

## Groupe des points de Weierstrass sur une famille de quartiques lisses

par

MARTINE GIRARD (Paris)

**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, par exemple [Mum, chapitre 3.2, pp. 28–39]).

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 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  $\beta \notin \{0, 1\}$ . 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  $S_K$ .*

**REMARQUE.** Le résultat que nous obtenons est en fait plus fort : nous obtenons un isomorphisme entre  $W_{\mathcal{C}_{\beta}}$  et  $\mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5$  pour tout  $\beta$  en dehors d'un ensemble de hauteur bornée.

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

Afin de démontrer le théorème 1.1, nous allons exhiber 9 points de Weierstrass  $P_1, \dots, P_9$  avec  $P_5, \dots, P_9$  d'ordre 3 tel que si l'on note  $\psi(m_1, \dots, m_9) = m_1P_1 + \dots + m_9P_9$ , on obtient le diagramme commutatif suivant :

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

où  $W_\eta$  est le groupe engendré par les points de Weierstrass de la courbe générique,  $W_s$  celui engendré par ceux de la courbe spéciale et  $\mu$  la spécialisation. Puis, nous allons montrer que :

- (i)  $\mu$  est surjective (argument de spécialisation (proposition 2.3)).
- (ii)  $\psi_s$  et  $\psi_\eta$  sont surjectives (proposition 4.1).
- (iii)  $\psi_s$  est un isomorphisme pour un  $s$  particulier (proposition 6.1).

Cela nous permettra de conclure que  $\psi_\eta$  est un isomorphisme, qui ne dépend pas de la spécialisation. Puis, comme  $\mu$  est un isomorphisme pour presque toute spécialisation en  $s$  (cela découle du théorème 7.1), cela nous permettra de conclure.

**CONVENTIONS.** Tous les corps que nous considérons sont de caractéristique 0. Pour une courbe définie sur un corps  $k$ , nous étudions les points géométriques de cette courbe (*i.e.* les points  $\bar{k}$ -rationnels). Lorsque nous nous intéressons à des points définis sur un sous-corps de  $\bar{k}$ , nous précisons si nécessaire leur corps de définition.

Je tiens à remercier mon directeur de thèse, Marc Hindry, pour toutes les précieuses discussions que nous avons eues, tout au long de l'élaboration de cet article.

**2. Points de Weierstrass.** Nous rappelons la définition et quelques propriétés bien connues des points de Weierstrass (voir, par exemple, [ACGH], [Mur] ou [HS]).

Soit  $\mathcal{C}$  une courbe lisse projective de genre  $g \geq 2$  définie sur un corps  $k$  et soit  $P$  un point quelconque de  $\mathcal{C}$ . Notons  $\ell(D) - 1$  la dimension du système linéaire associé à un diviseur  $D$  de  $\mathcal{C}$ .

**DÉFINITION.** On définit  $G(P) = \{n \in \mathbb{N} \setminus \{0\} \mid \ell(nP) = \ell((n - 1)P)\}$ .

DÉFINITION. Si  $G(P) \neq \{1, \dots, g\}$ , on dit que  $P$  est un *point de Weierstrass*.

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

PROPOSITION 2.1. *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

$$w(P) = \left( \sum_{n \in G(P)} n \right) - g(g+1)/2.$$

PROPOSITION 2.2. *On a :*

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

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

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

$$j : \mathcal{C} \rightarrow J, \quad P \mapsto [P - \infty]$$

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

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.

Pour une courbe hyperelliptique, les points de Weierstrass sont les points de ramification. Pour une quartique lisse, les points de Weierstrass sont ses points d'inflexion, c'est-à-dire les points où la multiplicité d'intersection de la courbe 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 24 points de Weierstrass comptés avec multiplicité correspondant à leur poids, une courbe générale en possède exactement 24. On a donc  $\text{rang}_{\mathbb{Z}} W \leq 23$ . Si on choisit  $\infty$  parmi les points d'hyper-inflexion,  $4\infty$  est un diviseur canonique, et comme  $\text{div}(\sum w(P)P)$  est linéairement équivalent à un multiple du diviseur canonique, on a 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  $\text{rang}_{\mathbb{Z}} W \leq 21$ .

Nous pouvons nous demander quelles sont les propriétés de rationalité de  $W$ . Rappelons que la courbe  $\mathcal{C}$  est définie sur  $k$ . Le groupe  $W$  est défini sur  $k$ . En effet, l'ensemble  $\mathcal{W}$  des points de Weierstrass est stable sous l'action de  $G = \text{Gal}(\bar{k}/k)$  et le groupe  $W$  est engendré par les  $[P - \infty]$  pour  $P \in \mathcal{W}$ . Ainsi pour  $s \in G$  le groupe  $s(W)$  est engendré par les  $[s(P) - s(\infty)]$  pour  $P \in \mathcal{W}$  donc par les  $[P - s(\infty)]$  pour  $P \in \mathcal{W}$ ; c'est donc  $W$ . Qu'en est-il des points de  $W$ ? Ils sont certainement définis sur le corps de définition des points de Weierstrass, mais sont-ils définis sur un corps intermédiaire  $K$ ? Lorsqu'il existe des points  $K$ -rationnels, il est aisé de répondre par la négative. Considérons donc un corps intermédiaire  $K$  (contenant  $k$ ) tel qu'il existe au moins un point de Weierstrass non-défini sur  $K$  et tel que  $\mathcal{C}(K)$  soit non-vidé; nous allons montrer qu'il existe des points de  $W$  non-définis sur  $K$ . En effet, on peut être dans l'une des deux situations suivantes: soit  $\infty$  est  $K$ -rationnel, auquel cas l'image d'un point de Weierstrass non-rationnel sur  $K$  n'est pas dans  $J(K)$  (sinon, la courbe serait de genre 0), soit  $\infty$  n'est pas  $K$ -rationnel, auquel cas considérons le plongement  $j'$  ayant comme base un point  $P_0$  rationnel sur  $K$  et là encore  $j(P) = j'(P) - j'(\infty)$  n'est pas dans  $J(K)$  d'après le lemme 6.3.

Des résultats classiques ([LT] dans le cas algébrique, [Hub] dans le cas analytique) indiquent que si  $X \rightarrow S$  est une famille de courbes, le diviseur des points de Weierstrass  $\sum w(P)P$  de chaque fibre forme un diviseur de Cartier effectif relatif sur  $X/S$ ; par ailleurs, la spécialisation est injective sur les points de torsion (voir, par exemple [Mil, corollary 20.8, p. 148] ou [HS, theorem C.1.4, p. 263]).

Nous en déduisons la proposition suivante que nous utiliserons par la suite :

**PROPOSITION 2.3.** *Soit  $X \rightarrow S$  une famille de courbes lisses de genre  $g$ .*

(a) *Le groupe engendré par les points de Weierstrass d'une fibre spéciale  $X_s$  est un quotient de celui engendré par les points de Weierstrass de la fibre générique  $X_\eta$ .*

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

**3. 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  $ZY^3 = Z^4 f(Y/Z)$  admet un unique point à l'infini, noté  $P_\infty$  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  $Y^3 Z = X(X - Z)(X^2 - 2\beta X Z + \beta Z^2)$ , il vient

$$H(X, Y, Z) = 54YG(X, Y, Z)$$

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

En repassant en coordonnées affines, et en remplaçant  $y^3$  par sa valeur en fonction de  $x$ , on obtient

$$\begin{aligned} G_0(x) &= 2x^6 + (-6\beta - 3)x^5 + 15\beta x^4 - 10\beta x^3 - 3\beta(\beta - 1)x^2 + 3\beta^2 x - \beta^2 \\ &= (2x^3 - 3x^2 + \beta)(x^3 - 3\beta x^2 + 3\beta x - \beta). \end{aligned}$$

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  $P_\infty$  et d'autre part, les points ayant pour abscisse les zéros du polynôme  $G_0(x) = (2x^3 - 3x^2 + \beta)(x^3 - 3\beta x^2 + 3\beta x - \beta)$ .

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.

**3.1. Premier facteur du hessien.** Nous avons noté  $x_1, x_2$  et  $x_3$  les racines de  $(2x^3 - 3x^2 + \beta)$  ; on a donc

$$\begin{aligned} x_1 + x_2 + x_3 &= 3/2, \\ x_1x_2 + x_1x_3 + x_2x_3 &= 0, \\ 2x_1x_2x_3 &= -\beta. \end{aligned}$$

D'où, en remplaçant  $x_3$  par  $3/2 - x_1 - x_2$  dans la deuxième équation, il vient

$$2x_1x_2 + 2x_1^2 - 3x_1 + 2x_2^2 - 3x_2 = 0.$$

C'est l'équation d'une conique passant par  $(0, 0)$ , que l'on paramètre par  $x_2 = tx_1$ . 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

$$\begin{cases} x_1 = \frac{3}{2} \cdot \frac{t + 1}{t^2 + t + 1}, \\ x_2 = \frac{3}{2} \cdot \frac{t(t + 1)}{t^2 + t + 1}, \\ x_3 = -\frac{3}{2} \cdot \frac{t}{t^2 + t + 1}. \end{cases}$$

et donc

$$\beta = \frac{27}{4} \cdot \frac{(t+1)^2 t^2}{(t^2+t+1)^3}.$$

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

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

et on obtient ainsi

$$\begin{cases} y_1^3 = -\frac{27}{16} \cdot \frac{(t+1)^3 (2t+1)^3 (t-1)^3}{(t^2+t+1)^6}, \\ y_2^3 = \frac{27}{16} \cdot \frac{(t+1)^3 t^3 (t+2)^3 (t-1)^3}{(t^2+t+1)^6}, \\ y_3^3 = \frac{27}{16} \cdot \frac{t^3 (t+2)^3 (2t+1)^3}{(t^2+t+1)^6}. \end{cases}$$

Notons alors

$$\begin{cases} y_{1,1} = -\frac{3}{4} \cdot 2^{2/3} \cdot \frac{(t+1)(2t+1)(t-1)}{(t^2+t+1)^2}, \\ y_{2,1} = \frac{3}{4} \cdot 2^{2/3} \cdot \frac{(t+1)t(t+2)(t-1)}{(t^2+t+1)^2}, \\ y_{3,1} = \frac{3}{4} \cdot 2^{2/3} \cdot \frac{t(t+2)(2t+1)}{(t^2+t+1)^2}. \end{cases}$$

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

Ces points sont dans une configuration particulière. Plus précisément, nous avons le résultat suivant dont la démonstration est immédiate.

**PROPOSITION 3.1.** *Pour tout triplet de points  $\{P_{1,\alpha_1}, P_{2,\alpha_2}, P_{3,\alpha_3}\}$  où les  $\alpha_i$  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  $P_{t_2}$ .*

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 d'abscisse  $1/2$  ; en effet, un calcul rapide montre que

**LEMME 3.2.** *Le quatrième point d'intersection de la tangente à la courbe en  $P_{1,j}$ ,  $P_{2,j}$  ou  $P_{3,j}$  avec  $\mathcal{C}$  est le point  $Q_{1,j} = (1/2, -2^{2/3} \zeta_3^{j-1} / 4)$ .*

**3.2. 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  $\alpha_i$  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

$$\begin{aligned}x_4 + x_5 + x_6 &= 3\beta, \\x_4x_5 + x_5x_6 + x_4x_6 &= 3\beta, \\x_4x_5x_6 &= \beta,\end{aligned}$$

d'où

$$\beta = \frac{1}{3}(x_4 + x_5 + x_6) \quad \text{et} \quad x_6 = -\frac{x_4x_5 - x_4 - x_5}{x_4 + x_5 - 1}.$$

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

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

et alors

$$x_6 = \frac{3 - i\sqrt{3}}{6x_4 - 3 - i\sqrt{3}}x_4 = \frac{1}{12} \cdot \frac{(3 - i\sqrt{3})(6x_4 - 3 + i\sqrt{3})}{3x_4^2 - 3x_4 + 1}x_4 = \bar{x}_5$$

et donc  $\beta = x_4^3/(3x_4^2 - 3x_4 + 1)$ . Si l'on pose  $u = x_4$ , on a donc

$$\begin{cases}x_4 = u, \\x_5 = \frac{(3 + i\sqrt{3})u}{6u - 3 + i\sqrt{3}}, \\x_6 = \frac{(3 - i\sqrt{3})u}{6u - 3 - i\sqrt{3}}\end{cases}$$

et alors  $\beta = u^3/(3u^2 - 3u + 1)$ .

Posons

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

On note alors  $P_{i,j}$  le point  $(x_i, y_{i,1}c_3^{j-1})$  où  $j \in \{1, 2, 3\}$ .

De même que précédemment, on peut montrer que

**PROPOSITION 3.3.** *Pour tout triplet de points  $\{P_{4,\alpha_4}, P_{5,\alpha_5}, P_{6,\alpha_6}\}$  où les  $\alpha_i$  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  $P_1$ .*

De la même façon que précédemment, les tangentes à  $\mathcal{C}$  en  $P_{4,j}$ ,  $P_{5,j}$  et  $P_{6,j}$  se coupent en un point d'abscisse  $\beta$ ; en effet, nous obtenons par un calcul immédiat :

LEMME 3.4. *Le quatrième point d'intersection de la tangente à la courbe en  $P_{4,j}$ ,  $P_{5,j}$  ou  $P_{6,j}$  avec  $\mathcal{C}$  est le point*

$$Q_{4,j} = \left( \beta, -\frac{u^2(u-1)^2}{(3u^2-3u+1)^{4/3}} \zeta_3^{j-1} \right).$$

REMARQUE. Selon que l'on s'intéresse au premier ou au second terme du hessien, la paramétrisation choisie diffère. L'expression de  $\beta$  dans chaque cas nous permet de trouver une relation entre les deux paramètres, à savoir

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

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  $\beta = r_0^2/(r_0^2 - 1)$  où  $r_0 \in K$  et alors les racines de  $P$  sont  $r_0/(r_0 + 1)$  et  $r_0/(r_0 - 1)$ . On peut exprimer  $r_0$  en fonction de  $t$ ,

$$r_0 = \frac{3i\sqrt{3}(t+1)t}{(2t+1)(t+2)(t-1)};$$

ou encore, en fonction de  $u$ ,  $r_0 = \left(\frac{u}{u-1}\right)^{3/2}$ .

**4. Étude géométrique des points de Weierstrass.** 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  $j(\mathcal{C}, \mathcal{D}) = [P_1 + P_2 + P_3 + P_4 - 4P_\infty]$ . Par la suite, on identifiera un point de  $\mathcal{C}$  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  $P_1 + P_2 + P_3 + P_4 = 0$ .

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

- $\text{div}(X) = 3P_0 + P_\infty$ ,
- $\text{div}(X - Z) = 3P_1 + P_\infty$ ,
- $\text{div}(X - t_1Z) = 3P_{t_1} + P_\infty$ ,
- $\text{div}(X - t_2Z) = 3P_{t_2} + P_\infty$ ,
- $\text{div}(Y) = P_0 + P_1 + P_{t_1} + P_{t_2}$ ,
- $\text{div}(X - x_iZ) = P_{i,1} + P_{i,2} + P_{i,3} + P_\infty$  pour  $1 \leq i \leq 6$ ,
- $\text{div}(2X - Z) = Q_{1,1} + Q_{1,2} + Q_{1,3} + P_\infty$ ,
- $\text{div}(X - \beta Z) = Q_{4,1} + Q_{4,2} + Q_{4,3} + P_\infty$ .

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  $\text{div}(T_{i,j}) = 3P_{i,j} + Q_{i,j}$  et donc, comme  $Q_{i,j} = Q_{i',j}$ , on en tire  $\text{div}(T_{i,j}/T_{i',j}) = 3P_{i,j} - 3P_{i',j}$ .

On a donc les relations :

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

On en déduit que :

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

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 :

PROPOSITION 4.1.  $W$  est un quotient de  $\mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5$ .

Plus précisément, nous avons obtenu une application  $\mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5 \xrightarrow{\psi_\beta} W_{C_\beta}$ ,  
 $(m_1, \dots, m_4)(n_1, \dots, n_5) \mapsto m_1P_{1,1} + m_2P_{1,2} + m_3P_{4,1} + m_4P_{4,2} + n_1P_0$   
 $+ n_2P_1 + n_3P_{t_1} + n_4(P_{1,1} - P_{2,1}) + n_5(P_{4,1} - P_{5,1})$

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  $\mathbb{Z}^2 \times (\mathbb{Z}/3\mathbb{Z})^4$ .

**5. 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  $\zeta$  est une racine cubique de l'unité. Plus précisément, nous allons utiliser une version de la descente explicitée dans un article de Schaefer ([Sch]) auquel nous renvoyons pour les détails et les démonstrations.

Soit  $C$  la courbe d'équation  $y^3 = f(x)$  et soit  $K$  un corps de nombres contenant une racine cubique de l'unité  $\zeta$ , tel que le polynôme  $f$  soit scindé. Le résultat que nous allons utiliser peut être décrit informellement ainsi : soit  $\alpha$  une racine de  $f(x) = x(x-1)(x^2 - 2\beta x + \beta)$ ; l'application  $P \mapsto x(P) - \alpha \pmod{K^{*3}}$  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  $S$ . 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  $J(K) \rightarrow K^*/K^{*3}$ . Le noyau du morphisme  $x - T$  de  $J(K)$  dans  $(K^*/K^{*3})^4$  est exactement  $\phi(J(K))$ , où  $\phi = 1 - \zeta$ . L'application  $x - T$  correspond au 4-uplet de fonctions  $(x, x-1, x-t_1, x-t_2)$ .

Nous aurons d'autre part besoin d'analyser la torsion d'ordre 3, et ce qui nous servira est résumé dans le lemme 5.1.

Notons  $\dim M$  la dimension d'un  $\mathbb{Z}/3\mathbb{Z}$ -espace vectoriel  $M$ . Comme  $K$  est un corps de nombres qui contient une racine cubique de l'unité, et tel que  $f$  soit scindé, on a  $\dim J(K)[\phi] = 3$ .

En effet, comme  $\phi^2 = -3\zeta$ , et  $\dim J[3] = 6$ , on a  $\dim J[\phi] = 3$ .

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

LEMME 5.1. *On a alors  $\dim J(K)[\phi]/\phi(J(K)[3]) = 6 - \dim(J(K)[3])$ .*

En effet,  $J(K)[\phi]/\phi(J(K)[3])$  s'injecte dans  $J(K)/\phi J(K)$  qui s'injecte à son tour dans  $(K^*/K^{*3})^4$ , et si  $J(K)[3] = (\mathbb{Z}/3\mathbb{Z})^r$ , comme  $J[\phi] \subset J(K)[3]$ , on a  $\phi(J(K)[3]) = (\mathbb{Z}/3\mathbb{Z})^{r-3}$  et donc  $J(K)[\phi]/\phi(J(K)[3]) = (\mathbb{Z}/3\mathbb{Z})^{6-r}$ .

**6. Descente explicite.** Nous connaissons la structure de  $W$  pour  $\beta = 1/2$ . Pour connaître la structure de  $W$  dans le cas général, nous allons la déterminer dans un autre cas particulier, ce qui nous permettra, en utilisant un argument de spécialisation, de conclure.

Soit  $K$  un corps de nombre contenant  $\mathbb{Q}(\sqrt{-3})$ . Notons

$$\zeta = -\frac{1 + \sqrt{-3}}{2}.$$

**6.1. Spécialisation en  $\beta = 1/2$ .** Lorsque  $\beta$  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  $(x, y) \mapsto (2x - 1, 4^{2/3}y)$ , 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  $W_{C_{1/2}} = W_{C_{1/2}}(\mathbb{Q}(\zeta_{12})) \cong (\mathbb{Z}/4\mathbb{Z})^2 \times (\mathbb{Z}/3\mathbb{Z})^5$ . 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 2.3, pour toute courbe  $C_\beta$ , 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  $(\mathbb{Z}/4\mathbb{Z})^2$ .

**6.2. Spécialisation en  $t = 7$ .** Nous allons montrer dans cette partie que pour certaines valeurs de  $\beta$ , il n'existe pas d'autres relations entre les générateurs de  $W$  que celles que nous avons déjà obtenues dans la partie 4. Plus précisément, lorsque  $\beta_0 = 784/6859$  (qui correspond à  $t = 7$ ), nous avons le résultat suivant :

PROPOSITION 6.1. *Pour  $\beta_0 = 784/6859$ , le groupe engendré par les points de Weierstrass est  $W_{C_{\beta_0}} = \mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5$ .*

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  $(x, y) \mapsto (2x, 2y\sqrt[3]{2})$  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  $2t_2 = \frac{1568}{6859} + \frac{2520}{6859}\sqrt{-3}$ .

Par abus de notation, on note encore  $P_{i,j}$  les points après changement de coordonnées. Soit  $P_\beta$  un point d'abscisse  $\beta$  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  $P_\beta$  son image après changement de coordonnées. Le point  $P_\beta$  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  $u = 196/(196 + 3\sqrt[3]{1470^2})$ . 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  $\mathfrak{ef}$  et 19 se décompose en  $\mathfrak{ab}$ . 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  $(x - T)_K : J(K) \rightarrow K[T]/(g(T))$  :

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

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. D’après le corollaire 5.1,  $\dim(J(K)[3]) = 4$ .

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  $(x - T)_{K(\sqrt[3]{105})} : J(K(\sqrt[3]{105})) \rightarrow K(\sqrt[3]{105})[T]/(g(T))$  des points engendrant  $W_1$  ainsi que celle de  $P_\beta$ .

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

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. Comme lorsqu’on spécialise en  $\beta_0 = 1/2$ , ils deviennent des points d’ordre 4, 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  $J[\phi]$ . De même que précédemment, nous avons, en appliquant le corollaire 5.1,  $\dim(J(K(\sqrt[3]{105}))[3]) = 4$ , et donc, nous avons le résultat suivant :

LEMME 6.2. *Les points de torsion d’ordre 3 de  $J(K(\sqrt[3]{105}))$  sont dans  $W_1$ .*

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 6.3. 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  $\sigma \in \text{Gal}(\bar{k}/k)$  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.  $\text{div}(g) = {}^\sigma P - P - {}^\sigma Q + Q$ . On a un morphisme de degré  $\leq 2$ ,  $\bar{g} : \mathcal{C} \rightarrow \mathbb{P}^1$ , 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  $(\mathbb{Z}/3\mathbb{Z})^5 \subset W$ .

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 avons déjà au paragraphe 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 6.4. 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  $((x - T)_{K(\sqrt[3]{105})}(P_\beta))^{r_1 + r_2}$  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  $P_\beta$ . Dans le cas contraire,

c'est-à-dire lorsque  $ef \equiv u_1 \pmod{K(\sqrt[3]{105})^*{}^3}$ ,  $5 \equiv u_2 \pmod{K(\sqrt[3]{105})^*{}^3}$  et  $\sqrt{-3} \equiv u_3 \pmod{K(\sqrt[3]{105})^*{}^3}$  (où les  $u_i$  sont des unités), les images par  $x - T$  de  $P_\beta$  et des points engendrant  $W_1$  deviennent dans  $K(\sqrt[3]{105})^*/K(\sqrt[3]{105})^*{}^3$  :

	$x - 0$	$x - 2$	$x - 2t_1$	$x - 2t_2$
$[(0, 0) - P_\infty]$	$4u_1$	$2$	$u_1$	$u_1$
$[(2, 0) - P_\infty]$	$2$	$u_2u_3^2$	$2u_2u_3^2$	$2u_2u_3^2$
$[P_{1,1} - P_{2,1}]$	$u_1^2$	$u_2u_3$	$u_2u_3u_1^2\zeta$	$u_2u_3u_1^2\zeta^2$
$[P_\beta - P_\infty]$	$4u_1^2$	$2u_2^2u_3$	$u_1u_2u_3^2$	$u_1u_2u_3^2$

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  $N(a) = \zeta^\epsilon x = \zeta^\epsilon a^3$ . Or cette équation n'a pas de solution  $a \in K(\sqrt[3]{105})$  pour  $x = 7$ .

Dans les deux cas, on conclut 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 6.5.** *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  $3 \nmid \text{pcgd}(m_1, m_2)$ .

*1er cas :*  $k = 0$ . 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  $r_1 = 0$  ou  $r_2 = 0$  on a  $r_iP_{4,i} \in J(K(\sqrt[3]{105}))$ , ce qui est faux.
- Si  $r_1 = r_2 = \pm 1$  on a  $P_{4,1} + P_{4,2} = -P_{4,3} \in J(K(\sqrt[3]{105}))$ , ce qui est faux.
- Si  $r_1 + r_2 = 0$  on a  $P_{4,1} - P_{4,2} \in J(K(\sqrt[3]{105}))$ , ce qui est exclu par le lemme 6.3.

*2ème cas :*  $k > 0$ . Cela revient à supposer que  $3^{k-1}(m_1P_{\beta,1} + m_2P_{\beta,2}) \in W_1 \subset J(K)$ , avec  $3 \nmid \text{pcgd}(m_1, m_2)$ . En appliquant le lemme 6.6, on peut supposer que  $m_1P_{\beta,1} + m_2P_{\beta,2} \in W_1$ . 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  $r_i \in \{0, \pm 1\}$ .

- Le cas  $r_1 + r_2 \neq 0$  n'est pas possible par le lemme 6.4.
- Si  $r_1 + r_2 = 0$ , 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 6.6, 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 6.6. *Si  $P \in J(K(\sqrt[3]{105}))$  est tel que  $3P \in W_1$ , alors  $3P$  est de la forme  $m_0(P_0 + P_1 - P_{t_1}) + m_3(P_{1,1} - P_{1,2}) + 3m'_4P_{1,2}$  et est donc déjà dans le noyau de  $(x - T)_K$ .*

*Démonstration.* Comme  $3P$  est dans  $W_1$ , on a une relation du type  $3P = m_0P_0 + m_1P_1 + m_2P_{t_1} + m_3P_{1,1} + m_4P_{1,2} + m_5(P_{1,1} - P_{2,1})$ .

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  $2^{2m_0+m_1}(ef)^{m_0+m_2+2m_5}(ab)^{2(m_3+m_4)} \equiv 1 \pmod{K(\sqrt[3]{105})^*{}^3}$ . Comme 2,  $a$ ,  $b$  et 7 ne sont pas des cubes dans  $K(\sqrt[3]{105})$ , cela entraîne que  $m_0 \equiv m_1 \pmod{3}$ ,  $m_3+m_4 \equiv 0 \pmod{3}$  et  $m_5 \equiv m_0+m_2 \equiv m_1+m_2 \pmod{3}$ . Les deuxième et troisième coordonnées doivent donc vérifier  $2^{m_0+m_2}5^{2(m_1+m_2)} \equiv 1 \pmod{K(\sqrt[3]{105})^*{}^3}$  et  $2^{m_1+m_2}5^{2(m_1+m_2)}\zeta^{m_0+m_2} \equiv 1 \pmod{K(\sqrt[3]{105})^*{}^3}$ . Les  $m_i$  doivent donc satisfaire les relations de congruence suivantes :  $m_0 \equiv m_1 \equiv -m_2 \pmod{3}$ ,  $m_3 + m_4 \equiv 0 \pmod{3}$  et  $m_5 \equiv 0 \pmod{3}$ . Ces relations ont pour conséquence que le point  $3P$  est déjà dans le noyau de  $(x - T)_K$ . ■

Montrons :

LEMME 6.7. *Si  $P \in J(K(\sqrt[3]{105}))$  est tel que  $3P$  appartient à  $W_1$ , alors  $P \in W_1$ .*

*Démonstration.* On sait déjà par le lemme précédent que  $3P = m_0(P_0 + P_1 - P_{t_1}) + m_3(P_{1,1} - P_{1,2}) + 3m'_4P_{1,2}$  est dans le noyau de  $(x - T)_K$ , à savoir que  $3P \in (1 - \zeta)J(K)$ .

*1er cas :*  $P \in J(K(\sqrt[3]{105})) \setminus J(K)$ . Comme  $(1 - \zeta)^2 = -3\zeta$  dans  $\text{End}(J)$ , cela revient à  $(1 - \zeta)^2P \in (1 - \zeta)J(K)$ , 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 6.3.

*2ème cas :*  $P \in J(K)$ . 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  $(1 - \zeta)P = -m_3P_{1,2} + m'_4P_{1,2} - m'_4P_{1,3} + T$  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  $(1 - \zeta)P = m'_4P_{1,1} + (2m'_4 - m_3)P_{1,2} + T$ . Les points  $P_{1,1}$  et  $P_{1,2}$  ayant la même image par  $(x - T)_K$ , on a  $3m'_4 - m_3 \equiv 0 \pmod{3}$ , 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 6.6.

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 6.2. ■

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 4.

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

**COROLLAIRE 6.8.** *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 4.1), et comme  $W_{\mathcal{C}_{\beta_0}}$  est un quotient de  $W_{\mathcal{C}_\eta}$  (d'après la proposition 6.1), on en déduit que  $W_{\mathcal{C}_\eta} \cong \mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5$ . ■

## 7. Conséquences

**7.1. Preuve du théorème 1.1.** Pour déduire la structure de  $W_{\mathcal{C}_\beta}$  dans le cas général, nous avons besoin d'appliquer un théorème dû à Silverman.

**THÉORÈME 7.1** ([Sil]). *Soit  $A \rightarrow C$  une famille (plate) de variétés abéliennes toutes définies sur un corps global  $K$ , où  $C$  est une courbe projective lisse. En un point  $t \in C(\bar{K})$  pour lequel la fibre  $A_t$  est non-singulière, on définit l'application de spécialisation  $\sigma_t : A(C) \rightarrow A_t(\bar{K})$ ,  $P \mapsto P_t$ .*

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

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

Nous allons appliquer ce théorème avec  $A = \text{Jac}(\mathcal{C}_\beta)$ ,  $C = \mathbb{P}^1$  (ici, paramétrée par  $\beta$ ). Nous devons donc vérifier qu'il n'y a pas de partie constante. Notons  $J_\beta$  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  $\mathcal{C}/\mathbb{Q}(\beta) \xrightarrow{\phi_\beta} A_0$ , où  $\phi_\beta$  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  $\mathcal{S} \cdots \rightarrow A_0$ . On en déduit une application non-constante  $\mathbb{P}^2 \cdots \rightarrow A_0$ , 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 6.8), on en déduit que pour presque tout  $\beta$ ,  $W_{\mathcal{C}_\beta} = \mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5$ .

**7.2. Preuve du corollaire 1.2.** Cela nous permet de démontrer le corollaire 1.2, dont nous rappelons l'énoncé :



COROLLAIRE 1.2. *Soit une famille de courbes lisses joignant une courbe hyperelliptique à une courbe  $C_\beta$  pour laquelle  $W_{C_\beta} = \mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5$ . Soit  $W_{C_\eta}$  le groupe engendré par les points de Weierstrass de la fibre générique. On a alors  $W_{C_\eta} \cong \mathbb{Z}^r$  avec  $9 \leq r \leq 23$ .*

*Démonstration.* En effet, la spécialisation  $W_{C_\eta} \rightarrow W_s$  étant injective sur la partie de torsion, si  $W_{C_\eta} = \mathbb{Z}^r \times G$ , où  $G$  est un groupe fini, on a pour un  $s$  correspondant à la courbe  $W_{C_\beta}$ ,  $G \hookrightarrow (\mathbb{Z}/3\mathbb{Z})^5$ , 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  $W_{C_\eta} \rightarrow \mathbb{Z}^4 \times (\mathbb{Z}/3\mathbb{Z})^5$  est surjective (prop. 2.3), on a  $r \geq 9$ . ■

REMARQUE. Si  $C_\eta$  est la courbe de genre 3 générique, on obtient de même que  $W_{C_\eta} \cong \mathbb{Z}^r$  avec  $9 \leq r \leq 23$ .

### Références

- [ACGH] E. Arbarello, M. Cornalba, P. A. Griffiths and J. Harris, *Geometry of Algebraic Curves*, Vol. I, Springer, New York, 1985.
- [HS] M. Hindry and J. H. Silverman, *Diophantine Geometry, An Introduction*, Grad. Texts in Math. 201, Springer, New York, 2000.
- [Hub] J. H. Hubbard, *Sur les sections analytiques de la courbe universelle de Teichmüller*, Mem. Amer. Math. Soc. 166 (1976).
- [KS] M. J. Klassen and E. F. Schaefer, *Arithmetic and geometry of the curve  $y^3 + 1 = x^4$* , Acta Arith. 74 (1996), 241–257.
- [LT] D. Laksov and A. Thorup, *Weierstrass points and gap sequences for families of curves*, Ark. Mat. 32 (1994), 393–422.
- [Mil] J. S. Milne, *Abelian varieties*, in: Arithmetic Geometry, G. Cornell and J. Silverman (eds.), Springer, 1986, 103–150.
- [Mum] D. Mumford, *Tata Lectures on Theta. II*, Birkhäuser, Boston, MA, 1984.
- [Mur] V. K. Murty, *Introduction to Abelian Varieties*, Amer. Math. Soc., Providence, RI, 1993.
- [Pra] D. T. Prapavessi, *On the Jacobian of the Klein curve*, Proc. Amer. Math. Soc. 122 (1994), 971–978.
- [Roh] D. E. Rohrlich, *Points at infinity on the Fermat curves*, Invent. Math. 39 (1977), 95–127.
- [Sch] E. F. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann. 310 (1998), 447–471.
- [Sil] J. H. Silverman, *Heights and the specialization map for families of abelian varieties*, J. Reine Angew. Math. 342 (1983), 197–211.

Théorie des Nombres  
 Institut de Mathématiques de Jussieu  
 175, rue du Chevaleret, 75013 Paris, France  
 E-mail: girard@math.jussieu.fr

Reçu le 14.6.2000  
 et révisé le 18.2.2002

(3839)