Points de Weierstrass et jacobienne de courbes algebriques de genre 3

Martine Girard

Université Paris 7 - Denis Diderot

THÈSE DE DOCTORAT

Spécialité : **Mathématiques**

Présentée par : **Martine GIRARD**

Sujet de la thèse :

Points de Weierstrass et jacobienne de courbes algébriques de genre 3

Soutenue le 21 juillet 2000 devant le jury composé de

John BOXALL (rapporteur)
Antoine CHAMBERT-LOIR
Marc HINDRY (directeur de thèse)
Jean-François MESTRE
Jean-Jacques SANSUC
René SCHOOF (rapporteur)

Remerciements

Je voudrais, tout d'abord, remercier mon directeur de thèse, Marc Hindry, pour sa patience (heureusement) inépuisable, sa disponibilité et sa gentillesse. Ces qualités, jointes à sa grande pédagogie que j'avais su apprécier dès le DEA, ne se sont jamais démenties.

Je suis honorée que John Boxall et René Schoof aient accepté d'être rapporteurs, tâche dont ils se sont acquittés avec diligence.

J'ai pu rencontrer John Boxall lors des divers colloques qu'il a organisés à Caen ou de son passage au séminaire à Paris. Je tiens à le remercier pour toutes ses judicieuses suggestions.

Quant à René Schoof, son cours sur les variétés abéliennes lors de l'école d'été sur les courbes elliptiques à Trieste en août 1997 a contribué à éclairer nombre de points obscurs. Je l'ai depuis revu avec plaisir. Je profite de l'occasion pour remercier les autres orateurs de cette école d'été, Bas Edixhoven, Gerhard Frey et Joseph Oesterlé.

Mon premier contact avec Jean-François Mestre fut par le biais d'un polycopié de licence où toutes les démonstrations se résumaient au seul mot «évident». J'ai depuis pu apprécier tant ses qualités d'enseignant que de chercheur, et je tiens à le remercier pour avoir répondu (plus amplement!) à mes questions les plus saugrenues sur les courbes elliptiques.

Je remercie Antoine Chambert-Loir et Jean-Jacques Sansuc d'avoir accepté de faire partie de mon jury.

Je profite de l'occasion pour remercier Joseph Le Potier, dont les cours, tant en maîtrise qu'en DEA m'ont enthousiasmée.

Je veux remercier Michèle Wasse pour sa grande compétence, Colette Orion pour sa gentillesse, Colette Valentin pour ses gâteaux, Marc Chardin, Eric Boix, Albert Shih, Catherine Flé et Joël Marchand pour des repas sans mathématiques.

Je tiens à remercier «mes p'tits camarades de bureau» (y compris notre logicien) et en particulier Leopoldo Kulesz, pour m'avoir supportée (sans anglicisme aucun) durant ces années de thèse, quelques (ex-) thésards de problèmes diophantiens, Hervé Billard, Vincent Bosser, Marc Halberstadt, Jean-Christophe Masseron et Federico Pellarin et enfin, toutes les personnes du «monde extérieur» qui m'ont soutenue pendant la durée de cette thèse.

Table des matières

Introduction

Cette thèse a pour thème la géométrie des courbes algébriques et de leur jacobienne (en caractéristique 0). Elle a, en particulier, pour objet l'étude du groupe engendré dans la jacobienne par les points de Weierstrass pour certaines courbes de genre 3.

Les points de Weierstrass sont les seuls points intrinsèques sur les courbes algébriques. Ce sont les points P tels qu'il existe une forme différentielle régulière s'annulant au moins à l'ordre g en P. Ces points sont très liés aux espaces de modules (voir par exemple, Eisenbud-Harris ([EH]), Arbarello ([Arb]), Diaz ([Dia]), Lax ([Lax])). En effet, les points de Weierstrass permettent d'obtenir diverses stratifications de l'espace de modules $\mathcal{M}_g$ des courbes lisses de genre g, en considérant, par exemple, le lieu des courbes possédant un point de Weierstrass avec une suite de lacunes fixée ([EH]) ou, plus grossièrement, le lieu $\mathcal{W}_\alpha$ des courbes possédant un point de Weierstrass P tel que $\ell(\alpha P) \geq 2$ ([Arb]). Signalons aussi la stratification de $\mathcal{M}_3$ due à Vermeulen ([Ver]) en fonction du nombre de points d'hyper-inflexion.

D'autre part, nous pouvons définir des points de Weierstrass d'ordre supérieur. Ce sont les points P où il existe une forme différentielle de poids n s'annulant au moins à l'ordre $(2n-1)(g-1)$. Ceux-ci permettent de construire explicitement l'espace de modules $\mathcal{M}_g$ (voir le paragraphe 1.2).

Soit $\mathcal{C}$ une courbe lisse de genre g. Après avoir choisi un point de Weierstrass, nous disposons d'un plongement de cette courbe dans sa jacobienne. Le groupe W engendré par les images des points de Weierstrass est indépendant du choix de la base du plongement. Nous disposons ainsi d'un invariant de la courbe, qui est l'objet de notre étude. Plus précisément, nous allons déterminer la structure de W pour diverses familles de courbes.

Nous nous intéressons aux quartiques planes lisses. En effet, pour les courbes hyperelliptiques, le groupe engendré par les points de Weierstrass dans la jacobienne est connu et est égal au groupe des points d'ordre 2 de la jacobienne, isomorphe à $(\mathbb{Z}/2\mathbb{Z})^{2g}$ (nous redonnons une démonstration de ce résultat au paragraphe 1.5). Les quartiques planes lisses sont donc les courbes lisses de plus petit genre pour lesquelles la structure de ce groupe n'est pas connue. Pour certaines courbes de genre 3, possédant beaucoup d'automorphismes, le groupe W a été déterminé explicitement :

- Pour la quartique de Klein (d'équation $X^3Y + Y^3Z + Z^3X = 0$), qui possède 168 automorphismes, $W = (\mathbb{Z}/2\,\mathbb{Z}) \times (\mathbb{Z}/7\,\mathbb{Z})^3$ ([Pra]).

- Pour la courbe de Fermat (d'équation $X^4 + Y^4 = Z^4$), qui possède 96 automorphismes, $W = (\mathbb{Z}/4\,\mathbb{Z})^5 \times (\mathbb{Z}/2\,\mathbb{Z})$ ([Roh]).
- Pour la courbe de Picard (d'équation $Y^3Z + Z^4 = X^4$), qui possède 48 automorphismes, $W = (\mathbb{Z}/4\,\mathbb{Z})^2 \times (\mathbb{Z}/3\,\mathbb{Z})^5$ ([KS]).

Remarquons que dans chacun de ces cas, la jacobienne est isogène au produit de trois courbes elliptiques à multiplication complexe.

Nous déterminons la structure de W pour certaines familles de courbes. Pour ce faire, nous procédons en deux étapes. Nous utilisons tout d'abord la géométrie de la courbe et de sa jacobienne pour restreindre le groupe cherché. Les restrictions obtenues par ces arguments géométriques s'avèreront être optimales. Pour démontrer cela, nous utilisons différentes techniques : dans la deuxième partie, nous appliquons une descente explicite via une isogénie (due à Schaefer ([Sch])) ; dans la troisième partie, nous utilisons des arguments de réduction modulo p. Lorsque nous nous intéressons à des familles, ces restrictions «d'ordre géométrique» s'obtiennent pour toute la famille. Par contre, les techniques mises en œuvre lors de la seconde étape ne nous donnent le résultat que pour une courbe particulière. Dans chaque cas, un argument de spécialisation nous permettra de conclure. Plus précisément :

-dans la deuxième partie, nous démontrons, pour une certaine famille de quartiques planes lisses contenant la courbe de Picard, le résultat suivant :

Théorème 2.1.1 *Soit $\mathcal{C}_\beta$ la courbe projective lisse birationnelle à la courbe affine $y^3 = x(x-1)(x^2 - 2\beta x + \beta)$ où $\beta \notin \{0,1,1/2\}$. Pour tout corps de nombres K, il existe un ensemble fini S_K tel que si $\beta \in K \setminus S_K$ alors $W_{\mathcal{C}_\beta} \cong \mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5$. Par exemple, $\beta = 784/6859$ n'appartient pas à S_K.*

-dans la troisième partie, nous démontrons, pour une certaine famille de quartiques planes lisses joignant la courbe de Picard à la courbe de Fermat, le résultat suivant :

Théorème 3.1.1 *Soit $\mathcal{C}_t$ la courbe projective lisse birationnelle à la courbe affine $y^4 = x(x-1)(x-t)$ où $t \notin \{0,1\}$. Pour tout corps de nombres K, il existe un ensemble fini S_K tel que si $t \in K \setminus S_K$ alors $W_{\mathcal{C}_t} \cong \mathbb{Z}^9 \times (\mathbb{Z}/4\mathbb{Z})^2$. Par exemple, $t = 76834/39593$ n'appartient pas à S_K.*

-dans la quatrième partie, nous déterminons ce groupe pour la seule courbe de genre 3, autre que la courbe de Fermat, possédant le nombre minimal de points de Weierstrass, à savoir douze :

Théorème 4.1.1 *Soit W le groupe engendré par les images des points de Weierstrass dans la jacobienne de la courbe projective lisse d'équation $X^4 + Y^4 + Z^4 + 3\,(X^2Y^2 + X^2Z^2 + Y^2Z^2) = 0$, alors $W \cong (\mathbb{Z}/4\mathbb{Z})^5$.*

Comme les points de Weierstrass «bougent en famille» (c'est-à-dire que si $\mathcal{C} \to T$ est une famille de courbes, il existe un diviseur D sur $\mathcal{C}$ tel que D_t soit le diviseur des points de Weierstrass de $\mathcal{C}_t$ *i.e.* la somme des points de Weierstrass comptés avec multiplicité), nous pouvions déjà déduire des résultats précédemment cités (de Rohrlich ([Roh]), de Prapavessi ([Pra]) et de Klassen et Schaefer ([KS])) des informations sur le groupe engendré par les points de Weierstrass W_η d'une quartique générique ; en effet, nous pouvions déjà obtenir la minoration $\mathrm{rang}_{\mathbb{Z}} \mathrm{W}_\eta \geq 8$. D'autre part, comme la spécialisation est injective sur la partie de torsion, nous pouvions déjà conclure que la partie finie de W_η est nulle ou isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

Les théorèmes ci-dessus permettent d'améliorer ces résultats. En effet, le résultat de la deuxième partie a pour corollaire direct que W_η est un groupe abélien libre et que $\mathrm{rang}_{\mathbb{Z}} \mathrm{W}_\eta \geq 9$; celui de la troisième partie entraîne que $\mathrm{rang}_{\mathbb{Z}} \mathrm{W}_\eta \geq 11$. Notons qu'un argument «naïf» (explicité au paragraphe 1.4) donne seulement $\mathrm{rang}_{\mathbb{Z}} \mathrm{W}_\eta \geq 6$.

Nous appelons point d'hyper-inflexion un point où la tangente a multiplicité d'intersection 4 avec la courbe. Si $\mathcal{M}_3^\circ$ est l'espace de modules de courbes de genre 3 non-hyperelliptiques, $Z_s = \{[C] \in \mathcal{M}_3^\circ,\ C$ possède au moins s points d'hyper-inflexion $\}$ et $Z_s^\circ = \{[C] \in \mathcal{M}_3^\circ,\ C$ possède exactement s points d'hyper-inflexion $\}$, Vermeulen ([Ver]) donne une description explicite des composantes irréductibles de chacun des Z_s. En particulier, Z_1 et Z_2 sont irréductibles, Z_3° possède deux composantes irréductibles et Z_4 en possède cinq.
Nous obtenons les deux théorèmes suivants :

Théorème 1.4.4 *Le groupe W_η engendré par les points de Weierstrass d'une quartique lisse générique possédant 4 points d'hyper-inflexion alignés est $\mathbb{Z}^r \times (\mathbb{Z}/4\mathbb{Z})^2$ avec $9 \leq r \leq 15$.*

Théorème 1.4.5 *Soit W_η le groupe engendré par les points de Weierstrass d'une quartique lisse générique possédant s points d'hyper-inflexion.*

- *Pour une quartique lisse générique (sans point d'hyper-inflexion), $W_\eta = \mathbb{Z}^r$ avec $11 \leq r \leq 23$.*
- *Pour une quartique lisse générique avec un point d'hyper-inflexion (i.e. un point générique de Z_1), $W_\eta = \mathbb{Z}^r$ avec $11 \leq r \leq 21$.*

- *Pour une quartique lisse générique avec 2 points d'hyper-inflexion (i.e. un point générique de Z_2), W_η est un quotient de $\mathbb{Z}^{19} \times (\mathbb{Z}/4\mathbb{Z})$ qui contient $(\mathbb{Z}/4\mathbb{Z})$.*
- *Pour chaque composante irréductible de Z_3°, le groupe W_η engendré par les points de Weierstrass d'une quartique lisse générique est un quotient de $\mathbb{Z}^{17} \times (\mathbb{Z}/4\mathbb{Z})^2$ qui contient $(\mathbb{Z}/4\mathbb{Z})^2$.*
- *Pour une quartique lisse générique avec 4 points d'hyper-inflexion tels qu'il y ait une conique tangente à la courbe en ces 4 points, W_η est un quotient de $\mathbb{Z}^{15} \times (\mathbb{Z}/4\mathbb{Z})^3$ qui contient $(\mathbb{Z}/4\mathbb{Z})^2 \times (\mathbb{Z}/2\mathbb{Z})$.*
- *Pour une quartique lisse générique de l'une des trois autres composantes de $\mathbb{Z}_4^\circ$ telles que aucun triplet de points d'hyper-inflexion n'est aligné, W_η est un quotient de $\mathbb{Z}^{15} \times (\mathbb{Z}/4\mathbb{Z})^3$ qui contient $(\mathbb{Z}/4\mathbb{Z})^3$.*

Cette thèse est composée de quatre parties : la première consiste en des généralités sur les points de Weierstrass, ainsi qu'en des résultats qui nous seront utiles par la suite (le paragraphe 1.4 contient la discussion sur le groupe $W_\mathcal{C}$ en fonction du nombre de points d'hyper-inflexion, ainsi que les preuves des théorèmes 1.4.4 et 1.4.5) ; les trois autres sont rédigées sous forme d'articles indépendants.

Dans la deuxième partie, nous considérons la famille $\mathcal{C}_\beta$ de courbes d'équation affine $y^3 = x(x-1)(x^2 - 2\beta x + \beta)$ avec $\beta \notin \{0,1\}$. Une courbe de cette famille (lorsque $\beta \neq 1/2$) possède 23 points de Weierstrass et son groupe d'automorphismes est $\mathbb{Z}/3\mathbb{Z}$. Pour $\beta = 1/2$, c'est la courbe de Picard, qui possède 20 points de Weierstrass et 48 automorphismes. Nous déterminons explicitement les points de Weierstrass et montrons qu'ils sont dans une configuration particulière, à savoir qu'il existe des droites (autres que celles qu'on attend) passant par quatre de ces points. Cela nous permet de réduire considérablement le nombre de générateurs de W : on obtient que W est un quotient de $\mathbb{Z}^4 \times (\mathbb{Z}/3\,\mathbb{Z})^5$ (proposition 2.3.1). En effectuant une descente via une isogénie (dont nous rappelons le principe au paragraphe 2.4), nous montrons que pour une certaine valeur du paramètre β, le groupe $W_{\mathcal{C}_\beta}$ est isomorphe à $\mathbb{Z}^4 \times (\mathbb{Z}/3\,\mathbb{Z})^5$ (proposition 2.5.1). Un argument de spécialisation dû à Silverman (1.3.5) nous permet d'obtenir le théorème 2.1.1. Nous en déduisons l'existence d'une famille où ce groupe est $\mathbb{Z}^r$ avec $9 \leq r \leq 23$.

Dans la troisième partie, nous considérons la famille $\mathcal{C}_t$ de courbes d'équation affine $y^4 = x(x-1)(x-t)$ avec $t \notin \{0,1\}$. Une courbe de cette famille

(lorsque $t \notin \{-1,2,1/2,(1 \pm i\sqrt{3})/2\}$) possède 20 points de Weierstrass et admet seize automorphismes. Pour $t \in \{(1 \pm i\sqrt{3})/2\}$, c'est la courbe de Picard, qui possède 20 points de Weierstrass et admet 48 automorphismes. Pour $t \in \{-1,2,1/2\}$, c'est la courbe de Fermat, qui possède 12 points de Weierstrass et admet 96 automorphismes. Nous déterminons explicitement les points de Weierstrass, ainsi que le groupe d'automorphismes. Nous montrons que la jacobienne est isogène à un produit de trois courbes elliptiques $\mathcal{E}_1 \times \mathcal{E}_2 \times \mathcal{E}_3$, que nous déterminons explicitement au paragraphe 3.5. Une étude géométrique des images des points de Weierstrass dans la première courbe elliptique (au paragraphe 3.4) permet de réduire le nombre de générateurs de W. Plus précisément, nous obtenons que W est un quotient de $\mathbb{Z}^9 \times (\mathbb{Z}/4\mathbb{Z})^2$ (proposition 3.4.2). Nous montrons alors, que pour une valeur particulière de t (à savoir $t = 76834/39593$), le groupe $W_{\mathcal{C}_{t_0}}$ est isomorphe à $\mathbb{Z}^9 \times (\mathbb{Z}/4\mathbb{Z})^2$ (proposition 3.6.1). Pour ce faire, nous allons regarder ce qu'il advient des images de certains points de Weierstrass sur chacune des courbes elliptiques lorsque l'on réduit modulo une place de bonne réduction. Le même argument de spécialisation que précédemment nous permet alors d'obtenir le théorème 3.1.1. Nous en déduisons l'existence d'une famille, où ce groupe est $\mathbb{Z}^r$ avec $11 \leq r \leq 23$. Nous donnons en appendice une démonstration du fait que le groupe W est égal à $(\mathbb{Z}/4\,\mathbb{Z})^5 \times (\mathbb{Z}/2\,\mathbb{Z})$ pour la courbe de Fermat (correspondant à $t = -1$).

Dans la quatrième partie, nous étudions la courbe plane projective d'équation $X^4+Y^4+Z^4+3\,(X^2Y^2+X^2Z^2+Y^2Z^2) = 0$. Cette courbe possède douze points de Weierstrass et admet 24 automorphismes. Là encore, les points de Weierstrass sont dans une configuration particulière ; cela permet de montrer que W est un quotient de $(\mathbb{Z}/4\mathbb{Z})^5$. Nous montrons que la jacobienne est isogène au produit de 3 fois la même courbe elliptique. Cette isogénie nous permet de montrer que W est isomorphe à $(\mathbb{Z}/4\mathbb{Z})^5$.

La majorité des calculs ont été effectués sur ordinateur, à l'aide d'outils de calcul formel, en particulier à l'aide de maple.

Première partie

Généralités sur les points de Weierstrass

Nous rappelons dans cette partie, d'une part, la définition et quelques propriétés bien connues des points de Weierstrass (voir, par exemple, [ACGH], [Mur] ou [HS]), d'autre part, des résultats qui nous serons utiles par la suite. En outre, nous y discutons brièvement des espaces de modules. Seule la partie 1.4 est nouvelle (lemmes 1.4.1 et 1.4.2, proposition 1.4.3, théorèmes 1.4.4 et 1.4.5), à notre connaissance. Par la suite, $\mathcal{C}$ désigne une courbe lisse projective de genre $g \geq 2$ et P un point de la courbe $\mathcal{C}$. Nous travaillons en caractéristique 0.

1.1 Points de Weierstrass

1.1.1 Définitions

Notons $\ell(D) - 1$ la dimension du système linéaire associé à un diviseur D de $\mathcal{C}$.

Définition : On définit $G(P) = \{n \in \mathbb{N}^* \mid \ell(nP) = \ell((n-1)P)\}$.

Définition : On dit que P est un point de Weierstrass si et seulement si $G(P) \neq \{1, \ldots, g\}$.

Le théorème de Riemann-Roch permet de démontrer facilement que :

Proposition 1.1.1. *Les propriétés suivantes sont équivalentes:*

- *P est un point de Weierstrass.*
- *Il existe une forme différentielle qui s'annule à l'ordre au moins g en P.*
- *$\ell(gP) \geq 2$.*

Définition : On définit le poids d'un point de Weierstrass par

$$w(P) = \sum_{n \in G(P)} n \; - \; \frac{g(g+1)}{2}.$$

Proposition 1.1.2. *On a :*

- *$w(P) \geq 0$ pour tout P.*
- *$w(P) \geq 1$ si et seulement si P est un point de Weierstrass.*

Remarque : En général, pour un point de Weierstrass, $w(P) = 1$. ∎

Soient $\omega_1, \ldots, \omega_g$ une base des 1-formes différentielles régulières. Soit x un paramètre local, il existe des fonctions rationnelles $f_i \in k(\mathcal{C})$ telles que $\omega_i = f_i(x)\, dx$.

On définit une fonction $Wr = Wr(f_1, \ldots, f_g)$ appelé wronskien par: $Wr(x) = \det\left(\left(\frac{d}{dx}\right)^{j-1} f_i(x)\right)_{1 \leq i,j \leq g}$.

Proposition 1.1.3. *Le wronskien Wr s'annule en P si et seulement si P est un point de Weierstrass.*

On définit alors une forme différentielle de poids $g(g+1)/2$ (*i.e.* une section de $\omega^{\frac{g(g+1)}{2}}$) par $\widetilde{\omega} = Wr(x)(dx)^{g(g+1)/2}$.

Proposition 1.1.4. *Le diviseur de $\widetilde{\omega}$ est $\sum w(P)\, P$.*

Corollaire 1.1.5. *Le poids total des points de Weierstrass est $(g-1)\, g\, (g+1)$.*

Remarque : En particulier, div $(\widetilde{\omega})$ est linéairement équivalent à $\dfrac{g(g+1)}{2} K_{\mathcal{C}}$.

■

1.1.2 Plongement dans la jacobienne

Pour un diviseur D, on note $[D]$ sa classe dans $\mathrm{Pic}^0(\mathcal{C})$. Choisissons un point de Weierstrass, qui sera noté ∞. On note J la jacobienne que l'on identifiera à $\mathrm{Pic}^0(\mathcal{C})$ et on définit le plongement jacobien suivant

$$j : \begin{array}{ccc} \mathcal{C} & \to & J \\ P & \mapsto & [P - \infty] \end{array}$$

que l'on étend par linéarité aux diviseurs $\mathrm{Div}(\mathcal{C})$.

Nous nous intéressons alors à la structure du groupe W engendré par les images par j des points de Weierstrass dans la jacobienne de $\mathcal{C}$. Cette structure est indépendante du point de Weierstrass choisi comme base du plongement.

Remarque : Dans le cas des quartiques planes lisses (qui est le cas que nous étudierons), nous commettrons l'abus de notation suivant : soient P_1,P_2,P_3,P_4 les quatre points d'intersection d'une droite $\mathcal{D}$ de $\mathbb{P}^2(\overline{\mathbb{Q}})$ avec $\mathcal{C}$. On a alors $j\,(\mathcal{C}.\mathcal{D}) = [P_1 + P_2 + P_3 + P_4 - 4\,\infty]$ Par la suite, on identifiera un point de Weierstrass avec son image par j et donc, si quatre points de $\mathcal{C}$ sont alignés, on dira que leur somme est nulle et on notera cela $P_1 + P_2 + P_3 + P_4 = 0$.

■

1.2 Points de Weierstrass d'ordre supérieur

Nous pouvons définir de manière similaire des points de Weierstrass d'ordre supérieur (d'ordre $n \geq 2$), comme les points P pour lesquels $\ell(nK_C - sP) \geq 1$ avec $s = (2n-1)(g-1)$ (dans le cas où $n = 1$, pour retrouver la définition usuelle des points de Weierstrass, il faut poser $s = g$). Nous pouvons leur associer une suite de lacunes et définir un poids de la même façon que pour les points de Weierstrass usuels.

Mumford ([Mum2]) suggère que ces points de Weierstrass d'ordre n sont les analogues des points de n-torsion dans le cas des courbes elliptiques. En particulier, ils permettent de construire explicitement l'espace de modules (grossier) des courbes de genre g (cf [Mum2] p30).

En effet, pour une courbe C de genre g, l'espace des formes différentielles de poids n, $H^0(C, \omega^{\otimes n})$ a pour dimension $d_n = (2n-1)(g-1)$. Choisissons une base $(\omega_i)_{1 \leq i \leq d_n}$ de cet espace. Le plongement (lorsque $n \geq 3$) pluri-canonique $C \to \mathbb{P}^{d_n - 1}$ est alors donné par $x \mapsto (w_1(x), \ldots, w_{d_n}(x))$.

Les points de Weierstrass d'ordre n comptés avec multiplicité égale à leur poids sont au nombre de $e_n = g\, d_n^2 = g(g-1)^2(2n-1)^2$. Notons les x_i pour $1 \leq i \leq e_n$.

Considérons alors pour tout sous-ensemble I de $\{1, \ldots, e_n\}$ de cardinal d_n, le mineur $M_I = \det((\omega_i(x_j))_{1 \leq i \leq d_n, j \in I})$.

C'est un élément de $H^0(C \times \ldots \times C, \otimes\, p_j^*(\omega_C))$ évalué au point $(x_j)_{j \in I}$.

Pour N_0 suffisamment grand, considérons les monômes en ces mineurs définis de la manière suivante

$$M_r = \prod_I M_I^{r_I}$$

où les r_I sont des entiers positifs tels que pour tout $i \in \{1, \ldots, e_n\}$, on ait $\sum_{I / i \in I} r_I = N_0$.

Ces monômes sont alors des produits de formes différentielles de poids nN_0 en chacun des x_i. Le quotient de deux de ces monômes est une fonction bien définie. Ainsi, s'il y a μ choix possibles d'entiers positifs r_I tels que $\sum_{I / i \in I} r_I = N_0$ pour tout i, les M_r définissent un point de $\mathbb{P}^{\mu - 1}$.

Ce point de $\mathbb{P}^{\mu-1}$ dépend de l'ordre de numérotation des points de Weierstrass d'ordre n. Pour enlever cette dépendance, on considère les

$$M'_r = \sum_{\sigma \in \mathfrak{S}_{e_n}} \prod_I M_{\sigma(I)}^{r_I}.$$

Les quotients M'_{r_1}/M'_{r_2} ne dépendent alors, ni du choix de la base de $H^0(C,\omega^{\otimes n})$, ni de l'ordre dans lequel on considère les points de Weierstrass d'ordre n. Les M'_r définissent alors un point de $\mathbb{P}^{\mu-1}$ qui ne dépend que de la classe d'isomorphisme de la courbe C.

Chaque courbe de genre g est plongée par le plongement n-canonique dans $\mathbb{P}^{(2n-1)(g-1)-1} = \mathbb{P}^N$. L'ensemble des paires formées d'une courbe $\mathcal{C}$ et d'un plongement n-canonique de $\mathcal{C}$ dans $\mathbb{P}^N$ est un sous-schéma $\mathcal{H}$ du schéma de Hilbert des courbes lisses de degré $2(g-1)n$ et de genre g de $\mathbb{P}^N$ qui est muni d'une action de $PGL(N+1)$. L'espace des modules $\mathcal{M}_g$ correspond au quotient de $\mathcal{H}$ par $PGL(N+1)$ ([MF], Appendix 7C).

La construction décrite ci-dessus permet d'obtenir explicitement l'espace de modules des courbes projectives lisses de genre g ; en effet, à une courbe C munie d'une base de ses formes différentielles de poids n et de ses points de Weierstrass d'ordre n ordonnés, nous associons un point de $\mathbb{P}^{\mu-1}$. Ce point a été construit de sorte à être indépendant de l'ordre sur les points de Weierstrass. De plus, il est aisé de voir qu'il ne change pas si l'on change la base des formes différentielles de poids n.

D'autre part, comme un isomorphisme entre deux courbes C et C' induit un isomorphisme entre $H^0(C',\omega_{C'}^{\otimes n})$ et $H^0(C,\omega_C^{\otimes n})$, deux courbes isomorphes ont même image dans $\mathbb{P}^{\mu-1}$.

La réciproque est vraie, ce qui est plus ardu à montrer ([MF], Appendix 7C), et donc, deux courbes non-isomorphes donnent des points distincts de $\mathbb{P}^{\mu-1}$. Le sous-schéma de $\mathbb{P}^{\mu-1}$ ainsi construit est donc l'espace des modules $\mathcal{M}_g$.

Notation: Nous noterons $W^{(n)}$ le groupe engendré par les points de Weierstrass d'ordre n. Le groupe W correspond à $W^{(1)}$.

1.3 Spécialisation des points de Weierstrass

Soit X une surface de Riemann compacte de genre g, et $\mathcal{F}$ un faisceau inversible sur X de degré d. Soit $n = \dim H^0(X,\mathcal{F})$, et $f_1,\ldots,f_n$ une base de $H^0(X,\mathcal{F})$ telle que $v_x(f_1) < v_x(f_2) < \cdots < v_x(f_n)$ (où l'on note v_x l'ordre d'annulation de f en x). On appelle trous de $\mathcal{F}$ en x les entiers $a_i = v_x(f_i)+1$. Ils satisfont aux inégalités $1 \leq a_1 < a_2 < \ldots < a_n \leq d+1 \leq n+g$. Le poids de $\mathcal{F}$ en x est l'entier $w(x) = \sum(a_i - i)$, et x est un point de Weierstrass si

et seulement si $w(x) > 0$.

Proposition 1.3.1 ([Hub]). *Il existe une section holomorphe $wr(f_1,\ldots,f_n)$ de $\mathcal{F}^{\otimes n}\otimes\omega^{\otimes(n(n-1)/2)}$ dont l'expression dans toute carte et toute trivialisation de $\mathcal{F}$ soit le wronskien des expressions de $f_1,\ldots,f_n$.*

En particulier, si l'on considère le faisceau canonique ω_X, on a $n = g$, $d = 2g-2$, on retrouve les points de Weierstrass usuels.

Notation: On note X_s la fibre au dessus de s.

Théorème 1.3.2 ([Hub]). *Soit $X \to S$ une courbe propre et lisse sur S, et $\mathcal{F}$ un faisceau inversible sur X, tel que la fonction $s \mapsto \dim H^0(X_s,\mathcal{F}\,|X_s)$ soit constante. Il existe un sous-espace analytique fermé $W \subset X$, plat sur S tel que $W \cap X_s$ soit le diviseur des points de Weierstrass de $\mathcal{F}\,|X_s$ avec leur poids.*

Lorsque l'on considère le faisceau canonique ω_X (resp. une puissance d'icelui), on a $s \mapsto \dim H^0(X_s,\omega_{X_s}) = g$ (resp. $s \mapsto \dim H^0(X_s,\omega_{X_s}^{\otimes n}) = (2n-1)(g-1)$) est constante. Auquel cas, on retrouve les points de Weierstrass usuels (resp. d'ordre n) sur chaque fibre.

En particulier, considérons une famille de courbes projectives lisses $X \to S$ de genre g. Soit η le point générique de S, et soit s un point spécial de S. Notons W_{X_η} (resp. $W_{X_\eta}^{(n)}$) le groupe engendré par les points de Weierstrass (resp. d'ordre n) de la fibre générique X_η et W_{X_s} (resp. $W_{X_s}^{(n)}$) celui engendré par les points de Weierstrass (resp. d'ordre n) d'une fibre spéciale X_s. On a alors: la spécialisation $W_{X\eta} \to W_{Xs}$ (resp. $W_{X\eta}^{(n)} \to W_{X_s}^{(n)}$) est surjective; par ailleurs, on sait qu'elle est injective sur les points de torsion (voir, par exemple [Mil1] ou [HS], Theorem C.1.4)).

Nous en déduisons que

Proposition 1.3.3. *Soit $X \to S$ une famille de courbes lisses de genre g.*

a) Le groupe engendré par les points de Weierstrass (d'ordre n) d'une fibre spéciale X_s est un quotient de celui engendré par les points de Weierstrass (d'ordre n) de la fibre générique X_η.

b) De plus, le passage au quotient est injectif sur la partie de torsion.

Remarque : Ces résultats semblent «classiques » (voir, par exemple ([LT]).∎

Citons enfin les théorèmes suivants de spécialisation sur les familles de variétés abéliennes :

Le premier est dû à Néron, le second à Silverman.

Théorème 1.3.4 (Néron [Ser]). *Soit k un corps de nombres, et soit A une variété abélienne définie sur $K = k(T_1, \ldots, T_n)$, où les T_i sont des indéterminées. Le groupe $A(K)$ est de type fini. Soit U un ouvert de $\mathbb{P}^n$ au-dessus duquel A se prolonge en un schéma abélien. L'ensemble $\{t \in U(k) \mid A(K) \to A_t(k)$ n'est pas injective $\}$ est un ensemble mince.*

Théorème 1.3.5 ([Sil1]). *Soit $A \to C$ une famille (plate) de variétés abéliennes toutes définies sur un corps global K, où C est une courbe projective lisse. En un point $t \in C(\overline{K})$ pour lequel la fibre A_t est non-singulière, on définit l'application de spécialisation $\sigma_t : A(C) \to A_t(\overline{K}), \quad P \mapsto P_t$.*

Si A n'a pas de partie constante, alors l'ensemble $\{t \in C(\overline{K}) \mid \sigma_t$ n'est pas injective $\}$ est un ensemble de hauteur bornée dans $C(\overline{K})$.

En particulier, lorsque K est un corps de nombres et $d \geq 1$ est un entier, alors σ_t est injective pour presque tout $t \in \bigcup_{[L:K] \leq d} C(L)$.

Nous utiliserons le théorème de Silverman, qui bien que plus restrictif quant aux conditions d'application, donne une meilleure caractérisation des valeurs de t où la spécialisation est non-injective.

1.4 Courbes lisses de genre 3

Soit $\mathcal{C}$ une courbe lisse de genre 3. Elle est soit hyperelliptique, soit son diviseur canonique $K_{\mathcal{C}}$ est très ample. Dans ce dernier cas, comme $\ell(K_{\mathcal{C}}) = 3$, nous disposons d'un plongement $\varphi_{K_{\mathcal{C}}}$ de $\mathcal{C}$ dans $\mathbb{P}^2$. De plus, comme $\deg(\varphi_{K_{\mathcal{C}}}) = \deg(K_{\mathcal{C}}) = 4$, $\mathcal{C}$ est isomorphe à une quartique plane.

Dans le cas d'une quartique lisse, les points de Weierstrass sont ses points d'inflexion. Ce sont les points où la multiplicité d'intersection avec leur tangente excède 3. Nous appellerons *points d'hyper-inflexion* les points de Weierstrass ayant 4 comme multiplicité d'intersection avec leur tangente. Une courbe de genre 3 possède au plus 24 points de Weierstrass, une courbe générale en possède exactement 24.

Remarque : Les points d'hyper-inflexion restent des points de Weierstrass d'ordre n pour tout n. ∎

Pour une quartique lisse possédant s points d'hyper-inflexion et r points de Weierstrass ordinaires, on a $r + 2s = 24$. De plus, en prenant un point d'hyper-inflexion comme base du plongement, nous obtenons que W est un quotient de $\mathbb{Z}^r \times (\mathbb{Z}/4\mathbb{Z})^{s-1}$; en effet, un point d'hyper-inflexion définit un

point d'ordre 4 dans la jacobienne (voir lemme ci-dessous). Nous pouvons obtenir une estimation plus précise de W en fonction du nombre de points d'hyper-inflexion.

Soit une quartique plane quelconque. Elle correspond à un point d'un ouvert de $\mathbb{P}^{14}$. En prenant 7 points génériquement indépendants, on peut imposer que chacun de ces points soit un point d'inflexion ; cela revient à imposer, à chaque fois, deux conditions sur les coordonnées de cette quartique. On peut donc obtenir une quartique avec 7 points d'inflexion génériquement indépendants. Cela permet de construire une quartique avec W de rang au moins 6.

Pour une quartique générique, W est au moins de rang 6, et a priori, au vu des exemples connus, rien ne permet d'exclure que la partie finie de W soit isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Nous allons montrer qu'il n'y a pas de partie de torsion, et que le rang est d'abord supérieur à 9 (à la deuxième partie), puis supérieur à 11 (à la troisième partie).

D'autre part, comme nous choisissons un point de Weierstrass comme base du plongement jacobien, nous avons la majoration $\mathrm{rang}_{\mathbb{Z}}\mathrm{W} \leq 23$. Si de plus, nous choisissons ∞ parmi les points d'hyper-inflexion, 4∞ est un diviseur canonique, et comme $\mathrm{div}\,(\sum w(P)P)$ est linéairement équivalent à un multiple du diviseur canonique, nous avons une première relation entre les points de Weierstrass, à savoir $\sum w(P)j(P) = 0$. Et donc, lorsqu'il existe un point d'hyper-inflexion, on a $\mathrm{rang}_{\mathbb{Z}}\mathrm{W} \leq 21$. Lorsqu'il en existe $s < 12$, on a $\mathrm{rang}_{\mathbb{Z}}\mathrm{W} \leq 24 - 2\mathrm{s} - 1$. Lorsqu'il y a douze points d'hyper-inflexion, le rang est nul.

Lemme 1.4.1. *Si une quartique lisse $\mathcal{C}$ possède 2 (resp. 3) points d'hyper-inflexion, ceux-ci engendrent un groupe isomorphe à $\mathbb{Z}/4\mathbb{Z}$ (resp. $(\mathbb{Z}/4\mathbb{Z})^2$).*

DÉMONSTRATION : On prend un de ces points (que l'on note ∞) comme base du plongement jacobien. Soit P un autre point d'hyper-inflexion. Si L_P (resp. L_∞) est la forme linéaire définissant la tangente à la courbe en P (resp. ∞), on a alors $\mathrm{div}\,(L_P/L_\infty) = 4(P) - 4(\infty)$, ce qui traduit le fait que l'ordre de $j(P)$ divise 4. Il est exactement 4 ; en effet, s'il était égal à 2, il existerait une fonction rationnelle de diviseur $2P - 2\infty$ et donc une application de degré 2 de $\mathcal{C}$ dans $\mathbb{P}^1$, ce qui entraînerait que $\mathcal{C}$ est hyperelliptique.
Soit Q un troisième point d'hyper-inflexion. Il n'existe pas de relation de la forme $mP + nQ - (m+n)\infty = \mathrm{div}\,(f)$ avec $0 \leq m,n \leq 3$, non tous les deux nuls. En effet,

– si $m = 0$ ou $n = 0$, on est ramené au cas précédent, et on voit que

l'autre coefficient doit être nul.

- si $m = 2$ ou $n = 2$, comme $j(P)$ et $j(Q)$ sont d'ordre 4, on a (par exemple) $2j(P) = -nj(Q)$ et donc n ne peut être impair,*i.e.* $m = n = 2$. Nous avons donc $2P + 2Q - 4\infty = \mathrm{div}\,(f)$, ce qui se traduit géométriquement par l'existence d'une bitangente passant par P et Q, ce qui est impossible.
- si $m = n = 1$ (ou $m = n = 3$), on a $P + Q - 2\infty = \mathrm{div}\,(f)$ et donc il existe une application de degré 2, $\bar{f} : \mathcal{C} \to \mathbb{P}^1$, ce qui contredit le fait que $\mathcal{C}$ n'est pas hyperelliptique. On obtient la même contradiction avec $-P$ et $-Q$.
- si $m = 1$ et $n = 3$, on a alors $j(P) + 3j(Q) = j(P) - j(Q) = 0$, ce qui veut dire que $P - Q$ est le diviseur d'une fonction rationnelle, *i.e.* $\mathcal{C}$ est rationnelle, ce qui est exclu.

∎

Lemme 1.4.2. *Soit une quartique lisse $\mathcal{C}$ possédant exactement 4 points d'hyper-inflexion. Si 3 de ces points sont alignés, le groupe engendré par ces 4 points est $(\mathbb{Z}/4\mathbb{Z})^2$. S'il n'existe pas de droite passant par 3 de ces points, le groupe engendré par ces 4 points est $(\mathbb{Z}/4\mathbb{Z})^3$ ou $(\mathbb{Z}/4\mathbb{Z})^2 \times (\mathbb{Z}/2\mathbb{Z})$. Plus précisément, ce groupe est $(\mathbb{Z}/4\mathbb{Z})^2 \times (\mathbb{Z}/2\mathbb{Z})$ si et seulement s'il existe une conique tangente à la courbe en ces 4 points.*

DÉMONSTRATION : Si 3 points d'hyper-inflexion P, Q et R sont alignés, le quatrième point d'intersection S de la droite qu'ils définissent avec $\mathcal{C}$ est encore un point d'hyper-inflexion. En effet, en prenant comme base du plongement un des 3 points alignés, disons R, on a une relation de la forme $j(P) + j(Q) + j(S) = 0$ avec $j(P)$ et $j(Q)$ d'ordre 4. Cela implique que $j(S)$ est aussi d'ordre 4 et donc, le quatrième point d'intersection de la courbe avec la droite est donc un point d'hyper-inflexion. On en déduit que le groupe qu'ils engendrent est $(\mathbb{Z}/4\mathbb{Z})^2$, d'après le lemme précédent.
Soient P, Q, R et ∞ les 4 points d'hyper-inflexion. Supposons qu'il n'existe pas de droite passant par 3 de ces points. On prend ∞ comme base du plongement. Choisissons des coordonnées de sorte que ∞ égale $(1 : 0 : 0)$ et que la tangente en ∞ ait pour équation $Z = 0$. Ainsi, $L(3\infty)$ est de dimension 2 et une base en est donnée par 1 et Y/Z.
Supposons que l'on ait une relation $mj(P) + nj(Q) + lj(R) = 0$, avec $1 \leq m,n,l \leq 3$.

- Si $m = 2$, alors $nj(Q) + lj(R)$ est un point de torsion d'ordre 2, or $(j(Q),j(R))$ engendrent $(\mathbb{Z}/4\mathbb{Z})^2$, donc $n = l = 2$. On a donc $2(j(P) +$

$j(Q)+j(R))=0$. Et on ne peut avoir $j(P)+j(Q)+j(R)=0$ car les points d'hyper-inflexion ne sont pas alignés. En effet, cela se traduit par l'existence d'une fonction rationnelle dans $L(3\infty)$ dont le diviseur des zéros serait $P+Q+R$, c'est-à-dire, d'après l'expression d'une base de $L(3\infty)$, par l'existence d'une droite passant par P, Q et R.

- si $m=n=l=1$ (ou $m=n=l=3$), on a $j(P)+j(Q)+j(R)=0$, ce qui n'est pas possible car les points ne sont pas alignés.
- si $m=n=1$ et $l=-1$, on a $P+Q-R-\infty=0$, ce qui se traduit par l'existence d'une application de degré 2 de $\mathcal{C}$ dans $\mathbb{P}^1$, et donc, la courbe serait hyperelliptique.

La seule relation possible entre les images de ces points est donc $2(j(P)+j(Q)+j(R))=0$, auquel cas, le groupe engendré par ces 4 points est $(\mathbb{Z}/4\mathbb{Z})^2\times\mathbb{Z}/2\mathbb{Z}$.
Cette relation $2(j(P)+j(Q)+j(R))=0$ se traduit par $2P+2Q+2R-6\infty=0$, c'est-à-dire qu'il existe un diviseur effectif dans le système linéaire associé à 6∞ dont les zéros sont P, Q et R , avec multiplicité 2. Cela revient à l'existence d'une conique tangente aux 4 points P, Q, R et ∞. En effet, $L(6\infty)$ est de dimension 4, et une base de $L(6\infty)$ est donnée par 1, X/Z, Y/Z et Y^2/Z^2 et donc $L(6\infty)=\{\frac{aXZ+bYZ+cZ^2+dY^2}{Z^2}|(a,b,c,d)\in K^4\}$. ∎

Proposition 1.4.3. *Soit $\mathcal{C}_{c,d,t}$ la courbe lisse projective d'équation affine*

$$y^4+cxy+dyx^2+by^2x=x(x-1)(x-t)$$

avec $b=\frac{(c+d)(dt+c)}{(t-1)^2}$, alors $\mathcal{C}_{c,d,t}$ possède 4 points d'hyper-inflexion alignés $P_0=(0:0:1)$, $P_1=(1:0:1)$, $P_t=(t:0:1)$ et $P_\infty=(1:0:0)$. De plus, toute quartique possédant 4 points d'hyper-inflexion alignés, après changement de coordonnées, est de la forme $\mathcal{C}_{c,d,t}$.

DÉMONSTRATION : La première partie de la proposition se vérifiant aisément, nous nous bornerons à démontrer la seconde partie. Sans perte de généralité, on peut choisir des coordonnées telles que les 4 points d'hyper-inflexion soient $P_0=(0:0:1)$, $P_1=(1:0:1)$, $P_t=(t:0:1)$ et $P_\infty=(1:0:0)$ et que la droite d'alignement soit la droite $(Y=0)$, que la tangente en P_∞ soit $(Z=0)$, et la tangente en P_0 soit $(X=0)$. On peut alors encore appliquer la dilatation $(X,Y,Z)\to(\alpha X,\beta Y,\alpha Z)$.

Une quartique lisse a pour équation $a_{0,0}Y^4+Y^3Q_1(X,Y)+Y^2Q_2(X,Z)+YQ_3(X,Z)+Q_4(X,Z)$ où les Q_i sont des polynômes homogènes de degré i. Posons $Q_1(X,Y)=(a_{1,0}X+a_{0,1}Z)$, $Q_2(X,Z)=(a_{2,0}X^2+a_{1,1}XZ+a_{0,2}Z^2)$, $Q_3(X,Z)=(a_{3,0}X^3+a_{2,1}X^2Z+a_{1,2}XZ^2+a_{0,3}Z^3)$.

Comme les 4 points doivent appartenir à la quartique, on a $Q_4(X,Z) = \lambda X(X-Z)(X-tZ)Z$. Quitte à multiplier par un scalaire l'équation, on peut supposer $\lambda = -1$. Le point P_∞ est un point d'hyper-inflexion et la tangente en ce point a pour équation $Z = 0$, ce qui entraîne que $a_{1,0} = a_{2,0} = a_{3,0} = 0$. Le point P_0 est un point d'hyper-inflexion et la tangente en ce point a pour équation $X = 0$, ce qui entraîne que $a_{0,1} = a_{0,2} = a_{0,3} = 0$.

La courbe admet donc pour équation $aY^4+bY^2XZ+cYXZ^2+dYX^2Z = X(X-Z)(X-tZ)Z$. Quitte à dilater, on peut supposer $a = 1$.

Le point P_1 est un point d'hyper-inflexion et la tangente en ce point a pour équation $X = (c+d)/(t-1)Y + Z$, ce qui entraîne que $b = \frac{(c+d)(dt+c)}{(t-1)^2}$. ∎

Le théorème 3.1.1 entraîne l'existence d'une sous-famille avec $W \cong \mathbb{Z}^9 \times (\mathbb{Z}/4\mathbb{Z})^2$, le lemme 1.4.2 entraîne que pour toute courbe de la famille, W contient $(\mathbb{Z}/4\mathbb{Z})^2$. Les arguments de spécialisation entraînent le théorème suivant

Théorème 1.4.4. *Le groupe W_η engendré par les points de Weierstrass d'une quartique lisse générique possédant 4 points d'hyper-inflexion alignés est $\mathbb{Z}^r \times (\mathbb{Z}/4\mathbb{Z})^2$ avec $9 \leq r \leq 15$.*

Les deux lemmes 1.4.1 et 1.4.2, joints aux arguments de spécialisation (avec, pour le premier alinea, le théorème 3.1.1) nous permettent d'améliorer l'encadrement de W_η en fonction du nombre s de points d'hyper-inflexion. En effet, si $\mathcal{M}_3^\circ$ est l'espace de modules de courbes de genre 3 non-hyperelliptiques, notons $Z_s = \{[C] \in \mathcal{M}_3^\circ,\ C$ possède au moins s points d'hyper-inflexion $\}$ et $Z_s^\circ = \{[C] \in \mathcal{M}_3^\circ,\ C$ possède exactement s points d'hyper-inflexion $\}$. Vermeulen ([Ver]) donne une description explicite des composantes irréductibles de chacun des Z_s. En particulier, Z_1 et Z_2 sont irréductibles, Z_3° possède deux composantes irréductibles et Z_4 en possède cinq.

Théorème 1.4.5. *Soit W_η le groupe engendré par les points de Weierstrass d'une quartique lisse générique possédant s points d'hyper-inflexion.*

- *Pour une quartique lisse générique (sans point d'hyper-inflexion), $W_\eta = \mathbb{Z}^r$ avec $11 \leq r \leq 23$.*
- *Pour une quartique lisse générique avec un point d'hyper-inflexion (i.e. un point générique de Z_1), $W_\eta = \mathbb{Z}^r$ avec $11 \leq r \leq 21$.*
- *Pour une quartique lisse générique avec 2 points d'hyper-inflexion (i.e. un point générique de Z_2), W_η est un quotient de $\mathbb{Z}^{19} \times (\mathbb{Z}/4\mathbb{Z})$ qui contient $(\mathbb{Z}/4\mathbb{Z})$.*
- *Pour chaque composante irréductible de Z_3°, le groupe W_η engendré par*

les points de Weierstrass d'une quartique lisse générique est un quotient de $\mathbb{Z}^{17} \times (\mathbb{Z}/4\mathbb{Z})^2$ *qui contient* $(\mathbb{Z}/4\mathbb{Z})^2$.

- *Pour une quartique lisse générique avec 4 points d'hyper-inflexion tels qu'il y ait une conique tangente à la courbe en ces 4 points,* W_η *est un quotient de* $\mathbb{Z}^{15} \times (\mathbb{Z}/4\mathbb{Z})^3$ *qui contient* $(\mathbb{Z}/4\mathbb{Z})^2 \times (\mathbb{Z}/2\mathbb{Z})$.
- *Pour une quartique lisse générique de l'une des trois autres composantes de* $\mathbb{Z}_4^\circ$ *telles que aucun triplet de points d'hyper-inflexion n'est aligné,* W_η *est un quotient de* $\mathbb{Z}^{15} \times (\mathbb{Z}/4\mathbb{Z})^3$ *qui contient* $(\mathbb{Z}/4\mathbb{Z})^3$.

Nous pouvons donc nous demander ce qu'il en est du rang du groupe engendré par les points de Weierstrass d'une quartique lisse générique. Plus précisément, nous pouvons nous poser la question suivante :

Question :

Pour une quartique lisse générique (donc sans point d'hyper-inflexion), a-t'on $\mathrm{rang}_{\mathbb{Z}} \mathrm{W}_\eta = 23$ *?*

Pour une quartique lisse générique possédant un point d'hyper-inflexion, a-t'on $\mathrm{rang}_{\mathbb{Z}} \mathrm{W}_\eta = 21$ *?*

Une étude d'autres familles de courbes de genre 3 permettra peut-être d'apporter une réponse à cette question. On peut espérer qu'à terme, les informations recueillies sur les points de Weierstrass permettront de mieux appréhender l'espace des modules de courbes de genre 3. Rappelons que l'on ne sait même pas si $\mathcal{M}_3$ est une variété rationnelle (*i.e.*, birationnelle à $\mathbb{P}^6$).

Nous pouvons aussi nous demander ce qui se passe en genre supérieur, à savoir si l'on peut obtenir des minorations du même type pour le rang du groupe engendré par les points de Weierstrass dans la jacobienne d'une courbe de genre g générique (nous savons juste que le rang est majoré par g^3-g-1).

On peut formuler des questions similaires pour les points de Weierstrass d'ordre supérieur.

1.5 Cas des courbes hyperelliptiques

Le groupe W engendré par les points de Weierstrass dans la jacobienne d'une courbe hyperelliptique se calcule immédiatement. Plus précisément, nous avons le résultat classique :

Proposition 1.5.1. *Pour une courbe hyperelliptique de genre* g*, le groupe engendré par les points de Weierstrass dans la jacobienne est* $J[2] = (\mathbb{Z}/2\mathbb{Z})^{2g}$.

Une courbe hyperelliptique de genre g est birationnelle à la courbe affine

$$y^2 = (x - e_1) \dots (x - e_{2g+1})$$

et les points de Weierstrass sont les points $P_i = (e_i,0)$ et le point à l'infini noté ∞.

Remarque : Dans ce cas, la suite de lacunes d'un point de Weierstrass est $G(P_i) = \{1,3,\dots,2g-1\}$ et le poids d'un point de Weierstrass est $w(P_i) = \dfrac{g(g-1)}{2}$. ∎

On a déjà $\operatorname{div}(x - e_i) = 2[P_i - \infty]$ et $\operatorname{div}(y) = P_1 + \dots P_{2g+1} - (2g+1)\infty$.
Si l'on note x_i l'élément $P_i - \infty$ de la jacobienne, on obtient les relations suivantes

- $2x_i = 0 \quad$ pour $1 \leq i \leq 2g+1$
- $x_1 + \dots + x_{2g+1} = 0$.

Cela nous permet déjà de dire que W est l'ensemble $\{\sum_{i \in I} x_i \ , \ I \subset \{1,\dots,2g\}\}$ et est un sous-groupe de $J[2] = (\mathbb{Z}/2\mathbb{Z})^{2g}$.
Nous allons montrer que W est égal à $J[2]$. Pour cela, il suffit de voir que $\sum_{i \in I} x_i = 0$ entraîne $I = \emptyset$ ou $I = \{1,\dots,2g+1\}$.
Supposons que l'on ait une relation entre ces points de la jacobienne du type $\sum_{i \in I} x_i = 0$, avec I de cardinal m. Cela revient à l'existence d'une fonction f rationnelle sur $\mathcal{C}$ dont le diviseur satisfait $\operatorname{div}(f) = \sum_{i \in I} P_i - m\,\infty$. On a $f \in k(x) + y\,k(x)$, et comme f n'a de pôle qu'en ∞, cela entraîne que f est de la forme $P(x) + y\,Q(x)$, avec P et Q des polynômes.
De plus, $\operatorname{ord}_\infty P(x) = -2 \deg P$ et $\operatorname{ord}_\infty(y\,Q(x)) = -2 \deg Q - 2g - 1$.

si $Q = 0$ on a $f = P(x)$ et donc $P = \prod(x - e_i)$. Chaque point qui intervient dans le diviseur intervient donc avec une multiplicité paire, ce qui est exclu.

si $Q \neq 0$ comme $m \leq 2g+1$, Q est nécessairement constant. La fonction rationnelle f est alors de la forme $P(x) + y$ avec $\deg P \leq g$, donc $m = 2g+1$ et donc $I = \{1,\dots,2g+1\}$. Mais alors, pour $i \in I$, on a $f(P_i) = P(e_i) = 0$, ce qui entraîne que $\prod_{1 \leq i \leq 2g+1}(x - e_i)$ divise P. Le polynôme P est nécessairement nul, et donc $f = y$; comme $I = \{1,\dots,2g+1\}$), cela nous donne une relation que nous avions déjà.

Remarque : Le cas des points Weierstrass d'ordre supérieur des courbes hyperelliptiques est étudié par Silverman ([Sil3]). En particulier, les points de Weierstrass sont des points de Weierstrass d'ordre n. Et lorsque $g \neq 2$ et $n \neq 2$, il y a des points de Weierstrass d'ordre n qui ne sont pas des points de Weierstrass. ∎

Deuxième partie

Etude de la famille de courbes lisses d'équation affine $y^3 = x(x-1)(x^2 - 2\beta\, x + \beta)$

Résumé

Nous déterminons, pour une famille de courbes lisses de genre 3, la structure du groupe engendré par les points de Weierstrass dans la jacobienne. Cela fournit un exemple, où ce groupe est infini. Plus précisément, nous exhibons une famille où ce groupe est isomorphe à $\mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5$ et en déduisons l'existence d'une famille où ce groupe est $\mathbb{Z}^r$ avec $9 \leq r \leq 23$.

Abstract

We describe the group generated by the Weierstrass points in the Jacobian, for a family of smooth curves of genus 3. This gives an example where this group is not finite. More precisely, we construct a family with a group isomorphic to $\mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5$. Thus we can conclude that there exists a family whose group is $\mathbb{Z}^r$ with $9 \leq r \leq 23$.

2.1 Introduction

Soit $\mathcal{C}$ une courbe lisse projective de genre $g \geq 2$. Une telle courbe possède un ensemble de points canoniques : ses points de Weierstrass. D'autre part, après avoir choisi un de ces points, on dispose d'un plongement de $\mathcal{C}$ dans sa jacobienne J, et la structure du groupe $W = W_{\mathcal{C}}$ engendré par les points de Weierstrass dans la jacobienne ne dépend pas du point de Weierstrass choisi ; ce groupe est donc un invariant géométrique de la courbe digne d'intérêt. Le cas le plus simple est celui d'une courbe hyperelliptique où l'on voit assez facilement que $W = (\mathbb{Z}/2\mathbb{Z})^{2g} = J[2]$ (voir le paragraphe 1.5).

Pour les courbes de genre 3 non hyperelliptiques, c'est-à-dire les quartiques planes, quelques cas particuliers ont été traités dans la littérature. Il s'agit de courbes possédant de nombreux automorphismes. En effet, pour la quartique de Klein (d'équation $X^3Y + Y^3Z + Z^3X = 0$), qui possède 168 automorphismes, $W = (\mathbb{Z}/2\,\mathbb{Z}) \times (\mathbb{Z}/7\,\mathbb{Z})^3$ ([Pra]). Pour la courbe de Fermat (d'équation $X^4 + Y^4 = Z^4$), qui possède 96 automorphismes, $W = (\mathbb{Z}/4\,\mathbb{Z})^5 \times (\mathbb{Z}/2\,\mathbb{Z})$ ([Roh]). Pour la courbe d'équation $Y^3Z + Z^4 = X^4$, qui en possède 48, $W = (\mathbb{Z}/4\,\mathbb{Z})^2 \times (\mathbb{Z}/3\,\mathbb{Z})^5$ ([KS]). Nous nous proposons d'analyser le groupe W pour des familles et en particulier de montrer :

Théorème 2.1.1. *Soit $\mathcal{C}_\beta$ la courbe projective lisse birationnelle à la courbe affine $y^3 = x(x-1)(x^2 - 2\beta x + \beta)$ où $\beta \notin \{0,1,1/2\}$. Pour tout corps de nombres K, il existe un ensemble fini S_K tel que si $\beta \in K \setminus S_K$ alors $W_{\mathcal{C}_\beta} \cong \mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5$. Par exemple, $\beta = 784/6859$ n'appartient jamais à S_K.*

Remarquons que le groupe d'automorphismes de cette famille est $\mathbb{Z}/3\mathbb{Z}$ et que le théorème fournit, à notre connaissance, le premier exemple de calcul

explicite avec W infini. En utilisant des arguments de spécialisation nous en tirerons :

Corollaire 2.1.2. *Soit une famille de courbes lisses joignant une courbe hyperelliptique à une courbe $\mathcal{C}_\beta$ pour laquelle $W_{\mathcal{C}_\beta} = \mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5$. Soit $W_{\mathcal{C}_\eta}$ le groupe engendré par les points de Weierstrass de la fibre générique, on a alors $W_{\mathcal{C}_\eta} \cong \mathbb{Z}^r$ avec $9 \leq r \leq 23$.*

Afin de démontrer le théorème 2.1.1, nous allons exhiber 9 points de Weierstrass $P_1, \ldots, P_9$ avec $P_5, \ldots, P_9$ d'ordre 3 tel que si l'on note $\psi(m_1, \ldots, m_9) = m_1P_1 + \ldots + m_9P_9$, on obtient, en notant W_η le groupe engendré par les points de Weierstrass de la courbe générique, et W_s celui engendré par ceux de la courbe spéciale, des applications ψ_η, ψ_s telles que, si l'on note μ la spécialisation, le diagramme suivant soit commutatif :

$$\begin{array}{ccc} \mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5 & \xrightarrow{\psi_\eta} & W_\eta \\ & \searrow^{\psi_s} & \downarrow \mu \\ & & W_s \end{array}$$

Puis, nous allons montrer que :

(i) μ est surjective (argument de spécialisation (proposition 1.3.3)).

(ii) ψ_s et ψ_η sont surjectives (proposition 2.3.1).

(iii) ψ_s est un isomorphisme pour un s particulier (proposition 2.5.1).

Cela nous permettra de conclure que ψ_η est un isomorphisme, qui ne dépend pas de la spécialisation. Puis, comme μ est un isomorphisme pour presque toute spécialisation en s (cela découle du théorème 1.3.5), cela nous permettra de conclure.

2.2 Calcul des points de Weierstrass

Considérons, pour $\beta \notin \{0,1\}$, la courbe lisse $\mathcal{C}_\beta$ d'équation affine

$$y^3 = x(x-1)(x^2 - 2\beta x + \beta).$$

Notons $f(x)$ le terme de droite. La courbe projective $ZY^3 = Z^4 f(\frac{Y}{Z})$ admet un unique point à l'infini, noté P_∞ de coordonnées $(0:1:0)$, qui est lisse, et que l'on prend comme base du plongement dans la jacobienne.

Les points d'inflexion de cette courbe sont définis par l'annulation du hessien H, que nous allons calculer. L'équation de la courbe en coordonnées homogènes étant $Y^3Z = X(X-Z)(X^2-2\beta XZ+\beta Z^2)$, il vient:

$$H(X,Y,Z) \;=\; 54\,Y\,G(X,Y,Z)$$

où $G(X,Y,Z) = (2\,X^2+(-2\,\beta-1)\,ZX+\beta\,Z^2)\,Y^3+(4\,\beta-1-4\,\beta^2)\,ZX^4+(-4\,\beta+8\,\beta^2)\,Z^2X^3+(-8\,\beta^2+2\,\beta)\,Z^3X^2+4\,\beta^2Z^4X-Z^5\beta^2$.

En repassant en coordonnées affines, et en remplaçant y^3 par sa valeur en fonction de x, on obtient
$G_0(x) = 2\,x^6+(-6\,\beta-3)\,x^5+15\,\beta\,x^4-10\,\beta\,x^3-3\,\beta\;(\beta-1)\,x^2+3\,\beta^2x-\beta^2$
$= (2\,x^3-3\,x^2+\beta)\,(x^3-3\,\beta\,x^2+3\,\beta\,x-\beta)$.

On dispose donc de la description suivante des points d'inflexion : ce sont d'une part, les zéros de f que l'on note P_0, P_1, P_{t_1}, P_{t_2}, le point à l'infini P_∞ et d'autre part, les points ayant pour abscisse les zéros du polynôme $G_0(x) = (2\,x^3-3\,x^2+\beta)(x^3-3\,\beta\,x^2+3\,\beta\,x-\beta)$.
Notons x_1,x_2,x_3 les racines du premier facteur et x_4,x_5,x_6 celles du second facteur.

Il y a de manière générale, 23 points de Weierstrass ; seul le point à l'infini a poids 2. Un calcul direct montre qu'il ne peut y avoir égalité entre certains de ces points que pour $\beta = 1/2$.

On va montrer que les points de Weierstrass sont dans une configuration particulière, plus précisément, on montre que si une droite passe par trois de ces points, son quatrième point d'intersection avec la quartique est encore un point de Weierstrass et que de telles droites existent. Cela nous donnera un certain nombre de relations entre ces points ; on montrera ensuite, par un procédé de descente, que ce sont, en général, les seules.

2.2.1 Premier facteur du hessien

Nous avons noté x_1, x_2 et x_3 les racines de $(2\,x^3-3\,x^2+\beta)$; on a donc

$$\left\{\begin{array}{rcl} x_1+x_2+x_3 & = & 3/2 \\ x_1x_2+x_1x_3+x_2x_3 & = & 0 \\ 2x_1x_2x_3 & = & -\beta. \end{array}\right.$$

D'où, en remplaçant x_3 par $3/2-x_1-x_2$ dans la deuxième équation, il vient
$2\,x_1x_2+2\,x_1^2-3\,x_1+2\,x_2^2-3\,x_2=0$.
C'est l'équation d'une conique passant par (0,0), que l'on paramètre par

$x_2 = t x_1$. L'abscisse x_1 est donc solution de $2\,(t^2+t+1\,)\,x_1^2 - 3\,(t+1)\,x_1 = 0$ et il vient alors

$$\left\{\begin{array}{rcl} x_1 & = & 3/2\,\dfrac{t+1}{t^2+t+1} \\ x_2 & = & 3/2\,\dfrac{t\,(t+1)}{t^2+t+1} \\ x_3 & = & -3/2\,\dfrac{t}{t^2+t+1}. \end{array}\right.$$

et donc $\beta = \dfrac{27}{4}\,\dfrac{(t+1)^2\,t^2}{(t^2+t+1)^3}$.
L'équation de $\mathcal{C}$ devient alors

$$y^3 = x^4 - \left(\frac{27}{2}\,\frac{(t+1)^2\,t^2}{(t^2+t+1)^3} + 1\right) x^3 + \frac{81}{4}\,\frac{(t+1)^2\,t^2}{(t^2+t+1)^3} x^2 - \frac{27}{4}\,\frac{(t+1)^2\,t^2}{(t^2+t+1)^3} x$$

et on obtient ainsi

$$\left\{\begin{array}{rcl} y_1^3 & = & -\dfrac{27}{16}\,\dfrac{(t+1)^3\,(2\,t+1)^3\,(t-1)^3}{(t^2+t+1)^6} \\ y_2^3 & = & \dfrac{27}{16}\,\dfrac{(t+1)^3\,t^3\,(t+2)^3\,(t-1)^3}{(t^2+t+1)^6} \\ y_3^3 & = & \dfrac{27}{16}\,\dfrac{t^3\,(t+2)^3\,(2\,t+1)^3}{(t^2+t+1)^6}. \end{array}\right.$$

Notons alors

$$\left\{\begin{array}{rcl} y_{1,1} & = & -\dfrac{3}{4}\,2^{2/3}\,\dfrac{(t+1)\,(2\,t+1)\,(t-1)}{(t^2+t+1)^2} \\ y_{2,1} & = & \dfrac{3}{4}\,2^{2/3}\,\dfrac{(t+1)\,t\,(t+2)\,(t-1)}{(t^2+t+1)^2} \\ y_{3,1} & = & \dfrac{3}{4}\,2^{2/3}\,\dfrac{t\,(t+2)\,(2\,t+1)}{(t^2+t+1)^2}. \end{array}\right.$$

Soit ζ_3 une racine cubique de l'unité, on note alors $P_{i,j}$ le point $(x_i, y_{i,1}{\zeta_3}^{j-1})$ où $j \in \{1,2,3\}$.

Proposition 2.2.1. *Pour tout triplet de points $\{P_{1,\alpha_1}, P_{2,\alpha_2}, P_{3,\alpha_3}\}$, où les α_i sont deux-à-deux distincts, il existe une droite $\mathcal{D}$ qui passe par ces trois points et le quatrième point d'intersection de $\mathcal{D}$ avec $\mathcal{C}$ est P_{t_1} ou P_{t_2}.*

La preuve découle immédiatement des deux lemmes suivants :

Lemme 2.2.2. *Pour* $(\alpha_i) \in \{1,2,3\}$ *deux-à-deux distincts, les points* P_{1,α_1}, P_{2,α_2}, *et* P_{3,α_3} *sont alignés.*

DÉMONSTRATION : Notons (x_i,y_i) un point de Weierstrass d'abscisse x_i. Soit la droite $\mathcal{D}$ passant par (x_1,y_1) et (x_2,y_2). Elle admet pour équation

$$y = \frac{(x-x_1)\,y_2}{x_2-x_1} + \frac{(x-x_2)\,y_1}{x_1-x_2}.$$

Cherchons l'ordonnée du point d'abscisse x_3. Notons la provisoirement y_0, et montrons qu'elle est égale à y_3.
En remplaçant x_1, x_2 et x_3 par leur valeur

$$y_0 = \frac{(t^2+2\,t)\,y_1 - (2t+1)\,y_2}{(t-1)\,(t+1)}.$$

Pour

$$\begin{cases} y_1 &= -\dfrac{3}{4}\,2^{2/3}\,\dfrac{(t+1)\,(2\,t+1)\,(t-1)\,\zeta_3^{\alpha_1}}{(t^2+t+1)^2} \\ y_2 &= \dfrac{3}{4}\,2^{2/3}\,\dfrac{(t+1)\,t\,(t+2)\,(t-1)\,\zeta_3^{\alpha_2}}{(t^2+t+1)^2} \end{cases}$$

il vient:

$$\begin{aligned} y_0 &= \frac{-3}{4}\,2^{2/3}\,\frac{1}{(t^2+t+1)^2}\,\left[(t^2+2t)\,(2t+1)\,\zeta_3^{\alpha_1} + t(t+2)(2t+1)\,\zeta_3^{\alpha_2}\right] \\ &= \frac{-3}{4}\,2^{2/3}\,\frac{(2t+1)t(t+2)}{(t^2+t+1)^2}\,(\zeta_3^{\alpha_1}+\zeta_3^{\alpha_2}) \end{aligned}$$

or $\alpha_1 \neq \alpha_2$, $\alpha_1 \neq \alpha_3$ et $\alpha_2 \neq \alpha_3$, donc on a $-(\zeta_3^{\alpha_1}+\zeta_3^{\alpha_2}) = \zeta_3^{\alpha_3}$ et donc $y_0 = y_3$. ∎

Lemme 2.2.3. *L'abscisse du quatrième point d'intersection de* $\mathcal{D}$ *(où* $\mathcal{D}$ *est la droite passant par* P_{1,α_1}, P_{2,α_2}, *et* P_{3,α_3} *) avec* $\mathcal{C}$ *est un zéro du polynôme* $x^2 - 2\beta x + \beta$.

DÉMONSTRATION : Montrons maintenant que le point d'ordonnée zéro de $\mathcal{D}$ est un point de Weierstrass. Ce sera donc le quatrième point d'intersection de $\mathcal{C}$ et $\mathcal{D}$. Soit x_0 l'abscisse de ce point:

On a alors $(x_0 - x_1)y_2 - (x_0 - x_2)y_1 = 0$ *i.e.* $x_0 = \dfrac{x_1y_2 - x_2y_1}{y_2 - y_1}$

comme $x_2 = tx_1$, on a $x_0 = \dfrac{3}{2}\,\dfrac{t+1}{t^2+t+1}\dfrac{y_2 - ty_1}{y_2 - y_1}$.

Calculons $x_0^2 - 2\beta x_0 + \beta$ on a

$x_0^2 - 2\beta x_0 + \beta = \dfrac{9}{4}\,\dfrac{(y_2 - ty_1)^2(t+1)^2}{(t^2+t+1)^2(y_2 - y_1)^2} - \dfrac{81}{4}\,\dfrac{(t+1)^3t^2(y_2 - ty_1)}{(t^2+t+1)^4(y_2 - y_1)} +$

$\dfrac{27}{4}\,\dfrac{(t+1)^2t^2}{(t^2+t+1)^3}$

$= \dfrac{9}{4}\,\dfrac{(t+1)^2(t-1)^2}{(t^2+t+1)^4(y_2 - y_1)^2}\left\{(4\,t^2 + 4\,t + 1)y_2^2 + (t^4 + 4\,t^3 + 4\,t^2){y_1}^2 - \right.$

$\left.(2\,t^3 + 5\,t^2 + 2\,t)y_1y_2\right\}$

$= \dfrac{9}{4}\dfrac{(t+1)^2(t-1)^2}{(t^2+t+1)^4(y_2 - y_1)^2}\left\{(2t+1)^2y_2^2 + (t+2)^2t^2{y_1}^2 - (2t+1)(t+2)ty_1y_2\right\}$.

Substituons $y_1 = -(2t+1)\,\zeta_3^{\alpha_1}\,C$,$y_2 = t(t+2)\,\zeta_3^{\alpha_2}\,C$ dans l'accolade, il vient que $x_0^2 - 2\beta x_0 + \beta$ est proportionnel à $(2t+1)^2\,t^2\,(t+2)^2\,(\zeta_3^{2\alpha_2} + \zeta_3^{2\alpha_1} + \zeta_3^{\alpha_1+\alpha_2})$ qui est nul. ∎

Il est naturel de s'intéresser au quatrième point d'intersection de la tangente en un de ces points de Weierstrass avec $\mathcal{C}$. On va voir que les tangentes à $\mathcal{C}$ en $P_{1,j}$, $P_{2,j}$ et $P_{3,j}$ se coupent en un point ayant pour abscisse $1/2$.

Lemme 2.2.4. *Le quatrième point d'intersection de la tangente à $\mathcal{C}$ en $P_{i,j}$ a pour abscisse 1/2.*

DÉMONSTRATION : Notons $T_{i,j}$ la tangente à $\mathcal{C}$ en $P_{i,j}$; elle ne coupe $\mathcal{C}$ que dans le plan affine, car le coefficient de y n'est nul que si l'ordonnée de $P_{i,j}$ est elle-même nulle, ce qui est exclu.

La tangente $T_{1,1}$ a pour équation affine :

$$\left((t^2 + t + 1)\,2\sqrt[3]{2}y + 2(t^2 - 2t - 2)x + 3(t+1)\right)(t-1)^2(2t+1)^2(t+1)^2 = 0.$$

La tangente $T_{2,1}$ a pour équation affine :

$$\left(2(t^2 + 2t - 1)x - 2\sqrt[3]{2}(t^2 + t + 1)y - 3t(t+1)\right)(t-1)^2(1+t)^2(t+2)^2t^2 = 0.$$

La tangente $T_{3,1}$ a pour équation affine :

$$\left(2\,\left(t^2 + 1 + 4\,t\right)x + (2\,\sqrt[3]{2}\,\left(t^2 + t + 1\right)\,y - 3\,t\right)\left(2\,t + 1\right)^2\,\left(t + 2\right)^2\,t^2 = 0.$$

On trouve que $T_{i,j}$ coupe $\mathcal{C}$ en $Q_{i,j}$ où $Q_{i,j} = (1/2, -\,2^{2/3}\,\zeta_3^{j-1}/4)$. ∎

2.2.2 Second facteur du hessien

Les points de Weierstrass restant sont dans une configuration similaire ; en effet, on va montrer que pour tout triplet de points $\{P_{4,\alpha_4},P_{5,\alpha_5},P_{6,\alpha_6}\}$ où les α_i sont deux-à-deux distincts, il existe une droite $\mathcal{D}$ qui passe par ces trois points et le quatrième point d'intersection de $\mathcal{D}$ avec $\mathcal{C}$ appartient à $\{P_0,P_1\}$.

Nous avons noté x_4,x_5 et x_6 les racines de $(x^3-3\,\beta\,x^2+3\,\beta\,x-\beta)$; on a donc

$$\left\{\begin{array}{lcl} x_4+x_5+x_6 & = & 3\beta \\ x_4x_5+x_5x_6+x_4x_6 & = & 3\beta \\ x_4x_5x_6 & = & \beta \end{array}\right.$$

d'où $\beta = 1/3\ (x_4+x_5+x_6)$ et $x_6 = -\dfrac{x_4x_5-x_4-x_5}{x_4+x_5-1}$. En remplaçant dans la dernière équation, il vient:

$$x_4^2+x_4x_5+x_5^2-3x_4x_5^2+3x_4^2x_5^2-3x_4^2x_5=0$$

i.e. $(3x_4^2-3x_4+1)x_5^2+(-3x_4^2+x_4)x_5+x_4^2=0$. C'est une équation du second degré en x_5. Le discriminant vaut $-3x_4^2(x_4-1)^2$ et donc

$$x_5=\frac{(3+i\,\sqrt{3})}{6x_4-3+i\,\sqrt{3}}\quad x_4=\frac{1}{12}\frac{(3+i\,\sqrt{3})(6x_4-3-i\,\sqrt{3})}{3x_4^2-3x_4+1}\quad x_4$$

et alors

$$x_6=\frac{(3-i\,\sqrt{3})}{6x_4-3-i\,\sqrt{3}}\quad x_4=\frac{1}{12}\frac{(3-i\,\sqrt{3})(6x_4-3+i\,\sqrt{3})}{3x_4^2-3x_4+1}\quad x_4=\bar{x_5}$$

et donc $\beta=\dfrac{x_4^3}{3x_4^2-3x_4+1}$. Si l'on pose $u=x_4$, on a donc

$$\left\{\begin{array}{lcl} x_4 & = & u \\ x_5 & = & \dfrac{(3+i\,\sqrt{3})\,u}{6u-3+i\,\sqrt{3}} \\ x_6 & = & \dfrac{(3-i\,\sqrt{3})\,u}{6u-3-i\,\sqrt{3}} \end{array}\right.$$

et alors $\beta=\dfrac{u^3}{3\,u^2-3\,u+1}$.

L'équation de $\mathcal{C}$ devient alors

$$y^3 = x^4 - 2\,\frac{u^3}{3\,u^2-3\,u+1}x^3 + 3\,\frac{u^3}{3\,u^2-3\,u+1}x^2 - \frac{u^3}{3\,u^2-3\,u+1}x$$

et on obtient ainsi

$$\begin{cases} y_4^3 &= \dfrac{u^3(u-1)^3}{3\,u^2-3\,u+1} \\ y_5^3 &= \dfrac{1}{72}\dfrac{i\,\sqrt{3}u^3(u-1)^3}{(3\,u^2-3\,u+1)^4}\ (6u-3-i\,\sqrt{3})^3 \\ y_6^3 &= -\dfrac{1}{72}\dfrac{i\,\sqrt{3}u^3(u-1)^3}{(3\,u^2-3\,u+1)^4}\ (6u-3+i\,\sqrt{3})^3. \end{cases}$$

Posons $y_{4,1} = \dfrac{u(u-1)}{(3\,u^2-3\,u+1)^{(1/3)}}$

comme $\left(\dfrac{i\,\sqrt{3}}{72}\right)^{(1/3)} = \zeta_3\ \left(-\dfrac{i\,\sqrt{3}}{6}\right)$, posons:

$$\begin{cases} y_{5,1} &= -\dfrac{i\,\sqrt{3}}{6}\dfrac{(6u-3-i\,\sqrt{3})}{(3\,u^2-3\,u+1)}\ y_{4,1} \\ y_{6,1} &= \dfrac{i\,\sqrt{3}}{6}\dfrac{(6u-3+i\,\sqrt{3})}{(3\,u^2-3\,u+1)}\ y_{4,1}. \end{cases}$$

On note alors $P_{i,j}$ le point $(x_i, y_{i,1}{\zeta_3}^{j-1})$ où $j \in \{1,2,3\}$.

Proposition 2.2.5. *Pour tout triplet de points $\{P_{4,\alpha_4}, P_{5,\alpha_5}, P_{6,\alpha_6}\}$ où les α_i sont deux-à-deux distincts, il existe une droite $\mathcal{D}$ qui passe par ces trois points et le quatrième point d'intersection de $\mathcal{D}$ avec $\mathcal{C}$ est P_0 ou P_1.*

La démonstration va se faire en deux étapes.

Lemme 2.2.6. *Pour $(\alpha_i) \in \{1,2,3\}$ deux-à-deux distincts, les points P_{4,α_4}, P_{5,α_5}, et P_{6,α_6} sont alignés.*

DÉMONSTRATION : Considérons la droite $\mathcal{D}$ passant par (x_4, y_4) et (x_5, y_5). Elle admet pour équation

$$y = \frac{(x-x_5)y_4}{x_4-x_5} + \frac{(x-x_4)y_5}{x_5-x_4}.$$

Cherchons l'ordonnée du point d'abscisse x_6. Notons la provisoirement y_0, et montrons qu'elle est égale à y_6.

On a, en remplaçant x_4, x_5 et x_6 par leur valeur:

$$\begin{aligned} y_0 &= \frac{(6u-3+i\sqrt{3})y_5 - 2i\sqrt{3}y_4}{6u-3-i\sqrt{3}} \\ &= \frac{(-2i\sqrt{3})y_{4,\alpha_5} - 2i\sqrt{3}y_{4,\alpha_4}}{6u-3-i\sqrt{3}} \\ &= \frac{(-2i\sqrt{3})}{6u-3-i\sqrt{3}}\,(\zeta_3^{\alpha_5}+\zeta_3^{\alpha_4})\,y_{4,1} \\ &= \frac{(i\sqrt{3})}{6}\frac{6u-3+i\sqrt{3}}{(3\,u^2-3\,u+1)}\,\zeta_3^{\alpha_6}\,y_{4,1} \end{aligned}$$

car $\alpha_4 \neq \alpha_5$, $\alpha_4 \neq \alpha_6$ et $\alpha_5 \neq \alpha_6$, donc on a $-(\zeta_3^{\alpha_4}+\zeta_3^{\alpha_5}) = \zeta_3^{\alpha_6}$ et donc $y_0 = y_6$. ∎

Lemme 2.2.7. *Le quatrième point d'intersection de $\mathcal{D}$ (où $\mathcal{D}$ est la droite passant par P_{4,α_4}, P_{5,α_5}) et P_{6,α_6}avec $\mathcal{C}$ est P_0 ou P_1.*

DÉMONSTRATION : Montrons maintenant que le quatrième point d'intersection de $\mathcal{C}$ avec $\mathcal{D}$ est un point de Weierstrass d'ordonnée zéro. Soit x_0 l'abscisse de ce point:
On a alors $(x_0-x_5)y_4-(x_0-x_4)y_5=0$
i.e. $x_0 = \dfrac{x_5y_4-x_4y_5}{y_4-y_5}$.
Donc si on remplace y_4 et y_5 par leur valeur,on a:

$$\begin{aligned} x_0 &= \frac{\frac{(3+i\sqrt{3})}{6u-3+i\sqrt{3}}\;u\;y_{4,1}\;\zeta_3^{\alpha_4} + u\frac{i\sqrt{3}}{6}\frac{12\,\zeta_3^{\alpha_5}}{(6u-3+i\sqrt{3})}\;y_{4,1}}{y_{4,1}\;\zeta_3^{\alpha_4} + \frac{i\sqrt{3}}{6}\frac{12\,\zeta_3^{\alpha_5}}{(6u-3+i\sqrt{3})}\;y_{4,1}} \\ &= \frac{((3+i\sqrt{3})\;+2i\sqrt{3}\,\zeta_3^{\alpha_5-\alpha_4})\;u}{(6u-3+i\sqrt{3})+2i\sqrt{3}\,\zeta_3^{\alpha_5-\alpha_4}}. \end{aligned}$$

Or $\alpha_4 \neq \alpha_5$ donc

- si $\alpha_5-\alpha_4 \equiv 1 \bmod 3$ alors comme $2\zeta_3 = -1+i\sqrt{3}$, $2i\sqrt{3}\;\zeta_3^{\alpha_5-\alpha_4} = -i\sqrt{3}-3$ et donc $x_0=0$.
- si $\alpha_5-\alpha_4 \equiv 2 \bmod 3$ alors comme $2\zeta_3^2 = -1-i\sqrt{3}$, $2i\sqrt{3}\;\zeta_3^{\alpha_5-\alpha_4} = -i\sqrt{3}+3$ et donc $x_0=1$. ∎

Il est naturel de s'intéresser au quatrième point d'intersection de la tangente en un de ces points de Weierstrass avec $\mathcal{C}$.

Lemme 2.2.8. *Le quatrième point d'intersection de la tangente à $\mathcal{C}$ en $P_{i,j}$ a pour abscisse β.*

DÉMONSTRATION : Notons $T_{i,j}$ la tangente à $\mathcal{C}$ en $P_{i,j}$; elle ne coupe $\mathcal{C}$ que dans le plan affine, car le coefficient de y n'est nul que si l'ordonnée de $P_{i,j}$ est elle-même nulle, ce qui est exclu.
La tangente $T_{4,1}$ a pour équation affine :

$$-3u^2(u-1)^2(-(3u^2-3u+1)^{(1/3)}y+(2u-1)x-u^2)(3u^2-3u+1)^{2/3}=0.$$

La tangente $T_{5,1}$ a pour équation affine :

$$(\tfrac{(1+i\sqrt{3})}{2}-u)(6u-3+i\sqrt{3})x-(3u^2-3u+1)^{(1/3)}(6u-3+i\sqrt{3})y-(i\sqrt{3}-3)u^2=0.$$

La tangente $T_{6,1}$ a pour équation affine :

$$(\tfrac{-1+i\sqrt{3}}{2}+u)(6u-3-i\sqrt{3})x+(6u-3-i\sqrt{3})(3u^2+1-3u)^{(1/3)}y-u^2(3+i\sqrt{3})=0.$$

On trouve que $T_{i,j}$ coupe $\mathcal{C}$ en $Q_{i,j}$ où $Q_{i,j}=\left(\beta,-\dfrac{u^2(u-1)^2}{(3\,u^2-3\,u+1)^{(4/3)}}\,\zeta_3^{j-1}\right)$. ∎

Remarque : Selon que l'on s'intéresse au premier ou au second terme du hessien, la paramétrisation choisie diffère. L'expression de β dans chaque cas nous permet de trouver une relation entre les deux paramètres, à savoir $u=\dfrac{3}{3+(\frac{(t-1)\,(t+2)\,(2t+1)}{t\,(t+1)})^{(2/3)}}$. ∎

Remarque : Soit K un corps de nombres. Les racines de $P=x^2-2\beta x+\beta$ sont de la forme $\beta\pm\sqrt{\beta^2-\beta}$. Elles sont rationnelles sur K si on a $\beta=\dfrac{r_0^2}{r_0^2-1}$, où $r_0\in K$ et alors les racines de P sont $\dfrac{r_0}{r_0+1}$ et $\dfrac{r_0}{r_0-1}$. On peut exprimer r_0 en fonction de t, $r_0=\dfrac{3\;i\;\sqrt{3}\;(t+1)\;t}{(2t+1)\;(t+2)\;(t-1)}$; ou encore, en fonction de u, $r_0=(\dfrac{u}{u-1})^{3/2}$. ∎

2.3 Etude géométrique des points de Weierstrass

Si L est une forme linéaire, notons $\mathrm{div}\,(L)$ le diviseur de L. On a donc, en considérant les droites projectives correspondant à une abscisse fixée:

- $\mathrm{div}\,(X) = 3P_0 + P_\infty$
- $\mathrm{div}\,(X - Z) = 3P_1 + P_\infty$
- $\mathrm{div}\,(X - t_1\ Z) = 3P_{t_1} + P_\infty$
- $\mathrm{div}\,(X - t_2\ Z) = 3P_{t_2} + P_\infty$
- $\mathrm{div}\,(Y) = P_0 + P_1 + P_{t_1} + P_{t_2}$
- $\mathrm{div}\,(X - x_i\ Z) = P_{i,1} + P_{i,2} + P_{i,3} + P_\infty \quad \text{pour} \quad 1 \leq i \leq 6$
- $\mathrm{div}\,(2X - Z) = Q_{1,1} + Q_{1,2} + Q_{1,3} + P_\infty$
- $\mathrm{div}\,(X - \beta Z) = Q_{4,1} + Q_{4,2} + Q_{4,3} + P_\infty$.

Notation: Par abus de notation, on confond P et $j(P)$, son image par le plongement jacobien de point base P_∞.
On en déduit donc que $3P_0 = 0$ *i.e.* que P_0 est d'ordre 3 ; de la même façon, on trouve que P_1, P_{t_1} et P_{t_2} sont d'ordre 3.
Si $T_{i,j}$ est l'équation homogène de la tangente en $P_{i,j}$, on a $\mathrm{div}\,(T_{i,j}) = 3P_{i,j} + Q_{i,j}$ et donc, comme $Q_{i,j} = Q_{i',j}$, on en tire $\mathrm{div}\,(T_{i,j}/T_{i',j}) = 3P_{i,j} - 3P_{i',j}$
On a donc les relations:

- $3P_0 = 3P_1 = 3P_{t_1} = 3P_{t_2} = 0$
- $3(P_{1,j} - P_{2,j}) = 3(P_{1,j} - P_{3,j}) = 0 \quad \text{pour} \quad 1 \leq j \leq 3$
- $3(P_{4,j} - P_{5,j}) = 3(P_{4,j} - P_{6,j}) = 0 \quad \text{pour} \quad 1 \leq j \leq 3$
- $P_0 + P_1 + P_{t_1} + P_{t_2} = 0$
- $P_{i,1} + P_{i,2} + P_{i,3} = 0 \quad \text{pour} \quad 1 \leq i \leq 6$
- $Q_{1,1} + Q_{1,2} + Q_{1,3} = 0$
- $Q_{4,1} + Q_{4,2} + Q_{4,3} = 0$
- $P_{1,j} + P_{2,j+1} + P_{3,j+2} + P_{t_2} = 0 \quad \text{pour} \quad 1 \leq j \leq 3$
- $P_{1,j} + P_{2,j+2} + P_{3,j+1} + P_{t_1} = 0 \quad \text{pour} \quad 1 \leq j \leq 3$
- $P_{4,j} + P_{5,j+1} + P_{6,j+2} + P_0 = 0 \quad \text{pour} \quad 1 \leq j \leq 3$
- $P_{4,j} + P_{5,j+2} + P_{6,j+1} + P_1 = 0 \quad \text{pour} \quad 1 \leq j \leq 3.$

On en déduit que:

- $P_{i,3} = -P_{i,1} - P_{i,2} \quad \text{pour} \quad 1 \leq i \leq 6$

- $P_{t_2} = -P_0 - P_1 - P_{t_1}$
- $P_{2,2} = P_{2,1} - P_{1,1} + P_{1,2} + P_{t_1} - P_{t_2} = P_{2,1} - P_{1,1} + P_{1,2} + P_0 + P_1 + 2P_{t_1}$
- $P_{3,1} = 2P_{1,1} - P_{2,1} + P_{t_1} - 2P_{t_2} = 2P_{1,1} - P_{2,1} + 2P_0 + 2P_1$
- $P_{3,2} = P_{1,2} + P_{2,1} - P_{3,1} + P_{t_1} = P_{1,1} - P_{2,1} + P_{1,2} + P_{t_1} + P_0 + P_1$
- $P_{5,2} = P_{5,1} - P_{4,1} + P_{4,2} + P_1 - P_0$
- $P_{6,1} = 2P_{4,1} - P_{5,1} + P_1 + P_0$
- $P_{6,2} = P_{4,2} + P_{5,1} - P_{6,1} + P_1 = P_{4,1} - P_{5,1} + P_{4,2} - P_0$.

On voit donc que W est engendré par $P_{1,1}$, $P_{1,2}$, $P_{4,1}$, $P_{4,2}$, P_0, P_1, P_{t_1}, $P_{1,1} - P_{2,1}$ et $P_{4,1} - P_{5,1}$. Les cinq derniers points sont d'ordre 3.
On a donc prouvé que:

Proposition 2.3.1. *W est un quotient de $\mathbb{Z}^4 \times (\mathbb{Z}/3\,\mathbb{Z})^5$.*

En fait, plus précisément, nous avons obtenu une application :

$$\begin{array}{ccc} \mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5 & \xrightarrow{\psi_\beta} & W_{\mathcal{C}_\beta} \\ (m_1,\ldots,m_4)(n_1,\ldots,n_5) & \longmapsto & m_1P_{1,1} + m_2P_{1,2} + m_3P_{4,1} + m_4P_{4,2} + n_1P_0 + \\ & & n_2P_1 + n_3P_{t_1} + n_4(P_{1,1} - P_{2,1}) + n_5(P_{4,1} - P_{5,1}) \end{array}$$

qui est surjective.
Nous allons montrer qu'en général, il n'y a pas d'autres relations entre ces points, et donc, que $W \cong \mathbb{Z}^4 \times (\mathbb{Z}/3\,\mathbb{Z})^5$. Notons W_1 le sous-groupe de W engendré par $P_{1,1}$, $P_{1,2}$, P_0, P_1, P_{t_1} et $P_{1,1} - P_{2,1}$, et notons W_2 celui engendré par $P_{4,1}$, $P_{4,2}$, P_0, P_1, P_{t_1}, et $P_{4,1} - P_{5,1}$. Ainsi W_1 et W_2 sont des quotients de $\mathbb{Z}^2 \times (\mathbb{Z}/3\,\mathbb{Z})^4$.

2.4 Descente via l'isogénie $1 - \zeta$

Pour calculer le rang et différencier les points d'ordre 3 dans le groupe engendré par les points de Weierstrass , on effectue une descente via l'isogénie «$1 - \zeta$» où ζ est une racine cubique de l'unité.

Nous utiliserons comme référence pour la descente l'article de Schaefer ([Sch]), dont nous conservons les notations, en indiquant au fur et à mesure le résultat que l'on obtient dans le cas que nous allons étudier. Les énoncés seront donc légèrement plus généraux que ceux dont nous aurons besoin.
Le résultat que nous allons utiliser peut être décrit informellement ainsi : soit α une racine de $f(x) = x(x-1)(x^2 - 2\beta x + \beta)$, l'application $P \mapsto x(P) - \alpha \bmod K^{*3}$ est a priori bien définie sauf si $P \in \{\infty, P_0, P_1, P_{t_1}, P_{t_2}\}$, ensemble que l'on note (disons) S. Par linéarité, on peut l'étendre aux diviseurs à support hors de S. On démontre alors qu'elle est invariante par équivalence

linéaire, et comme tout diviseur est linéairement équivalent à un diviseur à support disjoint de S, on obtient un homomorphisme $J(K) \to K^*/K^{*3}$. Le point clef est la proposition 2.4.4 qui affirme que le noyau du morphisme $J(K) \to (K^*/K^{*3})^4$ est exactement $\phi(J(K))$, où $\phi = 1 - \zeta$. Nous aurons d'autre part besoin d'analyser la torsion d'ordre 3, et ce qui nous servira est résumé dans la proposition 2.4.7. Tous les résultats de ce paragraphe sont contenus dans l'article de Schaefer ([Sch]) auquel nous renvoyons pour les détails des preuves.

Nous exposons les résultats de Schaefer dans le cadre général d'une courbe $\mathcal{C}$ de genre g, de jacobienne J et en remarque, dans le cas d'un revêtement cyclique de la droite projective.
Soit ϕ une isogénie de J. On suppose que le noyau de ϕ est d'exposant q premier. Soit $\widehat{\phi}$ l'isogénie duale. Notons $\widehat{J}[\widehat{\phi}]$ le noyau de $\widehat{\phi}$. Soit $\overline{K}$ une clôture algébrique de K.

Considérons alors la suite exacte courte $0 \to J[\phi] \to J \xrightarrow{\phi} J \to 0$. La cohomologie galoisienne induit une suite longue de cohomologie

$$0 \to J(K)[\phi] \to J(K) \xrightarrow{\phi} J(K) \xrightarrow{\delta} H^1(\mathrm{Gal}(\overline{K}/K), J[\phi]) \to \dots$$

Par abus de notation, on note encore $J(K)/\phi J(K) \xhookrightarrow{\delta} H^1(\mathrm{Gal}(\overline{K}/K), J[\phi])$.

Remarque : Soit ζ une racine primitive q-ième de l'unité. On suppose que $\zeta \in K$. Dans le cas particulier d'un revêtement cyclique de la droite projective, on considérera une isogénie particulière, «$1 - \zeta$» définie comme suit. Soit $f(x) = \prod_{i=1}^{n}(x - \alpha_i)$ un polynôme unitaire de degré n, sans racines doubles, à coefficients dans K, scindé sur K. On considère la courbe $\mathcal{C}$ définie par $y^q = f(x)$. Soit σ l'automorphisme de $\mathcal{C}$ qui sur la partie affine envoie (x,y) sur $(x,\zeta\, y)$. Cette application induit un automorphisme de J. Le diviseur de la fonction $x - x(P)$ est $\sigma^{q-1}\, P + \dots + \sigma\, P + P - q\infty$. C'est un diviseur principal, donc l'endomorphisme de la jacobienne J donné par $1 + \sigma + \sigma^2 + \dots + \sigma^{q-1}$ vaut 0. L'endomorphisme σ se comporte donc comme une racine primitive q-ième de l'unité dans $\mathrm{End}\,(J)$, que l'on appellera ζ par abus de notation. Notons $\phi = 1 - \zeta \in \mathrm{End}\,(J)$. ∎

Soit λ la polarisation principale canonique de J. Soit alors $\Psi = \lambda^{-1}(\widehat{J}[\widehat{\phi}])$. On a $\Psi \subset J[q]$. Choisissons un ensemble de diviseurs $\{D_1, \dots, D_n\}$ dans $\mathrm{Div}^0(C)$ invariant par $\mathrm{Gal}(\overline{K}/K)$ tel que les classes de diviseurs $\{[D_i]\}$ engendrent Ψ.

Soit $L' = \prod_{i=1}^{n} \overline{K_i}$ où $K_i = K$.
On définit une action de $\mathrm{Gal}(\overline{K}/K)$ sur L'. Pour $\sigma \in \mathrm{Gal}(\overline{K}/K)$, définissons $\overline{\sigma} \in S_n$ de la façon suivante : si ${}^{\sigma}D_i = D_j$, alors $\overline{\sigma} i = j$.
Posons ${}^{\sigma}(a_1, \ldots, a_n) = ({}^{\sigma}a_{\overline{\sigma}^{-1}1}, \ldots, {}^{\sigma}a_{\overline{\sigma}^{-1}n})$ pour $a_i \in \overline{K_i}$.
Soit alors L la sous-algèbre des éléments de L' invariants sous cette action de $\mathrm{Gal}(\overline{K}/K)$. On peut caractériser L de la façon suivante :
Soit Λ un sous-ensemble de $\{1, \ldots, n\}$ tel que $\{D_j\}_{j \in \Lambda}$ contienne un seul représentant de chaque orbite sous l'action de $\mathrm{Gal}(\overline{K}/K)$ des D_i. Soit alors $L_j = K(D_j)$ le corps de définition de D_j. On a: $L \cong \prod_{j \in \Lambda} L_j$.

Remarque : Dans le cas où la courbe $\mathcal{C}$ est donnée par une équation affine de la forme $y^q = f(x) = \prod_{i=1}^{n}(x - \alpha_i)$, on a $\Psi = J[\phi]$, et comme $J[\phi]$ est engendré par les $[(\alpha_i, 0) - \infty]$ ([Sch], Prop 3.2), on peut prendre $D_i = (\alpha_i, 0)$. On a alors:

$$L = K[T]/(f(T)) \cong K(\alpha_1) \times \ldots \times K(\alpha_r),$$

où $\alpha_1, \ldots, \alpha_r$ sont non conjuguées par $\mathrm{Gal}(\overline{K}/K)$.
Dans le cas où f est scindé, $L \cong K^n$. ∎

Soit alors f_i, définie sur $K(D_i)$ telle que qD_i soit le diviseur de f_i. Notons $\mathrm{Supp}(D_i)$ le support du diviseur D_i.
Définissons l'application $F = (f_1, \ldots, f_n)$ du complémentaire de $\bigcup \mathrm{Supp}(D_i)$ dans L'.

Définition : Un diviseur de degré 0 sur K ne rencontrant pas $\bigcup \mathrm{Supp}(D_i)$ est appelé un «bon diviseur». On note $\mathrm{Div}^0(\mathcal{C})_{bon}$ l'ensemble de ces diviseurs.

Remarque : Dès qu'il y a un point K-rationnel sur la courbe $\mathcal{C}$, tout élément de $J(K)/\phi J(K)$ est représenté par un bon diviseur. ∎

Remarque : Dans le cas d'un revêtement cyclique, si l'on fait le choix indiqué ci-dessus, les bons diviseurs sont ceux dont le support ne contient ni ∞, ni les points d'ordonnée nulle. ∎

Soit g une fonction définie sur K de C dans $\overline{K}$. Soit $R = \sum n_i R_i$ un diviseur de C de degré 0, défini sur K, dont le support ne rencontre pas celui de (g). On définit

$$g(R) = \prod (g(R_i))^{n_i} \in K^*.$$

On définit de même une application que l'on note encore F par

$$\begin{array}{ccc} \mathrm{Div}^0(\mathcal{C})_{bon} & \stackrel{F}{\to} & (K^*)^n \\ D & \mapsto & (f_i(D))_{1\leq i\leq n} \end{array}$$

Lemme 2.4.1. *Cette application passe au quotient, et fournit une application de $J(K)/\phi J(K)$ dans L^*/L^{*q}.*
Soit $\mu_q(L')$ le groupe des racines q-ièmes de l'unité dans L', *i.e.* $\mu_q(L') \cong \mu_q(\overline{K_1}) \times \ldots \times \mu_q(\overline{K_n})$.
L'accouplement de Weil est défini de la manière suivante : soient $P \in J[\phi]$ et $Q \in \widehat{J}[\widehat{\phi}]$, soit D un diviseur sur $\widehat{J}$ représentant P, il existe alors une fonction g sur $\widehat{J}$ de diviseur $\widehat{\phi}^{-1}D$. Posons $e_\phi(P,Q) = g(X+Q)/g(X)$ pour tout $X \in \widehat{J}$ pour lequel le terme de droite est défini.
Notons $e_\phi(P,Q)$ le ϕ-accouplement de Weil de $P \in J[\phi]$ et de $Q \in \widehat{J}[\widehat{\phi}]$. On définit alors w de $J[\phi]$ dans $\mu_q(L')$ par

$$w(P) = (e_\phi(P,\lambda[D_1]), \ldots, e_\phi(P,\lambda[D_n])).$$

Remarque : Dans le cas d'un revêtement cyclique de la courbe projective, vu les choix effectués, cette application s'écrit :

$$w(P) = (e_\phi(P,\lambda((\alpha_1,0) - \infty)), \ldots, e_\phi(P,\lambda((\alpha_{n-1},0) - \infty))). \qquad \blacksquare$$

Proposition 2.4.2. *L'application w de $J[\phi]$ dans $\mu_q(L')$ est injective et est invariante par* $\mathrm{Gal}(\overline{K}/K)$.

L'application w induit une application de $H^1(\mathrm{Gal}(\overline{K}/K),J[\phi])$ vers $H^1(\mathrm{Gal}(\overline{K}/K),\mu_q(L'))$, que l'on note encore w.
Comme $H^1(\mathrm{Gal}(\overline{K}/K),\overline{K}^*) = 0$ (théorème de Hilbert 90), on a l'isomorphisme de Kummer

$$k : H^1(K,\mu_q(L')) \stackrel{\cong}{\longrightarrow} L^*/L^{*q}.$$

Proposition 2.4.3. *Avec les notations précédentes, le diagramme suivant est commutatif:*

$$\begin{array}{rcl} J(K)/\phi J(K) & \stackrel{F}{\longrightarrow} & L^*/L^{*q} \\ \delta \downarrow & & \uparrow k \\ H^1(\mathrm{Gal}(\overline{K}/K),J[\phi]) & \stackrel{w}{\longrightarrow} & H^1(\mathrm{Gal}(\overline{K}/K),\mu_q(L')) \end{array}$$

Remarque : L'application δ est une injection, et k est un isomorphisme. ∎

Nous considérons dorénavant le cas particulier du revêtement cyclique de $\mathbb{P}^1$.
Dans ce cas, l'application F correspond au n-uplet de fonctions $(x-\alpha_1, \ldots, x-\alpha_n)$ que l'on note $x-T$. Elle est définie de l'ensemble des bons diviseurs dans L^* par

$$(x-T)(R) = \prod (x(R_i) - T)^{n_i}.$$

Comme q est premier, l'application

$$H^1(\mathrm{Gal}(\overline{K}/K), J[\phi]) \xrightarrow{w} H^1(\mathrm{Gal}(\overline{K}/K), \mu_q(L'))$$

est une injection (cf [Sch] p 462) ; l'application $x-T$ définit alors une injection de $J(K)/\phi J(K)$ dans L^*/L^{*q}, et son image est contenue dans le noyau de la norme de L^*/L^{*q} dans K^*/K^{*q}.
On obtient donc

Proposition 2.4.4. *L'application $J(K) \to L^*/L^{*q}$ ainsi définie a pour noyau $\phi(J(K))$.*

On a la caractérisation suivante de l'image d'un diviseur par l'application $x-T$:

Proposition 2.4.5. *Tout élément de $J(K)$ peut être représenté par un diviseur de degré 0, défini sur K dont le support ne contient ni ∞ ni les points d'ordonnée nulle. En particulier, soit $D = {}^{\sigma_1}Q + \ldots + {}^{\sigma_r}Q - r\infty$ où les ${}^{\sigma_i}Q$ sont les r conjugués sur K du point Q de $\mathcal{C}$ et $y(Q) \neq 0$. On a*

$$(x-T)([D]) \equiv \prod_{i=1}^{r} (x({}^{\sigma_i}Q) - T) (\mathrm{mod}\, L^{*q}).$$

Soit $D = (\alpha_1, 0) + \ldots + (\alpha_r, 0) - r\infty$ où les α_i sont conjugués sur K, et $r < n$. On a

$$(x-T)([D]) \equiv \prod_{i=r+1}^{n} (\alpha_i - T)^{-1} \times \prod_{i=1}^{r} (\alpha_i - T) \pmod{L^{*q}}.$$

Afin de comparer les dimensions respectives de $J(K)[3]$ et de $J(K)[\phi]$, on va se servir de la proposition suivante, dont la preuve est élémentaire :

Proposition 2.4.6. *On a la suite exacte:*

$$0 \to \frac{J(K)[\phi]}{\phi(J(K)[3])} \to J(K)/\phi J(K) \xrightarrow{\phi} J(K)/3J(K) \to J(K)/\phi J(K) \to 0.$$

Notons $\dim M$ la dimension d'un $\mathbb{Z}/3\mathbb{Z}$-espace vectoriel M. Comme K contient une racine cubique de l'unité et comme le polynôme f est supposé scindé sur K, on a $\dim J(K)[\phi] = 3$.
En effet, comme $\phi^2 = -3\zeta$, et $\dim J[3] = 6$, on a $\dim J[\phi] = 3$.

Proposition 2.4.7. *On a alors* $\dim J(K)[\phi]/\phi(J(K)[3]) = 6 - \dim(J(K)[3])$.

En effet, si $J(K)[3] = (\mathbb{Z}/3\mathbb{Z})^r$, comme $J[\phi] \subset J(K)[3]$, on a $\dim \phi(J(K)[3]) = r-3$ et donc $\dim J(K)[\phi]/\phi(J(K)[3]) = 3-(r-3) = 6-r$.

2.5 Descente explicite

Nous connaissons la structure de W pour $\beta = 1/2$. Nous pourrions tenter de déterminer la structure de W pour t générique. Cela n'est pas nécessaire ; en effet, la détermination de W dans un cas particulier nous permettra, en utilisant un argument de spécialisation, de le connaître dans le cas général. En fait, nous allons commencer ce calcul pour t générique (2.5.2), (2.5.3), mais nous ne le terminerons que pour une valeur spéciale (2.5.4), ce qui nous permettra de conclure. Soit K un corps de nombre contenant $\mathbb{Q}(\sqrt{-3})$. Notons $\zeta = -\dfrac{1+\sqrt{-3}}{2}$.

2.5.1 Spécialisation en $\beta = 1/2$

Lorsque β vaut $1/2$, la courbe admet 20 points de Weierstrass. En effet, pour $t = 1-\sqrt{3}$, on a $u = 1/2$ et donc les points d'abscisse x_1 et ceux d'abscisse x_4 coïncident. Ce sont en outre les quatrièmes points d'intersection de la tangente en un point de Weierstrass avec la courbe. On en déduit donc que les points $P_{1,j}$ et $P_{4,j}$ sont d'ordre 4. De plus, après le changement de variables $(x,y) \mapsto (2\,x - 1, 4^{2/3}\,y)$, la courbe admet pour équation $y^3 + 1 = x^4$, et on connaît exactement le groupe engendré par les points de Weierstrass de cette courbe ([KS]) : On a $W_{\mathcal{C}_{1/2}} = W_{\mathcal{C}_{1/2}}(\mathbb{Q}(\zeta_{12})) \cong (\mathbb{Z}/4\mathbb{Z})^2 \times (\mathbb{Z}/3\mathbb{Z})^5$.
Nous remarquons de plus que $P_{1,1}$ et $P_{1,2}$ engendrent $(\mathbb{Z}/4\mathbb{Z})^2$. En particulier, d'après la proposition 1.3.3, pour toute courbe C_β, le groupe engendré par $P_{1,1}$ et $P_{1,2}$ est soit $\mathbb{Z}^2$, soit $\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, soit $(\mathbb{Z}/4\mathbb{Z})^2$.

2.5.2 Détermination de W_1

Rappelons que W_1 est le sous-groupe de W engendré par $P_{1,1}$, $P_{1,2}$, P_0, P_1, P_{t_1} et $P_{1,1} - P_{2,1}$. Nous déterminons la partie infini de W_1 pour presque tout $t \in K$.
Pour que les points de Weierstrass qui engendrent W_1 soient K-rationnels, on effectue le changement de coordonnées $(x,y) \mapsto (2\,x,2\,\sqrt[3]{2}\,y)$; l'équation de la courbe devient

$$y^3 = x\,(x-2)\left(x^2 - 27\,\frac{(t+1)^2\,t^2}{(t^2+t+1)^3}\,x + 27\,\frac{(t+1)^2\,t^2}{(t^2+t+1)^3}\right).$$

Les racines de f sont 0, 2, $2\,t_1 = \dfrac{-24\,\sqrt{-3}\,(1+t)\,t}{\left(2\,t+1-\sqrt{-3}\right)^3}$ et $2\,t_2 = \dfrac{24\,\sqrt{-3}\,(1+t)\,t}{\left(2\,t+1+\sqrt{-3}\right)^3}$.

On a donc $L = K[T]/(f(T)) \cong K \times K \times K \times K$ via $T \mapsto (0,2,2\,t_1,2\,t_2)$ et L^*/L^{*3} est isomorphe à $(K^*/K^{*3})^4$. Par abus de notation, on note encore $P_{i,j}$ les points après changement de coordonnées.

Il y a bonne réduction hors de 2 et des places $\mathfrak{p}$ de K qui divisent le numérateur ou le dénominateur de $3\,t\,(t+1)\,(t^2+t+1)\,(t-1)\,(2t+1)\,(t+2)$.

Notons: $A = (2t+1+\sqrt{-3})$, $B = (2t+1-\sqrt{-3})$, $C = (2t+1)$, $D = (t+2)$, $E = (t-1)$, $F = (t+1)$.
On a $AB = 4(t^2+t+1)$.
Considérons d'abord les images des points qui engendrent $J[\phi]$ par l'application $x - T$; l'application $x - T$ étant le quadruplet de fonctions $(x,x-2,x-2\,t_1,x-2\,t_2)$, pour calculer l'image de $[(\alpha,0) - P_\infty]$, on évalue les trois autres coordonnées et en $x - \alpha$, la coordonnée vaut le produit des carrés des trois autres (dans K^*/K^{*3}).
Dans le tableau qui suit, on note dans chaque colonne l'image du point P par $x - \alpha_i$ dans K^*/K^{*3}.

	$x-0$	$x-2$	$x-2\,t_1$	$x-2\,t_2$
$[(0,0) - P_\infty]$	$4\,F\,t$	2	$F\,t$	$F\,t$
$[(2,0) - P_\infty]$	2	$4\,C\,D\,E$	$C\,D\,E$	$C\,D\,E$
$[(2\,t_1,0) - P_\infty]$	$F\,t$	$C\,D\,E$	$C\,D\,E\,F\,t$	$C\,D\,E\,F\,t$

Ce tableau permet de voir que les images des générateurs de $J[\phi]$ dans L^*/L^{*3} sont liées. L'image a dimension au plus 2 en tant que $\mathbb{Z}/3\mathbb{Z}$-espace vectoriel. D'après la proposition 2.4.7, $\dim J(K)[3] \geq 4$.

Calculons maintenant les images par l'application $x-T$ des autres points engendrant W_1.

	$x-0$	$x-2$	$x-2\,t_1$	$x-2\,t_2$
$[(0,0)-P_\infty]$	$4\,F\,t$	2	$F\,t$	$F\,t$
$[(2,0)-P_\infty]$	2	$4\,C\,D\,E$	$C\,D\,E$	$C\,D\,E$
$[P_{1,1}-P_\infty]$	$3.4\,A^2\,B^2\,F$	$4\,A^2\,B^2\,C\,E$	$2.3\,\zeta\,A^2\,C\,E\,F$	$2.3\,\zeta^2\,B^2\,C\,E\,F$
$[P_{2,1}-P_\infty]$	$3.4\,A^2\,B^2\,F\,t$	$4\,A^2\,B^2\,D\,E$	$2.3\,t\,A^2\,D\,E\,F$	$2.3\,t\,B^2\,D\,E\,F$
$[P_{1,1}-P_{2,1}]$	t^2	$C\,D^2$	$\zeta\,C\,D^2\,t^2$	$\zeta^2\,C\,D^2\,t^2$

Ce tableau permet de voir que, sauf pour un nombre fini de valeurs de t, les images de $[P_{1,1}-P_\infty]$ et de $[P_{1,2}-P_\infty]$ sont indépendantes des images de la torsion d'ordre premier à 3. En effet, tout point de torsion d'ordre premier à 3 est dans le noyau de $x-T$. Si $[P_{1,j}-P_\infty]$ était un point de torsion d'ordre premier à 3, son image serait dans le noyau de $x-T$, et donc, t satisferait les équations

$$\begin{cases} 3(t^2+t+1)^2(t+1) & \equiv \ 1 \bmod K^{*\,3} \\ (t^2+t+1)^2(t-1)(2t+1) & \equiv \ 1 \bmod K^{*\,3} \\ 2.3.\zeta(2t+1+\sqrt{-3})^2(2t+1)(t-1)(t+1) & \equiv \ 1 \bmod K^{*\,3}. \end{cases}$$

Les deux premières équations reviennent à considérer l'existence d'éléments s, s' de K tels que $3(t^2+t+1)^2(t+1)=s^3$ et $(t^2+t+1)^2(t-1)(2t+1)=s'^3$. Cela correspond à trouver des points K-rationnels sur des courbes lisses de genre au moins deux, et on sait qu'ils sont en nombre fini.
D'autre part, lorsqu'on spécialise en $\beta = 1/2$, les points $P_{1,1}$ et $P_{1,2}$ engendrent un groupe isomorphe à $(\mathbb{Z}/4\mathbb{Z})^2$. La proposition 1.3.3 permet de conclure qu'ils sont génériquement d'ordre infini.

Par contre, en ce qui concerne les points d'ordre 3 dans W_1, nous ne pouvons rien conclure par cette méthode, car cela nous amènerait à considérer le rang sur K de courbes elliptiques.

On en déduit donc que $\mathbb{Z}^2 \subset W_1$ pour presque tout $t \in K$.

2.5.3 Détermination de W_2

Rappelons que W_2 est le sous-groupe de W engendré par $P_{4,1}$, $P_{4,2}$, P_0, P_1, P_{t_1}, et $P_{4,1}-P_{5,1}$. Nous déterminons la partie infinie de W_2 lorsque $u \in K$ est tel que $u/(u-1)$ soit un carré dans K, c'est-à-dire lorsque u est de la

forme $w^2/(w^2-1)$, avec $w \in K$, ce qui correspond au cas particulier où $\frac{(t+1)\ t}{(2t+1)\ (t+2)\ (t-1)}$ est un cube dans K (d'après la remarque 2.2.2).
Pour que les points de Weierstrass $P_{4,i}$, $P_{5,i}$, et $P_{6,i}$ soient définis sur K, nous allons appliquer le changement de coordonnées $(x,y) \mapsto (x\,(3\,u^2-3\,u+1), y\,(3\,u^2-3\,u+1)^{(4/3)})$, et l'équation de la courbe devient

$$y^3 = x\left(x-3\,u^2+3\,u-1\right)\left(x^2-2\,u^3x+u^3\left(3\,u^2-3\,u+1\right)\right) = g(x).$$

Les racines de g sont 0, t'_0, t'_1 et t'_2 avec

$$\begin{cases} t'_0 &= \dfrac{(w^2-w+1)\,(w^2+w+1)}{(w-1)^2\,(w+1)^2} \\ t'_1 &= \dfrac{w^3\,(w^2+w+1)}{(w-1)^2\,(w+1)^3} \\ t'_2 &= \dfrac{w^3\,(w^2-w+1)}{(w+1)^2\,(w-1)^3}. \end{cases}$$

On a donc $L = K[T]/(f(T)) \cong K \times K \times K \times K$ via $T \mapsto (0,t_0,t_1,t_2)$ et L^*/L^{*3} est isomorphe à $(K^*/K^{*3})^4$. Par abus de notation, on note encore $P_{i,j}$ les points après changement de coordonnées.

La courbe a bonne réduction hors de 2 et des places $\mathfrak{p}$ de K qui divisent le numérateur ou le dénominateur de $3\,u\,(u-1)\,(3u^2-3u+1)$ *i.e.* des places $\mathfrak{p}$ qui divisent le numérateur ou le dénominateur de $3\,w\,(w-1)\,(w+1)\,(w^2-w+1)\,(w^2+w+1)$.

Notons: $A=(w-1)$, $B=(w+1)$, $C=(2\,w+1+\sqrt{-3}))$, $D=(2\,w+1-\sqrt{-3})$, $E=(2\,w-1+\sqrt{-3})$, $F=(2\,w-1-\sqrt{-3})$.
On a $C\,D = 4\,(w^2+w+1)$ et $E\,F = 4\,(w^2-w+1)$.

Considérons les images de $J[\phi]$

	$x-0$	$x-t'_0$	$x-t'_1$	$x-t'_2$
$[(0,0)-P_\infty]$	$4\,A\,B\,C\,D\,E\,F$	$4\,A\,B\,C\,D\,E\,F$	$2\,A\,C\,D$	$2\,B\,E\,F$
$[(t'_0,0)-P_\infty]$	$4\,A\,B\,C\,D\,E\,F$	$4\,A\,B\,C\,D\,E\,F$	$2\,A\,C\,D$	$2\,B\,E\,F$
$[(t'_1,0)-P_\infty]$	$2\,A\,C\,D$	$2\,A\,C\,D$	$A\,C\,D$	2

Ce tableau permet de conclure que l'image de $J[\phi]$ dans L^*/L^{*3} est de dimension au plus 2. D'après la proposition 2.4.7, $\dim J(K)[3] \geq 4$. Calculons

maintenant les images par l'application $x - T$ des autres points engendrant W_2.

	$x-0$	$x-t'_0$	$x-t'_1$	$x-t'_2$
$[(0,0)-P_\infty]$	$4\,A\,B\,C\,D\,E\,F$	$4\,A\,B\,C\,D\,E\,F$	$2\,A\,C\,D$	$2\,B\,E\,F$
$[(t'_1,0)-P_\infty]$	$2\,A\,C\,D$	$2\,A\,C\,D$	$A\,C\,D$	2
$[P_{4,1}-P_\infty]$	$2\,C\,D\,E\,F\,w^2$	$2\,C\,D\,E\,F$	$4\,w^2\,C\,D$	$4\,w^2\,E\,F$
$[P_{5,1}-P_\infty]$	$2\,A\,B\,C\,F\,w^2$	$2\,\zeta\,A\,B\,C\,F$	$4\,\zeta\,w^2\,A\,C$	$4\,\zeta\,w^2\,B\,F$
$[P_{4,1}-P_{5,1}]$	$A^2\,B^2\,D\,E$	$\zeta^2\,A^2\,B^2\,D\,E$	$\zeta^2\,A^2\,D$	$\zeta^2\,B^2\,E$

Ce tableau permet de voir que, sauf pour un nombre fini de valeurs de u, les images de $[P_{4,1}-P_\infty]$ et de $[P_{4,2}-P_\infty]$ sont indépendantes des images de la torsion d'ordre premier à 3. En effet, tout point de torsion d'ordre premier à 3 est dans le noyau de $x-T$. Si $[P_{4,j}-P_\infty]$ était un point de torsion d'ordre premier à 3, son image serait dans le noyau de $x-T$, et donc, u satisferait les équations

$$\left\{\begin{array}{rcl} 4\,(w^2+w+1)\,(w^2-w+1)\,w^2 & \equiv & 1 \bmod K^{*3} \\ 4\,(w^2+w+1)\,(w^2-w+1) & \equiv & 1 \bmod K^{*3} \\ 2\,w^2\,(w^2+w+1) & \equiv & 1 \bmod K^{*3} \\ 2\,w^2\,(w^2-w+1) & \equiv & 1 \bmod K^{*3}. \end{array}\right.$$

On en déduit que w^2 serait un cube, et donc en particulier, il existerait des éléments s et s' de K tels que $2\,(w^2+w+1) = s^3$ et que $2\,(w^2-w+1) = s'^3$. Cela revient à considérer l'existence de points K-rationnels sur la courbe elliptique d'équation $y^2 = x^3 - 12$. Comme cette courbe a rang 0 sur $\mathbb{Q}$, et est isogène à sa tordue par -3 , elle a rang 0 sur $\mathbb{Q}(\sqrt{-3})$. Lorsque K n'est pas le corps $\mathbb{Q}(\sqrt{-3})$, les autres équations nous donnent des courbes de genre supérieur à 2, qui n'ont donc qu'un nombre fini de points K-rationnels. D'autre part, lorsqu'on spécialise en $\beta = 1/2$, les points $P_{4,1}$ et $P_{4,2}$ engendrent un groupe isomorphe à $(\mathbb{Z}/4\mathbb{Z})^2$. La proposition 1.3.3 permet de conclure qu'ils sont génériquement d'ordre infini.

Par contre, en ce qui concerne les points d'ordre 3 dans W_2, nous ne pouvons rien conclure par cette méthode, car cela nous amènerait à considérer le rang sur K de courbes elliptiques.

On en déduit que $\mathbb{Z}^2 \subset W_2$ pour presque tout $u \in K$ tel que $u/(u-1)$ soit un carré dans K.

Il est probable que l'on puisse terminer directement l'analyse du groupe W pour β générique, néanmoins nous avons trouvé plus commode de compléter

les calculs pour une spécialisation bien choisie, ce qui est l'objet du paragraphe suivant.

2.5.4 Spécialisation en $t = 7$

On a (sauf pour un nombre fini de valeurs de t et de u), $\mathbb{Z}^2 \subset W_1 \subset W$ et $\mathbb{Z}^2 \subset W_2 \subset W$. Montrons que dans certains cas, $W = \mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5$. Considérons le cas où $\beta_0 = \frac{784}{6859}$ (qui correspond à $t = 7$) ; nous allons montrer dans cette partie le résultat suivant :

Proposition 2.5.1. *Pour $\beta_0 = \frac{784}{6859}$, le groupe engendré par les points de Weierstrass est $W_{\mathcal{C}_{\beta_0}} = \mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5$.*

La courbe $\mathcal{C}$ a pour équation affine : $y^3 = x\,(x-1)\left(x^2 - \frac{1568}{6859}\,x + \frac{784}{6859}\right)$.
Soit $K = \mathbb{Q}(\sqrt{-3})$. Pour que les points de Weierstrass $P_{1,i}$, $P_{2,i}$, $P_{3,i}$ aient des coordonnées K-rationnelles, on effectue le changement de coordonnées $(x,y) \mapsto (2\,x, 2\,y\sqrt[3]{2})$ la courbe devient $y^3 = x^4 - \frac{16854}{6859}\,x^3 + \frac{9408}{6859}\,x^2 - \frac{6272}{6859}\,x = g(x)$.
Les racines de g sont 0, 2, $2t_1 = \frac{1568}{6859} - \frac{2520}{6859}\sqrt{-3}$ et $2t_2 = \frac{1568}{6859} + \frac{2520}{6859}\sqrt{-3}$. On a donc $L = K[T]/(f(T)) \cong K \times K \times K \times K$ via $T \mapsto (0,2,2t_1,2t_2)$ et L^*/L^{*3} est isomorphe à $(K^*/K^{*3})^4$. Par abus de notation, on note encore $P_{i,j}$ les points après changement de coordonnées. Soit P_β un point d'abscisse β sur C (*i.e.* le quatrième point d'intersection de la tangente en un des points $P_{4,j}$, $P_{5,j}$ ou $P_{6,j}$ avec la courbe). On note encore P_β son image après changement de coordonnées. Le point P_β est à coordonnées dans $K(\sqrt[3]{105})$. Le corps de définition de tous les points de Weierstrass est $K(\sqrt[3]{105},\sqrt[3]{14})$, et on a $u = 196/\left(196 + 3\sqrt[3]{1470}\right)$.
Il y a bonne réduction hors des places au dessus de 2, 3, 5, 7, 19.
Dans K, 2 est inerte, 3 se ramifie en $\mathfrak{c}$ (*i.e.* $(3) = \mathfrak{c}^2$), 5 est inerte, 7 se décompose en $\mathfrak{e}\,\mathfrak{f}$ et 19 se décompose en $\mathfrak{a}\,\mathfrak{b}$. Puis dans $K(\sqrt[3]{105})$, 2 se décompose, $\mathfrak{c}$ se ramifie, 5 se ramifie, $\mathfrak{e}$ et $\mathfrak{f}$ se ramifient, et $\mathfrak{a}$ et $\mathfrak{b}$ sont inertes.

Notons $a = (4 + \sqrt{-3})$, $b = (4 - \sqrt{-3})$, $c = \sqrt{-3}$, $e = (2 - \sqrt{-3})$ et $f = (2 + \sqrt{-3})$.
Considérons d'abord les images des points qui engendrent $J[\phi]$ par l'application $(x - T)_K : J(K) \to K[T]/(g(T))$:

	$x - 0$	$x - 2$	$x - 2\,t_1$	$x - 2\,t_2$
$[(0,0) - P_\infty]$	$4\,e\,f$	2	$e\,f$	$e\,f$
$[(2,0) - P_\infty]$	2	$5\,c^2$	$2.5\,c^2$	$2.5\,c^2$
$[(2\,t_1,0) - P_\infty]$	$e\,f$	$2.5\,c^2$	$2.5\,c^2\,e\,f$	$2.5\,c^2\,e\,f$

Les images des générateurs de $J[\phi]$ dans L^*/L^{*3} sont liées. L'image a dimension 2 en tant que $\mathbb{Z}/3\mathbb{Z}$-espace vectoriel. Il nous faut déterminer les images des points dans $K(\sqrt[3]{105})^*/K(\sqrt[3]{105})^{*3}$. Considérons alors les images par l'application $(x-T)_{K(\sqrt[3]{105})} : J(K(\sqrt[3]{105})) \to K(\sqrt[3]{105})[T]/(g(T))$ des points engendrant W_1 ainsi que celle de P_β.

	$x-0$	$x-2$	$x-2\,t_1$	$x-2\,t_2$
$[(0,0)-P_\infty]$	$4\,e\,f$	2	$e\,f$	$e\,f$
$[(2,0)-P_\infty]$	2	$5\,c^2$	$2.5\,c^2$	$2.5\,c^2$
$[P_{1,1}-P_\infty]$	$a^2\,b^2$	$2.5\,a^2\,b^2\,c^2$	$2.5\,c^2\,b^2\,\zeta^2$	$2.5\,c^2\,a^2\,\zeta$
$[P_{2,1}-P_\infty]$	$a^2\,b^2\,e\,f$	$2\,c\,a^2\,b^2$	$2\,c\,b^2\,\zeta\,e\,f$	$2\,c\,a^2\,\zeta^2\,e\,f$
$[P_{1,1}-P_{2,1}]$	$e^2\,f^2$	$5\,c$	$5\,c\,e^2\,f^2\,\zeta$	$5\,c\,e^2\,f^2\,\zeta^2$
$[P_\beta-P_\infty]$	$4\,e^2\,f^2$	$2.5^2\,c$	$5\,c^2\,e\,f$	$5\,c^2\,e\,f$

Ce tableau nous permet de voir que les images de $[P_{1,1}-P_\infty]$ et de $[P_{1,2}-P_\infty]$ sont indépendantes des images de la torsion. En effet, leurs coordonnées font intervenir des puissances de 19, ce qui n'est le cas pour aucun des points de torsion. On en déduit que ces deux classes de diviseurs sont d'ordre infini.

En ce qui concerne les points d'ordre 3, ce tableau permet de voir que $P_{1,1}-P_{2,1}$ est $(\mathbb{Z}/3\mathbb{Z})$-indépendant des points de $J[\phi]$.
D'autre part, comme, ni $P_{4,1}$, ni $P_{5,1}$ n'est dans $J(K(\sqrt[3]{105}))$, leur différence non plus n'est pas dans $J(K(\sqrt[3]{105}))$. En effet cela découle du lemme suivant:

Lemme 2.5.2. *Soit k un corps de caractéristique 0, soit $\mathcal{C}$ une courbe non-hyperelliptique définie sur k et soient $j(P)$ et $j(Q)$ deux points distincts n'appartenant pas à $J(k)$, alors leur différence n'est pas non plus dans $J(k)$.*

DÉMONSTRATION : En effet, supposons que $j(P)-j(Q)$ soit dans $J(k)$. Soit $\sigma \in \mathrm{Gal}(\overline{\mathrm{k}}/\mathrm{k})$ tel que ${}^\sigma P \neq P$, on a alors ${}^\sigma(j(P)-j(Q)) = (j(P)-j(Q))$, et donc $j({}^\sigma P - P - {}^\sigma Q + Q) = 0$. Remarquons que ${}^\sigma P \neq P$ par construction. D'autre part, ${}^\sigma P \neq {}^\sigma Q$ puisque $P \neq Q$ par hypothèse. On obtient ainsi un diviseur principal non nul sur $\mathcal{C}$, *i.e.* $\mathrm{div}\,(g) = {}^\sigma P - P - {}^\sigma Q + Q$. On a un morphisme de degré ≤ 2, $\overline{g} : \mathcal{C} \to \mathbb{P}^1$, ce qui contredit le fait que $\mathcal{C}$ n'est pas hyperelliptique. ∎

On a donc quatre éléments d'ordre 3 $\mathbb{Z}/3\mathbb{Z}$-indépendant à coordonnées K-rationnelles, et un cinquième point d'ordre 3, qui n'est pas défini sur K. Il est donc $(\mathbb{Z}/3\mathbb{Z})$-indépendant des quatre autres (en effet, ni lui, ni son opposé n'étant à coordonnées K-rationnelles, aucun multiple de ce point n'est à coordonnées K-rationnelles) et donc $(\mathbb{Z}/3\mathbb{Z})^5 \subset W$.

D'autre part, nous allons montrer un résultat sur les points de torsion d'ordre 3, qui nous sera utile par la suite :

Lemme 2.5.3. *Les points de torsion d'ordre 3 de* $J(K(\sqrt[3]{105}))$ *sont dans* W_1.

DÉMONSTRATION : En effet, W_1 contient 4 points d'ordre 3 qui sont $(\mathbb{Z}/3\mathbb{Z})$-indépendants. De plus, ces points sont K-rationnels, donc *a fortiori* $K(\sqrt[3]{105})$-rationnels. D'autre part, le point $P_{4,1} - P_{5,1}$ est d'ordre 3, mais n'est pas dans $J(K(\sqrt[3]{105}))$. Tous ces points sont $K(\sqrt[3]{105}, \sqrt[3]{14})$-rationnels. Nous allons montrer qu'ils engendrent $J(K(\sqrt[3]{105}, \sqrt[3]{14})[3]$, et donc il n'existe pas de point d'ordre 3 à coordonnées $K(\sqrt[3]{105})$-rationnelles, qui ne soit pas dans W_1.

Dans $K(\sqrt[3]{105}, \sqrt[3]{14})$, les idéaux 13 et 37 sont totalement décomposés. On peut calculer le nombre de points de la jacobienne sur un corps fini, à partir des nombres de points de la courbe sur certaines extensions de ce corps fini, *i.e.* $\#J(\mathbb{F}_p) = \#\mathcal{C}(\mathbb{F}_p)^3/6 - p\,\#\mathcal{C}(\mathbb{F}_p) + \#\mathcal{C}(\mathbb{F}_p)\#\mathcal{C}(\mathbb{F}_{p^2})/2 + \#\mathcal{C}(\mathbb{F}_{p^3})/3$. En effet, pour une courbe C de genre g, de jacobienne J, on a pour tout p premier les formules suivantes $\#J(\mathbb{F}_p) = \prod_{1\leq i\leq 2g}(1 - a_i)$ ([Mil1] Theorem 19.1), $\#\mathcal{C}(\mathbb{F}_{p^m}) = p^m + 1 - \sum_{1\leq i\leq 2g} a_i^m$ ([Mil2] Theorem 11.1) et $|a_i| = \sqrt{p}$. De plus, la transformation $a \mapsto p/a$ laisse invariant l'ensemble $\{a_1, \ldots, a_{2g}\}$. Cela permet d'obtenir la formule ci-dessus.
Comme $\#J(\mathbb{F}_{13}) = 2^4.3^5$ et $\#J(\mathbb{F}_{37}) = 2^8.3^5$, on en déduit que
$J(K(\sqrt[3]{105}, \sqrt[3]{14}))[3] = (\mathbb{Z}/3\mathbb{Z})^5$. ∎

Remarque : Remarquons que W_1 est stable par l'action de $1 - \zeta$. En effet $\zeta(P_{1,1} - P_{2,1}) = P_{1,2} - P_{2,2} = P_{1,1} - P_{2,1} - P_0 - P_1 + P_{t_1}$. Et c'est immédiat pour les autres générateurs de W_1. ∎

Considérons maintenant la partie infinie de W. Nous allons montrer que les seules relations entre les points $P_{4,1}$ et $P_{4,2}$ et les générateurs de W_1 sont celles que nous avions déjà au paragraphe 3.4. Pour ce faire, nous allons raisonner avec $P_{\beta,1} = -3P_{4,1}$ et $P_{\beta,2} = -3P_{4,2}$ qui sont définis sur un corps plus petit.

Montrons d'abord le lemme suivant

Lemme 2.5.4. *Aucun élément de la forme* $(3n_1 + r_1)P_{\beta,1} + (3n_2 + r_2)P_{\beta,2}$ *avec* $r_1 + r_2 \neq 0$ *n'est dans* W_1.

DÉMONSTRATION : Supposons qu'il y ait un élément de la forme $(3n_1 + r_1)P_{\beta,1} + (3n_2 + r_2)P_{\beta,2}$ avec $r_1 + r_2 \neq 0$ dans W_1. Considérons l'image par $(x -$

$T)_{K(\sqrt[3]{105})}$ de cet élément ; elle est égale à $\left((x-T)_{K(\sqrt[3]{105})}(P_\beta)\right)^{r_1+r_2}$ et donc à l'image de $\pm P_\beta$. Pour éviter de calculer explicitement une décomposition de 3, 5 et 7 dans $K(\sqrt[3]{105})$, on raisonne selon deux cas :
Lorsque 3, 5, ou 7 ne sont pas congrus à une unité modulo les cubes dans $K(\sqrt[3]{105})$, le tableau précédent nous permet de montrer directement qu'un point de la forme $(3n_1+r_1)P_{\beta,1}+(3n_2+r_2)P_{\beta,2}$ (avec $r_1+r_2\neq 0$) ne peut être dans W_1. En effet, si l'on considère (par exemple) la valuation en 7 des images des points par $(x-T)_{K(\sqrt[3]{105})}$, on remarque que les images des points engendrant W_1 ont même valuation pour leur première et leur troisième coordonnée, ce qui n'est pas le cas pour l'image de P_β. Dans le cas contraire, c'est-à-dire lorsque $ef \equiv u_1 \bmod K(\sqrt[3]{105})^{*3}$, $5 \equiv u_2 \bmod K(\sqrt[3]{105})^{*3}$ et $\sqrt{-3}\equiv u_3 \bmod K(\sqrt[3]{105})^{*3}$ (où les u_i sont des unités), les images par $x-T$ de P_β et des points engendrant W_1 deviennent dans $K(\sqrt[3]{105})^*/K(\sqrt[3]{105})^{*3}$:

	$x-0$	$x-2$	$x-2\,t_1$	$x-2\,t_2$
$[(0,0)-P_\infty]$	$4\,u_1$	2	u_1	u_1
$[(2,0)-P_\infty]$	2	$u_2\,u_3^2$	$2\,u_2\,u_3^2$	$2\,u_2\,u_3^2$
$[P_{1,1}-P_{2,1}]$	u_1^2	$u_2\,u_3$	$u_2\,u_3\,u_1^2\,\zeta$	$u_2\,u_3\,u_1^2\,\zeta^2$
$[P_\beta-P_\infty]$	$4\,u_1^2$	$2\,u_2^2\,u_3$	$u_1\,u_2\,u_3^2$	$u_1\,u_2\,u_3^2$

auquel cas, ce tableau nous montre, que pour que les images de ces points soient liées, il faut nécessairement que u_1 soit égal à 1 (*i.e.* que 7 soit un cube dans $K(\sqrt[3]{105})$). Or ce n'est pas vrai dans $K(\sqrt[3]{105})$. En effet, si $x\in K$ était un cube dans $K(\sqrt[3]{105})$, *i.e.* $x=a^3$ on aurait $N(x)=N(a)^3=x^3$ et donc $N(a)=\zeta^\varepsilon\,x=\zeta^\varepsilon\,a^3$. Or cette équation n'a pas de solution $a\in K(\sqrt[3]{105})$ pour $x=7$.

Dans les deux cas, on peut conclure qu'aucun élément de la forme $(3n_1+r_1)P_{\beta,1}+(3n_2+r_2)P_{\beta,2}$ avec $r_1+r_2\neq 0$ n'est dans W_1. ∎

Proposition 2.5.5. *Il n'y a pas de point de la forme $m_1P_{4,1}+m_2P_{4,2}$ (avec $m_1m_2\neq 0$) dans W_1.*

DÉMONSTRATION : Supposons que l'on ait $3^k(m_1P_{4,1}+m_2P_{4,2})\in W_1$ avec $m_1m_2\neq 0$ et $\mathbf{3}\mid \mathrm{pcgd}\,(\mathbf{m_1},\mathbf{m_2})$.

1er cas : $\mathbf{k=0}$

En ajoutant à $m_1P_{4,1}+m_2P_{4,2}$ un certain nombre de fois $P_{\beta,1}$ et $P_{\beta,2}$, on a $r_1P_{4,1}+r_2P_{4,2}\in J(K(\sqrt[3]{105}))$ avec $r_i\in\{0,\pm 1\}$.

Si $\mathbf{r_1=0}$ ou $\mathbf{r_2=0}$ on a alors $r_iP_{4,i}\in J(K(\sqrt[3]{105}))$, ce qui est faux.

Si $\mathbf{r_1} = \mathbf{r_2} = \pm\mathbf{1}$ on a alors $P_{4,1} + P_{4,2} = -P_{4,3} \in J(K(\sqrt[3]{105}))$, ce qui est faux.

Si $\mathbf{r_1} + \mathbf{r_2} = \mathbf{0}$ on a alors $P_{4,1} - P_{4,2} \in J(K(\sqrt[3]{105}))$, ce qui est exclu par le lemme 2.5.2.

2ème cas : $\mathbf{k} > 0$

Cela revient à supposer que $3^{k-1}(m_1 P_{\beta,1} + m_2 P_{\beta,2}) \in W_1 \subset J(K)$, avec $3 \not| \operatorname{pcgd}(m_1, m_2)$.

En appliquant le lemme 2.5.7, on peut supposer que $m_1 P_{\beta,1} + m_2 P_{\beta,2} \in W_1$. On peut écrire ce point de W_1 sous la forme $(3n_1 + r_1)P_{\beta,1} + (3n_2 + r_2)P_{\beta,2} \in W_1$ avec $r_i \in \{0, \pm 1\}$.

Si $\mathbf{r_1} + \mathbf{r_2} \neq \mathbf{0}$ Ce cas-là n'est pas possible par le lemme 2.5.4.

Si $\mathbf{r_1} + \mathbf{r_2} = \mathbf{0}$ L'image par $\phi = 1 - \zeta$ de cet élément est encore dans W_1 et vaut $3(n_1 + n_2)P_{\beta,1} + 3(2n_2 - n_1 + r_2)P_{\beta,2}$, car $(1-\zeta)P_{\beta,1} = P_{\beta,1} - P_{\beta,2}$ et $(1-\zeta)P_{\beta,2} = P_{\beta,2} - P_{\beta,3} = P_{\beta,1} + 2P_{\beta,2}$. On applique de nouveau le lemme 2.5.7, et donc $(n_1 + n_2)P_{\beta,1} + (2n_2 - n_1 + r_2)P_{\beta,2} \in W_1$ On peut de nouveau écrire ce point sous la forme $(3n + r)P_{\beta,1} + (3(n_2 - n) + r_2 - r)P_{\beta,2}$ et on a $r + (r_2 - r) = r_2 \neq 0$, ce qui permet de conclure.

∎

Montrons d'abord que les triples de points dans $J(K(\sqrt[3]{105}))$ qui sont dans W_1 sont d'une forme particulière :

Lemme 2.5.6. *Si $P \in J(K(\sqrt[3]{105}))$ est tel que $3P \in W_1$, alors $3P$ est de la forme $m_0(P_0 + P_1 - P_{t_1}) + m_3(P_{1,1} - P_{1,2}) + 3m'_4 P_{1,2}$ et est donc déjà dans le noyau de $(x - T)_K$.*

DÉMONSTRATION : Comme $3P$ est dans W_1, on a une relation du type $3P = m_0 P_0 + m_1 P_1 + m_2 P_{t_1} + m_3 P_{1,1} + m_4 P_{1,2} + m_5(P_{1,1} - P_{2,1})$.

Comme $P \in J(K(\sqrt[3]{105}))$, $3P$ est dans le noyau de $(x - T)_{K(\sqrt[3]{105})}$, et donc, en particulier, si on considère la première coordonnée (selon $x - 0$), on doit avoir $2^{2m_0+m_1}(ef)^{m_0+m_2+2m_5}(ab)^{2(m_3+m_4)} \equiv 1 \bmod K(\sqrt[3]{105})^{*3}$ Comme 2, a, b et 7 ne sont pas des cubes dans $K(\sqrt[3]{105})$, cela entraîne que $m_0 \equiv m_1 \bmod 3$, $m_3 + m_4 \equiv 0 \bmod 3$ et $m_5 \equiv m_0 + m_2 \equiv m_1 + m_2 \bmod 3$. Les deuxième et troisième coordonnées doivent donc vérifier $2^{m_0+m_2} 5^{2(m_1+m_2)} \equiv 1 \bmod K(\sqrt[3]{105})^{*3}$ et $2^{m_1+m_2} 5^{2(m_1+m_2)} \zeta^{m_0+m_2} \equiv 1 \bmod K(\sqrt[3]{105})^{*3}$. Les m_i doivent donc satisfaire les relations de congruence suivantes $m_0 \equiv m_1 \equiv -m_2 \bmod 3$, $m_3 + m_4 \equiv 0 \bmod 3$ et $m_5 \equiv 0 \bmod 3$. Ces relations ont pour conséquence que le point $3P$ est déjà dans le noyau de $(x - T)_K$. ∎

Montrons que

Lemme 2.5.7. *Si $P \in J(K(\sqrt[3]{105}))$ est tel que $3P$ appartienne à W_1, alors $P \in W_1$.*

DÉMONSTRATION : On sait déjà par le lemme précédent que $3P = m_0(P_0 + P_1 - P_{t_1}) + m_3(P_{1,1} - P_{1,2}) + 3m'_4 P_{1,2}$ est dans le noyau de $(x-T)_K$, à savoir que $3P \in (1-\zeta)J(K)$.

1er cas Supposons que $P \in J(K(\sqrt[3]{105})) \setminus J(K)$.

Comme $(1-\zeta)^2 = -3\zeta$ dans $\mathrm{End}(J)$, cela revient à $(1-\zeta)^2 P \in (1-\zeta)J(K)$, et donc $(1-\zeta)P = Q + T$ avec $Q \in J(K)$ et $T \in \ker(1-\zeta) \subset J(K)$. Cela n'est pas possible car $(1-\zeta)P$ n'est pas dans $J(K)$ d'après le lemme 2.5.2.

2nd cas Supposons que $P \in J(K)$.

Comme $(1-\zeta)P_{1,1} = P_{1,1} - P_{1,2}$, on a en prenant l'image de $3P$ par $(1-\zeta)$, $3(1-\zeta)P = -3m_3\zeta P_{1,1} + 3m'_4(1-\zeta)P_{1,2}$ et donc $(1-\zeta)P = -m_3 P_{1,2} + m'_4 P_{1,2} - m'_4 P_{1,3} + T$ où $T \in J(K)[3] \subset W_1$ ce qui nous permet de conclure que $(1-\zeta)P \in W_1$.

Comme $P \in J(K)$, l'image par $(x-T)_K$ de $(1-\zeta)P$ est nulle, or $(1-\zeta)P = m'_4 P_{1,1} + (2m'_4 - m_3)P_{1,2} + T$. Les points $P_{1,1}$ et $P_{1,2}$ ayant la même image par $(x-T)_K$, cela entraîne que $3m'_4 - m_3 \equiv 0 \bmod 3$ *i.e.* $m_3 = 3m'_3$.

D'autre part $(1-\zeta)(1-\zeta)P = m'_4(1-\zeta)P_{1,1} + (2m'_4 - 3m'_3)(1-\zeta)P_{1,2} + (1-\zeta)m_5(P_{1,1} - P_{2,1}) = 3(m'_4 - m'_3)P_{1,1} + 3(m'_4 - 2m'_3)P_{1,2} = -3\zeta P$ car m_5 doit être un multiple de 3 d'après le lemme 2.5.7.

Cela entraîne que le point $\zeta P + (m'_4 - m'_3)P_{1,1} + (m'_4 - 2m'_3)P_{1,2}$ est un point de torsion d'ordre 3 et dans $J(K)$, il est donc dans W_1 d'après le lemme 2.5.3.

∎

On a ainsi montré qu'il n'existe pas d'autre relation entre $P_{4,1}$, $P_{4,2}$, $P_{1,1}$, $P_{1,2}$, P_0, P_1, P_{t_1}, et $P_{1,1} - P_{2,1}$ que celles fournies au paragraphe 2.3.

On a donc $W_{\mathcal{C}_{\beta_0}} = \mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5$, lorsque $\beta_0 = \frac{784}{6859}$.

Corollaire 2.5.8. *Soit $W_{\mathcal{C}_\eta}$ le groupe engendré par les points de Weierstrass de la courbe générique, on a $W_{\mathcal{C}_\eta} \cong \mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5$.*

DÉMONSTRATION : Comme $W_{\mathcal{C}_\eta}$ est un quotient de $\mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5$ (d'après la proposition 2.3.1), et comme $W_{\mathcal{C}_{\beta_0}}$ est un quotient de $W_{\mathcal{C}_\eta}$ (d'après la proposition 2.5.1), on en déduit que $W_{\mathcal{C}_\eta} \cong \mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5$. ∎

2.6 Conséquences

2.6.1 Preuve du théorème 2.1.1

Pour déduire la structure de $W_{\mathcal{C}_\beta}$ dans le cas général, nous avons besoin d'appliquer le théorème de spécialisation dû à Silverman ([Sil1]), dont nous redonnons l'énoncé.

Théorème 1.3.5 *Soit $A \to C$ une famille (plate) de variétés abéliennes toutes définies sur un corps global K, où C est une courbe projective lisse. En un point $t \in C(\overline{K})$ pour lequel la fibre A_t est non-singulière, on définit l'application de spécialisation $\sigma_t : A(C) \to A_t(\overline{K}), \quad P \mapsto P_t$.*

Si A n'a pas de partie constante, alors l'ensemble $\{t \in C(\overline{K}) \mid \sigma_t$ n'est pas injective $\}$ est un ensemble de hauteur bornée dans $C(\overline{K})$.

En particulier, lorsque K est un corps de nombres et $d \geq 1$ est un entier, alors σ_t est injective pour presque tout $t \in \bigcup_{[L:K] \leq d} C(L)$.

Nous allons appliquer ce théorème avec $A = \mathrm{Jac}(\mathcal{C}_\beta)$, $C = \mathbb{P}^1$ (ici, paramétrée par β). Nous devons donc vérifier qu'il n'y a pas de partie constante. Notons J_β la jacobienne de $\mathcal{C}_\beta$. Supposons que $J/\mathbb{Q}(\beta)$ ait une partie constante A_0, variété abélienne de dimension 1, 2 ou 3. Il existe alors un morphisme de $J/\mathbb{Q}(\beta)$ dans A_0, et donc un morphisme $\mathcal{C}/\mathbb{Q}(\beta) \stackrel{\phi_\beta}{\to} A_0$, où ϕ_β est défini sur $\mathbb{Q}(\beta)$. Soit $\mathcal{S}$ la surface algébrique définie par cette famille de courbes. Elle est birationnelle à la surface $\{(x,y,\beta) \in \mathbb{A}^3 \mid y^3 - x(x-1)(x^2 - 2\,\beta x + \beta) = 0\}$, et donc birationnelle à $\mathbb{P}^2$.
On a une application non constante $\mathcal{S} \cdots\!\!\longrightarrow A_0$. On en déduit une application non constante $\mathbb{P}^2 \cdots\!\!\longrightarrow A_0$, ce qui n'est pas possible.

Comme le groupe engendré par les points de Weierstrass de la fibre générique $W_{\mathcal{C}_\eta}$ est isomorphe à $\mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5$ (d'après le corollaire 2.5.8), on en déduit que pour presque tout β,$W_{\mathcal{C}_\beta} = \mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5$.

2.6.2 Preuve du corollaire 2.1.2

Cela nous permet de démontrer le corollaire 2.1.2, dont nous rappelons l'énoncé :

Corollaire 2.1.2 *Soit une famille de courbes lisses joignant une courbe hyperelliptique à une courbe $\mathcal{C}_\beta$ pour laquelle $W_{\mathcal{C}_\beta} = \mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5$. Soit $W_{\mathcal{C}_\eta}$ le groupe engendré par les points de Weierstrass de la fibre générique, on a alors $W_{\mathcal{C}_\eta} \cong \mathbb{Z}^r$ avec $9 \leq r \leq 23$.*

DÉMONSTRATION : En effet, la spécialisation $W_{\mathcal{C}_\eta} \to W_s$ étant injective sur la partie de torsion, si $W_{\mathcal{C}_\eta} = \mathbb{Z}^r \times G$, où G est un groupe fini, on a pour un s correspondant à la courbe $W_{\mathcal{C}_\beta}$, $G \hookrightarrow (\mathbb{Z}/3\mathbb{Z})^5$, et pour un s correspondant à la courbe hyperelliptique, $G \hookrightarrow (\mathbb{Z}/2\mathbb{Z})^6$. On en déduit donc qu'il n'y a pas de partie de torsion. D'autre part, comme $W_{\mathcal{C}_\eta} \to \mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5$ est surjective (prop. 1.3.3), on a $r \geq 9$. ∎

Remarque : Si $\mathcal{C}_\eta$ est la courbe de genre 3 générique, on obtient de même que $W_{\mathcal{C}_\eta} \cong \mathbb{Z}^r$ avec $9 \leq r \leq 23$. ∎

2.7 Appendice

Nous pouvons décrire plus précisément les valeurs de $t \in \mathbb{Q}(\sqrt{-3})$ hors desquelles la partie finie de W est $(\mathbb{Z}/3\mathbb{Z})^5$. En effet, pour que les points de Weierstrass qui engendrent W_1 soient $\mathbb{Q}(\sqrt{-3})$-rationnels, on effectue le changement de coordonnées $(x,y) \mapsto (2\,x, 2\,\sqrt[3]{2}\,y)$; l'équation de la courbe devient

$$y^3 = x\,(x-2)\left(x^2 - 27\,\frac{(t+1)^2\,t^2}{(t^2+t+1)^3}\,x + 27\,\frac{(t+1)^2\,t^2}{(t^2+t+1)^3}\right).$$

Pour que les points de Weierstrass qui engendrent W_2 soient définis, il faut rajouter deux racines cubiques, à savoir $\sqrt[3]{2\,t\,(t+1)}$ et $\sqrt[3]{2\,(t+2)\,(t-1)\,(2t+1)}$.

Soit alors $K = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{2\,t\,(t+1)}, \sqrt[3]{2\,(t+2)\,(t-1)\,(2t+1)})$. Considérons les images des points qui engendrent $J[\phi]$ par l'application $x - T$:

	$x-0$	$x-2$	$x-2\,t_1$	$x-2\,t_2$
$[(0,0)-P_\infty]$	2	2	4	4
$[(2,0)-P_\infty]$	2	2	4	4
$[(2\,t_1,0)-P_\infty]$	4	4	2	2

Si 2 n'est pas un cube dans K, le tableau nous montre que l'image est de dimension 1 en tant que $\mathbb{Z}/3\mathbb{Z}$-espace vectoriel. Et donc, $\dim J(K)[3] = 5$ d'après la proposition 2.4.7.

Lemme 2.7.1. *Il n'y a qu'un nombre fini de valeurs de $t \in \mathbb{Q}(\sqrt{-3})$ pour lesquelles 2 est un cube dans $K = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{2\,t\,(t+1)}, \sqrt[3]{2\,(t+2)\,(t-1)\,(2t+1)})$.*

DÉMONSTRATION : En effet, 2 est un cube dans K, si et seulement si on peut trouver $s \in \mathbb{Q}(\sqrt{-3})$ tel que $2\,s^3 = (2\,t\,(t+1))^a (2\,(t+2)\,(t-1)\,(2t+1))^b$. C'est l'équation affine d'une courbe $\mathcal{C}_{a,b}$. Et donc 2 est un cube dans K si et seulement si t est une coordonnée d'un point $\mathbb{Q}(\sqrt{-3})$-rationnel de la courbe $\mathcal{C}_{a,b}$. On sait que 2 n'est pas un cube dans $\mathbb{Q}(\sqrt{-3})$. Les courbes planes $\mathcal{C}_{1,1}$,

$\mathcal{C}_{2,1}$, $\mathcal{C}_{1,2}$, et $\mathcal{C}_{2,2}$ sont de genre 4 et n'ont donc qu'un nombre fini de points $\mathbb{Q}(\sqrt{-3})$-rationnels. D'autre part, La courbe $\mathcal{C}_{1,0}$ a pour équation affine $s^3 = t\,(t+1)$, et est isogène à la courbe elliptique $y^2 = x^3 + 1$. La courbe $\mathcal{C}_{0,1}$ a pour équation affine $s^3 = (t-1)\,(t+2)\,(2\,t+1)$, et est isogène à la courbe elliptique $y^2 = x^3 + 16$. La courbe $\mathcal{C}_{2,0}$ a pour équation affine $2\,s^3 = t\,(t+1)$, et est isogène à la courbe elliptique $y^2 = x^3 + 1/4$. La courbe $\mathcal{C}_{0,2}$ a pour équation affine $s^3 = 2\,(t-1)\,(t+2)\,(2\,t+1)$, et est isogène à la courbe elliptique $y^2 = x^3 + 1$. Toutes ces courbes elliptiques ont rang 0 sur $\mathbb{Q}$, sont isogènes à leur tordue par -3, et sont donc de rang 0 sur $\mathbb{Q}(\sqrt{-3})$. ∎

Pour déterminer les valeurs de t hors desquelles la partie infinie de W est $\mathbb{Z}^4$, il faudrait aussi considérer des points rationnels sur des courbes lisses.

Troisième partie

Etude de la famille de courbes lisses d'équation affine $y^4 = x(x-1)(x-t)$

Résumé

Nous déterminons, pour une famille de courbes lisses de genre 3, la structure du groupe engendré par les points de Weierstrass dans la jacobienne. Cela fournit un exemple où ce groupe est infini. Plus précisément, nous exhibons une famille où ce groupe est isomorphe à $\mathbb{Z}^9 \times (\mathbb{Z}/4\mathbb{Z})^2$ et en déduisons l'existence d'une famille où ce groupe est $\mathbb{Z}^r$ avec $11 \leq r \leq 23$.

Abstract

We describe the group generated by the Weierstrass points in the Jacobian, for a family of smooth curves of genus 3. This gives an example where this group is not finite. More precisely, we construct a family with a group isomorphic to $\mathbb{Z}^9 \times (\mathbb{Z}/4\mathbb{Z})^2$. Thus we can conclude that there exists a family whose group is $\mathbb{Z}^r$ with $11 \leq r \leq 23$.

3.1 Introduction

Soit $\mathcal{C}$ une courbe lisse projective de genre $g \geq 2$. Une telle courbe possède un ensemble de points canoniques : ses points de Weierstrass. Choisissons un de ces points ; cela définit un plongement de $\mathcal{C}$ dans sa jacobienne J. De plus, la structure du groupe $W = W_{\mathcal{C}}$ engendré par les points de Weierstrass dans la jacobienne ne dépend pas du point de Weierstrass choisi ; ce groupe est donc un invariant géométrique de la courbe digne d'intérêt. Nous allons analyser la structure du groupe W pour la famille de courbes donnée par l'équation affine $y^4 = x(x-1)(x-t)$ où $t \notin \{0,1\}$.

Nous verrons que lorsque $t \notin \{-1,2,1/2,(1 \pm i\sqrt{3})/2\}$, cette courbe admet seize automorphismes. Pour $t \in \{(1 \pm i\sqrt{3})/2\}$, c'est la courbe de Picard, et elle admet 48 automorphismes. Pour $t \in \{-1,2,1/2\}$, c'est la courbe de Fermat, et elle admet 96 automorphismes.

Pour ces deux courbes particulières, le groupe W engendré par les points de Weierstrass dans la jacobienne est décrit dans la littérature ; en effet, pour la courbe de Picard, on sait que $W = (\mathbb{Z}/4\,\mathbb{Z})^2 \times (\mathbb{Z}/3\,\mathbb{Z})^5$ ([KS]) et pour la courbe de Fermat, on sait que $W = (\mathbb{Z}/4\,\mathbb{Z})^5 \times (\mathbb{Z}/2\,\mathbb{Z})$ ([Roh]). Nous donnons une démonstration de ce résultat en appendice. Remarquons que les arguments de spécialisation décrits au paragraphe 1.3 permettent de montrer relativement facilement que W_η est de la forme $\mathbb{Z}^r \times (\mathbb{Z}/4\mathbb{Z})^2$, avec $r \geq 5$ (en effet, la partie de torsion de W s'injecte dans $(\mathbb{Z}/4\mathbb{Z})^5 \times \mathbb{Z}/2\mathbb{Z}$ et dans $(\mathbb{Z}/4\mathbb{Z})^2 \times (\mathbb{Z}/3\mathbb{Z})^5$, et contient de manière immédiate $(\mathbb{Z}/4\mathbb{Z})^2$ d'après le lemme 1.4.2).

Nous allons en fait déterminer le rang et plus précisément, montrer que

Théorème 3.1.1. *Soit $\mathcal{C}_t$ la courbe projective lisse birationnelle à la courbe affine $y^4 = x(x-1)(x-t)$ où $t \notin \{0,1\}$. Pour tout corps de nombres K, il existe un ensemble fini S_K tel que si $t \in K \setminus S_K$ alors $W_{\mathcal{C}_t} \cong \mathbb{Z}^9 \times (\mathbb{Z}/4\mathbb{Z})^2$. Par exemple, $t = 76834/39593$ n'appartient pas à S_K.*

En utilisant des arguments de spécialisation et le résultat de la partie II (donnant la structure du groupe engendré par les points de Weierstrass d'une courbe lisse d'équation affine $y^3 = x(x-1)(x^2-2\beta x+\beta)$) nous en tirerons :

Corollaire 3.1.2. *Soit une famille $\mathcal{C}$ de courbes lisses joignant une courbe $\mathcal{C}_0$ de la famille $y^3 = x(x-1)(x^2-2\beta x+\beta)$ pour laquelle $W_{\mathcal{C}_0} = \mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5$ à une courbe $\mathcal{C}_1$ de la forme $y^4 = x(x-1)(x-t)$ pour laquelle $W_{\mathcal{C}_1} = \mathbb{Z}^9 \times (\mathbb{Z}/4\mathbb{Z})^2$. Soit $W_{\mathcal{C}_\eta}$ le groupe engendré par les points de Weierstrass de la fibre générique, on a alors $W_{\mathcal{C}_\eta} \cong \mathbb{Z}^r$ avec $11 \leq r \leq 23$.*

Afin de démontrer le théorème 3.1.1, nous allons exhiber 11 points de Weierstrass $P_1, \ldots, P_{11}$ avec P_{10} et P_{11} d'ordre 4, tels que si l'on note Ψ l'application $(m_1, \ldots, m_{11}) \in \mathbb{Z}^9 \times (\mathbb{Z}/4\mathbb{Z})^2 \mapsto m_1P_1 + \ldots + m_{11}P_{11} \in W$, on obtient, en notant W_η le groupe engendré par les points de Weierstrass de la courbe générique, et W_s celui engendré par ceux de la courbe spéciale, des applications Ψ_η, Ψ_s telles que, si l'on note μ la spécialisation, le diagramme suivant soit commutatif :

$$\begin{array}{ccc} \mathbb{Z}^9 \times (\mathbb{Z}/4\mathbb{Z})^2 & \xrightarrow{\Psi_\eta} & W_\eta \\ & \searrow^{\Psi_s} & \downarrow \mu \\ & & W_s \end{array}$$

Puis, nous allons montrer que :

(i) μ est surjective (argument de spécialisation (proposition 1.3.3)).

(ii) Ψ_s et Ψ_η sont surjectives (proposition 3.4.2).

(iii) Ψ_s est un isomorphisme pour un s particulier (proposition 3.6.1).

Cela nous permettra de conclure que Ψ_η est un isomorphisme, qui ne dépend pas de la spécialisation. Puis, comme μ est un isomorphisme pour presque toute spécialisation en s (cela découle du théorème 1.3.5), cela nous permettra de conclure.

Remarque : Toute courbe de la forme $y^4 = P(x)$, avec P un polynôme de degré 3 ou 4 et de discriminant non-nul est birationnelle à une courbe de la forme $y^4 = x(x-1)(x-t)$. Géométriquement, cela correspond aux courbes

de genre 3 qui sont revêtement cyclique de degré 4 de la droite projective, avec 4 points totalement ramifiés. ∎

3.2 Détermination des points de Weierstrass

Considérons, pour $t \notin \{0,1\}$, la courbe lisse $\mathcal{C}_t$ d'équation affine

$$y^4 = x(x-1)(x-t).$$

Notons $f(x)$ le terme de droite. La courbe projective $Y^4 = Z^4 f(\frac{Y}{Z})$ admet un unique point à l'infini, noté P_∞ de coordonnées $(1:0:0)$, qui est lisse, et que l'on prend comme base du plongement dans la jacobienne.
Les points d'inflexion de cette courbe sont définis par l'annulation du hessien H, que nous allons calculer. L'équation de la courbe en coordonnées homogènes étant $Y^4 = X(X-Z)(X-tZ)Z$, il vient $H(X,Y,Z) = -36\,G(X,Z)Y^2$ où $G(X,Z) = 3\,X^4 - (4+4\,t)\,ZX^3 + (4+4\,t^2+2\,t)\,Z^2X^2 - (4\,t+4\,t^2)\,Z^3X + 3\,t^2Z^4$.

On dispose donc de la description suivante des points de Weierstrass ; ce sont d'une part les zéros de f, que l'on note P_0, P_1, P_t, le point à l'infini P_∞ et d'autre part les points ayant pour abscisse les zéros de g, où $g(x) = G(X/Z,1) = 3\,x^4 - 4\,(1+t)\,x^3 + 2\,(2\,t^2+t+2)\,x^2 - 4\,(t+1)\,tx + 3\,t^2$.

En posant $x' = x + t/x$, trouver les racines de g revient à résoudre $\widetilde{g}(x') = 3\,x'^2 - 4\,(1+t)\,x' + 4\,t^2 - 4\,t + 4 = 0$.
Les racines de $\widetilde{g}$ sont $\frac{2}{3}\left((1+t) \pm \sqrt{-(2\,t-1)\,(t-2)}\right)$.
Pour que $-(2\,t-1)\,(t-2)$ soit un carré, on paramètre par $t = \frac{u^2+2}{2u^2+1}$. Les racines de $\widetilde{g}$ sont alors $x'_1 = 2\,\frac{u^2+u+1}{2\,u^2+1}$ et $x'_2 = 2\,\frac{u^2-u+1}{2\,u^2+1}$.

Résolvons d'abord $x'_1 = x + t/x$.
Cela revient à résoudre $x^2\,(2\,u^2+1) + (-2\,u^2-2\,u-2)\,x + u^2 + 2 = 0$. Les racines sont

$$\frac{u^2+u+1 \pm \sqrt{-(u^2+1)\,(u-1)^2}}{2\,u^2+1}$$

or $-(u^2+1)\,(u-1)^2$ est un carré pour $u = \dfrac{2k}{k^2-1}$, soit pour $t = 2\,\dfrac{1+k^4}{k^4+6\,k^2+1}$.

Les racines de $x_1' = x + t/x$ sont alors

$$\begin{cases} x_{1,1} &= \dfrac{(1+i)\,(k^2-i)}{k^2+2\,i\,k+1} \\ \\ x_{2,1} &= \dfrac{(1-i)\,(k^2+i)}{k^2-2\,i\,k+1}. \end{cases}$$

Résolvons $x_2' = x + t/x$.
Cela revient à résoudre $x^2\,(2\,u^2+1) + (-2\,u^2-2+2\,u)x + u^2 + 2 = 0$.

Les racines sont

$$\frac{u^2+1-u \pm \sqrt{-\,(u^2+1)\,(u+1)^2}}{2\,u^2+1}$$

c'est-à-dire

$$\begin{cases} x_{3,1} &= \dfrac{(1-i\,)\,(k^2+i\,)}{k^2+2\,i\,k+1} \\ \\ x_{4,1} &= \dfrac{(1+i\,)\,(k^2-i\,)}{k^2-2\,i\,k+1}. \end{cases}$$

On en déduit les ordonnées des points de Weierstrass. Notons:

$$\begin{cases} y_{1,1} &= \dfrac{\sqrt{(1-i)\,(k^2-i)\,(k^2-2\,ik+1)\,(k^2-2\,k-1)\,\sqrt{k^4+6\,k^2+1}}}{(k^2+2\,ik+1)\,(k^2-2\,ik+1)} \\ \\ y_{2,1} &= \dfrac{\sqrt{(1+i)\,(k^2+i)\,(k^2+2\,ik+1)\,(k^2-2\,k-1)\,\sqrt{k^4+6\,k^2+1}}}{(k^2+2\,ik+1)\,(k^2-2\,ik+1)} \\ \\ y_{3,1} &= \dfrac{\sqrt{(1+i)\,(k^2+2\,k-1)\,(k^2+i)\,(k^2-2\,ik+1)\,\sqrt{k^4+6\,k^2+1}}}{(k^2+2\,ik+1)\,(k^2-2\,ik+1)} \\ \\ y_{4,1} &= \dfrac{\sqrt{(1-i)\,(k^2-i)\,(k^2+2\,ik+1)\,(k^2+2\,k-1)\,\sqrt{k^4+6\,k^2+1}}}{(k^2+2\,ik+1)\,(k^2-2\,ik+1)}. \end{cases}$$

Les points de Weierstrass d'ordonnée non nulle sont donc les points de coordonnées $(x_{j,1},y_{j,1}i^{\alpha})$ avec $\alpha \in \{0,1,2,3\}$.

D'après les calculs, on voit tout de suite que pour $t = 1/2$ ou $t = 2$, $\widetilde{g}$ admet une racine double. D'autre part, pour $t = -1$, $g(x)$ devient $3\,(x^2+1)^2$, auquel cas les abscisses des points de Weierstrass sont $\pm i$. Dans ces trois cas (qui correspondent à la courbe de Fermat), il y a donc 12 points de Weierstrass. Un calcul direct montre que ce sont les seules valeurs de t pour lesquelles g admet des racines doubles. Il y a donc, de manière générale 20 points de Weierstrass.

Dans le cas général, les points d'ordonnée non nulle sont de poids 1, et les points de Weierstrass d'ordonnée nulle sont de poids 2. Pour la courbe de Fermat, tous les points de Weierstrass sont de poids 2.

Pour que les points de Weierstrass soient définis sur un corps plus petit, on effectue le changement de coordonnées $(x,y) \mapsto (x(k^4+6\,k^2+1),y(k^4+6\,k^2+1)^{3/4})$, l'équation de la courbe devient $y^4 = x(x-a)(x-b)$, où $a = 2(1+k^4)$ et $b = k^4+6\,k^2+1$.

Notons $x_1 = (1+i)(k^2-i)(k^2-2ik+1)$, $x_2 = (1-i)(k^2+i)(k^2+2ik+1)$, $x_3 = (1-i)(k^2+i)(k^2-2ik+1)$, $x_4 = (1+i)(k^2-i)(k^2+2ik+1)$,
$y_1 = \sqrt{(1-i)(k^2-i)(k^2-2ik+1)(k^2-2k-1)}$,
$y_2 = \sqrt{(1+i)(k^2+i)(k^2+2ik+1)(k^2-2k-1)}$,
$y_3 = \sqrt{(1+i)(k^2+i)(k^2-2ik+1)(k^2+2k-1)}$,
$y_4 = \sqrt{(1-i)(k^2-i)(k^2+2ik+1)(k^2+2k-1)}$.

Notons $P_{m,n}$ le point de Weierstrass de coordonnées affines $(x_m,y_n\,i^{n-1})$ pour $1 \leq m \leq 4$ et $1 \leq n \leq 4$.

3.3 Géométrie de la courbe et de la jacobienne

Nous déterminons le groupe des automorphismes de la courbe et la structure de la jacobienne.

3.3.1 Automorphismes de $\mathcal{C}$

Cette courbe admet de manière générale 16 automorphismes ([KY]). Lorsque $t \notin \{-1,2,1/2,(1\pm i\sqrt{3})/2\}$, le groupe des automorphismes est engendré par:

$$\begin{cases} [i] : & (x,y) \mapsto & (x,iy) \\ \sigma : & (x,y) \mapsto & \left(\dfrac{t}{x}, \dfrac{\sqrt{t}y}{x}\right) \\ \tau : & (x,y) \mapsto & \left(\dfrac{x-t}{x-1}, -\dfrac{\sqrt{t-1}y}{x-1}\right). \end{cases}$$

En effet, les automorphismes permutent les points de Weierstrass et l'image d'un point de Weierstrass de poids 2 est un point de Weierstrass de poids 2. Une quartique plane lisse est une courbe canonique, donc un automorphisme peut être représenté par ${}^t(X,Y,Z) \mapsto M\,{}^t(X,Y,Z)$ avec $M \in PGL(2)$. Le fait que $\mathcal{C}$ doit être préservée par cet automorphisme entraîne des conditions sur les coefficients de M. Puis, comme les points P_0, P_1, P_t et P_∞ sont permutés par l'action de cet automorphisme, il y a 24 cas à considérer. Un calcul direct montre que seulement quatre de ces permutations conviennent. D'autre part, comme les quatre points P_0, P_1, P_t et P_∞ sont fixés par l'action de $\langle[i]\rangle$, chaque permutation correspond à quatre automorphismes de la courbe. Cela entraîne qu'il y a en tout seize automorphismes.

Remarque : Lorsque $t = \frac{1\pm i\sqrt{3}}{2}$, cette courbe admet 48 automorphismes. Lorsque $t \in \{-1,2,1/2\}$, elle en admet 96. ∎

Dorénavant, nous considérerons la courbe $\mathcal{C}'$ d'équation $y^4 = x(x-a)(x-b)$, où $a = 2(1+k^4)$ et $b = k^4 + 6\,k^2 + 1$.

Sur la courbe d'équation $y^4 = x(x-a)(x-b)$, le groupe des automorphismes est engendré par

$$\begin{cases} [i] : & (x,y) \mapsto & (x,iy) \\ \sigma : & (x,y) \mapsto & \left(\dfrac{ab}{x}, \dfrac{\sqrt{ab}y}{x}\right) \\ \tau : & (x,y) \mapsto & \left(\dfrac{b(x-a)}{x-b}, -\dfrac{\sqrt{b}\sqrt{b-a}y}{x-b}\right). \end{cases}$$

3.3.2 Structure de la jacobienne de $\mathcal{C}'$

Le quotient de $\mathcal{C}'$ par le groupe engendré par l'un des automorphisme $[i]^2 = [-1]$, σ ou τ est une courbe elliptique. Nous les noterons $\mathcal{E}_1 = \mathcal{C}'/\langle[-1]\rangle$, $\mathcal{E}_2 = \mathcal{C}'/\langle\sigma\rangle$ et $\mathcal{E}_3 = \mathcal{C}'/\langle\tau\rangle$.

Proposition 3.3.1. *La jacobienne est isogène au produit des trois courbes elliptiques $\mathcal{E}_1 \times \mathcal{E}_2 \times \mathcal{E}_3$. De plus, les $\mathcal{E}_i$ sont les courbes elliptiques d'équations respectives:*
$\mathcal{E}_1 : y^2 = x(x-a)(x-b)$, $\mathcal{E}_2 : y^2 = x^3 + 16(a+b+2\sqrt{ab})x$, $\mathcal{E}_3 : y^2 = x^3 + 16(a-2b-2\sqrt{b}\sqrt{b-a})x$.

DÉMONSTRATION : Comme nous allons le voir par la suite (au paragraphe 3.5), les courbes $\mathcal{E}_i$ sont birationnelles aux courbes $\mathcal{D}_i$ définies comme suit :
La courbe $\mathcal{D}_1$ est la courbe $\mathcal{E}_1$.
La courbe $\mathcal{D}_2$ a pour équation $v^2 = -\left(4\,b + 4\,a + 8\,\sqrt{ab}\right)u^4 + 1$.
La courbe $\mathcal{D}_3$ a pour équation $v^2 = \left(-4\,a + 8\,\sqrt{b}\sqrt{b-a} + 8\,b\right)u^4 + 1$. Notons φ_i les morphismes de $\mathcal{C}'$ dans $\mathcal{D}_i$ (donnés explicitement au paragraphe 3.5)
Si ω_i est une forme différentielle sur $\mathcal{D}_i$, on vérifie que $\varphi_1^*(\omega_1)$, $\varphi_2^*(\omega_2)$ et $\varphi_3^*(\omega_3)$ sont des formes différentielles sur $\mathcal{C}'$ qui sont indépendantes.
Une forme différentielle sur $\mathcal{D}_1$ est $\omega_1 = dx/y$ et donc $\varphi_1^*(\omega_1) = dx/y^2$.
Une forme différentielle sur $\mathcal{D}_2$ est $\omega_2 = du/v$ et donc
$\varphi_2^*(\omega_2) = d\left(\frac{y}{x+\sqrt{ab}}\right) \Big/ \left(-\frac{-x^2+2\sqrt{ab}x-ab+2\,xb+2\,ax}{\left(x+\sqrt{ab}\right)^2}\right) = 4\,\frac{(-x+\sqrt{a}\sqrt{b})}{y^3}dx.$
Une forme différentielle sur $\mathcal{D}_3$ est $\omega_3 = du/v$ et donc
$\varphi_3^*(\omega_3) = d\left(-\frac{y}{-x+b+\sqrt{b}\sqrt{b-a}}\right) \Big/ \left(\frac{x^2-2\,ax+2\,x\sqrt{b-a}\sqrt{b}+2\,xb+ab-2\,b^2-2\,b^{3/2}\sqrt{b-a}}{\left(-x+b+\sqrt{b}\sqrt{b-a}\right)^2}\right) =$
$-4\,\frac{\left(x-b+\sqrt{b}\sqrt{b-a}\right)}{y^3}dx.$
Une base des formes différentielles sur $\mathcal{C}'$ étant donnée par $\frac{dx}{y^3}$, $\frac{xdx}{y^3}$ et $\frac{ydx}{y^3}$, on vérifie que la matrice des $\varphi_i^*(\omega_i)$ a un déterminant non nul. ∎

3.4 Etude géométrique des points de Weierstrass

Notons j le plongement dans la jacobienne $P \mapsto [P - P_\infty]$. Si L est une forme linéaire, notons $\mathrm{div}\,(L)$ le diviseur de L. On a

- $\mathrm{div}\,(X - x_m\,Z) = P_{m,1} + P_{m,2} + P_{m,3} + P_{m,4}$

- $\text{div}\,(Y) = P_0 + P_a + P_b + P_\infty$
- $\text{div}\,(X) = 4P_0$
- $\text{div}\,(X - a) = 4P_a$
- $\text{div}\,(X - b) = 4P_b$.

En effet, le quatrième point d'intersection de la tangente en P_0 (resp. P_a, resp. P_b) avec la courbe est P_0 (resp. P_a, resp. P_b).

Notation: Rappelons que par abus de notation, nous identifions un point de Weierstrass et son image dans la jacobienne.

On a donc déjà certaines relations entre ces points de Weierstrass, à savoir

- $P_{m,1} + P_{m,2} + P_{m,3} + P_{m,4} = 0 \quad \text{pour} \quad 1 \leq m \leq 4$
- $P_0 + P_a + P_b = 0$
- $4P_0 = 4P_a = 4P_b = 0$.

3.4.1 Image par le premier automorphisme

Nous avons une application de $\mathcal{C}'$ vers la courbe elliptique $\mathcal{E}_1$ d'équation affine $u^2 = v(v-a)(v-b)$, donnée par $(x,y) \overset{\varphi_1}{\mapsto} (x,y^2)$. Notons $Q_{m,n}$ l'image du point de Weierstrass $P_{m,n}$ par φ_1, notons Q_m l'image de P_m pour $m \in \{0,a,b\}$ et $\mathcal{O}$ l'élément neutre de la loi de groupe. Les points d'ordre 2 sont Q_0, Q_a, et Q_b. Un calcul direct fournit alors les relations suivantes entre ces points sur la courbe elliptique $\mathcal{E}_1$:

- $Q_{1,1} + Q_0 = Q_{2,1}$
- $Q_{1,1} + Q_b = Q_{4,2}$
- $Q_{1,1} + Q_a = Q_{3,2}$
- $Q_{j,1} + Q_{j,2} = \mathcal{O}$
- $Q_0 + Q_a = Q_b$.

Tous les points s'obtiennent donc à partir de $Q_{1,1}$, de Q_0 et de Q_a.

Si D est le diviseur d'une fonction rationnelle f sur $\mathcal{E}_1$, alors $\phi_1^*(D)$ est le diviseur d'une fonction rationnelle sur $\mathcal{C}'$. Or on sait que sur une courbe elliptique, $D = \sum n_j P_j$ est le diviseur d'une fonction si et seulement si $\sum n_j = 0$ et $\sum [n_j] P_j = \mathcal{O}$. En appliquant cela aux diviseurs $Q_{1,1} + Q_0 - Q_{2,1} - \mathcal{O}$, $Q_{1,1} + Q_b - Q_{4,2} - \mathcal{O}$, $Q_{1,1} + Q_a - Q_{3,2} - \mathcal{O}$, on obtient le résultat suivant :

Lemme 3.4.1. *Les relations suivantes sont vérifiées dans la jacobienne de $\mathcal{C}$:*

- $P_{1,1} + P_{1,3} + P_{2,2} + P_{2,4} + 2P_0 = 0$

- $P_{1,1} + P_{1,3} + P_{3,1} + P_{3,3} + 2P_a = 0$
- $P_{1,1} + P_{1,3} + P_{4,1} + P_{4,3} + 2P_b = 0.$

Remarque : Ce résultat aurait pu être obtenu de manière plus géométrique. En effet, dans chacun des trois cas, on peut trouver une conique passant par $2P_\infty$ et les cinq autres points.

La conique d'équation affine $y^2 + (k^2 - 2ik + 1)x = 2\,(k^2 + i)(k^2 - i)(k^2 - 2\,ik + 1)$ intersecte $\mathcal{C}'$ en $\{P_{1,1},P_{1,3},P_{3,1},P_{3,3},P_a,P_\infty\}$, et a multiplicité d'intersection 2 en P_a et P_∞.

La conique d'équation affine $2(i-k^2)x+(-1+i)y^2+2(k^2-2ik+1)(k^2+2ik+1)(k^2-i) = 0$ intersecte $\mathcal{C}'$ en $\{P_{1,1},P_{1,3},P_{4,1},P_{4,3},P_b,P_\infty\}$, et a multiplicité d'intersection 2 en P_b et P_∞.

La conique d'équation affine $i(k^2 - 2k - 1)x + y^2 = 0$ intersecte $\mathcal{C}'$ en $\{P_{1,1},P_{1,3},P_{2,2},P_{2,4},P_0,P_\infty\}$, et a multiplicité d'intersection 2 en P_0 et P_∞. ∎

Cela nous permet de voir que W est engendré par $P_{1,1}$, $P_{1,2}$, $P_{1,3}$, $P_{2,1}$, $P_{2,2}$, $P_{3,1}$, $P_{3,2}$, $P_{4,1}$, $P_{4,2}$, P_0 et P_a, les deux derniers points étant d'ordre 4.
On a donc prouvé que:

Proposition 3.4.2. *W est un quotient de $\mathbb{Z}^9 \times (\mathbb{Z}/4\mathbb{Z})^2$.*

En fait, plus précisément, nous avons obtenu une application :

$$\begin{array}{ccc} \mathbb{Z}^9 \times (\mathbb{Z}/4\mathbb{Z})^2 & \xrightarrow{\Psi_t} & W_{\mathcal{C}_t} \\ (m_1,\ldots,m_9)(n_1,n_2) & \longmapsto & m_1P_{1,1} + m_2P_{1,2} + m_3P_{1,3} + m_4P_{2,1} + m_5P_{2,2} + \\ & & m_6P_{3,1} + m_7P_{3,2} + m_8P_{4,1} + m_9P_{4,2} + n_1P_0 + n_2P_1 \end{array}$$

qui est surjective.
Nous allons montrer qu'en général, il n'y a pas d'autres relations entre ces points, et donc, que $W \cong \mathbb{Z}^9 \times (\mathbb{Z}/4\,\mathbb{Z})^2$.

3.5 Etude des facteurs de la jacobienne

3.5.1 Facteur $\mathcal{E}_2$

Considérons l'automorphisme σ. En identifiant un point et son image par σ, on obtient une application de $\mathcal{C}'$ vers la courbe elliptique $\mathcal{E}_2 = \mathcal{C}'/\langle\sigma\rangle$.

Proposition 3.5.1. *Le morphisme ϕ_2 de degré 2 de $\mathcal{C}'$ vers la courbe ellip-*

tique $\mathcal{E}_2 = \mathcal{C}'/\langle\sigma\rangle$ *peut être décrit par*

$$(x,y) \mapsto \left(4\,\frac{y^2}{x}, 8\,\frac{y\left(x + \sqrt{2(1+k^4)(k^4+6\,k^2+1)}\right)}{x} \right)$$

en écrivant $\mathcal{E}_2$ *sous la forme*

$$y^2 = x^3 + 16(3k^4 + 6k^2 + 3 + 2\sqrt{2(1+k^4)(k^4+6k^2+1)})x.$$

DÉMONSTRATION : Rappelons que l'automorphisme σ est donné par

$$(x,y) \mapsto (ab/x, \sqrt{ab}y/x).$$

Soit (x,y) est un point de $\mathcal{C}'$, posons

$$X_1 = x + \frac{ab}{x} \quad \text{et} \quad Y_1 = y + \frac{\sqrt{ab}}{x}y$$

on a alors $Y_1^4 = (X_1 + 2\sqrt{ab})^2(X_1 - a - b)$.
En remplaçant Y_1 par $Y_2 = \dfrac{Y_1}{(X_1 + 2\sqrt{ab})}$, X_1 devient solution d'un polynôme de degré 2, à savoir

$$(X + 2\sqrt{ab})^2 {Y_2}^4 - (X - a - b) = a_2X^2 + a_1X + a_0.$$

En prenant le discriminant Δ en X, il vient que $X_2 = (2a_2X_1 + a_1)$ satisfait $X_2^2 = \Delta$.

On a donc une application φ_2 de $\mathcal{C}'$ dans la courbe $\mathcal{D}_2$ d'équation

$$v^2 = -\left(4\,b + 4\,a + 8\,\sqrt{ab}\right) u^4 + 1$$

donnée par $(x,y) \mapsto (u,v)$ où

$$u = \frac{y}{x + \sqrt{ab}} \quad \text{et} \quad v = -\frac{-x^2 + 2\,\sqrt{ab}x - ab + 2\,xb + 2\,ax}{\left(x + \sqrt{ab}\right)^2}.$$

Cette courbe elliptique est birationnelle à la courbe $\mathcal{E}_2$ d'équation

$$y^2 = x^3 + \left(16\,b + 16\,a + 32\,\sqrt{ab}\right) x$$

et le morphisme de $\mathcal{C}'$ vers $\mathcal{E}_2$ est donné (voir annexe) par

$$\phi_2 : (x,y) \mapsto \left(4\,\frac{y^2}{x}, 8\,\frac{y\left(x+\sqrt{ab}\right)}{x} \right).$$

En remplaçant a et b par leur valeur en fonction de k, on obtient le résultat escompté. ∎

Nous pouvons décrire l'action de σ sur les points de Weierstrass. On a $\sigma(P_{1,1}) = P_{2,4}$, $\sigma(P_{1,2}) = P_{2,1}$, $\sigma(P_{1,3}) = P_{2,2}$, $\sigma(P_{1,4}) = P_{2,3}$, $\sigma(P_{3,1}) = P_{4,2}$, $\sigma(P_{3,2}) = P_{4,3}$, $\sigma(P_{3,3}) = P_{4,4}$, $\sigma(P_{3,4}) = P_{4,1}$. D'autre part $\sigma(P_0) = P_\infty$ et $\sigma(P_a) = P_b$.

Nous noterons $Q_{m,n}$ l'image du point $P_{m,n}$ sur la courbe elliptique $\mathcal{E}_2$. Ainsi, nous avons les points $Q_{1,1}$, $Q_{1,2}$, $Q_{1,3} = -Q_{1,1}$, $Q_{1,4} = -Q_{1,2}$, $Q_{3,1}$, $Q_{3,2}$, $Q_{3,3} = -Q_{3,1}$, $Q_{3,4} = -Q_{3,2}$, Q_0 et $\mathcal{O}$, l'élément neutre de la loi de groupe.

Remarque : Si $\phi_2(x,y)$ est le point de coordonnées (x_0,y_0) sur la courbe elliptique $\mathcal{E}_2$, $\phi_2(x,-y)$ est son inverse pour la loi de groupe et $\phi_2(x,iy)$ est le point de coordonnées $(-x_0,iy_0)$, donc dès lors que l'image d'un point est définie sur un corps de nombres K contenant i, les images des autres points de Weierstrass de même abscisse sont définies sur le même corps de nombres K. ∎

La courbe elliptique $\mathcal{E}_2$ est isomorphe par $\psi : (x,y) \mapsto (xy_1^2, yy_1^3)$ à la courbe elliptique $\mathcal{E}_2'$ d'équation $y^2 = x^3 + 16((1-i)(k^2-i)(k^2-2ik+1)(k^2-2k-1))^2\,(3k^4+6k^2+3+2\sqrt{2(1+k^4)(k^4+6k^2+1)})x$.

Les images par $\psi \circ \phi_2$ des points de Weierstrass sont définies sur

$K = \mathbb{Q}(i, \sqrt{2(1+k^4)(-k^4+6k^2-1)}, \sqrt{2(1+k^4)(k^4+6k^2+1)})$.

Par abus de notation, nous noterons encore $Q_{1,1} = \psi \circ \phi_2(x_1,y_1)$, $Q_{1,2} = \psi \circ \phi_2(x_1,iy_1)$, $Q_{3,1} = \psi \circ \phi_2(x_2,y_2)$, $Q_{3,2} = \psi \circ \phi_2(x_2,iy_2)$ les images des points de Weierstrass sur la courbe elliptique $\mathcal{E}_2'$.

3.5.2 Facteur $\mathcal{E}_3$

Considérons l'automorphisme τ. En identifiant un point et son image par τ, on obtient une application de $\mathcal{C}'$ vers la courbe elliptique $\mathcal{E}_3 = \mathcal{C}'/\langle\tau\rangle$.

Proposition 3.5.2.
Le morphisme ϕ_3 de degré 2 de $\mathcal{C}'$ vers la courbe elliptique $\mathcal{E}_3 = \mathcal{C}'/\langle\tau\rangle$ peut

être décrit par

$$(x,y) \mapsto \left(4\frac{y^2}{x-(k^4+6k^2+1)}, 8\frac{y(x-(k^4+6k^2+1)-\sqrt{-k^8+34k^4-1})}{x-(k^4+6k^2+1)}\right)$$

en écrivant $\mathcal{E}_3$ sous la forme

$$y^2 = x^3 - 16\,(12k^2+2\,\sqrt{(k^4+6k^2+1)(-k^4+6k^2-1)})x.$$

DÉMONSTRATION : Rappelons que l'automorphisme τ est donné par

$$(x,y) \mapsto \left(\frac{b\,(x-a)}{x-b}, -\frac{\sqrt{b}\sqrt{b-a}y}{x-b}\right).$$

Soit (x,y) est un point de $\mathcal{C}'$, posons

$$X_1 = x + \frac{b\,(x-a)}{x-b} \quad \text{et} \quad Y_1 = y - \frac{\sqrt{b}\sqrt{b-a}}{x-b}y$$

on a alors $Y_1^4 = (X_1 - 2b - 2\sqrt{b}\sqrt{b-a})^2(X_1 - a)$.
En remplaçant Y_1 par $Y_2 = \dfrac{Y_1}{(X_1 - 2b - 2\sqrt{b}\sqrt{b-a})}$, X_1 devient racine d'un polynôme de degré 2, à savoir

$$(X - 2b - 2\sqrt{b}\sqrt{b-a})^2 Y_2^4 - (X-a) = a_2X^2 + a_1X + a_0.$$

En prenant le discriminant Δ en X, il vient que $X_2 = (2a_2X_1 + a_1)$ satisfait $X_2^2 = \Delta$.

On a donc une application φ_3 de $\mathcal{C}'$ vers la courbe elliptique $\mathcal{D}_3$ d'équation

$$v^2 = \left(-4\,a + 8\,\sqrt{b}\sqrt{b-a} + 8\,b\right)u^4 + 1$$

donnée par $(x,y) \mapsto (u,v)$ où

$$u = -\frac{y}{-x+b+\sqrt{b}\sqrt{b-a}} \quad \text{et}$$

$$v = \frac{x^2 + 2(-a+\sqrt{b-a}\sqrt{b}+b)\,x + ab - 2\,b^2 - 2\,b^{3/2}\sqrt{b-a}}{\left(-x+b+\sqrt{b}\sqrt{b-a}\right)^2}.$$

Cette courbe elliptique est birationnelle à la courbe $\mathcal{E}_3$ d'équation

$$y^2 = x^3 + 16(a - 2b - 2\sqrt{b}\sqrt{b-a})x$$

et le morphisme de $\mathcal{C}'$ vers $\mathcal{E}_3$ est donné (voir annexe) par

$$\phi_3 : (x,y) \mapsto (4\frac{y^2}{x-b},\ 8\ \frac{y(x-b-\sqrt{b}\sqrt{b-a})}{x-b}).$$

En remplaçant a et b par leur valeur en fonction de k, on obtient le résultat escompté. ∎

L'action de τ sur les points de Weierstrass est donnée par : $\tau(P_{1,1}) = P_{4,3}$, $\tau(P_{1,2}) = P_{4,4}$, $\tau(P_{1,3}) = P_{4,1}$, $\tau(P_{1,4}) = P_{4,2}$, $\tau(P_{2,1}) = P_{3,1}$, $\tau(P_{2,2}) = P_{3,2}$, $\tau(P_{2,3}) = P_{3,3}$, $\tau(P_{2,4}) = P_{3,4}$. D'autre part $\tau(P_b) = P_\infty$ et $\tau(P_a) = P_0$.

Nous noterons $Q_{m,n}$ l'image du point $P_{m,n}$ sur la courbe elliptique $\mathcal{E}_3$. Ainsi, nous avons les points $Q_{1,1}$, $Q_{1,2}$, $Q_{1,3} = -Q_{1,1}$, $Q_{1,4} = -Q_{1,2}$, $Q_{2,1}$, $Q_{2,2}$, $Q_{2,3} = -Q_{2,1}$, $Q_{2,4} = -Q_{2,2}$, Q_0 et $\mathcal{O}$, l'élément neutre de la loi de groupe.

Remarque : Si $\phi_3(x,y)$ est le point de coordonnées (x_0,y_0) sur la courbe elliptique $\mathcal{E}_3$, $\phi_3(x,-y)$ est son inverse pour la loi de groupe et $\phi_3(x,iy)$ est le point de coordonnées $(-x_0,iy_0)$, donc dès lors que l'image d'un point est définie sur un corps de nombres K contenant i, les images des autres points de Weierstrass de même abscisse sont définies sur le même corps de nombres K. ∎

La courbe elliptique $\mathcal{E}_3$ est isomorphe par $\psi : (x,y) \mapsto (xy_1^2, yy_1^3)$ à la courbe elliptique $\mathcal{E}_3'$ d'équation $y^2 = x^3 - 16((1-i)(k^2-i)(k^2-2ik+1)(k^2-2k-1))^2\,(12k^2 + 2\sqrt{(k^4+6k^2+1)(-k^4+6k^2-1)})x$.
Les images par $\psi \circ \phi_3$ des points de Weierstrass sont alors définies sur $K = \mathbb{Q}(i,\ \sqrt{(k^4+6k^2+1)(-k^4+6k^2-1)}, \sqrt{2(1+k^4)(k^4+6k^2+1)})$.
Par abus de notation, nous noterons encore $Q_{1,1} = \psi \circ \phi_3(x_1,y_1)$, $Q_{2,1} = \psi \circ \phi_3(x_2,y_2)$, $Q_{1,2} = \psi \circ \phi_3(x_1,iy_1)$, $Q_{2,2} = \psi \circ \phi_3(x_2,iy_2)$ les images des points de Weierstrass d'abscisse non nulle sur la courbe elliptique $\mathcal{E}_3'$.

3.6 Spécialisation en $k = 14$

Nous allons montrer que pour certaines valeurs de t, les relations obtenues entre les points de Weierstrass au paragraphe 3.4 sont les seules qui existent, plus précisément, nous allons montrer le résultat suivant :

Proposition 3.6.1. *Pour $t_0 = 76834/39593$, le groupe engendré par les points de Weierstrass est $W_{\mathcal{C}_{t_0}} = \mathbb{Z}^9 \times (\mathbb{Z}/4\mathbb{Z})^2$.*

Cette valeur de t_0 correspond à $k = 14$ et $t_0 = 2\,\frac{1+k^4}{k^4+6\,k^2+1}$.
Le corps de définition des points de Weierstrass est $\mathbb{Q}(i,\sqrt{5494133 - 7392923i}$, $\sqrt{5494133 - 7392923i},\sqrt{9796613 + 7436827i},\sqrt{9796613 - 7436827i})$.
Nous obtenons immédiatement le corollaire suivant :

Corollaire 3.6.2. *Soit $W_{\mathcal{C}_\eta}$ le groupe engendré par les points de Weierstrass de la courbe générique, on a $W_{\mathcal{C}_\eta} \cong \mathbb{Z}^9 \times (\mathbb{Z}/4\mathbb{Z})^2$.*

DÉMONSTRATION : Comme $W_{\mathcal{C}_\eta}$ est un quotient de $\mathbb{Z}^9 \times (\mathbb{Z}/4\mathbb{Z})^2$ (d'après la proposition 3.4.2), et comme $W_{\mathcal{C}_{t_0}}$ est un quotient de $W_{\mathcal{C}_\eta}$ (d'après la proposition 3.6.1), on en déduit que $W_{\mathcal{C}_\eta} \cong \mathbb{Z}^9 \times (\mathbb{Z}/4\mathbb{Z})^2$. ∎

Pour effectuer tous les calculs, nous avons utilisé maple d'une part, et gp-pari d'autre part.
Pour montrer que l'application Ψ_{t_0} est injective, nous allons regarder les images des points sur chacun des facteurs de la jacobienne. Les informations que nous en tirerons nous permettront de conclure.
Nous voulons montrer que certains points de l'une des courbes elliptiques $\mathcal{E}_1$, $\mathcal{E}_2$ ou $\mathcal{E}_3$ (qui correspondent aux images de points de Weierstrass) sont $\mathbb{Z}$-indépendants. Pour ce faire, nous allons regarder les images de ces points lorsque l'on réduit modulo $\mathfrak{p}$ pour une place $\mathfrak{p}$ de K au dessus de p totalement décomposé dans K. Plus précisément, nous allons utiliser le lemme suivant suggéré par Jean-François Mestre :

Lemme 3.6.3. *Soient $P_1,\ldots,P_r$ des points K-rationnels sur une variété abélienne $\mathcal{A}$ tels qu'il existe des premiers de K de bonne réduction $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$ et un nombre premier l tels que*

- *Les $\widetilde{P_i}$ sont d'ordre l modulo $\mathfrak{p}_j$.*
- *Il existe $a_{i,j}$ tels que $\widetilde{P_j} = a_{i,j}\widetilde{P_1} \bmod \mathfrak{p}_i$ et que la matrice formée par les $a_{i,j}$ a un déterminant non nul modulo l.*
- *$\mathcal{A}[l](K) = \{\mathcal{O}\}$.*

alors, les points $P_1,\ldots,P_r$ sont $\mathbb{Z}$-indépendants.

DÉMONSTRATION : En effet, supposons que l'on ait une relation entre ces points $m_1P_1 + \ldots + m_rP_r = 0$ que l'on choisit minimale, à savoir que si $h \neq 1$ divise tous les m_i, le point $(m_1/h)P_1 + \ldots + (m_r/h)P_r$ est un point non-nul de la variété abélienne. Lorsqu'on réduit modulo $\mathfrak{p}_{i,}$ cette relation devient, compte-tenu des hypothèses, $(m_1a_{i,1} + \ldots + m_ra_{i,r})\widetilde{P_1} = 0$. Comme $\widetilde{P_1}$ est d'ordre l, on a donc $m_1a_{i,1} + \ldots + m_ra_{i,r} \equiv 0 \bmod l$. La non-nullité

du déterminant modulo l entraîne que les m_i sont des multiples de l et donc, qu'il existe un point K-rationnel d'ordre l, ce qui est exclu. ∎

3.6.1 Sur la courbe elliptique $\mathcal{E}_1$

Lorsqu'on spécialise en $k = 14$, les points ont pour coordonnées

$Q_{1,1} = (44269 + 32899i, 5494133 - 7392923i)$, $Q_{2,1} = (44269 - 32899i, 5494133 + 7392923i)$, $Q_{3,1} = (33349 - 43931i, 9796613 + 7436827i)$ et $Q_{4,1} = (33349 + 43931i, 9796613 - 7436827i)$.

Comme 5, 13 et 37 sont totalement décomposés dans $\mathbb{Q}(i)$, on peut calculer $\#\widetilde{\mathcal{E}_1}(\mathbb{F}_5) = 8$, $\#\widetilde{\mathcal{E}_1}(\mathbb{F}_{13}) = 8$ et $\#\widetilde{\mathcal{E}_1}(\mathbb{F}_{37}) = 28$. Ainsi, $\#\mathcal{E}_1(\mathbb{Q}(i))_{\text{tors}}$ est de cardinal 4 ou 8. Cela montre que $Q_{1,1}$ est d'ordre infini (car on vérifie aisément qu'il n'est ni d'ordre 2, ni d'ordre 4).

3.6.2 Sur la courbe elliptique $\mathcal{E}_2$

Nous effectuons tous les calculs sur la courbe elliptique $\mathcal{E}'_2$, courbe pour laquelle le corps de définition des images des points de Weierstrass est plus petit. Lorsqu'on spécialise en $k = 14$, la courbe elliptique $\mathcal{E}'_2$ a pour équation $y^2 = x^3 + (-24469813062240 - 81235404441518i)(1862832 + 544\sqrt{10526258})x$ et les points ont pour coordonnées

$Q_{1,1} = (-4938472564 - 3670080844i, (-2151282717480 - 1169457388952i)(458813 + 454155i + 197\sqrt{10526258} + 28i\sqrt{10526258})/2329)$ et $Q_{3,1} = (6594487316 + 4900766636i, (1945758190216 - 586103306880i)\sqrt{2861374994}(458813 - 454155i + 197\sqrt{10526258} + 28i\sqrt{10526258})/89473193)$.

En utilisant la remarque au paragraphe 3.5.1, nous obtenons les coordonnées des points $Q_{1,2}$ et $Q_{3,2}$. Les points $Q_{1,1}$, $Q_{1,2}$, $Q_{3,1}$ et $Q_{3,2}$ sont définis sur le corps de nombres $K = \mathbb{Q}(i, \sqrt{10526258}, \sqrt{2861374994})$.

Lemme 3.6.4. *Sur la courbe elliptique $\mathcal{E}'_2$, les points $Q_{1,1}$, $Q_{1,2}$, $Q_{3,1}$ et $Q_{3,2}$ sont d'ordre infini et $\mathbb{Z}$-indépendants.*

DÉMONSTRATION : Comme 97 et 157 sont totalement décomposés dans K, et comme $\#\widetilde{\mathcal{E}'_2}(\mathbb{F}_{97}) = 2.53$ et $\#\widetilde{\mathcal{E}'_2}(\mathbb{F}_{157}) = 2.73$, cela permet de conclure que le seul point K-rationnel d'ordre fini est le point (0,0).
Les points $Q_{1,1}$, $Q_{1,2}$, $Q_{3,1}$ et $Q_{3,2}$ sont donc d'ordre infini. Nous voulons montrer qu'ils sont $\mathbb{Z}$-indépendants. Pour ce faire, nous allons appliquer le lemme 3.6.3 avec $\mathcal{A} = \mathcal{E}'_2$, $P_1 = 1300\,Q_{1,1}$, $P_2 = 1300\,Q_{1,2}$, $P_3 = 1300\,Q_{3,1}$,

$P_4 = 1300\,Q_{3,2}$, $K = \mathbb{Q}(i,\sqrt{10526258},\sqrt{2861374994})$, $\mathfrak{p}_i$ des places de K au dessus de 1237, 1549, 3061 et de 3109 et enfin avec $l = 61$.

$p = 1237$

Choisissons 546 comme racine carrée de -1 modulo 1237, 1212 comme racine carrée de 10526258 modulo 1237 et 385 comme racine carrée de 2861374994 modulo 1237.
La courbe elliptique réduite $\widetilde{\mathcal{E}'}_2$ a pour équation $y^2 = x^3 + 226x$.
On a $\#\widetilde{\mathcal{E}'_2}(\mathbb{F}_{1237}) = 2^2.5.61$ et les points satisfont :
$\widetilde{Q}'_{1,1} = 1300\,\widetilde{Q}_{1,1} = (738,1092)$ est d'ordre 61,
$\widetilde{Q}'_{1,2} = 1300\,\widetilde{Q}_{1,2} = (499,1235) = 50\,\widetilde{Q}'_{1,1}$,
$\widetilde{Q}'_{3,1} = 1300\,\widetilde{Q}_{3,1} = (79,555) = 39\,\widetilde{Q}'_{1,1}$,
$\widetilde{Q}'_{3,2} = 1300\,\widetilde{Q}_{3,2} = (1158,1202) = 59\,\widetilde{Q}'_{1,1}$.

$p = 1549$

Choisissons 88 comme racine carrée de -1 modulo 1549, 809 comme racine carrée de 10526258 modulo 1549 et 1319 comme racine carrée de 2861374994 modulo 1549.
La courbe elliptique réduite $\widetilde{\mathcal{E}'}_2$ a pour équation $y^2 = x^3 + 82x$.
On a $\#\widetilde{\mathcal{E}'_2}(\mathbb{F}_{1549}) = 2.13.61$ et les points satisfont :
$\widetilde{Q}'_{1,1} = 1300\,\widetilde{Q}_{1,1} = (417,1300)$ est d'ordre 61,
$\widetilde{Q}'_{1,2} = 1300\,\widetilde{Q}_{1,2} = (1132,1323) = 11\,\widetilde{Q}'_{1,1}$,
$\widetilde{Q}'_{3,1} = 1300\,\widetilde{Q}_{3,1} = (240,580) = 44\,\widetilde{Q}'_{1,1}$,
$\widetilde{Q}'_{3,2} = 1300\,\widetilde{Q}_{3,2} = (1309,1472) = 57\,\widetilde{Q}'_{1,1}$.

$p = 3061$

Choisissons 2560 comme racine carrée de -1 modulo 3061, 1074 comme racine carrée de 10526258 modulo 3061 et 408 comme racine carrée de 2861374994 modulo 3061.
La courbe elliptique réduite $\widetilde{\mathcal{E}'}_2$ a pour équation $y^2 = x^3 + 1800x$.
On a $\#\widetilde{\mathcal{E}'_2}(\mathbb{F}_{3061}) = 2.5^2.61$. Et donc on a :
$\widetilde{Q}'_{1,1} = 1300\,\widetilde{Q}_{1,1} = (2415,2612)$ est d'ordre 61,
$\widetilde{Q}'_{1,2} = 1300\,\widetilde{Q}_{1,2} = (646,1496) = 50\,\widetilde{Q}'_{1,1}$,
$\widetilde{Q}'_{3,1} = 1300\,\widetilde{Q}_{3,1} = (140,92) = 47\,\widetilde{Q}'_{1,1}$,
$\widetilde{Q}'_{3,2} = 1300\,\widetilde{Q}_{3,2} = (2921,2884) = 32\,\widetilde{Q}'_{1,1}$.

$p = 3109$

Choisissons 727 comme racine carrée de -1 modulo 3109, 2910 comme

racine carrée de 10526258 modulo 3109 et 1350 comme racine carrée de 2861374994 modulo 3109.
La courbe elliptique réduite $\widetilde{\mathcal{E}'}_2$ a pour équation $y^2 = x^3 + 2134x$.
On a $\#\widetilde{\mathcal{E}'}_2(\mathbb{F}_{3109}) = 2.5^2.61$. Et donc on a :
$\widetilde{Q}'_{1,1} = 1300\,\widetilde{Q}_{1,1} = (2600,1278)$ est d'ordre 61,
$\widetilde{Q}'_{1,2} = 1300\,\widetilde{Q}_{1,2} = (509,2624) = 11\,\widetilde{Q}'_{1,1}$,
$\widetilde{Q}'_{3,1} = 1300\,\widetilde{Q}_{3,1} = (2734,2317) = 29\,\widetilde{Q}'_{1,1}$,
$\widetilde{Q}'_{3,2} = 1300\,\widetilde{Q}_{3,2} = (375,2490) = 14\,\widetilde{Q}'_{1,1}$.

La matrice $\begin{pmatrix} 1 & 50 & 39 & 59 \\ 1 & 11 & 44 & 57 \\ 1 & 50 & 47 & 32 \\ 1 & 11 & 29 & 14 \end{pmatrix}$ a pour déterminant 3.7.13.107, qui est non nul modulo 61. Comme le seul point d'ordre fini de $\mathcal{E}'_2$ est (0,0), on conclut que les points $Q_{1,1}$, $Q_{1,2}$, $Q_{3,1}$ et $Q_{3,2}$ sont des points $\mathbb{Z}$-indépendants de $\widetilde{\mathcal{E}'}_2$. ∎

3.6.3 Sur la courbe elliptique $\mathcal{E}_3$

Nous effectuons tous les calculs sur la courbe elliptique $\mathcal{E}'_3$, courbe pour laquelle le corps de définition des images des points de Weierstrass est plus petit. Lorsqu'on spécialise en $k = 14$, la courbe elliptique $\mathcal{E}'_3$ a pour équation $y^2 = x^3 + (-24469813062240 - 81235404441518i)(-37632 - 544i\sqrt{5102017})x$ et les points ont pour coordonnées
$Q_{1,1} = (-10095856744 + 1540199584i, (3891516380432 - 1172206613760i)(-388943i + 197i\sqrt{5102017} - 28\sqrt{5102017})/2329)$ et $Q_{2,1} = (1437103136 + 10111047064i, \sqrt{10526258}(-59143384 - 43953064i)(388943i + 197i\sqrt{5102017} + 28\sqrt{5102017})/137)$.

En utilisant la remarque au paragraphe 3.5.2, nous obtenons les coordonnées des points $Q_{1,2}$ et $Q_{2,2}$. Les points $Q_{1,1}$, $Q_{1,2}$, $Q_{2,1}$ et $Q_{2,2}$ sont définis sur le corps $K = \mathbb{Q}(i, \sqrt{10526258}, \sqrt{5102017})$.
Remarque : Nous obtenons le même corps qu'au paragraphe précédent. De plus, les deux courbes elliptiques $\mathcal{E}'_2$ et $\mathcal{E}'_3$ sont K-isomorphes. ∎

Lemme 3.6.5. *Sur la courbe elliptique $\mathcal{E}'_3$, les points $Q_{1,1}$, $Q_{1,2}$, $Q_{2,1}$ et $Q_{2,2}$ sont d'ordre infini et $\mathbb{Z}$-indépendants.*

DÉMONSTRATION : Comme 97 et 157 sont totalement décomposés dans K, et comme $\#\widetilde{\mathcal{E}'}_3(\mathbb{F}_{97}) = 2.53$ et $\#\widetilde{\mathcal{E}'}_3(\mathbb{F}_{157}) = 2.73$, cela permet de conclure

que le seul point K-rationnel d'ordre fini est le point (0,0). Les points $Q_{1,1}$, $Q_{1,2}$, $Q_{2,1}$ et $Q_{2,2}$ sont donc d'ordre infini. Nous allons montrer que ces quatre points sont $\mathbb{Z}$-indépendants. Pour ce faire, nous allons regarder les images de ces points lorsque l'on réduit modulo $\mathfrak{p}$ pour une place $\mathfrak{p}$ de K au dessus de p totalement décomposé dans K.

Nous allons appliquer le lemme 3.6.3 avec $\mathcal{A} = \mathcal{E}'_3$, $P_1 = 1300\,Q_{1,1}$, $P_2 = 1300\,Q_{1,2}$, $P_3 = 1300\,Q_{2,1}$, $P_4 = 1300\,Q_{2,2}$, $K = \mathbb{Q}(i,\sqrt{10526258},\sqrt{5102017})$, $\mathfrak{p}_i$ des places de K au dessus de 1237, 1549, 3061 et de 3109 et enfin avec $l = 61$.

$p = 1237$

Choisissons 546 comme racine carrée de -1 modulo 1237, 1212 comme racine carrée de 10526258 modulo 1237 et 859 comme racine carrée de 5102017 modulo 1237.
La courbe elliptique réduite $\widetilde{\mathcal{E}}'_3$ a pour équation $y^2 = x^3 + 1172x$
On a $\#\widetilde{\mathcal{E}}'_3(\mathbb{F}_{1237}) = 2^2.5.61$ et les points satisfont :
$\widetilde{Q}'_{1,1} = 1300\,\widetilde{Q}_{1,1} = (986,1030)$ est d'ordre 61,
$\widetilde{Q}'_{1,2} = 1300\,\widetilde{Q}_{1,2} = (251,782) = 50\,\widetilde{Q}'_{1,1}$,
$\widetilde{Q}'_{2,1} = 1300\,\widetilde{Q}_{2,1} = (750,869) = 37\,\widetilde{Q}'_{1,1}$,
$\widetilde{Q}'_{2,2} = 1300\,\widetilde{Q}_{2,2} = (487,703) = 20\,\widetilde{Q}'_{1,1}$.

$p = 1549$

Choisissons 88 comme racine carrée de -1 modulo 1549, 809 comme racine carrée de 10526258 modulo 1549 et 1152 comme racine carrée de 5102017 modulo 1549.
La courbe elliptique réduite $\widetilde{\mathcal{E}}'_3$ a pour équation $y^2 = x^3 + 1152x$.
On a $\#\widetilde{\mathcal{E}}'_3(\mathbb{F}_{1549}) = 2.13.61$. Et donc on a :
$\widetilde{Q}'_{1,1} = 1300\,\widetilde{Q}_{1,1} = (729,177)$ est d'ordre 61,
$\widetilde{Q}'_{1,2} = 1300\,\widetilde{Q}_{1,2} = (820,86) = 11\,\widetilde{Q}'_{1,1}$,
$\widetilde{Q}'_{2,1} = 1300\,\widetilde{Q}_{2,1} = (1164,1484) = 31\,\widetilde{Q}'_{1,1}$,
$\widetilde{Q}'_{2,2} = 1300\,\widetilde{Q}_{2,2} = (385,476) = 36\,\widetilde{Q}'_{1,1}$.

$p = 3061$

Choisissons 2560 comme racine carrée de -1 modulo 3061, 1074 comme racine carrée de 10526258 modulo 3061 et 1745 comme racine carrée de 5102017 modulo 3061.
La courbe elliptique réduite $\widetilde{\mathcal{E}}'_3$ a pour équation $y^2 = x^3 + 1580x$.

On a $\#\widetilde{\mathcal{E}}'_3(\mathbb{F}_{3061}) = 2.5^2.61$. Et donc on a :
$\widetilde{Q}'_{1,1} = 1300\,\widetilde{Q}_{1,1} = (2415{,}783)$ est d'ordre 61,
$\widetilde{Q}'_{1,2} = 1300\,\widetilde{Q}_{1,2} = (646{,}2586) = 50\,\widetilde{Q}'_{1,1}$,
$\widetilde{Q}'_{2,1} = 1300\,\widetilde{Q}_{2,1} = (2316{,}1193) = 6\,\widetilde{Q}'_{1,1}$,
$\widetilde{Q}'_{2,2} = 1300\,\widetilde{Q}_{2,2} = (745{,}2263) = 56\,\widetilde{Q}'_{1,1}$.

$p = 3109$

Choisissons 727 comme racine carrée de -1 modulo 3109, 2910 comme racine carrée de 10526258 modulo 3109 et 961 comme racine carrée de 5102017 modulo 3109.
La courbe elliptique réduite $\widetilde{\mathcal{E}}'_3$ a pour équation $y^2 = x^3 + 1734x$.
On a $\#\widetilde{\mathcal{E}}'_3(\mathbb{F}_{3109}) = 2.5^2.61$ et les points satisfont :
$\widetilde{Q}'_{1,1} = 1300\,\widetilde{Q}_{1,1} = (853{,}5)$ est d'ordre 61,
$\widetilde{Q}'_{1,2} = 1300\,\widetilde{Q}_{1,2} = (2256{,}526) = 11\,\widetilde{Q}'_{1,1}$,
$\widetilde{Q}'_{2,1} = 1300\,\widetilde{Q}_{2,1} = (2515{,}1481) = 8\,\widetilde{Q}'_{1,1}$,
$\widetilde{Q}'_{2,2} = 1300\,\widetilde{Q}_{2,2} = (594{,}973) = 27\,\widetilde{Q}'_{1,1}$.

La matrice $\begin{pmatrix} 1 & 50 & 37 & 20 \\ 1 & 11 & 31 & 36 \\ 1 & 50 & 6 & 56 \\ 1 & 11 & 8 & 27 \end{pmatrix}$ a pour déterminant $-3^4.13.41$ qui est non nul modulo 61. Comme le seul point d'ordre fini de $\mathcal{E}'_3$ est (0,0), on conclut que les points $Q_{1,1}$, $Q_{1,2}$, $Q_{2,1}$ et $Q_{2,2}$ sont des points $\mathbb{Z}$-indépendants de $\widetilde{\mathcal{E}}'_3$. ∎

Remarque : Notons $P^{(2)}$ un point de $\mathcal{E}'_2$ et $P^{(3)}$ un point de $\mathcal{E}'_3$.
Comme les deux courbes $\mathcal{E}'_2$ et $\mathcal{E}'_3$ sont K-isomorphes, il est naturel de se demander ce qu'il advient du groupe engendré par les quatre points $Q^{(3)}_{1,1}$, $Q^{(3)}_{1,2}$, $Q^{(3)}_{2,1}$ et $Q^{(3)}_{2,2}$ par cet isomorphisme. On peut montrer en réduisant modulo 6221, 6421, 12101 et 20333 et en appliquant le lemme 3.6.3, que le groupe engendré par ces 8 points est de rang 8, et donc $\mathcal{E}'_2$ est de rang au moins 8 sur K. En effet, l'isomorphisme ξ de $\mathcal{E}'_3$ vers $\mathcal{E}'_2$ est donné par $(x,y) \mapsto (x\lambda^2, y\lambda^3)$ avec $\lambda = \dfrac{1-i}{2} + \dfrac{-(i+1)\sqrt{2861374994} + 17\,(1-i)\sqrt{10526258}}{153668}$.

En appliquant le lemme 3.6.3 avec $\mathfrak{p}_i$ des premiers au dessus de 1237, 1549, 3061, 3109, 6221, 6421, 12101 et 20333, les points $Q^{(2)}_{1,1}$, $Q^{(2)}_{1,2}$, $Q^{(2)}_{3,1}$, $Q^{(2)}_{3,2}$, $\xi(Q^{(3)}_{1,1})$, $\xi(Q^{(3)}_{1,2})$, $\xi(Q^{(3)}_{2,1})$ et $\xi(Q^{(3)}_{2,2})$ avec $l = 61$,

on obtient alors la matrice suivante $\begin{pmatrix} 1 & 50 & 39 & 59 & 41 & 37 & 53 & 27 \\ 1 & 11 & 44 & 57 & 16 & 54 & 8 & 27 \\ 1 & 50 & 47 & 32 & 55 & 5 & 25 & 30 \\ 1 & 11 & 29 & 14 & 60 & 50 & 53 & 34 \\ 1 & 50 & 21 & 13 & 43 & 15 & 48 & 21 \\ 1 & 11 & 30 & 25 & 35 & 19 & 46 & 18 \\ 1 & 11 & 31 & 36 & 43 & 46 & 19 & 26 \\ 1 & 50 & 42 & 26 & 22 & 2 & 29 & 47 \end{pmatrix}$ qui a pour déterminant $-2^2.3^2.5^2.13.29.59.3847$, qui est non-nul modulo 61. ∎

3.6.4 Preuve de la proposition 3.6.1

Notons dorénavant pour $1 \leq l \leq 3$ $P^{(l)}$ un point de la courbe elliptique $\mathcal{E}_l$.
Pour $k = 14$, supposons que l'on ait une relation entre les points de Weierstrass $P_{1,1}$, $P_{1,2}$, $P_{1,3}$, $P_{2,1}$, $P_{2,2}$, $P_{3,1}$, $P_{3,2}$, $P_{4,1}$ et $P_{4,2}$. Nous allons montrer que c'est la relation triviale. Comme ces points sont tous d'ordre infini, cela suffira pour montrer que le groupe engendré par ces neuf points, P_0 et P_a est $\mathbb{Z}^9 \times (\mathbb{Z}/4\mathbb{Z})^2$. Supposons donc que l'on ait $m_1P_{1,1} + m_2P_{1,2} + m_3P_{1,3} + m_4P_{2,1} + m_5P_{2,2} + m_6P_{3,1} + m_7P_{3,2} + m_8P_{4,1} + m_9P_{4,2} = 0$ dans la jacobienne. On regarde les images de cette relation sur les diverses courbes elliptiques.

Regardons l'image sur $\mathcal{E}_1$:
Cette relation se traduit par $m_1Q_{1,1}^{(1)} + m_2Q_{1,2}^{(1)} + m_3Q_{1,3}^{(1)} + m_4Q_{2,1}^{(1)} + m_5Q_{2,2}^{(1)} + m_6Q_{3,1}^{(1)} + m_7Q_{3,2}^{(1)} + m_8Q_{4,1}^{(1)} + m_9Q_{4,2}^{(1)} = \mathcal{O}^{(1)}$ avec des notations évidentes. Ce qui se traduit par $(m_1 + m_3 - m_2)Q_{1,1}^{(1)} + (m_4 - m_5)(Q_{1,1}^{(1)} + Q_0^{(1)}) + (m_7 - m_6)(Q_{1,1}^{(1)} + Q_a^{(1)}) + (m_9 - m_8)(Q_{1,1}^{(1)} + Q_b^{(1)}) = \mathcal{O}^{(1)}$. Comme $Q_{1,1}^{(1)}$ est d'ordre infini (d'après ce qu'on a vu au paragraphe 3.6.1), cela entraîne que $m_1 + m_3 - m_2 + m_4 - m_5 + m_7 - m_6 + m_9 - m_8 = 0$ et que $m_4 - m_5 + m_9 - m_8$ et $m_7 - m_6 + m_9 - m_8$ sont pairs.

Regardons l'image sur $\mathcal{E}_2$:
Cette relation se traduit par $m_1Q_{1,1}^{(2)} + m_2Q_{1,2}^{(2)} + m_3Q_{1,3}^{(2)} + m_4Q_{2,1}^{(2)} + m_5Q_{2,2}^{(2)} + m_6Q_{3,1}^{(2)} + m_7Q_{3,2}^{(2)} + m_8Q_{4,1}^{(2)} + m_9Q_{4,2}^{(2)} = \mathcal{O}^{(2)}$ avec des notations évidentes. Or d'après ce qu'on a vu, les points $P_{1,j}$ et $P_{2,j-1}$ ont même image par ϕ_2. De même, les points $P_{3,j}$ et $P_{4,j+1}$ ont même image. Cela revient à dire que $(m_1 - m_3 - m_5)Q_{1,1}^{(2)} + (m_2 + m_4)Q_{1,2}^{(2)} + (m_6 + m_9)Q_{3,1}^{(2)} + (m_7 - m_8)Q_{3,2}^{(2)} = \mathcal{O}^{(2)}$ sur la courbe elliptique $\mathcal{E}_2$. Comme on sait que ces quatre points sont

indépendants, on en déduit que les coefficients satisfont les relations $m_1 = m_3 + m_5$, $m_2 = -m_4$, $m_6 = -m_9$ et $m_7 = m_8$.

Regardons l'image sur $\mathcal{E}_3$:
Cette relation se traduit par $m_1 Q_{1,1}^{(3)} + m_2 Q_{1,2}^{(3)} + m_3 Q_{1,3}^{(3)} + m_4 Q_{2,1}^{(3)} + m_5 Q_{2,2}^{(3)} + m_6 Q_{3,1}^{(3)} + m_7 Q_{3,2}^{(3)} + m_8 Q_{4,1}^{(3)} + m_9 Q_{4,2}^{(3)} = \mathcal{O}^{(3)}$ avec des notations évidentes. Or d'après ce qu'on a vu, les points $P_{1,j}$ et $P_{4,j+2}$ ont même image par ϕ_3. De même, les points $P_{2,j}$ et $P_{3,j}$ ont même image. Cela revient à dire que $(m_1 - m_3 - m_8)Q_{1,1}^{(3)} + (m_2 - m_9)Q_{1,2}^{(3)} + (m_4 + m_6)Q_{2,1}^{(3)} + (m_5 + m_7)Q_{2,2}^{(3)} = \mathcal{O}^{(3)}$ sur la courbe elliptique $\mathcal{E}_3$. Comme on sait que ces quatre points sont indépendants, on en déduit que les coefficients satisfont les relations $m_1 = m_3 + m_8$, $m_2 = m_9$, $m_7 = -m_5$ et $m_6 = -m_4$.

Ces relations entraînent d'une part que $m_2 = m_9 = m_6 = m_4 = 0$, d'autre part que $m_7 = m_8 = m_5 = 0$ et finalement que $m_1 = m_3 = 0$.

Cela permet de conclure que pour $k = 14$, *i.e.* pour la courbe d'équation $y^4 = x(x-76834)(x-39593)$, le groupe engendré par les points de Weierstrass est $\mathbb{Z}^9 \times (\mathbb{Z}/4\mathbb{Z})^2$.

3.7 Conséquences

3.7.1 Preuve du théorème 3.1.1

Pour déduire la structure de $W_{\mathcal{C}_t}$ dans le cas général, nous avons besoin d'appliquer un théorème de spécialisation dû à Silverman ([Sil1]), dont nous redonnons l'énoncé.

Théorème 1.3.5 *Soit $A \to C$ une famille (plate) de variétés abéliennes toutes définies sur un corps global K, où C est une courbe projective lisse. En un point $t \in C(\overline{K})$ pour lequel la fibre A_t est non singulière, on définit l'application de spécialisation $\sigma_t : A(C) \to A_t(\overline{K}), \quad P \mapsto P_t$.*

Si A n'a pas de partie constante, alors l'ensemble $\{t \in C(\overline{K}) \mid \sigma_t$ n'est pas injective $\}$ est un ensemble de hauteur bornée dans $C(\overline{K})$.

En particulier, lorsque K est un corps de nombres et $d \geq 1$ est un entier, alors σ_t est injective pour presque tout $t \in \bigcup_{[L:K] \leq d} C(L)$.

Nous allons appliquer ce théorème avec $A = \mathrm{Jac}(\mathcal{C}_t)$, $C = \mathbb{P}^1$ (ici, paramétrée par t). Nous devons donc vérifier qu'il n'y a pas de partie constante.

Notons J_t la jacobienne de $\mathcal{C}_t$. Supposons que $J/\mathbb{Q}(t)$ ait une partie constante A_0, variété abélienne de dimension 1, 2 ou 3. Il existe alors un morphisme de $J/\mathbb{Q}(t)$ dans A_0, et donc un morphisme $\mathcal{C}/\mathbb{Q}(t) \stackrel{\phi_t}{\to} A_0$, où ϕ_t est défini sur $\mathbb{Q}(t)$. Soit $\mathcal{S}$ la surface algébrique définie par cette famille de courbes. Elle est birationnelle à la surface $\{(x,y,t) \in \mathbb{A}^3 \mid y^4 - x(x-1)(x-t) = 0\}$, et donc birationnelle à $\mathbb{P}^2$.
On a une application non constante $\mathcal{S} \cdots\!\!\longrightarrow A_0$. On en déduit une application non constante $\mathbb{P}^2 \cdots\!\!\longrightarrow A_0$, ce qui n'est pas possible.

Comme le groupe engendré par les points de Weierstrass de la fibre générique $W_{\mathcal{C}_\eta}$ est isomorphe à $\mathbb{Z}^9 \times (\mathbb{Z}/4\mathbb{Z})^2$ (d'après le corollaire 3.6.2), on en déduit que pour presque tout t, $W_{\mathcal{C}_t} = \mathbb{Z}^9 \times (\mathbb{Z}/4\mathbb{Z})^2$.

3.7.2 Preuve du corollaire 3.1.2

Nous avons montré dans la partie II le résultat suivant :

Théorème 3.7.1. *Soit $\mathcal{C}_\beta$ la courbe projective lisse birationnelle à la courbe affine $y^3 = x(x-1)(x^2 - 2\beta x + \beta)$ où $\beta \notin \{0,1,1/2\}$. Pour tout corps de nombres K, il existe un ensemble fini S_K tel que si $\beta \in K \setminus S_K$ alors $W_{\mathcal{C}_\beta} \cong \mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5$. Par exemple, $\beta = 784/6859$ n'appartient pas à S_K.*

Ce théorème et le théorème 3.1.1 entraînent le corollaire 3.1.2, dont nous rappelons l'énoncé :

Corollaire 3.1.2 *Soit une famille $\mathcal{C}$ de courbes lisses joignant une courbe $\mathcal{C}_0$ de la famille $y^3 = x(x-1)(x^2 - 2\beta x + \beta)$ pour laquelle $W_{\mathcal{C}_0} = \mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5$ à une courbe $\mathcal{C}_1$ de la forme $y^4 = x(x-1)(x-t)$ pour laquelle $W_{\mathcal{C}_1} = \mathbb{Z}^9 \times (\mathbb{Z}/4\mathbb{Z})^2$. Soit $W_{\mathcal{C}_\eta}$ le groupe engendré par les points de Weierstrass de la fibre générique, on a alors $W_{\mathcal{C}_\eta} \cong \mathbb{Z}^r$ avec $11 \leq r \leq 23$.*

DÉMONSTRATION : En effet, la spécialisation $W_{\mathcal{C}_\eta} \to W_s$ étant injective sur la partie de torsion, si $W_{\mathcal{C}_\eta} = \mathbb{Z}^r \times G$, où G est un groupe fini, on a pour un s correspondant à la courbe $\mathcal{C}_1$, $G \hookrightarrow (\mathbb{Z}/4\mathbb{Z})^2$, et pour un s correspondant à la courbe $\mathcal{C}_0$, $G \hookrightarrow (\mathbb{Z}/3\mathbb{Z})^5$. On en déduit donc qu'il n'y a pas de partie de torsion. D'autre part, comme $W_{\mathcal{C}_\eta} \to \mathbb{Z}^9 \times (\mathbb{Z}/4\mathbb{Z})^2$ est surjective (prop. 1.3.3), on a $r \geq 11$. ∎

Remarque : Si $\mathcal{C}_\eta$ est la courbe de genre 3 générique, on obtient de même que $W_{\mathcal{C}_\eta} \cong \mathbb{Z}^r$ avec $11 \leq r \leq 23$. ∎

3.8 Appendice : cas où $t = -1$

Dorénavant, nous supposerons que $t = -1$. La courbe $\mathcal{C}_{-1}$ est la courbe de Fermat. Elle admet 96 automorphismes.

Nous montrons comment retrouver le résultat de Rohrlich([Roh]), à savoir que $W_{\mathcal{C}_{-1}} = (\mathbb{Z}/4\mathbb{Z})^5 \times (\mathbb{Z}/2\mathbb{Z})^2$.

Dans ce cas, il y a 12 points de Weierstrass, tous de poids 2. Lorsque $k = i$, les coordonnées des points de Weierstrass deviennent, en posant $x_1 = i$, $y_1 = -\sqrt{i-1}$, $x_3 = -i$ et $y_3 = -\sqrt{i+1}$: $P_{m,n} = (x_m, y_m i^{n-1})$ pour $m \in \{1,3\}$ et $1 \leq n \leq 4$.
Les points de Weierstrass d'ordonnées 0 sont P_0, P_1, P_{-1} et P_∞.
On vérifie aisément que le quatrième point d'intersection de la tangente en chacun de ces points avec la courbe est lui-même. Cela entraîne que nous avons déjà les relations suivantes dans la jacobienne de $\mathcal{C}_{-1}$:

- $P_{1,1} + P_{1,2} + P_{1,3} + P_{1,4} = 0$
- $P_{3,1} + P_{3,2} + P_{3,3} + P_{3,4} = 0$
- $P_0 + P_1 + P_{-1} + P_\infty = 0$
- $4P_{1,1} = 4P_{1,2} = 4P_{1,3} = 4P_{1,4} = 0$
- $4P_{3,1} = 4P_{3,2} = 4P_{3,3} = 4P_{3,4} = 0$
- $4P_0 = 4P_1 = 4P_{-1} = 4P_\infty = 0$.

La jacobienne est isogène au produit de trois courbes elliptiques $\mathcal{E}_1 \times \mathcal{E}_2 \times \mathcal{E}_3$.

3.8.1 Image sur la première courbe elliptique

La courbe elliptique $\mathcal{E}_1$ a pour équation $y^2 = x(x-1)(x+1)$.
On a un morphisme de degré 2 $\phi_1 : (x,y) \mapsto (x,y^2)$ de $\mathcal{C}$ dans $\mathcal{E}_1$. Notons $Q_{1,1} = \phi_1(P_{1,1}) = \phi_1(P_{1,3})$, $Q_{1,2} = \phi_1(P_{1,2}) = \phi_1(P_{1,4})$, $Q_{3,1} = \phi_1(P_{3,1}) = \phi_1(P_{3,3})$, $Q_{3,2} = \phi_1(P_{3,2}) = \phi_1(P_{3,4})$, $Q_0 = \phi_1(P_0)$, $Q_1 = \phi_1(P_1)$, $Q_{-1} = \phi_1(P_{-1})$ et $\mathcal{O} = \phi_1(P_\infty)$, l'élément neutre de la loi de groupe.
Sur la courbe elliptique $\mathcal{E}_1$, les points d'ordre 2 sont Q_0, Q_1 et Q_{-1} ; on a les relations suivantes entre les points: $Q_0 = 2Q_{1,1}$, $Q_{1,2} = -Q_{1,1}$, $4Q_{1,1} = \mathcal{O}$, $Q_{3,1} = Q_{1,1} + Q_1$, $Q_{3,2} = -Q_{1,1} + Q_1$.
Si D est le diviseur d'une fonction rationnelle f sur $\mathcal{E}_1$, alors $\phi_1^*(D)$ est le diviseur d'une fonction rationnelle sur $\mathcal{C}$. Or on sait que sur une courbe elliptique, $D = \sum n_j P_j$ est le diviseur d'une fonction si et seulement si $\sum n_j = 0$ et $\sum [n_j] P_j = \mathcal{O}$.

Cela nous donne, comme nouvelles relations dans la jacobienne :

- $P_{1,1} + P_{1,3} = P_{3,1} + P_{3,3} + 2P_1$
- $2P_{1,1} + 2P_{1,3} = 2P_0$.

3.8.2 Image sur la deuxième courbe elliptique

Le deuxième automorphisme de la courbe σ est donné par $(x,y) \mapsto (-1/x, iy/x)$.
La courbe elliptique $\mathcal{E}_2$ a pour équation $y^2 = x^3 + 32ix$.
On a un morphisme de degré 2 de $\mathcal{C}$ dans $\mathcal{E}_2$ donné par

$$\phi_2 : (x,y) \mapsto (4y^2/x, 8y(x+i)/x).$$

Notons $Q_{1,1} = \phi_2(P_{1,1})$, $Q_{1,2} = \phi_2(P_{1,2})$, $Q_{1,3} = \phi_2(P_{1,3})$, $Q_{1,4} = \phi_2(P_{1,4})$, $Q_{3,1} = \phi_2(P_{3,1}) = \phi_2(P_{3,3})$, $Q_{3,2} = \phi_2(P_{3,2}) = \phi_2(P_{3,4})$, $Q_0 = \phi_2(P_1) = \phi_2(P_{-1})$, et $\mathcal{O} = \phi_2(P_\infty) = \phi_2(P_0)$, l'élément neutre de la loi de groupe.
Sur la courbe elliptique $\mathcal{E}_2$, les points d'ordre 2 sont Q_0, $Q_{3,1}$ et $Q_{3,2}$; on a les relations suivantes entre les points: $Q_0 = 2Q_{1,1}$, $Q_{1,3} = -Q_{1,1}$, $4Q_{1,1} = \mathcal{O}$, $Q_{3,1} + Q_{1,1} = Q_{1,2}$, $Q_{3,1} + 2Q_{1,1} = Q_{3,2}$, $Q_{1,4} = -Q_{1,2}$.
Si D est le diviseur d'une fonction rationnelle f sur $\mathcal{E}_2$, alors $\phi_2^*(D)$ est le diviseur d'une fonction rationnelle sur $\mathcal{C}$. Or on sait que sur une courbe elliptique, $D = \sum n_j P_j$ est le diviseur d'une fonction si et seulement si $\sum n_j = 0$ et $\sum [n_j] P_j = \mathcal{O}$.

Cela nous donne, comme nouvelle relation dans la jacobienne :

- $P_{3,1} + P_{3,3} + 2P_{1,1} = 2P_{1,2} + P_0$.

3.8.3 Image sur la troisième courbe elliptique

Le troisième automorphisme de la courbe τ est donné par $(x,y) \mapsto ((x+1)/(x-1), \sqrt{2}y/(x-1))$.
La courbe elliptique $\mathcal{E}_3$ a pour équation $y^2 = x^3 + 16(2\sqrt{2} - 3)x$.
On a un morphisme de degré 2 $\phi_3 : (x,y) \mapsto (4y^2/(x-1), 8(x - 1 + \sqrt{2})y/(x-1))$ de $\mathcal{C}$ dans $\mathcal{E}_3$. Notons $Q_{1,1} = \phi_3(P_{1,1}) = \phi_3(P_{3,2})$ $Q_{1,3} = \phi_3(P_{1,3}) = \phi_3(P_{3,4})$, $Q_{3,1} = \phi_3(P_{3,1}) = \phi_3(P_{1,4})$, $Q_{3,3} = \phi_3(P_{3,3}) = \phi_3(P_{1,2})$, $Q_0 = \phi_3(P_0) = \phi_3(P_{-1})$, et $\mathcal{O} = \phi_3(P_\infty) = \phi_3(P_1)$, l'élément neutre de la loi de groupe.
Sur la courbe elliptique $\mathcal{E}_3$, les points d'ordre 2 sont Q_0, $Q_\alpha = (-4 + 4\sqrt{2}, 0)$ et $Q_\beta = (4 - 4\sqrt{2}, 0)$; on a les relations suivantes entre les points: $Q_\alpha = 2Q_{1,1} = 2Q_{1,3}$, $Q_\beta = 2Q_{3,1} = 2Q_{3,3}$, $4Q_{1,1} = \mathcal{O}$, $Q_{1,3} = -Q_{1,1}$, $Q_{3,3} = -Q_{3,1}$, $Q_\alpha + Q_\beta = Q_0 = 2Q_{1,1} + 2Q_{3,1}$.
Si D est le diviseur d'une fonction rationnelle f sur $\mathcal{E}_3$, alors $\phi_3^*(D)$ est le diviseur d'une fonction rationnelle sur $\mathcal{C}$. Or on sait que sur une courbe elliptique, $D = \sum n_j P_j$ est le diviseur d'une fonction si et seulement si $\sum n_j = 0$ et $\sum [n_j] P_j = \mathcal{O}$.

Cela nous donne, comme nouvelle relation dans la jacobienne :

- $2(P_{1,1} + P_{3,2} + P_{3,1} + P_{1,4} + P_0 + P_{-1}) = 0$.

3.8.4 Conclusion

Les nouvelles relations entraînent que

- $P_{3,3} = P_{1,1} + P_{1,3} + 2P_1 - P_{3,1}$
- $P_{1,3} = 2P_{1,2} + 2P_1 + P_0 + P_{1,1}$
- $2(P_{1,1} + P_{1,2} + P_{3,1} + P_{3,2} + P_0 + P_1) = 0.$

Le groupe W est engendré par $P_{1,1}$, $P_{1,2}$, $P_{3,1}$, P_1, P_0 et par $P_{1,1} + P_{1,2} + P_{3,1} + P_{3,2} + P_0 + P_1$ qui est d'ordre 2 ; on a donc que W est un quotient de $(Z/4\mathbb{Z})^5 \times (\mathbb{Z}/2\mathbb{Z})$.

Notons dorénavant pour $1 \leq l \leq 3$ $P^{(l)}$ un point de la courbe elliptique $\mathcal{E}_l$.
Pour prouver que les relations que nous avons obtenues sont bien les seules relations dans la jacobienne, supposons qu'il y en ait une autre, à savoir $aP_{1,1} + bP_{1,2} + cP_{3,1} + dP_{3,2} + eP_0 + fP_1 = 0$, et regardons l'image de cette relation dans chacune des courbes elliptiques. Compte-tenu des relations entre les points sur la première courbe elliptique $\mathcal{E}_1$ (obtenues au paragraphe 3.8.1), on a $(a - b + c - d + 2e)Q_{1,1}^{(1)} + (c + d + f)Q_1^{(1)} = \mathcal{O}^{(1)}$. Comme $Q_{1,1}^{(1)}$ est d'ordre 4, et $Q_1^{(1)}$ d'ordre 2, comme de plus, $2Q_{1,1}^{(1)} \neq Q_1^{(1)}$, cela entraîne que $(a - b + c - d + 2e) \equiv 0 \bmod 4$ et que $(c + d + f) \equiv 0 \bmod 2$. Compte-tenu des relations entre les points sur la deuxième courbe elliptique $\mathcal{E}_2$ (obtenues au paragraphe 3.8.2), on obtient $(a + b + 2d + 2f)Q_{1,1}^{(2)} + (b + c + d)Q_{3,1}^{(2)} = \mathcal{O}^{(2)}$. Comme $Q_{1,1}^{(2)}$ est d'ordre 4, et $Q_{3,1}^{(2)}$ d'ordre 2, comme de plus, $2Q_{1,1}^{(2)} \neq Q_{3,1}^{(2)}$, cela entraîne que $(a + b + 2d + 2f) \equiv 0 \bmod 4$ et que $(b + c + d) \equiv 0 \bmod 2$. Compte-tenu des relations entre les points sur la troisième courbe elliptique $\mathcal{E}_3$ (obtenues au paragraphe 3.8.3), on obtient $(a + d + 2e)Q_{1,1}^{(3)} + (c - b + 2e)Q_{3,1}^{(3)} = \mathcal{O}^{(3)}$. Comme $Q_{1,1}^{(3)}$ est d'ordre 4, et $Q_{3,1}^{(3)}$ d'ordre 4, comme de plus, ni $Q_{1,1}^{(3)} + Q_{3,1}^{(3)}$, ni $Q_{1,1}^{(3)} - Q_{3,1}^{(3)}$ n'est d'ordre 2, cela entraîne que $(a + d + 2e) \equiv 0 \bmod 4$ et que $(c - b + 2e) \equiv 0 \bmod 4$. Cela se traduit par le système suivant

$$\begin{cases} a - b + c - d + 2e &= 0 \\ c + d + f &= 2\varepsilon \\ a + b + 2d + 2f &= 0 \\ b + c + d &= 2\varepsilon' \\ a + d + 2e &= 0 \\ c - b + 2e &= 0 \end{cases}$$

où les ε sont dans $\{0,1\}$.
Cela entraîne que $a = b = d = c = 2\varepsilon'$, que $f = 2\varepsilon$ et que $e = 2\varepsilon''$; la relation devient $2\varepsilon'(P_{1,1} + P_{1,2} + P_{3,1} + P_{3,2}) + 2\varepsilon'' P_0 + 2\varepsilon P_1 = 0$, or nous savons que $P_{1,1} + P_{1,2} + P_{3,1} + P_{3,2} + P_0 + P_1$ est un point d'ordre 2 de la jacobienne, donc,

cette relation peut s'écrire sous la forme $2(\varepsilon'' + \varepsilon')P_0 + 2(\varepsilon + \varepsilon')P_1 = 0$, ce qui est exclu. En effet, ni $2P_0$, ni $2P_1$, ni $2P_0 + 2P_1$ ne sont nuls dans J. Si l'on avait $2P_0 = 0$ dans la jacobienne, cela se traduirait par l'existence d'un diviseur principal sur $\mathcal{C}$, non nul, $\mathrm{div}\,(g) = 2P_0 - 2P_\infty$, et donc d'un morphisme de degré 2, $\overline{g} : \mathcal{C} \to \mathbb{P}^1$, ce qui contredirait le fait que $\mathcal{C}$ n'est pas hyperelliptique. D'autre part, dire que $2P_0 + 2P_1$ est nul dans la jacobienne revient à dire que $2P_0 + 2P_1 - 4P_\infty \sim 0$ et donc qu'il existe un diviseur effectif dans le système linéaire associé à $4P_\infty$ dont les zéros sont P_0 et P_1, avec multiplicité 2. Cela se traduit géométriquement par l'existence d'une bitangente à la courbe passant par P_0 et P_1, ce qui n'est pas possible, la tangente à $\mathcal{C}$ en chacun de ces points ayant multiplicité d'intersection 4 avec $\mathcal{C}$.

Quatrième partie

Etude de la courbe lisse d'équation affine $x^4 + y^4 + 1 + 3\left(x^2y^2 + x^2 + y^2\right) = 0$

Résumé

Nous déterminons la structure du groupe engendré par les points de Weierstrass dans la jacobienne de la courbe plane projective d'équation

$$X^4 + Y^4 + Z^4 + 3(X^2Y^2 + X^2Z^2 + Y^2Z^2) = 0.$$

Cette courbe est la seule courbe de genre 3, autre que la courbe de Fermat, possédant le nombre minimal de points de Weierstrass, à savoir 12.

Abstract

We describe the group generated by the Weierstrass points in the Jacobian of the curve

$$X^4 + Y^4 + Z^4 + 3\,(X^2Y^2 + X^2Z^2 + Y^2Z^2) = 0.$$

This curve is the only curve of genus 3, apart from the fourth Fermat curve, possessing exactly twelve Weierstass points.

4.1 Introduction

Soit $\mathcal{C}$ une courbe projective lisse de genre g. Pour un diviseur D, on note $[D]$ sa classe dans $\mathrm{Pic}^0(\mathcal{C})$. Choisissons un point de Weierstrass, qui sera noté ∞. On note J la jacobienne que l'on identifiera à $\mathrm{Pic}^0(\mathcal{C})$ et on définit le plongement jacobien suivant

$$j : \begin{array}{ccc} \mathcal{C} & \to & J \\ P & \mapsto & [P - \infty] \end{array}$$

que l'on étend par linéarité aux diviseurs $\mathrm{Div}(\mathcal{C})$.

Nous nous intéressons alors à la structure du groupe W engendré par les images par j des points de Weierstrass dans la jacobienne de $\mathcal{C}$. Cette structure est indépendante du point de Weierstrass choisi comme base du plongement.

Le cas le plus simple est celui d'une courbe hyperelliptique où l'on voit assez facilement que $W = (\mathbb{Z}/2\mathbb{Z})^{2g} = J[2]$ (voir le paragraphe 1.5).

Pour les courbes de genre 3 non hyperelliptiques, c'est-à-dire les quartiques planes, quelques cas particuliers ont été traités dans la littérature. Il s'agit de courbes possédant de nombreux automorphismes. En effet, pour la quartique de Klein (d'équation $X^3Y + Y^3Z + Z^3X = 0$), qui possède 168 automorphismes, $W = (\mathbb{Z}/2\,\mathbb{Z}) \times (\mathbb{Z}/7\,\mathbb{Z})^3$ ([Pra]). Pour la courbe de Fermat (d'équation $X^4 + Y^4 = Z^4$), qui possède 96 automorphismes, $W = (\mathbb{Z}/4\,\mathbb{Z})^5 \times (\mathbb{Z}/2\,\mathbb{Z})$ ([Roh]). Pour la courbe d'équation $Y^3Z + Z^4 = X^4$, qui en possède 48, $W = (\mathbb{Z}/4\,\mathbb{Z})^2 \times (\mathbb{Z}/3\,\mathbb{Z})^5$ ([KS]).

Dorénavant, nous nous intéressons à la courbe $\mathcal{C}$ lisse de genre 3 d'équation

$$X^4 + Y^4 + Z^4 + 3\,(X^2Y^2 + X^2Z^2 + Y^2Z^2) = 0.$$

Cette courbe possède 24 automorphismes ([KK]). Nous montrons que :

Théorème 4.1.1. *Soit W le groupe engendré par les images des points de Weierstrass dans la jacobienne de la courbe projective lisse d'équation $X^4 + Y^4 + Z^4 + 3\,(X^2Y^2 + X^2Z^2 + Y^2Z^2) = 0$, alors $W \cong (\mathbb{Z}/4\mathbb{Z})^5$.*

Cette courbe possède exactement 12 points de Weierstrass, tous de poids 2. Il n'y a que deux courbes qui possèdent douze points de Weierstrass, celle que nous considérons et la courbe de Fermat ([KK]).
Pour démontrer le théorème 4.1.1, nous allons tout d'abord utiliser des arguments géométriques pour réduire le nombre de générateurs de W. Puis, comme la jacobienne de la courbe est isogène au produit de trois fois la même courbe elliptique $\mathcal{E}$, l'étude des images de ces points dans $\mathcal{E}$ par les trois morphismes de $\mathcal{C}$ vers $\mathcal{E}$ nous permettra de déterminer exactement la structure de W.

REMERCIEMENTS : Je voudrais remercier Pavlos Tzermias pour m'avoir signalé une démonstration erronée et aidée à la corriger.

4.2 Détermination des points de Weierstrass

Dans le cas d'un quartique lisse, les points de Weierstrass sont les points d'inflexion. Le hessien H est donné par $H(X,Y,Z) = 2\,X^6 + (3\,Z^2 + 3\,Y^2)\,X^4 + (8\,Y^2Z^2 + 3\,Z^4 + 3\,Y^4)\,X^2 + 2\,Z^6 + 2\,Y^6 + 3\,Z^4Y^2 + 3\,Z^2Y^4$ et donc les points de Weierstrass sont définit par l'annulation de $(X^2+Y^2)(Y^2+Z^2)(Z^2+X^2)$. Les points de Weierstrass sont donc les points d'intersection de la courbe avec les 6 droites d'équation $L_1 : X = iY$, $L_2 : X = -iY$, $L_3 : Y = iZ$, $L_4 : Y = -iZ$, $L_5 : Z = iY$, $L_6 : Z = -iY$.

- Sur L_1 : $P_{1,1} = (i,1,1)$, $P_{1,2} = (-i,-1,1)$, $P_{1,3} = (-1,i,1)$, $P_{1,4} = (1,-i,1)$.
- Sur L_2 : $P_{2,1} = (-i,1,1)$, $P_{2,2} = (i,-1,1)$, $P_{2,3} = (1,i,1)$, $P_{2,4} = (-1,-i,1)$.
- Sur L_3 : $P_{1,3}$, $P_{2,3}$, $P_{3,3} = (-i,i,1)$, $P_{3,4} = (i,i,1)$
- Sur L_4 : $P_{1,4}$, $P_{2,4}$, $P_{4,3} = (-i,-i,1)$, $P_{4,4} = (i,-i,1)$.
- Sur L_5 : $P_{1,2}$, $P_{2,1}$, $P_{3,3}$, $P_{4,3}$.
- Sur L_6 : $P_{1,1}$, $P_{2,2}$, $P_{3,4}$, $P_{4,4}$.

D'autre part, la courbe a multiplicité d'intersection 4 avec la tangente en chacun de ces points. Cela nous donne tout de suite des relations entre les images des points de Weierstrass dans la jacobienne J. Choisissons comme base du plongement le point $P_{3,3}$. Le plongement j dans la jacobienne devient alors $P \mapsto P - P_{3,3}$. Par abus de notation, on confond un point et son image par j. On notera alors que $D = 0$ lorsqu'un diviseur D est dans le noyau de j.
Avec cette convention, on a donc

- $P_{1,1} + P_{1,2} + P_{1,3} + P_{1,4} = 0$
- $P_{2,1} + P_{2,2} + P_{2,3} + P_{2,4} = 0$
- $P_{1,3} + P_{2,3} + P_{3,3} + P_{3,4} = 0$
- $P_{1,4} + P_{2,4} + P_{4,3} + P_{4,4} = 0$
- $P_{1,2} + P_{2,1} + P_{3,3} + P_{4,3} = 0$
- $P_{1,1} + P_{2,2} + P_{3,4} + P_{4,4} = 0$
- $4P_{i,j} = 0$.

Cela nous permet d'exprimer $P_{1,4}$, $P_{2,4}$, $P_{3,4}$, $P_{4,3}$ et $P_{4,4}$ en fonction de $P_{1,1}$, $P_{1,2}$, $P_{1,3}$, $P_{2,1}$, $P_{2,2}$, de $P_{2,3}$ et de $P_{3,3}$ (qui est nul dans J). Comme nous le verrons par la suite (lemme 4.4.1 du paragraphe 4.4), nous avons en outre la relation $P_{1,2} + P_{2,2} - P_{1,1} - P_{2,1} = 2P_{1,3} - 2P_{2,3}$, qui nous permet d'exprimer $P_{2,2}$ en fonction de $P_{1,1}$, $P_{1,2}$, $P_{1,3}$, $P_{2,1}$ et de $P_{2,3}$, et donc de montrer que :

Proposition 4.2.1. *W est un quotient de $(\mathbb{Z}/4\mathbb{Z})^5$.*

Nous allons montrer que W est en fait égal à ce groupe, c'est-à-dire qu'il n'y a pas d'autres relations entre les points de Weierstrass que celles que nous avons déjà obtenues. Pour ce faire, nous allons utiliser la structure de la jacobienne qui est isogène au produit de trois fois la même courbe elliptique ([Kul]).

4.3 Structure de la jacobienne de $\mathcal{C}$

Soit $\mathcal{D}$ la courbe d'équation affine $x^4 + y^2 + 1 + 3(x^2y + x^2 + y) = 0$. Nous avons une application birationnelle que nous noterons ψ, de cette courbe vers la courbe elliptique $\mathcal{E}$ d'équation affine $v^2 = u(u - 1/4)(u - 5/4)$. Cette application birationnelle est donnée par $(x,y) \mapsto (u = \frac{1}{4}\frac{4y+11x^2+2x+11}{(x+1)^2}, v = -\frac{1}{4}\frac{(x-1)(4y+11x^2+2x+11)}{(x+1)^3})$ (voir annexe).

Notons ϕ_1, ϕ_2 et ϕ_3 les trois morphismes de $\mathcal{C}$ vers $\mathcal{D}$ définis par

$$\begin{cases} \phi_1 : (X,Y,Z) \mapsto (\frac{X}{Z},(\frac{Y}{Z})^2) \\ \phi_2 : (X,Y,Z) \mapsto (\frac{Y}{X},(\frac{Z}{X})^2) \\ \phi_3 : (X,Y,Z) \mapsto (\frac{Z}{Y},(\frac{X}{Y})^2). \end{cases}$$

Proposition 4.3.1. *La jacobienne de $\mathcal{C}$ est isogène à $\mathcal{E} \times \mathcal{E} \times \mathcal{E}$.*

DÉMONSTRATION : Si ω est une forme différentielle sur $\mathcal{D}$, on vérifie aisément que $\omega_1 = \phi_1^\star(\omega)$, $\omega_2 = \phi_2^\star(\omega)$ et $\omega_3 = \phi_3^\star(\omega)$ sont des formes différentielles indépendantes sur $\mathcal{C}$. En effet, si l'on prend $\omega = \frac{dx}{y+\frac{3}{2}x^2+\frac{3}{2}}$, on aura :

$\omega_1 = \frac{dx}{y^2+\frac{3}{2}x^2+\frac{3}{2}}$, $\omega_2 = \frac{d(\frac{y}{x})}{(\frac{1}{x})^2+\frac{3}{2}\frac{y^2}{x^2}+\frac{3}{2}} = \frac{xdy-ydx}{1+\frac{3}{2}y^2+\frac{3}{2}x^2} = \frac{1}{y}\frac{dx}{y^2+\frac{3}{2}x^2+\frac{3}{2}}$

et $\omega_3 = \frac{d(\frac{1}{y})}{(\frac{x}{y})^2+\frac{3}{2}\frac{1}{y^2}+\frac{3}{2}} = \frac{-dy}{x^2+\frac{3}{2}y^2+\frac{3}{2}} = \frac{x}{y}\frac{dx}{y^2+\frac{3}{2}x^2+\frac{3}{2}}$

car $y\,(2y^2+3x^2+3)dy + x\,(2x^2+3y^2+3)dx = 0$. ∎

Remarque : La courbe $\mathcal{E}$ a pour invariant $j(\mathcal{E}) = \frac{2^4 3^3 7^3}{5^2}$. Elle n'est donc pas à multiplication complexe. Cela fournit un exemple de calcul de W dans le cas d'une courbe avec beaucoup d'automorphismes sans néanmoins que la jacobienne soit isogène à un produit de courbes elliptiques à multiplication complexe. ∎

4.4 Images sur la courbe elliptique

Les images des points de Weierstrass par l'une des trois applications $\psi \circ \phi_i$ sont certains points particuliers de la courbe elliptique $\mathcal{E}$, à savoir :
$A = (\frac{1}{4}-\frac{1}{2}i,-\frac{1}{2}-\frac{1}{4}i)$, $B = (\frac{1}{4}+\frac{1}{2}i,-\frac{1}{2}+\frac{1}{4}i)$, $C = (5/4,0)$, $D = (\frac{1}{4}-\frac{1}{2}i,\frac{1}{2}+\frac{1}{4}i)$, $E = (\frac{1}{4}+\frac{1}{2}i,\frac{1}{2}-\frac{1}{4}i)$ et le point à l'infini, noté ∞, que l'on prend comme élément neutre de la loi de groupe.
Des calculs élémentaires fournissent les relations suivantes sur la courbe elliptique $\mathcal{E}$

$$\begin{cases} 2C = A + D = B + E = \infty \\ 2A = 2B = 2D = 2E = (\frac{1}{4},0) \\ A + B = D + E = C \\ A + E = B + D = (0,0) \\ C + (0,0) = (\frac{1}{4},0) \\ 2(0,0) = 2(\frac{1}{4},0) = 2(\frac{5}{4},0) = \infty \end{cases}$$

ce qu'on peut résumer en les relations suivantes:

$$\begin{cases} A+D=\infty \\ A+C-E=\infty \\ A+B+C=\infty \\ 2C=\infty\cdot \end{cases}$$

Ces points de $\mathcal{E}$ ont pour antécédents par $\psi\circ\phi_j$

P	$(\psi\circ\phi_1)^*(P)$	$(\psi\circ\phi_2)^*(P)$	$(\psi\circ\phi_3)^*(P)$
A	$P_{1,1}+P_{2,2}$	$P_{2,3}+P_{2,4}$	$P_{4,3}+P_{4,4}$
B	$P_{1,2}+P_{2,1}$	$P_{1,3}+P_{1,4}$	$P_{3,3}+P_{3,4}$
C	$P_{1,4}+P_{2,3}$	$P_{3,4}+P_{4,3}$	$P_{1,1}+P_{2,1}$
D	$P_{3,3}+P_{4,3}$	$P_{1,1}+P_{1,2}$	$P_{1,3}+P_{2,3}$
E	$P_{3,4}+P_{4,4}$	$P_{2,1}+P_{2,2}$	$P_{1,4}+P_{2,4}$
∞	$P_{1,3}+P_{2,4}$	$P_{3,3}+P_{4,4}$	$P_{1,2}+P_{2,2}$

En effet, ϕ_1 est de degré 2, et $P_{1,1}$ et $P_{2,2}$ ont la même image sur la courbe $\mathcal{D}$, à savoir le point de coordonnées $(i,1)$, qui a pour image A par ψ. Toutes les autres images se calculent de la même façon.

Cela nous permet d'obtenir une nouvelle relation entre les points de Weierstrass, à savoir

Lemme 4.4.1. $P_{1,2}+P_{2,2}-P_{1,1}-P_{2,1}=2P_{1,3}-2P_{2,3}$.

DÉMONSTRATION : Nous allons montrer que le diviseur $P_{1,2}+P_{2,2}-P_{1,1}-P_{2,1}-2P_{1,3}+2P_{2,3}$ sur $\mathcal{C}$ est principal. Le diviseur $A+D-2\infty$ sur $\mathcal{E}$ étant principal, le diviseur $(\psi\circ\phi_1)^*(A+D-2\infty)=P_{1,1}+P_{2,2}+P_{3,3}+P_{4,3}-2P_{1,3}-2P_{2,4}$ sur $\mathcal{C}$ est aussi principal. Il est linéairement équivalent à $P_{1,2}+P_{2,2}-P_{1,1}-P_{2,1}-2P_{1,3}+2P_{2,3}$, d'où le résultat. ∎

4.5 Preuve du théorème 4.1.1

Nous allons nous servir du lemme géométrique suivant

Lemme 4.5.1. *Pour des points de Weierstrass distincts P, Q, R sur $\mathcal{C}$, $2[P+Q-2R]\neq 0$.*

DÉMONSTRATION : Comme $4R$ est un diviseur canonique sur $\mathcal{C}$, l'existence d'une fonction rationnelle dans $L(4R)$ s'annulant à l'ordre 2 en P et Q correspond à l'existence d'une bitangente passant par P et Q. Or cela n'est

pas possible, car P et Q étant des points de Weierstrass, la tangente à $\mathcal{C}$ en chacun de ces points a multiplicité d'intersection 4 avec $\mathcal{C}$. ∎

DÉMONSTRATION DU THÉORÈME 4.1.1 D'après la proposition 4.2.1, il suffit de montrer que $2\,W$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^5$. De manière équivalente, cela revient à montrer que $[2P_{1,1}-2P_{3,3}]$, $[2P_{1,2}-2P_{3,3}]$, $[2P_{1,3}-2P_{3,3}]$, $[2P_{2,1}-2P_{3,3}]$ et $[2P_{2,3}-2P_{3,3}]$ sont linéairement indépendant sur $\mathbb{Z}/2\mathbb{Z}$. Par l'absurde, supposons qu'il existe des coefficents (non tous nuls) c_1, c_2, c_3, c_4, c_5 dans $\mathbb{Z}/2\mathbb{Z}$ tels que l'on ait

$$D = [2c_1P_{1,1}+2c_2P_{1,2}+2c_3P_{1,3}+2c_4P_{2,1}+2c_5P_{2,3}-2(c_1+c_2+c_3+c_4+c_5)P_{3,3}] = 0.$$

Considérons, pour $1 \leq j \leq 3$, les images par $(\psi \circ \phi_j)$ du diviseur D, on obtient

$$\begin{cases} 2c_1A + 2(c_2+c_4)B + 2c_5C - 2(c_1+c_2+c_3+c_4+c_5)D = \infty \\ 2(c_1+c_2)D + 2c_3B + 2c_4E + 2c_5A = \infty \\ 2(c_1+c_4)C + 2(c_3+c_5)D - 2(c_1+c_2+c_3+c_4+c_5)B = \infty\cdot \end{cases}$$

Comme $2A = 2B = 2D = 2E = (\frac{1}{4},0)$ et $2C = \infty$, on obtient que

$$(c_3+c_5)(\frac{1}{4},0) = (c_1+c_2+c_3+c_4+c_5)(\frac{1}{4},0) = (c_1+c_2+c_4)(\frac{1}{4},0) = \infty,$$

et donc les coefficients doivent satisfaire les deux relations
$c_3 = c_5$ et $c_1 + c_2 + c_4 = 0$.

Si $c_3 = c_5 = 0$ ou si $c_1 = c_2 = c_4 = 0$, alors exactement deux des coefficients c_j valent 1, et donc par le lemme 4.5.1, $D \neq 0$, ce qui est absurde.
Nous pouvons donc dorénavant supposer que $c_3 = c_5 = 1$ et qu'un et un seul des trois coefficients c_1, c_2, c_4 est égal à 0. Nous avons alors trois cas à considérer :

1er cas : $\mathbf{c_1 = 0}$

D'après les relations du paragraphe 4.2, on a

$$0 = D = [2(P_{1,2}+P_{1,3}+P_{2,1}+P_{2,3}) - 8P_{3,3}] = [4P_{3,3} - 2P_{3,4} - 2P_{4,3}],$$

ce qui contredit le lemme 4.5.1.

2ème cas : $\mathbf{c_4 = 0}$

D'après les relations du paragraphe 4.2, on a

$$0 = D = [2(P_{1,1} + P_{1,2} + P_{1,3} + P_{2,3}) - 8P_{3,3}] = [2P_{2,3} - 2P_{1,4}],$$

ce qui entraîne l'existence d'un morphisme $\mathcal{C} \to \mathbb{P}^1$ de degré 2, et donc contredit le fait que $\mathcal{C}$ n'est pas hyperelliptique.

3ème cas : $\mathbf{c_2 = 0}$

D'après les relations du paragraphe 4.2, on a

$$0 = D = [2(P_{1,1}+P_{1,3}+P_{2,1}+P_{2,3})-8P_{3,3}] = [2P_{1,1}+2P_{2,1}-2P_{3,3}-2P_{3,4}].$$

Soit f une fonction rationnelle sur $\mathcal{C}$ telle que $\mathrm{div}\,(f) = 2P_{1,1} + 2P_{2,1} - 2P_{3,3} - 2P_{3,4}$. Remarquons que le diviseur $E = 2P_{3,3} + 2P_{3,4}$ n'est pas un diviseur canonique. Par le théorème de Riemann-Roch, l'espace vectoriel $L(E)$ est de dimension 2 (en effet, s'il existait une fonction rationnelle de diviseur $2P_{3,3} - 2P_{3,4}$, la courbe serait hyperelliptique). Si l'on note ∞_j, $1 \leq j \leq 4$ les quatre points d'intersection de $\mathcal{C}$ avec la droite d'équation $Z = 0$, on a immédiatement que

$$\mathrm{div}\,(\frac{X^2 + Y^2 + 2Z^2}{Z}) = 2P_{3,3} + 2P_{3,4} + 2P_{4,3} + 2P_{4,4} - \sum_{j=1}^{4} 2\infty_j,$$

$$\mathrm{div}\,(\frac{Y + iZ}{Z}) = P_{1,4} + P_{2,4} + P_{4,3} + P_{4,4} - \sum_{j=1}^{4} \infty_j.$$

Une base de $L(E)$ est alors donnée par les fonctions rationnelles 1 et $(y+i)^2/(x^2+y^2+2)$. En particulier, on peut supposer que f est de la forme

$$f = \frac{a(x^2 + y^2 + 2) + (y + i)^2}{x^2 + y^2 + 2},$$

avec $a \in \mathbb{C}$. Comme $P_{1,1}$ annule f, on doit avoir $a = -i$. Mais alors, pour cette valeur de a, le point $(i\sqrt{5}, -1{,}1)$ est aussi un zéro de f, ce qui donne une contradiction.

Annexe

Soit $\mathcal{E}$ une courbe donnée sous la forme $y^2 = P(x)$ où P est un polynôme de degré 4 sans racine double et possédant un point rationnel, que nous noterons (x_0,y_0). Nous rappelons ici la procédure pour mettre cette courbe sous forme d'une cubique de Weierstrass ([Cas]).

Lemme *En envoyant le point rationnel à l'infini, l'équation de la courbe devient* $Y^2 = G(X)^2 + H(X)$, *avec* G *unitaire de degré 2 et* H *de degré 1. Il existe alors une application birationnelle de cette courbe vers la courbe elliptique d'équation*

$$v^2 = u^3 + (g_1^2 - 4g_0)u^2 + (2g_1h_1 - 4h_0)u + h_1^2$$

donnée explicitement par $(X,Y) \mapsto (2(Y + G(X)),2(2X + g_1)(Y + G(X)) + h_1)$.

En effet, après la transformation $(x,y) \mapsto (X,Y) = (\frac{1}{(x - x_0)}, \frac{y}{(x - x_0)^2\, y_0})$ (qui consiste à envoyer le point rationnel à l'infini), l'équation de la courbe devient

$$Y^2 = X^4 + a_3X^3 + a_2X^2 + a_1X + a_0.$$

On peut écrire la partie de droite de l'équation sous la forme $G(X)^2 + H(X)$ avec $G(X) = X^2 + g_1X + g_0$ et $H(X) = h_1X + h_0$. On a donc

$$(Y - G(X))(Y + G(X)) = H(X).$$

En posant $T = (Y+G(X))$, de la sorte, on a $Y - G(X) = H(X)/T$. Nous obtenons donc

$$2G(X) = T - H(X)/T.$$

En posant $S = TX$, nous obtenons que le point de coordonnées $(2T,4S)$ est sur la courbe elliptique d'équation

$$v^2 + 2g_1uv + 2h_1v = u^3 - 4g_0u^2 - 4h_0u.$$

Notons $\mathcal{E}'$ la courbe elliptique sous forme de Weierstrass

$$v^2 = u^3 + (g_1^2 - 4g_0)u^2 + (2g_1h_1 - 4h_0)u + h_1^2.$$

L'application birationnelle de $\mathcal{E}$ dans $\mathcal{E}'$ est alors donnée par $(x,y) \mapsto (u,v)$ où

$$\begin{cases} u &= 2\dfrac{(y/y_0 + g_0(x - x_0)^2 + g_1(x - x_0) + 1)}{(x - x_0)^2} \\ v &= (4 + 2g_1(x - x_0))\dfrac{(y/y_0 + g_0(x - x_0)^2 + g_1(x - x_0) + 1)}{(x - x_0)^3} + h_1. \end{cases}$$

Bibliographie

[ACGH] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris. *Geometry of algebraic curves. Vol. I.* Springer-Verlag, New York, 1985.

[Arb] E. Arbarello. Weierstrass points and moduli of curves. *Compositio Math.*, **29** (1974), 325–342.

[Cas] J. W. S. Cassels. *Lectures on elliptic curves.* Cambridge University Press, Cambridge, 1991.

[CF] F. Cukierman and L.-Y. Fong. On higher Weierstrass points. *Duke Math. J.*, **62**, n°1 (1991), 179–203.

[Dia] S. Diaz. Tangent spaces in moduli via deformations with applications to Weierstrass points. *Duke Math. J.*, **51**, n°4 (1984), 905–922.

[EH] D. Eisenbud and J. Harris. Existence, decomposition, and limits of certain Weierstrass points. *Invent. Math.*, **87**, n°3 (1987), 495–515.

[Har] R. Hartshorne. *Algebraic geometry.* Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, 52.

[HS] M. Hindry and J. H. Silverman. *Diophantine Geometry, An Introduction.* Springer-Verlag, New York, 2000. Graduate Texts in Mathematics, 201.

[Hub] J. H. Hubbard. Sur les sections analytiques de la courbe universelle de Teichmüller. *Mem. Amer. Math. Soc.*, 4(166):ix+137, 1976.

[KK] A. Kuribayashi and K. Komiya. On Weierstrass points and automorphisms of curves of genus three. In *Algebraic geometry, Proc. Summer Meet., Copenh. 1978.* Springer-Verlag, 1979. Lecture Notes in Mathematics, 732.

[KS] M. J. Klassen and E. F. Schaefer. Arithmetic and geometry of the curve $y^3 + 1 = x^4$. *Acta Arith.*, **74**, n°3 (1996), 241–257.

[Kul] L. Kulesz. Courbes elliptiques de rang ≥ 5 sur $\mathbb{Q}(t)$ avec un groupe de torsion isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. *C. R. Acad. Sci. Paris Sér. I Math.*, **329**, n°6 (1999), 503–506.

[KY] A. Kuribayashi and K. Yoshida. On the non-hyperelliptic compact Riemann surfaces defined by $Y^4 = X(X-1)(X-t)$. *Bull. Fac. Sci. Eng., Chuo Univ., Ser. I*, **21** (1978), 13–27.

[Lax] R. F. Lax. Gap sequences and moduli in genus 4. *Math. Z.*, **175**, n°1 (1980), 67–75.

[LT] D. Laksov and A. Thorup. Weierstrass points and gap sequences for families of curves. *Ark. Mat.*, **32**, n°2 (1994), 393–422.

[MF] D. Mumford and J. Fogarty. *Geometric invariant theory.* Springer-Verlag, Berlin, second edition, 1982.

[Mil1] J. S. Milne. Abelian varieties. In G. Cornell and J. H. Silverman, editors, *Arithmetic geometry.* Springer-Verlag, 1986.

[Mil2] J. S. Milne. Jacobian varieties. In G. Cornell and J. H. Silverman, editors, *Arithmetic geometry.* Springer-Verlag, 1986.

[Mum1] D. Mumford. *Abelian varieties.* Published for the Tata Institute of Fundamental Research, Bombay, 1970. Tata Institute of Fundamental Research Studies in Mathematics, n°5.

[Mum2] D. Mumford. *Curves and their Jacobians.* The University of Michigan Press, Ann Arbor, Mich., 1975.

[Mur] V. K. Murty. *Introduction to abelian varieties.* American Mathematical Society, Providence, RI, 1993.

[Nér] A. Néron. Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps. *Bull. Soc. Math. France*, **80** (1952), 101–166.

[Pra] D. T. Prapavessi. On the Jacobian of the Klein curve. *Proc. Amer. Math. Soc.*, **122**, n°4 (1994), 971–978.

[Roh] D. E. Rohrlich. Points at infinity on the Fermat curves. *Invent. Math.*, **39**, n°2 (1977), 95–127.

[Sch] E. F. Schaefer. Computing a Selmer group of a Jacobian using functions on the curve. *Math. Ann.*, **310**, n°3 (1998), 447–471.

[Ser] J.-P. Serre. *Lectures on the Mordell-Weil theorem.* Friedr. Vieweg & Sohn, 1989. Aspects of Mathematics, E 15.

[Sil1] J. H. Silverman. Heights and the specialization map for families of abelian varieties. *J. Reine Angew. Math.*, **342** (1983), 197–211.

[Sil2] J. H. Silverman. *The arithmetic of elliptic curves.* Springer-Verlag, New York, 1986. Graduate Texts in Mathematics, 106.

[Sil3] J. H. Silverman. Some arithmetic properties of Weierstrass points: hyperelliptic curves. *Bol. Soc. Brasil. Mat. (N.S.)*, **21**, n°1 (1990), 11–50.

[Sil4] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves.* Springer-Verlag, New York, 1994. Graduate Texts in Mathematics, 151.

[Ver] A. M. Vermeulen. *Weierstrass points of weight two on curves of genus three.* PhD thesis, Universiteit van Amsterdam, 1983.