Multiplication complexe et équivalence élémentaire dans le langage des corps

Xavier VIDAUX

Journal of Symbolic Logic 67 (2002), n2, pp 635-648

Résumé. Soit K et K' deux corps elliptiques avec multiplication complexe sur un corps algébriquement clos k de caractéristique 0, non k-isomorphes, et soit C et C' deux courbes ayant pour corps de fonctions K et K' respectivement. Nous démontrons que si les anneaux d'endomorphismes de C et de C' ne sont pas isomorphes, alors K et K' ne sont pas élémentairement équivalents dans le langage des corps enrichi d'une seule constante (l'invariant modulaire). Ce travail fait suite à un travail de David A. Pierce qui se place dans le langage des k-algèbres.

-Classification AMS : 03C

Complex multiplication and elementary equivalence in the language of fields

Abstract. Let K and K' be two elliptic fields with complex multiplication over an algebraically closed field k of characteristic 0, non k-isomorphic, and let C and C' be two curves with respectively K and K' as function fields. We prove that if the endomorphism rings of the curves are not isomorphic then K and K' are not elementarily equivalent in the language of fields expanded with a constant symbol (the modular invariant). This theorem is an analogue of a theorem from David A. Pierce in the language of k-algebras.

1 Contexte et notations

Nous considérons un corps algébriquement clos k. Un *corps de courbe sur* k est une extension finiment engendrée de degré de transcendance 1 sur k. Pour tout

sous-ensemble A de k, $\mathcal{L}(A)$ désigne le langage des corps enrichi de symboles de constantes pour les éléments de A. Dans [3], Jean-Louis Duret propose les deux conjectures, très liées, suivantes. :

(C1) *Soit K un corps de courbe sur k. Il existe un sous-ensemble fini A de k tel que tout corps de courbe sur k élémentairement équivalent à K dans le langage $\mathcal{L}(A)$ lui est k-isomorphe.*

(C2) *Deux corps de courbe sur k sont élémentairement équivalents dans le langage des corps si et seulement s'ils sont isomorphes.*

Les courbes se classent en géométrie algébrique à équivalence birationnelle près. Les conjectures affirment que la classification des corps de courbes à équivalence élémentaire près correspond à la classification de la géométrie algébrique. On peut rapprocher de ce travail l'article [1], où les auteurs étudient si l'élémentaire équivalence des anneaux de fonctions analytiques sur différents domaines entraîne l'isomorphisme de ces domaines.

J.-L. Duret (voir [3]) a prouvé les deux conjectures lorsque K est un corps de courbe de genre différent de 1, quelque soit la caractéristique de k, et, si la caractéristique de k est 0, lorsque le corps K est de genre 1 et sans multiplication complexe. L'objet de cet article est d'étudier la conjecture (C1) dans le cas où le corps k est de caractéristique 0, et le corps de courbe K est de genre 1 avec multiplication complexe (CM1). La spécificité des corps de courbe qui ont une multiplication complexe fait apparaître de nouvelles difficultés. Nous démontrons le théorème suivant.

Théorème principal *Soit k un corps algébriquement clos de caractéristique 0. Soient K et K' des corps de courbe elliptique sur k, le corps K étant avec multiplication complexe et d'invariant modulaire j. Soit $\mathcal{L}(j)$ le langage des corps enrichi d'un symbole de constante pour j. Soient E et E' des courbes dont les corps de fonctions sont respectivement K et K'. Si les corps K et K' sont élémentairement équivalents dans le langage $\mathcal{L}(j)$, alors les courbes E et E' ont des anneaux d'endomorphismes isomorphes.*

Ce théorème ne démontre pas (CM1), car il existe des courbes ayant le même anneau d'endomorphisme mais des corps de fonctions non k-isomorphes (voir exemples 20). Un théorème analogue a été démontré par D. A. Pierce dans le langage des k-algèbres (voir [7]). Pour pouvoir passer du langage des k-algèbres au langage $\mathcal{L}(j)$, et donc prouver ce théorème, nous avons du rendre effective la démonstration de D. A. Pierce. Pour cela, nous utilisons de nombreuses techniques et résultats des

articles [2], [3], [7], et à moindre mesure, de [9].

Nous avions remarqué, dans [9], qu'il suffit de démontrer (CM1) lorsque k est un sous-corps de $\mathbf{C}$, et pour une famille de corps K dépendant de deux paramètres : un entier $n \in \mathbf{N}$ et un nombre complexe algébrique quadratique τ. Ceci nous permet d'utiliser des techniques de la théorie des courbes elliptiques sur le corps des nombres complexes. En particulier, nous utiliserons, sans le rappeler, que la catégorie des courbes elliptiques est équivalente à la catégorie des réseaux (voir [8, chap. VI, thm. 5.3, p. 162]).

Nous nous référons à [5], [6] et [8] pour la théorie des courbes elliptiques.

Si ω_1 et ω_2 sont des nombres complexes $\mathbf{R}$-linéairement indépendants, notons

$$\langle \omega_1, \omega_2 \rangle = \{\lambda\omega_1 + \mu\omega_2 \mid \lambda, \mu \in \mathbf{Z}\}$$

le réseau de $\mathbf{C}$ ayant pour base (ω_1, ω_2). Étant donné un réseau Λ, nous noterons $\mathcal{P}(., \Lambda)$ la fonction de Weierstrass du réseau Λ :

$$\mathcal{P}(z, \Lambda) = \frac{1}{z^2} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right].$$

Nous noterons $\mathcal{P}'(., \Lambda)$ la dérivée de $\mathcal{P}(., \Lambda)$. Pour $i = 2, 3$, nous noterons $g_i(\Lambda)$ les nombres complexes tels que

$$\mathcal{P}'(., \Lambda)^2 = 4\mathcal{P}(., \Lambda)^3 - g_2(\Lambda)\mathcal{P}(., \Lambda) - g_3(\Lambda).$$

Si τ est un nombre complexe algébrique quadratique et $n \geq 1$ un entier, nous noterons

$$\Lambda_n^\tau = \langle \frac{1}{n}, \tau \rangle,$$

et $\mathcal{P}_n^\tau$ la fonction de Weierstrass de Λ_n^τ. Si k est un corps, notons $cl.a.(k)$ sa clôture algébrique. Nous rappelons que (voir [5, pp. 316-336]) pour tout corps de courbe elliptique K, d'invariant modulaire j, sur un corps algébriquement clos k de caractéristique 0 sous-corps de $\mathbf{C}$, il existe u et v dans K et des éléments a et b de k tels que $v^2 = 4u^3 - au - b$. Mais nous avons

$$j = 1728 \frac{a^3}{a^3 - 27b^2} \in k.$$

Il s'ensuit que le corps k contient $cl.a.(\mathbf{Q}(j))$. Notons j_τ l'invariant modulaire de la courbe elliptique associée à $\frac{\mathbf{C}}{\Lambda_1^\tau}$ et

$$\Delta_\tau = cl.a.(\mathbf{Q}(j_\tau)).$$

Enfin, notons $\mathcal{L}$ le langage des corps et $\mathcal{L}(j_\tau)$ le langage des corps ayant j_τ comme symbole de constante supplémentaire.

Si τ est un nombre complexe algébrique quadratique, k un sous-corps de $\mathbf{C}$ algébriquement clos contenant Δ_τ, et $n > 1$ un entier, soit $\mathbf{P}_n^\tau(k)$ la propriété : *les corps elliptiques $k(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau\prime})$ et $k(\mathcal{P}_1^\tau, \mathcal{P}_1^{\tau\prime})$ ne sont pas élémentairement équivalents dans le langage $\mathcal{L}(j_\tau)$.* Si K est un corps de courbe de genre 1 sur un corps algébriquement clos k de caractéristique 0, avec multiplication complexe et d'invariant modulaire j, et K' un corps de courbe sur k non isomorphe à K, soit $\mathbf{P}_k(K, K')$ la propriété : *les corps elliptiques K et K' ne sont pas élémentairement équivalents dans le langage $\mathcal{L}(j)$.*

Proposition 1 . *Si la propriété $\mathbf{P}_n^\tau(k)$ est vraie pour tout triplet (k, τ, n), alors la propriété $\mathbf{P}_k(K, K')$ est vraie pour tout triplet (k, K, K').*

Démonstration : Voir [9, prop. 6]. □

Dans toute la section 2, le corps k et le nombre τ seront fixés, il n'est donc plus nécessaire de les faire apparaître dans les notations.

2 Résultat principal

Pour tout entier $n \geq 1$, notons E_n le quotient $\frac{\mathbf{C}}{\Lambda_n}$ et C_n la courbe elliptique associée à E_n (voir [8, chap. VI, thm. 5.3, p. 162]). Pour des entiers naturels a, b et p, $p \neq 0$, notons :

$$\begin{aligned}
\Lambda_{a,b}^n &= \langle \frac{1}{n}, \frac{a}{pn} + \frac{b\tau}{p} \rangle \quad \text{si} \quad b \neq 0 \qquad \text{et} \quad \Lambda_{a,0}^n = \langle \frac{a}{pn}, \tau \rangle, \\
\mathcal{I}_p &= \{(a,b) \in \mathbf{N}^2 - \{(0,0)\} \mid 0 \leq a \leq p-1 \quad \text{et} \quad 0 \leq b \leq p-1\}, \\
E_{a,b}^n &= \frac{\mathbf{C}}{\Lambda_{a,b}^n}.
\end{aligned}$$

Soit $C_{a,b}^n$ la courbe elliptique associée à $E_{a,b}^n$.

Lemme 2 . *Soit p un nombre premier et soit G un sous-groupe d'ordre p de E_n. Alors il existe un couple $(a,b) \in \mathcal{I}_p$ tel que :*

$$G = \frac{\Lambda_{a,b}^n}{\Lambda_n \bigcap \Lambda_{a,b}^n}.$$

En particulier, il n'y a qu'un nombre fini de sous-groupes d'ordre p de E_n.

Démonstration : Les points d'ordre p de E_n sont précisément les points de la forme :

$$T_{a,b} = \frac{a}{pn} + \frac{b\tau}{p} + \Lambda_n$$

avec $(a,b) \in \mathcal{I}_p$. Soit $G^n_{a,b}$ le groupe engendré par $T_{a,b}$. Nous avons alors :

$$\frac{\Lambda^n_{a,b}}{\Lambda_n \bigcap \Lambda^n_{a,b}} = \begin{cases} \frac{\langle \frac{1}{n}, \frac{a}{pn} + \frac{b\tau}{p} \rangle}{\langle \frac{1}{n}, \tau \rangle \bigcap \langle \frac{1}{n}, \frac{a}{pn} + \frac{b\tau}{p} \rangle} = \{k(\frac{a}{pn} + \frac{b\tau}{p}) + \langle \frac{1}{n}, \tau \rangle \mid k = 1, \ldots, p\} = G^n_{a,b} \text{ si } b \neq 0 \\ \frac{\langle \frac{a}{pn}, \tau \rangle}{\langle \frac{1}{n}, \tau \rangle \bigcap \langle \frac{1}{n}, \frac{a}{pn} + \frac{b\tau}{p} \rangle} = \{k(\frac{a}{pn}) + \langle \frac{1}{n}, \tau \rangle \mid k = 1, \ldots, p\} = G^n_{a,0} \qquad \text{sinon.} \end{cases}$$

□

Si C et C' sont des courbes elliptiques, une isogénie entre C et C' est un morphisme de groupes algbriques entre C et C'. Si ϕ est une isogénie, nous noterons $\deg(\phi)$ son degré (voir [8, chap. III, §4]).

Lemme 3 . *Soit $\phi : C_1 \xrightarrow{\times \alpha^{-1}} C_n$ une isogénie (α^{-1} étant le nombre complexe associé). Soit p un nombre premier tel que p divise le degré de ϕ. Alors il existe un réseau $\Lambda^n_{a,b}$ tel que ϕ se factorise de la manière suivante :*

$$C_1 \xrightarrow[\times (p\alpha)^{-1}]{\lambda} C^n_{a,b} \xrightarrow[\times p]{\psi} C_n$$

où ψ est une isogénie de degré p.

Démonstration : Soit $\widehat{\phi} : C_n \to C_1$ l'isogénie duale de ϕ, et soit d le degré de ϕ ; $\widehat{\phi}$ est donc associée au nombre complexe $d\alpha$, car $\widehat{\phi} \circ \phi$ correspond à la multiplication par d. Soient $f : E_1 \xrightarrow{\times \alpha^{-1}} E_n$ et $\widehat{f} : E_n \xrightarrow{\times d\alpha} E_1$ les morphismes de groupes associés respectivement aux isogénies ϕ et $\widehat{\phi}$. Nous avons :

$$|\ker \widehat{f}| = \deg \widehat{\phi} = \deg \phi = |\ker f| = \left| \frac{\alpha \Lambda_n}{\Lambda_1} \right| = \left| \frac{\Lambda_n}{\alpha^{-1} \Lambda_1} \right| = |\alpha^{-1}|^2 \times \left| \frac{\langle \frac{1}{n}, \tau \rangle}{\langle 1, \tau \rangle} \right| = n |\alpha^{-1}|^2.$$

Voir [6, chap. 2, §2 et 3] pour l'avant-dernière egalité. Comme p divise le degré de ϕ, p divise aussi $|\ker \widehat{f}|$, donc $\ker \widehat{f}$ contient un sous-groupe d'ordre p, qui est donc d'après le lemme 2 de la forme $G^n_{a,b} = \frac{\Lambda^n_{a,b}}{\Lambda_n \bigcap \Lambda^n_{a,b}}$ avec $(a,b) \in \mathcal{I}_p$. Le morphisme de groupes $\widehat{f}$ se factorise donc de manière canonique (ligne du haut) :

$$\begin{array}{ccccc} E_n & \xrightarrow{\widehat{pr}} & \frac{E_n}{G^n_{a,b}} & \xrightarrow{\widehat{l}} & E_1 \\ & & i \downarrow \simeq & & \\ & & E^n_{a,b} & & \end{array}$$

où $\widehat{pr}$ est la projection canonique et donc

$$|\ker \widehat{pr}| = |G_{a,b}^n| = p.$$

Soit

$$\widehat{\psi}\colon C_n \longrightarrow C_{a,b}^n \qquad \text{et} \qquad \widehat{\lambda}\colon C_{a,b}^n \longrightarrow C_1$$

les morphismes de courbes associés respectivement à $i \circ \widehat{pr}$ et à $\widehat{l} \circ i^{-1}$. Nous obtenons alors une factorisation de $\widehat{\phi}$:

$$C_n \xrightarrow[\times 1]{\widehat{\psi}} C_{a,b}^n \xrightarrow[\times d\alpha]{\widehat{\lambda}} C_1$$

avec

$$\deg \widehat{\psi} = |\ker (i \circ \widehat{pr})| = |\ker \widehat{pr}| = p.$$

Donc si nous notons ψ le morphisme dual de $\widehat{\psi}$, ψ correspond à la multiplication par p. Nous notons de même λ le morphisme dual de $\widehat{\lambda}$. Nous avons donc la factorisation désirée pour ϕ :

$$C_1 \xrightarrow[\times (p\alpha)^{-1}]{\lambda} C_{a,b}^n \xrightarrow[\times p]{\psi} C_n.$$

□

Lemme 4 *Nous avons les propriétés suivantes, dites* propriétés d'homogénéité *:*

$$\mathcal{P}(cz, c\Lambda) = \frac{1}{c^2}\mathcal{P}(z, \Lambda), \qquad \mathcal{P}'(cz, c\Lambda) = \frac{1}{c^3}\mathcal{P}(cz, c\Lambda),$$
$$g_2(c\Lambda) = \frac{1}{c^4} g_2(\Lambda), \qquad g_3(c\Lambda) = \frac{1}{c^6} g_3(\Lambda).$$

Démonstration : Voir par exemple [6, chap. 1, §4, pp. 16-17]. □

Nous noterons $\mathcal{E}(\Lambda)$ le corps des fonctions méromorphes ayant pour ensemble de périodes Λ. Nous avons l'égalité suivante (voir [6, chap. 1, §2, thm. 4]) :

$$\mathcal{E}(\Lambda) = \mathbf{C}(\mathcal{P}(., \Lambda), \mathcal{P}'(., \Lambda)).$$

En termes de corps, nous obtenons, d'après le lemme 3, une factorisation du morphisme de corps $\phi^*\colon \mathcal{E}(\Lambda_n) \longrightarrow \mathcal{E}(\Lambda_1)$,

$$\mathcal{E}(\Lambda_n) \xrightarrow{\psi^*} \mathcal{E}(\Lambda_{a,b}^n) \xrightarrow{\lambda^*} \mathcal{E}(\Lambda_1) \qquad (\bigstar)$$

où :

$$(\phi^* f)(z) = f(\frac{z}{\alpha}), \quad (\psi^* f)(z) = f(pz) \quad \text{et} \quad (\lambda^* f)(z) = f(\frac{z}{p\alpha}).$$

Lemme 5 *L'image de ψ^* est*

$$\psi^*\mathcal{E}(\Lambda_n) = \mathcal{E}(\frac{1}{p}\Lambda_n).$$

Démonstration : Si $f \in \mathcal{E}(\Lambda_n)$, nous avons, pour tous entiers $r, s \in \mathbf{Z}$:

$$\psi^* f(z + \frac{1}{p}(\frac{r}{n} + s\tau)) = f(pz + \frac{r}{n} + s\tau) = f(pz) = \psi^* f(z),$$

donc $\psi^* f \in \mathcal{E}(\frac{1}{p}\Lambda_n)$. Nous obtenons ainsi l'inclusion $\psi^*\mathcal{E}(\Lambda_n) \subset \mathcal{E}(\frac{1}{p}\Lambda_n)$.

Réciproquement, si $g \in \mathcal{E}(\frac{1}{p}\Lambda_n)$, soit f la fonction méromorphe définie par $f(z) = g(\frac{z}{p})$. Nous avons alors $\psi^* f(z) = f(pz) = g(z)$ et, pour tous entiers $r, s \in \mathbf{Z}$:

$$f(z + \frac{r}{n} + s\tau) = g(\frac{z}{p} + \frac{1}{p}(\frac{r}{n} + s\tau)) = g(\frac{z}{p}) = f(z),$$

donc $f \in \mathcal{E}(\Lambda_n)$. Ceci démontre l'inclusion réciproque. □

Etudions l'extension $\mathcal{E}(\frac{1}{p}\Lambda_n) \subset \mathcal{E}(\Lambda^n_{a,b})$. Pour cela, nous avons besoin du lemme préliminaire suivant :

Lemme 6 . *Soient Λ et Λ' deux réseaux tels que Λ soit sous-réseau de Λ'. Alors $g_2(\Lambda')$ et $g_3(\Lambda')$ sont algébriques sur $\mathbf{Q}(g_2(\Lambda), g_3(\Lambda))$.*

Démonstration : D'après [4, §63, p. 132], il existe une base (ω_1, ω_2) de Λ, et des entiers $r, s \in \mathbf{N}$ non nuls, tels que $(\frac{\omega_1}{rs}, \frac{\omega_2}{r})$ soit une base de Λ'. Notons Λ_s le réseau $\langle \frac{\omega_1}{s}, \omega_2 \rangle$. Nous considérons le diagramme suivant :

$$\begin{array}{ccc}
\Lambda & \subset & \Lambda' \\
\shortparallel & & \shortparallel \\
\langle \omega_1, \omega_2 \rangle & \subset & \langle \frac{\omega_1}{rs}, \frac{\omega_2}{r} \rangle \\
\cap & & \cup \\
\langle \frac{\omega_1}{s}, \omega_2 \rangle & = & \langle \frac{\omega_1}{s}, \omega_2 \rangle \\
\shortparallel & & \shortparallel \\
\Lambda_s & & \Lambda_s
\end{array}$$

Nous savons que $g_i(\Lambda_s)$, pour $i = 2, 3$, est algébrique sur $\mathbf{Q}(g_2(\Lambda), g_3(\Lambda))$ (voir [3, prop. 31, p. 816]). D'après le lemme 4, nous avons : $g_i(\Lambda') = r^{2i} g_i(\Lambda_s)$, pour $i = 2, 3$, donc $g_i(\Lambda')$, pour $i = 2, 3$, est aussi algébrique sur $\mathbf{Q}(g_2(\Lambda), g_3(\Lambda))$. □

Pour un réseau Λ, si j_Λ désigne l'invariant modulaire de la courbe elliptique associée à $\frac{\mathbf{C}}{\Lambda}$, nous avons :

$$cl.a.(\mathbf{Q}(g_2(\Lambda), g_3(\Lambda))) = cl.a.(\mathbf{Q}(j_\Lambda)).$$

Voir par exemple [5, pp. 316-336]. Notons

$$j = j_{\Lambda_1} \qquad \text{et} \qquad \Delta = cl.a.(\mathbf{Q}(j)).$$

Corollaire 7 . *Les nombres complexes $g_2(\Lambda^n_{a,b})$ et $g_3(\Lambda^n_{a,b})$ sont éléments de Δ.*

Démonstration : L'égalité

$$\lambda^* \mathcal{E}(\Lambda^n_{a,b}) = \mathcal{E}(p\alpha\Lambda^n_{a,b})$$

se démontre de façon analogue à la démonstration du lemme 5. Donc nous avons, d'après ($\bigstar$),

$$\mathcal{E}(p\alpha\Lambda^n_{a,b}) \subset \mathcal{E}(\Lambda_1),$$

ou, en termes de réseaux :

$$\Lambda_1 \subset p\alpha\Lambda^n_{a,b}.$$

Donc par le lemme 6, pour $i = 2, 3$, le nombre $g_i(p\alpha\Lambda^n_{a,b})$ est algébrique sur

$$\mathbf{Q}(g_2(\Lambda_1), g_3(\Lambda_1)).$$

Mais nous avons, d'après le lemme 4,

$$g_i(p\alpha\Lambda^n_{a,b}) = (\frac{1}{p\alpha})^{2i} g_i(\Lambda^n_{a,b}), \quad \text{pour} \quad i = 2, 3.$$

D'après ($\bigstar$), le nombre α^{-1} est élément de $\mathrm{Hom}\,(E_1, E_n)$, donc d'après la proposition 15 (voir section 3), α est algébrique sur $\mathbf{Q}$. Par conséquent, $g_2(\Lambda^n_{a,b})$ et $g_3(\Lambda^n_{a,b})$ sont algébriques sur $\mathbf{Q}(g_2(\Lambda_1), g_3(\Lambda_1))$. □

Notons $\mathcal{P}^n_{a,b}$ la fonction de Weierstrass du réseau $\Lambda^n_{a,b}$.

Lemme 8 . *Il existe une fraction rationnelle F, à coefficients dans Δ, telle que :*

$$\psi^* \mathcal{P}_n = F(\mathcal{P}^n_{a,b}).$$

Démonstration : D'après le lemme 5 et ($\bigstar$), nous avons

$$\psi^* \mathcal{E}(\Lambda_n) = \mathcal{E}(\frac{1}{p}\Lambda_n) \subset \mathcal{E}(\Lambda^n_{a,b}),$$

et donc le réseau $\Lambda_{a,b}^n$ est inclus dans le réseau $\frac{1}{p}\Lambda_n$. Nous ne pouvons pas pour l'instant appliquer [3, prop. 30, p. 815], mais nous nous y ramenons en constatant la présence d'un réseau intermédiaire Γ; dans les deux cas : $b = 0$ et $b \neq 0$;

$$\begin{array}{lccccccc} \text{si } b=0 & \Lambda_{a,b}^n & = & \langle \frac{a}{np}, \tau \rangle & \subset & \langle \frac{1}{np}, \frac{\tau}{p} \rangle & = & \frac{1}{p}\Lambda_n \\ & & & \cap & & \cup & & \\ & \Gamma & = & \langle \frac{a}{np}, \frac{\tau}{p} \rangle & = & \langle \frac{a}{np}, \frac{\tau}{p} \rangle & = & \Gamma \end{array}$$

$$\begin{array}{lccccccc} \text{si } b\neq 0 & \Lambda_{a,b}^n & = & \langle \frac{1}{n}, \frac{a}{np} + \frac{b\tau}{p} \rangle & \subset & \langle \frac{1}{np}, \frac{\tau}{p} \rangle & = & \frac{1}{p}\Lambda_n \\ & & & \cap & & \cup & & \\ & \Gamma & = & \langle \frac{1}{np}, \frac{a}{np} + \frac{b\tau}{p} \rangle & = & \langle \frac{1}{np}, \frac{b\tau}{p} \rangle & = & \Gamma \end{array}$$

puis en considérant pour chaque inclusion les images des réseaux par la similitude qui convient. Par exemple, lorsque $b = 0$, pour l'inclusion de gauche, nous multiplions les deux réseaux par $\frac{1}{\tau}$ et nous appliquons [3, prop. 30, p. 815], à l'extension :

$$\mathcal{E}\left(\langle \frac{a}{np\tau}, \frac{1}{p} \rangle\right) \subset \mathcal{E}\left(\langle \frac{a}{np\tau}, 1 \rangle\right).$$

Il existe donc une fraction rationnelle G' à coefficients dans

$$cl.a.(\mathbf{Q}(g_2(\frac{1}{\tau}\Gamma), g_3(\frac{1}{\tau}\Gamma))) = cl.a.(\mathbf{Q}(g_2(\Gamma), g_3(\Gamma)))$$

(l'égalité provenant du lemme 4) telle que

$$\mathcal{P}\left(., \frac{1}{\tau p}\Lambda_n\right) = G' \circ \mathcal{P}\left(., \frac{1}{\tau}\Gamma\right).$$

La propriété d'homogénéité des fonctions de Weierstrass (voir lemme 4) nous permet de conclure qu'il existe une fraction rationnelle G à coefficients dans

$$cl.a.\left(\mathbf{Q}(g_2(\Gamma), g_3(\Gamma))\right)$$

telle que

$$\mathcal{P}\left(., \frac{1}{p}\Lambda_n\right) = G \circ \mathcal{P}\left(., \Gamma\right).$$

En effet, pour tout $z \in \mathbf{C}$, nous avons :

$$\mathcal{P}\left(\tau z, \frac{1}{p}\Lambda_n\right) = \frac{1}{\tau^2}\mathcal{P}\left(z, \frac{1}{\tau p}\Lambda_n\right) = \frac{1}{\tau^2}G' \circ \mathcal{P}\left(z, \frac{1}{\tau}\Gamma\right) = \frac{1}{\tau^2}G'(\tau^2\mathcal{P}(\tau z, \Gamma)).$$

Nous pouvons donc poser

$$G(X) = \frac{1}{\tau^2} G'(\tau^2 X).$$

En procédant de même pour les trois autres extensions, nous pouvons affirmer qu'il existe des fractions rationnelles G à coefficients dans $cl.a.(\mathbf{Q}(g_2(\Gamma), g_3(\Gamma)))$, et H à coefficients dans $cl.a.(\mathbf{Q}(g_2(\Lambda^n_{a,b}), g_3(\Lambda^n_{a,b})))$, telles que nous ayons :

$$\mathcal{P}(., \frac{1}{p}\Lambda_n) = G \circ \mathcal{P}(., \Gamma) \qquad \text{et} \qquad \mathcal{P}(., \Gamma) = H \circ \mathcal{P}^n_{a,b}.$$

Or nous avons :

$$(\psi^* \mathcal{P}_n)(z) = \mathcal{P}_n(pz) = \mathcal{P}(pz, \Lambda_n) = \mathcal{P}(pz, p.\frac{1}{p}\Lambda_n) = \frac{1}{p^2}\mathcal{P}(z, \frac{1}{p}\Lambda_n),$$

et il s'ensuit que :

$$\psi^* \mathcal{P}_n = \frac{1}{p^2}\mathcal{P}(., \frac{1}{p}\Lambda_n) = \frac{1}{p^2} G \circ H \circ \mathcal{P}^n_{a,b}.$$

De plus, d'après le lemme 6, les nombres $g_2(\Gamma)$ et $g_3(\Gamma)$ sont algébriques sur

$$\mathbf{Q}(g_2(\Lambda^n_{a,b}), g_3(\Lambda^n_{a,b})),$$

donc il en est de même des coefficients du polynôme $\frac{1}{p^2} G \circ H$. Le corollaire 7 permet alors de conclure. □

Le lemme 8 est l'analogue de [3, prop. 30, p. 815], qui permet de démontrer [3, prop. 32, p. 817]. Nous déduisons exactement de la même façon du lemme 8 le corollaire suivant, analogue de [3, prop. 32, p. 817] :

Corollaire 9 . *Soit k un sous-corps de $\mathbf{C}$, extension de Δ.*

1. *les corps $\Delta(\psi^*\mathcal{P}_n, \psi^*\mathcal{P}'_n)$ et $k(\psi^*\mathcal{P}_n, \psi^*\mathcal{P}'_n)$ sont sous-corps respectivement de $\Delta(\mathcal{P}^n_{a,b}, \mathcal{P}^{n'}_{a,b})$ et de $k(\mathcal{P}^n_{a,b}, \mathcal{P}^{n'}_{a,b})$.*

2. *la fonction de Weierstrass $\mathcal{P}^n_{a,b}$ est élément primitif de $\Delta(\mathcal{P}^n_{a,b}, \mathcal{P}^{n'}_{a,b})$ sur $\Delta(\psi^*\mathcal{P}_n, \psi^*\mathcal{P}'_n)$, de $k(\mathcal{P}^n_{a,b}, \mathcal{P}^{n'}_{a,b})$ sur $k(\psi^*\mathcal{P}_n, \psi^*\mathcal{P}'_n)$ et de $\mathbf{C}(\mathcal{P}^n_{a,b}, \mathcal{P}^{n'}_{a,b})$ sur $\mathbf{C}(\psi^*\mathcal{P}_n, \psi^*\mathcal{P}'_n)$.*

3. *Tout polynôme minimal de $\mathcal{P}^n_{a,b}$ sur $\Delta(\psi^*\mathcal{P}_n, \psi^*\mathcal{P}'_n)$ est polynôme minimal de $\mathcal{P}^n_{a,b}$ sur $k(\psi^*\mathcal{P}_n, \psi^*\mathcal{P}'_n)$ et sur $\mathbf{C}(\psi^*\mathcal{P}_n, \psi^*\mathcal{P}'_n)$. Il existe donc un polynôme $P^n_{a,b}(X, Y, Z)$ à coefficients dans Δ, tel que $P^n_{a,b}(\psi^*\mathcal{P}_n, \psi^*\mathcal{P}'_n, Z)$ soit polynôme minimal de $\mathcal{P}^n_{a,b}$ sur $\psi^*\mathcal{E}(\Lambda_n)$.*

Notons :

$$\mathrm{Hom}\,(E_1, E_n) = \{\alpha \in \mathbf{C} \mid \alpha\Lambda_1 \subset \Lambda_n\}$$

et $\mathrm{End}\,E_n = \mathrm{Hom}\,(E_n, E_n)$. Le corps k et le nombre τ ayant été fixés précédemment, nous avons les deux résultats suivants :

Théorème 10 .[Duret] *Si les réseaux* $\mathrm{Hom}\,(E_1, E_n)$ *et* $\mathrm{End}\,E_1$ *sont égaux, alors les corps elliptiques* $k(\mathcal{P}_n, \mathcal{P}_n{}')$ *et* $k(\mathcal{P}_1, \mathcal{P}_1{}')$ *ne sont pas élémentairement équivalents dans le langage* $\mathcal{L}(j)$.

Démonstration : Voir la remarque [2, rem. 37, p. 821] relative à [2, thm. 35, p. 818]. □

Théorème 11 . *S'il existe un entier* $p \in \mathbf{N}$ *tel que* $1 \leq p < n$ *et tel que les réseaux* $\mathrm{Hom}\,(E_1, E_n)$ *et* $\mathrm{Hom}\,(E_1, E_p)$ *soient égaux, alors les corps elliptiques* $k(\mathcal{P}_n, \mathcal{P}_n{}')$ *et* $k(\mathcal{P}_1, \mathcal{P}_1{}')$ *ne sont pas élémentairement équivalents dans le langage* $\mathcal{L}(j)$.

Démonstration : Voir [9, thm. 9]. □

Notons $R_n(X, Y)$ le polynôme

$$R_n(X, Y) = Y^2 - 4X^3 + g_2(\Lambda_n)X + g_3(\Lambda_n) \in \Delta[X, Y]$$

(appliquer le lemme 6 en choisissant $\Lambda = \Lambda_1$ et $\Lambda' = \Lambda_n$ pour voir que les coefficients de $R_n(X, Y)$ sont dans Δ). Voici maintenant le résultat principal de cet article :

Théorème 12 . *S'il existe un nombre premier* p *tel que, pour toute isogénie* $\phi \in \mathrm{Hom}\,(C_1, C_n)$, p *divise le degré de* ϕ, *alors les corps elliptiques* $k(\mathcal{P}_n, \mathcal{P}_n{}')$ *et* $k(\mathcal{P}_1, \mathcal{P}_1{}')$ *ne sont pas élémentairement équivalents dans le langage* $\mathcal{L}(j)$.

Démonstration : Nous allons construire une formule Θ_n du langage $\mathcal{L}(j)$ qui est vraie dans le corps $k(\mathcal{P}_n, \mathcal{P}_n{}')$ tandis qu'elle est fausse dans $k(\mathcal{P}_1, \mathcal{P}_1{}')$. D'après [3, prop. 33, p. 818], il suffit de trouver une telle formule dans le langage $\mathcal{L}(\Delta)$. D'après [2, prop. 10, p. 950], il existe une formule C du langage $\mathcal{L}(\Delta)$ définissant k dans $k(\mathcal{P}_n, \mathcal{P}_n{}')$ et dans $k(\mathcal{P}_1, \mathcal{P}_1{}')$, et $\mathbf{C}$ dans $\mathbf{C}(\mathcal{P}_n, \mathcal{P}_n{}')$ et dans $\mathbf{C}(\mathcal{P}_1, \mathcal{P}_1{}')$. Soit Θ_n la formule

$$\exists x, y\Big(\neg C(x) \wedge R_n(x, y) = 0 \wedge \forall z \bigwedge_{(a,b)\in\mathcal{I}_p} P^n_{a,b}(x, y, z) \neq 0\Big)$$

où $P^n_{a,b}(X, Y, Z) \in \Delta[X, Y, Z]$ est le polynôme défini dans le lemme 9(3).

Montrons que $k(\mathcal{P}_n, \mathcal{P}'_n)$ satisfait la formule Θ_n. Choisissons $x = \mathcal{P}_n$ et $y = \mathcal{P}'_n$. Supposons qu'il existe un couple (a, b) de $\mathcal{I}_p$ et un élément z de $k(\mathcal{P}_n, \mathcal{P}'_n)$ tels que

$$P^n_{a,b}(\mathcal{P}_n, \mathcal{P}'_n, z) = P^n_{a,b}(x, y, z) = 0.$$

Alors

$$\psi^*(P^n_{a,b}(\mathcal{P}_n, \mathcal{P}'_n, z)) = 0,$$

et nous avons donc

$$[k(\mathcal{P}^n_{a,b}, \mathcal{P}^{n'}_{a,b})\colon k(\psi^*\mathcal{P}_n, \psi^*\mathcal{P}'_n)] = [\mathcal{E}(\Lambda^n_{a,b})\colon \psi^*\mathcal{E}(\Lambda_n)] = 1.$$

Ceci est absurde puisque ψ est degré p (voir ($\bigstar$)).

Montrons que $k(\mathcal{P}_1, \mathcal{P}'_1)$ satisfait la formule $\neg\Theta_n$, i.e. :

$$k(\mathcal{P}_1, \mathcal{P}'_1) \models \forall x, y\Big(\neg C(x) \wedge R_n(x,y) = 0 \to \exists z \bigvee_{(a,b)\in\mathcal{I}_p} P^n_{a,b}(x,y,z) = 0\Big).$$

Soient donc u et v des éléments de $k(\mathcal{P}_1, \mathcal{P}'_1)$, avec $u \notin k$, qui annulent le polynôme $R_n(X,Y)$. Nous cherchons un élément w de $k(\mathcal{P}_1, \mathcal{P}'_1)$ tel qu'il existe un couple $(a,b) \in \mathcal{I}_p$ pour lequel $P^n_{a,b}(u,v,w) = 0$. S'il existe un tel w, il est algébrique sur $\Delta(u,v) \subset k(\mathcal{P}_1, \mathcal{P}'_1)$. Mais $k(\mathcal{P}_1, \mathcal{P}'_1)$ est algébriquement clos dans $\mathbf{C}(\mathcal{P}_1, \mathcal{P}'_1)$ (voir [3, prop. 32(3) et sa démonstration, p. 817]), donc il existe un tel w dans $k(\mathcal{P}_1, \mathcal{P}'_1)$ si et seulement s'il en existe un dans $\mathbf{C}(\mathcal{P}_1, \mathcal{P}'_1)$. Les conditions sur u et v nous donnent un isomorphisme et un morphisme de corps :

$$\rho^*\colon \mathbf{C}(\mathcal{P}_n, \mathcal{P}'_n) \xrightarrow{\sim} \mathbf{C}(u,v) \subset \mathbf{C}(\mathcal{P}_1, \mathcal{P}'_1)$$

avec $\rho^*(\mathcal{P}_n) = u$ et $\rho^*(\mathcal{P}'_n) = v$. Donc il existe des nombres complexes α et β, $\alpha \neq 0$, tels que pour toute fonction $f \in \mathbf{C}(\mathcal{P}_n, \mathcal{P}'_n)$, nous ayons :

$$(\rho^* f)(z) = f(\alpha^{-1}z + \beta)$$

(voir [4, §90, pp. 195-196]). Soit $\rho\colon C_1 \to C_n$ le morphisme de courbes associé à ρ^*, et $r\colon E_1 \to E_n$ le morphisme associé à ρ; il est donc donné par

$$r(z) = \alpha^{-1}z + \beta.$$

Si β n'est pas élément de Λ_n, r n'est pas un morphisme de groupes et donc ρ n'est pas une isogénie. Dans ce cas, nous composons avec la translation $t_{-\alpha\beta}\colon E_1 \to E_1$ donnée par

$$t_{-\alpha\beta}(z) = z - \alpha\beta.$$

Appelons f la composée $r \circ t_{-\alpha\beta}$. Nous avons alors :

$$f(z) = r \circ t_{-\alpha\beta}(z) = r(z - \alpha\beta) = \alpha^{-1}(z - \alpha\beta) + \beta = \alpha^{-1}z.$$

Notons $\tau_{-\alpha\beta}$ le morphisme de courbes associé à $t_{-\alpha\beta}$. Soit $\phi = \rho \circ \tau_{-\alpha\beta}$ le morphisme de courbes associé à f. Donc $\phi\colon C_1 \to C_n$ est une isogénie, et par hypothèse son

degré est divisible par p. D'après le lemme 3, il existe donc un couple $(a,b) \in \mathcal{I}_p$ tel que ϕ se factorise de la manière suivante, avec $\deg \psi = p$,

$$C_1 \xrightarrow[\times(p\alpha)^{-1}]{\lambda} C_{a,b}^n \xrightarrow[\times p]{\psi} C_n.$$

Ceci nous donne une factorisation pour $\rho = \psi \circ \lambda \circ (\tau_{-\alpha\beta})^{-1} = \psi \circ \lambda \circ \tau_{\alpha\beta}$,

$$C_1 \xrightarrow{\tau_{\alpha\beta}} C_1 \xrightarrow{\lambda} C_{a,b}^n \xrightarrow{\psi} C_n,$$

et en termes de corps, nous obtenons une factorisation de ρ^*,

$$\mathcal{E}(\Lambda_n) \xrightarrow{\psi^*} \mathcal{E}(\Lambda_{a,b}^n) \xrightarrow{\lambda^*} \mathcal{E}(\Lambda_1) \xrightarrow{\tau_{\alpha\beta}^*} \mathcal{E}(\Lambda_1).$$

L'élément que nous cherchions est $w = \tau_{\alpha\beta}^* \circ \lambda^*(\mathcal{P}_{a,b}^n)$. En effet, nous avons :

$$\begin{aligned} P_{a,b}^n(u,v,w) &= P_{a,b}^n(\rho^*\mathcal{P}_n, \rho^*\mathcal{P}'_n, \tau_{\alpha\beta}^* \circ \lambda^*(\mathcal{P}_{a,b}^n) \\ &= \tau_{\alpha\beta}^* \circ \lambda^* P_{a,b}^n(\psi^*\mathcal{P}_n, \psi^*\mathcal{P}'_n, \mathcal{P}_{a,b}^n) \\ &= 0. \end{aligned}$$

□

Pierce a démontré la proposition suivante (voir [7, thm. 8 et thm. 10 ensemble]) :

Proposition 13 . *Les anneaux d'endomorphismes* $\mathrm{End}\,(E_1)$ *et* $\mathrm{End}\,(E_n)$ *ne sont pas égaux si et seulement s'il existe un nombre premier* p *qui divise le degré de toute isogénie* $\Phi \in \mathrm{Hom}\,(C_1, C_n)$.

Nous obtenons donc, en combinant le théorème 12 et la proposition 13, le théorème annoncé en introduction :

Théorème 14 . *Si les anneaux d'endomorphismes* $\mathrm{End}\,(E_1)$ *et* $\mathrm{End}\,(E_n)$ *sont distincts, alors les corps elliptiques* $k(\mathcal{P}_n, \mathcal{P}_n{}')$ *et* $k(\mathcal{P}_1, \mathcal{P}_1{}')$ *ne sont pas élémentairement équivalents dans le langage* $\mathcal{L}(j)$.

3 Limites et portée des résultats

Soit $AX^2 + BX + C$ un polynôme dont τ est la racine, où $A \in \mathbf{N}$ est non nul, et $B, C \in \mathbf{Z}$ sont tels que $A \wedge B \wedge C = 1$ (par la suite, le symbole $\wedge$ désignera toujours le plus grand diviseur commun positif). Si $\bar{\tau}$ désigne la racine conjuguée à τ, nous avons bien sûr

$$\tau\bar{\tau} = \frac{C}{A} \qquad \text{et} \qquad \tau + \bar{\tau} = -\frac{B}{A}.$$

Notons

$$\delta_n = A \wedge nB \wedge nC = A \wedge n \qquad \text{et} \qquad \delta'_n = A \wedge nB \wedge n^2C.$$

Il est immédiat, d'après la définition de Hom, que pour tout entier $n \geq 1$, nous avons

$$\text{End}\, E_1 \subset \text{Hom}\,(E_1, E_n) \qquad \text{et} \qquad \text{End}\, E_n \subset \text{Hom}\,(E_1, E_n).$$

Proposition 15 . *Pour tout entier $n \geq 1$, nous avons :*

$$\text{Hom}\,(E_1, E_n) = \langle 1, \frac{A}{\delta_n}\bar{\tau}\rangle$$

Démonstration : Voir [9, prop. 1]. □

Etant donnés deux entiers naturels k et k', nous avons :

$$\langle 1, k\tau\rangle = \langle 1, k'\tau\rangle \Longleftrightarrow |k| = |k'|.$$

En effet, si les réseaux $\langle 1, k\tau\rangle$ et $\langle 1, k'\tau\rangle$ sont égaux, alors il existe des entiers $a, b \in \mathbf{Z}$ tels que $k\tau = ak'\tau$ et $k'\tau = bk\tau$, donc nous avons $|a| = |b| = 1$.

Corollaire 16 . *Pour tout entier $n \geq 1$, nous avons :*

1. $\text{End}\, E_1 = \langle 1, A\tau\rangle = \langle 1, A\bar{\tau}\rangle$
2. $\text{End}\, E_n = \langle 1, \frac{An}{\delta'_n}\tau\rangle = \langle 1, \frac{An}{\delta'_n}\bar{\tau}\rangle$
3. *Si* $\text{End}\, E_1 = \text{End}\, E_n$, *alors* $n|A$.
4. *Si* $\text{End}\, E_1 = \text{End}\, E_n$, *alors* $\text{Hom}\,(E_1, E_n) = \langle 1, \frac{A}{n}\bar{\tau}\rangle$.

Démonstration :

1. La première égalité vient du fait que $A \wedge B \wedge C = 1$. Pour la seconde, nous remarquons que
$$\langle 1, A\bar{\tau}\rangle = \langle 1, -B - A\tau\rangle = \langle 1, A\tau\rangle.$$
2. Nous avons la première égalité car
$$\text{End}\, E_n = \text{End}\left(\frac{\mathbf{C}}{\langle 1, n\tau\rangle}\right)$$
et le polynôme $AX^2 + BnX + Cn^2$ s'annule en $n\tau$. Il faut diviser par δ'_n pour que les coefficients soient premiers entre eux. Nous concluons grâce à (1). Pour obtenir la seconde égalité, nous remarquons que
$$\langle 1, \frac{An}{\delta'_n}\tau\rangle = \langle 1, \frac{n}{\delta'_n}(-B - A\bar{\tau})\rangle = \langle 1, \frac{n}{\delta'_n}A\bar{\tau}\rangle,$$
car $\frac{nB}{\delta'_n}$ est un entier.

3. Si les réseaux End E_1 et End E_n sont égaux, alors $\frac{An}{\delta'_n}$ est égal à $\pm A$. Les entiers n et δ'_n étant strictement positifs, nous avons

$$n = \delta'_n = A \wedge nB \wedge n^2C,$$

et donc n divise A.

4. Si les réseaux End E_1 et End E_n sont égaux, alors d'après (3), n divise A, donc nous avons

$$\delta_n = n(\frac{A}{n} \wedge B \wedge C) = n,$$

car $\frac{A}{n} \wedge B \wedge C = 1$.

□

Proposition 17 . *L'application*

$$\begin{array}{rcl} \{p \in \mathbf{N}^* \mid p \text{ divise } A\} & \longrightarrow & \{\mathrm{Hom}\,(E_1, E_p) \mid p \in \mathbf{N}^*\} \\ p & \longmapsto & \mathrm{Hom}\,(E_1, E_p) \end{array}$$

est une bijection. En particulier, la cardinal de l'ensemble $\{\mathrm{Hom}\,(E_1, E_p) \mid p \in \mathbf{N}^*\}$ *est le nombre de diviseurs de A.*

Démonstration : Voir [9, cor. 5]. □

Par conséquent, nous pouvons énoncer le théorème 11 de la manière suivante :

Théorème 18 . *Si n ne divise pas A, alors les corps elliptiques* $k(\mathcal{P}_n, \mathcal{P}_n{}')$ *et* $k(\mathcal{P}_1, \mathcal{P}_1{}')$ *ne sont pas élémentairement équivalents dans le langage* $\mathcal{L}(j)$.

Soient $m, r, s, d \in \mathbf{Z}$ tels que $m \geq 1$, $s \neq 0$, $d \geq 1$ et non divisible par un carré, et tels que

$$\tau = \frac{1}{m}(r + is\sqrt{d}).$$

Notons $D = r^2 + ds^2$ et $e = m^2 \wedge 2rm \wedge D$.

Proposition 19 . *Nous pouvons choisir* $A = \frac{m^2}{e}$, $B = \frac{-2rm}{e}$ *et* $C = \frac{D}{e}$ *comme coefficients entiers premiers entre eux du polynôme minimal de* τ.

Démonstration : Montrons que $m^2\tau^2 - 2rm\tau + D = 0$.
Nous avons $\tau^2 = \frac{1}{m^2}(r^2 + 2ris\sqrt{d} - ds^2)$. Nous en déduisons que

$$m^2\tau^2 - 2rm\tau + D = m^2\frac{1}{m^2}(r^2 + 2ris\sqrt{d} - ds^2) - 2rm\frac{1}{m}(r + is\sqrt{d}) + D = r^2 + 2ris\sqrt{d} - ds^2 - 2r(r + is\sqrt{d}) + r^2 + ds^2 = 0.$$

Donc le polynôme $\frac{m^2}{e}X^2 - \frac{2rm}{e}X + \frac{D}{e}$ s'annule en τ et a bien ses coefficients premiers entre eux. □

Exemples 20 . Dans les deux exemples suivants, nous ne faisons que les calculs qui nous permettront de mieux apprécier le champ d'action et les limites des théorèmes 10, 11 et 12.

1. Pour $\tau = \frac{1}{2} + i = \frac{1}{2}(1 + 2i)$, nous trouvons $D = 5$, $e = 1$, $A = 4$, $B = -4$, $C = 5$, et donc nous avons $\delta_1 = 1$, $\delta_2 = 2$, $\delta_4 = 4$, $\delta'_2 = \delta'_4 = 4$.

   Nous en déduisons que :

   $\mathrm{End}\, E_1 = \langle 1, 4i\rangle$, $\mathrm{Hom}\,(E_1, E_2) = \langle 1, 2i\rangle$, $\mathrm{Hom}\,(E_1, E_4) = \langle 1, i\rangle$, $\mathrm{End}\, E_2 = \langle 1, 2i\rangle$ et $\mathrm{End}\, E_4 = \mathrm{End}\, E_1$.

2. Pour $\tau = \frac{1}{6}(2+5i\sqrt{2})$, nous trouvons $D = 54$, $e = 6$, $A = 6$, $B = -4$, $C = 9$, et donc nous avons $\delta_2 = \delta'_2 = 2$, $\delta_3 = \delta'_3 = 3$, $\delta_6 = \delta'_6 = 6$.

   Nous en déduisons que :

   $\mathrm{End}\, E_1 = \langle 1, 5i\sqrt{2}\rangle$, $\mathrm{Hom}\,(E_1, E_2) = \langle 1, 2i\rangle$, $\mathrm{Hom}\,(E_1, E_4) = \langle 1, i\rangle$, $\mathrm{End}\, E_2 = \langle 1, \frac{5}{2}i\sqrt{2}\rangle$, $\mathrm{Hom}\,(E_1, E_3) = \langle 1, \frac{1}{3}(2 - 5i\sqrt{2})\rangle$, $\mathrm{Hom}\,(E_1, E_6) = \langle 1, \frac{1}{6}(2 - 5i\sqrt{2})\rangle$, et $\mathrm{End}\, E_2 = \mathrm{End}\, E_3 = \mathrm{End}\, E_6 = \mathrm{End}\, E_1$.

D'après le corollaire 16(3), si les réseaux $\mathrm{End}\,(E_1)$ et $\mathrm{End}\,(E_n)$ sont égaux, alors n est un diviseur de A. Par conséquent, le théorème 12, tout comme 11, donne une formule Θ_n pour tous les entiers $n \in \mathbf{N}$ qui ne divisent pas A. Mais comme nous pouvons le voir dans l'exemple 20(1), la réciproque de l'item (3) du corollaire 16 est fausse. En effet, dans cet exemple, nous trouvons $A = 4$ et $\mathrm{End}\,(E_1) \neq \mathrm{End}\,(E_2)$. Le théorème 12 donne dans cet exemple une des deux formules qui n'était pas donnée par le théorème 11, soit la formule Θ_2. Par contre, il n'apporte rien de nouveau pour $\tau = \frac{1}{6}(2 + 5i\sqrt{2})$, puisque dans cet exemple, nous avons $A = 6$ et $\mathrm{End}\,(E_1) = \mathrm{End}\,(E_2) = \mathrm{End}\,(E_3) = \mathrm{End}\,(E_6)$.

Si p est un nombre premier, notons $E^n_{a,b}(p)$ le quotient $\frac{\mathbf{C}}{p\Lambda^n_{a,b}}$.

Proposition 21 . *Nous avons l'équivalence suivante :*

$$\mathrm{End}\,(E_1) \neq \mathrm{End}\,(E_n) \Longleftrightarrow \exists p \text{ premier} \quad \mathrm{Hom}\,(E_1, E_n) \subset \bigcup_{(a,b)\in\mathcal{I}_p} \mathrm{Hom}\,(E_1, E^n_{a,b}(p)).$$

Démonstration :
$\mathrm{End}\,(E_1) \neq \mathrm{End}\,(E_n)$

$\Longleftrightarrow$ $\exists p$ premier $\forall \Phi \in \mathrm{Hom}\,(C_1, C_n),\ p|\deg(\Phi)$
$\Longleftrightarrow$ $\exists p$ premier $\forall \alpha^{-1} \in \mathrm{Hom}\,(E_1, E_n),\ \exists (a,b) \in \mathcal{I}_p,\ (p\alpha)^{-1}\Lambda_1 \subset \Lambda^n_{a,b}$
$\Longleftrightarrow$ $\exists p$ premier $\forall \beta \in \mathrm{Hom}\,(E_1, E_n),\ \exists (a,b) \in \mathcal{I}_p,\ \beta\Lambda_1 \subset p\Lambda^n_{a,b}$
$\Longleftrightarrow$ $\exists p$ premier $\forall \beta \in \mathrm{Hom}\,(E_1, E_n),\ \exists (a,b) \in \mathcal{I}_p,\ \beta \in \mathrm{Hom}\,(\frac{\mathbf{C}}{\Lambda_1}, \frac{\mathbf{C}}{p\Lambda^n_{a,b}})$
$\Longleftrightarrow$ $\exists p$ premier $\forall \beta \in \mathrm{Hom}\,(E_1, E_n),\ \beta \in \bigcup_{(a,b)\in\mathcal{I}_p} \mathrm{Hom}\,(E_1, E^n_{a,b}(p))$
$\Longleftrightarrow$ $\exists p$ premier, $\mathrm{Hom}\,(E_1, E_n) \subset \bigcup_{(a,b)\in\mathcal{I}_p} \mathrm{Hom}\,(E_1, E^n_{a,b}(p))$.

La première équivalence n'est autre que la proposition 13. La seconde vient du lemme 3. Pour la troisième, nous posons $\beta = \alpha^{-1}$. □

Nous pouvons donc énoncer les hypothèses des théorèmes 10, 11 et 12 de la manière suivante :

théorème 10 :		$\mathrm{Hom}\,(E_1, E_n) \subset \mathrm{Hom}\,(E_1, E_1)$	(1)
théorème 11 :	$\exists p < n$	$\mathrm{Hom}\,(E_1, E_n) \subset \mathrm{Hom}\,(E_1, E_p)$	(2)
théorème 12 :	$\exists p$ premier	$\mathrm{Hom}\,(E_1, E_n) \subset \bigcup_{(a,b)\in\mathcal{I}_p} \mathrm{Hom}\,(E_1, E^n_{a,b}(p))$	(3)

Nous avons bien sûr (1) ⇒ (2). Nous avons aussi (2) ⇒ (3) d'après la remarque qui précède la proposition 21. Nous pouvons aussi les énoncer d'un point de vue arithmétique :

théorème 10 :	n et A sont premiers entre eux	
théorème 11 :	n ne divise pas A	
théorème 12 :	$n \neq A \wedge nB \wedge n^2C$	(•)

où (•) se déduit directement du corollaire 16 (1 et 2).

References

[1] L. Becker, C. W. Henson, L. A. Rubel, *First order conformal invariants*, Ann. Math. (2) **112** (1980), 123-178.

[2] J.-L. Duret, *Sur la théorie élémentaire des corps de fonctions*, Journ. Symb. Logic **51**, n4 (1986), 948-956.

[3] J.-L. Duret, *Équivalence élémentaire et isomorphisme des corps de courbe sur un corps algébriquement clos*, Journ. Symb. Logic **57**, n3 (1992), 808-823.

[4] P. Du Val, *Elliptic Functions and elliptic curves*, Lond. Math. Soc. Lect. Note Series **9**, Cambridge University Press (1973).

[5] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New-York (1977).

[6] S. Lang, *Elliptic functions, 2nd edition*, Springer Verlag, Grad. Texts in Math. (1987).

[7] D. A. Pierce, *Function fields and elementary equivalence*, Bull. Lond. Math. Soc. **31**, 4 (1999).

[8] J. H. Silverman, *The arithmetic of elliptic curves*, Springer Verlag, Grad. texts in math. (1986).

[9] X. Vidaux, *Équivalence élémentaire de corps elliptiques*, C. R. Acad. Sci. Paris, Série I **330**, (2000), 1-4.

Université d'Angers,
Département de Mathématiques,
2 Bd Lavoisier,
49045 Angers
France

University of Crete-Heraklion,
Department of Mathematics,
71 409 Heraklion,
Crete-Greece

Xavier.Vidaux@univ-angers.fr
vidaux@math.itia.uch.gr