cases} b_1 = 0 \\ b_2^2 + b_3^2 = A - 2c_1 \\ b_2 c_2 + b_3 c_3 = 0 \\ c_2^2 + c_3^2 = B - c_1^2 \end{cases}$$

Cela implique que :

$$\begin{aligned}(A-2c_1)(B-c_1^2) &= (b_2^2+b_3^2)(c_2^2+c_3^2)\\ &= (b_2c_2+b_3c_3)^2+(b_2c_3+b_3c_2)^2\\ &= (b_2c_3+b_3c_2)^2\end{aligned}$$

On pose $\alpha = A-2c_1$ et $\beta = 2(b_2c_3+b_3c_2)$, et comme $B-c_1^2 = B-\frac{1}{4}(\alpha-A)^2$, on obtient : $\alpha((\alpha-A)^2-4B) = -\beta^2$ avec $\alpha = b_2^2+b_3^2$ et $-((\alpha-A)^2-4B) = 4(c_2^2+c_3^2)$. Donc α et $-(\alpha^2-2A\alpha+A^2-4B)$ sont bien des sommes de 2 carrés dans $\mathbb{R}(x)$ et le point (α,β) ainsi obtenu est spécial.

Réciproquement, s'il existe un point spécial sur $\mathcal{C}^{-1}_{\mathbb{R}(x)}$, deux cas se présentent :

* Soit $\alpha = 0$, dans ce cas $4B-A^2 = d^2+e^2$ $(d,e \in \mathbb{R}(x))$ et on prend $b_1 = b_2 = b_3 = 0$, $2c_1 = A$, $2c_2 = d$, $2c_3 = e$.

* Soit $\alpha \neq 0$ et on peut écrire $\alpha = b_2^2+b_3^2 \neq 0$ et alors $4B-(\alpha-A)^2 = \left(\frac{\beta}{\alpha}\right)^2(b_2^2+b_3^2)$. On peut donc prendre $b_1 = 0$, $2c_1 = A-\alpha$, $2c_2 = \frac{\beta}{\alpha}b_3$ et $2c_3 = -\frac{\beta}{\alpha}b_2$.

On vérifie alors facilement que dans ces deux cas on obtient une représentation de $F(x,y)$ comme somme de 3 carrés. □

Remarque 1.1.2 Si (α,β) est un point de $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ et si $\beta \neq 0$, c'est-à-dire (α,β) n'est pas un point d'ordre 2, alors (α,β) est spécial si et seulement si α est somme de 2 carrés.

Preuve. Il suffit de remarquer qu'alors $\alpha(4B-A^2+2A\alpha-\alpha^2) = \beta^2 \neq 0$ et on en déduit que $(4B-A^2+2A\alpha-\alpha^2)$ est, comme α, somme de 2 carrés. □

Remarque 1.1.3 *On peut signaler que l'équation de la courbe* $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ *:* $-\beta^2 = \alpha(\alpha^2-2A(x)\alpha+A^2(x)-4B(x))$ *est aussi une forme de Weierstrass de l'équation de la jacobienne de la quartique* $Z^2+F(x,y)=0$*, toujours avec* $F(x,y) = 1+A(x)y^2+B(x)y^4$*, définie sur le corps* $\mathbb{R}(x)$*. Le résultat précédent apparaît donc comme un cas particulier de celui démontré dans [HM] : un point spécial sur la courbe* $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ *correspond à un point qui reste toujours sur la composante non-neutre de cette jacobienne pour tout ordre de* $\mathbb{R}(x)$*.*

1.2 Idée générale pour obtenir la non-existence de points spéciaux

D'après le théorème 1.1.1, démontrer qu' un polynôme $F(x,y) = y^4 + A(x)y^2 + B(x)$ n'est pas somme de 3 carrés dans $\mathbb{R}(x,y)$ revient à démontrer la non existence d'un point spécial sur la courbe elliptique $\mathcal{C}^{-1}$ associée à ce polynôme $F(x,y)$.

Suivant en cela Cassels, Ellison et Pfister, Christie traite ce problème par une étude presque complète du groupe $\mathcal{C}^{-1}_{\mathbb{C}(x)}$. Dans un premier temps, il montre que les points d'ordre fini ne sont pas spéciaux, puis dans un second temps, il prouve que la courbe $\mathcal{C}^{-1}$ est de rang nul sur $\mathbb{C}(x)$.

Voici dans les grandes lignes l'architecture de cette démonstration : on notera k_0 le plus petit corps tel que $\mathcal{C}^{-1}$ soit définie sur $k_0(x)$ (c'est-à-dire $A(x)$ et $B(x)$ sont tous deux éléments de $k_0[x]$). Par l'application du théorème de Lang-Néron [La], en se plaçant dans les conditions requises, on obtiendra que tous les points de la courbe $\mathcal{C}^{-1}_{\mathbb{C}(x)}$ sont définis sur un corps $K_0(x)$ où K_0 est une extension Galoisienne finie du corps k_0, puis grâce à des éléments de théorie de Galois appliqués à K_0/k, où k est une extension intermédiaire spécifique et connue de k_0, on montrera que l'existence de points d'ordre infini sur $\mathcal{C}^{-1}_{\mathbb{C}(x)} = \mathcal{C}^{-1}_{K_0(x)}$ implique l'existence de points d'ordre infini sur des courbes $\mathcal{C}^{-d}_{k(x)}$ pour certaines valeurs de $d \in k^*$. On se sera ainsi ramené à étudier des courbes elliptiques sur le corps $k(x)$ plutôt que sur $\mathbb{C}(x)$, ce qui en pratique se révèle plus aisé. Pour permettre cette étude, on énoncera une proposition donnant des conditions suffisantes pour qu'aucune des courbes $\mathcal{C}^{-d}_{k(x)}$ pour $d \in k^*$ n'ait de point d'ordre infini défini sur $k(x)$. Il restera alors à s'assurer que ces conditions sont vérifiées mais, pour cela, il n'y a pas d'argument général et il faudra procéder à l'étude au cas par cas des exemples proposés.

1.3 Notations-définitions

Pour démontrer que le polynôme $F(x,y) = y^4 + A(x)y^2 + B(x)$ n'est pas une somme de trois carrés de fractions rationnelles, on doit faire l'étude de la courbe $\mathcal{C}^{-1} : -\beta^2 = \alpha(\alpha^2 - 2A(x)\alpha + A^2(x) - 4B(x))$. Afin d'alléger les notations, on remplacera $A(x)$ par A et $B(x)$ par B. On rappelle que A et B sont définis sur $k_0(x)$, avec $k_0 \subset \mathbb{R}$.

L'etude de cette courbe $\mathcal{C}^{-1}$ nécessite l'introduction de plusieurs éléments :

Courbes elliptiques associées au polynôme F :

Soit $d \in \mathbb{C}^*$, on définit deux courbes elliptiques par les équations de Weierstrass suivantes :

* La courbe $\mathcal{C}^{-d}$ d'équation : $-d\beta^2 = \alpha(\alpha^2 - 2A\alpha + A^2 - 4B)$,

* La courbe $\mathcal{D}^{-d}$ d'équation $-d\beta^2 = \alpha(\alpha^2 + 4A\alpha + 16B)$.

Si K est une extension de $k_0(x)$, on appelle $\mathcal{C}_K^{-d}$ et $\mathcal{D}_K^{-d}$ les groupes des points de $\mathcal{C}^{-d}$ et $\mathcal{D}^{-d}$ définis sur le corps K.

On note $\mathcal{O}_\mathcal{C}$ et $\mathcal{O}_\mathcal{D}$ les points à l'infini sur $\mathcal{C}^{-d}$ et $\mathcal{D}^{-d}$ respectivement, pris comme origine des groupes de Mordell-Weil. Dans tous les cas, les courbes $\mathcal{C}^{-d}$ et $\mathcal{D}^{-d}$ ont au moins un point d'ordre 2, $\mathcal{P}_\mathcal{C} = (0,0)$ sur $\mathcal{C}^{-d}$ et $\mathcal{P}_\mathcal{D} = (0,0)$ sur $\mathcal{D}^{-d}$. L'existence d'autres points K-rationnels d'ordre 2 dépend de l'éventuelle possibilité de factoriser, sur le corps K, les polynômes $(\alpha^2 - 2A\alpha + A^2 - 4B)$ et $(\alpha^2 + 4A\alpha + 16B)$.

Isogénies :

On connait les isogénies de degré 2 suivantes, leurs composées étant les multiplications par 2 dans les groupes correspondants :

$\varphi_{\mathcal{C},\mathcal{D}} : \mathcal{C}^{-d} \to \mathcal{D}^{-d}$ définie par :

$$\varphi_{\mathcal{C},\mathcal{D}}(\alpha,\beta) = \left(\tfrac{-d\beta^2}{\alpha^2}, \tfrac{\alpha^2-(A^2-4B)}{\alpha^2}\beta\right) \text{ si } \alpha \neq 0,$$
$$\varphi_{\mathcal{C},\mathcal{D}}(\mathcal{P}_\mathcal{C}) = \mathcal{O}_\mathcal{D} \quad \text{et} \quad \varphi_{\mathcal{C},\mathcal{D}}(\mathcal{O}_\mathcal{C}) = \mathcal{O}_\mathcal{D}.$$

$\varphi_{\mathcal{D},\mathcal{C}} : \mathcal{D}^{-d} \to \mathcal{C}^{-d}$ définie par :

$$\varphi_{\mathcal{D},\mathcal{C}}(\alpha,\beta) = \left(\tfrac{-d\beta^2}{4\alpha^2}, \tfrac{\alpha^2-16B}{8\alpha^2}\beta\right) \text{ si } \alpha \neq 0,$$
$$\varphi_{\mathcal{D},\mathcal{C}}(\mathcal{P}_\mathcal{D}) = \mathcal{O}_\mathcal{C} \quad \text{et} \quad \varphi_{\mathcal{D},\mathcal{C}}(\mathcal{O}_\mathcal{D}) = \mathcal{O}_\mathcal{C}.$$

Morphismes :

On aura aussi besoin pour étudier $\mathcal{C}^{-1}$ des morphismes $\gamma_{\mathcal{C}} : \mathcal{C}_K^{-d} \to K^*/K^{*2}$ et $\gamma_{\mathcal{D}} : \mathcal{D}_K^{-d} \to K^*/K^{*2}$ définis respectivement par:

$$\gamma_{\mathcal{C}}(\alpha, \beta) = -d\alpha K^{*2} \text{ si } \alpha \neq 0,$$

$$\gamma_{\mathcal{C}}(\mathcal{P}_{\mathcal{C}}) = (A^2 - 4B)K^{*2} \quad \text{et} \quad \gamma_{\mathcal{C}}(\mathcal{O}_{\mathcal{C}}) = K^{*2},$$

et par :

$$\gamma_{\mathcal{D}}(\alpha, \beta) = -d\alpha K^{*2} \text{ si } \alpha \neq 0,$$

$$\gamma_{\mathcal{D}}(\mathcal{P}_{\mathcal{D}}) = 16BK^{*2} \quad \text{et} \quad \gamma_{\mathcal{D}}(\mathcal{O}_{\mathcal{D}}) = K^{*2}.$$

L'intérêt de ces morphisme est que le noyau de $\gamma_{\mathcal{C}}$ est $\varphi_{\mathcal{D},\mathcal{C}}(\mathcal{D}_K^{-d})$ et que le noyau de $\gamma_{\mathcal{D}}$ est $\varphi_{\mathcal{C},\mathcal{D}}(\mathcal{C}_K^{-d})$, cela donne, entre autre, un critère simple pour affirmer qu'un point du groupe $\mathcal{C}_K^{-d}$ ne peut pas être un double.

Remarque 1.3.1 Lorsque $K = \mathbb{R}(x)$, le morphisme $\gamma_{\mathcal{C}}$ permet aussi de donner une caractérisation des points spéciaux de $\mathcal{C}^{-1}_{\mathbb{R}(x)}$. En effet, on constate que, par définition (voir théorème 1.1.1), un point de $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ est spécial si et seulement si son image dans $\mathbb{R}(x)^*/\mathbb{R}(x)^{*2}$ par le morphisme $\gamma_{\mathcal{C}}$ est la classe d'une fraction négative ou nulle de $\mathbb{R}(x)^*$.

Pour pouvoir appliquer la technique d'étude de la courbe $\mathcal{C}^{-1}$ proposée ici, il faut que cette courbe présente certaines propriétés, on est donc amené à donner la définition suivante :

Définition 1.3.2 *On dira que la courbe $\mathcal{C}^{-1}$ (respectivement $\mathcal{D}^{-1}$) est à 2-torsion K-rationnelle lorsque tous les points d'ordre 2 de cette courbe $\mathcal{C}^{-1}$ (respectivement $\mathcal{D}^{-1}$) sont définis sur le corps K.*

Remarque 1.3.3 La courbe elliptique $\mathcal{C}^{-1}$ (respectivement $\mathcal{D}^{-1}$) est à 2-torsion K-rationnelle quand le polynôme $\alpha^2 - 2A\alpha + A^2 - 4B$ (respectivement $\alpha^2 + 4A\alpha + 16B$) est décomposé sur K (en tant que polynôme en la variable α), c'est-à-dire quand B (respectivement $A^2 - 4B$) est un carré dans K.

Pour la suite de l'étude, il est nécessaire que l'une des deux courbes $\mathcal{C}^{-1}$ ou $\mathcal{D}^{-1}$ soit à 2-torsion $\mathbb{C}(x)$-rationnelle, c'est pourquoi on se placera dans ce cas de figure et on va supposer que la courbe $\mathcal{C}^{-1}$ est à 2-torsion $\mathbb{C}(x)$-rationnelle. Dans le cas où seule la courbe $\mathcal{D}^{-1}$ est à 2-torsion $\mathbb{C}(x)$-rationnelle, l'étude se déroule de la même manière, il suffit d'intervertir les deux courbes $\mathcal{C}^{-1}$ et $\mathcal{D}^{-1}$: en effet, comme l'image par $\varphi_{\mathcal{C},\mathcal{D}}$ d'un point d'ordre infini de $\mathcal{C}^{-1}$ est un point d'ordre infini de $\mathcal{D}^{-1}$, l'existence de points d'ordre infini sur $\mathcal{C}^{-1}$ est équivalente à l'existence de points d'ordre infini sur $\mathcal{D}^{-1}$.

On va donc supposer que B est un carré dans $\mathbb{C}(x)$, B étant un polynôme, on a alors $B = C^2$, $C \in \mathbb{C}[x]$. On peut alors écrire l'équation de $\mathcal{C}^{-1}$ sous la forme :

$$-\beta^2 = \alpha(\alpha - A + 2C)(\alpha - A - 2C)$$

La courbe $\mathcal{C}^{-1}$ a alors deux autres points d'ordre 2 : $\mathcal{P}_1 = (A - 2C, 0)$ et $\mathcal{P}_2 = (A + 2C, 0)$.

On peut, lorsque $\mathcal{C}^{-1}$ est à 2-torsion K-rationnelle, définir un morphisme $\pi : \mathcal{C}_K^{-1} \to (K^*/K^{*2})^3$ dont le noyau est $2\mathcal{C}_K^{-1}$, défini par:

$$\pi(\alpha, \beta) = (-\alpha K^{*2}, -(\alpha - A + 2C)K^{*2}, -(\alpha - A - 2C)K^{*2}) \text{ si } \beta \neq 0,$$

$$\pi(\mathcal{P}_\mathcal{C}) = ((A^2 - 4B)K^{*2}, -(-A + 2C)K^{*2}, -(-A - 2C)K^{*2}),$$

$$\pi(\mathcal{P}_1) = (-(A - 2C)K^{*2}, -4C(A - 2C)K^{*2}, 4CK^{*2}),$$

$$\pi(\mathcal{P}_2) = (-(A + 2C)K^{*2}, -4CK^{*2}, 4C(A + 2C)K^{*2}),$$

$$\pi(\mathcal{O}_\mathcal{C}) = (K^{*2}, K^{*2}, K^{*2}).$$

Ce morphisme π permet de caractériser les doubles de $\mathcal{C}^{-1}$ sur K et dans l'utilisation que l'on en fera, il est nécessaire d'énoncer le lemme suivant :

Lemme 1.3.4 ([Chr] lemme 1) *Si k est une extension de k_0 sur laquelle les polynômes B et $A^2 - 4B$ sont scindés, les représentants dans $(\mathbb{C}(x)^*/\mathbb{C}(x)^{*2})^3$ des images par π des points de $\mathcal{C}_{\mathbb{C}(x)}^{-1}$ peuvent être choisis dans $k[x]$.*

Preuve. C'est évident pour les points d'ordre inférieur à 2, car ils sont définis sur $k_0[x]$.

Pour $(\alpha,\beta)\in\mathcal{C}^{-1}_{\mathbb{C}(x)}$ avec $\beta\neq 0$, on peut poser $\alpha=\frac{\omega}{P}$ et $\beta=\frac{\chi}{Q}$, où χ, ω, P et Q sont des polynômes de $\mathbb{C}[x]^*$ tels que $\mathrm{pgcd}(\omega,P)=\mathrm{pgcd}(\chi,Q)=1$. Cela donne alors :

$$-\frac{\chi^2}{Q^2}=\frac{\omega}{P}\left(\frac{\omega^2}{P^2}-2A\frac{\omega}{P}+A^2-4B\right),$$

ou encore, après simplification :

$$-\chi^2P^3=\omega\left(\omega^2-2A\omega P+(A^2-4B)P^2\right)Q^2.$$

On voit que Q^2 divise χ^2P^3 et comme $\mathrm{pgcd}(\chi,Q)=1$, Q^2 divise P^3. On remarque aussi que P^3 divise $\omega\left(\omega^2-2A\omega P+(A^2-4B)P^2\right)Q^2$ et comme on a aussi $\mathrm{pgcd}(\omega,P)=1$, ce dont on déduit que $\mathrm{pgcd}(P^3,\omega)=\mathrm{pgcd}(P^3,\omega^2-2A\omega P+(A^2-4B)P^2)=1$, cela montre que P^3 divise Q^2. On a donc, quitte à multiplier Q et χ par une même constante non nulle, $P^3=Q^2$ ce qui implique que P est un carré dans $\mathbb{C}[x]$, et en notant $P=\psi^2$, on peut écrire $Q=\psi^3$, $\alpha=\frac{\omega}{\psi^2}$ et $\beta=\frac{\chi}{\psi^3}$, où ψ, χ, $\omega\in\mathbb{C}[x]$ avec $\mathrm{pgcd}(\omega,\psi)=\mathrm{pgcd}(\chi,\psi)=1$.

Puisque $\pi(\alpha,\beta)=(-\alpha\mathbb{C}(x)^{*2},-(\alpha-A+2C)\mathbb{C}(x)^{*2},-(\alpha-A-2C)\mathbb{C}(x)^{*2})$, on obtient :

$$\pi(\alpha,\beta)=(-\omega\mathbb{C}(x)^{*2},(-\omega+(A-2C)\psi^2)\mathbb{C}(x)^{*2},(-\omega+(A+2C)\psi^2)\mathbb{C}(x)^{*2}).$$

On pose alors $-\omega=fR^2$, $-\omega+(A-2C)\psi^2=gS^2$ et $-\omega+(A+2C)\psi^2=hT^2$, où R, S, T, f, g et h sont des éléments de $\mathbb{C}[x]$, f, g et h étant sans facteur carré et unitaires. On a ainsi : $\pi(\alpha,\beta)=(f\mathbb{C}(x)^{*2},g\mathbb{C}(x)^{*2},h\mathbb{C}(x)^{*2})$.

Etant donné que $fghR^2S^2T^2=\chi^2$, on a $fgh\in\mathbb{C}[x]^{*2}$, ce qui implique que $f=f_1f_2$, $g=f_1f_3$ et $h=f_2f_3$, avec f_1, f_2, $f_3\in\mathbb{C}[x]$, unitaires.

Alors f_1 divise ω et $(-\omega+(A-2C)\psi^2)$, donc divise aussi $(A-2C)\psi^2$. Etant donné que f_1 divise ω et que $\mathrm{pgcd}(\omega,\psi)=1$, on a f_1 qui divise $(A-2C)$, ainsi que (A^2-4B) dans $\mathbb{C}[x]$. Comme f_1 est unitaire et que A^2-4B est scindé sur $k[x]$, alors $f_1\in k[x]$.

De même, f_2 divise ω et $(-\omega+(A+2C)\psi^2)$ donc il divise $(A+2C)\psi^2$, étant premier avec ψ, on en déduit qu'il divise $(A+2C)$ et donc aussi A^2-4B, étant unitaire il appartient à $k[x]$.

Dans le cas de f_3, on sait que ce polynôme divise $(-\omega+(A-2C)\psi^2)$ et $(-\omega+(A+2C)\psi^2)$ donc divise aussi la différence de ces deux polynômes c'est-à-dire $4C\psi^2$. Mais on a aussi $\mathrm{pgcd}(f_3,\psi)=1$, sinon on obtiendrait un facteur

commun à ω et à ψ (car $-\omega + (A-2C)\psi^2 = f_1 f_3 S^2$). Donc f_3 divise C, alors f_3 qui est unitaire, divise B qui est scindé sur k et cela donne $f_3 \in k[x]$.

Comme f_1, f_2 et f_3 sont des éléments de $k[x]$, f, g et h le sont aussi et, d'après ce qui précède, $\pi(\alpha,\beta) = (f\mathbb{C}(x)^{*2}, g\mathbb{C}(x)^{*2}, h\mathbb{C}(x)^{*2})$, ce qui donne le résultat énoncé. □

Remarque 1.3.5 Pour la suite, il sera nécessaire de choisir le corps k de telle façon que le polynôme B soit un carré dans $k(x)$ afin que la courbe elliptique $\mathcal{C}^{-1}$ soit à 2-torsion $k(x)$-rationnelle.

1.4 Points d'ordre fini

L'objet de cette section est d'énoncer des résultats permettant de déterminer si les points d'ordre fini de la courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ sont ou non spéciaux.

(A) Etude des points d'ordre 2^n.

Bien qu'il n'y ait pas de résultat général concernant ces points, leur étude sur une courbe particulière ou sur une famille de courbe donnée ne pose pas de problème. En effet il est assez simple de déterminer explicitement ces points et donc de savoir s'ils sont spéciaux, il suffit pour cela de suivre le schéma suivant :

Partant des points d'ordre 2 sur $\mathcal{C}^{-d}_{\mathbb{R}(x)}$ que l'on détermine sans aucune difficulté, on calcule leur(s) image(s) dans $\mathbb{R}(x)^*/\mathbb{R}(x)^{*2}$ par le morphisme $\gamma_{\mathcal{C}}$, si l'un de ces points est dans $\ker\gamma_{\mathcal{C}} = \varphi_{\mathcal{D},\mathcal{C}}(\mathcal{D}^{-d}_{\mathbb{R}(x)})$, on recherche ses antécédents par $\varphi_{\mathcal{D},\mathcal{C}}$, ce qui revient à résoudre une équation de degré 2 dans le corps $\mathbb{R}(x)$.

On a ainsi obtenu sur $\mathcal{D}^{-d}_{\mathbb{R}(x)}$, des points qui seront soit d'ordre 2 (s'ils sont les antécédents par $\varphi_{\mathcal{D},\mathcal{C}}$ du point $\mathcal{P}_{\mathcal{C}}$), soit 4 (s'ils sont les antécédents par $\varphi_{\mathcal{D},\mathcal{C}}$ d'un autre point d'ordre 2 de $\mathcal{C}^{-1}$). On étudie alors les images par $\gamma_{\mathcal{D}}$ de ces points de $\mathcal{D}^{-d}_{\mathbb{R}(x)}$, si certains d'entre eux appartiennent à $\ker\gamma_{\mathcal{D}} = \varphi_{\mathcal{C},\mathcal{D}}(\mathcal{C}^{-d}_{\mathbb{R}(x)})$, on recherche leurs antécédents par $\varphi_{\mathcal{C},\mathcal{D}}$ ce qui donne sur $\mathcal{C}^{-d}_{\mathbb{R}(x)}$ des points d'ordre 4 ou d'ordre 8, points dont on va calcule l'image par $\gamma_{\mathcal{C}}$, et ainsi de suite jusqu'à ce qu'aucun des derniers points obtenus ne soit dans le noyau de $\gamma_{\mathcal{C}}$ ou $\gamma_{\mathcal{D}}$, alors ces points ne pourront pas être des doubles et l'étude des points d'ordre 2^n sera achevée.

En pratique, on pourra s'assurer, grâce à des hypothèses simples portant sur A et B, qu'il n'y a pas de points d'ordre 2^n avec $n > 1$, $n > 2$ ou $n > 3$ selon les exemples traités.

Une fois que les points d'ordre 2^n de $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ ont été tous déterminés, il reste à vérifier qu'aucun d'entre eux n'est spécial, ce qui, là encore dépend de la forme de A et$B$.

(B) Etude des points d'ordre impair.

Il n'est pas nécessaire de chercher à déterminer ces points car on a le résultat suivant :

Proposition 1.4.1 *Sur $\mathcal{C}^{-1}_{\mathbb{R}(x)}$, aucun des points d'ordre impair n'est spécial.*

Preuve. Soit p un point d'ordre $m = 2k+1$, $k \in \mathbb{N}^*$ sur $\mathcal{C}^{-1}_{\mathbb{R}(x)}$, alors sa première coordonnée α_p est non nulle et de plus on a $p = 2\left(\frac{m+1}{2}\right)p$, donc $p = \varphi_{\mathcal{D},\mathcal{C}}(\varphi_{\mathcal{C},\mathcal{D}}(\frac{m+1}{2}p))$ d'où $p \in \varphi_{\mathcal{C},\mathcal{D}}(\mathcal{D}^{-1}_{\mathbb{R}(x)}) = \ker\gamma_{\mathcal{C}}$, donc $-\alpha_p \in \mathbb{R}(x)^{*2}$.

Ainsi α_p n'est clairement pas somme de 2 carrés dans $\mathbb{R}(x)$ et p n'est pas un point spécial. □

Remarque 1.4.2 On sait aussi, d'après Hellegouarch [He], que sur une telle courbe elliptique $\mathcal{C}^{-1}$ non birationnellement équivalente à une courbe définie sur $\mathbb{C}$, il n'y a pas de point d'ordre premier supérieur à 3, et un point d'ordre 3 serait de la forme (α, β), défini sur $\mathbb{C}(x)$ avec $\alpha \in \mathbb{C}[x]$ solution de :

$$3\alpha^4 - 8A\alpha^3 + 6(A^2 - 4B)\alpha^2 - (A^2 - 4B)^2 = 0$$

Lorsque $A^2 - 4B$ est de faible degré, on pourrait éventuellement vérifier si un tel point peut exister et le déterminer si c'est le cas.

(C) Etude des points d'ordre $2^n(2k+1)$, pour n, k entiers non nuls.

Ici encore on a un résultat général permettant d'éviter le recours à la détermination de tous ces points :

Proposition 1.4.3 *Sur $\mathcal{C}^{-1}_{\mathbb{R}(x)}$, si aucun des points d'ordre 2^m, $m \in \mathbb{N}^*$, n'est spécial, alors aucun des points d'ordre $2^n(2k+1)$, $n, k \in \mathbb{N}^*$, n'est spécial.*

Preuve. Soit p un point d'ordre $2^n(2k+1)$, alors $\gamma_c((2k+1)p) = \gamma_c(kp)^2\gamma_c(p)$ et comme $\gamma_c(kp)^2 \in \mathbb{R}(x)^{*2}$, on obtient $\gamma_c(p) = \gamma_c((2k+1)p)$. Le point $(2k+1)p$, d'ordre 2^n, n'est pas spécial et d'après la remarque 1.3.1, son image dans $\mathbb{R}(x)^*/\mathbb{R}(x)^{*2}$ par le morphisme γ_c n'est pas la classe d'une fraction négative ou nulle de $\mathbb{R}(x)^*$. On en déduit que l'image de p par γ_c n'est pas non plus négative ou nulle et que p n'est donc pas un point spécial. □

D'après les propositions précédentes, on constate que l'étude des points d'ordre fini de $\mathcal{C}^{-1}_{\mathbb{R}[x]}$ pourra se limiter à la détermination des points d'ordre 2^n, $n \in \mathbb{N}$.

1.5 Points d'ordre infini

L'objectif de cette section est de substituer à l'étude des points d'ordre infini de la courbe complexe $\mathcal{C}^{-1}_{\mathbb{C}(x)}$ celle, plus simple, des points d'ordre infini des courbes elliptiques $\mathcal{C}^{-d}_{k(x)}$ et $\mathcal{D}^{-d}_{k(x)}$ où $d \in k$ et k est le corps de décomposition du polynôme $B(A^2-4B)$ (cf lemme 1.3.4), en particulier, on souhaite arriver au résultat suivant :

Proposition 1.5.1 (D'après [Chr], corollaire de la proposition 2) *Si pour tout nombre $d \in k^*$, les images des morphismes $\gamma_c : \mathcal{C}^{-d}_{k(x)} \to k(x)^*/k(x)^{*2}$ et $\gamma_{\mathcal{D}} : \mathcal{D}^{-d}_{k(x)} \to k(x)^*/k(x)^{*2}$ sont les images des points de torsion, alors il n'y a pas de point d'ordre infini ni sur la courbe $\mathcal{C}^{-1}_{\mathbb{C}(x)}$, ni sur la courbe $\mathcal{D}^{-1}_{\mathbb{C}(x)}$.*

C'est la partie la plus délicate de ce chapitre et il n'est pas inutile d'indiquer les lignes principales de la démonstration avant d'entrer dans les détails :

(A) On montre qu'il existe une extension finie galoisienne $k \to K$ telle que $\mathcal{C}^{-1}_{\mathbb{C}(x)} = \mathcal{C}^{-1}_{K(x)}$. On note $\mathcal{A}$ le groupe quotient de $\mathcal{C}^{-1}_{K(x)}$ par sa torsion.

(B) On montre que l'action de $\Gamma = Gal(K/k)$ sur $\mathcal{A}/2\mathcal{A}$ est triviale et on en déduit qu'il existe une base de $\mathcal{A}$ sur laquelle Γ agit comme ± 1.

(C) Ceci permet de montrer que si $\mathcal{A}$ est non nul, alors une courbe $\mathcal{C}^{-d}_{k(x)}$ est aussi de rang non nul pour un certain $d \in k^*$.

(D) On termine en énonçant une proposition permettant de montrer, sur les exemples choisis, que toutes les courbes $\mathcal{C}^{-d}_{k(x)}$ sont de rang nul.

La faiblesse principale de cette méthode vient de ce que l'utilisation de la théorie de Galois force à faire abstraction des questions réelles et la notion de point spécial en particulier n'a plus de sens dans ce contexte. Pour montrer que la courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ n'a pas de point spécial, on est donc amené à montrer que la courbe $\mathcal{C}^{-1}_{\mathbb{C}(x)}$ est de rang nul, ce qui est extrêmement plus fort.

(A) Première descente sur le corps $K(x)$

Ce raisonnement repose sur un argument clé, le théorème de Lang-Néron ([La], p. 27, Théorème 4.2), analogue du théorème de Mordell-Weil pour les corps de fonctions :

Théorème 1.5.2 (Théorème de Lang-Néron) *Si la courbe $\mathcal{C}^{-1}$ (respectivement $\mathcal{D}^{-1}$) n'est pas birationnellement équivalente à une courbe définie sur $\mathbb{C}$, alors le groupe $\mathcal{C}^{-1}_{\mathbb{C}(x)}$ (respectivement $\mathcal{D}^{-1}_{\mathbb{C}(x)}$) est de type fini.*

On peut facilement, dans les exemples traités, s'assurer que les courbes $\mathcal{C}^{-1}$ et $\mathcal{D}^{-1}$ ne sont pas birationnellement équivalentes à des courbes définies sur $\mathbb{C}$ grâce à la propriété suivante :

Propriété 1.5.3 *Lorsque la fraction rationnelle $\frac{A^2}{B}$ n'est pas constante, les courbes $\mathcal{C}^{-1}_{\mathbb{C}(x)}$ et $\mathcal{D}^{-1}_{\mathbb{C}(x)}$ étudiées ici ne sont pas birationnellement équivalentes à des courbes définies sur $\mathbb{C}$.*

Preuve. Pour que la courbe $\mathcal{C}^{-1}_{\mathbb{C}(x)}$ ne soit pas birationnellement équivalente à une courbe définie sur $\mathbb{C}$, il suffit que son invariant j ne soit pas une constante et cet invariant j est donné, à multiplication par une constante près, par la formule $\frac{(A^2-3B)^3}{B^2(A^2-4B)}$. En posant $D = A^2 - 4B$, $Q = \mathrm{pgcd}(B, D)$, $B = B'Q$ et $D = D'Q$ (B' et D' sont alors deux polynômes premiers entre eux), on obtient :

$$\frac{(A^2-3B)^3}{B^2(A^2-4B)} = \frac{(B+D)^3}{B^2D} = \frac{(B'+D')^3}{B'^2D'}.$$

Si cet invariant j est constant, alors B' divise $(B'+D')^3$ donc aussi D'^3 et, comme $\mathrm{pgcd}(B', D') = 1$, alors $B' = c_1 \in \mathbb{C}$, de même $D' = c_2 \in \mathbb{C}$ et on en déduit que $B = c_1Q$ et que $A^2 - 4B = c_2Q$ donc $A^2 = (c_2 - 4c_1)Q$ (on remarque au passage que Q est un carré dans $\mathbb{C}[x]$) et cela implique que $\frac{A^2}{B} = \frac{c_2-4c_1}{c_1}$.

En conclusion, si l'invariant j est une constante, alors $\frac{A^2}{B} \in \mathbb{C}$, ce qui démontre la propriété. □

Par la suite, on choisira A et B de telle façon que $\frac{A^2}{B} \notin \mathbb{C}$, les courbes $\mathcal{C}^{-1}$ et $\mathcal{D}^{-1}$ ne seront alors pas birationnellement équivalentes à des courbes définies sur $\mathbb{C}$, et donc les groupes $\mathcal{C}^{-1}_{\mathbb{C}(x)}$ et $\mathcal{D}^{-1}_{\mathbb{C}(x)}$ seront de type fini d'après le théorème de Lang-Néron. On en déduit le résultat suivant :

Corollaire 1.5.4 *Si la courbe $\mathcal{C}^{-1}$ est définie sur $k_0(x)$, alors tous les points de $\mathcal{C}^{-1}_{\mathbb{C}(x)}$ sont définis sur $K(x)$ où K est une extension algébrique finie fixée de k_0.*

Preuve. On montre premièrement que chaque point p de $\mathcal{C}^{-1}_{\mathbb{C}(x)}$ est défini sur $k_p(x)$ où k_p est une extension algébrique finie de k_0 : Supposons qu'un point p ne soit pas défini sur un tel corps, alors p est défini sur un corps de la forme $k'(x)$ où k' est une extension algébrique finie, contenue dans $\mathbb{C}$, de $k_0(t_1, \ldots, t_n)$ où les $t_1, \ldots, t_n$ sont algébriquement indépendants sur k_0. En spécialisant $t_1, \ldots, t_n$ sur le corps $\mathbb{C}$, on peut alors obtenir une infinité non dénombrable de points sur la courbe $\mathcal{C}^{-1}_{\mathbb{C}(x)}$ car elle est définie sur $k_0(x)$. Cela est impossible étant donné que $\mathcal{C}^{-1}_{\mathbb{C}(x)}$ est de type fini.

On définit alors K comme étant la plus petite extension de k_0 telle qu'un ensemble de générateurs de $\mathcal{C}^{-1}_{\mathbb{C}(x)}$ soit défini sur $K(x)$. Ainsi K est une extension algébrique finie de k_0 : les générateurs de $\mathcal{C}^{-1}_{\mathbb{C}(x)}$ sont en nombre fini et chacun d'entre eux est défini sur un corps du type $k_p(x)$ où k_p est une extension finie de k_0. Comme tout point est une combinaison de ces générateurs et que la formule d'addition de deux points d'une courbe elliptique est une fonction rationnelle, à coefficients dans $k_0(x)$, des coordonées de ces deux points, on vérifie aisément que tous les points de $\mathcal{C}^{-1}_{\mathbb{C}(x)}$ sont définis sur le corps $K(x)$. □

Remarque 1.5.5 Quitte à remplacer K par sa clôture normale sur k, on peut de plus supposer que l'extension K/k est galoisienne.

On est ici arrivé à la première étape de la preuve de la proposition 1.5.1, on a démontré que $\mathcal{C}^{-1}_{\mathbb{C}(x)} = \mathcal{C}^{-1}_{K(x)}$ où K est une extension finie de k_0, galoisienne sur k.

(B) Actions du groupe de Galois

On fait ici appel à des éléments de la théorie de Galois appliquée à l'action du groupe $\Gamma = Gal(K/k)$ sur un groupe quotient de $\mathcal{C}^{-1}_{K(x)}$. Tout d'abord, Γ agit sur $\mathcal{C}^{-1}_{\mathbb{C}(x)}$ ainsi que sur $\pi(\mathcal{C}^{-1}_{\mathbb{C}(x)})$, c'est à cette étape qu'apparaît la nécessité de choisir le corps k de telle manière que la courbe $\mathcal{C}^{-1}$ soit à 2-torsion $k(x)$-rationnelle car

alors les polynômes $A+2C$ et $A-2C$ sont définis sur $k(x)$ et on peut mettre en place les résultats intermédiaires suivants :

Proposition 1.5.6 *Les actions de Γ commutent avec le morphisme π. De plus, l'action de Γ sur $\pi(\mathcal{C}^{-1}_{\mathbb{C}(x)})$ est triviale.*

Preuve. Soient $(\alpha,\beta)\in\mathcal{C}^{-1}_{\mathbb{C}(x)}$ et $\sigma\in\Gamma$:
Si $\beta\neq 0$ on a, comme $A+2C,\ A-2C\in k(x)$:

$$\begin{aligned}\sigma(\pi(\alpha,\beta)) &= (\sigma(\alpha)\mathbb{C}(x)^{*2},\sigma(\alpha-(A-2C))\mathbb{C}(x)^{*2},\sigma(\alpha-(A+2C))\mathbb{C}(x)^{*2})\\ &= (\sigma(\alpha)\mathbb{C}(x)^{*2},(\sigma(\alpha)-(A-2C))\mathbb{C}(x)^{*2},(\sigma(\alpha)-(A+2C))\mathbb{C}(x)^{*2})\\ &= \pi(\sigma(\alpha,\beta)).\end{aligned}$$

Si $\beta=0$, le résultat est évident.

On a prouvé la première partie de la proposition et d'après le lemme 1.3.4, les repésentants de $\pi(\mathcal{C}^{-1}_{\mathbb{C}(x)})$ peuvent être choisis dans $k(x)$, donc l'action de Γ sur $\pi(\mathcal{C}^{-d}_{\mathbb{C}(x)})$ est triviale. □

Corollaire 1.5.7 *L'action de Γ sur $\mathcal{C}^{-1}_{\mathbb{C}(x)}/2\mathcal{C}^{-1}_{\mathbb{C}(x)}$ induite par l'action sur $\mathcal{C}^{-1}_{\mathbb{C}(x)}$ est triviale.*

Preuve. D'après la proposition précédente, si $(\alpha,\beta)\in\mathcal{C}^{-1}_{\mathbb{C}(x)}$ et $\sigma\in\Gamma$,

$$\pi(\sigma(\alpha,\beta))=\sigma(\pi(\alpha,\beta))=\pi(\alpha,\beta)$$

Donc $\sigma(\alpha,\beta)-(\alpha,\beta)\in\ker\pi$ c'est-à-dire $\sigma(\alpha,\beta)\equiv(\alpha,\beta)\,(\mathrm{mod}\ 2\mathcal{C}^{-1}_{\mathbb{C}(x)})$, l'action de σ sur $\mathcal{C}^{-1}_{\mathbb{C}(x)}/2\mathcal{C}^{-1}_{\mathbb{C}(x)}$ est triviale. □

On a maintenant réuni les conditions nécessaires pour appliquer le lemme suivant :

Lemme 1.5.8 ([Chr], lemme 3) *Soit Γ un groupe fini et $\mathcal{A}$ un groupe abélien libre de type fini sur lequel Γ agit. On suppose que l'action induite de Γ sur $\mathcal{A}/2\mathcal{A}$ est triviale. Alors il existe une base $\{a_i \mid 1\leq i\leq t\}$ de $\mathcal{A}$ telle que pour tout $\sigma\in\Gamma$, $\sigma(a_i)=a_i$ ou $\sigma(a_i)=-a_i$.*

Preuve. Quitte à remplacer Γ par Γ/Γ_0 où Γ_0 est le sous groupe des éléments de Γ agissant trivialement sur $\mathcal{A}$, on peut supposer que Γ agit fidèlement sur $\mathcal{A}$.

(i) On va d'abord montrer que Γ ne contient pas d'élément d'ordre impair non trivial :

On va prouver par récurrence sur m que pour tout $a \in \mathcal{A}$ et pour tout $\sigma \in \Gamma$ d'ordre impair, on a, pour tout $m \in \mathbb{N}^*$, $a - \sigma(a) \in 2^m\mathcal{A}$.

Pour $m = 1$, c'est vrai car Γ agit trivialement sur $\mathcal{A}/2\mathcal{A}$, ainsi pour tout $a \in \mathcal{A}$ et tout $\sigma \in \Gamma$, $a - \sigma(a) \in 2\mathcal{A}$, c'est donc aussi vrai dans le cas particulier où σ est d'ordre impair.

Soit maintenant $m \in \mathbb{N}^*$, on suppose que pour tout $a \in \mathcal{A}$ et tout $\sigma \in \Gamma$ d'ordre impair on a : $a - \sigma(a) \in 2^m\mathcal{A}$. On considère alors un élément $\sigma \in \Gamma$ d'ordre impair, on veut montrer que $a - \sigma(a) \in 2^{m+1}\mathcal{A}$. Pour cela on pose $\tau = \sigma^{(n+1)/2}$ où n est l'ordre de σ, alors τ est d'ordre impair et $\tau^2 = \sigma^{n+1} = \sigma$. Par l'hypothèse de récurrence, on sait que $a - \tau(a) \in 2^m\mathcal{A}$ c'est-à-dire $a - \tau(a) = 2^m b$ avec $b \in \mathcal{A}$. On a ainsi :

$$\begin{aligned} a - \sigma(a) &= a - \tau(a) + \tau(a) - \tau^2(a) \\ &= a - \tau(a) + \tau(a - \tau(a)) \\ &= 2^m b + \tau(2^m b) \\ &= 2^{m+1}b - 2^m b + 2^m\tau(b) \\ &= 2^{m+1}b - 2^m(b - \tau(b)) \end{aligned}$$

Or $b - \tau(b) \in 2\mathcal{A}$, donc on a bien $a - \sigma(a) \in 2^{m+1}\mathcal{A}$. On en déduit par récurrence que pour tout $\sigma \in \Gamma$ d'ordre impair et pour tout $m \in \mathbb{N}^*$, $a - \sigma(a) \in 2^m\mathcal{A}$.

Donc si σ est un élément d'ordre impair de Γ et a un élément quelconque de $\mathcal{A}$, on a : $a - \sigma(a) \in \cap_{m=1}^{\infty} 2^m\mathcal{A} = \{0\}$. Cela prouve que pour tout $a \in \mathcal{A}$, $\sigma(a) = a$, comme on a supposé que l'action de Γ sur $\mathcal{A}$ est fidèle, ce résultat implique que $\sigma = id$. Il n'y a donc pas d'élément d'ordre impair non trivial dans le groupe Γ.

(ii) Soit σ un élément d'ordre 2 de Γ, on pose $\mathcal{A}_+ = \{a \in \mathcal{A} \mid \sigma(a) = a\}$ et $\mathcal{A}_- = \{a \in \mathcal{A} \mid \sigma(a) = -a\}$. On va montrer que $\mathcal{A} = \mathcal{A}_+ \oplus \mathcal{A}_-$:

Soit $a \in \mathcal{A}$, on sait que $a - \sigma(a) \in 2\mathcal{A}$ donc on peut poser $a - \sigma(a) = 2b$ avec $b \in \mathcal{A}$.On peut ainsi écrire que $a = a - \sigma(a) + \sigma(a) = 2b + \sigma(a)$ c'est-à-dire $a = b + (b + \sigma(a))$. Il reste à démontrer que $b \in \mathcal{A}_-$ et que $b + \sigma(a) \in \mathcal{A}_+$.

Par définition de b, $2b = a - \sigma(a)$ donc $\sigma(2b) = \sigma(a - \sigma(a))$ et σ étant d'ordre 2, $\sigma(2b) = \sigma(a) - a = -2b$. Puisque $\mathcal{A}$ est sans torsion, $\sigma(b) = -b$ d'où $b \in \mathcal{A}_-$.

On a aussi $2(b + \sigma(a)) = a - \sigma(a) + 2\sigma(a) = a + \sigma(a)$ donc $\sigma(2(b + \sigma(a))) = \sigma(a + \sigma(a)) = \sigma(a) + a$ c'est-à-dire $\sigma(2(b + \sigma(a))) = 2(b + \sigma(a))$. Comme $\mathcal{A}$ est sans torsion, on obtient $\sigma(b + \sigma(a))) = b + \sigma(a)$ donc $b + \sigma(a) \in \mathcal{A}_+$.

Etant donné que $a = (b + \sigma(a)) + b$, on a bien $a \in \mathcal{A}_+ + \mathcal{A}_-$, ce qui prouve que $\mathcal{A} = \mathcal{A}_+ + \mathcal{A}_-$. De plus $\mathcal{A}$ est sans torsion donc $\mathcal{A}_+ \cap \mathcal{A}_- = \{0\}$ d'où $\mathcal{A} = \mathcal{A}_+ \oplus \mathcal{A}_-$.

(iii) On montre ensuite que Γ ne contient pas d'élément d'ordre 4 :

Supposons que $\tau \in \Gamma$ soit d'ordre 4, alors $\sigma = \tau^2$ est d'ordre 2 donc $\mathcal{A}_- = \{a \in \mathcal{A} \mid \sigma(a) = -a\}$ est non vide. Comme $\mathcal{A}$ est libre, il existe (au moins) un élément a de $\mathcal{A}_-$ non divisible par 2. Le groupe Γ agissant trivialement sur $\mathcal{A}/2\mathcal{A}$, $\tau(a) = a + 2c$ avec $c \in \mathcal{A}$ et $\tau(c) = c + 2d$ avec $d \in \mathcal{A}$. Donc :

$$\begin{array}{rcccl} -a & = & \sigma(a) & = & \tau^2(a) & = & \tau(a+2c) \\ & = & \tau(a) + 2\tau(c) & = & a + 2c + 2(c+2d) \\ & = & a + 4c + 4d \end{array}$$

D'où $2a = -4(c+d)$, comme $\mathcal{A}$ est sans torsion, $a = -2(c+d)$ ce qui contredit l'hypothèse disant que a n'est pas un double dans $\mathcal{A}$.

Il n'y a donc pas d'élément d'ordre 4 dans le groupe Γ.

(iv) On a ainsi montré que le groupe Γ est d'exposant 2 et est donc abélien. On peut maintenant prouver le lemme par récurrence sur l'ordre n de Γ :

Si $n = 1$, le résultat est évident.

Soit $n > 1$, on suppose que l'énoncé du lemme est vrai pour tout groupe d'ordre inférieur ou égal à $n-1$. Soit Γ un groupe d'ordre n vérifiant les conditions de l'énoncé, alors il admet un sous groupe G d'indice 2 (donc d'ordre strictement inférieur à n). Soit $\sigma \notin G$, ici encore on pose $\mathcal{A}_+ = \{a \in \mathcal{A} \mid \sigma(a) = a\}$ et $\mathcal{A}_- = \{a \in \mathcal{A} \mid \sigma(a) = -a\}$. Comme on l'a vu en *(ii)*, $\mathcal{A} = \mathcal{A}_+ \oplus \mathcal{A}_-$, de plus puisque Γ est abélien les groupes libres $\mathcal{A}_+$ et $\mathcal{A}_-$ sont invariants par l'action de G et les actions induites de G sur $\mathcal{A}_+/2\mathcal{A}_+$ et sur $\mathcal{A}_-/2\mathcal{A}_-$ sont, comme celles de Γ, triviales.

En appliquant l'hypothèse de récurrence au groupe G agissant sur $\mathcal{A}_+$ et sur $\mathcal{A}_-$, on peut choisir des bases $\{a_i \mid 1 \leq i \leq s\}$ et $\{a_i \mid s+1 \leq i \leq t\}$ de $\mathcal{A}_+$ et $\mathcal{A}_-$ respectivement telles que pour tout $\tau \in G$, $\tau(a_i) = a_i$ et $\tau(a_i) = -a_i$.

Donc si $\rho \in \Gamma$, soit $\rho \in G$, soit $\rho = \sigma\tau$ avec $\tau \in G$ et dans les deux cas on vérifie aisément que pour $1 \leq i \leq t$, $\rho(a_i) = \pm a_i$, ce qui achève la démonstration du lemme. □

Pour appliquer ce lemme, on note $\mathcal{F}$ le groupe de torsion de $\mathcal{C}^{-1}_{\mathbb{C}(x)}$ et on pose $\mathcal{A} = \mathcal{C}^{-1}_{\mathbb{C}(x)}/\mathcal{F}$. Le groupe fini $\Gamma = gal(K/k)$ agit sur $\mathcal{A}$ (action induite par celle sur $\mathcal{C}^{-1}_{\mathbb{C}(x)}$) qui est un groupe abélien libre de type fini, et l'action induite de Γ sur $\mathcal{A}/2\mathcal{A}$ est triviale d'après le corollaire 1.5.7.

D'après le lemme, il existe donc une base $\{a_i \mid 1 \leq i \leq t\}$ de $\mathcal{A}$ telle que pour tout $\sigma \in \Gamma$, $\sigma(a_i) = a_i$ ou $\sigma(a_i) = -a_i$.

(C) Descente sur le corps $k(x)$

On va maintenant montrer que l'existence d'un point d'ordre infini sur $\mathcal{C}^{-1}_{\mathbb{C}(x)} = \mathcal{C}^{-1}_{K(x)}$ implique celle d'un point d'ordre infini sur $\mathcal{C}^{-d}_{k(x)}$ pour un certain $d \in k^*$.

Soient $\{b_i \mid 1 \leq i \leq t\}$ des représentants dans $\mathcal{C}^{-1}_{\mathbb{C}(x)}$ des éléments de la base $\{a_i \mid 1 \leq i \leq t\}$ de $\mathcal{A}$ dont il est question ci-dessus, alors comme pour tout $\sigma \in \Gamma$ on a : $\sigma(a_i) = \pm a_i$ on en déduit que $\sigma(b_i) \equiv \pm b_i \pmod{\mathcal{F}}$. Si m est l'exposant de $\mathcal{F}$ alors pour tout $\sigma \in \Gamma$ et tout $i \in \{1, ..., t\}$, $\sigma(mb_i) = \pm mb_i$.

Soit $i \in \{1, ..., t\}$, on alors deux cas de figure :

* Si pour tout $\sigma \in \Gamma$, $\sigma(mb_i) = mb_i$, alors mb_i est défini sur $k(x)$ et donc $mb_i \in \mathcal{C}^{-1}_{k(x)}$.

* S'il existe $\tau \in \Gamma$ tel que $\tau(mb_i) = -mb_i$, alors $\Gamma_i = \{\sigma \in \Gamma \mid \sigma(mb_i) = mb_i\}$ est un sous groupe d'indice 2 de Γ, donc il existe $d_i \in k^*$ tel que $k(\sqrt{d_i})$ soit le corps des invariants de Γ_i. Alors si on note τ_i l'élément de Γ tel que $\tau_i(\sqrt{d_i}) = -\sqrt{d_i}$ (c'est la conjugaison de $k(\sqrt{d_i})$ sur k), on a $\tau_i(mb_i) = -mb_i$ (sinon $\tau_i(mb_i) = mb_i$ et $\tau_i \in \Gamma_i$, ce qui est absurde car $k(\sqrt{d_i})$ est le corps des invariants de Γ_i). Donc en posant $mb_i = (\alpha_i, \beta_i)$, on a: $\tau_i(\alpha_i, \beta_i) = -(\alpha_i, \beta_i)$ c'est à dire $(\tau_i(\alpha_i), \tau_i(\beta_i)) = (\alpha_i, -\beta_i)$. Finalement $\tau_i(\alpha_i) = \alpha_i$ donc $\alpha_i \in k(x)$ et $\tau_i(\beta_i) = -\beta_i$ donc $\beta_i \in k(\sqrt{d_i})(x)$ et est de la forme $\beta_i = \sqrt{d_i}\beta_i'$, avec $\beta_i' \in k(x)$. L'existence du point mb_i sur $\mathcal{C}^{-1}_{\mathbb{C}(x)}$ implique bien celle d'un point (α_i, β_i') sur $\mathcal{C}^{-d_i}_{k(x)}$.

On peut alors en déduire le résultat suivant :

Proposition 1.5.9 *Si $\mathcal{C}^{-1}_{\mathbb{C}(x)}$ a des points d'ordre infini, alors il existe $d \in k^*$ tel que $\mathcal{C}^{-d}_{k(x)}$ ait aussi des points d'ordre infini.*

Preuve. Avec les notations précédentes, si $\mathcal{C}^{-1}_{\mathbb{C}(x)}$ a des points d'ordre infini la famille $\{b_i \mid 1 \leq i \leq t\}$ est non vide, et il suffit d'appliquer le raisonnement précédent à l'un des points b_i, car alors mb_i est d'ordre infini et donc correspond à un point sur $\mathcal{C}^{-d_i}_{k(x)}$ (avec éventuellement $d_i = 1$) qui ne peut pas être de torsion. □

Remarque 1.5.10 Avec les notations précédentes, à isomorphisme près, on a: $m\mathcal{C}^{-1}_{\mathbb{C}(x)} \subset \oplus_{i=1}^{t} \mathcal{C}^{-d_i}_{k(x)}$.

(D) Courbes $\mathcal{C}_{k(x)}^{-d}$ de rang nul

Pour démontrer la proposition 1.5.1, il ne reste plus qu'à exprimer une condition suffisante pour justifier la non-existence d'un point d'ordre infini $\mathcal{C}_{k(x)}^{-d}$ lorsque $d \in k^*$:

Proposition 1.5.11 *Soit d un élément quelconque de k^*, si les images des morphismes $\gamma_{\mathcal{C}} : \mathcal{C}_{k(x)}^{-d} \to k(x)^*/k(x)^{*2}$ et $\gamma_{\mathcal{D}} : \mathcal{D}_{k(x)}^{-d} \to k(x)^*/k(x)^{*2}$ sont les images des points de torsion, alors il n'y a pas de point d'ordre infini, ni sur $\mathcal{C}_{k(x)}^{-d}$, ni sur $\mathcal{D}_{k(x)}^{-d}$.*

Preuve. Supposons $\mathcal{C}_{k(x)}^{-d}$ infini, on choisit un élément $\overline{a_0} \in \mathcal{C}_{k(x)}^{-d}/\mathcal{F}$ (où $\mathcal{F}$ est le sous groupe de torsion de $\mathcal{C}_{k(x)}^{-d}$) faisant partie d'une base de $\mathcal{C}_{k(x)}^{-d}/\mathcal{F}$, en particulier $\overline{a_0}$ n'est pas un double dans $\mathcal{C}_{k(x)}^{-d}/\mathcal{F}$, donc si on note a_0 un de ses représentants dans $\mathcal{C}_{k(x)}^{-d}$, alors aucun des points $a_0 - p$, où p est un point de torsion, n'est un double dans $\mathcal{C}_{k(x)}^{-d}/\mathcal{F}$.

Comme l'image de $\mathcal{C}_{k(x)}^{-d}$ par $\gamma_{\mathcal{C}}$ est l'image des points de torsion, il existe un point p_0 d'ordre fini tel que $\gamma_{\mathcal{C}}(a_0) = \gamma_{\mathcal{C}}(p_0)$ donc en posant $a_0' = a_0 - p_0$, on sait que a_0' n'est pas divisible par 2 et appartient à $\ker \gamma_{\mathcal{C}} = \varphi_{\mathcal{D},\mathcal{C}}(\mathcal{D}_{k(x)}^{-d})$, ainsi $a_0' = \varphi_{\mathcal{D},\mathcal{C}}(b_0)$ avec $b_0 \in \mathcal{D}_{k(x)}^{-d}$.

Mais comme l'image de $\gamma_{\mathcal{D}}$ est l'image des points de torsion, il existe un point $q_0 \in \mathcal{D}_{k(x)}^{-d}$ d'ordre fini tel que $\gamma_{\mathcal{D}}(b_0) = \gamma_{\mathcal{D}}(q_0)$. Alors on pose $a = a_0' - \varphi_{\mathcal{D},\mathcal{C}}(q_0) = a_0 - (p_0 + \varphi_{\mathcal{D},\mathcal{C}}(q_0))$ et $b = b_0 - q_0$. Le point a n'est pas non plus divisible par 2 car $p_0 + \varphi_{\mathcal{D},\mathcal{C}}(q_0)$ est un point de torsion de $\mathcal{C}_{k(x)}^{-d}$ et de plus on sait que $a = \varphi_{\mathcal{D},\mathcal{C}}(b)$ et que $\gamma_{\mathcal{D}}(b) = \gamma_{\mathcal{D}}(b_0 - q_0) = k(x)^{*2}$.

Ainsi $b \in \ker \gamma_{\mathcal{D}} = \varphi_{\mathcal{C},\mathcal{D}}(\mathcal{C}_{k(x)}^{-d})$, c'est-à-dire $b = \varphi_{\mathcal{C},\mathcal{D}}(c)$, avec $c \in \mathcal{C}_{k(x)}^{-d}$. Cela implique que $a = \varphi_{\mathcal{D},\mathcal{C}}(\varphi_{\mathcal{C},\mathcal{D}}(c)) = 2c$, contredisant alors l'hypothèse "a n'est pas un double dans $\mathcal{C}_{k(x)}^{-d}$".

Il ne peut donc pas y avoir de point d'ordre infini sur $\mathcal{C}_{k(x)}^{-d}$. Le groupe $\mathcal{D}_{k(x)}^{-d}$ est lui aussi fini car un point d'ordre infini sur $\mathcal{D}_{k(x)}^{-d}$ aurait pour image par $\varphi_{\mathcal{D},\mathcal{C}}$ un point d'ordre infini sur $\mathcal{C}_{k(x)}^{-d}$. □

La proposition 1.5.1, est alors un corollaire direct des propositions 1.5.9 et 1.5.11 : Si pour tout $d \in k^*$, les conditions de la proposition 1.5.11 sont vérifiées alors, pour tout $d \in k^*$, la courbe $\mathcal{C}_{k(x)}^{-d}$ (de même que $\mathcal{D}_{k(x)}^{-d}$) est d'ordre fini. En appliquant la proposition 1.5.9, on peut alors exclure l'existence d'un point d'ordre infini sur la courbe $\mathcal{C}_{\mathbb{C}(x)}^{-1}$ ainsi que sur $\mathcal{D}_{\mathbb{C}(x)}^{-1}$ car si l'une de ces deux courbes est de rang nul il en est de même pour l'autre.

Remarque 1.5.12 C'est ici que se trouve l'erreur dans l'article de Christie, il y est énoncé au corollaire de la proposition 2 : "Si pour tout $d \in k^*$ l'image de $\gamma_{\mathcal{C}} : \mathcal{C}^{-d}_{k(x)} \to \mathbb{C}(x)^*/\mathbb{C}(x)^{*2}$ est l'image des points de torsion et si l'image de $\gamma_{\mathcal{D}} : \mathcal{D}^{-d}_{k(x)} \to \mathbb{C}(x)^*/\mathbb{C}(x)^{*2}$ est triviale, alors il n'y a pas de point d'ordre infini, ni sur $\mathcal{C}^{-1}_{\mathbb{C}(x)}$, ni sur $\mathcal{D}^{-1}_{\mathbb{C}(x)}$."

Dans la démonstration, il est dit que s'il y a un point d'ordre infini sur $\mathcal{C}^{-1}_{\mathbb{C}(x)}$, il y a aussi un point d'ordre infini sur $\mathcal{C}^{-d}_{k(x)}$. On peut alors trouver un tel point a qui ne soit pas un double (sur $\mathcal{C}^{-d}_{k(x)}$) tel que $\gamma_{\mathcal{C}}(a) = \mathbb{C}(x)^{*2}$. Le point a est alors l'image d'un point b par l'isogénie $\varphi_{\mathcal{D},\mathcal{C}}$, mais comme $\gamma_{\mathcal{C}}$ est un morphisme à image dans $\mathbb{C}(x)^*/\mathbb{C}(x)^{*2}$, alors le point b appartient à la courbe $\mathcal{D}^{-d}_{\mathbb{C}(x)}$ mais pas forcément à $\mathcal{D}^{-d}_{k(x)}$ comme l'a écrit Christie. Puis comme l'image de $\gamma_{\mathcal{D}}$ est triviale, $\gamma_{\mathcal{D}}(b) = \mathbb{C}(x)^{*2}$ donc $b \in \varphi_{\mathcal{C},\mathcal{D}}(\mathcal{C}^{-d}_{\mathbb{C}(x)})$ et on a : $b = \varphi_{\mathcal{C},\mathcal{D}}(c)$ avec $c \in \mathcal{C}^{-d}_{\mathbb{C}(x)}$, d'où $a = \varphi_{\mathcal{D},\mathcal{C}}(\varphi_{\mathcal{C},\mathcal{D}}(c)) = 2c$. Le point a serait un double, mais sur la courbe $\mathcal{C}^{-d}_{\mathbb{C}(x)}$ ce qui, à priori, n'est pas une contradiction car on a juste supposé que a n'est pas un double sur $\mathcal{C}^{-d}_{k(x)}$.

Ainsi d'après la proposition 1.5.1, pour démontrer que la courbe $\mathcal{C}^{-1}$ est de rang nul, on démontrera que les conditions de la proposition 1.5.11 sont bien vérifiées pour tout $d \in k^*$: cela revient à étudier la forme des points des courbes $\mathcal{C}^{-d}_{k(x)}$ et $\mathcal{D}^{-d}_{k(x)}$ afin de montrer que leurs images par les morphismes $\gamma_{\mathcal{C}}$ et $\gamma_{\mathcal{D}}$ sont toujours les mêmes que celles des points d'ordre fini.

Evidemment cette étude ne peut pas se faire de manière générale car il faut utiliser les propriétés des courbes $\mathcal{C}^{-d}$ et $\mathcal{D}^{-d}$ et celles du corps k : la justification des conditions requises pour pouvoir appliquer la proposition 1.5.1 aux exemples choisis se fait essentiellement par des arguments de spécialisation aux points $x_0 \in k$ pour lesquelles la courbe $\mathcal{C}^{-d}$ dégénère et nécessitera une étude soigneuse d'un grand nombre de cas.

On peut cependant énoncer ici un résultat essentiel dans le traitement des divers exemples que l'on étudiera :

Lemme 1.5.13 *Si (α, β) est un point de la courbe $\mathcal{C}^{-d}_{k(x)}$ (respectivement $\mathcal{D}^{-d}_{k(x)}$) avec $\beta \neq 0$, si on écrit $\alpha = f\frac{\theta^2}{\psi^2}$, $\beta = \frac{\chi}{\psi^3}$, avec f, θ, χ, $\psi \in k[x]$, f sans facteur carré et $pgcd(f\theta, \psi) = pgcd(\chi, \psi) = 1$. Alors le polynôme f divise $A^2 - 4B$ (respectivement B).*

Preuve. Si $(\alpha, \beta) \in \mathcal{C}^{-d}_{k(x)}$, on a vu dans la preuve du lemme 1.3.4 que l'on peut poser $\alpha = \frac{\omega}{\psi^2}$, $\beta = \frac{\chi}{\psi^3}$ avec ω, χ, $\psi \in k[x]$ tels que $\mathrm{pgcd}(\omega, \psi) = \mathrm{pgcd}(\chi, \psi) = 1$

puis on écrit $\omega = f\theta^2$ où $f,\theta \in k[x]$, f étant sans facteur carré. L'équation de la courbe $\mathcal{C}^{-d}_{k(x)}$, qui est $-d\beta^2 = \alpha(\alpha^2 - 2A\alpha + A^2 - 4B)$, implique alors que :

$$-d\chi^2 = f\theta^2(f^2\theta^4 - 2Af\theta^2\psi^2 + (A^2 - 4B)\psi^4)$$

Comme f est sans facteur carré, on peut écrire $\chi = f\theta\mu$ avec $\mu \in k[x]$ et après simplification, on obtient :

$$-df\mu^2 = f^2\theta^4 - 2Af\theta^2\psi^2 + (A^2 - 4B)\psi^4$$

On en déduit que f divise $(A^2 - 4B)\psi^4$ et comme $\text{pgcd}(f, \psi) = 1$, alors f divise $(A^2 - 4B)$.

Pour la courbe $\mathcal{D}^{-d}_{k(x)}$, le même raisonnement montre que $\alpha = f\frac{\theta^2}{\psi^2}$ avec f divisant B. □

Remarque 1.5.14 On a en même temps démontré que si (α, β) est un point de la courbe $\mathcal{C}^{-d}_{k(x)}$ (respectivement $\mathcal{D}^{-d}_{k(x)}$), avec les notations du lemme 1.5.13, il existe $\mu \in k[x]$ tel que $-df\mu^2 = f^2\theta^4 - 2Af\theta^2\psi^2 + (A^2 - 4B)\psi^4$ (respectivement $-df\mu^2 = f^2\theta^4 + 4Af\theta^2\psi^2 + 16B\psi^4$). Ce résultat sera lui aussi utile par la suite.

L'un des intérêt du lemme 1.5.13 est que, avec les notations précédentes, on a $\gamma_{\mathcal{C}}(\alpha, \beta) = -d\alpha k(x)^{*2} = -dfk(x)^{*2}$ lorsqu'on considère un point (α, β) de la courbe $\mathcal{C}^{-d}_{k(x)}$ tel que $\alpha \neq 0$ ou $\gamma_{\mathcal{D}}(\alpha, \beta) = -d\alpha k(x)^{*2} = -dfk(x)^{*2}$ pour un point (α, β) de $\mathcal{D}^{-d}_{k(x)}$ vérifiant $\alpha \neq 0$. Ce lemme va donc permettre de limiter le nombre de cas à traiter et on s'aperçoit qu'il sera intéressant pour faciliter cette étude de choisir des polynômes $A^2 - 4B$ et B possédant le moins possible de facteurs irréductibles.

Pour terminer cette section, on va s'intéresser aux quelques modifications à apporter aux résultats précédents pour adapter ce raisonnement lorsque seule la courbe $\mathcal{D}^{-1}$ est à 2-torsion $\mathbb{C}(x)$-rationnelle :

Dans le cas où $\mathcal{C}^{-1}$ n'est pas à 2-torsion $\mathbb{C}(x)$-rationnelle, c'est-à-dire où B n'est pas un carré dans $\mathbb{C}[x]$, cette courbe ne possède plus qu'un seul point d'ordre 2 défini sur $\mathbb{C}(x)$: $\mathcal{P}_{\mathcal{C}} = (0, 0)$. Le morphisme $\pi : \mathcal{C}^{-1}_{\mathbb{C}(x)} \to (\mathbb{C}(x)^*/\mathbb{C}(x)^{*2})^3$ n'est alors plus défini et on ne peut pas appliquer telle quelle la méthode précédente.

Cependant on va pouvoir substituer à π un autre morphisme π'. En effet, pour prouver que $\mathcal{C}^{-1}$ est de rang nul, on peut de manière équivalente démontrer

que $\mathcal{D}^{-1}$ n'a pas de points d'ordre infini. Or cette courbe $\mathcal{D}^{-1}$ étant à 2-torsion $\mathbb{C}(x)$-rationnelle, on a $A^2 - 4B = D^2$ avec $D \in \mathbb{C}[x]$, son équation est donc : $-\beta^2 = \alpha(\alpha^2 + 4A\alpha + 16B) = \alpha(\alpha + 2A - 2D)(\alpha + 2A + 2D)$ et ses trois points $\mathbb{C}(x)$-rationnels d'ordre 2 sont : $\mathcal{P}_{\mathcal{D}} = (0,0)$, $\mathcal{P}'_1 = (-2(A-D), 0)$ et $\mathcal{P}'_2 = (-2(A+D), 0)$. On peut alors définir le morphisme $\pi' : \mathcal{D}^{-1}_{\mathbb{C}(x)} \to (\mathbb{C}(x)^*/\mathbb{C}(x)^{*2})^3$ par :

$\pi'(\alpha, \beta) = (-\alpha\mathbb{C}(x)^{*2}, -(\alpha + 2A + 2D)\mathbb{C}(x)^{*2}, -(\alpha + 2A - 2D)\mathbb{C}(x)^{*2})$ si $\beta \neq 0$,

$\pi'(\mathcal{P}_{\mathcal{D}}) = (16B\mathbb{C}(x)^{*2}, -(2A + 2D)\mathbb{C}(x)^{*2}, -(2A - 2D)\mathbb{C}(x)^{*2})$,

$\pi'(\mathcal{P}'_1) = (2(A - D)\mathbb{C}(x)^{*2}, -4D\mathbb{C}(x)^{*2}, -8(A - D)D\mathbb{C}(x)^{*2})$,

$\pi'(\mathcal{P}'_2) = (2(A + D)\mathbb{C}(x)^{*2}, 8(A + D)D\mathbb{C}(x)^{*2}, 4D\mathbb{C}(x)^{*2})$,

$\pi'(\mathcal{O}_{\mathcal{D}}) = (\mathbb{C}(x)^{*2}, \mathbb{C}(x)^{*2}, \mathbb{C}(x)^{*2})$.

Ce morphisme π' possède des propriétés similaires à celles de π, en particulier son noyau est $2\mathcal{D}^{-1}_{\mathbb{C}(x)}$. On pourra utiliser un raisonnement analogue à celui qui précède mais en intervertissant les courbes $\mathcal{C}^{-1}$ et $\mathcal{D}^{-1}$, en suivant la même démarche et en choisissant le corps k de telle façon que le polynôme $B(A^2 - 4B)$ soit décomposé sur $k(x)$ et que $A^2 - 4B$ soit un carré dans $k(x)$, on obtiendra la proposition suivante, correspondant à la proposition 1.5.9 :

Proposition 1.5.15 *Si $\mathcal{D}^{-1}_{\mathbb{C}(x)}$ possède des points d'ordre infini, alors il existe $d \in k^*$ tel que $\mathcal{D}^{-d}_{k(x)}$ ait aussi des points d'ordre infini.*

Il suffit alors d'appliquer la proposition 1.5.11 pour montrer que la la proposition 1.5.1 est encore vraie.

1.6 Application à une première famille de polynômes

Dans l'article [Chr], Christie a énoncé le résultat suivant :

Soient λ, μ et ν trois entiers tels que $0 < \mu < \nu$, $\mu = (-3)^n\lambda$ avec $n \in \mathbb{N}^*$ et λ non multiple de 3 vérifiant $\lambda \equiv -\nu \pmod 3$, si $3\mu(\nu - \mu)$ et $\mu^2 + \mu\nu + \nu^2$ ne sont pas des carrés dans $\mathbb{N}$, alors le polynôme $F(x,y) = 1 + x\left((x + \mu)^3 - \frac{1}{2}\nu^3\right)y^2 + \frac{1}{16}\nu^6x^2y^4$ est défini positif et n'est pas une somme de trois carrés dans $\mathbb{R}(x,y)$.

On peut tout d'abord rappeler l'erreur de signe se trouvant dans l'article de Christie, déjà signalée dans Maths Reviews : à la place du terme $\mu^2 + \mu\nu + \nu^2$, il est écrit $\mu^2 - \mu\nu + \nu^2$, la même erreur se retrouve dans l'écriture du polynôme

$F(x,y)$. De plus, étant donné l'erreur commise par Christie dans le corollaire de la proposition 2, erreur que l'on a mise en évidence dans la section précédente, il apparaît que le traitement de cet exemple comporte certaines lacunes. En effet, il n'a pas abordé le cas où, avec les notations de la section précédente, on a $\alpha = f\frac{\theta^2}{\psi^2}$ avec $f \in k^*$ car alors il est évident que $-df \in \mathbb{C}(x)^{*2}$, ce qui apparemment semblait être suffisant pour traiter ce cas (voir remarque 1.5.12). En fait, avec la version corrigée de la méthode de Christie, il apparaît nécessaire de vérifier que dans ce cas on a : $-df \in k(x)^{*2}$ c'est-à-dire $-df \in k^{*2}$. On retrouve le même oubli dans l'étude des courbes $\mathcal{D}^{-d}_{k(x)}$.

De plus, en effectuant une étude plus approfondie des différents cas de figure, on peut obtenir des conditions plus faibles sur les paramètres et généraliser ce résultat à une famille plus large de polynômes. Il semble en effet que Christie n'ait pas exploité jusqu'au bout certaines pistes, c'est pourquoi on va ici reprendre et compléter l'étude de cette famille de polynômes.

On va donc considérer $F(X,Y) = 1 + X\left((X+\mu)^3 - \frac{1}{2}\nu^3\right)Y^2 + \frac{1}{16}\nu^6X^2Y^4$ avec ν, $\mu \in \mathbb{R}$ tels que $\nu > \mu > 0$. Il faut remarquer tout d'abord que l'on peut considérer cette famille de polynômes comme étant paramétrée par un seul nombre réel : en effet, quitte à poser $X = \mu x$ et $Y = \frac{y}{\mu^2}$, on a : $F(x,y) = 1 + x\left((x+1)^3 - \frac{1}{2}r^3\right)y^2 + \frac{1}{16}r^6x^2y^4$ avec $r = \frac{\nu}{\mu}$. On vérifie aisément que F est positif si $r > 1$.

L'objectif de cette section est de parvenir à démontrer le résultat suivant :

Théorème 1.6.1 *Soit r un nombre réel vérifiant $r > 1$ et tel que ni r ni r^2+r+1 ne sont des carrés dans le corps $\mathbb{Q}(r)$, alors le polynôme positif $F(x,y) = 1 + x\left((x+1)^3 - \frac{1}{2}r^3\right)y^2 + \frac{1}{16}r^6x^2y^4$ n'est pas somme de 3 carrés dans $\mathbb{R}(x,y)$.*

On va pour cela poser $A(x) = x\left((x+1)^3 - \frac{1}{2}r^3\right)$ et $B(x) = \frac{1}{16}r^6x^2$ afin que $F(x,y)$ soit de la forme $1 + A(x)y^2 + B(x)y^4$. Les polynômes A et B sont définis sur $k_0(x)$ avec $k_0 = \mathbb{Q}(r)$. Le polynôme B étant un carré dans $k_0(x)$, la courbe $\mathcal{C}^{-1}$ est à 2-torsion $k_0(x)$-rationnelle et a pour équation :

$$-\beta^2 = \alpha(\alpha - x(x+1)^3)(\alpha - x[(x+1)^3 - r^3]).$$

De plus, étant donné que $A^2 - 4B = x^2(x+1)^3\left((x+1)^3 - r^3\right) = x^2(x+1)^3(x+1-r)(x+1-rj)(x+1-rj^2)$, le corps de décomposition de $A^2 - 4B$

et de B est donc $\mathbb{Q}(j,r)$. On pourra choisir, toujours en conservant les notations des sections précédentes, $k = \mathbb{Q}(j,r)$.

L'étude de la courbe $\mathcal{C}^{-1}$ par la méthode exposée dans ce chapitre se fera en trois étapes :

(A) L'étude des points de torsion de la courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ dans le but de vérifier qu'aucun d'entre eux n'est spécial.

(B) L'étude des points des courbes $\mathcal{C}^{-d}_{k(x)}$ pour $d \in k^*$ avec pour objectif de déterminer des conditions suffisantes pour que l'image de $\gamma_{\mathcal{C}} : \mathcal{C}^{-d}_{k(x)} \to k(x)^*/k(x)^{*2}$ soit l'image des points de torsion.

(C) L'étude des points des courbes $\mathcal{D}^{-d}_{k(x)}$ avec $d \in k^*$, toujours pour exprimer des conditions suffisantes pour que l'image de $\gamma_{\mathcal{D}} : \mathcal{D}^{-d}_{k(x)} \to k(x)^*/k(x)^{*2}$ soit triviale.

(D) Les parties (B) et (C) auront permis de démontrer, sous certaines conditions, la non-existence de point d'ordre infini sur $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ en se ramenant aux conditions de la proposition 1.5.1. Dans cette dernière partie, on s'intéressera plus en détail à ces conditions afin de les exprimer sous une forme plus simple et on montrera que les exemples donnés par Christie sont en fait des cas particuliers de la famille de polynômes que l'on étudie ici.

(A) Points d'ordre fini

Il est clair que les points d'ordre 2 sur la courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ ne sont pas spéciaux, en effet ces points sont : $(0,0)$, $(x(x+1)^3, 0)$, $(x[(x+1)^3 - r^3], 0)$, et on voit aisément ni $4B - A^2$, ni $x(x+1)^3$, ni $x[(x+1)^3 - r^3]$, ne sont des sommes de deux carrés.

De plus sur $\mathcal{C}^{-1}_{\mathbb{C}(x)}$, aucun de ces points n'est un double (il suffit de calculer leurs images par le morphisme $\gamma_{\mathcal{C}}$), il n'y a donc pas de point d'ordre 4 sur $\mathcal{C}^{-1}_{\mathbb{C}(x)}$ et donc à fortiori il n'y en a pas non plus sur $\mathcal{C}^{-1}_{\mathbb{R}(x)}$. L'étude des points d'ordre fini peut donc s'arrêter ici, les points d'ordre impair ne pouvant pas être spéciaux comme on l'a vu auparavant.

(B) Etude de la courbe $\mathcal{C}^{-\mathbf{d}}_{\mathbf{k(x)}}$

Soit $d \in k^*$, on rappelle que cette courbe a pour équation :

$$-d\beta^2 = \alpha(\alpha - x(x+1)^3)(\alpha - x[(x+1)^3 - r^3]).$$

Pour démontrer que l'image de $\gamma_c : \mathcal{C}^{-d}_{k(x)} \to k(x)^*/k(x)^{*2}$ est l'image des points de torsion, on va premièrement déterminer certains points de torsion de cette courbe ainsi que leurs images par γ_c.

On connait sur cette courbe l'origine $\mathcal{O}_\mathcal{C}$ et trois points d'ordre 2 qui sont $\mathcal{P}_\mathcal{C} = (0,0)$, $\mathcal{P}_1 = (x(x+1)^3, 0)$ et $\mathcal{P}_2 = (x[(x+1)^3 - r^3], 0)$. Leurs images par γ_c sont :

$\gamma_c(\mathcal{O}_\mathcal{C}) = k(x)^{*2}$
$\gamma_c(\mathcal{P}_\mathcal{C}) = (x+1)(x+1-r)(x+1-rj)(x+1-rj^2)k(x)^{*2}$
$\gamma_c(\mathcal{P}_1) = -dx(x+1)k(x)^{*2}$
$\gamma_c(\mathcal{P}_2) = -dx(x+1-r)(x+1-rj)(x+1-rj^2)k(x)^{*2}$.

On va maintenant considérer un point d'ordre infini $(\alpha, \beta) \in \mathcal{C}^{-d}_{k(x)}$. On a donc $\beta \neq 0$, alors d'après le lemme 1.5.13, on peut écrire $\alpha = f\frac{\theta^2}{\psi^2}$ avec f, θ, $\psi \in k[x]$, $\text{pgcd}(f\theta, \psi) = 1$ et f sans facteur carré divisant $A^2 - 4B = x^2(x+1)^3((x+1)^3 - r^3)$. On sait aussi que $\gamma_c(\alpha, \beta) = -dfk(x)^{*2}$, donc pour arriver au résultat souhaité on doit montrer que, sous certaines conditions, le polynôme f ne peut prendre que certaines valeurs.

Tout d'abord, puisque f est sans facteur carré, il divise $x(x+1)(x+1-r)(x+1-rj)(x+1-rj^2)$. On remarque que, quitte à ajouter un des points d'ordre 2 au point (α, β), on peut supposer que ni x ni $(x+1)$ ne divisent f : En effet, si x divise f, comme $\gamma_c(\mathcal{P}_2) = -dx[(x+1)^3 - r^3]k(x)^{*2}$, il suffit de remplacer (α, β) par $(\alpha, \beta) + \mathcal{P}_2$ et on peut alors supposer que x ne divise plus f. De même, si $x+1$ divise f, comme $\gamma_c(\mathcal{P}_\mathcal{C}) = (x+1)[(x+1)^3 - r^3]k(x)^{*2}$, on remplace (α, β) par $(\alpha, \beta) + \mathcal{P}_\mathcal{C}$ ce qui permet de supposer que $(x+1)$ ne divise pas f.

Ainsi on obtient que f divise $(x+1-r)(x+1-rj)(x+1-rj^2)$ et est sans facteur carré. Ensuite en étudiant les différents cas suivant le degré de α, on montre que f est de degré pair. En posant $\alpha = f\frac{\theta^2}{\psi^2}$, on sait, d'après la remarque 1.5.14 qu'il existe $\mu \in k[x]$ tel que :

$$-df\mu^2 = f^2\theta^4 - 2Af\theta^2\psi^2 + (A^2 - 4B)\psi^4.$$

Comme $\deg(A) = 4$ et $\deg(A^2 - 4B) = 8$, trois cas se présentent :

$*$ Si $\deg(f\theta^2) > \deg(\psi^2) + 4$, alors $\deg(f\mu^2) = \deg(f^2\theta^4)$.

* Si $\deg(f\theta^2) < \deg(\psi^2) + 4$, alors $\deg(f\mu^2) = \deg((A^2 - 4B)\psi^4) = 8 + 4\deg(\psi)$.

* Si $\deg(f\theta^2) = \deg(\psi^2) + 4$, alors $\deg(f) = 4 + 2\deg(\psi) - 2\deg(\theta)$.

On voit bien que dans ces trois cas, f est toujours de degré pair.

On a donc démontré que f divise $(x+1-r)(x+1-rj)(x+1-rj^2)$ et est de degré pair, on peut donc supposer que $f = e$ ou $f = e(x-r_2)(x-r_3)$, avec $e \in k^*$ unique à multiplication par un carré près et où r_1, r_2, r_3 est une permutation de $r-1$, $jr-1$, j^2r-1. Avec cette notation, on a $(x+1)^3-r^3 = (x-r_1)(x-r_2)(x-r_3)$.

Avant de considérer ces deux possibilités pour f, il est intéressant de noter le résultat suivant :

Lemme 1.6.2 *Si on note $P = f\theta^2 - x(x+1)^3\psi^2$ et $Q = f\theta^2 - x[(x+1)^3 - r^3]\psi^2$, alors $pgcd(P,Q) = 1$ lorsque $\theta(0) \neq 0$ ou $pgcd(P,Q) = x$ lorsque $\theta(0) = 0$.*

Preuve. Soit p_0 un facteur commun à P et à Q, alors p_0 divise $P - Q = r^3 x\psi^2$. Or p_0 est premier avec ψ (sinon $f\theta$ et ψ auraient un facteur commun, ce qui est impossible car, par définition, $\mathrm{pgcd}(f\theta, \psi) = 1$), donc p_0 divise x. On a ainsi deux possibilités : $\mathrm{pgcd}(P,Q) = 1$ ou $\mathrm{pgcd}(P,Q) = x$.

Pour terminer, on remarque que si $\theta(0) \neq 0$, on a alors $P(0) = Q(0) = f(0)\theta^2(0) \neq 0$ et donc $\mathrm{pgcd}(P,Q) = 1$ et si $\theta(0) = 0$, on a alors $P(0) = Q(0) = 0$ et $\mathrm{pgcd}(P,Q) = x$. □

Ce lemme va présenter un certain intérêt car les polynômes P et Q apparaissent dans l'équation $-df\mu^2 = (f\theta^2 - x(x+1)^3\psi^2)(f\theta^2 - x[(x+1)^3 - r^3]\psi^2)$.

On peut maintenant étudier les différents cas suivant la forme de f :

(B1) $f = e \in k^*$

(B2) $f = e(x - r_2)(x - r_3)$, avec $e \in k^*$.

Cas (B1) : Si f = e

Dans ce cas, l'élément e de k^* ne peut prendre que deux valeurs à multiplication par un carré près :

Proposition 1.6.3 *Si $f = e \in k^*$, on a soit $-de \in k^{*2}$, soit $e \in k^{*2}$*

Preuve. Il suffit de compléter l'étude du degré dans l'équation $-f\mu^2 = (f\theta^2 - x(x+1)^3\psi^2)(f\theta^2 - x[(x+1)^3 - r^3]\psi^2)$ par celle des coefficients dominants.

En posant a_θ, a_ψ et a_μ les coefficients dominants respectifs de θ, ψ et μ on a :

* Si $\deg(\theta) > \deg(\psi) + 2$, alors $-dea_\mu^2 = e^2a_\theta^4$.
* Si $\deg(\theta) < \deg(\psi) + 2$, alors $-dea_\mu^2 = a_\psi^4$.
* Si $\deg(\theta) = \deg(\psi)+2$ et $e^2a_\theta^4 - 2ea_\theta^2a_\psi^2 + a_\psi^4 \neq 0$, alors $-dea_\mu^2 = (ea_\theta^2 - a_\psi^2)^2$.
* Si $\deg(\theta) = \deg(\psi) + 2$ et $(ea_\theta^2 - a_\psi^2) = 0$, alors $e = \left(\frac{a_\psi}{a_\theta}\right)^2$.

Dans les trois premiers cas on a $-de \in k^{*2}$ et dans le dernier $e \in k^{*2}$. □

Dans le cas où $-de \in k^{*2}$, alors $\gamma_c(\alpha, \beta) = -dek(x)^{*2} = k(x)^{*2}$ donc $(\alpha, \beta) \in \ker(\gamma_c)$ et on est bien dans les conditions de la proposition 1.5.1.

Il ne reste donc qu'à étudier que le cas où $e \in k^{*2}$. On peut alors supposer que $e = 1$ et cela donne l'équation :

$$-d\mu^2 = (\theta^2 - x(x+1)^3\psi^2)(\theta^2 - x[(x+1)^3 - r^3]\psi^2).$$

Si on spécialise en $x = 0$, on obtient $-d\mu^2(0) = \theta^4(0)$, donc à condition que $\theta(0) \neq 0$, on a $-d \in k^{*2}$. Comme $e = 1$, cela implique que $-de \in k^{*2}$ et on peut conclure que, dans ce cas, $(\alpha, \beta) \in \ker(\gamma_c)$. Le problème est résolu lorsque $\theta(0) \neq 0$.

On suppose donc maintenant que $\theta(0) = 0$: il s'agit du dernier cas pouvant poser un problème. D'après le lemme 1.6.2, on est dans le cas où on a $\mathrm{pgcd}(\theta^2 - x(x+1)^3\psi^2, \theta^2 - x[(x+1)^3 - r^3]\psi^2) = x$. A partir de cette propriété et de l'équation : $-d\mu^2 = (\theta^2 - x(x+1)^3\psi^2)(\theta^2 - x[(x+1)^3 - r^3]\psi^2)$, on peut déduire qu'il existe $s \in k^*$, μ_1, $\mu_2 \in k[x]^*$ tels que :

$$\begin{cases} \theta^2 - x(x+1)^3\psi^2 = sx\mu_1^2 \\ \theta^2 - x[(x+1)^3 - r^3]\psi^2 = -dsx\mu_2^2 \end{cases}$$

Et puisque $\theta(0) = 0$, on peut poser $\theta = x\theta'$, $\theta' \in k[x]^*$ et on a après simplification :

$$\begin{cases} x\theta'^2 - (x+1)^3\psi^2 = s\mu_1^2 \\ x\theta'^2 - [(x+1)^3 - r^3]\psi^2 = -ds\mu_2^2 \end{cases}$$

En posant $x = 0$ dans la seconde équation, on a $-ds\mu_2^2(0) = (r^3-1)\psi^2(0)$. Comme $\text{pgcd}(\theta, \psi) = 1$, alors $\psi(0) \neq 0$ et donc $-ds \in (r^3-1)k^{*2} = r_1r_2r_3k^{*2}$.

Puis en posant $x = r_1$ dans cette même équation, on obtient la relation $r_1\theta'^2(r_1) = -ds\mu_2^2(r_1)$. Or $\mu_2(r_1) \neq 0$, sinon on en déduirait que $\theta'^2(r_1) = 0$ et que $(x-r_1)^2$ divise les deux membres de l'équation $x\theta'^2 - [(x+1)^3 - r^3]\psi^2 = -ds\mu_2^2$, on devrait alors avoir ψ multiple de $(x-r_1)$, ce qui contredit l'hypothèse $pgcd(\theta, \psi) = 1$. Cela implique que $r_1 \in -dsk^{*2}$.

En regroupant ces résultat, on obtient que $r_1 \in r_1r_2r_3k^{*2}$ ce dont on déduit que $r_2r_3 \in k^{*2}$.

On a ainsi dégagé une condition suffisante pour que ce dernier cas ($\theta(0) = 0$) ne puisse pas se produire : il suffit de s'assurer que r_2r_3 n'est pas un carré dans le corps k, ce que l'on fera, à la partie (D), en imposant certaines hypothèses sur le réel r. Donc, en se plaçant sous ces hypothèses, on aura toujours $(\alpha, \beta) \in \ker(\gamma_c)$ lorsque $f = e \in k^*$.

Cas (B2) : Si $\mathbf{f = e(x - r_2)(x - r_3)}$

Dans ce cas l'équation de $\mathcal{C}^{-d}$ devient :

$$-def\mu^2 = (ef\theta^2 - x(x+1)^3\psi^2)(ef\theta^2 - x[(x+1)^3 - r^3]\psi^2).$$

Comme $f = e(x-r_2)(x-r_3)$ et $(x+1)^3 - r^3 = (x-r_1)(x-r_2)(x-r_3)$, après simplification, on a :

$$-de\mu^2 = (e(x-r_2)(x-r_3)\theta^2 - x(x+1)^3\psi^2)(e\theta^2 - x(x-r_1)\psi^2) \qquad (1).$$

De plus, comme dans le cas (B1), l'étude des coefficients dominants montre que l'on a soit $-de \in k^{*2}$, soit $e \in k^{*2}$: La seule variation dans la démonstration est, qu'au lieu de comparer $\deg(\theta)$ et $\deg(\psi)+2$, on s'intéresse aux différents cas suivant que $\deg(\theta)$ est supérieur, inférieur ou égal à $\deg(\psi) + 1$, cela est dû au fait que cette fois f n'est plus de degré 0 mais de degré 2.

(i) On suppose d'abord que l'on est dans le cas où $-de \in k^{*2}$:

Si $\theta(0) \neq 0$, on a d'après l'équation (1), $-de\mu^2(0) = e^2 r_2 r_3 \theta^4(0) \neq 0$ donc $r_2 r_3 \in dek^{*2}$ c'est-à-dire $r_2 r_3 \in k^{*2}$. Comme on l'a vu auparavant, cette hypothèse sera exclue par le choix de r, le cas $\theta(0) \neq 0$ ne pourra alors pas se produire.

Si $\theta(0) = 0$, alors d'après le lemme 1.6.2, on est dans le cas où les polynômes $(e(x-r_2)(x-r_3)\theta^2 - x(x+1)^3\psi^2)$ et $(e\theta^2 - x(x-r_1)\psi^2)$ admettent x pour pgcd, de plus, d'après (1), leur produit est $-de\mu^2 \in k[x]^{*2}$. Donc il existe $s \in k^*$, μ_1, $\mu_2 \in k[x]$ tels que :

$$\begin{cases} e(x-r_2)(x-r_3)\theta^2 - x(x+1)^3\psi^2 = sx\mu_1^2 \\ e\theta^2 - x(x-r_1)\psi^2 = sx\mu_2^2 \end{cases}$$

En posant $\theta = x\theta'$, avec $\theta' \in k[x]$, on obtient après simplification par x :

$$\begin{cases} ex(x-r_2)(x-r_3)\theta'^2 - (x+1)^3\psi^2 = s\mu_1^2 \\ ex\theta'^2 - (x-r_1)\psi^2 = s\mu_2^2 \end{cases}$$

Comme $\mathrm{pgcd}(f\theta, \psi) =$ et que $\theta(0) = 0$, on a $\psi(0) \neq 0$, donc pour $x = 0$ dans la première équation de ce système, on a $-\psi^2(0) = s\mu_1^2(0)$ donc $-s \in k^{*2}$.

On a aussi $f(r_2) = 0$ ce qui implique que $\psi(r_2) \neq 0$ donc, toujours dans la même équation, pour $x = r_2$, $-(r_2+1)^3\psi^2(r_2) = s\mu_1^2(r_2) \neq 0$, on en déduit que $(r_2+1) \in -sk^{*2}$.

En regroupant les résultats $-s \in k^{*2}$ et $(r_2+1) \in -sk^{*2}$, on obtient que $(r_2+1) \in k^{*2}$.

On remarque alors que, comme r_2 est de la forme $rj^{n_2} - 1$ avec $n_2 \in \{0,1,2\}$, alors on a $(r_2+1) = rj^{n_2}$. Or $j = (j^2)^2$ donc $j^{n_2} \in k^{*2}$, la condition $(r_2+1) \in k^{*2}$ devient ainsi $r \in k^{*2}$.

Pour exclure le cas $\theta(0) = 0$, il suffira d'ajouter l'hypothèse $r \notin k^{*2}$ qui fournira la contradiction souhaitée.

(ii) Si on est dans le cas où $e \in k^{*2}$:

On peut alors supposer que $e = 1$ et on a deux possibilités à étudier suivant que $\theta(0)$ est nul ou non.

Si $\theta(0) \neq 0$, alors les polynômes $(x-r_2)(x-r_3)\theta^2 - x(x+1)^3\psi^2$ et $\theta^2 - x(x-r_1)\psi^2$ sont premiers entre eux (conséquence directe du lemme 1.6.2), leur produit étant, d'après l'équation (1), $-de\mu^2 = -d\mu^2$, on en déduit qu'il existe $s \in k^*$, μ_1, $\mu_2 \in k[x]^*$ tel que :

$$\begin{cases} (x-r_2)(x-r_3)\theta^2 - x(x+1)^3\psi^2 = -ds\mu_1^2 \\ \theta^2 - x(x-r_1)\psi^2 = s\mu_2^2 \end{cases}$$

Etant donné que $f = (x-r_2)(x-r_3)$ et que ψ est premier avec f, on a $\psi(r_2) \neq 0$ et $\psi(r_3) \neq 0$ donc dans la première équation de ce système :

* Pour $x = r_2$, on a : $-r_2(r_2+1)^3\psi^2(r_2) = -ds\mu_2^2(r_2)$, cela implique que $-r_2(r_2+1) \in -dsk^{*2}$

* Pour $x = r_3$, on a : $-r_3(r_3+1)^3\psi^2(r_3) = -ds\mu_2^2(r_3)$, cela implique que $-r_3(r_3+1) \in -dsk^{*2}$

On déduit de ces deux relations que $r_2r_3(r_2+1)(r_3+1) \in k^{*2}$. Or on sait que $r_2 = rj^{n_2} - 1$ et $r_3 = rj^{n_3} - 1$ avec $n_2, n_3 \in \{0,1,2\}$, on a donc $(r_2+1)(r_3+1) = r^2j^{n_2+n_3}$ et comme $j = (j^2)^2 \in k^{*2}$ alors $(r_2+1)(r_3+1) \in k^{*2}$. Cela donne finalement $r_2r_3 \in k^{*2}$, cette condition est déjà apparue précédemment et le réel r sera choisi de telle façon qu'elle ne pourra pas se réaliser : On ne pourra ainsi pas avoir $\theta(0) \neq 0$.

Si $\theta(0) = 0$, alors $\mathrm{pgcd}((x-r_2)(x-r_3)\theta^2 - x(x+1)^3\psi^2, \theta^2 - x(x-r_1)\psi^2) = x$ (c'est toujours une conséquence du lemme 1.6.2), leur produit étant $-d\mu^2$, on en déduit comme auparavant l'existence de $s \in k^*$, μ_1, $\mu_2 \in k[x]$ tels que, en posant $\theta = x\theta'$ et en simplifiant par x :

$$\begin{cases} x(x-r_2)(x-r_3)\theta'^2 - (x+1)^3\psi^2 = -ds\mu_1^2 \\ x\theta'^2 - (x-r_1)\psi^2 = s\mu_2^2 \end{cases}$$

Comme $\mathrm{pgcd}(f\theta, \psi) = 1$, alors $\psi(0) \neq 0$ et pour $x = 0$ dans la première équation de ce système, on a $-\psi^2(0) = -ds\mu_1^2(0)$ donc $ds \in k^{*2}$.

De plus, comme $f(r_2) = 0$, $\psi(r_2) \neq 0$ donc pour $x = r_2$ dans cette même équation, on a $-(r_2+1)^3\psi^2(r_2) = -ds\mu_1^2(r_2) \neq 0$ d'où $(r_2+1) \in dsk^{*2}$.

On obtient ainsi $(r_2+1) \in k^{*2}$, ce qui comme on l'a vu auparavant équivaut à $r \in k^{*2}$. Ici encore, on voit apparaître la nécessité de supposer que $r \notin k^{*2}$ pour pouvoir exclure le cas $\theta(0) = 0$.

En s'assurant que r et r_2r_3 ne sont pas des carrés dans k, on ne peut donc pas avoir $f = e(x-r_2)(x-r_3)$. On peut conclure de l'étude qui précède (c'est-à-dire des cas (B1) et (B2)) que sous ces conditions, si $(\alpha,\beta) \in \mathcal{C}^{-d}_{k(x)}$ n'est pas un point d'ordre fini, on a alors, quitte à lui ajouter un point d'ordre 2, $-d\alpha k^{*2} = k^{*2}$.

Cela signifie que l'image de (α, β) par γ_c est l'image de ce point d'ordre 2. On est donc bien dans les hypothèses de la proposition 1.5.1.

(C) Etude de la courbe $\mathcal{D}^{-\mathbf{d}}_{\mathbf{k(x)}}$

Soit $d \in k^*$, la courbe $\mathcal{D}^{-d}_{k(x)}$ a pour équation :

$$-d\beta^2 = \alpha\left(\alpha^2 + 4x\left((x+1)^3 - \frac{1}{2}r^3\right)\alpha + r^6x^2\right).$$

Cette courbe ne possède qu'un seul point d'ordre 2, $\mathcal{P}_{\mathcal{D}} = (0,0)$ et son image dans $k(x)^*/k(x)^{*2}$ par $\gamma_{\mathcal{D}}$ est triviale.

Soit $(\alpha, \beta) \in \mathcal{D}^{-d}_{k(x)}$ un point d'ordre infini, alors on peut écrire $\alpha = f\frac{\theta^2}{\psi^2}$ avec les notations et les propriétés du lemme 1.5.13. En particulier f est sans facteur carré et divise $B = \frac{1}{16}r^6x^2$ donc on a deux cas de figure :

(C1) Soit $f = e \in k^*$

(C2) Soit $f = ex$ avec $e \in k^*$.

Cas (C1) : Si f = e

Dans ce cas, l'équation de $\mathcal{D}^{-d}$ donne :

$$-de\mu^2 = e^2\theta^4 + 4x\left((x+1)^3 - \frac{1}{2}r^3\right)e\theta^2\psi^2 + r^6x^2\psi^4.$$

Mais on peut aussi l'écrire sous la forme :

$$-de\mu^2 = \left(e\theta^2 + 2x\left((x+1)^3 - \frac{1}{2}r^3\right)\psi^2\right)^2 - 4x^2(x+1)^3[(x+1)^3 - r^3]\psi^4.$$

Etant donné que $[(x+1)^3 - r^3] = (x-r_1)(x-r_2)(x-r_3)$, pour $x = r_1$ (on aurait pu tenir le même raisonnement avec $x = r_2$ ou $x = r_3$), on a :

* Soit $\left(e\theta^2(r_1) + 2r_1\left((r_1+1)^3 - \frac{1}{2}r^3\right)\psi^2(r_1)\right) \neq 0$, alors cela implique que $\mu^2(r_1) \neq 0$ d'où $-de \in k^{*2}$. Le problème est réglé car $\gamma_{\mathcal{D}}(\alpha, \beta) = -dek^{*2}$ et est donc trivial.

* Soit $\left(e\theta^2(r_1) + 2r_1\left((r_1+1)^3 - \frac{1}{2}r^3\right)\psi^2(r_1)\right) = 0$, alors $\mu^2(r_1) = 0$ et donc le polynôme $(x - r_1)$ divise μ. On en déduit que $(x-r_1)^2$ divise le membre de droite de l'équation précédente, impliquant que $(x-r_1)$ divise ψ. Puis comme $(x-r_1)$ divise ψ et $\left(e\theta^2 + 2x\left((x+1)^3 - \frac{1}{2}r^3\right)\psi^2\right)$ alors il divise à la fois ψ et θ. Cela est impossible car, par hypothèse, ψ et θ sont premiers entre eux.

Seul le premier cas peut se produire et donc, lorsque $f = e \in k^*$, on a toujours $(\alpha, \beta) \in \ker(\gamma_{\mathcal{D}})$

Cas (C2) : Si f = ex

Dans ce cas, l'équation de la courbe donne la relation :

$$-dex\mu^2 = \left(ex\theta^2 + 2x\left((x+1)^3 - \frac{1}{2}r^3\right)\psi^2\right)^2 - 4x^2(x+1)^3[(x+1)^3 - r^3]\psi^4.$$

Par un raisonnement analogue à celui donné dans le cas (C1), on montre que pour $i = 1$, 2 et 3, on a $-der_i\mu^2(r_i) = \left(er_i\theta^2(r_i) + 2r_i\left((r_i+1)^3 - \frac{1}{2}r^3\right)\psi^2(r_i)\right) \neq 0$, sinon θ et ψ auraient $(x - r_i)$ pour facteur commun. Donc pour $i = 1$, 2 et 3, on la relation $-der_i\mu^2(r_i) \in k^{*2}$, en particulier, $-der_2 \in k^{*2}$ et $-der_3 \in k^{*2}$ d'où on obtient que $r_2r_3 \in k^{*2}$. On a déjà auparavant mentionné que cette condition doit être exclue par un choix judicieux du réel r, ce qui fait que le cas (C2) ne peut pas se produire.

Ainsi l'étude des cas (C1) et (C2) montre qu'à condition que $r_2r_3 \notin k^{*2}$, tout point d'ordre infini de $\mathcal{D}^{-d}_{k(x)}$ appartient au noyau de $\gamma_{\mathcal{D}}$.

(D) Reformulation des conditions

On a donc en étudiant les courbes $\mathcal{C}^{-d}_{k(x)}$ et $\mathcal{D}^{-d}_{k(x)}$ montré que si r et r_2r_3 ne sont pas des carrés dans le corps $k = \mathbb{Q}(j, r)$, alors les conditions de la proposition 1.5.1 sont réalisées et ainsi il n'y a pas de point d'ordre infini sur $\mathcal{C}^{-1}_{\mathbb{Q}(x)}$ donc il n'y a pas non plus de point spécial sur $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ car, comme on l'a déjà vu, les points de torsion ne sont pas spéciaux. On va maintenant reformuler les conditions $r \notin k^{*2}$

et $r_2 r_3 \notin k^{*2}$ pour les exprimer en tant que conditions portant sur le réel r dans dans le corps $\mathbb{Q}(r)$.

Lemme 1.6.4 *Soit r un réel, $r > 1$, soit r_1, r_2, r_3 une permutation de $r-1$, $rj-1$, rj^2-1. Si $r \notin \mathbb{Q}(r)^{*2}$ et $r^2+r+1 \notin \mathbb{Q}(r)^{*2}$, alors ni r ni $r_2 r_3$ ne sont des carrés dans $k = \mathbb{Q}(j,r)$.*

Preuve. On considère un élément $a \in k^{*2}$, deux cas de figure peuvent se présenter :

* Si $a \in k^{*2} \cap \mathbb{Q}(r)$, comme $k = \mathbb{Q}(r,j) = \mathbb{Q}(r)(i\sqrt{3})$, on peut écrire $a = (u + vi\sqrt{3})^2$ avec $u, v \in \mathbb{Q}(r)$, d'où $a = u^2 - 3v^2 + 2uvi\sqrt{3}$. Comme $a \in \mathbb{Q}(r)$ et que r est un nombre réel, alors soit $u = 0$, soit $v = 0$ donc on a respectivement soit $a \in \mathbb{Q}(r)^{*2}$, soit $-3a \in \mathbb{Q}(r)^{*2}$.

* Si $a \in k^{*2} \backslash \mathbb{Q}(r)$ alors on a $Norme_{k/\mathbb{Q}(r)}(a) \in \mathbb{Q}(r)^{*2}$.

On peut maintenant appliquer ce résultat aux éléments r et à $r_2 r_3$ du corps k.

Ainsi, si on suppose que $r \in k^{*2}$, alors $r \in k^{*2} \cap \mathbb{Q}(r)$ et on doit avoir soit $r \in \mathbb{Q}(r)^{*2}$, soit $-3r \in \mathbb{Q}(r)^{*2}$. Le premier cas est exclu par hypothèse, le second ne peut se produire car $r > 0$ et $\mathbb{Q}(r) \subset \mathbb{R}$. Sous les conditions de l'énoncé, r ne peut pas être un carré dans le corps k.

On suppose maintenant que $r_2 r_3 \in k^{*2}$:

* Soit on est dans le cas où r_2, r_3 est une permutation de $\{rj-1, rj^2-1\}$ et donc on a $r_2 r_3 = r^2+r+1 \in k^{*2} \cap \mathbb{Q}(r)$. On devrait alors avoir, d'après ce qui précède, soit $r^2+r+1 \in \mathbb{Q}(r)^{*2}$, ce qui est impossible par hypothèse, soit $-3(r^2+r+1) \in \mathbb{Q}(r)^{*2}$ ce qui est impossible car $r^2+r+1 > 0$.

* Soit on est dans le cas où $r_2 r_3 = (r-1)(rj-1)$ (ou $r_2 r_3 = (r-1)(rj^2-1)$) et alors $r_2 r_3 \in k^{*2} \backslash \mathbb{Q}(r)$. Dans ce cas, on a vu que $Norme_{k/\mathbb{Q}(r)}(r_2 r_3) \in \mathbb{Q}(r)^{*2}$ c'est-à-dire $(r-1)^2(r^2+r+1) \in \mathbb{Q}(r)^{*2}$, donc $r^2+r+1 \in \mathbb{Q}(r)^{*2}$ contredisant les hypothèses de l'énoncé.

On voit donc que, lorsqu'on se place sous les conditions de ce lemme, $r_2 r_3$ n'est pas un carré dans le corps k. □

Le théorème 1.6.1 est une conséquence directe de ce lemme et de l'étude qui précède. En effet, si r un nombre réel vérifiant $r > 1$ et tel que ni r, ni r^2+r+1

ne sont des carrés dans le corps $\mathbb{Q}(r)$ alors la courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ n'a pas de point spécial et donc le polynôme $F(x,y)$ n'est pas une somme de trois carrés dans $\mathbb{R}(x,y)$.

On peut remarquer deux cas particuliers de ce théorème :

Corollaire 1.6.5 *Le polynôme* $F(x,y) = 1 + x\left((x+1)^3 - \frac{1}{2}r^3\right)y^2 + \frac{1}{16}r^6x^2y^4$ *est positif et n'est pas somme de 3 carrés dans* $\mathbb{R}(x,y)$ *lorsque le réel* $r > 1$ *vérifie l'une des deux conditions suivantes :*

(1) Le nombre r est un rationnel tel que ni r, ni $r^2 + r + 1$ ne sont des carrés de rationnels.

(2) Le nombre réel r est transcendant.

Preuve. C'est une conséquence immédiate du théorème 1.6.1 car si r est un rationnel, alors $\mathbb{Q}(r) = \mathbb{Q}$ et si r est transcendant, alors ni r, ni r^2+r+1 ne peuvent être des carrés dans $\mathbb{Q}(r)$. □

On va maintenant vérifier que la famille de polynômes proposée par Christie est bien un cas particulier de celle donnée ici :

Lemme 1.6.6 *Si μ et ν sont deux entiers tels que $\mu = (-3)^n\lambda$ avec $n \in \mathbb{N}^*$ et λ non multiple de 3 vérifiant $\lambda \equiv -\nu \pmod 3$, alors le nombre rationnel $r = \frac{\nu}{\mu}$ n'est pas un carré de rationnel.*

Preuve. Supposons que $r \in \mathbb{Q}^{*2}$, alors $\mu\nu = \mu^2 r \in \mathbb{Q}^{*2} \cap \mathbb{Z}$ donc $\mu\nu \in \mathbb{Z}^{*2}$. Or on sait que $\mu = (-3)^n\lambda$ et que $\lambda \equiv -\nu \pmod 3$ donc il existe un entier m tel que $\nu = 3m - \lambda$. Ainsi $\mu\nu = (-3)^n\lambda(3m-\lambda) \in \mathbb{Z}^{*2}$ d'où n est pair, sinon 3 diviserait $\lambda(3m-\lambda)$ et donc diviserait aussi λ ce qui contredirait les hypothèses. on en déduit que $\lambda(3m-\lambda) \in \mathbb{Z}^{*2}$.

On pose alors $\lambda = a^2b$ où a et b sont deux entiers, b étant sans facteur carré. Comme 3 ne divise pas λ, alors il ne divise ni a, ni b. On obtient donc avec cette nouvelle notation, $b(3m - a^2b) \in \mathbb{Z}^{*2}$ d'où, comme b est sans facteur carré, il divise $3m - a^2b$ et donc b divise $3m$. Mais on sait que 3 ne divise pas b donc $\mathrm{pgcd}(b,3) = 1$ et cela montre que b divise m, on peut poser $m = kb$ avec $k \in \mathbb{Z}$.

De la relation $b(3m - a^2b) \in \mathbb{Z}^{*2}$, on déduit alors que $(3k - a^2) \in \mathbb{Z}^{*2}$ c'est-à-dire qu'il existe $c \in \mathbb{Z}^*$ tel que $a^2 + c^2 = 3k$ ou encore $a^2 + c^2 \equiv 0 \pmod 3$. Mais, si p est un entier, on a soit $p^2 \equiv 0 \pmod 3$, soit $p^2 \equiv 1 \pmod 3$, donc ici on a forcément $a \equiv 0 \pmod 3$ et $c \equiv 0 \pmod 3$ ce qui est impossible car 3 ne divise pas l'entier a.

Sous les conditions de ce lemme, on a donc $\mu\nu \notin \mathbb{Z}^{*2}$ et $r \notin \mathbb{Q}^{*2}$. □

Les conditions énoncées par Christie peuvent donc être regroupées en quatre catégories et on vérifie que chacune d'entre elle constitue un cas particulier d'une des hypothèses du théorème 1.6.1 :

* La condition μ et ν sont deux entiers tels que $0 < \mu < \nu$ se traduit par $r = \frac{\nu}{\mu}$ est un nombre rationnel tel que $r > 1$: il s'agit de la condition assurant la positivité du polynôme $F(x, y)$.

* D'après le lemme 1.6.6, $\mu = (-3)^n \lambda$ avec $n \in \mathbb{N}^*$ et λ non multiple de 3 tel que $\lambda \equiv -\nu \pmod 3$ implique que $r \notin \mathbb{Q}^{*2}$.

* On vérifie aisément que la condition $\mu^2+\mu\nu+\nu^2 \notin \mathbb{N}^{*2}$ équivaut à $r^2+r+1 \notin \mathbb{Q}^{*2}$.

* Enfin $3\mu(\nu - \mu) \notin \mathbb{N}^{*2}$ pourrait se traduire par $3(r - 1) \notin \mathbb{Q}^{*2}$ et apparaît comme une condition superflue.

On voit alors que tout polynôme de la famille proposée par Christie se retrouve dans le cas (1) du corollaire 1.6.5. Le théorème 1.6.1 constitue donc bien une généralisation du résultat de Christie.

Remarque 1.6.7 Pour terminer ce chapitre, on peut noter que, même si sous les conditions énoncées ci-dessus $F(x, y)$ n'est pas somme de 3 carrés dans $\mathbb{R}(x, y)$, on peut toujours, pour $r > 1$, écrire $F(x, y)$ comme somme de 4 carrés de polynômes dans $\mathbb{R}[x, y]$. En effet on peut vérifier que :

$$F(x,y) = \left(\left(x + \frac{3}{2}\right)xy\right)^2 + \left(\frac{\sqrt{3}}{2}xy\right)^2 + \left(\left(\frac{1}{2} - \frac{r^3}{4}\right)xy^2 + 1\right)^2 + \left(\frac{1}{2}\sqrt{r^3 - 1}xy^2\right)^2.$$

Cela montre que $F(x, y)$ est défini positif et de plus, on s'aperçoit que la configuration est différente de celle du cas étudié par Cassels, Ellison et Pfister car le polynôme de Motzkin n'est pas somme de 3 carrés dans $\mathbb{R}(x, y)$, mais n'est pas non plus somme carrés de polynômes dans $\mathbb{R}[x, y]$.

Chapitre 2

Polynômes factorisés

L'objectif de ce chapitre est de construire de nouvelles familles de polynômes positifs qui ne sont pas somme de 3 carrés dans $\mathbb{R}(x,y)$: On va ici s'intéresser plus particulièrement aux polynômes $F(x,y)$ factorisés dans $\mathbb{R}[x,y]$ sous la forme $(y^2+a(x))(y^2+b(x))$ où $a(x)$ et $b(x)$ sont des polynômes positifs définis sur le corps $k_0[x]$, avec k_0 sous-corps de $\mathbb{R}$.

Les courbes elliptiques associées à $F(x,y)$ ont alors pour équations de Weierstrass $\mathcal{C}^{-1} : -\beta^2 = \alpha(\alpha^2 - 2(a+b)\alpha + (a-b)^2)$ et $\mathcal{D}^{-1} : -\beta^2 = \alpha(\alpha+4a)(\alpha+4b)$. Cette dernière courbe est à 2-torsion $k_0[x]$-rationnelle et il est alors possible d'utiliser la méthode donnée dans le chapitre 1 pour montrer la non-existence de point d'ordre infini $\mathbb{C}(x)$-rationnel sur les courbes $\mathcal{C}^{-1}$ et $\mathcal{D}^{-1}$. Cela amène à étudier les courbes $\mathcal{C}^{-d} : -d\beta^2 = \alpha(\alpha^2-2(a+b)\alpha+(a-b)^2)$ et $\mathcal{D}^{-d} : -d\beta^2 = \alpha(\alpha+4a)(\alpha+4b)$ sur $k(x)$ où k est le corps de décomposition des polynômes ab et $(a-b)$. On observe aussi en adaptant la remarque 1.5.13 que pour limiter le nombre de cas à traiter pour les points de ces courbes, il faut que les décompositions en facteurs dans $\mathbb{C}[x]$ de ces polynômes ab et $(a-b)$ soient les plus simples possibles. Cependant, comme Hilbert a montré que les polynômes semi-définis positifs de degré total au plus 4 sont sommes de 3 carrés dans $\mathbb{R}[x,y]$, l'un au moins des polynômes a ou b doit être de degré supérieur ou égal à 4. Un choix intéressant est donc de prendre pour $a(x)$ le carré d'un polynôme de $\mathbb{R}[x]$ de degré 2, de plus, avec cette configuration, F est le produit d'une somme de 2 carrés par une somme de 3 carrés de polynômes dans $\mathbb{R}[x,y]$, c'est un cas de figure qui n'avait jusqu'à présent jamais été rencontré dans ce type de problème, aucun des polynômes proposé par Cassels, Ellison et Pfister ou par Christie ne se présentant sous cette forme. Par ailleurs, si l'on cherche à ce que $F(x,y)$ soit strictement positif, il faut que a n'ait pas de zéro réel, et après transformation linéaire, on supposera que $a = (x^2+1)^2$.

On choisira aussi, toujours pour limiter le nombre de facteurs dans $\mathbb{C}[x]$ des polynômes b et $(a-b)$, de prendre pour $(a-b)$ une constante réelle ou le carré d'un polynôme de degré 2 de la forme mx^2+n, avec $m,\ n \in \mathbb{R}$, le polynôme $F(x,y)$ ne dépendra alors que de x^2.

Dans la section 2.1, on fera une étude générale suivant la forme de a et de b des points de torsion d'ordre 2^n, $n \in \mathbb{N}^*$ des courbes $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ associées aux polynômes $F(x,y)=(y^2+a(x))(y^2+b(x))$ ce qui permettra d'exclure certains cas où la courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ possède des points de torsion spéciaux. Il sera utile aussi de déterminer les points d'ordre 2^n, $n \in \mathbb{N}^*$ sur les courbes $\mathcal{C}^{-d}_{k(x)}$ et $\mathcal{D}^{-d}_{k(x)}$, où k est le corps de décomposition de $ab(a-b)$ et $d \in k^*$, dans le but de faciliter ultérieurement l'étude des autres points de ces courbes.

Comme on l'a précisé ci-dessus, les polynômes $F(x,y)$ étudiés dans ce chapitre ne dépendront que de x^2, on proposera dans la section 2.2 une variante de la méthode du chapitre 1 qui s'applique à ce cas de figure et permet alors de se ramener à la démonstration de la non-existence de point d'ordre infini sur deux courbes elliptiques auxilliaires $\hat{\mathcal{C}}^{-1}$ et $\check{\mathcal{C}}^{-1}$ dont l'étude est plus simple que celle de $\mathcal{C}^{-1}$. On pourra, par un choix judicieux des polynômes a et b, faire en sorte que le corps k sur lequel on doit faire l'étude reste réel.

Ensuite, à la section 2.3, on s'intéressera au cas de la famille de polynômes $(y^2+(x^2+1)^2)(y^2+(x^2+1)^2-r^2)$ pour $0<r<1$, et on montrera que pour certaines de ces valeurs de r, ces polynômes ne sont pas des sommes de 3 carrés de fractions rationnelles et à la section 2.4, on proposera l'étude du cas limite $r=1$.

Il semble, à travers les différents exemples étudiés, que l'étude de ce qui se passe aux valeurs réelles de x où la courbe $\mathcal{C}^{-1}$ est singulière soit insuffisante pour conclure à la non-existence de point spécial sur cette courbe. De plus, dans l'exemple $(y^2+(x^2+1)^2)(y^2+(x^2+1)^2-r^2)$ avec $0<r<1$, on s'aperçoit que la fibration de la courbe $\mathcal{C}^{-1}$ ne présente pas de singularité réelle excepté à l'infini, l'existence des singularités réelles ne semble donc pas être une condition nécessaire dans ce type de problème. Cela deviendra plus évident dans la section 2.5 où l'on proposera l'étude d'une famille de polynômes pour lesquels la fibration sur $\mathbb{P}^1(\mathbb{R})$ de $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ et de $\mathcal{D}^{-1}_{\mathbb{R}(x)}$ ne présente aucune singularité réelle, pas même à l'infini : on montrera que pour certaines valeurs de $r \in [0,1]$, le polynôme $(y^2+(x^2+2)^2)(y^2+(x^2+2)^2-r^2(x^2+1)^2)$ n'est pas une somme de 3 carrés dans $\mathbb{R}(x,y)$

2.1 Etude des points d'ordre fini

On va considérer dans cette section les polynômes de la forme $F(x,y) = (y^2+a(x))(y^2+b(x)) = y^4+(a(x)+b(x))y^2+a(x)b(x))$ où $a(x)$ et $b(x)$ sont des polynômes positifs non constants de $\mathbb{R}[x]$. Avec cette nouvelle notation, on doit prendre pour k le corps de décomposition du polynôme $ab(a-b)$.

La courbe $\mathcal{C}^{-1}$ a pour équation $-\beta^2 = \alpha(\alpha^2-2(a+b)\alpha+(a-b)^2)$ et admet toujours le point $\mathcal{P}_\mathcal{C} = (0,0)$ d'ordre 2. La courbe $\mathcal{D}^{-1}$ a pour équation $-\beta^2 = \alpha(\alpha+4a)(\alpha+4b)$ et elle admet donc trois points $\mathbb{R}(x)$-rationnels d'ordre 2 qui sont $\mathcal{P}_\mathcal{D} = (0,0)$, $\mathcal{P}_1 = (-4a,0)$ et $\mathcal{P}_2 = (-4b,0)$.

L'objectif de cette section est double. D'une part, on veut s'assurer qu'aucun des points d'ordre 2^n, $n \in \mathbb{N}$, de la courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ n'est spécial et pour cela, il va falloir tous les déterminer. D'autre part, afin de faciliter l'étude ultérieure des courbes $\mathcal{C}^{-d}_{k(x)}$ et $\mathcal{D}^{-d}_{k(x)}$, avec $d \in k^*$, il est intéressant de connaître le plus possible de points de torsion de ces deux courbes : cela permettra de se ramener plus simplement aux conditions de la proposition 1.5.1. C'est pourquoi dans la suite de cette section, k va désigner un sous-corps quelconque de $\mathbb{C}$ et on étudiera, lorsque $d \in k^*$, la situation des points d'ordre 2^n sur les courbes $\mathcal{C}^{-d}_{k(x)}$ et $\mathcal{D}^{-d}_{k(x)}$ en s'intéresserant plus en détail au cas particulier où $k = \mathbb{R}$ et $d = 1$.

Pour cette étude, on va principalement utiliser les morphismes $\gamma_\mathcal{C}$ et $\gamma_\mathcal{D}$ et les isogénies $\varphi_{\mathcal{C},\mathcal{D}}$ et $\varphi_{\mathcal{D},\mathcal{C}}$ dont on rappelle ici les formules en les adaptant aux nouvelles notations :

Pour $\varphi_{\mathcal{C},\mathcal{D}} : \mathcal{C}^{-d} \to \mathcal{D}^{-d}$:

$\varphi_{\mathcal{C},\mathcal{D}}(\alpha,\beta) = \left(\frac{-d\beta^2}{\alpha^2}, \frac{\alpha^2-(a-b)^2}{\alpha^2}\beta\right)$ si $\alpha \neq 0$,

$\varphi_{\mathcal{C},\mathcal{D}}(\mathcal{P}_\mathcal{C}) = \mathcal{O}_\mathcal{D}$ et $\varphi_{\mathcal{C},\mathcal{D}}(\mathcal{O}_\mathcal{C}) = \mathcal{O}_\mathcal{D}$.

Pour $\varphi_{\mathcal{D},\mathcal{C}} : \mathcal{D}^{-d} \to \mathcal{C}^{-d}$:

$\varphi_{\mathcal{D},\mathcal{C}}(\alpha,\beta) = \left(\frac{-d\beta^2}{4\alpha^2}, \frac{\alpha^2-16ab}{8\alpha^2}\beta\right)$ si $\alpha \neq 0$

$\varphi_{\mathcal{C},\mathcal{D}}(\mathcal{P}_\mathcal{D}) = \mathcal{O}_\mathcal{C}$ et $\varphi_{\mathcal{C},\mathcal{D}}(\mathcal{O}_\mathcal{D}) = \mathcal{O}_\mathcal{C}$.

On rappelle aussi les équations des courbes $\mathcal{C}^{-d}$ et $\mathcal{D}^{-d}$:

$\mathcal{C}^{-d} : -d\beta^2 = \alpha(\alpha^2-2(a(x)+b(x))\alpha+(a(x)-b(x))^2)$,

$\mathcal{D}^{-d} : -d\beta^2 = \alpha(\alpha+4a(x))(\alpha+4b(x))$.

(A) Points d'ordre 2

Proposition 2.1.1 *Les points d'ordre 2 sur les courbes $\mathcal{C}^{-d}_{k(x)}$ et $\mathcal{D}^{-d}_{k(x)}$ sont les suivants :*

(i) Il y a toujours sur la courbe $\mathcal{C}^{-d}_{k(x)}$ le point $\mathcal{P}_{\mathcal{C}} = (0,0)$ d'ordre 2.

(ii) La courbe $\mathcal{C}^{-d}_{k(x)}$ possède deux autres points d'ordre 2 si et seulement si $ab \in k(x)^{*2}$. Si $k = \mathbb{R}$ et $d = 1$, ces deux points sont spéciaux.

(iii) La courbe $\mathcal{D}^{-d}_{k(x)}$ possède toujours trois points d'ordre 2 : $\mathcal{P}_{\mathcal{D}} = (0,0)$, $\mathcal{P}_1 = (-4a, 0)$ et $\mathcal{P}_2 = (-4b, 0)$.

Preuve. Les points (i) et (iii) sont évidents. Démontrer le (ii) revient à prouver que la courbe $\mathcal{C}^{-d}$ est à 2-torsion $k(x)$-rationnelle si et seulement si $ab \in k(x)^{*2}$, ce qui est une conséquence directe de la remarque 1.3.3 adaptée aux nouvelles notations.

Dans le cas où $k = \mathbb{R}$ et $d = 1$, on peut poser $ab = c^2$ avec $c \in \mathbb{R}[x]$ et on a alors :

$$\begin{aligned} \alpha^2 - 2(a+b)\alpha + (a-b)^2 &= \left(\alpha - (a+b)^2\right)^2 - 4ab \\ &= \left(\alpha - (a+b+2c)\right)\left(\alpha - (a+b-2c)\right). \end{aligned}$$

On obtient donc sur $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ des points d'ordre 2 de première coordonnée $\alpha = a + b \pm 2c$ et on vérifie aisément que ces points sont spéciaux : étant donné que $ab = c^2$ dans $\mathbb{R}[x]$, on peut écrire $a = PQ^2$ et $b = PR^2$ où P, Q, $R \in \mathbb{R}[x]$ et P est sans facteur carré, de plus P est positif car a et b le sont. On a alors $c = \pm PQR$ et $a + b \pm 2c = PQ^2 + PR^2 \pm 2PQR = P(Q \pm R)^2$, donc $a + b \pm 2c$ est positif. Ces points étant spéciaux, d'après le théorème 1.1.1 le polynôme F est somme de 3 carrés de fractions rationnelles. □

Remarque 2.1.2 On peut aussi voir directement que si ab est un carré dans $\mathbb{R}[x]$, le polynôme F est somme de 3 carrés de fractions rationnelles. En effet, comme $b = as^2$ avec $s \in \mathbb{R}(x)$ et $a = u_1^2 + u_2^2$, avec u_1, $u_2 \in \mathbb{R}[x]$, on a :

$$\begin{aligned} F(x,y) &= s^2\left(y^2 + u_1^2 + u_2^2\right)\left(\left(\frac{y}{s}\right)^2 + u_1^2 + u_2^2\right) \\ &= s^2\left(y^2 + 0^2 + u_1^2 + u_2^2\right)\left(0^2 + \left(\frac{y}{s}\right)^2 + (u_2)^2 + (-u_1)^2\right), \end{aligned}$$

et la formule de multiplication de quaternions donne une représentation de $F(x,y)$ comme somme de 3 carrés de fractions rationnelles.

Comme on s'intéresse au cas où il n'y a pas de points spéciaux sur $\mathcal{C}^{-1}_{\mathbb{R}(x)}$, on supposera à partir de maintenant que $ab \notin \mathbb{R}(x)^{*2}$. Dans ce cas, on ne peut pas non plus avoir $ab \in k(x)^{*2}$, car on aurait alors $ab \in \mathbb{C}(x)^{*2}$ et donc $-ab \in \mathbb{R}(x)^{*2}$, ce qui est impossible car ab est non négatif.

Corollaire 2.1.3 *Lorsque $ab \notin \mathbb{R}(x)^{*2}$, la courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ ne possède qu'un seul point d'ordre 2, $\mathcal{P}_\mathcal{C}$, qui n'est jamais spécial.*

Preuve. C'est une conséquence directe de la proposition 2.1.1, sachant que $\mathcal{P}_\mathcal{C}$ n'est jamais spécial car sa première coordonnée α est nulle et donc $-(\alpha^2 - 2(a+b)\alpha + (a-b)^2) = -(a-b)^2$ n'est pas somme de 2 carrés dans $\mathbb{R}(x)$. □

Avant d'étudier les points d'ordre 2^n supérieur à 2, on peut remarquer que :

Lemme 2.1.4 *Dans le cas général, les antécédents dans $\mathcal{D}^{-d}_{k(x)}$ par $\varphi_{\mathcal{D},\mathcal{C}}$ du point $\mathcal{P}_\mathcal{C}$, sont les points $\mathcal{P}_1 = (-4a, 0)$ et $\mathcal{P}_2 = (-4b, 0)$.*

Preuve. Comme $\gamma_\mathcal{C}(\mathcal{P}_\mathcal{C}) = (a-b)^2 k(x)^{*2}$, alors $\mathcal{P}_\mathcal{C} \in \ker(\gamma_\mathcal{C}) = \varphi_{\mathcal{D},\mathcal{C}}(\mathcal{D}^{-d}_{k(x)})$. Pour trouver ses antécédents par $\varphi_{\mathcal{D},\mathcal{C}}$, on va chercher $(\alpha, \beta) \in \mathcal{D}^{-d}_{k(x)}$ tel que $\varphi_{\mathcal{D},\mathcal{C}}(\alpha, \beta) = (0,0)$, lorsque $\alpha \neq 0$ cela donne :

$$\begin{cases} \frac{-\beta^2}{4\alpha^2} & = & 0 \\ \frac{\alpha^2 - 16ab}{8\alpha^2}\beta & = & 0 \end{cases}$$

On doit donc avoir $\beta = 0$, il n'y a que 3 possibilités sur $\mathcal{D}^{-d}_{k(x)}$ pour (α, β) : les points d'ordre 2 qui sont $\mathcal{P}_\mathcal{D} = (0,0)$, $\mathcal{P}_1 = (-4a, 0)$ et $\mathcal{P}_2 = (-4b, 0)$. Le point $\mathcal{P}_\mathcal{D}$ ne convient pas car $\varphi_{\mathcal{D},\mathcal{C}}(\mathcal{P}_\mathcal{D}) = \mathcal{O}_\mathcal{C}$, les antécédents de $\mathcal{P}_\mathcal{C}$ par $\varphi_{\mathcal{D},\mathcal{C}}$ sont donc les points $\mathcal{P}_1 = (-4a, 0)$ et $\mathcal{P}_2 = (-4b, 0)$. □

Le point $\mathcal{P}_\mathcal{C}$ peut donc éventuellement être un double sur $\mathcal{C}^{-d}_{k(x)}$, ce qui impliquerait l'existence de points d'ordre 4 sur cette courbe.

(B) Points d'ordre 2^n supérieur ou égal à 4

Proposition 2.1.5 *Les points d'ordre 2^n supérieur ou égal à 4 sur les courbes $\mathcal{C}^{-d}_{k(x)}$ et $\mathcal{D}^{-d}_{k(x)}$ sont les suivants :*

(i) Si ni da ni db ne sont des carrés dans $k(x)$, il n'y a pas de point d'ordre 4 ni sur $\mathcal{C}^{-d}_{k(x)}$, ni sur $\mathcal{D}^{-d}_{k(x)}$. En particulier cela se produit lorsque ni a ni b ne sont des carrés dans $\mathbb{C}(x)$.

(ii) Si $a = u^2$ avec $u \in k(x)^*$ et si $b \notin \mathbb{C}(x)^{*2}$, alors :

- *Si $d \notin k^{*2}$, il n'y a pas de point d'ordre 4, ni sur $\mathcal{C}^{-d}_{k(x)}$, ni sur $\mathcal{D}^{-d}_{k(x)}$.*
- *Si $d \in k^{*2}$, il y a des points d'ordre 4 sur $\mathcal{C}^{-d}_{k(x)}$ qui sont de la forme $(b-a, \pm\frac{2}{\sqrt{d}}(b-a)u)$. Dans le cas où $k = \mathbb{R}$ et $d = 1$, si $b - a$ est positif, alors ces points sont spéciaux.*
  - *Si $a - b$ n'est pas un carré dans $k(x)^*$, il n'y a pas de point d'ordre 4 sur $\mathcal{D}^{-d}_{k(x)}$ et pas de point d'ordre 8 sur $\mathcal{C}^{-d}_{k(x)}$.*
  - *Si $a - b = v^2$ avec $v \in k(x)$, il y a des points d'ordre 4 sur $\mathcal{D}^{-d}_{k(x)}$ qui sont : $(-4u(u+v), \pm\frac{8}{\sqrt{d}}uv(u+v))$ et $(-4u(u-v), \pm\frac{8}{\sqrt{d}}uv(u-v))$. Enfin, lorsque $u \notin k(x)^{*2}$ et $pgcd(u,v) = 1$, il n'y a aucun point d'ordre 8 ni sur $\mathcal{C}^{-d}_{k(x)}$, ni sur $\mathcal{D}^{-d}_{k(x)}$.*

Preuve. Pour déterminer d'éventuels points d'ordre 4 sur les courbes $\mathcal{C}^{-d}_{k(x)}$ et $\mathcal{D}^{-d}_{k(x)}$, il faut étudier l'existence d'antécédents par l'isogénie $\varphi_{\mathcal{C},\mathcal{D}}$ des points $\mathcal{P}_\mathcal{D}$, $\mathcal{P}_1$ et $\mathcal{P}_2$ de la courbe $\mathcal{D}^{-d}_{k(x)}$.

Tout d'abord on a $\gamma_\mathcal{D}(\mathcal{P}_\mathcal{D}) = abk(x)^{*2}$, or on a supposé que ab n'est pas un carré dans $k(x)$ donc $\mathcal{P}_\mathcal{D} \notin \ker(\gamma_\mathcal{D}) = \varphi_{\mathcal{C},\mathcal{D}}(\mathcal{C}^{-d}_{k(x)})$, ce point n'étant pas l'image d'un point de $\mathcal{C}^{-d}_{k(x)}$ par l'isogénie $\varphi_{\mathcal{C},\mathcal{D}}$, il ne peut donc pas non plus être un double sur $\mathcal{D}^{-d}_{k(x)}$. Par contre pour $\mathcal{P}_1$ et $\mathcal{P}_2$ la situation est différente : $\gamma_\mathcal{D}(\mathcal{P}_1) = dak(x)^{*2}$ et $\gamma_\mathcal{D}(\mathcal{P}_2) = dbk(x)^{*2}$ et on n'est pas dans le même cas de figure suivant que da ou db sont ou ne sont pas des carrés dans $k(x)$.

Pour démontrer le (i), il suffit de remarquer que si ni da ni db ne sont des carrés dans $k(x)$, alors aucun des points $\mathcal{P}_1$ et $\mathcal{P}_2$ n'appartient à $\ker(\gamma_\mathcal{D}) = \varphi_{\mathcal{C},\mathcal{D}}(\mathcal{C}^{-d}_{k(x)})$ et il n'y a pas de point d'ordre 4 ni sur $\mathcal{C}^{-1}_{k(x)}$, ni sur $\mathcal{D}^{-1}_{k(x)}$. Ceci sera en particulier le cas si a et b ne sont pas des carrés dans $\mathbb{C}(x)$.

On va maintenant démontrer le (ii), on suppose que $a = u^2$ avec $u \in k(x)^*$. Comme $b \notin \mathbb{C}(x)^{*2}$, db n'est un carré dans $k(x)$ pour aucune valeur de $d \in k^*$, et $\gamma_\mathcal{D}(\mathcal{P}_2) = dbk(x)^{*2} \neq k(x)^{*2}$. Le point $\mathcal{P}_2$ n'appartient donc pas à $\varphi_{\mathcal{C},\mathcal{D}}(\mathcal{C}^{-d}_{k(x)})$.

Par contre, $\gamma_\mathcal{D}(\mathcal{P}_1) = dak(x)^{*2} = du^2k(x)^{*2} = dk(x)^{*2}$, et $\mathcal{P}_1 \in \ker(\gamma_\mathcal{D}) = \varphi_{\mathcal{C},\mathcal{D}}(\mathcal{C}^{-d}_{k(x)})$ si et seulement si $d \in k^{*2}$. Ainsi, si $d \notin k^{*2}$, le point $\mathcal{P}_1$ n'admet pas d'antécédent par $\varphi_{\mathcal{C},\mathcal{D}}$ et il n'y a alors de point d'ordre 4 ni sur $\mathcal{C}^{-1}_{k(x)}$, ni sur $\mathcal{D}^{-1}_{k(x)}$.

On suppose désormais que $d \in k^{*2}$. Dans ce cas, il existe $(\alpha, \beta) \in \mathcal{C}^{-d}_{k(x)}$ tel que

$\varphi_{\mathcal{C},\mathcal{D}}(\alpha,\beta) = (-4a, 0)$ c'est-à-dire $\alpha \neq 0$ et :

$$\begin{cases} \frac{-d\beta^2}{\alpha^2} = -4a = -4u^2 \neq 0 & (1) \\ \frac{\alpha^2-(a-b)^2}{\alpha^2}\beta = 0 & (2) \\ -d\beta^2 = \alpha(\alpha^2 - 2(a+b)\alpha + (a-b)^2) & (3) \end{cases}$$

D'après (1), $\beta \neq 0$ donc dans (2) on obtient $\alpha^2 = (a-b)^2$.

* Si $\alpha = (a-b)$, on a dans (3), après calcul, $-d\beta^2 = (a-b)^2(-4b)$ ce qui est impossible car b n'est pas un carré dans $\mathbb{C}(x)$.

* Si $\alpha = (b-a)$, on a, d'après (3), $-d\beta^2 = (a-b)^2(-4a)$ donc $d\beta^2 = 4(a-b)^2u^2$, d'où $\beta = \pm\frac{2}{\sqrt{d}}(b-a)u$, ce qui donne les points $(b-a, \pm\frac{2}{\sqrt{d}}(b-a)u)$ sur la courbe $\mathcal{C}^{-d}_{k(x)}$.

Ces points sont bien d'ordre 4, car leur image par $\varphi_{\mathcal{D},\mathcal{C}} \circ \varphi_{\mathcal{C},\mathcal{D}}$, c'est-à-dire leur double, est le point $\mathcal{P}_{\mathcal{C}}$ d'ordre 2.

Il apparaît alors que, dans le cas où $k = \mathbb{R}$ et $d = 1$, si $b-a$ est un polynôme positif alors les points $(b-a, \pm 2(b-a)u)$, d'ordre 4 sur la courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$, sont spéciaux et donc $F(x,y)$ est une somme de 3 carrés dans $\mathbb{R}(x,y)$.

Remarque 2.1.6 Dans ce cas on pouvait voir directement que $F(x,y)$ est somme de 3 carrés dans $\mathbb{R}[x,y]$, en effet :

$$\begin{aligned} F(x,y) &= (y^2+a)(y^2+b) \\ &= (y^2+a)(y^2+a+b-a) \\ &= (y^2+a)^2 + (y^2+a)(b-a) \\ &= (y^2+a)^2 + (y^2+u^2)(b-a) \end{aligned}$$

Comme le polynôme $b-a$ est positif, il est somme de 2 carrés dans $\mathbb{R}[x]$, donc $(y^2+u^2)(b-a)$ est une somme de 2 carrés dans $\mathbb{R}[x,y]$, ce qui donne une écriture de $F(x,y)$ comme somme de 3 carrés de polynômes.

On observe maintenant que l'existence de points d'ordre 4 sur la courbe $\mathcal{D}^{-d}_{k(x)}$ est équivalente à celle d'antécédents par $\varphi_{\mathcal{D},\mathcal{C}}$ des points $(b-a, \pm\frac{2}{\sqrt{d}}(b-a)u)$. Or $\gamma_{\mathcal{C}}(b-a, \pm\frac{2}{\sqrt{d}}(b-a)u) = -d(b-a)k(x)^{*2} = (a-b)k(x)^{*2}$, donc si $a-b$ n'est pas un carré dans $k(x)^*$, il n'y a pas de point d'ordre 4 sur la courbe $\mathcal{D}^{-d}_{k(x)}$ et pas de point d'ordre 8 sur $\mathcal{C}^{-d}_{k(x)}$.

Par contre, si $(a-b)=v^2$, avec $v \in k(x)$, alors $(b-a, \pm\frac{2}{\sqrt{d}}(b-a)u) \in \ker(\gamma_{\mathcal{C}})$ et il existe $(\alpha,\beta) \in \mathcal{D}^{-d}_{k(x)}$ tel que $\varphi_{\mathcal{D},\mathcal{C}}(\alpha,\beta) = (b-a, \pm\frac{2}{\sqrt{d}}(b-a)u)$, ce qui équivaut à :

$$\begin{cases} \frac{-d\beta^2}{4\alpha^2} = b-a = -v^2 & (4) \\ \frac{\alpha^2-16ab}{8\alpha^2}\beta = \pm 2(b-a)u = \pm 2uv^2 & (5) \\ -d\beta^2 = \alpha(\alpha^2+4(a+b)\alpha+16ab) & (6) \end{cases}$$

D'après l'équation (4), $-d\beta^2 = -4v^2\alpha^2$ et donc en substituant dans l'équation (6), on a :

$$-4v^2\alpha^2 = \alpha(\alpha^2+4(a+b)\alpha+16ab).$$

Or $a=u^2$ et $a-b=v^2$, ce qui donne :

$$\alpha(\alpha^2+8u^2\alpha+16u^2(u^2-v^2)) = 0.$$

Mais $\alpha \neq 0$, sinon on aurait soit $\varphi_{\mathcal{D},\mathcal{C}}(\alpha,\beta) = \mathcal{O}_{\mathcal{C}}$, soit $\varphi_{\mathcal{D},\mathcal{C}}(\alpha,\beta) = \mathcal{P}_{\mathcal{C}}$, on obtient donc :

$$\alpha^2+8u^2\alpha+16u^2(u^2-v^2) = 0.$$

Comme le discriminant du polynôme $X^2+8u^2X+16u^2(u^2-v^2)$ est $64u^2v^2$, alors $\alpha = -4u(u \pm v)$ et on en déduit la seconde coordonnée β grâce à l'équation (5) ou à l'équation (6).

Enfin, pour qu'il n'y ait pas de point d'ordre 2^n supérieur ou égal à 8 ni sur $\mathcal{C}^{-d}_{k(x)}$, ni sur $\mathcal{D}^{-d}_{k(x)}$, il suffit alors qu'aucun des points d'ordre 4 de $\mathcal{D}^{-d}_{k(x)}$ n'appartienne à $\ker(\gamma_{\mathcal{D}})$, et comme on connait les images de ces points par $\gamma_{\mathcal{D}}$:

* $\gamma_{\mathcal{D}}(-4u(u+v), \pm\frac{8}{\sqrt{d}}uv(u+v)) = du(u+v)k(x)^{*2} = u(u+v)k(x)^{*2}$,
* $\gamma_{\mathcal{D}}(-4u(u-v), \pm\frac{8}{\sqrt{d}}uv(u-v)) = du(u-v)k(x)^{*2} = u(u-v)k(x)^{*2}$,

on s'aperçoit que cela est le cas lorsque ni $u(u+v)$, ni $u(u-v)$ ne sont des carrés dans $k(x)$.

Remarque 2.1.7 On peut supposer u et v premiers entre eux sinon, comme $a=u^2$ et $b=u^2-v^2$, alors a et b ont un facteur carré commun p^2 où $p=\mathrm{pgcd}(u,v)$, il est alors possible de se ramener au cas ou $\mathrm{pgcd}(u,v)=1$ par une transformation linéaire en y en posant $y=py'$.

Puisque $\mathrm{pgcd}(u,v)=1$, alors $\mathrm{pgcd}(u,u+v) = \mathrm{pgcd}(u,u-v) = 1$, donc il suffira de supposer que u n'est pas un carré dans $k(x)$ pour qu'il n'y ait pas de point d'ordre 8 sur aucune des courbes $\mathcal{C}^{-d}_{k(x)}$ et $\mathcal{D}^{-d}_{k(x)}$.

Cette remarque achève la démonstration de la proposition 2.1.5. □

On pourrait continuer l'étude des points d'ordre 2^n, par exemple dans le cas où $u = \mu^2$ et $u + v = \lambda^2$, λ, $\mu \in k(x)$. Il y a alors des points d'ordre 8 sur $\mathcal{C}^{-d}_{k(x)}$, de la forme :

$$\left((\mu^2 - \lambda^2)(\mu + \lambda)^2, \pm\tfrac{2}{\sqrt{d}}\mu\lambda(\mu^2 - \lambda^2)(\mu + \lambda)^2\right),$$

ainsi que les points :

$$\left((\mu^2 - \lambda^2)(\mu - \lambda)^2, \pm\tfrac{2}{\sqrt{d}}\mu\lambda(\mu^2 - \lambda^2)(\mu - \lambda)^2\right).$$

Il faudrait alors s'assurer, dans le cas où $k = \mathbb{R}$ et $d = 1$ que ces points d'ordre 8 ne sont pas spéciaux et, dans le cas génŕal, continuer l'étude lorsque ces points appartiennent à $\ker(\gamma_c)$ c'est-à-dire quand $-(\mu^2 - \lambda^2) \in \mathbb{R}(x)^{*2}$. Comme on peut supposer $\mathrm{pgcd}(\lambda, \mu) = 1$, on aurait alors $\lambda = \eta^2 + \xi^2$ et $\mu = \eta^2 - \xi^2$, avec η, $\xi \in k(x)$. Mais continuer ainsi cette étude s'avère très fastidieux et en pratique, on ne va étudier que des cas où u n'est pas un carré dans $\mathbb{C}(x)$ et donc où on n'a aucun point d'ordre 8.

(C) Lorsque le corps de base est $\mathbb{R}$

Il est intéressant pour la suite de limiter le nombre de facteurs irréductibles du polynôme $ab(a - b)$ en choisissant a et b tels que $a = u^2$ et $a - b = v^2$ avec u, $v \in \mathbb{R}(x)$, et dans ce cas les courbes $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ et $\mathcal{D}^{-1}_{\mathbb{R}(x)}$ peuvent posséder des points d'ordre 4. C'est pourquoi on termine cette section par un résumé des conditions nécessaires afin de ne pas avoir de point spécial d'ordre 2^n sur la courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$, ce qui permettra d'orienter le choix des polynômes a et b pour les exemples traités :

- On doit avoir $ab \notin \mathbb{R}(x)^{*2}$, sinon la courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ possède des points d'ordre 2 spéciaux.
- Lorsque $a = u^2$ avec $u \in \mathbb{R}(x)$, on doit supposer que $b - a$ n'est pas positif sinon la courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ possède des points d'ordre 4 spéciaux.
- Lorsque $a - b = v^2$ avec $v \in \mathbb{R}(x)$, on supposera que $\mathrm{pgcd}(u, v) = 1$ et que $u \notin \mathbb{R}(x)^{*2}$, cela suffira à interdire l'existence de point d'ordre supérieur ou égal à 8 sur la courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$.

2.2 Polynômes pairs

Dans cette section, on va s'intéresser au cas particulier où le polynôme $F(x,y)$ est pair relativement à x et où on peut donc écrire $F(x,y) = y^4 + A(x^2)y^2 + B(x^2)$, A et B étant des polynômes en une variable et à coefficients dans le corps $k_0 \subset \mathbb{R}$.

Il est alors intéressant de remarquer que la courbe $\mathcal{C}^{-1}$ a ici pour équation : $-\beta^2 = \alpha(\alpha^2 - 2A(x^2)\alpha + A^2(x^2) - 4B(x^2))$ et est donc globalement invariante par l'involution $\sigma_x : \mathbb{R}(x) \to \mathbb{R}(x)$ définie par :

$$\begin{cases} \sigma_x|_{\mathbb{R}} = Id|_{\mathbb{R}} \\ \sigma_x(x) = -x \end{cases}$$

Cette particularité va permettre dans certains cas de remplacer l'étude des points d'ordre infini de la courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ par celle de courbes elliptiques plus faciles à étudier, cela se fera en appliquant la proposition suivante :

Proposition 2.2.1 *Si la courbe $\mathcal{C}^{-1} : -\beta^2 = \alpha(\alpha^2 - 2A(x^2)\alpha + A^2(x^2) - 4B(x^2))$ admet un point d'ordre infini $\mathbb{R}(x)$-rationnel, alors il existe un point d'ordre infini, défini sur le corps des fractions $\mathbb{R}(z)$, sur l'une des deux courbes $\hat{\mathcal{C}}^{-1}$ ou $\check{\mathcal{C}}^{-1}$ d'équations :*

* $\hat{\mathcal{C}}^{-1} : -\beta^2 = \alpha(\alpha^2 - 2A(z)\alpha + A^2(z) - 4B(z))$
* $\check{\mathcal{C}}^{-1} : -\beta^2 = \alpha(\alpha^2 - 2zA(z)\alpha + z^2A^2(z) - 4z^2B(z))$.

Preuve. On suppose qu'il existe un point P, non de torsion, sur $\mathcal{C}^{-1}_{R(x)}$. Comme la courbe $\mathcal{C}^{-1}_{R(x)}$ est globalement invariante par la transformation σ_x, alors le point $\sigma_x(P)$ appartient aussi à $\mathcal{C}^{-1}_{R(x)}$, car si on pose $P = (\alpha_P, \beta_P)$, alors $\sigma_x(P) = (\sigma_x(\alpha_P), \sigma_x(\beta_P)))$.

Considérons maintenant le point $Q = P + \sigma_x(P)$:

* Dans le cas où ce point n'est pas de torsion, il est invariant par σ_x et ses coordonnées sont donc des fractions rationnelles paires en x. On a donc $Q = (\alpha_Q(x^2), \beta_Q(x^2))$ vérifiant la relation :
  $-\beta_Q^2(x^2) = \alpha_Q(\alpha_Q^2(x^2) - 2A(x^2)\alpha_Q(x^2) + A^2(x^2) - 4B(x^2))$
  En posant $z = x^2$, on obtient :
  $-\beta_Q^2(z) = \alpha_Q(z)(\alpha_Q^2(z) - 2A(z)\alpha_Q(z) + A^2(z) - 4B(z))$.
  On a ainsi un point $(\alpha_Q(z), \beta_Q(z)) \in \hat{\mathcal{C}}^{-1}_{\mathbb{R}(z)}$ et ce point est d'ordre infini sur $\hat{\mathcal{C}}^{-1}_{\mathbb{R}(z)}$ car Q n'est pas de torsion sur $\mathcal{C}^{-1}_{R(x)}$.

* Si le point Q est de torsion sur $\mathcal{C}^{-1}_{R(x)}$, on note $n \in \mathbb{N}$ son ordre et alors $nQ = \mathcal{O}_{\mathcal{C}}$ donc $nP = -n\sigma_x(P)$. En posant $R = nP$, on obtient un point d'ordre infini sur $\mathcal{C}^{-1}_{R(x)}$ vérifiant $\sigma_x(R) = -R$. La première coordonnée de R est donc invariante par la transformation σ_x, ce qui prouve que c'est une fraction rationnelle paire en x. La seconde coordonnée β_1 de ce point vérifie $\sigma_x(\beta_1) = -\beta_1$ et est donc une fraction rationnelle impaire en x. On peut alors écrire: $R = (\alpha_R(x^2), x\beta_R(x^2))$ où α_R et β_R sont des fractions rationnelles à coefficients dans $\mathbb{R}$.

  Cela donne, dans l'équation de $\mathcal{C}^{-1}_{R(x)}$:
  $-x^2\beta_R^2(x^2) = \alpha_R(x^2)(\alpha_R^2(x^2) - 2A(x^2)\alpha_R(x^2) + A^2(x^2) - 4B(x^2))$.
  En posant $z = x^2$, on obtient :
  $-z\beta_R^2(z) = \alpha_R(z)(\alpha_R^2(z) - 2A(z)\alpha_R(z) + A^2(z) - 4B(z))$.
  On a ainsi, avec la notation introduite au chapitre 1, un point d'ordre infini sur la courbe elliptique $\mathcal{C}^{-z}_{\mathbb{R}(z)}$. Pour achever la démonstration de la proposition, on pose :

$$\begin{cases} \alpha = z\alpha_R \\ \beta = z^2\beta_R \end{cases}$$

  Ce qui donne la relation : $-\frac{\beta^2}{z^3} = \frac{\alpha}{z}(\frac{\alpha^2}{z^2} - 2A(z)\frac{\alpha}{z} + A^2(z) - 4B(z))$, c'est-à-dire après simplification:

$$-\beta^2 = \alpha(\alpha^2 - 2zA(z)\alpha + z^2A^2(z) - 4z^2B(z)).$$

  On a alors un point sur la courbe $\check{\mathcal{C}}^{-1}_{\mathbb{R}(z)}$ qui n'est pas de torsion car le point R est d'ordre infini sur $\mathcal{C}^{-1}_{R(x)}$.

L'existence d'un point P d'ordre infini sur $\mathcal{C}^{-1}_{R(x)}$ implique donc soit celle d'un point d'ordre infini sur la courbe $\hat{\mathcal{C}}^{-1}_{\mathbb{R}(z)}$ dans le premier cas, soit celle d'un point d'ordre infini sur la courbe $\check{\mathcal{C}}^{-1}_{\mathbb{R}(z)}$ dans le second cas. □

Grâce à cette proposition, on peut se ramener à travailler sur les courbes $\hat{\mathcal{C}}^{-1}$ et $\check{\mathcal{C}}^{-1}$: Pour démontrer que la courbe $\mathcal{C}^{-1}_{R(x)}$ n'a pas de point d'ordre infini, on prouvera qu'aucune des deux courbes $\hat{\mathcal{C}}^{-1}_{R(x)}$ et $\check{\mathcal{C}}^{-1}_{R(x)}$ n'en possède et pour cela, on pourra utiliser la méthode donnée au chapitre 1.

On introduira donc les courbes $\hat{\mathcal{D}}^{-1} : -\beta^2 = \alpha(\alpha^2 + 4A(z)\alpha + 16B(z))$ et $\check{\mathcal{D}}^{-1} : -\beta^2 = \alpha(\alpha^2 + 4zA(z)\alpha + 16z^2B(z))$. Comme on l'a remarqué auparavant, pour que l'étude de $\hat{\mathcal{C}}^{-1}$ par cette méthode soit possible, il faut que l'une des deux courbes $\hat{\mathcal{C}}^{-1}$ ou $\hat{\mathcal{D}}^{-1}$ soit à 2-torsion $\mathbb{C}(z)$-rationnelle. De même pour étudier $\check{\mathcal{C}}^{-1}$, il

est nécessaire que $\check{\mathcal{C}}^{-1}$ ou $\check{\mathcal{D}}^{-1}$ soit aussi à 2-torsion $\mathbb{C}(z)$-rationnelle. On remarque que si $\hat{\mathcal{C}}^{-1}$ (respectivement $\hat{\mathcal{D}}^{-1}$) est à 2-torsion $\mathbb{C}(z)$-rationnelle, alors c'est aussi le cas de $\check{\mathcal{C}}^{-1}$ (respectivement $\check{\mathcal{D}}^{-1}$) : cela est vérifié lorsque $B(z)$ (respectivement $A^2(z)-4B(z)$) est un carré dans $\mathbb{C}(z)$ et on se placera donc dans l'un de ces cas. On choisira le corps k de telle manière que les polynômes $A^2(z)-4B(z)$ et $B(z)$ soient décomposés sur $k(z)$ et que $B(z)$ (respectivement $A^2(z)-4B(z)$) soit un carré dans $k(z)$. En suivant la méthode du chapitre 1, on sera amené à étudier, pour $d \in k^*$, les points des courbes $\hat{\mathcal{C}}^{-d}_{k(z)}$, $\hat{\mathcal{D}}^{-d}_{k(z)}$ d'une part et $\check{\mathcal{C}}^{-d}_{k(z)}$ et $\check{\mathcal{D}}^{-d}_{k(z)}$ d'autre part afin de se ramener aux conditions de la proposition 1.5.1 pour chacune des courbes $\hat{\mathcal{C}}^{-1}$ et $\check{\mathcal{C}}^{-1}$.

L'intérêt de substituer à l'étude de $\mathcal{C}^{-1}$ celle des deux courbes auxilaires $\hat{\mathcal{C}}^{-1}$ et $\check{\mathcal{C}}^{-1}$ est que dans certains cas il sera plus simple de travailler sur ces deux dernières. En effet, pour étudier les points des courbes $\hat{\mathcal{C}}^{-d}_{k(z)}$, $\hat{\mathcal{D}}^{-d}_{k(z)}$, $\check{\mathcal{C}}^{-d}_{k(z)}$ et $\check{\mathcal{D}}^{-d}_{k(z)}$ on travaillera sur le corps k, alors qu'auparavant on considérait les courbes $\mathcal{C}^{-d}$ et $\mathcal{D}^{-d}$ définies sur le corps de décomposition des polynômes $A^2(x^2)-4B(x^2)$ et $B(x^2)$, le corps k est très souvent plus restreint que ce dernier, en particulier, sur des exemples bien choisis, on a $k \subset \mathbb{R}$, ce qui permet d'utiliser des conditions de signe. De plus le nombre de facteurs premiers des polynômes $A^2(z)-4B(z)$ et $B(z)$ dans $\mathbb{C}(z)$ est moins important que le nombre de facteurs de $A^2(x^2)-4B(x^2)$ et $B(x^2)$ dans $\mathbb{C}(x)$, ce qui, étant donné ce qu'on a démontré dans le lemme 1.5.13, permet de diminuer le nombre de cas à étudier sur chaque courbe.

Ainsi pour prouver qu'une courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ n'a pas de point spécial, on commencera toujours par effectuer l'étude des points d'ordre 2^n, $n \in \mathbb{N}$, pour s'assurer qu'aucun d'entre eux n'est spécial, puis on fera l'étude des points des quatre courbes $\hat{\mathcal{C}}^{-d}_{k(z)}$, $\hat{\mathcal{D}}^{-d}_{k(z)}$, $\check{\mathcal{C}}^{-d}_{k(z)}$ et $\check{\mathcal{D}}^{-d}_{k(z)}$ afin de se ramener aux conditions de la proposition suivante, où $\hat{\gamma}_{\mathcal{C}}$ (respectivement $\hat{\gamma}_{\mathcal{D}}$, $\check{\gamma}_{\mathcal{C}}$, $\check{\gamma}_{\mathcal{D}}$) désigne l'analogue du morphisme $\gamma_{\mathcal{C}}$ pour la courbe $\hat{\mathcal{C}}^{-d}_{k(z)}$ (respectivement $\hat{\mathcal{D}}^{-d}_{k(z)}$, $\check{\mathcal{C}}^{-d}_{k(z)}$, $\check{\mathcal{D}}^{-d}_{k(z)}$) :

Proposition 2.2.2 *Si pour tout élément $d \in k^*$, les images des morphismes $\hat{\gamma}_{\mathcal{C}} : \hat{\mathcal{C}}^{-d}_{k(z)} \to k(z)^*/k(z)^{*2}$, $\hat{\gamma}_{\mathcal{D}} : \hat{\mathcal{D}}^{-d}_{k(z)} \to k(z)^*/k(z)^{*2}$, $\check{\gamma}_{\mathcal{C}} : \check{\mathcal{C}}^{-d}_{k(z)} \to k(z)^*/k(z)^{*2}$ et $\check{\gamma}_{\mathcal{D}} : \check{\mathcal{D}}^{-d}_{k(z)} \to k(z)^*/k(z)^{*2}$ sont les images des points de torsion alors la courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ est de rang nul.*

Preuve. On démontre, comme au chapitre 1, que sous ces conditions, il n'y a pas de point d'ordre infini ni sur $\hat{\mathcal{C}}^{-1}_{\mathbb{R}(z)}$, ni sur $\check{\mathcal{C}}^{-1}_{\mathbb{R}(z)}$ donc d'après la proposition 2.2.1, il ne peut pas y avoir de point d'ordre infini sur $\mathcal{C}^{-1}_{\mathbb{R}(x)}$. □

2.3 Une première famille de polynômes factorisés

On va considérer dans cette section le polynôme $F(x,y) = (y^2 + a(x))(y^2 + b(x))$ avec $a(x) = (x^2+1)^2$ et $b(x) = (x^2+1)^2 - r^2$ et $0 < r < 1$, on va montrer que pour certaines valeurs de r, ce polynôme n'est pas une somme de 3 carrés dans $\mathbb{R}(x,y)$, en particulier on prouvera le théorème suivant :

Théorème 2.3.1 *Soit r un nombre réel tel que $0 < r < 1$, si r est transcendant ou si r est un nombre rationnel tel que ni r, ni $r(r+1)$ ne sont des carrés de rationnels, alors le polynôme $F(x,y) = (y^2 + (x^2+1)^2)(y^2 + (x^2+1)^2 - r^2)$ est strictement positif mais n'est pas une somme de 3 carrés dans $\mathbb{R}(x,y)$.*

Parmi les polynômes positifs factorisés sous cette forme, $F(x,y) = (y^2 + (x^2+1)^2)(y^2 + (x^2+1)^2 - r^2)$ est l'exemple le plus simple à étudier : Comme on l'a signalé dans l'introduction de ce chapitre, en prenant pour $a(x)$ le carré d'un polynôme de degré 2 et strictement positif, après transformation linéaire, on peut supposer que $a(x) = (x^2+1)^2$, et pour limiter le nombre de facteurs dans $\mathbb{C}[x]$ des polynômes b et $(a-b)$, on prend pour $(a-b)$ une constante réelle sous forme d'un carré r^2, car alors on peut écrire $b(x) = (x^2+1)^2 - r^2 = (x^2+1-r)(x^2+1+r)$, ce qui permet d'effectuer une première factorisation sans introduire de racine carrée.

Les courbes elliptiques associées à ce polynôme F sont :

* $\mathcal{C}^{-1} : -\beta^2 = \alpha(\alpha^2 - 2(a+b)\alpha + (a-b)^2)$, ce qui donne :
  $-\beta^2 = \alpha(\alpha^2 - 2(2(x^2+1)^2 - r^2)\alpha + r^4)$

* $\mathcal{D}^{-1} : -\beta^2 = \alpha(\alpha + 4a)(\alpha + 4b)$, c'est-à-dire :
  $-\beta^2 = \alpha(\alpha + 4(x^2+1)^2)(\alpha + 4[(x^2+1)^2 - r^2])$

On remarque que pour tout $x_0 \in \mathbb{R}$, $0 < a(x_0) < b(x_0)$, cela implique alors clairement que pour tout $x_0 \in \mathbb{R}$, les points d'ordre 2 de la courbe elliptique d'équation $-\beta^2 = \alpha(\alpha + 4a(x_0))(\alpha + 4b(x_0))$ définie sur $\mathbb{R}$ sont tous distincts, donc la fibration de la courbe $\mathcal{D}^{-1}$ n'admet pas de singularité réelle autre qu'à l'infini. De même si $x_0 \in \mathbb{R}$, les points d'ordre 2 de la courbe elliptique d'équation $-\beta^2 = \alpha(\alpha^2 - 2(a(x_0)+b(x_0))\alpha + (a(x_0)-b(x_0))^2)$ définie sur $\mathbb{R}$ ont pour premières coordonnées 0, $a(x_0) + b(x_0) - 2\sqrt{a(x_0)b(x_0)}$ et $a(x_0) + b(x_0) + 2\sqrt{a(x_0)b(x_0)}$ et comme les polynômes ab et $a-b$ ne s'annulent pas sur $\mathbb{R}$, ces points sont distincts et la fibration de la courbe $\mathcal{C}^{-1}$ n'admet de singularité en aucun point $x_0 \in \mathbb{R}$. Par

contre les coefficients dominants des polynômes a et b étant égaux, cette fibration admet une singularité réelle à l'infini.

Ainsi l'étude de ces courbes ne peut pas être basée sur des arguments de spécialisation en des valeur réelles pour lesquelles la courbe dégénère, il faut utiliser des arguments correspondants à des singularités complexes de la fibration. Ce recours à des spécialisations de x en des valeurs complexes sera masqué par l'application de la proposition 2.2.1, ayant posé $z = x^2$, les spécialisations de z se feront ici en des valeurs réelles.

On remarque en effet que le polynôme F est pair relativement à x donc, comme on l'a vu à la section précédente, on sera amené à considérer les courbes elliptiques suivantes :

* $\hat{\mathcal{C}}^{-1} : -\beta^2 = \alpha(\alpha^2 - 2(2(z+1)^2 - r^2)\alpha + r^4)$
* $\hat{\mathcal{D}}^{-1} : -\beta^2 = \alpha(\alpha + 4(z+1)^2)(\alpha + 4[(z+1)^2 - r^2])$
* $\check{\mathcal{C}}^{-1} : -\beta^2 = \alpha(\alpha^2 - 2(2(z+1)^2 - r^2)z\alpha + r^4z^2)$
* $\check{\mathcal{D}}^{-1} : -\beta^2 = \alpha(\alpha + 4(z+1)^2z)(\alpha + 4[(z+1)^2 - r^2]z)$

Ces courbes elliptiques sont définies sur le corps $k_0(z)$ avec $k_0 = \mathbb{Q}(r)$. Si les deux courbes $\hat{\mathcal{C}}^{-1}$ et $\check{\mathcal{C}}^{-1}$ ne sont pas à 2-torsion $k_0(z)$-rationnelle, en revanche, $\hat{\mathcal{D}}^{-1}$ et $\check{\mathcal{D}}^{-1}$ le sont, on est donc bien dans un cas de figure où l'on peut prouver la non-existence de point d'ordre infini sur les courbes $\hat{\mathcal{C}}^{-1}$ et $\check{\mathcal{C}}^{-1}$ avec la méthode proposée au chapitre 1. Pour cela on doit introduire k le corps de décomposition des polynômes $a-b = r^2$ et $ab = (z+1)^2[(z+1)^2-r^2] = (z+1)^2(z+1+r)(z+1-r)$, c'est-à-dire $k = \mathbb{Q}(r) = k_0$.

Voici le plan que l'on suivra pour montrer que sous certaines conditions sur le nombre r, $F(x,y) = (y^2 + (x^2+1)^2)(y^2 + (x^2+1)^2 - r^2)$ n'est pas somme de 3 carrés dans $\mathbb{R}(x,y)$:

(A) On commence par déterminer les points d'ordre 2^n, $n \in \mathbb{N}$, de la courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ pour s'assurer qu'aucun d'entre eux n'est spécial.

(B) Pour $d \in k^*$, on étudie les points de la courbe $\hat{\mathcal{C}}^{-d} : -d\beta^2 = \alpha(\alpha^2 - 2(2(z+1)^2 - r^2)\alpha + r^4)$ définis sur le corps $k(z)$ afin de déterminer des conditions suffisantes sur le réel r pour que l'image du morphisme $\hat{\gamma}_c : \hat{\mathcal{C}}^{-d}_{k(z)} \to k(z)^*/k(z)^{*2}$ soit l'image des points de torsion c'est-à-dire , dans ce cas, triviale. Il apparaîtra en fait que cela est vrai pour toutes les valeurs de r.

(C) Pour $d \in k^*$, on étudie les points de la courbe $\hat{\mathcal{D}}^{-d} : -d\beta^2 = \alpha(\alpha + 4(z+1)^2)(\alpha + 4[(z+1)^2 - r^2])$ définis sur le corps $k(z)$ afin de déterminer des conditions suffisantes sur le réel r pour que l'image du morphisme $\hat{\gamma}_{\mathcal{D}} : \hat{\mathcal{C}}^{-d}_{k(z)} \to k(z)^*/k(z)^{*2}$ soit l'image des points de torsion, et comme à la partie (B), on verra qu'aucune condition spécifique sur r n'est requise.

(D) On recherche en étudiant la courbe $\check{\mathcal{C}}^{-d} : -d\beta^2 = \alpha(\alpha^2 - 2(2(z+1)^2 - r^2)z\alpha + r^4z^2)$ des conditions suffisantes sur r pour que, pour tout $d \in k^*$, l'image du morphisme $\check{\gamma}_{\mathcal{C}} : \check{\mathcal{C}}^{-d}_{k(z)} \to k(z)^*/k(z)^{*2}$ soit l'image des points de torsion.

(E) On recherche en étudiant $\check{\mathcal{D}}^{-d} : -d\beta^2 = \alpha(\alpha+4(z+1)^2z)(\alpha+4[(z+1)^2-r^2]z)$ des conditions suffisantes sur r pour que. pour tout $d \in k^*$, l'image du morphisme $\check{\gamma}_{\mathcal{D}} : \check{\mathcal{C}}^{-d}_{k(z)} \to k(z)^*/k(z)^{*2}$ soit l'image des points de torsion.

(F) Pour conclure cette section on reformulera certaines des conditions portant sur le nombre r obtenues aux parties (D) et (E) et qui permettent de se ramener aux hypothèses de la proposition 2.2.2 prouvant alors que la courbe $\mathcal{C}^{-1}$ n'a pas de point spécial.

Pour alléger l'écriture lors de l'étude de ces courbes, ainsi que pour les cas traités dans les sections suivantes, on introduit la notation suivante :

Notation 2.3.2 *Si k est un corps et si g et h sont deux éléments de k^*, on écrira $g \sim h$ quand $gk^{*2} = hk^{*2}$, c'est-à-dire quand g et h appartiennent à la même classe de carrés dans k^*.*

(A) Etude des points d'ordre 2^n

On est dans le cas où $a = u^2$ avec $u = x^2 + 1$, de plus $a - b = v^2$, avec $v = r$, mais par contre le polynôme u n'est pas un carré dans $\mathbb{R}(x)$, donc d'après les résultats démontrés à la section 2.1, il y a des points $\mathbb{R}(x)$-rationnels d'ordre 4 sur les courbes $\mathcal{C}^{-1}$ (et aussi sur $\mathcal{D}^{-1}$) mais comme u et v sont premier entre eux, et que u n'est pas un carré, il n'y a pas de points d'ordre 8 sur la courbe $\mathcal{C}^{-1}$. Les points d'ordre 2^n définis sur $\mathbb{R}(x)$ sur la courbe $\mathcal{C}^{-1}$ sont donc :

* Le point $\mathcal{P}_{\mathcal{C}} = (0, 0)$ d'ordre 2.

$*$ Les points $(-r^2, 2r^2(x^2+1))$ et $(-r^2, -2r^2(x^2+1))$ d'ordre 4.

On vérifie aisément qu'aucun de ces points de $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ n'est spécial.

(B) Etude de $\hat{\mathcal{C}}^{-\mathbf{d}}_{\mathbf{k(z)}}$

On va dans cette partie démontrer que pour tout $d \in k^*$, l'image du morphisme $\hat{\gamma}_c : \hat{\mathcal{C}}^{-d}_{k(z)} \to k(z)^*/k(z)^{*2}$ est celle des points d'ordre fini. Les seuls points d'ordre 2^n sont le point $\mathcal{P}_\mathcal{C}$ d'ordre 2 et deux points d'ordre 4 lorsque d est un carré dans k. Ce sont les seuls points de torsion que l'on connait, l'existence de points d'ordre impair n'ayant pas été étudiée. Comme $\hat{\gamma}_c(\mathcal{P}_\mathcal{C}) = k(z)^{*2}$, et que l'image des points d'ordre 4, lorsqu'ils existent, est elle aussi triviale, il faut donc montrer que l'image de $\hat{\gamma}_c$ est triviale.

Soit (α, β) un point de $\hat{\mathcal{C}}^{-d}_{k(z)}$ vérifiant $\beta \neq 0$, c'est-à-dire $(\alpha, \beta) \neq \mathcal{P}_\mathcal{C}$, alors on sait d'après le lemme 1.5.13 qu'il est possible d'écrire $\alpha = f\frac{\theta^2}{\psi^2}$ avec f, θ, $\psi \in k[z]$ tel que $\mathrm{pgcd}(f\theta, \psi) = 1$ et f soit sans facteur carré et divise le terme constant r^4. Donc $f = e \in k^*$ et comme $\hat{\gamma}_c(\alpha, \beta) = -dfk^{*2} = -dek^{*2}$, on doit montrer que $-de \in k^{*2}$.

De l'équation $-d\beta^2 = \alpha(\alpha^2 - 2(2(z+1)^2 - r^2)\alpha + r^4)$, on déduit, toujours d'après le lemme 1.5.13, qu'il existe $\mu \in k[z]$ tel que $-de\mu^2 = e^2\theta^4 - 2(2(z+1)^2 - r^2)e\theta^2\psi^2 + r^4\psi^4$ donc on a :

$$-de\mu^2 = (e\theta^2 - r^2\psi^2)^2 - 4((z+1)^2 - r^2)e\theta^2\psi^2 \quad \text{c'est-à-dire,}$$
$$-de\mu^2 = (e\theta^2 - r^2\psi^2)^2 - 4(z+1-r)(z+1+r)e\theta^2\psi^2 \qquad (1).$$

En posant $z = r-1$ (ou de même $z = -r-1$), on a : $-de\mu^2(r-1) = (e\theta^2(r-1) - r^2\psi^2(r-1))^2$.

Si on suppose que $(e\theta^2(r-1) - r^2\psi^2(r-1))^2 = -de\mu^2(r-1) = 0$ alors le polynôme irréductible $(z+1-r)$ divise à la fois $(e\theta^2 - r^2\psi^2)$ et μ, donc $(z+1-r)^2$ divise les deux menbres de l'équation (1) ainsi que $(e\theta^2 - r^2\psi^2)^2$. Cela implique que $(z+1-r)$ divise aussi $(z+1+r)e\theta^2\psi^2$, d'où $(z+1-r)$ divise θ ou ψ. Mais étant donné que $(z+1-r)$ divise aussi $(e\theta^2 - r^2\psi^2)$, on obtient que $(z+1-r)$ divise à la fois θ et ψ contredisant ainsi l'hypothèse $\mathrm{pgcd}(\theta, \psi) = 1$. On peut donc déduire que $\mu^2(r-1) \neq 0$ et $-de = \left(\frac{e\theta^2(r-1) - r^2\psi^2(r-1)}{\mu(r-1)}\right)^2 \neq 0$ d'où $-de \in k^{*2}$, on a le résultat souhaité.

(C) Etude de $\hat{\mathcal{D}}^{-\mathbf{d}}_{\mathbf{k(z)}}$

On va ici démontrer que l'image du morphisme $\hat{\gamma}_{\mathcal{D}} : \hat{\mathcal{D}}^{-d}_{k(z)} \to k(z)^*/k(z)^{*2}$ est l'image des points d'ordre fini. Pour cela, il est intéressant de rappeler que dans la section 2.2 on a déterminé les points d'ordre 2^n des courbes $\hat{\mathcal{D}}^{-d}_{k(z)}$ dont l'équation est de la forme $-d\beta^2 = \alpha(\alpha + 4a(z))(\alpha + 4b(z))$, avec ici $a(z) = (z+1)^2$ et $b(z) = (z+1)^2 - r^2$. On a donc $a = u^2$ et $a - b = v^2$ avec $u = z + 1$ et $v = r$, on connait ainsi sur la courbe $\hat{\mathcal{D}}^{-d}_{k(z)}$ les points suivants :

* Les points $\mathcal{P}_{\mathcal{D}} = (0,0)$, $\mathcal{P}_1 = (-4(z+1)^2, 0)$ et $\mathcal{P}_2 = (-4(z+1-r)(z+1+r), 0)$ d'ordre 2 qui existent dans tous les cas.

* Les points $(-4(z+1)(z+1-r), \pm\frac{8}{\sqrt{d}}r(z+1)(z+1-r))$ et $(-4(z+1)(z+1+r), \pm\frac{8}{\sqrt{d}}r(z+1)(z+1+r))$ d'ordre 4 qui existent lorsque d est un carré dans k.

Comme u n'est pas un carré dans $\mathbb{C}(x)$ et que u et v sont premiers entre eux, alors il n'y a pas de point d'ordre 8 sur cette courbe. On voit aussi qu'il faudra distinguer deux cas suivant que d est ou n'est pas un carré dans k. Cependant, il est intéressant de remarquer auparavant le résultat suivant :

Lemme 2.3.3 *En utilisant les notations du lemme 1.5.13, si (α, β) est un point de $\hat{\mathcal{D}}^{-d}_{k(z)}$ vérifiant $\beta \neq 0$, on a vu que $\alpha = f\frac{\theta^2}{\psi^2}$, avec f, θ, $\psi \in k[z]$, $pgcd(f\theta, \psi) = 1$ et f sans facteur carré, mais de plus ici, f est de degré pair et si on note e son coefficient dominant, alors on a soit $-de \in k^{*2}$, soit $-e \in k^{*2}$.*

Preuve. Il suffit de remarquer que comme $-d\beta^2 = \alpha(\alpha^2 + 4[2(z+1)^2 - r^2]\alpha + 16[(z+1)^2 - r^2](z+1)^2)$, on obtient avec les notations du lemme 1.5.13,

$$-df\mu^2 = f^2\theta^4 + 4[2(z+1)^2 - r^2]f\theta^2\psi^2 + 16[(z+1)^2 - r^2](z+1)^2\psi^4.$$

Donc, comme $\deg((z+1)^2 - r^2) = 2$ et $\deg[(z+1)^2 - r^2](z+1)^2 = 4$, on a, en notant a_θ, a_ψ et a_μ les coefficients dominants respectifs de θ, ψ et μ :

* Si $\deg(f\theta^2) > \deg(\psi^2) + 2$, alors $\deg(f\mu^2) = \deg(f^2\theta^4)$ et $-dea_\mu^2 = e^2a_\theta^4$.

* Si $\deg(f\theta^2) < \deg(\psi^2) + 2$, alors $\deg(f\mu^2) = 4 + \deg(\psi^4)$ et $-dea_\mu^2 = 16a_\psi^4$.

* Si $\deg(f\theta^2) = \deg(\psi^2) + 2$ et $ea_\theta^2 + 4a_\psi^2 \neq 0$, alors $\deg(f) = 2 + 2\deg(\psi) - 2\deg(\theta)$ et $-dea_\mu^2 = (ea_\theta^2 + a_\psi^2)^2$.

* Si $\deg(f\theta^2) = \deg(\psi^2) + 2$ et $(ea_\theta^2 + 4a_\psi^2) = 0$, alors $\deg(f)$ est encore pair et $e = -\left(\frac{2a_\psi}{a_\theta}\right)^2$.

On voit que f est toujours de degré pair, que dans les trois premiers cas $-de \in k^{*2}$ et que dans le dernier $-e \in k^{*2}$. □

Cas (C1) : Si d n'est pas un carré dans k

Les seuls points d'ordre fini connus sont les points d'ordre 2 et on doit donc montrer que l'image de $\hat{\gamma}_{\mathcal{D}}$ est l'image de ces points. On sait que :

* $\hat{\gamma}_{\mathcal{D}}(\mathcal{P}_{\mathcal{D}}) = (z+1-r)(z+1+r)k(z)^{*2}$,
* $\hat{\gamma}_{\mathcal{D}}(-4(z+1)^2, 0) = 4d(z+1)^2k(z)^{*2} = dk(z)^{*2}$,
* $\hat{\gamma}_{\mathcal{D}}(-4(z+1-r)(z+1+r), 0) = d(z+1-r)(z+1+r)k(z)^{*2}$.

On doit donc montrer que :

$$\hat{\gamma}_{\mathcal{D}}\left(\hat{\mathcal{D}}^{-d}_{k(z)}\right) = \Big\{k(z)^{*2}, dk(z)^{*2}, d(z+1-r)(z+1+r)k(z)^{*2}, \cdots$$
$$\cdots (z+1-r)(z+1+r)k(z)^{*2}\Big\}$$

Si (α, β) est un point de $\hat{\mathcal{D}}^{-d}_{k(z)}$ vérifiant $\beta \neq 0$, en écrivant $\alpha = f\frac{\theta^2}{\psi^2}$ avec les conditions énoncées ci-dessus, on sait, d'après le lemme 1.5.13, que f divise $a(z)b(z) = (z+1)^2(z+1+r)(z+1-r)$. Comme de plus f est sans facteur carré, on peut supposer que f divise $(z+1)(z+1+r)(z+1-r)$.

Proposition 2.3.4 *Si d n'est pas un carré dans k, alors on ne peut pas avoir $(z+1)$ comme facteur de f.*

Preuve. Si on suppose que $(z+1)$ divise f, alors on peut écrire $f = (z+1)P$, avec $P(-1) \neq 0$ car f est sans facteur carré. Comme on a, en conservant les notations du lemme 1.5.13, la relation :

$$-df\mu^2 = f^2\theta^4 + 4[2(z+1)^2 - r^2]f\theta^2\psi^2 + 16[(z+1)^2 - r^2](z+1)^2\psi^4,$$

cela donne avec $f = (z+1)P$ et après simplification par $(z+1)$:

$$-dP\mu^2 = (z+1)P^2\theta^4 + 4[2(z+1)^2 - r^2]P\theta^2\psi^2 + 16[(z+1)^2 - r^2](z+1)\psi^4.$$

Donc pour $z = -1$, on obtient $-dP(-1)\mu^2(-1) = -4r^2P(-1)\theta^2(-1)\psi^2(-1)$ c'est-à-dire $d\mu^2(-1) = 4r^2\theta^2(-1)\psi^2(-1)$.

Si on suppose que $\mu^2(-1) \neq 0$ alors $d = \left(\frac{2r\theta(-1)\psi(-1)}{\mu(-1)}\right)^2 \in k^{*2}$, or par hypothèse d n'est pas un carré dans k donc $\mu^2(-1) = 0$.

On en déduit que $-4r^2P(-1)\theta^2(-1)\psi^2(-1) = 0$, mais comme $f(-1) = 0$ et que ψ est premier avec f, alors $\psi^2(-1) \neq 0$ d'où $\theta^2(-1) = 0$ et $\theta = (z+1)\theta'$, avec $\theta' \in k[z]$. On a alors la relation :

$$-dP\mu^2 = (z+1)^5P^2\theta'^4 + 4[2(z+1)^2 - r^2](z+1)^2P\theta'^2\psi^2 + 16[(z+1)^2 - r^2](z+1)\psi^4.$$

Ainsi le polynôme irréductible $(z+1)$ divise $P\mu^2$ et est premier avec P, donc il divise μ et son carré $(z+1)^2$ divise donc les deux membres de l'égalité précédente, ce qui implique que $(z+1)$ divise aussi ψ contredisant l'hypothèse $\mathrm{pgcd}(\theta, \psi) = 1$. Cela prouve que, lorsque d n'est pas un carré dans k, le polynôme $(z+1)$ ne peut pas diviser f. □

On peut déduire de cette proposition que le polynôme f est de degré pair et divise $(z+1-r)(z+1+r)$, c'est-à-dire soit $f = e$, soit $f = e(z+1-r)(z+1+r)$, avec $e \in k^*$. Alors quitte à ajouter au point (α, β) le point $\mathcal{P}_\mathcal{D}$ (ou le point $\mathcal{P}_2 = (-4(z+1-r)(z+1+r), 0)$), on peut supposer que $f = e \in k^*$. Mais alors d'après le lemme 2.3.3, on a soit $-de \in k^{*2}$, soit $-e \in k^{*2}$.

* Si $-de \in k^{*2}$, alors $\hat{\gamma}_\mathcal{D}(\alpha, \beta) = -dek(z)^{*2} = k(z)^{*2}$ donc $(\alpha, \beta) \in \ker(\hat{\gamma}_\mathcal{D})$ le problème est résolu,

* Si $-e \in k^{*2}$, alors $\hat{\gamma}_\mathcal{D}(\alpha, \beta) = -dek(z)^{*2} = dk(z)^{*2} = \hat{\gamma}_\mathcal{D}(\mathcal{P}_1)$, on est encore dans l'image des points d'ordre 2.

Si d n'est pas un carré dans k, quitte à ajouter au point (α, β) un point d'ordre 2, l'image $\hat{\gamma}_\mathcal{D}(\alpha, \beta)$ est bien égale à celle d'un des points d'ordre 2, ce qui permet de terminer l'étude de $\hat{\mathcal{D}}^{-d}_{k(z)}$ dans le cas (C1).

Cas (C2) : Si d est un carré dans k

Dans ce cas, en plus des points d'ordre 2, il y a sur $\hat{\mathcal{D}}^{-d}_{k(z)}$ des points d'ordre 4 : $(-4(z+1)(z+1-r), \pm\frac{8}{\sqrt{d}}r(z+1)(z+1-r))$ et $(-4(z+1)(z+1+r), \pm\frac{8}{\sqrt{d}}r(z+1)(z+1+r))$. Leurs images par le morphisme $\hat{\gamma}_\mathcal{D}$ sont :

* $\hat{\gamma}_\mathcal{D}(\mathcal{P}_\mathcal{D}) = (z+1-r)(z+1+r)k(z)^{*2}$,

* $\hat{\gamma}_{\mathcal{D}}(\mathcal{P}_1) = dk(z)^{*2} = k(z)^{*2}$ (car d est un carré),

* $\hat{\gamma}_{\mathcal{D}}(\mathcal{P}_2) = (z+1-r)(z+1+r)k(z)^{*2} = \hat{\gamma}_{\mathcal{D}}(\mathcal{P}_{\mathcal{D}})$,

* $\hat{\gamma}_{\mathcal{D}}(-4(z+1)(z+1-r), \pm\frac{8}{\sqrt{d}}r(z+1)(z+1-r)) = (z+1)(z+1-r)k(z)^{*2}$,

* $\hat{\gamma}_{\mathcal{D}}(-4(z+1)(z+1+r), \pm\frac{8}{\sqrt{d}}r(z+1)(z+1+r)) = (z+1)(z+1+r)k(z)^{*2}$.

On doit donc montrer que :

$$\hat{\gamma}_{\mathcal{D}}\left(\hat{\mathcal{D}}^{-d}_{k(z)}\right) = \Big\{k(z)^{*2}, (z+1-r)(z+1+r)k(z)^{*2}, (z+1)(z+1-r)k(z)^{*2}, \cdots$$
$$\cdots (z+1)(z+1+r)k(z)^{*2}\Big\}.$$

Soit (α, β) un point de $\hat{\mathcal{D}}^{-d}_{k(z)}$ vérifiant $\beta \neq 0$, on écrit encore α sous la forme $f\frac{\theta^2}{\psi^2}$ avec les mêmes conditions et on sait, d'après les lemmes 1.5.13 et 2.3.3, que f divise $(z+1)(z+1+r)(z+1-r)$ et est de degré pair donc on a quatre possibilités : soit $f = e$, soit $f = e(z+1)(z+1+r)$, soit $f = e(z+1)(z+1-r)$, soit $f = e(z+1+r)(z+1-r)$ avec $e \in k^*$. Quitte à ajouter un des points d'ordre 2 ou 4, on peut supposer que $f = e$ et alors, encore grâce au lemme 2.3.3, on obtient que $-de \in k^{*2}$ ou $-e \in k^{*2}$.

* Si $-de \in k^{*2}$, alors il est évident que $\hat{\gamma}_{\mathcal{D}}(\alpha, \beta) = -dek(z)^{*2} = k(z)^{*2}$.

* Si $-e \in k^{*2}$, comme $d \in k^{*2}$ alors on a encore $-de \in k^{*2}$ et cela implique qu'on a toujours $\hat{\gamma}_{\mathcal{D}}(\alpha, \beta) = k(z)^{*2}$.

L'étude du cas (C2) est achevée car quitte à ajouter un des points d'ordre 2 ou 4, on a $(\alpha, \beta) \in \ker \hat{\gamma}_{\mathcal{D}}$.

On a donc montré que pour tout $d \in k^*$, que d soit un carré ou non dans k, l'image du morphisme $\hat{\gamma}_{\mathcal{D}}$ est toujours celle des points d'ordre 2.

(D) Etude de $\check{\mathcal{C}}^{-\mathbf{d}}_{\mathbf{k(z)}}$

On doit dans cette partie chercher des conditions suffisantes sur le réel r pour que l'image du morphisme $\check{\gamma}_{\mathcal{C}}$ soit celle des points d'ordre fini, c'est-à-dire triviale étant donné qu'on ne connait sur cette courbe qu'un seul point de torsion $(0,0)$ et que $\check{\gamma}_{\mathcal{C}}(0,0) = k(z)^{*2}$.

On rappelle que l'équation de la courbe $\check{\mathcal{C}}^{-d}_{k(z)}$ est $-d\beta^2 = \alpha(\alpha^2 - 2(2(z+1)^2 - r^2)z\alpha + r^4z^2)$. Si on considère un point (α, β) d'ordre infini sur cette courbe, alors il vérifie $\beta \neq 0$, en utilisant les notations de la proposition 1.5.13, on obtient l'équation :

$$-df\mu^2 = f^2\theta^4 - 2(2(z+1)^2 - r^2)zf\theta^2\psi^2 + r^4z^2\psi^4$$

Comme dans les cas déjà traités, f est sans facteur carré et divise r^4z^2 donc on a soit $f = e$, soit $f = ez$.

Cas (D1) : Si f = e

Dans ce cas, comme $\check{\gamma}_c(\alpha, \beta) = -dek(z)^{*2}$, il suffit de démontrer que $-de \in k^{*2}$, ce qui se fait comme pour $\hat{\mathcal{C}}^{-d}_{k(z)}$, en écrivant :

$$-de\mu^2 = (e\theta^2 - r^2z\psi^2)^2 - 4(z+1-r)(z+1+r)ze\theta^2\psi^2,$$

puis en spécialisant en $z = r-1$ (ou en $z = -r-1$), et alors $-de\mu^2(r-1) = (e\theta^2(r-1) - r^2(r-1)\psi^2(r-1))^2$ avec $(e\theta^2(r-1) - r^2(r-1)\psi^2(r-1))^2 \neq 0$ car θ et ψ sont premier entre eux (il suffit de refaire le même raisonnement que pour $\hat{\mathcal{C}}^{-d}_{k(z)}$). On a $-de \in k^{*2}$ et donc $\check{\gamma}_c(\alpha, \beta) = k(z)^{*2}$.

Cas (D2) : Si f = ez

Dans ce cas, $\check{\gamma}_c(\alpha, \beta) = -dezk^{*2}$, donc pour prouver que l'image de $\check{\gamma}_c$ est triviale, il faut démontrer que ce cas ne peut pas se produire et cela va amener à poser certaines conditions sur le nombre r.

On a, dans l'équation de $\check{\mathcal{C}}^{-d}_{k(z)}$, toujours avec les notations du lemme 1.5.13 :

$$-dez\mu^2 = (ez\theta^2 - r^2z\psi^2)^2 - 4(z+1-r)(z+1+r)z^2e\theta^2\psi^2.$$

Le polynôme z^2 doit donc diviser les deux membres de cette égalité, on en déduit que z divise μ et on peut poser $\mu = z\mu'$ avec $\mu' \in k[z]$. Après simplication par z^2, on a :

$$-dez\mu'^2 = (e\theta^2 - r^2\psi^2)^2 - 4(z+1-r)(z+1+r)e\theta^2\psi^2.$$

En posant $z = r-1$, il suffit de faire le même raisonnement que dans le cas (D1) pour obtenir que $-de(r-1)\mu'^2(r-1) = (e\theta^2(r-1) - r^2\psi^2(r-1))^2 \neq 0$ et

donc que $de(1-r) \sim 1$. De même pour $z = -r-1$, on a $-de(-r-1)\mu'^2(r-1) = (e\theta^2(-r-1)-r^2\psi^2(-r-1))^2 \neq 0$ donc $de(1+r) \sim 1$, on en déduit que $(1-r^2) \sim 1$.

Il apparaît donc que si $(1-r^2)$ n'est pas un carré dans k, le cas $f = ez$ ne peut pas se produire, cette condition est donc suffisante pour que l'image du morphisme $\check{\gamma}_c$ soit triviale.

On va maintenant s'intéresser au cas où $(1-r^2)$ est un carré dans k et d'après ce qui précède, on sait que $de \sim (1-r) \sim (1+r)$. On a aussi la relation suivante :

$$-dez\mu'^2 = (e\theta^2 + r^2\psi^2)^2 - 4(z+1)^2 e\theta^2\psi^2.$$

De plus pour $z = 0$, on obtient : $(e\theta(0)^2 + r^2\psi(0)^2)^2 - 4e\theta(0)^2\psi^2(0) = 0$ d'où $(e\theta^2(0) + r^2\psi^2(0))^2 = 4e\theta^2(0)\psi^2(0) \neq 0$, car si ce terme s'annulait, on aurait à la fois $\theta(0) = 0$ et $\psi(0) = 0$, ce qui est impossible puisque $\mathrm{pgcd}(\theta, \psi) = 1$. Le coefficient dominant e est donc un carré dans k et on peut alors supposer que $e = 1$, ce qui implique que $d \sim (1-r) \sim (1+r)$.

On obtient alors la relation $-dz\mu'^2 = (\theta^2 + r^2\psi^2)^2 - 4(z+1)^2\theta^2\psi^2$ et pour $z = -1$, on a $d\mu'^2(-1) = (\theta^2(-1) + r^2\psi^2(-1))^2$. Or $\theta^2(-1) + r^2\psi^2(-1)$ est un élément de $k = \mathbb{Q}(r)$ qui est un corps réel donc si $\theta^2(-1) + r^2\psi^2(-1) = 0$, on doit aussi avoir $\theta^2(-1) = \psi^2(-1) = 0$ ce qui est impossible étant donné que θ et ψ sont premiers entre eux. On ainsi $d\mu'^2(-1) = (\theta^2(-1) + r^2\psi^2(-1))^2 \neq 0$ d'où $d \sim 1$, ce qui donne $(1-r) \sim (1+r) \sim 1$.

Ainsi, lorsque $(1-r^2)$ est un carré dans k, il suffit de supposer que $(1-r)$, ou de manière équivalente $(1+r)$, n'est pas un carré dans k pour que le cas $f = ez$ ne puisse pas se produire et donc que l'image du morphisme $\check{\gamma}_c$ soit triviale.

Que se passe-t-il maintenant lorsque $(1-r)$ et $(1+r)$ sont des carrés dans le corps k?

On peut poser $(1+r) = \lambda^2$ et $(1-r) = \nu^2$ avec $\lambda, \nu \in k$ et on a alors $1 - r^2 = \lambda^2\nu^2$ et $r = \lambda^2 - 1 = 1 - \nu^2$, donc $k = \mathbb{Q}(r) = \mathbb{Q}(\lambda) = \mathbb{Q}(\nu)$. On sait aussi, d'après ce qui précède, que $d \sim 1$ et on a la relation :

$$\begin{aligned} -dz\mu'^2 &= (\theta^2 + r^2\psi^2)^2 - 4(z+1)^2\theta^2\psi^2 \\ &= (\theta^2 + r^2\psi^2 + 2(z+1)\theta\psi)(\theta^2 + r^2\psi^2 - 2(z+1)\theta\psi) \end{aligned}$$

Lemme 2.3.5 *Les polynômes $(\theta^2 + r^2\psi^2 - 2(z+1)\theta\psi)$ et $(\theta^2 + r^2\psi^2 + 2(z+1)\theta\psi)$ sont premiers entre eux.*

Preuve. Il suffit de remarquer que si P est un facteur premier commun à ces deux polynômes , alors P divise aussi leur différence $4(z+1)\theta\psi$ et leur somme $2(\theta^2+r^2\psi^2)$. Mais on a forcément $P \neq (z+1)$, car sinon on aurait $(\theta^2(-1)+r^2\psi^2(-1))=0$ et comme le corps k est inclu dans $\mathbb{R}$, on aurait aussi $\theta(-1)=\psi(-1)=0$, ce qui est impossible θ et ψ étant premiers entre eux. Donc P divise θ ou ψ, ainsi que $\theta^2+r^2\psi^2$, d'où P divise à la fois θ et ψ. Comme on a supposé que θ et ψ sont premiers entre eux, on a alors $P=1$. □

Le produit de ces deux polynômes $(\theta^2+r^2\psi^2-2(z+1)\theta\psi)$ et $(\theta^2+r^2\psi^2+2(z+1)\theta\psi)$ premiers entre eux est $-dz\mu'^2$ avec $d\sim 1$, il y a donc deux possibilités :

(i) Soit on a $\theta^2+r^2\psi^2+2(z+1)\theta\psi=-sz\mu_1^2$ et $\theta^2+r^2\psi^2-2(z+1)\theta\psi=s\mu_2^2$ pour un certain $s\in k^*$ et avec μ_1, $\mu_2\in k[z]^*$,

(ii) Soit on a $\theta^2+r^2\psi^2+2(z+1)\theta\psi=s\mu_1^2$ et $\theta^2+r^2\psi^2-2(z+1)\theta\psi=-sz\mu_2^2$ pour un certain $s\in k^*$ et avec μ_1, $\mu_2\in k[z]^*$.

(i) Etude de la première possibilité :

On a ici :

$$\begin{cases} \theta^2+r^2\psi^2+2(z+1)\theta\psi &= -sz\mu_1^2 \qquad (1)\\ \theta^2+r^2\psi^2-2(z+1)\theta\psi &= s\mu_2^2 \qquad (2)\end{cases}$$

Dans l'équation (1), pour $z=(r-1)$, on a $\theta^2(r-1)+r^2\psi^2(r-1)+2r\theta(r-1)\psi(r-1)=-s(r-1)\mu_1^2(r-1)$ c'est-à-dire $(\theta(r-1)+r\psi(r-1))^2=s(1-r)\mu_1^2(r-1)$ donc on obtient soit $(\theta(r-1)+r\psi(r-1))=0$ soit $s\sim(1-r)\sim 1$.

Dans l'équation(2), pour $z=(r-1)$, cela donne $\theta^2(r-1)+r^2\psi^2(r-1)-2r\theta(r-1)\psi(r-1)=s\mu_2^2(r-1)$ c'est-à-dire $(\theta(r-1)-r\psi(r-1))^2=s\mu_2^2(r-1)$, finalement soit $(\theta(r-1)-r\psi(r-1))=0$ soit $s\sim 1$.

Comme θ et ψ sont premiers entre eux, $(\theta(r-1)+r\psi(r-1))$ et $(\theta(r-1)-r\psi(r-1))$ ne peuvent pas s'annuler simultanément, on en déduit que $s\sim 1$.

Maintenant on pose $z=0$ dans (1) : $\theta^2(0)+r^2\psi^2(0)+2\theta(0)\psi(0)=0$ et $\psi(0)\neq 0$ car sinon θ et ψ s'annuleraient simultanément en 0. Donc si on pose $X=\frac{\theta(0)}{\psi(0)}$, on obtient l'équation : $X^2+2X+r^2=0$. Le discriminant du trinôme X^2+2X+r^2 est $4(1-r^2)=\lambda^2\nu^2$ et on obtient $X=-1\pm\lambda\nu$.

Ensuite pour $z=0$ dans (2), on a $\theta^2(0)+r^2\psi^2(0)-2\theta(0)\psi(0)=s\mu_2^2(0)$ avec $\mu_2^2(0)\neq 0$ car les polynômes $(\theta^2+r^2\psi^2-2(z+1)\theta\psi)$ et $(\theta^2+r^2\psi^2+2(z+1)\theta\psi)$ sont premiers entre eux et que l'on a déjà $\theta^2(0)+r^2\psi^2(0)+2\theta(0)\psi(0)=0$. Comme

$s \sim 1$, cela donne $\theta^2(0) + r^2\psi^2(0) - 2\theta(0)\psi(0) \sim 1$ et donc, en divisant par $\psi(0)^2$, on a $X^2 - 2X + r^2 \sim 1$ d'où :

* Si $X = -1 + \lambda\nu$, alors $X^2 - 2X + r^2 = 4(1 - \lambda\nu)$ et donc $(1 - \lambda\nu) \sim 1$.

* Si $X = -1 - \lambda\nu$, alors $X^2 - 2X + r^2 = 4(1 + \lambda\nu)$ et $(1 + \lambda\nu) \sim 1$.

Il faudra alors poser des conditions sur λ et ν, pour s'assurer que ni $(1 - \lambda\nu)$ ni $(1 + \lambda\nu)$ ne sont des carrés dans k.

(ii) Etude de la seconde possibilité :

On a le système d'équations :

$$\begin{cases} \theta^2 + r^2\psi^2 + 2(z+1)\theta\psi &= s\mu_1^2 & (3) \\ \theta^2 + r^2\psi^2 - 2(z+1)\theta\psi &= -sz\mu_2^2 & (4) \end{cases}$$

Dans (3) pour $z = (r-1)$, on obtient $(\theta(r-1) + r\psi(r-1))^2 = s\mu_1^2(r-1)$ donc on a soit $(\theta(r-1) + r\psi(r-1)) = 0$, soit $s \sim 1$.

Dans (4) pour $z = (r-1)$, on a $(\theta(r-1) - r\psi(r-1))^2 = s(1-r)\mu_2^2(r-1)$,avec $(1-r) \sim 1$. Finalement soit $(\theta(r-1) - r\psi(r-1)) = 0$ soit $s \sim 1$.

Et, ici encore, comme θ et ψ sont premiers entre eux, $(\theta(r-1) + r\psi(r-1))$ et $(\theta(r-1) - r\psi(r-1))$ ne peuvent pas s'annuler simultanément, on en déduit que $s \sim 1$.

On pose maintenant $z = 0$ dans l'équation(4) ce qui donne $\theta^2(0) + r^2\psi^2(0) - 2\theta(0)\psi(0) = 0$. Comme dans le cas précédent, $\psi(0) \neq 0$ et si on pose $X = \frac{\theta(0)}{\psi(0)}$, on obtient l'équation $X^2 - 2X + r^2 = 0$ d'où $X = 1 \pm \lambda\nu$.

Alors pour $z = 0$ dans (3), on obtient $\theta^2(0) + r^2\psi^2(0) + 2\theta(0)\psi(0) = s\mu_1^2(0)$ avec $\mu_1(0) \neq 0$ et $\psi(0) \neq 0$.

On a finalement $X^2 + 2X + r^2 = s\frac{\mu_1^2(0)}{\psi(0)^2} \sim 1$ car $s \sim 1$ et :

* Si $X = 1 + \lambda^2\nu^2$, alors $X^2 + 2X + r^2 = 4(1 + \lambda\nu)$ et donc $(1 - \lambda\nu) \sim 1$.

* Si $X = 1 - \lambda^2\nu^2$, alors $X^2 + 2X + r^2 = 4(1 - \lambda\nu)$ et $(1 + \lambda\nu) \sim 1$.

On retrouve les mêmes condition à exclure que dans le cas précédent : ni $(1 - \lambda\nu)$ ni $(1 + \lambda\nu)$ ne doivent être des carrés dans k.

On a donc trouvé différentes conditions suffisantes pour exclure le cas (D2) et ainsi faire en sorte que l'image du morphisme $\check{\gamma}_c$ soit triviale :

* *Il suffit que $(1 - r^2)$ ne soit pas un carré dans $k = \mathbb{Q}(r)$.*

* *Si* $(1-r^2)$ *est un carré dans* k*, il suffit de supposer que* $(1-r)$*, ou de manière équivalente* $(1+r)$*, n'est pas un carré dans* k*.*

* *Si* $(1-r)$ *et* $(1+r)$ *sont des carrés dans le corps* k*, on pose* $(1+r)=\lambda^2$ *et* $(1-r)=\nu^2$ *avec* λ*,* $\nu \in k$ *et alors on doit supposer que ni* $(1-\lambda\nu)$ *ni* $(1+\lambda\nu)$ *ne sont des carrés dans* k*.*

(E) Etude de $\check{\mathcal{D}}^{-\mathbf{d}}_{\mathbf{k(z)}}$

L'objectif de cette partie est de déterminer des conditions suffisantes sur le réel r pour que l'image du morphisme $\check{\gamma}_{\mathcal{D}}$ soit celle des points de torsion.

L'équation de la courbe $\check{\mathcal{D}}^{-d}$ est $-d\beta^2=\alpha(\alpha+4(z+1)^2z)(\alpha+4[(z+1)^2-r^2]z)$, avec les notations de la section 2.1, on a $a(z)=(z+1)^2z$ et $b(z)=((z+1)^2-r^2)z$, donc comme ni $a(z)$ ni $b(z)$ ne sont des carrés dans $\mathbb{C}(z)$, il n'y a pas de point d'ordre 4 sur $\check{\mathcal{D}}^{-d}_{k(z)}$ (ni sur $\check{\mathcal{C}}^{-d}_{k(z)}$). Les seuls points d'ordre finis connus sur cette courbe sont donc les points d'ordre 2 : $(0,0)$, $(-4(z+1)^2z,0)$ et $(-4[(z+1)^2-r^2]z,0)$. Les images de ces points par $\check{\gamma}_{\mathcal{D}}$ sont :

* $\check{\gamma}_{\mathcal{D}}(0,0)=[(z+1)^2-r^2]k(z)^{*2}$,

* $\check{\gamma}_{\mathcal{D}}(-4(z+1)^2z,0)=dzk(z)^{*2}$,

* $\check{\gamma}_{\mathcal{D}}(-4[(z+1)^2-r^2]z,0)=d[(z+1)^2-r^2]zk(z)^{*2}$

On doit donc montrer que :

$$\check{\gamma}_{\mathcal{D}}(\check{\mathcal{D}}^{-d}_{k(z)})=\left\{k(z)^{*2},[(z+1)^2-r^2]k(z)^{*2},dzk(z)^{*2},d[(z+1)^2-r^2]zk(z)^{*2}\right\}.$$

En utilisant les notations du lemme 1.5.13, si (α,β) est un point de $\hat{\mathcal{D}}^{-d}_{k(z)}$ vérifiant $\beta\neq 0$, on a, ici encore, $\alpha=f\frac{\theta^2}{\psi^2}$, avec f, θ, $\psi\in k[x]$, $\mathrm{pgcd}(f\theta,\psi)=1$ et f sans facteur carré divisant $16z^2(z+1)^2((z+1)^2-r^2)$. Le polynôme f divise donc $z(z+1)(z+1-r)(z+1+r)$.

Mais quitte à ajouter au point (α,β) l'un des point d'ordre deux, on peut supposer que ni z ni $(z+1+r)$ ne sont des facteurs de f qui va alors diviser $(z+1)(z+1-r)$. On doit ainsi étudier quatre cas :

* Cas (E1) : $f=e$, avec $e\in k^*$,

* Cas (E2) : $f = e(z+1)$, avec $e \in k^*$,

* Cas (E3) : $f = e(z+1-r)$, avec $e \in k^*$,

* Cas (E4) : $f = e(z+1)(z+1-r)$, avec $e \in k^*$.

Le lemme suivant reste vrai dans ces quatre cas et permet d'en faire l'étude :

Lemme 2.3.6 *D'après l'équation de $\check{\mathcal{D}}^{-d}_{k(z)}$, on a, en conservant les notations du lemme 1.5.13 et après simplification, $-df\mu^2 = (f\theta^2 + 4z(z+1)^2\psi^2)(f\theta^2 + 4z(z+1-r)(z+1+r)\psi^2)$ et de plus les polynômes $(f\theta^2 + 4z(z+1)^2\psi^2)$ et $(f\theta^2 + 4z(z+1-r)(z+1+r)\psi^2)$ sont soit premiers entre eux lorsque $\theta(0) \neq 0$, soit admettent z pour seul diviseur commun lorsque $\theta(0) = 0$.*

Preuve. Si P est un diviseur commun à ces deux polynômes, alors il divise leur différence $8r^2z\psi^2$. Mais P est premier avec ψ sinon $f\theta^2$ et ψ admettraient un facteur premier en commun, ce qui est exclu car $\mathrm{pgcd}(f\theta, \psi) = 1$, donc P divise z. Pour conclure, il suffit de remarquer que z ne divise $f\theta^2 + 4z(z+1)^2\psi^2$ et $f\theta^2 + 4z(z+1-r)(z+1+r)\psi^2$ que lorsque $\theta(0) = 0$. □

Cas (E1) : Si f = e

Puisque dans ce cas on a $\check{\gamma}_{\mathcal{D}}(\alpha, \beta) = -dek^{*2}$, il suffit de montrer que $-de \in k^{*2}$ c'est-à-dire que $-de \sim 1$, ce qui est évident car on a :

$$-de\mu^2 = (e\theta^2 + 4z(z+1)^2\psi^2)(e\theta^2 + 4z(z+1-r)(z+1+r)\psi^2)$$

et alors en notant a_θ, a_ψ et a_μ les coefficients dominants respectifs de θ, ψ et μ, cela donne :

* Si $\deg(\theta^2) > \deg(\psi^2) + 3$, $-dea_\mu^2 = e^2a_\theta^4$.

* Si $\deg(\theta^2) < \deg(\psi^2) + 3$, $-dea_\mu^2 = 16a_\psi^4$.

Dans les deux cas, on a bien $-de \sim 1$.

Cas (E2) : Si f = e(z + 1)

On va montrer que ce cas ne peut jamais se produire. La relation $-df\mu^2 = (f\theta^2 + 4z(z+1)^2\psi^2)(f\theta^2 + 4z(z+1-r)(z+1+r)\psi^2)$ devient après simplification par $z+1$:

$$-de\mu^2 = (e\theta^2 + 4z(z+1)\psi^2)(e(z+1)\theta^2 + 4z(z+1-r)(z+1+r)\psi^2)$$

Et on a deux possibilités à étudier suivant que θ s'annule ou non en 0.

(i) Si $\theta(0) \neq 0$:

Dans ce cas, d'après le lemme 2.3.6, les polynômes $e\theta^2 + 4z(z+1)\psi^2$ et $e(z+1)\theta^2 + 4z(z+1-r)(z+1+r)\psi^2$ sont premiers entre eux et leur produit est $-de\mu^2$, donc il existe $s \in k^*$, μ_1, $\mu_2 \in k[z]$ tels que :

$$\begin{cases} e\theta^2 + 4z(z+1)\psi^2 &= s\mu_1^2 & (1) \\ e(z+1)\theta^2 + 4z(z+1-r)(z+1+r)\psi^2 &= -des\mu_2^2 & (2) \end{cases}$$

Pour $z = 0$ dans (2), on a $e\theta^2(0) = -des\mu_2^2(0) \neq 0$ donc $e \sim -des$. Pour $z = -1$, dans (2), $4r^2\psi^2(-1) = -des\mu_2^2(-1)$, or $\psi(-1) \neq 0$ étant donné que $f = e(z-1)$ et que ψ est premier avec f donc on obtient que $-des \sim 1$. On en déduit en regroupant ces résultats que $-des \sim e \sim 1$.

Mais pour $z = -r-1$ dans l'équation (2), on a $-er\theta^2(-r-1) = -des\mu_2^2(-r-1)$. De plus on a $\theta^2(-r-1) \neq 0$ et $\mu_2^2(-r-1) \neq 0$, car si ces termes étaient nuls $(z+1+r)^2$ diviserait les deux membres de l'équation (2) et cela impliquerait que $(z+1+r)$ divise aussi ψ, ce qui est exclu car alors θ et ψ ne seraient pas premiers entre eux. On a donc $-er \sim -des$ et d'après ce qui précède, cela permet de dire que comme $e \sim 1$ et $-des \sim 1$, on a $-r \sim -er \sim -des \sim 1$.

Dans le corps réel $k = \mathbb{Q}(r)$, le nombre $-r$ serait donc un carré, ce qui est impossible, car on a supposé que $0 < r$. On ne peut donc pas avoir $\theta(0) \neq 0$ dans le cas (E2).

(ii) Si $\theta(0) = 0$:

Alors, d'après le lemme 2.3.6, les polynômes $e\theta^2 + 4z(z+1)\psi^2$ et $e(z+1)\theta^2 + 4z(z+1-r)(z+1+r)\psi^2$ admettent z pour pgcd, et on obtient, avec $s \in k^*$, μ_1, $\mu_2 \in k[z]$:

$$\begin{cases} e\theta^2 + 4z(z+1)\psi^2 &= sz\mu_1^2 \\ e(z+1)\theta^2 + 4z(z+1-r)(z+1+r)\psi^2 &= -desz\mu_2^2 \end{cases}$$

Et puisque $\theta(0) = 0$, on peut poser $\theta = z\theta'$ avec $\theta' \in k[z]$, ce qui donne :

$$\begin{cases} ez\theta'^2 + 4(z+1)\psi^2 &= s\mu_1^2 & (3) \\ ez(z+1)\theta'^2 + 4(z+1-r)(z+1+r)\psi^2 &= -des\mu_2^2 & (4) \end{cases}$$

Pour $z = 0$, dans (4), on a $4(1-r)(1+r)\psi^2(0) = -des\mu_2^2(0)$ avec $\psi(0) \neq 0$ car θ et ψ sont premiers entre eux, donc on a aussi $\mu_2^2(0) \neq 0$ d'où $-des \sim (1-r^2)$.

D'autre part pour $z = -1$ dans (4), on a $-4r^2\psi^2(-1) = -des\mu_2^2(-1)$ et les termes de cette égalité sont non nuls car $f = e(z-1)$ et ψ sont premiers entre eux, donc $-des \sim -1$.

En regroupant les résultat précédents, on devrait alors avoir $(1-r^2) \sim -1$, ce qui est impossible car $0 < r < 1$ et donc $(1-r^2) > 0$, ce ne peut donc pas être l'opposé d'un carré dans le corps k qui est réel. On ne peut donc pas avoir $\theta(0) = 0$ dans le cas (E2).

On a montré que le cas (E2) ne peut jamais se produire lorsque $0 < r < 1$*, il n'y a ici aucune condition à ajouter.*

Cas (E3) : Si f = e(z + 1 − r)

On va déterminer des conditions sur r permettant de rendre ce cas impossible.

La relation $-df\mu^2 = (f\theta^2 + 4z(z+1)^2\psi^2)(f\theta^2 + 4z(z+1-r)(z+1+r)\psi^2)$ donne ici, après simplification par $(z+1-r)$:

$$-de\mu^2 = (e(z+1-r)\theta^2 + 4z(z+1)^2\psi^2)(e\theta^2 + 4z(z+1+r)\psi^2)$$

Ici encore, il faut distinguer les cas $\theta(0) \neq 0$ et $\theta(0) = 0$. D'après le lemme 2.3.6 si $\theta(0) \neq 0$, les polynômes $(e(z+1-r)\theta^2 + 4z(z+1)^2\psi^2)$ et $(e\theta^2 + 4z(z+1+r)\psi^2)$ sont premiers entre eux et si $\theta(0) = 0$, leur seul facteur commun est z, cela donne :

(i) Si $\theta(0) \neq 0$:

$$\begin{cases} e(z+1-r)\theta^2 + 4z(z+1)^2\psi^2 &= s\mu_1^2 & (1) \\ e\theta^2 + 4z(z+1+r)\psi^2 &= -des\mu_2^2 & (2) \end{cases}$$

Dans l'équation (1), pour $z = 0$ on a $e(1-r)\theta^2(0) = s\mu_1^2(0) \neq 0$, donc $e(1-r) \sim s$. Dans (1), pour $z = -(1-r)$, on obtient $-4(1-r)r^2\psi^2(r-1) = s\mu_1^2(r-1)$ et $\psi(r-1) \neq 0$ car ψ est premier avec $f = e(z+1-r)$, d'où $(r-1) \sim s$. On en déduit que $e(1-r) \sim (r-1)$ d'où $e \sim -1$.

Pour $z=-1$ dans (1), on $-er\theta^2(-1)=s\mu_1^2(-1)$. Si on suppose que $\theta(-1)\neq 0$ cela implique que $s\sim -er$, et comme $s\sim e(1-r)$ cela donne $-er\sim e(1-r)$ d'où $r\sim(r-1)$, ce qui est impossible car $r>0$ et $r-1<0$. On doit donc avoir $\theta(-1)=0$.

Ainsi pour $z=-1$ dans (2), on obtient $-4r\psi^2(-1)=-des\mu_2^2(-1)$. Comme θ et ψ sont premiers entre eux et que $\theta(-1)=0$, alors $\psi(-1)\neq 0$ donc $-des\sim -r$. D'autre part pour $z=0$ dans (2), $e\theta^2(0)=-des\mu_2^2(0)\neq 0$, donc $-des\sim e$. On a alors $-r\sim -des\sim e\sim -1$ et $r\sim 1$.

Il suffira de supposer que r n'est pas un carré dans $k=\mathbb{Q}(r)$ pour obtenir une contradiction permettant d'exclure la possibilité $\theta(0)\neq 0$ dans le cas (E3).

(ii) Si $\theta(0)=0$:

$$\left\{\begin{array}{rcl} e(z+1-r)\theta^2+4z(z+1)^2\psi^2 &=& sz\mu_1^2 \\ e\theta^2+4z(z+1+r)\psi^2 &=& -desz\mu_2^2 \end{array}\right.$$

Et en posant $\theta=z\theta'$ avec $\theta'\in k[z]$ et en simplifiant par z :

$$\left\{\begin{array}{rcll} ez(z+1-r)\theta'^2+4(z+1)^2\psi^2 &=& s\mu_1^2 & (3) \\ ez\theta'^2+4(z+1+r)\psi^2 &=& -des\mu_2^2 & (4) \end{array}\right.$$

On a alors, dans l'équation (4), pour $z=0$, $4(1+r)\psi^2(0)=-des\mu_2^2(0)$ et $\psi^2(0)\neq 0$ car $\theta(0)=0$, donc $-des\sim(1+r)$. Toujours dans l'équation (4), pour $z=-(1+r)$, on a $-e(1+r)\theta'^2(-1-r)=-des\mu_2^2(-1-r)$ et $\theta'(-1-r)\neq 0$ sinon on obtiendrait que $(z+1+r)$ divise à la fois θ et ψ, donc $-des\sim -e(1+r)$. On a ainsi $(1+r)\sim -e(1+r)$ c'est-à-dire $e\sim -1$.

Dans (3), pour $z=0$, on a $4\psi^2(0)=s\mu_1^2(0)$ avec $\psi(0)\neq 0$ donc $s\sim 1$. Pour $z=-1$ dans la même équation, on obtient $er\theta'^2(-1)=s\mu_1^2(-1)$. Si on suppose que $\theta'(-1)\neq 0$, alors $s\sim er$ et comme $s\sim 1$ et $e\sim -1$, on aurait $r\sim -1$, ce qui est exclu car $r>0$ et le corps k est réel. On a donc $\theta'(-1)=0$.

Alors dans (4), pour $z=-1$, on a $4r\psi^2(-1)=-des\mu_2^2(-1)$ et $\psi(-1)\neq 0$ car θ et ψ sont premiers entre eux, donc $-des\sim r$. Or on sait déjà que $-des\sim(1+r)$, donc $r\sim(1+r)$ ou encore $r(1+r)\sim 1$.

Il suffit donc de supposer que $r(1+r)$ n'est pas un carré dans $k=\mathbb{Q}(r)$ pour qu'il ne soit plus possible d'avoir $\theta(0)=0$ dans le cas (E3).

On a donc terminé l'étude du cas (E3) :

Sous les hypothèses que ni r ni $r(1+r)$ ne sont des carrés dans k, on ne peut pas avoir $f=e(z+1-r)$.

Cas (E4) : Si $\mathbf{f = e(z+1)(z+1-r)}$

On va rechercher les conditions sur r permettant d'exclure ce cas. La relation $-df\mu^2 = (f\theta^2 + 4z(z+1)^2\psi^2)(f\theta^2 + 4z(z+1-r)(z+1+r)\psi^2)$ donne, après simplification par $(z+1)(z+1-r)$:

$$-de\mu^2 = (e(z+1-r)\theta^2 + 4z(z+1)\psi^2)(e(z+1)\theta^2 + 4z(z+1+r)\psi^2).$$

On a toujours deux possibilités suivant que θ s'annule ou non en 0 :

(i) Si $\theta(0) \neq 0$:

Alors les polynômes $(e(z+1-r)\theta^2+4z(z+1)\psi^2)$ et $(e(z+1)\theta^2+4z(z+1-r)\psi^2)$ sont premiers entre eux et donc :

$$\begin{cases} e(z+1-r)\theta^2 + 4z(z+1)\psi^2 &= s\mu_1^2 & (1) \\ e(z+1)\theta^2 + 4z(z+1+r)\psi^2 &= -des\mu_2^2 & (2) \end{cases}$$

Dans (1), pour $z = 0$, on a $e(1-r)\theta^2(0) = s\mu_1^2(0) \neq 0$ donc $s \sim e(1-r)$. Toujours dans (1), pour $z = -1$, $-er\theta^2(-1) = s\mu_1^2(-1)$ et ces termes ne sont pas nuls car sinon $(z+1)^2$ diviserait les deux membres de l'égalité (1) et on aurait $(z+1)$ comme facteur commun à θ et à ψ, ce qui est impossible. On a donc $s \sim -er$, ce qui donne $e(1-r) \sim -er$ c'est-à-dire $(1-r) \sim -r$. Mais comme $r > 0$ et $1-r > 0$ et que le corps k est réel, on ne peut pas avoir $(1-r) \sim -r$ donc il est impossible que $\theta(0) \neq 0$ dans le cas (E4).

(ii) Si $\theta(0) = 0$:

Le pgcd des polynômes $(e(z+1-r)\theta^2 + 4z(z+1)\psi^2)$ et $(e(z+1)\theta^2 + 4z(z+1-r)\psi^2)$ est alors z et en posant $\theta = z\theta'$ avec $\theta' \in k[z]$, on a :

$$\begin{cases} ez(z+1-r)\theta'^2 + 4(z+1)\psi^2 &= s\mu_1^2 & (3) \\ ez(z+1)\theta'^2 + 4(z+1+r)\psi^2 &= -des\mu_2^2 & (4) \end{cases}$$

Dans l'équation (3), pour $z = 0$, on a $4\psi^2(0) = s\mu_1^2(0)$ et $\psi(0) \neq 0$ donc $s \sim 1$. Pour $z = r-1$ dans cette même équation, on obtient $4r\psi^2(r-1) = s\mu_1^2(r-1)$ et comme ψ est premier avec $f = e(z+1)(z+1-r)$ alors $\psi(r-1) \neq 0$, donc $s \sim r$ et on obtient finalement que $r \sim 1$.

Donc en supposant que r n'est pas un carré dans k, on peut exclure le cas $f = e(z+1)(z+1-r)$.

On peut donc conclure la partie (E) car on obtenu des conditions suffisantes sur le réel r pour que l'image du morphisme $\check{\gamma}_D$ soit celle des points de torsion :

Pour cela il suffit de supposer que ni r, ni $r(r+1)$ ne sont des carrés dans le corps $k = \mathbb{Q}(r)$.

(F) Synthèse des résultats

Plusieurs conditions sur le nombre r sont apparues dans les parties précédentes pour que les images des morphismes $\hat{\gamma}_{\mathcal{C}}$, $\hat{\gamma}_{\mathcal{D}}$, $\check{\gamma}_{\mathcal{C}}$ et $\check{\gamma}_{\mathcal{D}}$ soient les images des points de torsion : il faut que ni r ni $r(r+1)$ ne soient des carrés dans $\mathbb{Q}(r)$ et que de plus :

* Soit $(1-r^2)$ ne soit pas un carré dans $\mathbb{Q}(r)$.
* Soit, quand $(1-r^2)$ est un carré dans $\mathbb{Q}(r)$, $(1-r)$, ou de manière équivalente $(1+r)$, ne soit un carré dans $\mathbb{Q}(r)$.
* Soit, quand $(1+r) = \lambda^2$ et $(1-r) = \nu^2$ avec $\lambda, \nu \in \mathbb{Q}(r)$, ni $(1-\lambda\nu)$ ni $(1+\lambda\nu)$ ne soient des carrés dans $\mathbb{Q}(r)$.

On va ici chercher à exprimer plus simplement cette dernière condition :

Lemme 2.3.7 *Lorsque $(1+r) = \lambda^2$ et $(1-r) = \nu^2$ avec $\lambda, \nu \in \mathbb{Q}(r)$, la condition : "ni $(1-\lambda\nu)$ ni $(1+\lambda\nu)$ ne sont des carrés dans $\mathbb{Q}(r)$ équivaut à : 2 n'est pas un carré dans $\mathbb{Q}(r)$.*

Preuve. Puisque $(1+r) = \lambda^2$ et $(1-r) = \nu^2$, alors $\lambda^2 + \nu^2 = 2$, on pose alors $c = \frac{\lambda+\nu}{2}$ et $s = \frac{\lambda-\nu}{2}$, on a clairement $c \in \mathbb{Q}(r)$ et $s \in \mathbb{Q}(r)$. De plus on a aussi $c^2 + s^2 = \frac{1}{4}\left((\lambda+\nu)^2 + (\lambda-\nu)^2\right) = \frac{\lambda^2+\nu^2}{2} = 1$.

On exprime maintenant λ et ν en fonction de c et de s, cela donne $\lambda = c+s$ et $\nu = c-s$, on obtient donc :

* $(1+\lambda\nu) = 1 + (c+s)(c-s) = 1 + c^2 - s^2 = 2c^2$,
* $(1-\lambda\nu) = 1 - (c+s)(c-s) = 1 - c^2 + s^2 = 2s^2$,

on voit alors que $(1+\lambda\nu)$ et $(1-\lambda\nu)$ sont des carrés dans $\mathbb{Q}(r)$ si et seulement si 2 est un carré dans $\mathbb{Q}(r)$. □

On peut maintenant regrouper les résultats obtenus et énoncer le principal théorème de cette section :

Théorème 2.3.8 *Soit r un nombre réel tel que $0 < r < 1$, alors le polynôme strictement positif $F(x,y) = (y^2 + (x^2+1)^2)(y^2 + (x^2+1)^2 - r^2)$ n'est pas une somme de 3 carrés dans $\mathbb{R}(x,y)$ si les deux conditions suivantes sont vérifiées :*

(1) ni r, ni $r(r+1)$ ne sont des carrés dans le corps $\mathbb{Q}(r)$

(2) soit $(1-r^2)$, soit $1+r$, soit $1-r$, soit 2 n'est pas un carré dans le corps $\mathbb{Q}(r)$.

Preuve. Sous ces conditions, les images des morphismes $\hat{\gamma}_{\mathcal{C}}$, $\hat{\gamma}_{\mathcal{D}}$, $\check{\gamma}_{\mathcal{C}}$ et $\check{\gamma}_{\mathcal{D}}$ sont les images des points de torsion donc la courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ est de rang nul. On a vu à la partie (A) qu'aucun des points de torsion n'est spécial, donc cette courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ n'a pas de point spécial, ce qui prouve que le polynôme F auquel elle est associée n'est pas une somme de 3 carrés dans $\mathbb{R}(x,y)$. □

On peut alors remarquer deux cas particuliers simples qui démontrent le théorème 2.3.1 :

Corollaire 2.3.9 *Soit r un nombre réel transcendant tel que $0 < r < 1$, alors le polynôme $F(x,y) = (y^2 + (x^2+1)^2)(y^2 + (x^2+1)^2 - r^2)$ est strictement positif mais n'est pas une somme de 3 carrés dans $\mathbb{R}(x,y)$.*

Preuve. Comme r est transcendant, il est évident que ni r, ni $r(r+1)$, ni $(1-r^2)$ ne sont des carrés dans le corps $\mathbb{Q}(r)$. □

Corollaire 2.3.10 *Soit r un nombre rationnel tel que $0 < r < 1$ et ni r, ni $r(r+1)$ ne sont des carrés dans $\mathbb{Q}$, alors le polynôme $F(x,y) = (y^2 + (x^2+1)^2)(y^2 + (x^2+1)^2 - r^2)$ est strictement positif mais n'est pas une somme de 3 carrés dans $\mathbb{R}(x,y)$.*

Preuve. Il suffit de remarquer que 2 n'est pas un carré dans $\mathbb{Q}$ pour voir que la condition *(2)* du théorème 2.3.8 est toujours vérifiée dans ce cas. □

2.4 Etude du cas limite $r = 1$

L'objectif de cette section est démontrer le théorème suivant :

Théorème 2.4.1 *Le polynôme $F(x,y) = (y^2 + (x^2+1)^2)(y^2 + (x^2+1)^2 - 1)$ est non négatif mais n'est pas une somme de 3 carrés dans $\mathbb{R}(x,y)$.*

La démonstration de ce résultat est très proche de celle du théorème 2.3.8 effectuée à la section 2.3 (et où $0 < r < 1$), mais elle présente toutefois quelques spécificités concernant certains cas.

Ici encore, il faut prouver que la courbe elliptique $\mathcal{C}^{-1} : -\beta^2 = \alpha(\alpha^2 - 2(2(x^2+1)^2 - 1)\alpha + 1)$ n'a pas de point spécial, et comme le polynôme F est pair relativement à x, on peut se ramener à l'étude des points des quatre courbes :

* $\hat{\mathcal{C}}^{-d} : -d\beta^2 = \alpha(\alpha^2 - 2(2(z+1)^2 - 1)\alpha + 1)$,
* $\hat{\mathcal{D}}^{-d} : -d\beta^2 = \alpha(\alpha + 4(z+1)^2)(\alpha + 4[(z+1)^2 - 1])$,
* $\check{\mathcal{C}}^{-d} : -d\beta^2 = \alpha(\alpha^2 - 2(2(z+1)^2 - 1)z\alpha + z^2)$,
* $\check{\mathcal{D}}^{-d} : -d\beta^2 = \alpha(\alpha + 4(z+1)^2 z)(\alpha + 4[(z+1)^2 - 1]z)$.

Cette étude devra se faire sur le corps $k(z)$ et pour $d \in k^*$, où k est, comme dans le cas $0 < r < 1$, le corps $\mathbb{Q}(r)$ c'est-à-dire $k = \mathbb{Q}$. Les démonstrations effectuées dans la section précédente pour l'étude des points $\mathbb{R}(x)$-rationnels d'ordre 2^n de $\mathcal{C}^{-1}$ (partie (A)), l'étude de $\hat{\mathcal{C}}^{-d}_{k(z)}$ (partie (B)) et l'étude de $\hat{\mathcal{D}}^{-d}_{k(z)}$ (partie (C)) restent vraies lorsque $r = 1$, on se contentera donc ici de remanier les parties (D) et (E).

(D') Etude de $\check{\mathcal{C}}^{-d}_{\mathbb{Q}(z)}$

On va démontrer que l'image de $\check{\gamma}_c$ est l'image des points d'ordre fini. Comme dans le cas où $0 < r < 1$, on ne connait qu'un seul point de torsion sur cette courbe et il s'agit de $(0,0)$ qui vérifie $\check{\gamma}_c(0,0) = \mathbb{Q}(z)^{*2}$, on doit donc prouver que l'image du morphisme $\check{\gamma}_c$ est triviale.

L'équation de $\check{\mathcal{C}}^{-d}_{\mathbb{Q}(z)}$ étant $-d\beta^2 = \alpha(\alpha^2 - 2(2(z+1)^2 - 1)z\alpha + z^2)$, si on a un point (α, β) tel que $\beta \neq 0$ sur cette courbe, en utilisant les notations du lemme 1.5.13, on obtient l'équation :

$$-df\mu^2 = f^2\theta^4 - 2(2(z+1)^2 - 1)zf\theta^2\psi^2 + z^2\psi^4.$$

Puisque f est sans facteur carré, il divise z^2 donc soit $f = e$, soit $f = ez$, avec $e \in k^*$.

Cas (D'1) : Si f = e

Dans ce cas, il faut démontrer que $-de \in \mathbb{Q}^{*2}$, on peut effectuer un raisonnement similaire à celui employé quand $0 < r < 1$. On part de la relation :

$$-de\mu^2 = (e\theta^2 - z\psi^2)^2 - 4(z+2)z^2e\theta^2\psi^2,$$

puis en spécialisant en $z = -2$, on obtient $-de\mu^2(-2) = (e\theta^2(-2) + 2\psi^2(-2))^2$ avec $(e\theta^2(-2) + 2\psi^2(-2)) \neq 0$ car sinon $(z+2)$ divise à la fois θ et ψ or ces polynômes sont toujours premiers entre eux. On obtient donc bien $-de \in \mathbb{Q}^{*2}$.

Cette spécialisation en $z = -2$ correspond à la spécialisation en $z = -r - 1$ dans le cas $0 < r < 1$, la différence avec ce cas est qu'ici la spécialisation en $z = r - 1 = 0$ ne permet plus comme auparavant de conclure directement car on peut avoir $e\theta^2(0) + 2\psi^2(0) = 0$, la configuration est donc légèrement différente.

Cas (D'2) : Si f = ez

On doit démontrer que ce cas ne peut pas se produire. L'équation de $\check{\mathcal{C}}^{-d}_{\mathbb{Q}(z)}$, donne, toujours avec les mêmes notations la relation :

$$-dez\mu^2 = (ez\theta^2 - z\psi^2)^2 - 4z^3(z+2)e\theta^2\psi^2.$$

Cela implique que z divise μ, après avoir posé $\mu = z\mu'$, $\mu' \in k[z]$, et simplifié par z^2, on a :

$$-dez\mu'^2 = (e\theta^2 - \psi^2)^2 - 4z(z+2)e\theta^2\psi^2 \quad (1).$$

D'autre part, on a aussi l'égalité :

$$-dez\mu'^2 = (e\theta^2 + \psi^2)^2 - 4(z+1)^2e\theta^2\psi^2 \quad (2).$$

Pour $z = -2$ dans (1), on obtient $2de\mu'^2(-2) = (e\theta^2 - \psi^2)^2(-2)$ et on a encore $(e\theta^2 - r^2\psi^2)^2(-2) \neq 0$, l'argument le justifiant est le même que dans le cas (D'1). On obtient donc $2de \sim 1$.

Pour $z = -1$ dans (2), on a $de\mu'^2(-1) = (e\theta^2(-1) + \psi^2(-1))^2$. Si on suppose que $e\theta^2(-1) + \psi^2(-1) \neq 0$, on obtient $de \sim 1$, et comme on a montré auparavant que $2de \sim 1$, on aurait $2 \sim 1$, ce qui est impossible car 2 n'est pas un carré dans $\mathbb{Q}$. On a donc forcément $(e\theta^2(-1) + \psi^2(-1)) = 0$, ce qui implique que $e\theta^2(-1) = -\psi^2(-1)$. Les polynômes θ et ψ étant premiers entre eux, ils ne peuvent pas

s'annuler simultanément en -1, les deux termes de l'égalité précédente sont donc non nuls, d'où $e \sim -1$.

Pour conclure, on pose $z = 0$ dans (1) et on a $(e\theta^2(0) - \psi^2(0))^2 = 0$ d'où, comme θ et ψ sont premiers entre eux et qu'ils ne peuvent donc pas s'annuler simultanément en 0, $e\theta^2(0) = \psi^2(0) \neq 0$ et $e \sim 1$. En regroupant les résultats précédents, on obtient $1 \sim -1$ dans le corps $\mathbb{Q}$, c'est la contradiction recherchée.

Le cas (D'2) ne peut pas se produire et l'étude de $\check{\mathcal{C}}^{-d}_{\mathbb{Q}(z)}$ est achevée : on a prouvé que l'image du morphisme $\check{\gamma}_{\mathcal{C}}$ est triviale.

(E') Etude de $\check{\mathcal{D}}^{-\mathbf{d}}_{\mathbb{Q}(\mathbf{z})}$

On doit montrer que l'image du morphisme $\check{\gamma}_{\mathcal{D}}$ est l'image des points de torsion. L'équation de la courbe $\check{\mathcal{D}}^{-d}$ est $-d\beta^2 = \alpha(\alpha+4(z+1)^2z)(\alpha+4[(z+1)^2-1]z)$, c'est-à-dire de la forme $-d\beta^2 = \alpha(\alpha+4a(z))(\alpha+4b(z))$, avec $a(z) = (z+1)^2z$ et $b(z) = ((z+1)^2-1)z = (z+2)z^2$. Comme ni $a(z)$ ni $b(z)$ ne sont des carrés dans $\mathbb{Q}(z)$, il n'y a pas de point d'ordre 4 sur $\check{\mathcal{D}}^{-d}_{\mathbb{Q}(z)}$. Les seuls points d'ordre finis connus sur cette courbe sont donc les points d'ordre 2 : $(0,0)$, $(-4(z+1)^2z, 0)$ et $(-4(z+2)z^2, 0)$ et leurs images par $\check{\gamma}_{\mathcal{D}}$ sont :

* $\check{\gamma}_{\mathcal{D}}(0,0) = z(z+2)\mathbb{Q}(z)^{*2}$,
* $\check{\gamma}_{\mathcal{D}}(-4(z+1)^2z, 0) = dz\mathbb{Q}(z)^{*2}$
* $\check{\gamma}_{\mathcal{D}}(-4(z+2)z^2, 0) = d(z+2)\mathbb{Q}(z)^{*2}$.

On doit donc montrer que :

$$\check{\gamma}_{\mathcal{D}}(\check{\mathcal{D}}^{-d}_{\mathbb{Q}(z)}) = \left\{\mathbb{Q}(z)^{*2}, z(z+2)\mathbb{Q}(z)^{*2}, dz\mathbb{Q}(z)^{*2}, d(z+2)\mathbb{Q}(z)^{*2}\right\}.$$

On utilise encore les notations du lemme 1.5.13, si (α, β) est un point de $\hat{\mathcal{D}}^{-d}_{\mathbb{Q}(z)}$ vérifiant $\beta \neq 0$, on pose $\alpha = f\frac{\theta^2}{\psi^2}$, avec f sans facteur carré divisant $z(z+1)(z+2)$. Quitte à ajouter au point (α, β) un des points d'ordre 2, on peut supposer que ni z ni $(z+2)$ ne sont des facteurs de f qui va donc diviser $(z+1)$. Il ne reste ici que deux cas à étudier (contre quatre lorsque $0 < r < 1$) :

* Si $f = e$: Il faut alors montrer que $-de \in k^{*2}$ c'est-à-dire $-de \sim 1$.
* Si $f = e(z+1)$: on doit prouver que ce cas est impossible.

Cas (E'1) : Si f = e

Il suffit ici de reprendre la démonstration faite pour $0 < r < 1$ à la section 2.3 partie (E1), pour montrer que $-de \in \mathbb{Q}^{*2}$: En étudiant les coefficients dominants dans l'équation $-de\mu^2 = (e\theta^2 + 4z(z+1)^2\psi^2)(e\theta^2 + 4(z+2)z^2\psi^2)$, on montre qu'on a toujours $-de \sim 1$, ce qui est le résultat recherché.

Cas (E'2) : Si f = e(z + 1)

Partant de la relation $-df\mu^2 = (f\theta^2 + 4z(z+1)^2\psi^2)(f\theta^2 + 4(z+2)z^2\psi^2)$, en simplifiant par $(z+1)$ on a :

$$-de\mu^2 = (e\theta^2 + 4z(z+1)\psi^2)(e(z+1)\theta^2 + 4(z+2)z^2\psi^2)$$

On a aussi un résultat analogue au lemme 2.3.6 :

Lemme 2.4.2 *Dans l'équation de $\check{\mathcal{D}}^{-d}_{\mathbb{Q}(z)}$, on a avec les notations du lemme 1.5.13 et après simplification, $-df\mu^2 = (f\theta^2 + 4z(z+1)^2\psi^2)(f\theta^2 + 4(z+2)z^2\psi^2)$ et les polynômes $(f\theta^2+4z(z+1)^2\psi^2)$ et $(f\theta^2+4(z+2)z^2\psi^2)$ sont soit premiers entre eux lorsque $\theta(0) \neq 0$, soit admettent z pour seul diviseur commun lorsque $\theta(0) = 0$.*

Par conséquent, ici les polynômes $(e\theta^2 + 4z(z+1)\psi^2)$ et $(e(z+1)\theta^2 + 4(z+2)z^2\psi^2)$ vérifient aussi cette propriété, donc on a deux possibilités suivant que le polynôme θ s'annule ou non en 0.

(i) Si $\theta(0) \neq 0$:

Alors les polynômes $e\theta^2+4z(z+1)\psi^2$ et $e(z+1)\theta^2+4(z+2)z^2\psi^2$ sont premiers entre eux et leur produit est $-de\mu^2$, donc il existe $s \in \mathbb{Q}^*$, μ_1, $\mu_2 \in \mathbb{Q}[z]$ tels que :

$$\begin{cases} e\theta^2 + 4z(z+1)\psi^2 &= s\mu_1^2 & (1) \\ e(z+1)\theta^2 + 4(z+2)z^2\psi^2 &= -des\mu_2^2 & (2) \end{cases}$$

Pour $z = 0$ dans (2), on a $e\theta^2(0) = -des\mu_2^2(0) \neq 0$ donc $-des \sim e$. Pour $z = -2$ dans (2), on a $-e\theta^2(-2) = -des\mu_2^2(-2)$, or $\theta(-2) \neq 0$ sinon $(z+2)^2$ doit diviser les deux membres de l'égalité (2) et on en déduirait qu'il divise à la fois θ et ψ que l'on a supposés premiers entre eux, on a donc $-des \sim -e$.

On obtient ainsi $e \sim -e$ ce qui est impossible car on travaille dans le corps $\mathbb{Q}$. Lorsque $f = e(z+1)$, on ne peut pas avoir $\theta(0) \neq 0$.

(ii) Si $\theta(0) = 0$:

Dans ce cas les polynômes $e\theta^2 + 4z(z+1)\psi^2$ et $e(z+1)\theta^2 + 4(z+2)z^2\psi^2$ admettent z pour pgcd, et il existe $s \in \mathbb{Q}^*$, μ_1, $\mu_2 \in \mathbb{Q}[z]$ tels que :

$$\left\{ \begin{array}{rcl} e\theta^2 + 4z(z+1)\psi^2 & = & sz\mu_1^2 \\ e(z+1)\theta'^2 + 4(z+2)z^2\psi^2 & = & -desz\mu_2^2 \end{array} \right.$$

En posant $\theta = z\theta'$, avec $\theta' \in k[z]$ et après simplification par z, on obtient :

$$\left\{ \begin{array}{rcll} ez\theta'^2 + 4(z+1)\psi^2 & = & s\mu_1^2 & (3) \\ ez(z+1)\theta'^2 + 4z(z+2)\psi^2 & = & -des\mu_2^2 & (4) \end{array} \right.$$

Dans (3), pour $z = 0$, on a $4\psi^2(0) = s\mu_1^2(0)$, avec $\psi(0) \neq 0$ car $\theta(0) = 0$, donc $s \sim 1$. Pour $z = -1$, toujours dans (3), on a $-e\theta'^2(-1) = s\mu_1^2(-1)$, et $\theta'(-1) \neq 0$ sinon $(z+1)$ diviserait à la fois θ' et ψ, donc $s \sim -e$. On a alors $e \sim -s \sim -1$.

Puis d'une part, pour $z = -1$, dans (4), on a $-4\psi^2(-1) = -des\mu_2^2(-1)$ et $\psi(-1) \neq 0$ car $f = e(x+1)$ et ψ sont premiers entre eux, donc $des \sim 1$.

D'autre part pour $z = -2$ dans (4), on a $2e\theta'^2(-2) = -des\mu_2^2(-2)$ et $\theta'(-2) \neq 0$ sinon $(z+2)$ diviserait à la fois θ' et ψ, d'où $des \sim -2e$, or on sait déjà que $e \sim -1$, donc $des \sim 2$.

On devrait alors avoir à la fois $des \sim 1$ et $des \sim 2$ et donc $2 \sim 1$, ce qui est impossible car 2 n'est pas un carré dans $\mathbb{Q}$. Lorsque $f = e(z+1)$, on ne peut pas non plus avoir $\theta(0) = 0$ ce qui fait qu'on n'a jamais $f = e(z+1)$.

Le cas (E'2) ne pouvant pas se produire, on a donc prouvé que quitte à ajouter au point (α, β) un des point d'ordre deux, on a $\check{\gamma}_{\mathcal{D}}(\alpha, \beta) = \mathbb{Q}(z)^{*2}$. Cela montre que l'image du morphisme $\check{\gamma}_{\mathcal{D}}$ est effectivement l'image des points d'ordre fini.

Conclusion

On a donc montré que les images des morphismes $\hat{\gamma}_{\mathcal{C}}$, $\hat{\gamma}_{\mathcal{D}}$, $\check{\gamma}_{\mathcal{C}}$ et $\check{\gamma}_{\mathcal{D}}$ sont les images des points de torsion et on peut conclure que la courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ est de rang nul. Comme les points d'ordre fini de cette courbe ne sont pas spéciaux, elle n'a donc aucun point spécial et on en déduit le théorème 2.4.1.

2.5 Un exemple où la fibration sur la droite projective n'a pas de singularité réelle.

On va étudier ici des polynômes $F(x, y) = (y^2 + a(x))(y^2 + b(x))$ avec $a(x) = (x^2+2)^2$ et $b(x) = (x^2+2)^2 - r^2(x^2+1)^2$ pour $0 < r < 1$. L'intérêt de ces exemples

est de prouver que pour certaines valeurs de r, il n'y a pas de point spécial, ni même de point d'ordre infini sur la courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ associée, alors que la fibration de $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ sur $\mathbb{P}^1(\mathbb{R})$ ne présente aucune singularité, pas même à l'infini. On ne cherchera pas ici à faire l'étude appronfondie de cette famille de polynômes dans la mesure où on se contentera de démontrer l'existence de valeurs du paramètre r pour lesquelle il n'y a pas de point spécial sur $\mathcal{C}^{-1}_{\mathbb{R}(x)}$. Cela suffit à montrer que l'existence de singularité de la fibration de $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ sur $\mathbb{P}^1(\mathbb{R})$ n'est pas une condition nécessaire pour que la courbe elliptique étudiée ne possède pas de point autre que ses points de torsion.

Les courbes elliptiques associées à ce polynôme F sont :

* $\mathcal{C}^{-1} : -\beta^2 = \alpha(\alpha^2 - 2(2(x^2+2)^2 - r^2(x^2+1)^2)\alpha + r^4(x^2+1)^4)$

* $\mathcal{D}^{-1} : -\beta^2 = \alpha(\alpha + 4(x^2+2)^2)(\alpha + 4[(x^2+2)^2 - r^2(x^2+1)^2])$.

On remarque que, comme dans l'exemple de la section 2.3, les points d'ordre 2 de la courbe elliptique d'équation $-\beta^2 = \alpha(\alpha^2 - 2(a(x_0)+b(x_0))\alpha + (a(x_0) - b(x_0))^2)$, qui est définie sur $\mathbb{R}$, ont pour premières coordonnées 0, $a(x_0)+b(x_0) - 2\sqrt{a(x_0)b(x_0)}$ et $a(x_0)+b(x_0)+2\sqrt{a(x_0)b(x_0)}$ et comme les polynômes ab et $a-b$ ne s'annulent pas sur $\mathbb{R}$, ces points sont distincts et la fibration de la courbe $\mathcal{C}^{-1}$ n'admet de singularité en aucun point $x_0 \in \mathbb{R}$. Mais de plus ici les coefficients dominants des polynômes a et b sont distincts, et donc cette fibration n'admet pas de singularité réelle à l'infini.

Comme dans les exemples précédents de ce chapitre, la courbe $\mathcal{C}^{-1}$ est globalement invariante par rapport à la transformation σ_x définie à la section 2.2, on peut donc se ramener à l'étude des quatres courbes :

* $\hat{\mathcal{C}}^{-d} : -d\beta^2 = \alpha(\alpha^2 - 2(2(z+2)^2 - r^2(z+1)^2)\alpha + r^4(z+1)^4)$

* $\hat{\mathcal{D}}^{-d} : -d\beta^2 = \alpha(\alpha + 4(z+2)^2)(\alpha + 4[(z+2)^2 - r^2(z+1)^2])$

* $\check{\mathcal{C}}^{-d} : -d\beta^2 = \alpha(\alpha^2 - 2(2(z+2)^2 - r^2(z+1)^2)z\alpha + r^4z^2(z+1)^4)$

* $\check{\mathcal{D}}^{-d} : -d\beta^2 = \alpha(\alpha + 4(z+2)^2z)(\alpha + 4[(z+2)^2 - r^2(z+1)^2]z)$

Ces courbes elliptiques sont définies sur le corps $k_0(z)$ avec $k_0 = \mathbb{Q}(r)$ et les courbes $\hat{\mathcal{D}}^{-1}$ et $\check{\mathcal{D}}^{-1}$ sont à 2-torsion $k_0(z)$-rationnelle, on peut donc utiliser la

méthode proposée au chapitre 1. On remarque que si k est le corps de décomposition du polynôme $ab(a-b)$, alors $k = \mathbb{Q}(r) = k_0$. Dans la définition de ces quatre courbes, d est un élément de k^*.

On suivra un plan (A), (B), (C), (D), (E), (F) similaire à celui de la section 2.3 et on obtiendra ainsi des conditions sur r suffisantes pour que la courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ n'ait pas de point spécial, donc pour les valeurs du nombre r vérifiant ces conditions, le polynôme $F(x,y) = (y^2 + (x^2+2)^2)(y^2 + (x^2+2)^2 - r^2(x^2+1)^2)$ ne sera pas somme de 3 carrés dans $\mathbb{R}(x,y)$.

Remarque 2.5.1 On utilisera encore la notation $g \sim h$ lorsque g et h appartiennent à la même classe de carrés dans k^*.

Notation 2.5.2 *Pour alléger l'écriture de certaines formules, on définit les polynômes* $P_1 = (1-r)z + (2-r)$ *et* $P_2 = (1+r)z + (2+r)$ *et on note* $z_1 = -\frac{2-r}{1-r}$ *et* $z_2 = -\frac{2+r}{1+r}$ *leurs racines respectives.*

Remarque 2.5.3 Il est clair que :

* on a $P_1P_2 = (z+2)^2 - r^2(z+1)^2 = b(z)$,
* pour $0 < r < 1$, les polynômes P_1 et P_2 sont premiers avec z, $z+1$ et $z+2$,
* lorsque $0 < r < 1$, on a $z_1 < -2$ et $-2 < z_2 < -1$, donc par la suite, les termes z_1, z_1+1, z_1+2, z_2, z_2+1 et z_2+2 ne seront jamais nuls.

(A) Etude des points d'ordre 2^n

On se retrouve dans un cas similaire aux précédents, car a est un carré : $a = u^2$ avec $u = x^2+2$, et $a-b = v^2$, avec $v = r(x^2+1)$, donc d'après les résultats de la section 2.1, il y a des points d'ordre 4 définis sur $\mathbb{R}(x)$ sur les courbes $\mathcal{C}^{-1}$ et $\mathcal{D}^{-1}$. De plus, comme u et v sont premiers entre eux et comme u n'est pas un carré, il n'y a pas de point d'ordre 8 ni sur la courbe $\mathcal{C}^{-1}$, ni sur la courbe $\mathcal{D}^{-1}$. Les points $\mathbb{R}(x)$-rationnels d'ordre 2^n de $\mathcal{C}^{-1}$ sont :

* Le point $\mathcal{P}_{\mathcal{C}} = (0,0)$ d'ordre 2,
* Les points $(-r^2, 2r^2(x^2+2))$ et $(-r^2, -2r^2(x^2+2))$ d'ordre 4.

Il est clair qu'aucun de ces points d'ordre fini sur $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ n'est spécial.

(B) Etude de $\hat{\mathcal{C}}^{-d}_{k(z)}$

On veut trouver des conditions sur r qui suffiront à prouver que l'image du morphisme $\hat{\gamma}_c : \hat{\mathcal{C}}^{-d}_{k(z)} \to k(z)^*/k(z)^{*2}$ est celle des points de torsion, or les points d'ordre 2^n sont ceux d'ordre 2 ou 4 (lorsque d est un carré dans k) et ils appartiennent au noyau de $\hat{\gamma}_c$. Comme ce sont les seuls points de torsion connus sur cette courbe, on doit donc montrer que l'image de $\hat{\gamma}_c$ est triviale.

Soit (α, β) un point de $\hat{\mathcal{C}}^{-d}_{k(z)}$ d'ordre infini donc vérifiant $\beta \neq 0$, on écrit $\alpha = f\frac{\theta^2}{\psi^2}$ avec les conditions habituelles. Le polynôme f est sans facteur carré et divise $(a-b)^2 = r^4(z+1)^4$, donc soit $f = e \in k^*$, soit $f = e(z+1)$ avec $e \in k^*$.

L'équation de $\hat{\mathcal{C}}^{-d}_{k(z)}$ étant $-\beta^2 = \alpha(\alpha^2 - 2(2(z+2)^2 - r^2(z+1)^2)\alpha + r^4(z+1)^4)$, on déduit, d'après le lemme 1.5.13, qu'il existe $\mu \in k[z]$ tel que :

$$-df\mu^2 = f^2\theta^4 - 2(2(z+2)^2 - r^2(z+1)^2)f\theta^2\psi^2 + r^4(z+1)^4\psi^4.$$

Mais, comme $(z+2)^2 - r^2(z+1)^2 = P_1P_2$, on peut aussi écrire cette équation sous la forme

$$-df\mu^2 = (f\theta^2 - r^2(z+1)^2\psi^2)^2 - 4P_1(z)P_2(z)f\theta^2\psi^2.$$

Cas (B1) : Si f = e

La relation précédente donne alors l'équation :

$$-de\mu^2 = (e\theta^2 - r^2(z+1)^2\psi^2)^2 - 4P_1(z)P_2(z)e\theta^2\psi^2.$$

Pour $z = z_1$, on a $-de\mu^2(z_1) = (e\theta^2(z_1) - r^2(z_1+1)^2\psi^2(z_1))^2$. Or $(e\theta^2(z_1) - r^2(z_1+1)^2\psi^2(z_1)) \neq 0$ sinon $(z - z_1)$ diviserait $(e\theta^2 - r^2\psi^2)$ ainsi que μ, et on montre par le même raisonnement que dans les sections précédentes que $(z - z_1)$ diviserait à la fois θ et ψ que l'on a supposés premiers entre eux.

On peut donc en déduire que $-de \in k^{*2}$ et donc que le point (α, β) considéré appartient bien au noyau de $\hat{\gamma}_c$.

Cas (B2) : Si f = e(z + 1)

On a, après simplification par $z+1$, l'équation :

$$-de\mu^2 = (z+1)(e\theta^2 - r^2(z+1)\psi^2)^2 - 4P_1(z)P_2(z)e\theta^2\psi^2.$$

Pour $z = z_1$, on a $-de\mu^2(z_1) = (z_1+1)(e\theta^2(z_1) - r^2(z_1+1)^2\psi^2(z_1))^2)$ et comme précédemment, on montre que ce terme ne peut pas s'annuler car θ et ψ sont premiers entre eux, donc $-de \sim (z_1+1)$.

De même pour $z = z_2$, on a $-de\mu^2(z_2) = (z_2+1)(e\theta^2(z_2) - r^2(z_2+1)^2\psi^2(z_2))^2) \neq 0$, donc $-de \sim (z_2+1)$.

On doit donc avoir $(z_1+1) \sim (z_2+1)$ c'est-à-dire $(1 - \frac{2-r}{1-r}) \sim (1 - \frac{2+r}{1+r})$ ce qui revient à $(1-r) \sim (1+r)$ ou encore à $(1-r^2) \sim 1$

Pour exclure le cas (B2), il suffira de s'assurer que $(1-r^2)$ n'est pas un carré dans $k = \mathbb{Q}(r)$, avec cette hypothèse, l'image du morphisme $\hat{\gamma}_c$ sera triviale.

(C) Etude de $\hat{\mathcal{D}}^{-\mathbf{d}}_{\mathbf{k(z)}}$

On doit ici chercher des conditions sur le réel r permettant de s'assurer que l'image du morphisme $\hat{\gamma}_{\mathcal{D}} : \hat{\mathcal{D}}^{-d}_{k(z)} \to k(z)^*/k(z)^{*2}$ est l'image des points d'ordre fini : en fait, cette propriété est toujours vraie quelle que soit la valeur de r. On connait déjà, d'après la section 2.3, les points de torsion suivants sur la courbe $\hat{\mathcal{D}}^{-d}_{k(z)}$:

* Les points $\mathcal{P}_{\mathcal{D}} = (0,0)$, $(-4(z+2)^2, 0)$ et $(-4((1-r)z+(2-r))((1+r)z+(2+r)), 0)$ d'ordre 2 qui existent dans tous les cas.

* Les points $(-4(z+2)((1-r)z+(2-r)), \pm\frac{8}{\sqrt{d}}r(z+2)((1-r)z+(2-r)))$ et $(-4(z+2)((1+r)z+(2+r)), \pm\frac{8}{\sqrt{d}}r(z+2)((1+r)z+(2+r)))$ d'ordre 4 dans le cas où d est un carré dans k.

On va donc distinguer les deux cas d est un carré dans k et d n'est pas un carré dans k.

On a ici un résultat proche de celui du lemme 2.3.3 :

Lemme 2.5.4 *En utilisant les notations du lemme 1.5.13, si (α, β) est un point de $\hat{\mathcal{D}}^{-d}_{k(z)}$ vérifiant $\beta \neq 0$, on a $\alpha = f\frac{\theta^2}{\psi^2}$, avec f, θ, $\psi \in k[z]$, $pgcd(f\theta, \psi) = 1$ et f est sans facteur carré et de degré pair. On sait aussi que si $f = e \in k^*$, alors soit $-de \in k^{*2}$, soit $-e \in k^{*2}$.*

Preuve. La démonstration de la première partie de ce résultat est analogue à celle effectuée pour prouver le lemme 2.3.3. Pour démontrer que lorsque $f = e \in k^*$ alors on a soit $-de \in k^{*2}$, soit $-e \in k^{*2}$, on utilise la relation :

$$-de\mu^2 = (e\theta^2 + 4(z+2)^2\psi^2)(e\theta^2 + 4((z+2)^2 - r^2(z+1)^2)\psi^2),$$

et on pose $z = -1$, ce qui donne $-de\mu^2(-1) = (e\theta^2(-1) + 4\psi^2(-1))^2$, donc si $e\theta^2(-1) + 4\psi^2(-1) \neq 0$ alors $-de \in k^{*2}$ et si ce terme est nul, on a $e\theta^2(-1) = -4\psi^2(-1)$ avec $\theta(-1) \neq 0$ et $\psi(-1) \neq 0$ car θ et ψ ne peuvent pas s'annuler simultanément en -1 et on obtient $-e \in k^{*2}$. □

(C1) Si d n'est pas un carré

Les seuls points d'ordre fini connus sont les points d'ordre 2 et on va montrer que l'image de $\hat{\gamma}_{\mathcal{D}}$ est l'image de ces points. On rappelle que les images de ces points sont :

* $\hat{\gamma}_{\mathcal{D}}(\mathcal{P}_{\mathcal{D}}) = P_1P_2k(z)^{*2}$,
* $\hat{\gamma}_{\mathcal{D}}(-4(z+2)^2, 0) = dk(z)^{*2}$,
* $\hat{\gamma}_{\mathcal{D}}(-4((1-r)z + (2-r))((1+r)z + (2+r)), 0) = dP_1P_2k(z)^{*2}$.

On doit donc montrer que :

$$\hat{\gamma}_{\mathcal{D}}\left(\hat{\mathcal{D}}^{-d}_{k(z)}\right) = \left\{k(z)^{*2}, dk(z)^{*2}, dP_1P_2k(z)^{*2}, P_1P_2k(z)^{*2}\right\}$$

Si (α, β) est un point de $\hat{\mathcal{D}}^{-d}_{k(z)}$ vérifiant $\beta \neq 0$, en écrivant $\alpha = f\frac{\theta^2}{\psi^2}$ avec les conditions habituelles, on sait, d'après le lemme 1.5.13, que f divise $ab = (z+2)^2P_1P_2$ de plus f est sans facteur carré, on peut donc supposer que f divise $(z+2)P_1P_2$. On a aussi un résultat analogue à la proposition 2.3.4 :

Proposition 2.5.5 *Si d n'est pas un carré dans k, alors on ne peut pas avoir $(z+2)$ comme facteur de f.*

Preuve. Il suffit d'adapter la démonstration de la proposition 2.3.4. □

On peut donc en conclure que f est de degré pair et divise P_1P_2, c'est-à-dire soit $f = e$, soit $f = eP_1P_2$, avec $e \in k^*$ et quitte à ajouter au point (α, β) le point $\mathcal{P}_{\mathcal{D}}$, ou le point $(-4P_1P_2, 0)$, on peut supposer que $f = e \in k^*$, mais alors d'après le lemme 2.5.4, on a soit $-de \in k^{*2}$, soit $-e \in k^{*2}$. Si $-de \in k^{*2}$, alors $\hat{\gamma}_{\mathcal{D}}(\alpha, \beta) = k(z)^{*2}$ donc $(\alpha, \beta) \in \ker(\hat{\gamma}_{\mathcal{D}})$ le problème est résolu, et si $-e \in k^{*2}$, alors $\hat{\gamma}_{\mathcal{D}}(\alpha, \beta) = dk(z)^{*2} = \hat{\gamma}_{\mathcal{D}}(-4(z+2)^2, 0)$, on est encore dans l'image des points d'ordre 2, ce qui permet de terminer l'étude de $\hat{\mathcal{D}}^{-d}_{k(z)}$ dans le cas où d n'est pas un carré dans k.

(C2) Si d est un carré

Dans ce cas, en plus des points d'ordre 2, il y a sur $\hat{\mathcal{D}}^{-d}_{k(z)}$ des points d'ordre 4, $(-4(z+2)P_1, \pm\frac{8}{\sqrt{d}}r(z+2)P_1)$ et $(-4(z+2)P_2, \pm\frac{8}{\sqrt{d}}r(z+2)P_2)$. Leurs images par le morphisme $\hat{\gamma}_{\mathcal{D}}$ sont :

* $\hat{\gamma}_{\mathcal{D}}(\mathcal{P}_{\mathcal{D}}) = P_1P_2k(z)^{*2}$,
* $\hat{\gamma}_{\mathcal{D}}((-4(z+2)^2, 0) = k(z)^{*2}$ car d est un carré,
* $\hat{\gamma}_{\mathcal{D}}(-4P_1P_2, 0) = P_1P_2k(z)^{*2} = \hat{\gamma}_{\mathcal{D}}(\mathcal{P}_{\mathcal{D}})$,
* $\hat{\gamma}_{\mathcal{D}}(-4(z+2)P_1, \pm\frac{8}{\sqrt{d}}r(z+2)P_1) = (z+2)P_1k(z)^{*2}$,
* $\hat{\gamma}_{\mathcal{D}}(-4(z+2)P_2, \pm\frac{8}{\sqrt{d}}r(z+2)P_2) = (z+2)P_2k(z)^{*2}$.

On doit donc montrer que :

$$\hat{\gamma}_{\mathcal{D}}\left(\hat{\mathcal{D}}^{-d}_{k(z)}\right) = \left\{k(z)^{*2}, P_1P_2k(z)^{*2}, (z+2)P_1k(z)^{*2}, (z+2)P_2k(z)^{*2}\right\}.$$

Si (α, β) est un point de $\hat{\mathcal{D}}^{-d}_{k(z)}$ vérifiant $\beta \neq 0$, on écrit encore α sous la forme $f\frac{\theta^2}{\psi^2}$ avec les mêmes conditions et on sait, d'après les lemmes 1.5.13 et 2.5.4, que f divise $(z+2)P_1P_2$ et est de degré pair donc on a soit $f = e$, soit $f = e(z+2)P_1$, soit $f = e(z+2)P_2$, soit $f = eP_1P_2$ avec $e \in k^*$. On alors remarque que quitte à ajouter un des points d'ordre 2 ou 4, on peut supposer que $f = e$ et le lemme 2.5.4 montre que soit $-de \in k^{*2}$, soit $-e \in k^{*2}$. Comme ici $d \in k^{*2}$, cela implique qu'on a toujours $\hat{\gamma}_{\mathcal{D}}(\alpha, \beta) = -dek(z)^{*2} = k(z)^{*2}$.

On a donc prouvé que pour tout $d \in k^*$, l'image du morphisme $\hat{\gamma}_{\mathcal{D}}$ est celle des points d'ordre 2.

(D) Etude de $\check{\mathcal{C}}^{-\mathbf{d}}_{\mathbf{k(z)}}$

Comme le seul point de torsion connu sur $\check{\mathcal{C}}^{-d}_{k(z)}$ est $(0,0)$ et qu'il appartient au noyau de $\check{\gamma}_c$, on va rechercher des conditions sur le réel r impliquant que l'image de $\check{\gamma}_c$ est triviale.

Si on a un point (α, β) tel que $\beta \neq 0$ sur cette courbe, en utilisant les notations habituelles, on sait qu'il existe un polynôme μ tel que :

$$-df\mu^2 = f^2\theta^4 - 2(2(z+2)^2 - r^2(z+1)^2)zf\theta^2\psi^2 + r^4(z+1)^4z^2\psi^4$$

ou encore, comme $(z+2)^2 - r^2(z+1)^2 = P_1P_2$:

$$-df\mu^2 = (f\theta^2 - r^2z(z+1)^2\psi^2)^2 - 4zP_1(z)P_2(z)f\theta^2\psi^2.$$

On sait aussi que f est sans facteur carré et divise $r^4(z+1)^4z^2$ on a quatre possibilités : soit $f = e$, soit $f = ez$, soit $f = e(z+1)$, soit $f = ez(z+1)$.

Cas (D1) : Si f = e

On montre qu'on a toujours $-de \in k^{*2}$ en spécialisant en $z = z_1$ ou $z = z_2$: la méthode est analogue à celle employée pour le cas $f = e$ dans l'étude de $\hat{\mathcal{C}}^{-d}_{k(z)}$.

Remarque 2.5.6 On peut obtenir le même résultat en posant $z = 0$, ce qui donne $-de\mu^2(0) = e^2\theta^4(0)$, si $\theta(0) \neq 0$, $-de \in k^{*2}$, si $\theta(0) = 0$, on a alors $\mu(0) = 0$ et $\psi(0) \neq 0$ et en posant $\mu = z\mu'$ et $\theta = z\theta'$, on a : $-de\mu'^2 = e^2z^2\theta'^4 - 2(2(z+2)^2 - r^2(z+1)^2)zf\theta'^2\psi^2 + r^4(z+1)^4\psi^4$, donc $-de\mu'^2(0) = r^4\psi^4(0) \in k^{*2}$.

Cas (D2) : Si f = ez

Pour prouver que l'image de $\check{\gamma}_c$ est triviale, il faut démontrer que ce cas ne peut pas se produire. On a, dans l'équation de $\check{\mathcal{C}}^{-d}_{k(z)}$, toujours avec les mêmes notations :

$$-dez\mu^2 = (ez\theta^2 - r^2z(z+1)^2\psi^2)^2 - 4z^2P_1(z)P_2(z)e\theta^2\psi^2.$$

Et, en posant $\mu = z\mu'$ avec $\mu' \in k[x]$, après simplication par z^2 :

$$-dez\mu'^2 = (e\theta^2 - r^2(z+1)^2\psi^2)^2 - 4P_1(z)P_2(z)e\theta^2\psi^2.$$

Pour $z = z_1$, on obtient $-dez_1\mu'^2(z_1) = (e\theta^2(z_1) - r^2(z_1+1)^2\psi^2(z_1))^2$, avec $e\theta^2(z_1) - r^2(z_1+1)^2\psi^2(z_1)) \neq 0$ (il suffit de faire le même raisonnement que dans les cas similaires déjà traités), donc $-dez_1 \sim 1$, de même pour $z = z_2$, on a $-dez_2 \sim 1$ on en déduit que $z_1z_2 \sim 1$.

Il va donc suffire que $z_1z_2 = \left(\frac{2-r}{1-r}\right)\left(\frac{2+r}{1+r}\right)$ ne soit pas un carré dans k pour que le cas $f = ez$ ne puisse pas se produire, cela revient à imposer que $(4-r^2)(1-r^2)$ ne soit pas un carré dans $\mathbb{Q}(r)$.

Cas (D3) : Si f = e(z + 1)

Ici dans l'équation de $\check{\mathcal{C}}^{-d}_{k(z)}$, on a :

$$-de(z+1)\mu^2 = (e(z+1)\theta^2 - r^2 z(z+1)^2\psi^2)^2 - 4zP_1(z)P_2(z)e(z+1)\theta^2\psi^2$$

et après simplification par $(z+1)$, on obtient :

$$-de\mu^2 = (z+1)(e\theta^2 - r^2 z(z+1)\psi^2)^2 - 4zP_1(z)P_2(z)e\theta^2\psi^2.$$

Pour $z = z_1$, on a $-de\mu^2(z_1) = (z_1+1)(e\theta^2(z_1) - r^2 z_1(z_1+1)\psi^2(z_1))^2 \neq 0$ et pour $z = z_2$, on a $-de\mu^2(z_2) = (z_2+1)(e\theta^2(z_2) - r^2 z_2(z_2+1)\psi^2(-z_2))^2 \neq 0$, ce qui donne respectivement $-de \sim (z_1+1)$ et $-de \sim (z_2+1)$, donc $(z_1+1)(z_2+1) \sim 1$ c'est-à-dire $(1-r^2) \sim 1$.

Il suffit donc que $1 - r^2$ ne soit pas un carré dans k pour éliminer le cas $f = e(z+1)$, cette condition était déjà apparue lors de l'étude de $\hat{\mathcal{C}}^{-d}_{k(z)}$.

Cas (D4) : Si f = ez(z + 1)

On a ici l'équation :

$$-dez(z+1)\mu^2 = (ez(z+1)\theta^2 - r^2 z(z+1)^2\psi^2)^2 - 4z^2(z+1)P_1(z)P_2(z)e\theta^2\psi^2.$$

On constate que z^2 divise le membre de droite donc z divise μ, on pose $\mu = z\mu'$ et après simplification par $z^2(z+1)$, on a :

$$-dez\mu'^2 = (z+1)(e\theta^2 - r^2(z+1)\psi^2)^2 - 4P_1(z)P_2(z)e\theta^2\psi^2.$$

Pour $z = z_1$, on a $-dez_1\mu'^2(z_1) = (z_1+1)(e\theta^2(z_1) - r^2(z_1+1)\psi^2(z_1))^2 \neq 0$ (toujours grâce au même argument), et pour $z = z_2$, on a $-dez_2\mu'^2(z_2) = (z_2+1)(e\theta^2(z_2) - r^2(z_2+1)\psi^2(z_2))^2 \neq 0$. Cela donne $-dez_1 \sim (z_1+1)$ et $-dez_2 \sim (z_2+1)$, d'où $-de \sim z_1(z_1+1) \sim z_2(z_2+1)$, c'est-à-dire $(2-r) \sim (2+r)$ ou encore $(4-r^2) \sim 1$. On devra, afin d'éliminer le cas $f = ez(z+1)$, s'assurer que cette condition n'est pas réalisée.

On a donc démontré que l'image du morphisme $\check{\gamma}_c$ est triviale dans le cas où ni $(1-r^2)$, ni $(4-r^2)$, ni $(4-r^2)(1-r^2)$ ne sont des carrés dans le corps $k = \mathbb{Q}(r)$.

(E) Etude de $\check{\mathcal{D}}^{-\mathbf{d}}_{\mathbf{k(z)}}$

L'équation de la courbe $\check{\mathcal{D}}^{-d}$ est $-d\beta^2 = \alpha(\alpha + 4(z+2)^2 z)(\alpha + 4[(z+2)^2 - r^2(z+1)^2]z)$, comme ni $a(z) = (z+2)^2 z$ ni $b(z) = ((z+2)^2 - r^2(z+1)^2)z$ ne sont des carrés dans $k[z]$, d'après la section 2.2, il n'y a pas de point d'ordre 4 sur $\check{\mathcal{D}}^{-d}_{k(z)}$. Les seuls points d'ordre finis connus sur cette courbe sont donc les points d'ordre 2 : $(0,0)$, $(-4(z+2)^2 z, 0)$ et $(-4[(z+2)^2 - r^2(z+1)^2]z, 0) = (-4zP_1P_2, 0)$, leurs images par $\check{\gamma}_{\mathcal{D}}$ sont :

* $\check{\gamma}_{\mathcal{D}}(0,0) = P_1P_2k(z)^{*2}$,
* $\check{\gamma}_{\mathcal{D}}(-4(z+2)^2 z, 0) = dzk(z)^{*2}$,
* $\check{\gamma}_{\mathcal{D}}(-4zP_1P_2, 0) = dzP_1P_2k(z)^{*2}$.

On doit donc montrer que :

$$\check{\gamma}_{\mathcal{D}}(\check{\mathcal{D}}^{-d}_{k(z)}) = \left\{k(z)^{*2}, P_1P_2k(z)^{*2}, dzk(z)^{*2}, dzP_1P_2k(z)^{*2}\right\}.$$

En utilisant les notations habituelles, si (α, β) est un point de $\hat{\mathcal{D}}^{-d}_{k(z)}$ vérifiant $\beta \neq 0$, on a, ici encore, $\alpha = f\frac{\theta^2}{\psi^2}$, avec f sans facteur carré divisant $z^2(z+2)^2P_1P_2$ d'ø'u f divise $z(z+2)P_1P_2$. Quitte à ajouter à (α, β) un des point d'ordre deux, on peut supposer que ni z ni P_2 ne sont pas des facteurs de f, qui va alors diviser $(z+2)P_1$. On doit ainsi étudier quatre cas :

* Cas (E1) : $f = e$, avec $e \in k^*$,
* Cas (E2) : $f = e(z+2)$, avec $e \in k^*$,
* Cas (E3) : $f = eP_1$, avec $e \in k^*$,
* Cas (E4) : $f = e(z+2)P_1$, avec $e \in k^*$.

On doit trouver des conditions portant sur r pour que, dans le cas (E1) on ait $-de \sim 1$ et pour que les cas (E2), (E3) et (E4) ne puissent pas se produire, pour cela, il est important de connaître le lemme suivant :

Lemme 2.5.7 *D'après l'équation de $\check{\mathcal{D}}^{-d}_{k(z)}$, il existe un polynôme μ tel que :*

$$-df\mu^2 = (f\theta^2 + 4z(z+2)^2\psi^2)(f\theta^2 + 4zP_1P_2\psi^2),$$

et le pgcd des polynômes $f\theta^2 + 4z(z+2)^2\psi^2$ et $f\theta^2 + 4zP_1P_2\psi^2$ est un diviseur de $z(z+1)^2$.

Preuve. La démonstration est analogue à celle du lemme 2.3.6 : si P est un diviseur commun à ces deux polynômes, alors il divise leur différence : $8r^2z(z+1)^2\psi^2$. Or P est premier avec ψ, sinon il admet un diviseur premier p commun avec ψ et ce diviseur premier est aussi un facteur de $f\theta^2$ ce qui est exclu car $\text{pgcd}(f\theta^2, \psi) = 1$. On en déduit donc que P divise $z(z+1)^2$. □

Notation 2.5.8 *On notera P_0 le pgcd de $f\theta^2+4z(z+2)^2\psi^2$ et de $f\theta^2+4zP_1P_2\psi^2$, on a donc six cas possibles $P_0 = 1$, $P_0 = z$, $P_0 = (z+1)$, $P_0 = z(z+1)$, $P_0 = (z+1)^2$ et $P_0 = z(z+1)^2$.*

Cas (E1) : Si f = e

L'objectif est ici de montrer que l'on a toujours $-de \in k^{*2}$. On connait la relation :

$$-de\mu^2 = (e\theta^2 + 4z(z+2)^2\psi^2)(e\theta^2 + 4z((z+2)^2 - r^2(z+1)^2)\psi^2).$$

Si $\deg(\theta^2) > \deg(\psi^2) + 3$, alors en examinant les coefficients dominants dans cette équation, on trouve que $-de \in k^{*2}$, le problème est réglé dans ce cas. Si $\deg(\theta^2) < \deg(\psi^2) + 3$, alors l'étude des coefficients dominants montre que $-de \sim 1 - r^2$. Puis pour $z = 0$, on a $-de\mu^2(0) = (e\theta^2(0))^2$, si $\theta(0)$ et $\mu(0)$ ne sont pas nuls on obtient que $-de \in k^{*2}$ ce qui résout le problème. Si $\theta(0) = \mu(0) = 0$, on pose $\theta = z\theta'$ et $\mu = z\mu'$ avec θ', $\mu' \in k[z]^*$ ce qui donne, après simplification par z^2, l'équation :

$$-de\mu'^2 = (ez\theta'^2 + 4(z+2)^2\psi^2)(ez\theta'^2 + 4((z+2)^2 - r^2(z+1)^2)\psi^2).$$

Et pour $z = 0$ dans cette dernière relation, on a $-de\mu'^2(0) = 64(4 - r^2)\psi^4(0)$, avec $\psi(0) \neq 0$ car on a déjà $\theta(0) = 0$ d'où $-de \sim 4 - r^2$, ce qui implique que $1 - r^2 \sim 4 - r^2$ ou $(1 - r^2)(4 - r^2) \sim 1$ et cette possibilité a déjà été exclue précédemment.

On a donc toujours $-de \in k^{*2}$ lorsque $f = e$, le cas (E1) est traité.

Cas (E2) : Si f = e(z + 2)

On a, après simplification par $z + 2$, l'équation :

$$-de\mu^2 = (e\theta^2 + 4z(z+2)\psi^2)(e(z+2)\theta^2 + 4zP_1P_2\psi^2)$$

On va considérer quatre cas suivant la valeur du pgcd P_0 :

(i) Si $P_0 = 1$ ou si $P_0 = (z+1)^2$:

Dans ce cas, le produit des polynômes $e\theta^2+4z(z+2)\psi^2$ et $e(z+2)\theta^2+4zP_1P_2\psi^2$ est $-de\mu^2$ et leur pgcd P_0 est un carré, il existe donc $s \in k^*$, μ_1, $\mu_2 \in k[z]$ tels que :

$$\left\{ \begin{array}{rcll} e\theta^2 + 4z(z+2)\psi^2 & = & s\mu_1^2 & (1) \\ e(z+2)\theta^2 + 4zP_1P_2\psi^2 & = & -des\mu_2^2 & (2) \end{array} \right.$$

On a alors :

* Pour $z = z_1$, dans (2), $e(z_1+2)\theta^2(z_1) = -des\mu_2^2(z_1)$ et le terme $\mu_2^2(z_1)$ est non nul, car sinon P_1 serait un facteur commun à θ et à ψ. On a donc $e(z_1+2) \sim -des$.

* Pour $z = z_2$, dans (2), $e(z_2+2)\theta^2(z_2) = -des\mu_2^2(z_2) \neq 0$ d'où on obtient $e(z_2+2) \sim -des$.

On en déduit que $(z_1+2) \sim (z_2+2)$ c'est-à-dire $\frac{-r}{1-r} \sim \frac{r}{1+r}$ ou encore $(r-1) \sim (r+1)$ ce qui est impossible car $0 < r < 1$ et le corps k est réel. Le cas (i) ne peut jamais se produire.

(ii) Si $P_0 = z$ ou si $P_0 = z(z+1)^2$:

Alors, dans ce cas, le produit des polynômes $e\theta^2 + 4z(z+2)\psi^2$ et $e(z+2)\theta^2 + 4zP_1P_2\psi^2$ est $-de\mu^2$ et leur pgcd P_0 est le produit du polynôme z par un carré, donc il existe $s \in k^*$, μ_1, $\mu_2 \in k[z]$ tels que :

$$\left\{ \begin{array}{rcll} e\theta^2 + 4z(z+2)\psi^2 & = & sz\mu_1^2 & (3) \\ e(z+2)\theta^2 + 4zP_1P_2\psi^2 & = & -desz\mu_2^2 & (4) \end{array} \right.$$

Dans (3) ou (4), on a, pour $z = 0$, $\theta(0) = 0$, on pose $\theta = z\theta'$ dans $k[z]$, mais alors l'équation (4) donne :

$$ez(z+2)\theta'^2 + 4P_1P_2\psi^2 = -des\mu_2^2 \quad (4').$$

Et dans (4'), pour $z = 0$, on a $4P_1(0)P_2(0)\psi^2(0) = -des\mu_2^2(0)$ avec $\psi(0) \neq 0$ car $\theta(0) = 0$, donc $P_1(0)P_2(0) \sim -des$ c'est-à-dire $(4 - r^2) \sim -des$. Toujours dans (4'), pour $z = -2$, on obtient $4P_1(-2)P_2(-2)\psi^2(-2) = -des\mu_2^2(-2)$, et $\mu_2(-2) \neq 0$ sinon $z+2$ diviserait à la fois θ' et ψ ce qui est impossible. Donc $P_1(-2)P_2(-2) \sim -des$, c'est-à-dire $-r^2 \sim -des$. On en déduit alors que $(4-r^2) \sim -r^2$, ce qui est impossible pour des raisons de signe. Le cas (ii) ne se produit donc jamais.

(iii) Si $P_0 = z+1$:

Le produit des polynômes $e\theta^2 + 4z(z+2)\psi^2$ et $e(z+2)\theta^2 + 4zP_1P_2\psi^2$ est toujours $-de\mu^2$ mais leur pgcd est $z+1$, donc il existe $s \in k^*$, μ_1, $\mu_2 \in k[z]$ tels que :

$$\begin{cases} e\theta^2 + 4z(z+2)\psi^2 &= s(z+1)\mu_1^2 & (5) \\ e(z+2)\theta^2 + 4zP_1P_2\psi^2 &= -des(z+1)\mu_2^2 & (6) \end{cases}$$

Dans (5), pour $z = 0$, $e\theta^2(0) = s\mu_1^2(0)$ et ces deux termes sont non nuls car sinon z^2 diviserait les deux membres de l'équation (5), et donc z diviserait à la fois θ et ψ, on a ainsi $e \sim s$. D'autre part, pour $z = -2$, toujours dans (5), on a $e\theta^2(-2) = -s\mu_1^2(-2)$, ces termes étant non nuls, on a donc $e \sim -s$. Cela implique que $s \sim -s$, ce qui est clairement impossible, le corps k étant un sous-corps de $\mathbb{R}$. Le cas (iii) est ainsi exclu.

(iv) Si $P_0 = z(z+1)$:

Le pgcd des polynômes $e\theta^2+4z(z+2)\psi^2$ et $e(z+2)\theta^2+4zP_1P_2\psi^2$ est $z(z+1)$, leur produit est toujours $-de\mu^2$ donc il existe $s \in k^*$, μ_1, $\mu_2 \in k[z]$ tels que :

$$\begin{cases} e\theta^2 + 4z(z+2)\psi^2 &= sz(z+1)\mu_1^2 & (7) \\ e(z+2)\theta^2 + 4zP_1P_2\psi^2 &= -desz(z+1)\mu_2^2 & (8) \end{cases}$$

En posant $z = 0$ dans (7) ou dans (8), on obtient que $\theta(0) = 0$, on pose donc $\theta = z\theta'$ et l'équation (8) devient après simplification :

$$ez(z+2)\theta'^2 + 4P_1P_2\psi^2 = -des(z+1)\mu_2^2 \quad (8')$$

Et dans (8'), pour $z = 0$, on a $4P_1(0)P_2(0)\psi^2(0) = -des\mu_2^2(0) \neq 0$, donc $P_1(0)P_2(0) \sim -des$. D'autre part, pour $z = -2$, on a $4P_1(-2)P_2(-2)\psi^2(-2) = des\mu_2^2(-2) \neq 0$ ce qui donne $P_1(-2)P_2(-2) \sim des$. On en déduit alors que $P_1(0)P_2(0) \sim -P_1(-2)P_2(-2)$ c'est-à-dire $(4 - r^2) \sim r^2 \sim 1$. Il va donc être nécessaire de supposer que $(4 - r^2)$ n'est pas un carré dans k pour exclure le cas (iv). On remarque que cette condition est déjà apparue précédemment.

A condition que $(4-r^2)$ ne soit pas un carré dans le corps k, on n'aura jamais $f = e(z+2)$, l'étude de la partie (E2) est donc terminée.

Cas (E3) : Si $\mathbf{f = eP_1 = e((1-r)z + (2-r))}$

L'équation de $\check{\mathcal{D}}^{-d}_{k(z)}$ donne dans ce cas :

$$-deP_1\mu^2 = (eP_1\theta^2 + 4z(z+2)^2\psi^2)(eP_1\theta^2 + 4zP_1P_2\psi^2)$$

Et après simplification :

$$-de\mu^2 = (eP_1\theta^2 + 4z(z+2)^2\psi^2)(e\theta^2 + 4zP_2\psi^2)$$

Ici encore, il faut distinguer quatre différents cas suivant les valeurs du polynôme P_0.

(i) Si $P_0 = 1$ ou si $P_0 = (z+1)^2$:

Dans ce cas le produit des polynômes $eP_1\theta^2 + 4z(z+2)^2\psi^2$ et $e\theta^2 + 4zP_2\psi^2$ est $-de\mu^2$ et leur pgcd est un carré, donc il existe $s \in k^*$, μ_1, $\mu_2 \in k[z]$ tels que :

$$\begin{cases} eP_1\theta^2 + 4z(z+2)^2\psi^2 &= s\mu_1^2 & (1) \\ e\theta^2 + 4zP_2\psi^2 &= -des\mu_2^2 & (2) \end{cases}$$

Dans (1), pour $z = 0$, $eP_1(0)\theta^2(0) = s\mu_1^2(0)$ avec $\theta(0) \neq 0$ sinon z serait un facteur commun à θ et à ψ, donc $s \sim eP_1(0)$ c'est-à-dire $\boxed{s \sim e(2-r)}$.

D'autre part, pour $z = -2$, on a $eP_1(-2)\theta^2(-2) = s\mu_1^2(-2)$, si ces termes étaient non nuls, on aurait $s \sim eP_1(-2)$ c'est-à-dire $s \sim er$, on en déduirait que $r \sim (2-r)$.

Il va alors falloir rajouter la condition suivante sur le paramètre r : on va supposer que $r(2-r)$ n'est pas un carré dans $k = \mathbb{Q}(r)$.

Avec cette hypothèse, on ne pas avoir $r \sim (2-r)$ et cela implique que $eP_1(-2)\theta^2(-2) = s\mu_1^2(-2) = 0$ et donc que $\theta(-2) = 0$. Alors pour $z = -2$ dans (2), on obtient $-8P_2(-2)\psi^2(-2) = -des\mu_2^2(-2)$ et $\psi(-2) \neq 0$ car $\theta(-2) = 0$, donc $-2P_2(-2) \sim -des$ c'est-à-dire $2r \sim -des$. Mais pour $z = 0$ dans (2), on a $e\theta^2(0) = -des\mu_2^2(0)$ et on a déjà montré que $\theta(0) \neq 0$ donc $-des \sim e$, d'où $\boxed{2r \sim e}$.

D'autre part, dans (1), pour $z = z_1$, on a $4z_1(z_1+2)^2\psi^2(z_1) = s\mu_1^2(z_1)$ avec $\psi(z_1) \neq 0$ car z_1 est la racine de P_1 et annule donc f. On obtient $s \sim z_1$, mais comme on sait déjà que $s \sim e(2-r)$, on en déduit que $e \sim z_1(2-r)$ avec $z_1(2-r) = -\frac{(2-r)^2}{1-r}$ d'où $\boxed{e \sim -(1-r)}$.

Finalement, on a montré que $2r \sim e \sim (r-1)$ ce qui conduit à une contradiction de signe car $0 < r < 1$ et le corps k est réel.

Ainsi, il suffit de supposer que $r(2-r)$ n'est pas un carré dans $k = \mathbb{Q}(r)$ pour éliminer les cas $P_0 = 1$ et $P_0 = (z+1)^2$.

(ii) Si $P_0 = z$ ou si $P_0 = z(z+1)^2$:

Comme le pgcd des polynômes $e\theta^2 + 4z(z+2)\psi^2$ et $e(z+2)\theta^2 + 4zP_1P_2\psi^2$ est un multiple de z, on peut poser $\theta = z\theta'$ dans $k[z]$, on sait alors que $\psi(0) \neq 0$ et comme précédemment, il existe $s \in k^*$, μ_1, $\mu_2 \in k[z]$ tels que :

$$\begin{cases} ezP_1\theta'^2 + 4(z+2)^2\psi^2 &= s\mu_1^2 & (3) \\ ez\theta'^2 + 4P_2\psi^2 &= -des\mu_2^2 & (4) \end{cases}$$

Dans (4) on a, pour $z = 0$, $4P_2(0)\psi^2(0) = -des\mu_2^2(0) \neq 0$ donc $P_2(0) \sim -des$ c'est-à-dire $\boxed{-des \sim (2+r)}$. Toujours dans (4) pour $z = z_2$, on obtient $ez_2\theta'^2(z_2) = -des\mu_2^2(z_2)$ et $\theta'(z_2) \neq 0$ sinon P_2 diviserait à la fois θ et ψ, donc $-des \sim ez_2$, d'où $(2+r) \sim ez_2$. Or on a $z_2 = -\frac{2+r}{1+r}$, donc $\boxed{e \sim -(1+r)}$.

Dans (3), pour $z = 0$, on obtient $16\psi^2(0) = s\mu_1^2(0) \neq 0$ donc $\boxed{s \sim 1}$. D'autre part, pour $z = -2$, on a $-2eP_1(-2)\theta'^2(-2) = s\mu_1^2(-2)$ c'est-à-dire , comme $P_1(-2) = r$, $-2er\theta'^2(-2) = s\mu_1^2(-2)$.

Si on suppose que $\theta'(-2) \neq 0$, alors $s \sim -2er \sim 2r(1+r)$ et puisque $s \sim 1$, on a $2r(1+r) \sim 1$.

On va désormais ajouter la condition : $2r(1+r)$ n'est pas un carré dans k.

Cette hypothèse supplémentaire implique que $\theta(-2) = 0$. On pose alors $z = -2$ dans (4), ce qui donne $4P_2(-2)\psi^2(-2) = -des\mu_2^2(-2)$ et, comme $\theta'(-2) = 0$, on a alors $\psi^2(-2) \neq 0$. Ainsi $-des \sim P_2(-2)$ c'est-à-dire $-des \sim -r$. Comme on a aussi $-des \sim (2+r)$, cela donne $(2+r) \sim -r$ ce qui est impossible pour des raisons de signe.

Il suffit donc de rajouter la condition : " $2r(1+r)$ *n'est pas un carré dans* $\mathbb{Q}(r)$" pour que les cas $P_0 = z$ et $P_0 = z(z+1)^2$ ne puissent pas se produire.

(iii) Si $P_0 = z+1$:

Dans ce cas, il existe $s \in k^*$, μ_1, $\mu_2 \in k[z]$ tels que :

$$\begin{cases} eP_1\theta^2 + 4z(z+2)^2\psi^2 &= s(z+1)\mu_1^2 & (5) \\ e\theta^2 + 4zP_2\psi^2 &= -des(z+1)\mu_2^2 & (6) \end{cases}$$

Dans (5), pour $z = 0$, on a $eP_1(0)\theta^2(0) = s\mu_1^2(0)$ et ces termes sont non nuls donc $eP_1(0) \sim s$ c'est-à-dire $\boxed{e(2-r) \sim s}$.

D'autre part, pour $z = -2$, toujours dans (5), on a $eP_1(-2)\theta^2(-2) = -s\mu_1^2(-2)$ et donc, comme $P_1(-2) = r$, $er\theta^2(-2) = -s\mu_1^2(-2)$. Si on suppose que $\theta(-2) \neq 0$, on a alors $s \sim -er$ et donc on en déduit que $e(2-r) \sim -er$ d'où $(2-r) \sim -r$

ce qui est impossible car le premier terme est positif et le second est négatif. On a donc $\theta(-2) = 0$.

Dans (6), pour $z = 0$, on a $e\theta^2(0) = -des\mu_1^2(0) \neq 0$ donc $-des \sim e$, et pour $z = -2$, $-8P_2(-2)\psi^2(-2) = des\mu_2^2(-2) \neq 0$ donc $des \sim -2P_2(-2)$ c'est-à-dire $des \sim 2r$. Ainsi on obtient $\boxed{e \sim -des \sim -2r}$.

D'autre part, pour $z = z_1$, dans (5), $4z_1(z_1+2)^2\psi^2(z_1) = s(z_1+1)\mu_1^2(z_1)$ et ces termes sont non nuls sinon P_1 serait un facteur commun à θ et à ψ. On a donc $s(z_1+1) \sim z_1$ et comme $z_1 = -\frac{2-r}{1-r}$ et $(z_1+1) = \frac{-1}{1-r}$, alors on obtient $\boxed{s \sim (2-r)}$.

Enfin, étant donné que $e(2-r) \sim s$, $s \sim (2-r)$ implique que $e \sim 1$, on en déduit alors que $-2r \sim 1$ ce qui entraine une contradiction de signe.

On a donc prouvé qu'on ne peut pas avoir $P_0 = (z+1)$.

(iv) Si $P_0 = z(z+1)$:

Dans ce cas, on a $\theta(0) = 0$ et on peut poser $\theta = z\theta'$ dans $k[z]$, on sait alors que $\psi(0) \neq 0$ et qu'il existe $s \in k^*$, μ_1, $\mu_2 \in k[z]$ tels que :

$$\begin{cases} ezP_1\theta'^2 + 4(z+2)^2\psi^2 &= s(z+1)\mu_1^2 & (7) \\ ez\theta'^2 + 4P_2\psi^2 &= -des(z+1)\mu_2^2 & (8) \end{cases}$$

Dans (7), pour $z = 0$, on a $16\psi^2(0) = s\mu_1^2(0) \neq 0$ donc $s \sim 1$. D'autre part pour $z = z_1$ dans (7), on obtient $4(z_1+2)^2\psi^2(z_1) = s(z_1+1)\mu_1^2(z_1)$ et $\psi(z_1) \neq 0$ car $f(z_1) = 0$, d'où $s(z_1+1) \sim 1$ ce qui implique que $(z_1+1) \sim 1$ or $(z_1+1) = \frac{-1}{1-r} < 0$ on a alors une contradiction et il n'est pas possible d'avoir $P_0 = z(z+1)$.

Pour éliminer le cas $f = eP_1$, il aura donc fallu rajouter deux conditions : $r(2-r)$ et $2r(1+r)$ ne doivent pas être des carrés dans $\mathbb{Q}(r)$.

Cas (E4) : Si $\mathbf{f = e(z+2)P_1 = e(z+2)((1-r)z + (2-r))}$

L'équation de $\check{\mathcal{D}}_{k(z)}^{-d}$ donne ici :

$$-de(z+2)P_1\mu^2 = (e(z+2)P_1\theta^2 + 4z(z+2)^2\psi^2)(e(z+2)P_1\theta^2 + 4zP_1P_2\psi^2)$$

Et après simplification par $(z+2)P_1$, on a :

$$-de\mu^2 = (eP_1\theta^2 + 4z(z+2)\psi^2)(e(z+2)\theta^2 + 4zP_2\psi^2)$$

Il y a toujours quatre cas à distinguer suivant la valeur du pgcd P_0.

(i) Si $P_0 = 1$ ou si $P_0 = (z+1)^2$:

Dans ce cas, on a $\theta^2(0) \neq 0$ et il existe $s \in k^*$, μ_1, $\mu_2 \in k[z]$ tels que :

$$\begin{cases} eP_1\theta^2 + 4z(z+2)\psi^2 &= s\mu_1^2 & (1) \\ e(z+2)\theta^2 + 4zP_2\psi^2 &= -des\mu_2^2 & (2) \end{cases}$$

Dans (1), pour $z = 0$, on a $eP_1(0)\theta^2(0) = s\mu_1^2(0) \neq 0$, donc $s \sim eP_1(0)$ c'est-à-dire $s \sim e(2-r)$. D'autre part, pour $z = -2$ dans (1), on a $eP_1(-2)\theta^2(-2) = s\mu_1^2(-2)$ et ces termes sont non nuls sinon $(z+2)$ serait un facteur commun à θ et à ψ. On a donc $s \sim eP_1(-2)$ c'est-à-dire $s \sim er$, on en déduit alors que $r \sim (2-r)$.

Dans l'étude du cas (E3), on avait déjà supposé que $r(2-r)$ n'est pas un carré dans k, sous cette hypothèse, on obtient donc aussi une contradiction permettant de montrer qu'on ne peut avoir ni $P_0 = 1$ ni $P_0 = (z+1)^2$.

(ii) Si $P_0 = z$ ou si $P_0 = z(z+1)^2$:

Dans ce cas $\theta(0) = 0$ et on pose $\theta = z\theta'$ dans $k[z]$ on a aussi $\psi(0) \neq 0$ et il existe $s \in k^*$, μ_1, $\mu_2 \in k[z]$ tels que :

$$\begin{cases} ezP_1\theta'^2 + 4(z+2)\psi^2 &= s\mu_1^2 & (3) \\ ez(z+2)\theta'^2 + 4P_2\psi^2 &= -des\mu_2^2 & (4) \end{cases}$$

Dans (4), pour $z = 0$, on a $4P_2(0)\psi^2(0) = -des\mu_2^2(0) \neq 0$, donc $P_2(0) \sim -des$ c'est-à-dire $-des \sim (2+r)$. Toujours dans (4), pour $z = -2$, on obtient $4P_2(-2)\psi^2(-2) = -des\mu_2^2(-2)$ et comme $f(-2) = 0$, on a $\psi(-2) \neq 0$ donc $-des \sim P_2(-2)$ c'est-à-dire $-des \sim -r$. Comme on a montré que $-des \sim (2+r)$, on obtient alors que $(2+r) \sim -r$ ce qui amène une contradiction de signe : on ne peut donc avoir ni $P_0 = z$ ni $P_0 = z(z+1)^2$.

(iii) Si $P_0 = z+1$:

Dans ce cas on a $\theta(0) \neq 0$ et il existe $s \in k^*$, μ_1, $\mu_2 \in k[z]$ tels que :

$$\begin{cases} eP_1\theta^2 + 4z(z+2)\psi^2 &= s(z+1)\mu_1^2 & (5) \\ e(z+2)\theta^2 + 4zP_2\psi^2 &= -des(z+1)\mu_2^2 & (6) \end{cases}$$

Dans (5), pour $z = 0$, on a $eP_1(0)\theta^2(0) = s\mu_1^2(0) \neq 0$ donc $eP_1(0) \sim s$ c'est-à-dire $e(2-r) \sim s$. D'autre part, pour $z = -2$, toujours dans (5), on a $eP_1(-2)\theta^2(-2) = -s\mu_1^2(-2)$ et ces termes ne sont pas nuls sinon le polynôme $(z+2)$ diviserait à la fois θ et ψ, donc, comme $P_1(-2) = r$, on a $s \sim -er$. En regroupant ces résultats, on obtient $e(2-r) \sim s \sim -er$, donnant ainsi la relation

$(2-r) \sim -r$, ce qui est impossible pour des raisons de signe. On ne peut donc pas avoir $P_0 = z+1$.

(iv) Si $P_0 = z(z+1)$:

Dans ce cas $\theta(0) = 0$, $\psi(0) \neq 0$ et en posant $\theta = z\theta'$ dans $k[z]$, on sait qu'il existe $s \in k^*$, μ_1, $\mu_2 \in k[z]$ tels que :

$$\begin{cases} ezP_1\theta'^2 + 4(z+2)\psi^2 &= s(z+1)\mu_1^2 & (7) \\ ez(z+2)\theta'^2 + 4P_2\psi^2 &= -des(z+1)\mu_2^2 & (8) \end{cases}$$

Dans l'équation (7) :

* pour $z = 0$, on a $8\psi^2(0) = s\mu_1^2(0) \neq 0$ donc $s \sim 2$,
* pour $z = z_1$, $4(z_1+2)\psi^2(z_1) = s(z_1+1)\mu_1^2(z_1)$ et $\psi(z_1) \neq 0$ car $f(z_1) = 0$, donc $(z_1+2) \sim s(z_1+1)$ ce qui équivaut à $r \sim s$

On a alors $r \sim s \sim 2$ et il suffit de supposer que $2r$ n'est pas un carré dans le corps k pour que le cas $P_0 = z(z+1)$ devienne impossible.

Remarque 2.5.9 Pour éliminer cette dernière possibilité, il y a une autre méthode :

Dans l'équation (8) :

* pour $z = 0$, on a $4P_2(0)\psi^2(0) = -des\mu_2^2(0) \neq 0$ donc $-des \sim P_2(0) \sim (2+r)$,
* pour $z = -2$, on a $4P_2(-2)\psi^2(-2) = des\mu_2^2(-2) \neq 0$ donc $des \sim P_2(-2) \sim -r$.

On a alors $-des \sim r \sim (2+r)$ et en supposant que $r(2+r)$ n'est pas un carré dans le corps k le cas $P_0 = z(z+1)$ est exclu.

Ainsi, pour éliminer le dernier cas $f = e(z+2)P_1$, il suffit de rajouter l'une de ces deux conditions : *" $2r$ n'est pas un carré dans le corps k"* ou *" $r(2+r)$ n'est pas un carré dans le corps k"*.

Pour traiter le cas (E4), il suffit donc de supposer que $r(2-r)$ n'est pas un carré dans le corps k et que l'un des deux termes $2r$ ou $r(2+r)$ n'est pas non plus un carré dans le corps k.

On a donc démontré que l'image du morphisme $\check{\gamma}_{\mathcal{D}}$ est l'image des points de torsion lorsque $(4-r^2)(1-r^2)$, $(4-r^2)$, $r(2-r)$ et $2r(1+r)$ ne sont des carrés

dans le corps $\mathbb{Q}(r)$ *et que l'un des deux termes* $2r$ *ou* $r(2+r)$ *n'est pas un carré dans le corps* $\mathbb{Q}(r)$.

(F) Synthèse des résultats

On a donc dans les parties (B), (C), (D) et (E) trouvé des conditions suffisantes sur le réel $0 < r < 1$ pour que la courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ n'ait pas de point spécial bien que sa fibration sur $\mathbb{P}^1(\mathbb{R})$ ne présente aucune singularité, cela se produit lorsque :

- les éléments $(1-r^2)$, $(4-r^2)$, $(4-r^2)(1-r^2)$, $r(2-r)$ et $2r(1+r)$ ne sont des carrés dans le corps $\mathbb{Q}(r)$,
- soit $2r$, soit $r(2+r)$ n'est pas un carré dans le corps $\mathbb{Q}(r)$.

Sous ces conditions, le polynôme $F(x,y) = (y^2+(x^2+2)^2)(y^2+(x^2+2)^2-r^2(x^2+1)^2)$ est positif mais n'est pas une somme de 3 carrés de fractions rationnelles.

Remarque 2.5.10 Il est très simple de trouver des valeurs réelles du paramètre r vérifiant les conditions ci-dessus : il suffit de prendre r transcendant.

Chapitre 3

Polynômes de haut degré et polynômes de degré 4

Ce chapitre comporte deux sections indépendantes. Dans la section 3.1, on donnera une méthode permettant d'obtenir des polynômes positifs de $\mathbb{R}[x,y]$ de degré aussi grand que souhaité et qui ne sont pas sommes de 3 carrés de fractions rationnelles. La section 3.2 consiste en une étude de la forme de certains points spéciaux des courbes elliptiques associées aux polynômes $(y^2+a(x))(y^2+b(x))$ lorsque a et b sont positifs et de degré 4, l'existence de points spéciaux sur ces courbes elliptiques étant une conséquence directe du résultat démontré par Hilbert [Hi1] : en degré 4, tout polynôme positif ou nul est somme de 3 carrés dans $\mathbb{R}[x,y]$.

3.1 Polynômes de grand degré

Colliot-Thélène a démontré dans [CT] l'existence en tout degré supérieur ou égal à 6 de polynômes positifs qui ne sont pas somme de 3 carrés dans $\mathbb{R}(x,y)$, ces polynômes doivent en particulier vérifier la propriété d'avoir tous leurs coefficients algébriquement indépendants. On va dans cette section donner une méthode permettant d'obtenir explicitement, et sans cette condition sur les coefficients, des polynômes positifs de degré aussi élevé que souhaité qui ne sont pas somme de 3 carrés de fractions rationnelles. Pour cela il suffit de connaître un polynôme $F(x,y)$ positif qui n'est pas somme de 3 carrés dans $\mathbb{R}(x,y)$, par exemple le polynôme de Motzkin ou l'un des polynômes étudiés dans les chapitres précédents, et de substituer à l'indéterminée x un polynôme $P(x,y)$ de degré impair en x.

Pour démontrer ce résultat, il faut d'abord prouver le lemme suivant :

Lemme 3.1.1 *Soit $P(x,y)$ un polynôme de $\mathbb{R}[x,y]$ de degré d impair en x, si on note $t = P(x,y)$, alors $\mathbb{R}(x,y)$ est une extension algébrique finie, de degré d, du corps $\mathbb{R}(t,y)$.*

Preuve. On pose $P(x) = \sum_{k=0}^{d} a_k(y)x^k$, avec pour $0 \leq k \leq d$, $a_k(y) \in \mathbb{R}[y]$ et $a_d(y) \neq 0$.

Comme $t = P(x,y)$, il est évident que t est transcendant sur $\mathbb{R}(y)$ et que $\mathbb{R}(t,y) \subset \mathbb{R}(x,y)$. De plus on a aussi $t = \sum_{k=0}^{d} a_k(y)x^k$, ce qui donne la relation $a_d(y)x^d + ...a_1(y)x + a_0(y) - t = 0$ prouvant que x est algébrique sur $\mathbb{R}(t,y)$.

Pour démontrer que $[\mathbb{R}(x,y) : \mathbb{R}(t,y)] = d$, il reste donc à prouver que le polynôme $M(Z) = a_d(y)Z^d + a_{d-1}(y)Z^{d-1} + \cdots + a_1(y)Z + a_0(y) - t \in \mathbb{R}(t,y)[Z]$ est le polynôme minimal de x sur $\mathbb{R}(t,y)$, pour cela, il suffit de montrer qu'il est irréductible sur $\mathbb{R}(t,y)$. Tout d'abord on remarque que $M(Z)$ est irréductible dans $\mathbb{R}(y)[t][Z]$: c'est évident car c'est un polynôme en deux variables t et Z, à coefficients dans $\mathbb{R}(y)$, de degré 1 et unitaire en la variable t, de plus, $\mathrm{pgcd}_{\mathbb{R}(y)[t]}(a_d(y), a_{d-1}(y), \cdots, a_1(y), a_0(y) - t) = 1$, il en résulte que $M(Z)$ est irréductible dans $\mathbb{R}(y)(t)[Z]$ et c'est donc bien le polynôme minimal de x sur $\mathbb{R}(t,y)$.

Ainsi x est un élément algébrique de degré d sur $\mathbb{R}(t,y)$ et le corps $\mathbb{R}(x,y)$ est bien une extension algébrique de degré d de $\mathbb{R}(t,y)$. □

On peut maintenant démontrer que :

Théorème 3.1.2 *Soit $F(x,y) \in \mathbb{R}[x,y]$ un polynôme positif qui n'est pas somme de 3 carrés dans $\mathbb{R}(x,y)$. Soit $P(x,y)$ un polynôme de $\mathbb{R}[x,y]$ de degré impair en x, alors le polynôme $F(P(x,y),y)$ est aussi positif et n'est pas non plus somme de 3 carrés dans $\mathbb{R}(x,y)$.*

Preuve. Il est évident que si $F(x,y)$ est positif, alors $F(P(x,y),y)$ est aussi un polynôme positif.

Supposons maintenant que $F(P(x,y),y)$ soit une somme de 3 carrés dans $\mathbb{R}(x,y)$ c'est-à-dire que $F(t,y) = u^2 + v^2 + w^2$, avec u, v, $w \in \mathbb{R}(x,y)$, la forme quadratique $\Phi =< 1,1,1,-F >$ définie sur le corps $\mathbb{R}(t,y)$ serait donc isotrope sur $\mathbb{R}(x,y)$ car elle est annulée par $(u,v,w,1)$. Or d'après le lemme précédent, le corps $\mathbb{R}(x,y)$ est une extension algébrique de degré impair de $\mathbb{R}(t,y)$, et le théorème de Springer impliquerait que Φ soit aussi isotrope sur $\mathbb{R}(t,y)$.

Etant donné que la forme quadratique $< 1,1,1 >$ est anisotrope sur $\mathbb{R}(t,y)$, cela donnerait une représentation de $F(t,y)$ comme somme de 3 carrés dans

$\mathbb{R}(t,y)$, ce qui est impossible : t étant transcendant sur $\mathbb{R}(y)$, par hypothèse, $F(t,y)$ n'est pas somme de 3 carrés dans $\mathbb{R}(t,y)$. □

On peut déduire de ce théorème les résultats suivants :

Corollaire 3.1.3 *Soit $F(x,y) \in \mathbb{R}[x,y]$ un polynôme positif qui n'est pas somme de 3 carrés dans $\mathbb{R}(x,y)$. Soit $Q(x,y)$ un polynôme de $\mathbb{R}[x,y]$ de degré impair en y, alors le polynôme $F(x,Q(x,y))$ est aussi positif et n'est pas non plus somme de 3 carrés dans $\mathbb{R}(x,y)$.*

Preuve. Il suffit d'intervertir les rôles des variables x et y. □

Dans le cas particulier où l'on considère des polynômes P et Q ne dépendant que d'une seule variable, respectivement x et y, on obtient :

Corollaire 3.1.4 *Soit $F(x,y) \in \mathbb{R}[x,y]$ un polynôme positif qui n'est pas somme de 3 carrés dans $\mathbb{R}(x,y)$. Soient $P(x) \in \mathbb{R}[x]$ de degré impair et $Q(y) \in \mathbb{R}[y]$ de degré impair, alors le polynôme $F(P(x),Q(y))$ est positif et n'est pas somme de 3 carrés dans $\mathbb{R}(x,y)$.*

Preuve. D'après le théorème 3.1.2, $F(P(x),y)$ n'est pas somme de 3 carrés dans $\mathbb{R}(x,y)$, pour terminer la démonstration de ce corollaire, il suffit d'appliquer le même raisonnement à $G(x,y) = F(P(x),y)$ pour montrer que le polynôme $G(x,Q(y)) = F(P(x),Q(y))$ n'est pas somme de 3 carrés dans $\mathbb{R}(x,y)$. □

On en déduit aisément que :

Corollaire 3.1.5 *Il existe dans $\mathbb{R}[x,y]$ des polynômes positifs de degrés en x et en y aussi élevés que souhaité qui ne sont pas somme de 3 carrés dans $\mathbb{R}(x,y)$.*

Preuve. Pour obtenir des polynômes positifs de degrés en x et en y aussi élevé que souhaité, il suffit de partir d'un polynôme positif non somme de 3 carrés connu et de substituer $P(x)$ à x et $Q(y)$ à y avec P et Q polynômes en une variable de degrés assez grands. □

3.2 Etude générale de $(y^2+a(x))(y^2+b(x))$ lorsque a et b sont positifs de degré au plus 2

Hilbert a démontré dans [Hil] qu'un polynôme $F(x,y)$ de degré total inférieur ou égal à 4 est somme de 3 carrés dans $\mathbb{R}[x,y]$. Il est alors évident qu'une courbe

elliptique associée à un tel polynôme admet au moins un point spécial. Le but de cette section est de produire une forme explicite pour un de ces points spéciaux dans le cas où le polynôme $F(x,y)$ se factorise sous la forme $(y^2+P_1(x))(y^2+P_2(x))$ avec P_1 et P_2 polynômes de $\mathbb{R}[x]$ positifs de degrés inférieurs ou égaux à 2. Cela permettra de donner, sur des exemples numériques, une expression non triviale de F comme somme de trois carrés de polynômes.

Il faut d'abord remarquer que si $P_1 = P_2$ ou si P_1 et P_2 sont tous les deux des carrés dans $\mathbb{R}[x]$, alors $F(x,y)$ s'écrit de manière évidente comme carré ou somme de 2 carrés dans $\mathbb{R}[x]$ et dans ces cas, un des points spéciaux de la courbe elliptique associée à ce polynôme est directement donné par la preuve du théorème 1.1.1. On posera donc comme hypothèse que $P_1 \neq P_2$ et que P_1 n'est pas un carré dans $\mathbb{R}[x]$. Dans ce cas, l'écriture de $F(x,y)$ comme somme de 3 carrés n'apparaît pas, en général, de manière triviale. Afin d'alléger les notations et de limiter le nombre de paramètres, on va supposer, quitte à effectuer un changement de variable affine, que $P_1(x) = x^2+1$, on pose alors $P_2(x) = ax^2+bx+c$, avec a, b et $c \in \mathbb{R}$. Pour que P_2 soit positif, on supposera que $a \geq 0$ et $b^2-4ac \leq 0$.

Proposition 3.2.1 *Si le polynôme $F(x,y) = (y^2+P_1(x))(y^2+P_2(x))$ est positif ou nul et de degré inférieur ou égal à 4, alors il y a un point spécial, défini sur l'anneau $\mathbb{R}[x]$, sur la courbe $\mathcal{C}^{-1} : -\beta^2 = \alpha(\alpha^2 - 2(P_1+P_2)\alpha + (P_1-P_2)^2)$.*

Preuve. Il suffit de reprendre la démonstration du théorème 1.1.1, en notant d'abord que d'après le résultat montré par Hilbert, le polynôme $F(x,y)$ est somme de 3 carrés dans $\mathbb{R}[x,y]$ c'est-à-dire :

$$F(x,y) = y^4 + (P_1(x)+P_2(x))y^2 + P_1(x)P_2(x) = \sum_{i=1}^{3}(a_iy^2+b_iy+c_i)^2$$

où, pour $i = 1, 2, 3$, les termes a_i, b_i et c_i sont des éléments de $\mathbb{R}[x]$.

On a donc $a_1^2+a_2^2+a_3^2 = 1$, d'où pour $i = 1, 2, 3$, on a $\deg(a_i) = 0$ c'est-à-dire $a_i \in \mathbb{R}$. Ainsi l'une des transformations orthogonales de $\mathbb{R}(x)^3$ qui transforment le vecteur (a_1, a_2, a_3) en $(1, 0, 0)$ est définie sur $\mathbb{R}$, en effet on rappelle que l'on peut prendre pour cette transformation celle qui à tout $(u, v, w) \in \mathbb{R}(x)^3$ associe ;

$$h(u,v,w) = \left(u - 2(a_1-1)\frac{(a_1-1)u+a_2v+a_3w}{(a_1-1)^2+a_2^2+a_3^2}, v - 2a_2\frac{(a_1-1)u+a_2v+a_3w}{(a_1-1)^2+a_2^2+a_3^2},\right.$$

$$\left. w - 2a_3\frac{(a_1-1)u+a_2v+a_3w}{(a_1-1)^2+a_2^2+a_3^2}\right).$$

Comme, pour $i = 1, 2, 3$, b_i et c_i sont des éléments de $\mathbb{R}[x]$, on constate alors que les images par h des vecteurs (b_1, b_2, b_3) et (c_1, c_2, c_3) sont aussi des éléments de $\mathbb{R}[x]^3$.

De même que dans la démonstration du théorème 1.1.1, en posant $\alpha = b_2^2 + b_3^2$ et $\beta = 2(b_2c_3 + b_3c_2)$, on obtient un point spécial sur la courbe elliptique $\mathcal{C}^{-1}$ d'équation $-\beta^2 = \alpha(\alpha^2 - 2(P_1 + P_2)\alpha + (P_1 + P_2)^2 - 4P_1P_2)$, mais de plus ici, pour $i = 2$ et 3, b_i et c_i sont des polynômes de $\mathbb{R}[x]$, ce point spécial est donc à coordonnées polynomiales. □

Remarque 3.2.2 Si $P_2 = ax^2 + a = aP_1$ avec $a \in \mathbb{R}^{*+}$ alors la courbe $\mathcal{C}^{-1}$ a pour équation $-\beta^2 = \alpha(\alpha - (1 + a + 2\sqrt{a})P_1)(\alpha - (1 + a - 2\sqrt{a})P_1)$ et on a des points d'ordre 2, $\mathcal{P}_1 = ((1 + \sqrt{a})^2P_1, 0)$ et $\mathcal{P}_2 = ((1 - \sqrt{a})^2P_1, 0)$, qui sont spéciaux.

En revanche, lorsque P_2 n'est pas de la forme aP_1 avec $a \in \mathbb{R}^{*+}$, le seul point d'ordre 2 défini sur $\mathbb{R}(x)$ est $\mathcal{P}_\mathcal{C} = (0, 0)$ car alors P_1P_2 n'est pas un carré dans $\mathbb{R}[x]$. De plus ce point $(0, 0)$ n'est jamais spécial étant donné que $-(P_1 - P_2)^2$ n'est clairement pas somme de 2 carrés dans $\mathbb{R}(x)$.

On supposera donc que P_2 n'est pas le produit de P_1 par un réel positif a, c'est-à-dire que $a \neq c$ ou $b \neq 0$. Cela permettra de s'assurer que le point spécial (α, β) recherché n'est pas d'ordre 2 et qu'il vérifie $\beta \neq 0$. En suivant la démarche du lemme 1.5.13, on montre que :

Lemme 3.2.3 *Pour ce point spécial (α, β), on peut écrire $\alpha = f\theta^2$, avec f, $\theta \in \mathbb{R}[x]^*$ et où f est un polynôme positif sans facteur carré qui divise $P_1 - P_2$.*

Preuve. D'après le lemme 1.5.13, on peut écrire $\alpha = f\frac{\theta^2}{\psi^2}$, avec f, θ, $\psi \in \mathbb{R}[x]^*$ et f sans facteur carré. Comme ce point est $\mathbb{R}[x]$-rationnel, on peut supposer que $\psi = 1$. La positivité de f découle directement de celle de α qui est somme de deux carrés dans $\mathbb{R}[x]$.

Enfin, comme $-\beta^2 = f\theta^2(f^2\theta^4 - 2(P_1 + P_2)f\theta^2 + (P_1 - P_2)^2)$, après simplification, il existe un polynôme $\mu \in \mathbb{R}[x]$ tel que :

$$-f\mu^2 = f^2\theta^4 - 2(P_1 + P_2)f\theta^2 + (P_1 - P_2)^2.$$

On en déduit immédiatement que f divise $(P_1 - P_2)^2$, étant sans facteur carré, f divise $P_1 - P_2$. □

La forme du point spécial recherché va donc dépendre de celle du polynôme $P_1 - P_2 = (1 - a)x^2 - bx - (1 - c)$, en particulier du nombre de facteurs dans $\mathbb{R}[x]$

de ce dernier polynôme. C'est pourquoi on est amené à étudier les différents cas suivant le degré de $P_1 - P_2$:

(A) Le polynôme $P_1 - P_2$ est une constante non nulle c'est-à-dire $a = 1$, $b = 0$ et $c \neq 1$.

(B) Le polynôme $P_1 - P_2$ est de degré 1 c'est-à-dire $a = 1$ et $b \neq 0$.

(C) Le polynôme $P_1 - P_2$ est de degré 2 et n'est pas irréductible sur $\mathbb{R}[x]$, c'est-à-dire $a \neq 1$ et $\delta = \text{discr}(P_1 - P_2) = b^2 - 4(1-a)(1-c) \geq 0$.

(D) Le polynôme $P_1 - P_2$ est de degré 2 et est irréductible sur $\mathbb{R}[x]$ c'est-à-dire $a \neq 1$ et $\delta = b^2 - 4(1-a)(1-c) < 0$.

Remarque 3.2.4 Pour la suite, il est intéressant de remarquer que si (α, β) est un point spécial de $\mathcal{C}^{-1}_{\mathbb{R}(x)}$, comme $\mathcal{P}_\mathcal{C} \in \ker(\gamma_c)$, alors $(\alpha, \beta) + \mathcal{P}_\mathcal{C}$ est un autre point spécial de $\mathcal{C}^{-1}$ et sa première coordonnée est $\alpha' = \frac{(P_1 - P_2)^2}{\alpha}$. Il est évident que lorsque α divise $P_1 - P_2$, ce deuxième point spécial est aussi $\mathbb{R}[x]$-rationnel.

(A) $\mathbf{P_1 - P_2}$ est de degré 0

Dans ce cas, d'après la proposition 3.2.3, le polynôme f est une constante positive et on peut supposer que $f = 1$, donc $\alpha = \theta^2$. On a alors d'après l'équation de $\mathcal{C}^{-1}$, $\theta^4 - 2(P_1 + P_2)\theta^2 + (P_1 - P_2)^2 = -\mu^2$ et l'étude du signe des coefficients dominants dans cette dernière égalité montre que le degré de θ doit être inférieur ou égal à 1. Mais si $\deg(\theta) = 1$, il existe $x_0 \in \mathbb{R}$ tel que $\theta(x_0) = 0$, on aurait alors $-\mu^2(x_0) = (P_1 - P_2)^2(x_0) = (1 - c^2)^2 \neq 0$ ce qui est impossible. Donc lorsque $P_1 - P_2$ est de degré 0 et est non nul, alors il existe un point spécial dont la première coordonnée est de la forme $\alpha = m \in \mathbb{R}^{*+}$.

On recherche maintenant la valeur de m :

Dans l'équation de la courbe $\mathcal{C}^{-1}$, avec $\alpha = m > 0$, on doit alors avoir :

$$m^2 - 2(P_1 + P_2)m + (P_1 - P_2)^2 = -\mu^2.$$

Or on a $P_1 = x^2 + 1$ et $P_2 = x^2 + c$, ce qui donne la relation $m^2 - 2(2x^2 + 1 + c)m + (1 - c)^2 = -\mu^2$ et on en déduit que :

$$-4mx^2 + \left(m^2 - 2(1 + c)m + (1 - c)^2\right) = -\mu^2.$$

Mais, puisque $m \neq 0$, le polynôme $-4mx^2 + (m^2 - 2(1+c)m + (1-c)^2)$ sera l'opposé d'un carré dans $\mathbb{R}[x]$ si et seulement si $m^2 - 2(1+c)m + (1-c)^2 = 0$ c'est-à-dire $m = 1+c \pm 2\sqrt{c} = (1 \pm \sqrt{c})^2$. On a ainsi les premières coordonnées de points spéciaux de $\mathcal{C}^{-1}$ dans le cas où $P_1 - P_2$ est de degré 0. En choisissant $\alpha = (1+\sqrt{c})^2$ et en substituant dans l'équation de $\mathcal{C}^{-1}$, on obtient $\beta = \pm 2(1+\sqrt{c})^2 x$. On pose, en reprennant les notations du théorème 1.1.1 :

* $b_2 = 1 + \sqrt{c}$ et $b_3 = 0$,
* $c_1 = \frac{1}{2}(A - \alpha) = x^2 - \sqrt{c}$,
* $c_2 = \frac{\beta}{2\alpha} b_3 = 0$ et $c_3 = -\frac{\beta}{2\alpha} b_2 = (1+\sqrt{c})x$.

Cela donne la relation :

$$(y^2 + x^2 + 1)(y^2 + x^2 + c) = (y^2 + x^2 - \sqrt{c})^2 + ((1+\sqrt{c})y)^2 + ((1+\sqrt{c})x)^2.$$

(B) $P_1 - P_2$ est de degré 1

Comme f est positif et divise $P_1 - P_2$, alors ce polynôme est constant et on peut supposer que $f = 1$ d'où $\alpha = \theta^2$ et l'étude du signe des coefficients dominants prouve que $\deg(\theta) \leq 1$.

Ainsi le point spécial recherché a une première coordonnée qui est soit de la forme $\alpha = m \in \mathbb{R}^{*+}$, soit de la forme $\alpha' = \theta^2$, avec $\deg(\theta) = 1$. Dans ce second cas, $\deg(\theta) = 1$ donc le polynôme θ s'annule en une valeur réelle x_0 et on a $(P_1 - P_2)^2(x_0) = -\mu^2(x_0)$, d'où $(P_1 - P_2)^2(x_0) = 0$ et θ divise $P_1 - P_2$ qui est irréductible car de degré 1, donc cela donne $\alpha' = m'(P_1 - P_2)^2$, $m' \in \mathbb{R}^{*+}$.

D'après la remarque 3.2.4, on vérifie aisément que chaque point spécial dont la première coordonnée est de la forme $\alpha' = m'(P_1 - P_2)^2$ peut se déduire d'un point spécial dont la première coordonnée α est une constante m en lui ajoutant $\mathcal{P}_{\mathcal{C}}$ et on a $\alpha = \frac{(P_1 - P_2)^2}{\alpha'}$, les réels m et m' sont donc liés par la relation $m = \frac{1}{m'}$. On peut donc se contenter de rechercher les points spéciaux dont la première coordonnée est une constante $m > 0$.

Recherche de la valeur de m :

On a ici $P_1 = x^2+1$ et $P_2 = x^2+bx+c$ avec $b^2-4c \leq 0$, donc si on pose $\alpha = m > 0$ dans l'équation de $\mathcal{C}^{-1}$, on obtient : $m^2-2(2x^2+bx+1+c)m+(bx+c-1)^2 = -\mu^2$ ce qui donne :

$$(b^2-4m)x^2 + 2b(c-1-m)x + (m^2-2(1+c)m+(1-c)^2) = -\mu^2.$$

Il faut donc que le discriminant de ce polynôme de degré 2 en x soit nul c'est-à-dire que $b^2(c-1-m)^2 - (b^2-4m)(m^2-2(1+c)m+(1-c)^2) = 0$, ou encore :

$$m^3 - 2(1+c)m^2 + (b^2+(1-c)^2)m = 0$$

Comme $m > 0$, on a $m^2 - 2(1+c)m + (b^2+(1-c)^2) = 0$, et donc, comme le discriminant réduit de ce polynôme de degré 2 en m est $(1+c)^2-(b^2+(1-c)^2) = 4c-b^2 > 0$, on a $m = c+1 \pm \sqrt{4c-b^2}$.

On vérifie que la constante m trouvée est strictement positive : on a bien $c+1\pm\sqrt{4c-b^2} > 0$ car $c+1 > \sqrt{4c-b^2}$ étant donné que ces termes sont positifs et que $(c+1)^2-(4c-b^2) = (c-1)^2+b^2 > 0$. Il reste maintenant à s'assurer qu'on a effectivement trouvé un point de la courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$, en effet pour ces valeurs de m, le discriminant de $(b^2-4m)x^2+2b(c-1-m)x+(m^2-2(1+c)m+(1-c)^2)$ est nul donc ce polynôme est, dans $\mathbb{R}[x]$, soit un carré, soit l'opposé d'un carré et seul ce second cas fournit un point sur $\mathcal{C}^{-1}_{\mathbb{R}(x)}$. On va pour cela calculer b^2-4m : on a $b^2-4m = b^2-4c-4\pm 4\sqrt{4c-b^2}$ et en posant $t = \sqrt{4c-b^2} \geq 0$, on obtient $b^2-4m = -t^2 \pm 4t - 4 = -(t\pm 2)^2$:

* Si $t \neq 2$, alors $t \pm 2 \neq 0$ et $b^2-4m < 0$ donc le polynôme $(b^2-4m)x^2 + 2b(c-1-m)x+(m^2-2(1+c)m+(1-c)^2)$ est bien l'opposé d'un carré dans $\mathbb{R}[x]$.

* Si $t = 2$, pour $m = c+1+\sqrt{4c-b^2}$ on a $b^2-4m = -(t+2)^2 < 0$ et donc cela donne bien un point spécial sur $\mathcal{C}^{-1}$. Pour $m = c+1-\sqrt{4c-b^2}$, on a $b^2-4m = -(t-2)^2 = 0$, dans ce cas, comme $t = 2$, on a aussi $b^2 = 4(c-1)$ et on $m = c-1$, le polynôme $(b^2-4m)x^2+2b(c-1-m)x+(m^2-2(1+c)m+(1-c)^2)$ est alors égal à $m^2-2(1+c)m+(1-c)^2 = -4(c-1) = -b^2 < 0$ et est effectivement l'opposé d'un carré dans $\mathbb{R}[x]$.

On a donc trouvé des valeur réelles $m = c+1\pm\sqrt{4c-b^2}$ qui sont toujours les premières coordonnées de points spéciaux de $\mathcal{C}^{-1}_{\mathbb{R}(x)}$, on en déduit aussi d'autres points spéciaux dont les les premières coordonnées sont de la forme $\alpha' = \frac{1}{m}(P_1-P_2)^2$ c'est-à-dire $\alpha = \frac{(bx+c-1)^2}{c+1\pm\sqrt{4c-b^2}}$.

Exemple

On va traiter le cas où $a = 1$, $b = 2$ et $c = 5$, c'est-à-dire $F(x, y) = (y^2 + x^2 + 1)(y^2 + x^2 + 2x + 5)$. La courbe $\mathcal{C}^{-1}$ a alors pour équation : $-\beta^2 = \alpha(\alpha^2 - 2(2x^2 + 2x + 6)\alpha + (2x + 4)^2)$.

Comme $4c - b^2 = 16$, les points spéciaux obtenus avec les formules données ci-dessus ont pour premières coordonnées $\alpha = 2$, $\alpha = 10$, $\alpha = 2(x - 2)^2$ et $\alpha = \frac{2}{5}(x - 2)^2$. En choisissant $\alpha = 2$, on obtient la seconde coordonnée $\beta = \pm 2\sqrt{2}(x - 1)$. On peut donc poser, en reprennant les notations du théorème 1.1.1 :

* $b_2 = \sqrt{2}$ et $b_3 = 0$,
* $c_1 = \frac{1}{2}(A - \alpha) = x^2 + x + 2$,
* $c_2 = \frac{\beta}{2\alpha} b_3 = 0$ et $c_3 = -\frac{\beta}{2\alpha} b_2 = x - 1$.

Cela donne la relation :

$$(y^2 + x^2 + 1)(y^2 + x^2 + 2x + 5) = (y^2 + x^2 + x + 2)^2 + (\sqrt{2}y)^2 + (x - 1)^2.$$

(C) $P_1 - P_2$ est de degré 2 et n'est pas irréductible

On rappelle que dans ce cas on a $a \neq 1$ et $\delta = \mathrm{discr}(P_1 - P_2) = b^2 - 4(1 - a)(1 - c) > 0$ et $P_1 - P_2$ est scindé sur $\mathbb{R}$, on pose $P_1 - P_2 = UV$ dans $\mathbb{R}[x]$.

Comme le polynôme f divise $P_1 - P_2$ et est positif, alors il est constant, on peut donc supposer que $f = 1$. Ainsi la première coordonnée du point spécial recherché est de la forme $\alpha = \theta^2$ et on a $\theta^4 - 2(P_1 + P_2)\theta^2 + (P_1 - P_2)^2 = -\mu^2$ dans $\mathbb{R}[x]$. L'étude du signe des coefficients dominants indique que $\deg(\theta) = 1$, donc θ admet une racine réelle x_0 qui vérifie alors $(P_1 - P_2)^2(x_0) = -\mu^2(x_0)$. On doit ainsi avoir $(P_1 - P_2)(x_0) = 0$ d'où θ divise $P_1 - P_2$ et on peut donc écrire la première coordonnée du point spécial recherché sous la forme $\alpha = mU^2$ ou $\alpha' = m'V^2$, avec m, $m' \in \mathbb{R}^{*+}$.

D'après la remarque 3.2.4, chaque point de première coordonnée $\alpha' = m'V^2$ se déduit d'un point tel que $\alpha = mU^2$ en ajoutant $\mathcal{P}_\mathcal{C}$ et comme $\alpha' = \frac{(P_1 - P_2)^2}{\alpha} = \frac{U^2V^2}{mU^2}$, on a la relation $m' = \frac{1}{m}$. On se contentera donc de rechercher les points spéciaux de première coordonnée $\alpha = mU^2$.

Recherche des valeurs de m :

On a $P_1 = x^2 + 1$ et $P_2 = ax^2 + bx + c$ avec $b^2 - 4ac < 0$ et $\delta = b^2 - 4(1-a)(1-c) \geq 0$, cela donne $P_1 - P_2 = (1-a)x^2 - bx + (1-c)$. On va écrire $P_1 - P_2$ comme produit de deux polynômes U et V :

$$P_1 - P_2 = \left((1-a)x - \frac{b+\sqrt{\delta}}{2}\right)\left(x - \frac{b-\sqrt{\delta}}{2(1-a)}\right)$$

On peut donc prendre $U = (1-a)x - \frac{b+\sqrt{\delta}}{2}$ et $V = x - \frac{b-\sqrt{\delta}}{2(1-a)}$ et on cherchera des points tels que $\alpha = mU^2 = m\left((1-a)x - \frac{b+\sqrt{\delta}}{2}\right)^2$ avec $m > 0$.

Il existe un polynôme $\mu \in \mathbb{R}[x]$ tel que $m^2U^4 - 2(P_1+P_2)mU^2 + (P_1-P_2)^2 = -\mu^2$ et comme $P_1 - P_2 = UV$, alors U^2 divise μ^2 et on peut poser $\mu = \mu' U$ avec $\mu' \in \mathbb{R}[x]$ d'où la relation :

$$m^2U^2 - 2(P_1+P_2)m + V^2 = -\mu'^2,$$

ce qui donne que $-\mu'^2$ est égal à :

$$m^2\left((1-a)x - \frac{b+\sqrt{\delta}}{2}\right)^2 - 2\left((1+a)x^2 + bx + (1+c)\right)m + \left(x - \frac{b-\sqrt{\delta}}{2(1-a)}\right)^2.$$

Après regroupement suivant les puissances de x, le terme suivant doit être égal à $-\mu'^2$:

$$\left((1-a)^2m^2 - 2(1+a)m + 1\right)x^2 + \left((a-1)(b+\sqrt{\delta})m^2 - 2bm - \frac{b-\sqrt{\delta}}{1-a}\right)x + \cdots$$
$$\cdots + \left(\frac{(b+\sqrt{\delta})^2}{4}m^2 - 2(1+c)m + \frac{(b-\sqrt{\delta})^2}{4(1-a)^2}\right).$$

Le discriminant de ce polynôme en x doit donc être nul c'est-à-dire , après calculs :

$$\left(2(1-a)(c-a) + b^2 + b\sqrt{\delta}\right)m^3 - 4(a+c)m^2 + \frac{2(1-a)(c-a) + b^2 - b\sqrt{\delta}}{(1-a)^2}m = 0.$$

Comme $m \neq 0$, on doit donc avoir :

$$\left(2(1-a)(c-a) + b^2 + b\sqrt{\delta}\right)m^2 - 4(a+c)m + \frac{2(1-a)(c-a) + b^2 - b\sqrt{\delta}}{(1-a)^2} = 0.$$

Le discriminant de ce polynôme de degré 2 en m est :

$$16(a+c)^2 - 4\left(2(1-a)(c-a) + b^2 + b\sqrt{\delta}\right)\left(\frac{2(1-a)(c-a) + b^2 - b\sqrt{\delta}}{(1-a)^2}\right)$$

Après simplifications, on trouve que ce terme est égal à $16(4ac - b^2)$ et donc ce discriminant est, d'après les hypothèses, positif ce qui implique que :

$$m = \frac{2(a+c) \pm 2\sqrt{4ac - b^2}}{2(1-a)(c-a) + b^2 + b\sqrt{\delta}} \ .$$

Pour ces valeurs de m, le polynôme $m^2U^2 - 2(P_1 - P_2)m + V^2$ est, dans $\mathbb{R}[x]$, soit un carré, soit l'opposé d'un carré, et de plus on sait que l'un des points spéciaux de $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ a pour première coordonnée $\alpha = mU^2$ pour l'une au moins de ces valeurs de m, peut-être les deux. Pour savoir si l'une de ces deux valeurs de m fournit un point spécial, sur la courbe $\mathcal{C}^{-1}$, il reste à vérifier deux propriétés :

(i) Il faudrait vérifier que $\alpha = mU^2$ est effectivement la première coordonnée d'un point de $\mathcal{C}^{-1}$, c'est-à-dire s'assurer que $m^2U^2 - 2(P_1 - P_2)m + V^2$ est l'opposé d'un carré dans $\mathbb{R}[x]$ et non pas un carré en montrant par exemple que le terme $(1-a)^2m^2 - 2(1+a)m + 1$ est négatif.

(ii) Il faudrait vérifier que ce point est spécial c'est-à-dire que $\alpha = mU^2$ est positif, ce qui revient à montrer que m est positif.

On peut montrer que ces deux conditions sont remplies pour les deux valeurs de m données ci-dessus, mais étant donné la complexité des formules et la longueur de cette démonstration, on se contentera ici d'appliquer sur un exemple numérique le résultat obtenu, ¸est-à-dire, les points spéciaux recherchés sont les points dont la première coordonnée est de la forme :

$$\alpha = mU^2 = \frac{2(a+c) \pm 2\sqrt{4ac - b^2}}{2(1-a)(c-a) + b^2 + b\sqrt{\delta}}\left((1-a)x - \frac{b + \sqrt{\delta}}{2}\right)^2 .$$

On sait aussi qu'il y a sur cette courbe elliptique des points spéciaux dont la première coordonnée est :

$$\alpha' = \frac{1}{k}V^2 = \frac{2(1-a)(c-a) + b^2 + b\sqrt{\delta}}{2(a+c) \pm 2\sqrt{4ac - b^2}}\left(x - \frac{b - \sqrt{\delta}}{2(1-a)}\right)^2 .$$

Exemple

On va traiter le cas où $a = 2$, $b = 4$ et $c = 4$, c'est-à-dire $F(x, y) = (y^2 + x^2 + 1)(y^2 + 2x^2 + 4x + 4)$. Alors $P_1 - P_2 = -x^2 - 4x - 3 = -(x + 1)(x + 3)$ et la courbe $\mathcal{C}^{-1}$ a pour équation : $-\beta^2 = \alpha(\alpha^2 - 2(3x^2 + 4x + 5)\alpha + (x + 1)^2(x + 3)^2)$.

Comme $\delta = 4$, les points spéciaux obtenus avec les formules données ci-dessus ont pour premières coordonnées $\alpha = (x + 3)^2$, $\alpha = \frac{1}{5}(x + 3)^2$, $\alpha = (x + 1)^2$ et $\alpha = 5(x + 1)^2$. En choisissant $\alpha = (x + 1)^2$, on obtient la seconde coordonnée $\beta = \pm 2x(x + 1)^2$ et on pose, en reprennant les notations du théorème 1.1.1 :

* $b_2 = x + 1$ et $b_3 = 0$,
* $c_1 = \frac{1}{2}(A - \alpha) = x^2 + x + 2$,
* $c_2 = \frac{\beta}{2\alpha} b_3 = 0$ et $c_3 = -\frac{\beta}{2\alpha} b_2 = x(x + 1)$.

Cela donne la relation :

$$(y^2 + x^2 + 1)(y^2 + 2x^2 + 4x + 4) = (y^2 + x^2 + x + 2)^2 + ((x + 1)y)^2 + (x(x + 1))^2.$$

(D) $P_1 - P_2$ est de degré 2 et irréductible

On est alors dans le cas où $a \neq 0$ et $\delta = \mathrm{discr}(P_1 - P_2) = b^2 - 4(1 - a)(1 - c) < 0$, le polynôme $P_1 - P_2 = (1 - a)x^2 - bx + (1 - c)$ est alors de signe constant. On pose toujours $\alpha = f\theta^2 \neq 0$ avec les mêmes conditions, et comme f est positif et divise $P_1 - P_2$, on peut supposer qu'on a soit $f = 1$, soit $f = \varepsilon(P_1 - P_2)$ avec $\varepsilon = \pm 1$ suivant le signe de $P_1 - P_2$, de façon que $\varepsilon(1 - a)$ soit positif.

Si on suppose que $f = 1$, alors $\alpha = \theta^2$ et la relation $\theta^4 - 2(P_1 + P_2)\theta^2 + (P_1 - P_2)^2 = -\mu^2$ implique, d'après le signe des coefficients dominants des deux termes de cette égalité, que $\deg(\theta) = 1$. Il existe alors $x_0 \in \mathbb{R}$ annulant θ et donc $(P_1 - P_2)^2(x_0) = -\mu^2(x_0)$ d'où $(P_1 - P_2)^2(x_0) = 0$ ce qui est impossible car $x_0 \in \mathbb{R}$ et $\delta = \mathrm{discr}(P_1 - P_2) < 0$.

La seule possibilité est donc $f = \varepsilon(P_1 - P_2)$ c'est-à-dire $\alpha = \varepsilon(P_1 - P_2)\theta^2$ et alors il existe $\mu \in \mathbb{R}[x]$ tel que :

$$-\varepsilon(P_1 - P_2)\mu^2 = \varepsilon^2(P_1 - P_2)^2\theta^4 - 2(P_1 + P_2)\varepsilon(P_1 - P_2)\theta^2 + (P_1 - P_2)^2,$$

et comme $\varepsilon^2 = 1$, on a :

$$-\mu^2 = \varepsilon(P_1 - P_2)\theta^4 - 2(P_1 + P_2)\theta^2 + \varepsilon(P_1 - P_2)$$

Alors puisque $\varepsilon(P_1 - P_2)$ est positif, l'étude du signe des coefficients dominants dans cette dernière égalité donne $\deg(\theta) = 0$. On peut donc conclure que le point spécial recherché a une première coordonnée de la forme $\alpha = s(P_1 - P_2)$ où s est un réel non nul du signe de $1 - a$.

D'après la remarque 3.2.4, si $\alpha = s(P_1 - P_2)$ est la première coordonnée d'un point spécial sur $\mathcal{C}^{-1}$, alors on a un autre point spécial de première coordonnée $\alpha' = \frac{(P_1 - P_2)^2}{\alpha} = \frac{1}{s}(P_1 - P_2)$, on retrouve ainsi un autre point avec $\alpha' = s'(P_1 - P_2)$: les points spéciaux recherchés ont donc tous la même forme.

Recherche des valeurs de s :

On recherche α sous la forme $s(P_1 - P_2) = s(1 - a)x^2 - sbx + s(1 - c)$ avec $s(1 - a) > 0$, de même que $s(1 - c)$ car δ étant négatif $1 - a$ et $1 - c$ sont de même signe. D'après l'équation de $\mathcal{C}^{-1}$, il existe un polynôme μ de $\mathbb{R}[x]$ tel que :

$$-s(P_1 - P_2)\mu^2 = s^2(P_1 - P_2)^2 - 2(P_1 + P_2)s(P_1 - P_2) + (P_1 - P_2)^2.$$

On en déduit que $(P_1 - P_2)s^2 - 2(P_1 + P_2)s + (P_1 - P_2) = -s\mu^2$, c'est-à-dire que :

$$\Big((1 - a)x^2 - bx + (1 - c)\Big)\, s^2 - 2\Big((1 + a)x^2 + bx + (1 + c)\Big)\, s + \cdots$$

$$\cdots + \Big((1 - a)x^2 - bx + (1 - c)\Big) = -s\mu^2.$$

Et après calculs on a :

$$\Big((1 - a)s^2 - 2(1 + a)s + (1 - a)\Big)\, x^2 + \Big(-bs^2 - 2bs - b\Big)\, x + \cdots$$

$$\cdots + \Big((1 - c)s^2 - 2(1 + c)s + (1 - c)\Big) = -s\mu^2.$$

Le discriminant de ce polynôme de degré 2 en x doit donc être nul, cela implique que :

$$[bs^2 + 2bs + b]^2 - 4[(1 - a)s^2 - 2(1 + a)s + (1 - a)][(1 - c)s^2 - 2(1 + c)s + (1 - c)] = 0$$

Après calculs et simplifications, on obtient :

$$\delta s^4 + (4\delta + 16(2 - a - c))\, s^3 + (6\delta + 32(2 - a - c) - 64)\, s^2 + \cdots$$

$$\cdots + (4\delta + 16(2-a-c))\, s + \delta = 0.$$

Il reste donc à résoudre cette équation pour trouver les valeurs de s parmi lesquelles se trouvent les solutions du problème. Quitte à diviser cette équation par s^2, qu'on a supposé non nul, on obtient :

$$\delta\left(s^2 + \frac{1}{s^2}\right) + (4\delta + 16(2-a-c))\left(s + \frac{1}{s}\right) + (6\delta + 32(2-a-c) - 64) = 0.$$

On pose $T = s + \frac{1}{s}$, et comme $s^2 + \frac{1}{s^2} = \left(s + \frac{1}{s}\right)^2 - 2 = T^2 - 2$, on a finalement l'équation :

$$\delta T^2 + (4\delta + 16(2-a-c))\, T + (4\delta + 32(2-a-c) - 64) = 0.$$

Pour déterminer s, on va d'abord calculer T qui est racine du polynôme de degré 2 écrit ci-dessus. Le discriminant de ce polynôme est $(4\delta + 16(2-a-c))^2 - 4\delta(4\delta + 32(2-a-c) - 64)$ et après simplification cette expression peut s'écrire $16^2(b^2 + (a-c)^2)$, donc on a comme candidates pour les valeurs de T :

$$T = \frac{-2\delta - 8(2-a-c) \pm 8\sqrt{b^2 + (a-c)^2}}{\delta}\ .$$

Comme $T = s + \frac{1}{s}$, on a aussi la relation $s^2 - Ts + 1 = 0$ et puisque le discriminant de ce polynôme de degré 2 en s est $T^2 - 4$, cela implique, à condition que $T^2 - 4$ soit positif, que $s = \frac{T \pm \sqrt{T^2-4}}{2}$.

Les points spéciaux recherchés sont donc parmi les points ayant une première coordonnées de la forme :

$$\alpha = \frac{T \pm \sqrt{T^2-4}}{2}\left((1-a)x^2 - bx + (1-c)\right),$$

le réel T prenant les valeurs données ci-dessus.

Cependant rien ne permet d'affirmer à priori que tous ces points seront bien solution du problème, il reste à faire plusieurs vérifications :

(i) Tout d'abord il faudrait s'assurer que $T^2 - 4$ est positif afin que s soit bien défini sur le corps $\mathbb{R}$.

(ii) Ensuite il faudrait vérifier que le polynôme $\alpha = s(P_1 - P_2)$ est bien la première coordonnée d'un point de $\mathcal{C}^{-1}_{\mathbb{R}(x)}$, en effet pour les valeurs de s

trouvées, $(P_1-P_2)s^2-2(P_1+P_2)s+(P_1-P_2)$ est un polynôme de degré 2 en x dont le discriminant est nul, c'est donc, dans $\mathbb{R}[x]$, soit un carré, soit l'opposé d'un carré. Or on veut que $(P_1-P_2)s^2-2(P_1+P_2)s+(P_1-P_2)=-s\mu^2$ dont il faudrait vérifier par exemple que pour la valeur de s obtenue, le terme $(1-a)s^2-2(1+a)s+(1-a)$ est du même signe que $-s$.

(iii) Enfin il faudrait s'assurer que le point de la courbe $\mathcal{C}^{-1}_{\mathbb{R}(x)}$ obtenu est spécial c'est-à-dire que $\alpha = s(P_1-P_2)$ est positif ou encore que s est du même signe que $1-a$.

On peut montrer que la condition (i) est vérifiée pour les deux valeurs de T obtenues, mais que les conditions (ii) et (iii) ne sont vérifiées que pour deux des valeurs de s données ci-dessus et on remarque que l'expression de ces deux valeurs de s varie suivant le signe de $1-a$ si $b\neq 0$ et de $(1-a)(a-c)$ si $b=0$. Ici encore, la complexité des formules rend ces vérifications très fastidieuses dans le cas général, on remarquera cependant qu'il y a toujours sur $\mathcal{C}^{-1}$ deux points spéciaux dont les premières coordonnées sont données par deux des formules ci-dessus.

Exemple

On va traiter le cas où $a=4$, $b=0$ et $c=9$, c'est-à-dire $F(x,y)=(y^2+x^2+1)(y^2+4x^2+9)$. Comme $P_1-P_2=-3x^2-8$, la courbe $\mathcal{C}^{-1}$ a pour équation : $-\beta^2=\alpha(\alpha^2-2(5x^2+10)\alpha+(3x^2+8)^2)$.

On a ici $\delta=-96$, ce qui donne $T=-\frac{10}{3}$ ou $T=-\frac{5}{2}$. On en déduit que $s=-3$, $s=-\frac{1}{3}$, $s=-2$ ou $s=-\frac{1}{2}$ et donc on a quatre possibilités pour α, celles-ci étant liées deux-à-deux :

* soit les solutions sont $\alpha=-3(3x^2+8)$ et $\alpha=-\frac{1}{3}(3x^2+8)$,

* soit les solutions sont $\alpha=-2(3x^2+8)$ et $\alpha=-\frac{1}{2}(3x^2+8)$.

On va donc poser $\alpha=t(3x^2+8)$, avec $t=3$, $t=\frac{1}{3}$, $t=2$ et $t=\frac{1}{2}$ et en substituant dans l'équation de $\mathcal{C}^{-1}$, on a :

$$-\beta^2=t(3x^2+8)^2\left((3t^2-10t+3)x^2+(8t^2-20t+8)\right).$$

On voit alors que si $t=3$ (respectivement $t=\frac{1}{3}$), on obtient $\beta^2=-60(3x^2+8)^2$ (respectivement $\beta^2=-\frac{20}{27}(3x^2+8)^2$), ce qui ne donne pas un point $\mathbb{R}(x)$-rationnel sur $\mathcal{C}^{-1}$. En revanche, pour $t=2$ (respectivement $t=\frac{1}{2}$), on obtient

$\beta^2 = 10x^2(3x^2+8)^2$ (respectivement $\beta^2 = \frac{5}{8}x^2(3x^2+8)^2$). On a bien des points $\mathbb{R}(x)$-rationnels sur $\mathcal{C}^{-1}$ de secondes coordonnées $\beta = \pm\sqrt{10}x(3x^2+8)$ $\beta^2 = \pm\sqrt{\frac{5}{8}}x(3x^2+8)$.

En choisissant $\alpha = 2(3x^2+8) = (4)^2 + (\sqrt{6}x)^2$ et $\beta = \sqrt{10}x(3x^2+8)$. On peut donc poser, en reprennant les notations du théorème 1.1.1 :

* $b_2 = 4$ et $b_3 = \sqrt{6}x$,
* $c_1 = \frac{1}{2}(A-\alpha) = -\frac{1}{2}x^2 - 3$,
* $c_2 = \frac{\beta}{2\alpha}b_3 = \frac{\sqrt{15}}{2}x^2$ et $c_3 = -\frac{\beta}{2\alpha}b_2 = -\sqrt{10}x$.

Cela donne la relation :

$$(y^2+x^2+1)(y^2+4x^2+9) = (y^2 - \frac{1}{2}x^2 - 3)^2 + (4y + \frac{\sqrt{15}}{2}x^2)^2 + (\sqrt{6}xy - \sqrt{10}x)^2.$$

Chapitre 4

Sur la hauteur d'une solution à l'équation $u^2 + v^2 = -1$ dans le corps des fonctions d'une courbe sans point réel

4.1 Résultat central

Soit $\mathcal{C}_F$ une courbe projective plane, définie sur $\mathbb{R}$ par l'équation homogène $F(X,Y,Z) = 0$, irréductible et sans point réel, on sait que le corps des fonctions $\mathbb{R}(\mathcal{C}_F)$ est de niveau au plus 2 (Witt, [Wi]). L'objectif de ce chapitre est, lorsque ce corps est de niveau 2, de trouver un entier n tel qu'il existe des solutions (u,v) dans $\mathbb{R}(\mathcal{C}_F)^* \times \mathbb{R}(\mathcal{C}_F)^*$ de l'équation $u^2 + v^2 = -1$ ayant des représentants dans $\mathbb{R}(X,Y,Z)$ dont les numérateurs et dénominateurs sont de degré total inférieur ou égal à n, de manière équivalente, cela revient à déterminer une borne sur le degré total de polynômes A_1, A_2 et A_3 de $\mathbb{R}[X,Y,Z]$ vérifiant $(A_1)^2 + (A_2)^2 + (A_3)^2 \equiv 0 \pmod F$. On démontrera le théorème suivant :

Théorème 4.1.1 *Soit $\mathcal{C}_F$ une courbe projective irréductible plane, sans point réel, de genre g, définie par l'équation $F(X,Y,Z) = 0$ où F est un polynôme homogène de degré total d dans $\mathbb{R}[X,Y,Z]$. Si le corps de fonctions $K = \mathbb{R}(\mathcal{C}_F)$ est de niveau 2 et si tous les points singuliers de $\mathcal{C}_F$ sont ordinaires, alors il existe un entier N_F tel qu'on peut trouver des polynômes homogènes A_1, A_2, $A_3 \in \mathbb{R}[X,Y,Z]$ de même degré total égal à N_F et vérifiant la relation $(A_1)^2 + (A_2)^2 + (A_3)^2 \equiv 0 \pmod F$. Cet entier N_F est donné par la formule :*

$$N_F = 2\left[\frac{1 + 2g + \sum_{P \in \mathcal{C}} m_P(\mathcal{C}_F)(m_P(\mathcal{C}_F) - 1)}{d}\right] + 2$$

où le terme $[x]$ *désigne la partie entière du nombre réel* x *et* $m_P(\mathcal{C}_F)$ *la multiplicité de la courbe* $\mathcal{C}_F$ *en* P.

Un résultat analogue, dans un cadre plus général, a été récemment démontré par Pfister [Pf2].

4.2 Généralités sur les courbes projectives

Soit F un polynôme homogène irréductible de $\mathbb{C}[X,Y,Z]$, on note $\mathcal{C}_F$ la courbe projective plane irréductible définie sur $\mathbb{C}$ par l'équation $F(X,Y,Z)=0$. Soit Γ_F un modèle non singulier de $\mathcal{C}_F$ et φ le morphisme birationnel de Γ_F sur $\mathcal{C}_F$. Si P est un point singulier ordinaire de $\mathcal{C}_F$, on note $r_{_P}$ la multiplicité de $\mathcal{C}_F$ en P et on pose $\varphi^{-1}(P)=\{P_1,...,P_{r_P}\}\subset\Gamma_F$. Les points de $\Gamma_F(\mathbb{C})$ peuvent être identifiés aux valuations du corps de fonctions $\mathbb{C}(\mathcal{C}_F)\simeq\mathbb{C}(\Gamma_F)$.

On va maintenant rappeler le théorème fondamental de Nœther (voir [Fu], p.120): on considère des courbes projectives planes $\mathcal{C}_F$, $\mathcal{C}_G$ et $\mathcal{C}_H$, d'équations homogènes respectives $F(X,Y,Z)=0$, $G(X,Y,Z)=0$ et $H(X,Y,Z)=0$ où F, G et H sont des polynômes homogènes de $\mathbb{C}[X,Y,Z]$. Pour la suite on désignera par $\mathbb{P}^2$ le plan projectif complexe.

Notations 4.2.1 *Pour appliquer le théorème fondamental de Nœther, on aura besoin des notations suivantes :*

- *Si* P *est un point de la courbe* $\mathcal{C}_F$ *et si* $\mathcal{D}$ *est une autre courbe projective plane, on note* $I(P,\mathcal{C}_F\cap\mathcal{D})$ *la multiplicité d'intersection des courbes* $\mathcal{C}_F$ *et* $\mathcal{D}$ *au point* P.
- *Si* P *est un point de* Γ_F *on note* ord_P^F, *ou* ord_P *s'il n'y a pas ambiguïté sur la courbe considérée, la valuation du corps de fonctions* $\mathbb{C}(\mathcal{C}_F)$ *associée au point* P. *Si* R *est un polynôme homogène de* $\mathbb{C}[X,Y,Z]$ *de degré* n, *on définira* $ord_P(R)$ *comme étant* $ord_P(R_*)$, *où* $R_*=\frac{R}{L^n}$, L *étant l'équation homogène d'une droite ne passant pas par le point* P.

Définition 4.2.2 *On dit que les conditions de Nœther sont satisfaites en un point* $P\in\mathcal{C}_F\cap\mathcal{C}_G$ *si* $H_*\in(F_*,G_*)\subset\mathcal{O}_P(\mathbb{P}^2)$, *la notation* R_* *correpondant ici à l'équation homogène* L *d'une droite ne passant par aucun des points de* $\mathcal{C}_F\cap\mathcal{C}_G$.

En particulier, on sait que ([Fu], p.121 et p.183):

Proposition 4.2.3 *Les conditions de Nœther sont satisfaites en un point P dans les cas suivants :*

* *Quand P est un point simple de $\mathcal{C}_F$ et que $I(P, \mathcal{C}_F \cap \mathcal{C}_H) \geq I(P, \mathcal{C}_F \cap \mathcal{C}_G)$.*
* *Quand P est un point singulier ordinaire de $\mathcal{C}_F$ et que, avec la notation $\varphi^{-1}(P) = \{P_1, ..., P_{r_P}\}$, on a pour $i \in \{1, ..., r_P\}$: $ord_{P_i}(H) \geq ord_{P_i}(G) + r_P - 1$.*

Théorème 4.2.4 (Théorème fondamental de Nœther) *Si F, G et H sont des polynômes homogènes de $\mathbb{C}[X, Y, Z]$ telles que les courbes projectives planes $\mathcal{C}_F$ et $\mathcal{C}_G$ n'ont pas de composante commune, alors il existe des polynômes homogènes S et T vérifiant $H = SF + TG$ si et seulement si les conditions de Nœther sont satisfaites en chaque point de $\mathcal{C}_F \cap \mathcal{C}_G$.*

Par la suite les diviseurs considérés seront des diviseurs sur la courbe $\mathcal{C}_F$. Si A est un polynôme homogène de $\mathbb{C}[X, Y, Z]$ ne contenant pas F comme composante, on appelle diviseur de A le diviseur d'intersection, qui est un diviseur effectif, $\mathrm{div}(A) = \sum_{p \in \Gamma_F} \mathrm{ord}_P(A)P$. Soit $c \in \mathbb{C}(\mathcal{C}_F)$ et soit $\frac{A}{B}$ l'un de ses représentants dans $\mathbb{C}(X, Y, Z)$, A et B étant deux polynômes homogènes de même degré, alors $\mathrm{div}(c) = \mathrm{div}(A) - \mathrm{div}(B)$.

On peut traduire très simplement la proposition 4.2.3 en termes de diviseurs : en conservant les mêmes notations, on introduit le diviseur effectif E défini par :

$$E = \sum_{P \in \mathcal{C}} \left(\sum_{i=1}^{r_P} (r_P - 1) P_i \right).$$

Ce diviseur est de degré $r = \sum_{P \in \mathcal{C}} (r_P(r_P - 1))$. On obtient alors la proposition :

Proposition 4.2.5 *Si $div(H) \geq div(G) + E$ alors les conditions de Nœther sont satisfaites en tout point de $\mathcal{C}_F$.*

On utilisera aussi par la suite le théorème de Riemann-Roch ([Fu], p196). Soit D un diviseur de $\mathcal{C}_F$, on note $\mathcal{L}(D)$ le $\mathbb{C}$-espace vectoriel $\{f \in \mathbb{C}(\mathcal{C}_F) / \mathrm{div}(f) \geq -D\}$ et $l(D)$ sa dimension.

Théorème 4.2.6 (Riemann-Roch) *Si $\mathcal{C}_F$ est une courbe projective plane de genre g et D un diviseur de $\mathcal{C}_F$, alors $l(D) \geq \deg(D) + 1 - g$.*

4.3 Idèles et extensions de corps

Dans tout ce chapitre le terme "valuation sur un corps k" désigne une valuation discrète de rang 1 sur ce corps et on utilisera la notation additive.

Définition 4.3.1 *Soit K un corps, on note $\mathcal{V}_K$ l'ensemble des valuations de K et pour $v \in \mathcal{V}_K$, on appelle K_v le complété de K pour la valuation v. Un idèle sur K est un élément $(\alpha_v) \in \prod_{v\in\mathcal{V}_K} K_v^*$ avec $v(\alpha_v) = 0$ sauf pour un nombre fini de valuations v. On note $\mathcal{J}_K$ l'ensemble des idèles sur K.*

On vérifie aisément que $\mathcal{J}_K$ est un sous-groupe multiplicatif de $\prod_{v\in\mathcal{V}_K} K_v^*$. On a aussi un morphisme injectif de K^* dans $\mathcal{J}_K$: si $a \in K^*$, on lui associe un idèle $(a_v)_{v\in\mathcal{V}_K}$ où $a_v = \mu_v(a)$, μ_v étant l'injection de K dans K_v. On identifiera a et cet idèle.

(A) Extension d'une valuation

Soit $k \subset k'$ deux corps et v une valuation sur k, on dit qu'une valuation v' de k' étend v si la restriction de v' à k est v.

Théorème 4.3.2 *Si k est un corps complet par rapport à la valuation v et si k' est une extension finie de k de degré N, alors il y a exactement une extension v' de v au corps k' qui est donnée par : pour tout $u \in k'$, $v'(u) = \frac{1}{N} v\left(Norme_{k'/k}(u)\right)$.*

Preuve. Voir [Ca2], p.56. □

On s'intéresse maintenant à un corps K muni d'une valuation v lorsque ce corps n'est pas nécessairement complet relativement à v : l'objectif est ici d'étendre la valuation v au corps $L = K(\omega)$ où ω est un élément algébrique de degré N sur K et de polynôme minimal $f(X) \in K[X]$. Le polynôme f n'étant peut-être plus irréductible sur le complété K_v de K relativement à v, on écrit f sous la forme $f(X) = \prod_{j=1}^{J} g_j(X)$ où pour $1 \leq j \leq J$, $g_j(X) \in K_v[X]$ est un polynôme irréductible sur K_v. On pose pour $1 \leq j \leq J$, $L_j = K_v(\omega_j)$ avec ω_j vérifiant $g_j(\omega_j) = 0$. On va énoncer les résultats démontrés dans [Ca2] en les adaptant aux notations utilisées ici, en particulier à la notation additive des valuations.

Lemme 4.3.3 *Avec les notations ci-dessus, $K_v \otimes_K L$ est isomorphe à $\oplus_{j=1}^{J} L_j$ et chaque L_j contient un sous-corps isomorphe à K_v et un sous-corps isomorphe à L.*

On retiendra de la preuve de ce lemme ([Ca2], p.57-58) que pour $1 \leq j \leq J$, le sous-corps de L_j isomorphe à K_v est l'image de K_v par l'injection canonique dans $L_j = K_v(\omega_j)$ et que le sous-corps de L_j isomorphe à L est $\lambda_j(L)$ où λ_j est le morphisme injectif de L dans L_j qui à tout $c \in L$, que l'on peut écrire la forme $h(\omega)$ avec $h \in K[x]$, associe $\lambda_j(c) = h(\omega_j)$.

On donne aussi dans [Ca2], p.55, une propriété concernant les normes de ces extensions :

Lemme 4.3.4 *Pour tout $c \in L$, $Norme_{L/K}(c) = \prod_{j=1}^{J} Norme_{L_j/K_v}(\lambda_j(c))$.*

On peut caractériser toutes les valuations qui étendent v au corps L :

Théorème 4.3.5 *Avec les notations précédentes, il existe exactement J extensions w_j, $1 \leq j \leq J$, de la valuation v au corps L. De plus pour $1 \leq j \leq J$, le complété de L relativement à w_j est isomorphe au corps L_j.*

Pour une preuve de ce théorème voir [Ca2], p.57-58, on se contentera ici d'expliciter les formules donnant les valuations w_j :

Soit $1 \leq j \leq J$, on sait que v définit une valuation sur le corps K_v, de plus le corps L_j est une extension finie, de degré n_j, de K_v qui est complet relativement à v, d'après le théorème 4.3.2, il y a donc une unique valuation v_j étendant v au corps L_j et pour tout $u \in L_j$, $v_j(u) = \frac{1}{n_j} v\left(\text{Norme}_{L_j/K_v}(u)\right)$.

La valuation w_j sur le corps L est alors définie par : pour tout $c \in L$, $w_j(c) = v_j(\lambda_j(c))$ c'est-à-dire $w_j(c) = \frac{1}{n_j} v\left(\text{Norme}_{L_j/K_v}(\lambda_j(c))\right)$ et le complété de L relativement à w_j est isomorphe à L_j.

Corollaire 4.3.6 *Si $c \in L^*$, alors l'idèle de $\mathcal{J}_L$ associé à c est $(c_w)_{w \in \mathcal{V}_L}$ où $c_w = \mu_w(c)$, μ_w étant l'injection de L dans le complété L_w. Mais comme w étend sur L sa restriction v à K, alors w est l'une des valuations w_j définies ci-dessus, on a donc $L_w \simeq L_j$ et $c_w = \lambda_j(c)$.*

Remarque 4.3.7 Il existe un morphisme de groupe injectif Δ de $\mathcal{J}_K$ dans $\mathcal{J}_L$: soit $\alpha = (\alpha_v)_{v \in \mathcal{V}_K}$ un élément de $\mathcal{J}_K$, si $w \in \mathcal{V}_L$, alors w est l'une des valuations w_j étendant la restriction v de w à K et $L_w \simeq L_j \simeq K_v(\omega_j)$. On prend pour $\Delta(\alpha)_w$ l'image, que l'on notera aussi α_v, de α_v par l'injection canonique de K_v dans L_j. On a ainsi défini un idèle $\Delta(\alpha) = (\Delta(\alpha)_w)_{w \in \mathcal{V}_L}$. On vérifie facilement que l'application diagonale Δ de $\mathcal{J}_K$ dans $\mathcal{J}_L$ est un morphisme de groupe et qu'il est injectif.

Notation 4.3.8 *Afin d'alléger les formules, lorsque le corps k' est une extension finie du corps k, on notera la norme de cette extension $N_{k'/k}$ plutôt que $Norme_{k'/k}$.*

On s'intéresse plus particulièrement pour la suite au cas où $i = \sqrt{-1} \notin K$ et où $L = K(i)$, ce corps L est alors une extension quadratique de K. Soit $v \in \mathcal{V}_K$, deux cas se présentent :

* Si -1 n'est pas un carré dans K_v, alors le polynôme $X^2 + 1$ est toujours irréductible dans K_v et $K_v \otimes_K L = K_v \otimes_K K(i)$ est isomorphe à $K_v(i)$. D'après le théorème 4.3.5, il y a alors une seule valuation w_1 étendant v à L, le complété L_1 de L relativement à w_1 est isomorphe à $K_v(i)$ et si $c = a + ib \in L$, avec $a, b \in K$, $w_1(c) = \frac{1}{2} v\left(N_{K_v(i)/K_v}(\lambda_1(c))\right) = \frac{1}{2} v(a^2 + b^2)$, en effet d'après le lemme 4.3.4, $N_{K_v(i)/K_v}(\lambda_1(a + ib)) = N_{K(i)/K}(a + ib)$.

* Si -1 est un carré dans K_v, alors il existe $i_v \in K_v$ tel que $-1 = (i_v)^2$, le polynôme $X^2 + 1 = (X - i_v)(X + i_v)$ n'est plus irréductible dans K_v et donc $K_v \otimes_K L \simeq K_v \otimes_K K[X]/(X^2 + 1)$ est isomorphe à $K_v[X]/(X - i_v) \oplus K_v[X]/(X + i_v) \simeq K_v \times K_v$. On a alors deux valuations w_1 et w_2 sur L étendant v, et les complétés respectifs L_1 et L_2 de L pour ces valuations sont isomorphes à K_v. Ces valuations sont définies grâce aux injections $\lambda_1 : L \to K_v$ et $\lambda_2 : L \to K_v$ qui à $c = a + ib \in L$, avec $a, b \in K$, associent $\lambda_1(c) = a + i_v b$ et $\lambda_2(c) = a - i_v b$. On a alors $w_1(c) = v(\lambda_1(c)) = v(a + i_v b)$ et $w_2(c) = v(\lambda_2(c)) = v(a - i_v b)$.

(B) Extension de la norme aux idèles

D'après le lemme 4.3.4, pour tout $c \in L$, $\mathrm{N}_{L/K}(c) = \prod_{j=1}^{J} \mathrm{N}_{L_j/K_v}(\lambda_j(c))$, on peut étendre la norme $\mathrm{N}_{L/K}$ aux idèles par une application elle aussi multiplicative $\mathrm{N}_{\mathcal{J}_L/\mathcal{J}_K} : \mathcal{J}_L \to \mathcal{J}_K$ qui à $\alpha \in \mathcal{J}_L$ associe l'idèle $\mathrm{N}_{\mathcal{J}_L/\mathcal{J}_K}(\alpha)$ définie pour tout $v \in \mathcal{V}_K$ par $\mathrm{N}_{\mathcal{J}_L/\mathcal{J}_K}(\alpha)_v = \prod_{j=1}^{J} \mathrm{N}_{L_j/K_v}(\alpha_{w_j}) \in K_v$.

En particulier quand $L = K(i)$ cela se traduit de la manière suivante, soit $\alpha \in \mathcal{J}_L$, avec $\alpha = (\alpha_w)_{w \in \mathcal{V}_L}$, et soit v une valuation sur K :

* Si -1 n'est pas un carré dans K_v, il y a une seule valuation w_1 étendant v à L et le complété de L pour w_1 est isomorphe à K_v, on a alors $\mathrm{N}_{\mathcal{J}_L/\mathcal{J}_K}(\alpha)_v = \mathrm{N}_{K_v(i)/K_v}(\alpha_{w_1})$.

* Si -1 est un carré dans K_v, il y a 2 valuations w_1 et w_2 étendant v à L et les complétés respectifs L_1 et L_2 sont isomorphes à K_v, on a donc $\mathrm{N}_{\mathcal{J}_L/\mathcal{J}_K}(\alpha)_v = \prod_{j=1}^{2} \mathrm{N}_{K_v/K_v}(\alpha_{w_j}) = \alpha_{w_1}\alpha_{w_2}$.

(C) Définition de la conjugaison pour les idèles.

Lorsque $L = K(i)$, on cherche à étendre aux idèles la conjugaison $\sigma_{L/K}$ par une application $\sigma_{\mathcal{J}_L/\mathcal{J}_K} : \mathcal{J}_L \to \mathcal{J}_L$ qui étende la conjugaison de L sur K. Soit $c = a + ib \in L$, avec $a, b \in K$, on va étudier les idèles $c = (c_w)_{w\in\mathcal{V}_L}$ et $\sigma_{L/K}(c) = (\sigma_{L/K}(c)_w)_{w\in\mathcal{V}_L}$. Soit $w \in \mathcal{V}_L$, alors w induit une valuation v sur K :

* Si -1 n'est pas un carré dans K_v, $w = w_1$ est l'unique valuation étendant v à L et on a $L_1 \simeq K_v(i)$ d'où $c_w = \lambda_1(a+ib) = a+ib$ et $\sigma_{L/K}(c)_w = \lambda_1(\sigma_{L/K}(a+ib)) = \lambda_1(a-ib) = a-ib$. On constate que $\sigma_{L/K}(c)_w = \sigma_{K_v(i)/K_v}(c_w)$ et on pose alors $\sigma_{\mathcal{J}_L/\mathcal{J}_K}(\alpha)_w = \sigma_{K_v(i)/K_v}(\alpha_w)$.

* Si -1 est un carré dans K_v, w est l'une des deux valuations w_1 et w_2 qui étendent v à L et $L_1 \simeq L_2 \simeq K_v$, on a alors $c_{w_1} = \lambda_1(c) = a + i_v b$ et $c_{w_2} = \lambda_2(c) = a - i_v b$. D'autre part, $\sigma_{L/K}(c)_{w_1} = \lambda_1(\sigma_{L/K}(c)) = \lambda_1(a - ib) = a - i_v b$ et $\sigma_{L/K}(c)_{w_2} = \lambda_2(\sigma_{L/K}(c)) = \lambda_2(a - ib) = a + i_v b$. On remarque que $\sigma_{L/K}(c)_{w_1} = c_{w_2}$ et que $\sigma_{L/K}(c)_{w_2} = c_{w_1}$ et on pose alors : $\sigma_{\mathcal{J}_L/\mathcal{J}_K}(\alpha)_{w_1} = \alpha_{w_2} \in K_v$ et $\sigma_{\mathcal{J}_L/\mathcal{J}_K}(\alpha)_{w_2} = \alpha_{w_1} \in K_v$.

Cela définit un idèle $\sigma_{\mathcal{J}_L/\mathcal{J}_K}(\alpha) = \left(\sigma_{\mathcal{J}_L/\mathcal{J}_K}(\alpha)_w\right)_{w\in\mathcal{V}_L}$, conjugué de α au sens des idèles.

Remarque 4.3.9 Pour $\alpha \in \mathcal{J}_L$, on peut identifier l'idèle $\mathrm{N}_{\mathcal{J}_L/\mathcal{J}_K}(\alpha) \in \mathcal{J}_K$ à l'idèle $\alpha.\sigma_{\mathcal{J}_L/\mathcal{J}_K}(\alpha) \in \mathcal{J}_L$ au moyen de l'application diagonale Δ définie à la remarque 4.3.7, généralisant ainsi aux idèles la formule $N_{L/K}(c) = c.\sigma_{L/K}(c)$ connue pour $c \in L$.

On a, lorsque $L = K(i)$, un résultat analogue au théorème 90 de Hilbert pour les idèles :

Proposition 4.3.10 *Si $\alpha \in \mathcal{J}_L$ et $N_{\mathcal{J}_L/\mathcal{J}_K}(\alpha) = 1_{\mathcal{J}_K}$ c'est-à-dire $N_{\mathcal{J}_L/\mathcal{J}_K}(\alpha) = (1)_{v\in\mathcal{V}_K}$, alors il existe un idèle $\delta \in \mathcal{J}_L$ tel que $\alpha = \delta^{-1}\sigma_{\mathcal{J}_L/\mathcal{J}_K}(\delta)$.*

Preuve. Soit un idèle $\alpha \in \mathcal{J}_L$ tel que $N_{\mathcal{J}_L/\mathcal{J}_K}(\alpha) = 1_{\mathcal{J}_K}$, soit $v \in \mathcal{V}_K$:

* S'il y a une unique valuation w_1 étendant v à L, alors on a $L_1 \simeq K_v(i)$, et $\mathrm{N}_{\mathcal{J}_L/\mathcal{J}_K}(\alpha) = 1$ implique que $\mathrm{N}_{\mathcal{J}_L/\mathcal{J}_K}(\alpha)_v = 1 \in K_v$ ce qui signifie que $\mathrm{N}_{K_v(i)/K_v}(\alpha_{w_1}) = 1$. D'après le théorème 90 de Hilbert appliqué à l'extension $K_v(i)/K_v$, il existe $\delta_{w_1} \in K_v(i)$ tel que $\alpha_{w_1} = \delta_{w_1}^{-1}\sigma_{K_v(i)/K_v}(\delta_{w_1})$.

* S'il y a deux valuations w_1 et w_2 étendant v à L, on a $L_1 \simeq L_2 \simeq K_v$, et $\mathrm{N}_{\mathcal{J}_L/\mathcal{J}_K}(\alpha)_v = 1$ implique que $\alpha_{w_1}\alpha_{w_2} = 1$ dans K_v. On peut alors prendre, entre autres, $\delta_{w_1} = 1$ et $\delta_{w_2} = \alpha_{w_1} = (\alpha_{w_2})^{-1}$.

Par définition l'idèle $\delta = (\delta_w)_{w\in\mathcal{V}_L} \in \mathcal{J}_L$ vérifie la propriété $\delta^{-1}\sigma_{\mathcal{J}_L/\mathcal{J}_K}(\delta) = \alpha$. □

4.4 Idèles et corps de fonctions d'une courbe

On s'intéresse au cas où $\mathcal{C}_F$ est une courbe projective irréductible définie par $F(X,Y,Z) = 0$, avec F polynôme homogène de $\mathbb{R}[X,Y,Z]$, telle que -1 n'est pas un carré dans $\mathbb{R}(\mathcal{C}_F)$ afin que $L = \mathbb{C}(\mathcal{C}_F)$ soit bien une extension quadratique de $\mathbb{R}(\mathcal{C}_F)$. On va appliquer les résultats de la section précédente à $K = \mathbb{R}(\mathcal{C}_F)$ et $L = K(i) = \mathbb{C}(\mathcal{C}_F)$. On sait que toutes les valuations de L (et donc aussi de K) sont discrètes et que l'on peut les identifier aux points complexes de Γ_F, un modèle non singulier de $\mathcal{C}_F$: si $w \in \mathcal{V}_L$, on notera P_w le point de Γ_F associé à cette valuation et pour tout $c \in L$, on a $w(c) = \mathrm{ord}_{P_w}(c)$.

A un idèle $\alpha = (\alpha_w)_{w\in\mathcal{V}_L} \in \mathcal{J}_L$ on peut associer un diviseur, noté $\mathrm{div}(\alpha)$, défini par :

$$\mathrm{div}(\alpha) = \sum_{w\in\mathcal{V}_L} w(\alpha_w)P_w.$$

On appelle degré de l'idèle α le degré du diviseur $\mathrm{div}(\alpha)$ c'est-à-dire $\sum_{w\in\mathcal{V}_L} w(\alpha_w)$. Si $f \in L = \mathbb{C}(\mathcal{C}_F)$ et α est l'idèle associé à f, on vérifie aisément que $\mathrm{div}(f) = \mathrm{div}(\alpha)$.

Proposition 4.4.1 *Si $\alpha \in \mathcal{J}_L$ et si on note $\sigma(\alpha) = \sigma_{\mathcal{J}_L/\mathcal{J}_K}(\alpha)$, alors les diviseurs $div(\alpha)$ et $div(\sigma(\alpha))$ ont le même nombre de zéros et de pôles comptés avec multiplicité.*

Preuve. Par définition $\mathrm{div}(\alpha) = \sum_{w \in \mathcal{V}_L} w(\alpha_w) P_w$ et $\mathrm{div}(\sigma(\alpha)) = \sum_{w \in \mathcal{V}_L} w(\sigma(\alpha)_w) P_w$. Soit w un élément de $\mathcal{V}_L$:

$*$ Si w est la seule extension de sa restriction v à K, on a d'une part $w(\alpha_w) = \frac{1}{2} v\left(\mathrm{N}_{K_v(i)/K_v}(\alpha_w)\right)$ et d'autre part $w(\sigma(\alpha)_w) = \frac{1}{2} v\left(\mathrm{N}_{K_v(i)/K_v}(\sigma_{\mathcal{J}_L/\mathcal{J}_K}(\alpha)_w)\right)$. Or par définition de $\sigma_{\mathcal{J}_L/\mathcal{J}_K}(\alpha)$, $\mathrm{N}_{K_v(i)/K_v}(\sigma_{\mathcal{J}_L/\mathcal{J}_K}(\alpha)_w) = \mathrm{N}_{K_v(i)/K_v}(\sigma_{K_v(i)/K_v}(\alpha_w))$ et ce terme est égal à $\mathrm{N}_{K_v(i)/K_v}(\alpha_w)$. Cela implique que $w(\sigma(\alpha)_w) = w(\alpha_w)$.

$*$ Si w_1 et w_2 sont les deux extensions sur L de la restriction v de w à L, alors d'une part $w_1(\alpha_{w_1}) = v(\alpha_{w_1})$ et $w_2(\alpha_{w_2}) = v(\alpha_{w_2})$, d'autre part $w_1(\sigma(\alpha)_{w_1}) = v\left(\sigma_{\mathcal{J}_L/\mathcal{J}_K}(\alpha)_{w_1}\right) = v(\alpha_{w_2})$ et $w_2(\sigma(\alpha)_{w_2}) = v\left(\sigma_{\mathcal{J}_L/\mathcal{J}_K}(\alpha)_{w_2}\right) = v(\alpha_{w_1})$. On a donc $w_1(\sigma(\alpha)_{w_1}) = w_2(\alpha_{w_2})$ et $w_2(\sigma(\alpha)_{w_2}) = w_1(\alpha_{w_1})$.

Cela prouve alors que :

$$\sum_{\substack{w \in \mathcal{V}_L \\ w(\alpha_w) > 0}} w(\alpha_w) = \sum_{\substack{w \in \mathcal{V}_L \\ w(\sigma(\alpha)_w) > 0}} w(\sigma(\alpha)_w),$$

et que :

$$\sum_{\substack{w \in \mathcal{V}_L \\ w(\alpha_w) < 0}} w(\alpha_w) = \sum_{\substack{w \in \mathcal{V}_L \\ w(\sigma(\alpha)_w) < 0}} w(\sigma(\alpha)_w).$$

Ces relations montrent que les diviseurs $\mathrm{div}(\alpha)$ et $\mathrm{div}(\sigma(\alpha))$ ont le même nombre de zéros et le même nombre de pôles comptés avec multiplicité. □

Remarque 4.4.2 On note $\sigma(P_w) = P_w$ quand w est l'unique valuation de L étendant sa restriction v à K, et $\sigma(P_{w_1}) = P_{w_2}$, $\sigma(P_{w_2}) = P_{w_1}$ quand w_1 et w_2 sont deux valuations de L ayant même restriction sur K. Alors si $\mathrm{div}(\alpha) = \sum_{w \in \mathcal{V}_L} w(\alpha_w) P_w$, on vérifie facilement que $\mathrm{div}(\sigma(\alpha)) = \sum_{w \in \mathcal{V}_L} w(\alpha_w) \sigma(P_w)$.

Proposition 4.4.3 *Soit P un point de Γ_F, on note w_P la valuation sur $L = \mathbb{C}(\mathcal{C}_F)$ associée à P, si $\overline{P}$ est le conjugué du point P au sens de la conjugaison de $\mathbb{C}/\mathbb{R}$ et si $w_{\overline{P}}$ est la valuation sur L associée à $\overline{P}$, alors w_P et $w_{\overline{P}}$ étendent à L une même valuation v de $K = \mathbb{R}(\mathcal{C}_F)$.*

Preuve. Il suffit de vérifier que pour tout $a \in K$, $w_P(a) = w_{\overline{P}}(a)$. Or si $a \in K = \mathbb{R}(\mathcal{C}_F)$, $a = \overline{a}$ d'où $w_P(a) = \mathrm{ord}_P(a) = \mathrm{ord}_{\overline{P}}(\overline{a}) = \mathrm{ord}_{\overline{P}}(a) = w_{\overline{P}}(a)$. □

Corollaire 4.4.4 *Avec les notations de la remarque 4.4.2, pour tout $w \in \mathcal{V}_L$, $\sigma(P_w) = \overline{P_w}$.*

Corollaire 4.4.5 *Si $\mathcal{C}_F$ est sans point réel, alors pour toute valuation v de K, il existe exactement deux valuations distinctes de L prolongeant v.*

Preuve. On sait que toute valuation de K peut être étendue à L soit par une valuation soit par deux valuations. Supposons que v soit une valuation de K qui ne peut être prolongée sur L que par une unique valuation w. Soit P le point de Γ_F associé à cette valuation et $\overline{P}$ son conjugué, d'après la proposition 4.4.3, la valuation associée à $\overline{P}$ étend aussi v, cette valuation est donc w. Les valuations sur L associées à P et $\overline{P}$ sont identiques, on en déduit que $P = \overline{P}$, contredisant ainsi le fait que la courbe $\mathcal{C}_F$ est sans point réel. □

Pour la suite, il est nécessaire de démontrer les deux propositions suivantes :

Proposition 4.4.6 *Si la courbe $\mathcal{C}_F$ est sans point réel, il existe un idèle $\varepsilon \in \mathcal{J}_L$ tel que $N_{\mathcal{J}_L/\mathcal{J}_K}(\varepsilon) = -1$ et $w(\varepsilon_w) = 0$ pour toute valuation $w \in \mathcal{V}_L$. Le diviseur associé à ε est donc nul.*

Preuve. D'après le corollaire 4.4.5, comme $\mathcal{C}_F$ est sans point réel, on peut regrouper les valuations de L par couples $(w_P, w_{\overline{P}})$ où w_P et $w_{\overline{P}}$ sont les valuations respectivement associées au point $P \in \Gamma_F$ et à son conjugué $\overline{P}$, ces deux valuations ont la même restriction v à K et les complétés de L pour ces valuations sont isomorphes à K_v.

On définit alors l'idèle ε par $\varepsilon_{w_P} = 1 \in K_v$ et $\varepsilon_{w_{\overline{P}}} = -1 \in K_v$ pour chaque couple de valuations $(w_P, w_{\overline{P}})$. Ainsi pour tout $w \in \mathcal{V}_L$, on a $\varepsilon_w = 1$ ou $\varepsilon_w = -1$ donc $w(\varepsilon_w) = 0$ et le diviseur $\mathrm{div}(\varepsilon)$ est nul. La relation $N_{\mathcal{J}_L/\mathcal{J}_K}(\varepsilon) = -1$ est bien vérifiée car si $v \in \mathcal{V}_K$, alors v est prolongée à L par deux valuations w_P et $w_{\overline{P}}$ et par définition de $N_{\mathcal{J}_L/\mathcal{J}_K}$, on a $N_{\mathcal{J}_L/\mathcal{J}_K}(\varepsilon)_v = \varepsilon_{w_P}\varepsilon_{w_{\overline{P}}} = -1 \in K_v$. □

Proposition 4.4.7 *Soit $\mathcal{C}_F$ une courbe plane, il existe des idèles de $\mathcal{J}_L$ de degré 2 invariants par la conjugaison $\sigma_{\mathcal{J}_L/\mathcal{J}_K}$.*

Preuve. Soit P un point non réel de Γ_F et $\overline{P}$ son conjugué, les valuations w_P et $w_{\overline{P}}$ sont distinctes et ont même restriction v à K et les complétés de L par rapport à ces valuations sont isomorphes à K_v. On pose $\alpha_{w_P} = \alpha_{w_{\overline{P}}} = \pi$, où π est un élément de K_v tel que $v(\pi) = 1$, et pour toute valuation $w \in \mathcal{V}_L$ distincte de w_P et de $w_{\overline{P}}$, on pose $\alpha_w = 1$. Alors l'idèle $\alpha = (\alpha_w)_{w \in \mathcal{V}_L}$ est, par construction, invariant par $\sigma_{\mathcal{J}_L/\mathcal{J}_K}$ et est de degré 2 car $w_P(\alpha_{w_P}) = w_{\overline{P}}(\alpha_{w_{\overline{P}}}) = v(\pi) = 1$ et $w(\alpha_w) = 0$ si $w \neq w_P$ et $w \neq w_{\overline{P}}$. □

4.5 Courbes de niveau 2

On va dans cette section donner la preuve du théorème 4.1.1 dont on rappelle les conditions :

La courbe projective plane $\mathcal{C}_F$ est définie par l'équation $F(X,Y,Z)=0$ où F est un polynôme homogène irréductible de degré d dans $\mathbb{R}[X,Y,Z]$. On suppose que $\mathcal{C}_F$ est sans point réel, de genre g et que tous ses points singuliers sont ordinaires. On suppose aussi que -1 n'est pas un carré dans le corps de fonctions $K=\mathbb{R}(\mathcal{C}_F)$, qui est alors de niveau 2, et le corps $L=\mathbb{C}(\mathcal{C}_F)=K(i)$ est une extension quadratique de K.

Pour démontrer le théorème 4.1.1, on va dans un premier temps (partie (A)) prouver, à l'aide des résultats sur les idèles établis précédemment et du théorème de Riemann-Roch, l'existence d'une fonction $\gamma\in L$ dont on aura borné le nombre de zéros et de pôles et vérifiant $N_{L/K}(\gamma)=-1$. Ensuite dans la partie (B), grâce à cette fonction γ, en appliquant une seconde fois le théorème de Riemann-Roch puis le théorème fondamental de Nœther, on montrera qu'il existe des polynômes homogènes A_1, A_2 et A_3 de $\mathbb{R}[X,Y,Z]$ de même degré total inférieur ou égal à N_F et vérifiant $(A_1)^2+(A_2)^2+(A_3)^2\equiv 0 \pmod F$.

(A) Borne sur le degré des diviseurs

Proposition 4.5.1 *Il existe $\gamma\in L$ vérifiant $N_{L/K}(\gamma)=-1$ et dont le diviseur s'écrit $div(\gamma)=D_0-D_1$ où D_0 et D_1 sont des diviseurs effectifs de degré inférieur ou égal à $g+1$.*

Preuve. Comme le corps K est de niveau 2, il existe β_1, $\beta_2\in K$ tels que $\beta_1^2+\beta_2^2=-1$. Si on pose $\beta=\beta_1+i\beta_2$ alors on a $\beta\in L$ et $N_{L/K}(\beta)=\beta_1^2+\beta_2^2=-1$.

On va maintenant, en raisonnant localement, construire à partir de β la fonction γ. Comme $N_{L/K}(\beta)=-1$, l'idèle de $\mathcal{J}_L$ associé à β, noté aussi β, vérifie $N_{\mathcal{J}_L/\mathcal{J}_K}(\beta)=-1$. Or d'après la proposition 4.4.6, il existe un idèle $\varepsilon\in\mathcal{J}_L$ tel que $N_{\mathcal{J}_L/\mathcal{J}_K}(\varepsilon)=-1$ et $\mathrm{div}(\varepsilon)=0$, donc l'idèle $\varepsilon\beta\in\mathcal{J}_L$ est de norme $N_{\mathcal{J}_L/\mathcal{J}_K}(\varepsilon\beta)=1$. D'après la proposition 4.3.10, il existe un idèle $\delta\in\mathcal{J}_L$ tel que $\varepsilon\beta=\delta^{-1}\sigma_{\mathcal{J}_L/\mathcal{J}_K}(\delta)$.

Lemme 4.5.2 *L'idèle δ ci-dessus peut être choisi de degré $g-1$.*

Preuve. En effet d'après la proposition 4.4.7, il existe des idèles de $\mathcal{J}_L$ de degré 2 invariants par conjugaison, donc quitte à multiplier δ par une puissance, éventuellement négative, d'un de ces idèles, on peut se ramener au cas où son degré est $g-1$ ou g et on aura toujours la relation $\varepsilon\beta = \delta^{-1}\sigma_{\mathcal{J}_L/\mathcal{J}_K}(\delta)$. De plus, d'après un résultat dû à Geyer [Ge], on sait que $\deg(\delta) \equiv g-1 \pmod 2$, ce qui achève la démonstration de ce lemme. □

Lemme 4.5.3 *L'idèle δ peut s'écrire sous la forme $h^{-1}\theta$ avec $h \in L$ et $\theta \in \mathcal{J}_L$ tel que div(θ) a au plus un pôle d'ordre inférieur à 1 et au plus g zéros comptés avec multiplicité.*

Preuve. On applique le théorème de Rieman-Roch au diviseur $H = nP + \mathrm{div}(\delta)$ où P est un point de Γ_F et $n \in \mathbb{N}$:

$$l(H) \geq \deg H + 1 - g = n + \deg(\delta) - g + 1.$$

Donc $l(H) \geq 1$ lorsque $n \geq g - \deg(\delta)$, on va donc prendre $n = g - \deg(\delta)$, c'est-à-dire $n = 1$ car δ est de degré $g-1$. Il existe alors une fonction $h \in \mathcal{L}(H)$, ce qui signifie que $\mathrm{div}(h) \geq -H = -(P + \mathrm{div}(\delta))$.

On pose $\theta = h\delta \in \mathcal{J}_L$, alors $\mathrm{div}(\theta) = \mathrm{div}(\delta) + \mathrm{div}(h) \geq -P$. De plus $h \in L$ donc $\deg(\mathrm{div}(h)) = 0$ d'où $\deg(\theta) = \deg(\delta) = g-1$. On en déduit que θ a au plus un pôle d'ordre 1 en P et au plus g zéros comptés avec multiplicité. □

On déduit facilement de ce lemme et de la proposition 4.4.1 le corollaire suivant :

Corollaire 4.5.4 *Le diviseur div($\sigma_{\mathcal{J}_L/\mathcal{J}_K}(\theta)$) a au plus g zéros comptés avec multiplicité et un seul pôle éventuel, d'ordre au plus 1, au point $\sigma(P) = \overline{P}$ conjugué du point P.*

On peut maintenant achever la démonstration de la proposition 4.5.1. On sait que :

$$\varepsilon\beta = \delta^{-1}\sigma_{\mathcal{J}_L/\mathcal{J}_K}(\delta) = h\theta^{-1}\sigma_{\mathcal{J}_L/\mathcal{J}_K}(h^{-1}\theta).$$

Mais, étant donné que $h \in L$, on a aussi :

$$\sigma_{\mathcal{J}_L/\mathcal{J}_K}(h^{-1}\theta) = \sigma_{\mathcal{J}_L/\mathcal{J}_K}(h)^{-1}\sigma_{\mathcal{J}_L/\mathcal{J}_K}(\theta) = \sigma_{L/K}(h)^{-1}\sigma_{\mathcal{J}_L/\mathcal{J}_K}(\theta).$$

On en déduit que :

$$h^{-1}\sigma_{L/K}(h)\beta = \varepsilon^{-1}\theta^{-1}\sigma_{\mathcal{J}_L/\mathcal{J}_K}(\theta).$$

On pose $\gamma = h^{-1}\sigma_{L/K}(h)\beta \in L$ et comme $N_{L/K}(\beta) = -1$, on a $N_{L/K}(\gamma) = -1$. D'autre part $\gamma = \varepsilon^{-1}\theta^{-1}\sigma_{\mathcal{J}_L/\mathcal{J}_K}(\theta) \in \mathcal{J}_L$ donc $\mathrm{div}(\gamma) = \mathrm{div}(\varepsilon^{-1}) + \mathrm{div}(\theta^{-1}) + \mathrm{div}(\sigma_{\mathcal{J}_L/\mathcal{J}_K}(\theta))$ et étant donné que $\mathrm{div}(\varepsilon) = 0$ alors $\mathrm{div}(\gamma) = \mathrm{div}(\sigma_{\mathcal{J}_L/\mathcal{J}_K}(\theta)) - \mathrm{div}(\theta)$. D'après les résultats précédents, γ a au plus $g+1$ zéros comptés avec multiplicité et au plus $g+1$ pôles comptés avec multiplicité, ce qui équivaut à écrire $\mathrm{div}(\gamma) = D_0 - D_1$ avec D_0, D_1 diviseurs effectifs de degré inférieur ou égal à $g+1$. □

Remarque 4.5.5 On notera que jusqu'à présent, on n'a pas utilisé la condition disant que tous les points singuliers de $\mathcal{C}_F$ sont ordinaires, en effet la proposition 4.5.1 est vraie pour toute courbe projective irréductible plane sans point réel telle que le corps de fonctions $K = \mathbb{R}(\mathcal{C}_F)$ est de niveau 2. Les conditions portant sur les points singuliers de $\mathcal{C}_F$ ne serviront que dans la partie suivante pour l'application du théorème fondamental de Nœther.

(B) Borne sur les degrés des représentants

On va maintenant prouver l'existence de polynômes homogènes U et V de même degré inférieur ou égal à un certain entier n_0 connu tels que $\frac{U}{V}$ est un représentant de la fonction $\gamma \in \mathbb{C}(\mathcal{C}_F)$. Cela se fait en deux étapes :

Proposition 4.5.6 *Si n est un entier supérieur à $\frac{1+2g+r}{d}$, la fonction γ peut s'écrire comme quotient $\frac{u}{v}$ avec u, $v \in L$ tels que $div(u) \geq E - n\,div(Z)$ et $div(v) \geq E - n\,div(Z)$ (on rappelle que E est le diviseur $\sum_{P\in\mathcal{C}} (\sum_{i=1}^{r_P}(r_P - 1)P_i)$).*

Preuve. On applique le théorème de Rieman-Roch au diviseur $D = -D_1 - E + n\mathrm{div}(Z)$ où D_1 est le diviseur des pôles de γ : comme le polynôme F définissant la courbe $\mathcal{C}_F$ est de degré d, alors $\deg(\mathrm{div}(Z)) = d$. D'autre part $\deg(E) = r$ donc $l(D) \geq -\deg D_1 - r + nd + 1 - g$.

On a donc $l(D) \geq 1$ lorsque $nd \geq g + \deg D_1 + r$. Mais, comme d'après la proposition 4.5.1, $\deg D_1 \leq g+1$, il suffit que $nd \geq 1+2g+r$ pour que $l(D) \geq 1$ et donc pour qu'il existe $v \in \mathcal{L}(D)$, c'est-à-dire $v \in L$ tel que $\mathrm{div}(v) \geq D_1 + E - n(Z)$.

On pose $u = \gamma v$, alors $u \in L$ et $\mathrm{div}(u) = \mathrm{div}(\gamma) + \mathrm{div}(v) = D_0 - D_1 + (v)$ d'où $\mathrm{div}(u) \geq D_0 + E - n(Z)$.

Etant donné que D_0 et D_1 sont des diviseurs effectifs, on pourra finalement écrire $\gamma = \frac{u}{v}$ avec u, v éléments de L tels que $\mathrm{div}(u) \geq E - n(Z)$ et $\mathrm{div}(v) \geq E - n(Z)$ dès que l'entier n est supérieur à $\left(\frac{1+2g+r}{d}\right)$. □

Ainsi, si on pose $n_0 = \left[\frac{1+2g+r}{d}\right] + 1$, il suffit d'appliquer la proposition précédente pour montrer qu'il existe u et v dans L tels que $\gamma = \frac{u}{v}$, $\mathrm{div}(u) \geq E - n_0(Z)$ et $\mathrm{div}(v) \geq E - n_0(Z)$.

Proposition 4.5.7 *Il existe des polynômes homogènes U et V de $\mathbb{C}[X,Y,Z]$ de degré total n_0 tels que $\frac{U}{Z^{n_0}}$ et $\frac{V}{Z^{n_0}}$ soient des représentants respectifs des fonctions u et v de L.*

Preuve. Soit $\frac{R}{S}$ un représentant dans $\mathbb{C}(X,Y,Z)$ de la fonction $u \in L = \mathbb{C}(\mathcal{C}_F)$, avec R et S polynômes homogènes de même degré dans $\mathbb{C}[X,Y,Z]$, on a alors $\mathrm{div}(u) = \mathrm{div}(R) - \mathrm{div}(S) \geq E - n_0(Z)$ d'où $\mathrm{div}(Z^{n_0}R) \geq \mathrm{div}(S) + E$ et d'après la proposition 4.2.5 appliquée à $Z^{n_0}R$ et S, les conditions de Nœther sont satisfaites en tout point de $\mathcal{C}_F$.

Ainsi, d'après le théorème fondamental de Nœther, il existe des polynômes homogènes U et T de $\mathbb{C}[X,Y,Z]$ tels que $Z^{n_0}R = US + TF$. Ces polynômes vérifient $\deg R + n_0 = \deg U + \deg S = \deg T + \deg F$ et comme $\deg R = \deg S$, alors U est de degré total n_0.

On peut alors écrire, dans $\mathbb{C}(X,Y,Z)$, $\frac{R}{S} = \frac{US+TF}{Z^{n_0}S} = \frac{U}{Z^{n_0}} + \frac{TF}{Z^{n_0}S}$ et donc $\frac{U}{Z^{n_0}}$ est un autre représentant dans $\mathbb{C}(X,Y,Z)$ de l'élément u de $\mathbb{C}(\mathcal{C}_F)$.

Etant donné qu'on a aussi $\mathrm{div}(v) \geq E - n_0(Z)$, on démontre de même qu'il existe un représentant dans $\mathbb{C}(X,Y,Z)$ de la fonction $v \in L$ de la forme $\frac{V}{Z^{n_0}}$ avec V polynôme homogène de degré total n_0. □

Corollaire 4.5.8 *Il existe des polynômes homogènes U et V de $\mathbb{C}[X,Y,Z]$ de degré total n_0 tels que $\frac{U}{V}$ soit un représentant dans $\mathbb{C}(X,Y,Z)$ de la fonction γ.*

Maintenant le théorème 4.1.1 se déduit directement de ce corollaire, il suffit de poser $U = U_1 + iU_2$ et $V = V_1 + iV_2$ où U_1, U_2, V_1 et V_2 sont des polynômes homogènes de $\mathbb{R}[X,Y,Z]$ de degré total n_0. Puisque $\mathrm{N}_{L/K}(\gamma) = -1$, $\frac{U_1^2+U_2^2}{V_1^2+V_2^2}$ est un représentant dans $\mathbb{R}(X,Y,Z)$ de $-1 \in L$. D'où on a, dans $\mathbb{R}(X,Y,Z)$, $U_1^2 + U_2^2 +$

$V_1^2 + V_2^2 \equiv 0 \pmod F$ et donc, en multipliant cette identité par $V_1^2 + V_2^2$ qui est non nul,

$$(U_1V_1 + U_2V_2)^2 + (U_1V_2 - U_2V_1)^2 + (V_1^2 + V_2^2)^2 \equiv 0 \pmod F.$$

On note $A_1 = U_1V_1 + U_2V_2$, $A_2 = U_1V_2 - U_2V_1$ et $A_3 = V_1^2 + V_2^2$ et on a, pour $i = 1, 2, 3$, $A_i \in \mathbb{R}[X, Y, Z]$, $\deg A_i = 2n_0$, et enfin $A_1^2 + A_2^2 + A_3^2 \equiv 0 \pmod F$.

Cela démontre le théorème 4.1.1, l'entier N_F étant donné par la relation $N_F = 2n_0 = 2\left[\frac{1+2g+r}{d}\right] + 2$.

On peut donner une version de ce théorème dans le cas d'une courbe affine, pour cela on introduit les notations suivantes : si $\mathcal{C}$ une courbe affine irréductible plane définie par l'équation $P(X, Y) = 0$ où P est un polynôme de degré total d dans $\mathbb{R}[X, Y]$, on définit $P^* \in \mathbb{R}[X, Y, Z]$ comme étant le polynôme homogénéisé de P, c'est-à-dire $P^*(X, Y, Z) = Z^d P(\frac{X}{Z}, \frac{Y}{Z})$, et on dira que la courbe projective $\mathcal{C}_{P^*}$ d'équation homogène $P^*(X, Y, Z) = 0$ est la courbe projectivisée de $\mathcal{C}$.

Théorème 4.5.9 *Soit $\mathcal{C}$ une courbe affine irréductible plane, sans point réel, de genre g, définie par l'équation $P(X, Y) = 0$ où P est un polynôme de degré total d dans $\mathbb{R}[X, Y]$. On suppose que tous les points singuliers de la courbe projectivisée de $\mathcal{C}$ sont ordinaires, si le corps de fonctions $K = \mathbb{R}(\mathcal{C})$ est de niveau 2 , alors il existe un entier $N_{\mathcal{C}}$ tel qu'on peut trouver des polynômes P_1, P_2, $P_3 \in \mathbb{R}[X, Y]$ de degré total inférieur ou égal à $N_{\mathcal{C}}$ et vérifiant $(P_1)^2 + (P_2)^2 + (P_3)^2 \equiv 0 \pmod P$. Cet entier $N_{\mathcal{C}}$ est encore donné par la formule $N_{\mathcal{C}} = 2\left[\frac{1+2g+r}{d}\right] + 2$.*

Preuve. En appliquant le théorème 4.1.1 à la courbe $\mathcal{C}_{P^*}$ projectivisée de $\mathcal{C}$, on sait qu'il existe des polynômes homogènes A_1, A_2, $A_3 \in \mathbb{R}[X, Y, Z]$ de degré total égal à $N_{P^*} = 2\left[\frac{1+2g+r}{d}\right] + 2$ tels que $(A_1)^2 + (A_2)^2 + (A_3)^2 \equiv 0 \pmod{P^*}$ dans $\mathbb{R}[X, Y, Z]$. Pour $i = 1, 2, 3$, on note P_i le polynôme déshomogénéisé de A_i, ces polynômes P_i sont clairement de degré total inférieur ou égal à $N_{\mathcal{C}} = N_{P^*}$ et on a bien $(P_1)^2 + (P_2)^2 + (P_3)^2 \equiv 0 \pmod P$ dans $\mathbb{R}[X, Y]$. □

Bibliographie

[Ca1] J.W.S. Cassels, On the representation of rationnal functions as sums of squares, **Acta Arith.**, 9, 79-82 (1964).

[Ca2] J.W.S. Cassels, Global Fields, in Algebraic number theory, J.W.S. Cassels, A. Frohlich, London New-York Academic Press, 42-84 (1967).

[CEP] J.W.S. Cassels, W.J. Ellison, A. Pfister, On sums of squares and on elliptic curves over function fields, **J. of Number Theory**, 3, 125-149 (1971).

[Chr] M.R. Christie, Positive definite functions of two variables which are not sums of three squares, **J. of Number Theory**, 8, 224-232 (1976).

[CT] J.L. Colliot-Thélène, The Nœther-Lefschetz theorem and sums of 4 squares in the rationnal function field $\mathbb{R}(x, y)$, **Compositio** 86, 235-243 (1993).

[Fu] W. Fulton, Algebraic curves, W.A. Benjamin, Inc. (1969).

[Ge] W.D. Geyer, Ein algebraischer Beweis des Satzes von Weichold über reele algebraische Funktionenkörper, Algebraische Zahlentheorie (Ber. Tagung Math. Forschungsinst. Oberwolfach, 1964) 83-98 Bibliographisches Institut, Mannheim (1967).

[He] Y. Hellegouarch, Etude des points d'ordre fini de varétés abĺiennes de dimension un définies sur un anneau principal, **J. Reine Angew. Math.**, 244, 20-36 (1970).

[Hi1] D. Hilbert, Über die Darstellung definiter Formen als Summe von Formenquadraten, **Math. Ann.**, 32, 342-350 (1888) = Ges Abh 2, 154-161.

[Hi2] D. Hilbert, Über ternäre definite Formen, **Acta Arith.**, 17, 169-197 (1893) = Ges Abh 2, 345-366.

[HM] J. Huisman, L. Mahé, Geometrical aspects of the level of curves, Prépublication IRMAR, Rennes 1 99-61 (1999).

[La] S. Lang, Survey of diophantine geometry, Springer (1997).

[Pf1] A. Pfister, Zur Darstellung definiter Funktionen als Summe von Quadraten, **Invent. Math.**, 4, 229-237 (1967).

[Pf2] A. Pfister, Small zeros of quadratic forms over algebraic function fields, **Acta Arith.**, LXXIX.3, 221-238 (1997).

[Wi] E. Witt, Zerlegung reeller algebraischer Funktionen in Quadrate, J. Crelle, Vol. 171, 4-11 (1934).