# Sur la courbe modulaire $X_E(7)$

Emmanuel Halberstadt et Alain Kraus

CONTENTS



2000 AMS Subject Classification: Primary 11G

Keywords: Modular curves, elliptic curves, Galois representations

Soient $k$ un corps de caractéristique 0 et $E$ une courbe elliptique définie sur $k$. Il existe une courbe modulaire définie sur $k$, unique à $k$-isomorphisme près, qui classifie les courbes elliptiques $E'$ telles que les modules galoisiens des points de 7-torsion de $E$ et $E'$ soient symplectiquement isomorphes. Dans cet article, nous explicitons une équation de cette courbe, et nous en précisons l'interprétation modulaire.

Let $k$ be a field of characteristic 0, and $E$ be an elliptic curve defined over $k$. There exists a modular curve defined over $k$, unique up to $k$-isomorphism, which classifies the elliptic curves $E'$ such that the modules of the 7-torsion points of $E$ and $E'$ are galois symplectically isomorphic. In this paper, we explicit an equation of this curve and precise its modular interpretation.

## 1. INTRODUCTION

Soit $k$ un corps de caractéristique 0. On notera toujours $\overline{k}$ une clôture algébrique de $k$ et $G_k$ le groupe de Galois de $\overline{k}/k$. Considérons par ailleurs un entier $n \geq 3$. Désignons par $\mu_n$ le $k$-schéma en groupes des racines $n$-ièmes de l'unité, ou encore le $G_k$-module $\mu_n(\overline{k})$. Étant donnée une courbe elliptique $E$ sur $k$, soit $E[n]$ le $k$-schéma en groupes noyau de la multiplication par $n$ dans $E$. Il est muni d'une forme bilinéaire alternée inversible à valeurs dans $\mu_n$, à savoir l'accouplement de Weil. Par abus de notation, $E[n](\overline{k})$ sera aussi noté $E[n]$ ; c'est un $G_k$-module et, comme $\mathbb{Z}/n\mathbb{Z}$-module, il est libre de rang 2. L'accouplement de Weil sur $E[n]$ (défini comme dans [Silverman 86, page 95]) est invariant par $G_k$.

Soient $k, n$ et $E$ comme ci-dessus. Il existe une courbe algébrique affine $Y_E(n)$ définie sur $k$, lisse et absolument irréductible, qui est unique à $k$-isomorphisme près, et qui paramètre les classes d'isomorphisme de couples $(E', v)$, où $E'$ est une courbe elliptique et $v$ un isomorphisme symplectique (i.e., compatible aux accouplements de Weil) de $k$-schémas en groupes de $E[n]$ sur $E'[n]$. La compactifiée lisse $X_E(n)$ de $Y_E(n)$ est une tordue galoisienne de la courbe modulaire standard $X(n)$ (cf. section 3). En particulier, si $g$ est le genre de $X_E(n)$, on a $g = 0$ si $n \leq 5$, $g = 1$ si $n = 6$ et $g \geq 3$ si $n \geq 7$.

On s'intéresse dans ce travail à la courbe $X_E(7)$. Son genre est égal à 3. On donne dans la section 2 une équation de $X_E(7)$. On obtient une quartique lisse dans $\mathbb{P}^2$ dont les coefficients sont fonction de ceux d'un modèle de Weierstrass de $E$ sur $k$. Elle est isomorphe sur $\overline{k}$ à la quartique de Klein d'équation $X^3Y + Y^3Z + Z^3X = 0$. Nous explicitons l' interprétation modulaire de $X_E(7)$ dans le modèle obtenu (cf. section 5).

Si $k$ est un corps de nombres, l'ensemble des points rationnels sur $k$ de $X_E(7)$ est fini. Notons que la courbe $Y_E(7)$ a toujours au moins un point rationnel sur $k$, à savoir le point-base, correspondant à la classe du couple $\left(E, 1_{E[7]}\right)$. Plus généralement, soit $\varphi$ une $k$-isogénie de $E$ sur une autre courbe elliptique $E'$ sur $k$. Supposons que le degré $d$ de $\varphi$ vérifie $\left(\frac{d}{7}\right) = 1$, et soit $\delta$ un entier tel que $d\delta^2 \equiv 1 \bmod 7$. La classe du couple $(E', \delta\varphi)$ correspond alors à un point de $Y_E(7)(k)$. Nous dirons qu'un tel point de $Y_E(7)(k)$ est *trivial*. Un problème naturel qui se pose est celui de la détermination des points non triviaux de $Y_E(7)(k)$. Ce problème suggère par exemple l'étude des quotients non triviaux éventuels de la jacobienne de $X_E(7)$. Nous signalons en complément dans la section 8 quelques remarques à ce sujet assurant qu'en général il n'existe pas de tels quotients.

Si $k = \mathbb{Q}$, la question de l'existence de courbes elliptiques $E$ sur $\mathbb{Q}$ pour lesquelles $Y_E(7)(\mathbb{Q})$ possède des points non triviaux a été posé par B. Mazur en 1978 ([Mazur 78]). Des exemples de telles courbes elliptiques figurent déjà dans des travaux antérieurs (on pourra consulter à ce sujet [Kraus et Oesterlé 92] et [Halberstadt and Kraus 99]). Nous donnons dans la section 6 un exemple de courbe elliptique $E/\mathbb{Q}$ telle que $Y_E(7)(\mathbb{Q})$ ait au moins sept points non triviaux. Plus précisément, nous explicitons un huituplet de courbes elliptiques sur $\mathbb{Q}$, qui ne sont pas mutuellement $\mathbb{Q}$-isogènes, et dont les modules galoisiens des points de 7-torsion sont symplectiquement isomorphes.

Nous tenons à remercier le rapporteur de cet article pour les suggestions qu'il nous a faites. En particulier, la formulation du théorème 4.1, qui améliore une version antérieure, lui est dûe.

## 2. ÉNONCÉ DES RÉSULTATS

**Théorème 2.1.** *Supposons qu'un modèle de Weierstrass de $E$ soit donné par*

$$y^2 = x^3 + ax + b, \tag{2–1}$$

*où $a$ et $b$ sont deux éléments de $k$. La courbe $X_E(7)$ est alors isomorphe sur $k$ à la complétée projective de la courbe d'équation*

$$ax^4 + 7bx^3 + 3(y^2 - a^2)x^2 - b(6y + 5a)x + (2y^3 + 3ay^2 + 2a^2y - 4b^2) = 0, \tag{2–2}$$

*via un isomorphisme appliquant le point-base de $Y_E(k)$ sur $[0, 1, 0]$.*

Lorsque $E$ a tous ses points d'ordre 2 rationnels sur $k$, on a l'énoncé suivant :

**Théorème 2.2.** *Supposons qu'un modèle de Weierstrass de $E$ soit donné par*

$$y^2 = (x - a)(x - b)(x - c), \tag{2–3}$$

*où $a, b, c$ sont trois éléments de $k$ distincts. La courbe $X_E(7)$ est alors isomorphe sur $k$ à la courbe projective d'équation $Q(x, y, z) = 0$, où*

$$Q(x, y, z) = (c - b)\mathfrak{q}(x, y, z) + (a - c)\mathfrak{q}(y, z, x) + (b - a)\mathfrak{q}(z, x, y), \tag{2–4}$$

*en posant $\mathfrak{q}(x, y, z) = (y + z)x^3 - 3x^2yz$.*

## 3. RAPPPELS SUR LES COURBES MODULAIRES $X(n)$ ET $X_E(n)$

Soit en général $n \geq 1$ un entier. Notons $A$ le $\mathbb{Q}$-schéma en groupes $(\mathbb{Z}/n\mathbb{Z}) \times \mu_n$. On munit $A$ de la forme bilinéaire alternée inversible $<,>$ à valeurs dans $\mu_n$ donnée par

$$< (a, \zeta), (a', \zeta') > = \zeta'^{a}\, \zeta^{-a'}.$$

La courbe $X(n)$ est une courbe projective, lisse, absolument irréductible, définie sur $\mathbb{Q}$. On en trouve une construction dans [Deligne et Rapoport 73] ou, lorque $n$ est premier, dans [Ligozat 77]; en fait, $X(n)$ est, avec les notations de [Ligozat 77], la courbe modulaire $X_G$ associée au sous-groupe $G$ de $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ formé des matrices du type $\begin{pmatrix} \pm 1 & 0 \\ 0 & a \end{pmatrix}$, où $a$ décrit $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$. L'ensemble $X(n)(\mathbb{C})$ des points complexes de $X(n)$, muni de sa structure naturelle de surface de Riemann, peut être identifié (ce que nous ferons désormais) à la surface de Riemann $\Gamma(n)\backslash\mathfrak{h}^*$, en notant $\mathfrak{h}$ le demi-plan de Poincaré, $\mathfrak{h}^*$ la réunion de $\mathfrak{h}$ et de $\mathbb{P}^1(\mathbb{Q})$, et $\Gamma(n)$ le sous-groupe de $\mathrm{SL}_2(\mathbb{Z})$ formé des matrices congrues à l'identité modulo $n$. L'ensemble (fini) $\Pi_n$ des pointes de $X(n)$ est l'image canonique de $\mathbb{P}^1(\mathbb{Q})$ dans $X(n)(\mathbb{C})$, il est défini sur $\mathbb{Q}$,

et l'on note $Y(n)$ l'ouvert complémentaire de $\Pi_n$ dans $X(n)$. Ainsi $Y(n)(\mathbb{C})$ est l'image canonique de $\mathfrak{h}$ dans $X(n)(\mathbb{C})$. L'action naturelle du groupe $\mathrm{Aut}(\mathbb{C})$ sur $\Pi_n$ est décrite dans [Ligozat 77].

Soit $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ une matrice de $\mathrm{SL}_2(\mathbb{Z})$. Puisque $\Gamma(n)$ est distingué dans $\mathrm{SL}_2(\mathbb{Z})$, $g$ induit un $\mathbb{C}$-automorphisme de $X(n)$, que nous noterons $\widetilde{g}$, associant à la classe de $\tau \in \mathfrak{h}^*$ la classe de $g.\tau = \frac{a\tau+b}{c\tau+d}$. Le morphisme $g \longmapsto \widetilde{g}$ induit un morphisme injectif de $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})/\{\pm 1\}$ dans $\mathrm{Aut}(X(n))$, groupe des $\mathbb{C}$-automorphismes de $X(n)$. Si $g$ appartient à $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$, ou au quotient de ce groupe par $\{\pm 1\}$, on notera encore $\widetilde{g}$ l'automorphisme de $X(n)$ correspondant.

Rappelons l'interprétation modulaire de $Y(n)$. Pour tout corps $k$ de caractéristique nulle, il y a une bijection, fonctorielle en $k$, de $Y(n)(k)$ sur l'ensemble des classes d'isomorphisme de couples $(E, u)$ où $E$ est une courbe elliptique sur $k$ et $u$ un isomorphisme symplectique de $k$-schémas en groupes de $A$ sur $E[n]$. Lorsque $k = \mathbb{C}$, la bijection ci-dessus peut être précisée ainsi. Soient $\tau$ un point de $\mathfrak{h}$ et $\eta \in Y(n)(\mathbb{C})$ sa classe. Le point $\eta$ correspond à la classe du couple $(E_\tau, u_\tau)$, où $E_\tau$ est la courbe elliptique $\mathbb{C}^*/e^{2i\pi\tau\mathbb{Z}}$ et $u_\tau$ est l'isomorphisme de $A$ sur $E_\tau[n]$ défini par

$$u_\tau(a, \zeta) \;=\; \text{classe de } \zeta e^{2i\pi a\tau/n}\,.$$

Soit maintenant $E$ une courbe elliptique sur un corps $k$ de caractéristique 0. La courbe $X_E(n)$ est une courbe projective, lisse, absolument irréductible, définie sur $k$. On peut par exemple la construire comme tordue galoisienne de $X(n)$ (cf. [Kraus 90]). Plus précisément, un isomorphisme symplectique $u$ de $A(\overline{k})$ sur $E[n]$ étant choisi, on obtient un $\overline{k}$-isomorphisme

$$t \;:\; X_E(n) \longrightarrow X(n)$$

tel que, en désignant par $Y_E(n)$ l'image de $Y(n)$ par $t^{-1}$, les deux propriétés suivantes soient vérifiées:
(a) pour toute extension $L$ de $k$, il y a une bijection, fonctorielle en $L$, entre $Y_E(n)(L)$ et l'ensemble des classes d'isomorphisme de couples $(E', v)$, où $E'/L$ est une courbe elliptique et $v$ est un isomorphisme symplectique de $L$-schémas en groupes de $E[n]$ sur $E'[n]$ ; deux tels couples $(E'_1, v_1)$ et $(E'_2, v_2)$ sont dits isomorphes s'il existe un $L$-isomorphisme $\varphi$ de $E'_1$ sur $E'_2$ tel que $\varphi \circ v_1 = v_2$ ;
(b) soient $L$ une extension de $k$ et $\xi$ un point de $Y_E(n)(L)$. Si le point $\xi$ est associé, par la bijection ci-dessus, à la classe d'un certain couple $(E', v)$, alors $t(\xi) \in Y(n)(\overline{L})$ est associé à la classe du couple $(E', v \circ u)$.

La courbe $Y_E(n)$ classifie ainsi les courbes elliptiques telles que les représentations de Galois dans $E[n]$ et $E'[n]$ sont symplectiquement isomorphes.

Venons-en plus particulièrement à la courbe $X(7)$. Il y a exactement vingt-quatre pointes sur $X(7)(\mathbb{C})$, parmi elles trois sont rationnelles sur $\mathbb{Q}$, à savoir $P_1, P_2, P_3$, en notant $P_j \in Y(7)$ la classe de $j/7 \in \mathbb{P}^1(\mathbb{Q})$. La pointe $P_1$ est la pointe ordinaire $\infty$, classe de $\infty \in \mathbb{P}^1(\mathbb{Q})$. On sait que $X(7)$ est isomorphe sur $\mathbb{Q}$ à la quartique de Klein $\mathcal{C}$ d'équation

$$X^3Y + Y^3Z + Z^3X \;=\; 0\,. \qquad (3\text{–}1)$$

De façon plus précise, il existe un unique $\mathbb{Q}$-isomorphisme $\theta$ de $X(7)$ sur $\mathcal{C}$ appliquant $P_1, P_2, P_3$ sur $[0,0,1], [0,1,0], [1,0,0]$, respectivement. On peut expliciter $\theta$ comme suit. Soient $k$ un corps de caractéristique 0 et $\xi$ un point de $Y(7)(k)$. On écrit $\theta(\xi) = [X, Y, 1]$, où $X, Y \in k$.
1) Supposons d'abord que $\xi$ soit représenté par un couple $(E, u)$, où $E$ est une courbe elliptique sur $k$, donnée par l'équation

$$y^2 \;=\; x^3 + a_2x^2 + a_4x + a_6\,,$$

et où $u$ est un isomorphisme symplectique de $G_k$-modules de $A(\overline{k})$ sur $E[7]$. Soit $\zeta \in \overline{k}$ une racine primitive 7-ième de l'unité. Posons $P = u(1,1)$ et $Q = u(0,\zeta)$. On a alors:

$$X \;=\; \frac{y(3P)}{y(P)} \times \left(\frac{x(3P) - x(2P)}{x(P) - x(2P)}\right) \times \prod_{j=1}^{3} \left(\frac{x(P) - x(jQ)}{x(3P) - x(jQ)}\right) \quad \text{et} \quad (3\text{–}2)$$

$$Y \;=\; \frac{y(3P)}{y(2P)} \times \left(\frac{x(3P) - x(P)}{x(2P) - x(P)}\right) \times \prod_{j=1}^{3} \left(\frac{x(2P) - x(jQ)}{x(3P) - x(jQ)}\right). \quad (3\text{–}3)$$

2) Supposons maintenant que $k = \mathbb{C}$ et que $\xi$ soit la classe d'un point $\tau$ de $\mathfrak{h}$. Comme fonctions de $\tau$, $X$ et $Y$ sont des fonctions modulaires de poids 0 pour $\Gamma(7)$. On peut exprimer $X$ et $Y$ en fonction des diverses formes de Klein $\mathfrak{k}_{(r,s)}$ de niveau 7 (cf. [Lang 87, page 260]):

$$X \;=\; -\frac{\mathfrak{k}_{(1,0)}}{\mathfrak{k}_{(3,0)}} \times \prod_{s=1}^{3} \left(\frac{\mathfrak{k}_{(1,s))}\mathfrak{k}_{(1,-s)}}{\mathfrak{k}_{(3,s)}\mathfrak{k}_{(3,-s)}}\right) \quad \text{et} \quad (3\text{–}4)$$

$$Y \;=\; \frac{\mathfrak{k}_{(2,0)}}{\mathfrak{k}_{(3,0)}} \times \prod_{s=1}^{3} \left(\frac{\mathfrak{k}_{(2,s))}\mathfrak{k}_{(2,-s)}}{\mathfrak{k}_{(3,s)}\mathfrak{k}_{(3,-s)}}\right). \quad (3\text{–}5)$$

Ces formules sont équivalentes aux formules (3–2) et (3–3), on le voit en utilisant la fonction $\sigma$ de Weierstrass et les formules classiques de l'exercice I.6.3 de [Silverman 86]. Par ailleurs, le morphisme $g \longmapsto \widetilde{g}$ est ici un isomorphisme de $\mathrm{PSL}_2(\mathbb{F}_7)$ sur $\mathrm{Aut}(X(7))$.

3) Soient $k$ un corps de caractéristique 0 et $M = [x, y, z]$ un point de $\mathcal{C}(k)$, on suppose que $M$ n'est pas un point d'inflexion de $\mathcal{C}$. Au point $M$ correspond comme ci-dessus, via $\theta$, un couple $(E, u)$, unique à isomorphisme près. La courbe elliptique $E$ est donc unique à un $k$-isomorphisme près. Rappelons la formule de Klein (cf. [Klein 1878]) donnant $j(E)$ en fonction de $x, y, z$. Comme dans loc. cit. on introduit d'abord, pour tout polynôme $f$ en $x, y, z$ les polynômes suivants:

$$\nabla(f) = \frac{1}{54}\begin{vmatrix} \frac{\partial^2 f}{\partial x^2} & \frac{\partial^2 f}{\partial x \partial y} & \frac{\partial^2 f}{\partial x \partial z} \\ \frac{\partial^2 f}{\partial y \partial x} & \frac{\partial^2 f}{\partial y^2} & \frac{\partial^2 f}{\partial y \partial z} \\ \frac{\partial^2 f}{\partial z \partial x} & \frac{\partial^2 f}{\partial z \partial y} & \frac{\partial^2 f}{\partial z^2} \end{vmatrix}$$

$$C(f) = \frac{1}{9}\begin{vmatrix} \frac{\partial^2 f}{\partial x^2} & \frac{\partial^2 f}{\partial x \partial y} & \frac{\partial^2 f}{\partial x \partial z} & \frac{\partial \nabla}{\partial x} \\ \frac{\partial^2 f}{\partial y \partial x} & \frac{\partial^2 f}{\partial y^2} & \frac{\partial^2 f}{\partial y \partial z} & \frac{\partial \nabla}{\partial y} \\ \frac{\partial^2 f}{\partial z \partial x} & \frac{\partial^2 f}{\partial z \partial y} & \frac{\partial^2 f}{\partial z^2} & \frac{\partial \nabla}{\partial z} \\ \frac{\partial \nabla}{\partial x} & \frac{\partial \nabla}{\partial y} & \frac{\partial \nabla}{\partial z} & 0 \end{vmatrix},$$

$$K(f) = \frac{1}{14}\begin{vmatrix} \frac{\partial f}{\partial x} & \frac{\partial \nabla}{\partial x} & \frac{\partial C}{\partial x} \\ \frac{\partial f}{\partial y} & \frac{\partial \nabla}{\partial y} & \frac{\partial C}{\partial y} \\ \frac{\partial f}{\partial z} & \frac{\partial \nabla}{\partial z} & \frac{\partial C}{\partial z} \end{vmatrix}.$$

À un coefficient multiplicatif près, $\nabla$ est le hessien de $f$ et $K$ est le wronskien de $f, \nabla, C$. Si $f$ est homogène de degré 4, les polynômes $\nabla(f), C(f), K(f)$ sont homogènes de degré $6, 14, 21$, respectivement. Si l'on multiplie $f$ par un scalaire $\lambda$, $\nabla(f), C(f), K(f)$ sont multipliés par $\lambda^3, \lambda^8, \lambda^{12}$, respectivement. Par ailleurs, soient $f \in k[x, y, z]$ et $F \in k[X, Y, Z]$ deux polynômes se déduisant l'un de l'autre par un changement de variables

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = B \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}, \quad B \in \mathrm{GL}_3(k) \tag{3–6}$$

i.e., $f(x, y, z) = F(X, Y, Z)$. On a alors:

$$\nabla(F)(X, Y, Z) = (\det B)^2 \nabla(f)(x, y, z), \tag{3–7}$$

$$C(F)(X, Y, Z) = (\det B)^6 C(f)(x, y, z), \tag{3–8}$$

$$K(F)(X, Y, Z) = (\det B)^9 K(f)(x, y, z). \tag{3–9}$$

Cela étant, revenons à $M \in \mathcal{C}(k)$ et au couple $(E, u)$ correspondant. Notons $F$ le premier membre de l'équation (3–1), et posons $\nabla = \nabla(F)(x, y, z)$, de même pour $C$ et $K$. Dans loc. cit., Klein donne les formules suivantes (en remplaçant $j$ par $1728J$):

$$j(E) = \frac{-C^3}{\nabla^7}, \quad j(E) - 1728 = \frac{-K^2}{\nabla^7}, \tag{3–10}$$

la seconde formule résultant de la première, compte tenu de la congruence ci-dessous:

$$C(F)^3 - K(F)^2 \equiv -1728\, \nabla(F)^7 \mod F. \tag{3–11}$$

En fait, dans un modèle de $E$ sur $k$ convenable, on a:

$$c_4(E) = C\,(-xyz)^2, \quad c_6(E) = K\,(-xyz)^3. \tag{3–12}$$

Ceci se démontre à l'aide notamment des formules (3–2) à (3–5).

## 4. L'IDÉE GÉNÉRALE DE LA DÉMONSTRATION

### 4.1 Préliminaires

Le théorème 2.1 est une conséquence du théorème 2.2, comme nous le verrons. Soient donc $k$ un corps de carac-téristique 0 et $E/k$ une courbe elliptique ayant tous ses points d'ordre 2. On suppose que $E$ est définie par l'équation (2–3). On observe d'abord que $Y_E(7)(k)$ possède quatre points triviaux évidents $\xi_0, \xi_a, \xi_b, \xi_c$. Le point $\xi_0$ correspond au couple $\left(E, 1_{E[7]}\right)$, comme signalé dans l'introduction. Notons ensuite $E_a$ la courbe elliptique sur $k$ quotient de $E$ par le sous-groupe de $E(k)$ engendré par le point $(a, 0)$, et soit $\varphi_a$ une $k$-isogénie de $E$ sur $E_a$ ayant pour noyau ledit sous-groupe. On peut par exemple appliquer les formules de [Vélu 71] pour obtenir $E_a$ et $\varphi_a$. L'isogénie $\varphi_a$ induit un isomorphisme de $E[7]$ sur $E_a[7]$, noté encore $\varphi_a$; puisque l'isogénie $\varphi_a$ est de degré 2, $2\varphi_a$ est un isomorphisme symplectique de $G_k$-modules de $E[7]$ sur $E_a[7]$. Le point $\xi_a$ est alors le point de $Y_E(k)$ correspondant au couple $(E_a, 2\varphi_a)$. Noter que $\xi_a$ ne dépend pas du choix de $\varphi_a$. On définit de même $\xi_b, \xi_c$ à partir de $E_b, \varphi_b, E_c, \varphi_c$.

La courbe $X_E(7)$ est de genre 3 et n'est pas hyperelliptique. Il existe donc un $k$-plongement de $X_E(7)$ dans $\mathbb{P}^2$, unique à une homographie de $\mathbb{P}^2(k)$ près, et son image est une quartique lisse $\mathcal{C}_E$ de $\mathbb{P}^2$ définie sur $k$. Tout le problème est d'expliciter une telle quartique! Dans ce qui vient d'être dit, on peut évidemment remplacer $k$ par $\overline{k}$.

Choisissons maintenant un isomorphisme symplectique $u$ de $A(\overline{k})$ sur $E[7]$. Associons à $u$ un $\overline{k}$-isomorphisme $t$ de $X_E(7)$ sur $X(7)$ vérifiant les propriétés (a) et (b) de la section 3. Soit $\theta$ le $k$-isomorphisme de $X(7)$ sur $\mathcal{C}$ précisé dans la section 3. D'après l'alinéa précédent, $\theta \circ t$ étant un $\overline{k}$-plongement de $X_E(7)$ dans $\mathbb{P}^2$,

il existe une homographie $h$ de $\mathbb{P}^2(\overline{k})$ telle que le composé $\psi$ ci-dessous:

$$\psi \,:\, X_E(7) \xrightarrow{\ t\ } X(7) \xrightarrow{\ \theta\ } \mathcal{C} \xrightarrow{\ h\ } \mathbb{P}^2$$

soit un $k$-plongement de $X_E(7)$ dans $\mathbb{P}^2$. Ici $h$ désigne en fait la restriction de $h$ à $\mathcal{C}$.

Indiquons une façon de choisir l'homographie $h$. Notons $M_0, M_a, M_b, M_c \in \mathcal{C}(\overline{k})$ les images par $\theta\circ t$ des points $\xi_0, \xi_a, \xi_b, \xi_c$, respectivement. Admettons provisoirement le lemme suivant:

**Lemme 4.1.** *Les points $M_0, M_a, M_b, M_c \in \mathcal{C}(\overline{k})$ forment un repère projectif de $\mathbb{P}^2(\overline{k})$.*

Ce lemme étant admis, il existe une unique homographie $h$ de $\mathbb{P}^2(\overline{k})$ appliquant les points $M_0, M_a, M_b, M_c$ sur les points $[1,1,1], [1,0,0], [0,1,0], [0,0,1]$, respectivement. Vérifions que le composé $\psi$ correspondant à ce choix de $h$ est défini sur $k$. Soit $\sigma$ un élément de $G_k$. Il existe une homographie $h'$ de $\mathbb{P}^2(\overline{k})$ telle que $\psi^\sigma = h' \circ \psi$. Puisque les points $\xi_0, \xi_a, \xi_b, \xi_c$ sont rationnels sur $k$, les images de chacun d'eux par $\psi$ et $\psi^\sigma$ sont égales. On en déduit que $h'$ laisse fixes les points $[1,1,1], [1,0,0], [0,1,0], [0,0,1]$, c'est donc l'identité, d'où notre assertion. Ainsi $\psi$ définit un $k$-isomorphisme de $X_E(7)$ sur $h(\mathcal{C})$, qui est la quartique $\mathcal{C}_E$ cherchée. Noter que $\psi$ ne dépend ni de $\overline{k}$ ni de $u$.

Pour démontrer le théorème 2.2, on devra expliciter les points $M_0, M_a, M_b, M_c$ de $\mathcal{C}(\overline{k})$, en déduire $h$, puis une équation de $\mathcal{C}_E$. Rappelons ici que $t$ vérifie la propriété (b) de la section 3. Les points $M_0, M_a, M_b, M_c$ sont donc les images respectives par $\theta$ des points de $Y(7)(\overline{k})$ correspondant aux couples $(E,u), (E_a, 2\varphi_a \circ u), (E_b, 2\varphi_b \circ u), (E_c, 2\varphi_c \circ u)$. Dans la suite, on écrira les points $M_0, M_a, M_b, M_c$ sous la forme:

$$M_0 \,=\, [X_0, Y_0, 1] \;\; ; \;\; M_a \,=\, [X_a, Y_a, 1]\,;$$

$$M_b \,=\, [X_b, Y_b, 1] \;\; ; \;\; M_c \,=\, [X_c, Y_c, 1]\,.$$

### 4.2 Mise en œuvre numérique

En fait, nous avons d'abord obtenu expérimentalement l'équation (2–4) de $\mathcal{C}_E$ figurant dans le théorème 2.2. Soit $E/\mathbb{Q}$ une courbe elliptique définie par l'équation (2–3), $a, b, c$ étant des nombres rationnels. Posons $\zeta = \exp(2i\pi/7)$, et soit $(P,Q)$ une base de $E[7]$ symplectique pour ce choix de $\zeta$. Soient $u$ l'isomorphisme de $A$ sur $E[7]$ appliquant $(1,1), (0,\zeta)$ sur $P, Q$, respectivement, et $t$ le $\mathbb{C}$-isomorphisme de $X_E(7)$ sur $X(7)$ correspondant. On calcule les coordonnées des points $P, Q$, de manière approchée, en paramétrant $E(\mathbb{C})$ par une fonction $\mathfrak{p}$ de Weierstrass convenable et sa dérivée. Via les formules (3–2) et (3–3), on en déduit des valeurs approchées de $X_0$ et $Y_0$. On explicite ensuite une équation de $E_a$, ainsi qu'une formule donnant $\varphi_a$, par exemple à l'aide des formules de Vélu ([Vélu 71]). On en déduit comme ci-dessus des valeurs approchées de $X_a, Y_a$, de même pour $X_b, Y_b, X_c, Y_c$. À ce stade, on peut déjà constater que le lemme 4.1 est vrai pour la courbe $E$ considérée. On connaît également, de manière approchée, l'homographie $h$, i.e. une matrice $3 \times 3$ la définissant. Via le changement de variables défini par $h$, l'équation de $\mathcal{C}$ est transformée en une équation approchée de $\mathcal{C}_E$, de la forme $Q(x,y,z) = 0$, où $Q$ est un polynôme homogène de degré 4. On constate alors que, si l'on divise $Q$ par l'un de ses coefficients non nuls, on obtient une équation de $\mathcal{C}_E$ très proche de l'équation (2–4). C'est ainsi que nous avons pu deviner l'équation (2–4) de $\mathcal{C}_E$.

### 4.3 La démonstration proprement dite

Reprenons les hypothèses et notations introduites en 4.1. Il s'agit de démontrer d'une part que le lemme 4.1 est vrai (pour le couple $(E,u)$), d'autre part que, à un coefficient non nul près, l'équation (2–4) du théorème 2.2 se déduit de l'équation de $\mathcal{C}$ par le changement de variables défini par l'homographie $h$. Pour cela, en vertu du principe de Lefschetz, on peut se limiter au cas où $k = \mathbb{C}$. De plus, la conclusion ne dépend que de la classe d'isomorphisme du couple $(E,u)$. On peut ainsi supposer qu'il existe un point $\tau \in \mathfrak{h}$ tel que $(E,u) = (E_\tau, u_\tau)$, avec les notations de la section 3, en particulier $E_\tau = \mathbb{C}^*/e^{2i\pi\tau\mathbb{Z}}$. Une équation de $E_\tau$ est:

$$y^2 \;=\; x^3 - 4g_2(\tau)x - 16g_3(\tau) \;=\; (x-a)(x-b)(x-c) \qquad (4\text{–}1)$$

où, en notant $\mathfrak{p}$ la fonction de Weierstrass associée au réseau $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$, on a posé:

$$a \;=\; 4\mathfrak{p}(1/2) \;\;,\;\; b \;=\; 4\mathfrak{p}(\tau/2) \;\;,\;\; c \;=\; 4\mathfrak{p}((\tau+1)/2)\,. \qquad (4\text{–}2)$$

Les formules (4–2) définissent des fonctions holomorphes $a, b, c$ sur $\mathfrak{h}$, elles induisent des fonctions modulaires de poids 2 sur $X(2)$, notées aussi $a, b, c$.

Associons en général, à tout $\tau \in \mathfrak{h}$, les points $M_0, M_a, M_b, M_c \in \mathcal{C}(\mathbb{C})$, comme à la section 4.1. Les coordonnées $X_0, Y_0, X_a, \ldots$ de ces points définissent des fonctions holomorphes et non nulles sur $\mathfrak{h}$. En fait ces fonctions induisent des fonctions méromorphes sur $X(14)$. En effet, notons $\pi_7$ le morphisme canonique de $X(14)$ sur $X(7)$ et de même $\pi_2$ le morphisme canonique de $X(14)$ sur $X(2)$. Soit par ailleurs $B_2 \,:\, X(14) \longrightarrow X(7)$ le

morphisme de dégénérescence, associant à la classe modulo $\Gamma(14)$ de tout $\tau \in \mathfrak{h}^*$ la classe modulo $\Gamma(7)$ de $2\tau$. Ces trois morphismes sont définis sur $\mathbb{Q}$. Considérons ensuite les deux matrices suivantes:

$$g \;=\; \begin{pmatrix} 5 & 0 \\ 0 & 3 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_7), \qquad \ell \;=\; \begin{pmatrix} 1 & 7 \\ 7 & 8 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/14\mathbb{Z})\,.$$

Notons enfin $X, Y \in \mathbb{Q}(X(7))$ les coordonnées de $\theta$. On a alors:

$$\begin{cases} (X_0, Y_0) \;=\; (X, Y) \circ \pi_7 \;\;,\;\; (X_a, Y_a) \;=\; (X, Y) \circ \widetilde{g} \circ B_2 \\ (X_b, Y_b) \;=\; (X_a, Y_a) \circ \widetilde{\ell} \;\;,\;\; (X_c, Y_c) \;=\; (X_b, Y_b) \circ \widetilde{\ell}. \end{cases} \tag{4–3}$$

Ces formules résultent de la définition des points $\xi_0, \xi_a, \xi_b, \xi_c$ et de la courbe $E_\tau$ d'une part, de l'interprétation modulaire de $Y(7), Y_E(7)$ d'autre part. Elles montrent effectivement que les fonctions $X_0, Y_0, X_a, \ldots$ définissent des fonctions méromorphes sur $X(14)$, holomorphes et non nulles sur $Y(14)$. Les formules (4–3) permettent aussi de développer les fonctions considérées en les différentes pointes de $X(14)$, notamment à la pointe ordinaire $\infty$, classe de $1/14$. Commençons par les fonctions $X, Y$ sur $X(7)$. À l'aide des formules (3–4) et (3–5), ainsi que des développements en produit des formes de Klein (cf. [Lang 87]), on obtient pour $X, Y$ des développements de la forme ci-dessous, par rapport à l'uniformisante $w = \exp(2i\pi\tau/7)$:

$$\begin{aligned} X \;&=\; -w^3 \prod_{n=0}^{+\infty} \frac{\left(1 - w^{7(7n+1)}\right)\left(1 - w^{7(7n+6)}\right)}{\left(1 - w^{7(7n+3)}\right)\left(1 - w^{7(7n+4)}\right)} \\ Y \;&=\; w \prod_{n=0}^{+\infty} \frac{\left(1 - w^{7(7n+2)}\right)\left(1 - w^{7(7n+5)}\right)}{\left(1 - w^{7(7n+3)}\right)\left(1 - w^{7(7n+4)}\right)}\,, \end{aligned} \tag{4–4}$$

voir aussi [Elkies 99]. On déduit ensuite des formules (4–3) les développements suivants à la pointe $\infty$ de $X(14)$, par rapport à l'uniformisante $q = \exp(2i\pi\tau/14)$:

$$\begin{aligned} &X_0 = X(q^2), && Y_0 = Y(q^2), \\ &X_a = Y(q^4)/X(q^4), && Y_a = 1/X(q^4) \\ &X_b = 1/Y(q), && Y_b = X(q)/Y(q), \\ &X_c = 1/Y(-q), && Y_c = X(-q)/Y(-q). \end{aligned}$$

Ainsi, par exemple, le développement de $X_0$ s'obtient en remplaçant $w$ par $q^2$ dans le membre de droite de la première formule (4–4).

Considérons maintenant les déterminants suivants:

$$D_0 \;=\; \begin{vmatrix} X_a & X_b & X_c \\ Y_a & Y_b & Y_c \\ 1 & 1 & 1 \end{vmatrix}\,,\; D_a \;=\; \begin{vmatrix} X_0 & X_b & X_c \\ Y_0 & Y_b & Y_c \\ 1 & 1 & 1 \end{vmatrix}\,,$$

$$D_b \;=\; \begin{vmatrix} X_0 & X_c & X_a \\ Y_0 & Y_c & Y_a \\ 1 & 1 & 1 \end{vmatrix}\,,\; D_c \;=\; \begin{vmatrix} X_0 & X_a & X_b \\ Y_0 & Y_a & Y_b \\ 1 & 1 & 1 \end{vmatrix}\,.$$

Ces déterminants sont des fonctions méromorphes sur $X(14)$, on vérifie que leurs diviseurs sont concentrés aux pointes de $X(14)$, ce qui prouve déjà le lemme 4.1. Définissons aussi sur $X(14)$ trois fonctions méromorphes $\lambda_a, \lambda_b, \lambda_c$ comme suit:

$$\lambda_a \;=\; \frac{D_a}{D_0} \;\;,\;\; \lambda_b \;=\; \frac{D_b}{D_0} \;\;,\;\; \lambda_c \;=\; \frac{D_c}{D_0}\,.$$

Comme à la section 4.1, considérons l'homographie $h$ de $\mathbb{P}^2$ appliquant les points $M_0, M_a, M_b, M_c$ correspondant à un $\tau \in \mathfrak{h}$ fixé sur les points $[1,1,1], [1,0,0], [0,1,0], [0,0,1]$, respectivement. L'homographie $h^{-1}$ est définie par la matrice suivante:

$$W \;=\; \begin{pmatrix} \lambda_a X_a & \lambda_b X_b & \lambda_c X_c \\ \lambda_a Y_a & \lambda_b Y_b & \lambda_c Y_c \\ \lambda_a & \lambda_b & \lambda_c \end{pmatrix}. \tag{4–5}$$

Il en résulte que les formules

$$\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \;=\; W \begin{pmatrix} x \\ y \\ z \end{pmatrix} \tag{4–6}$$

transforment l'équation (3–1) de la quartique de Klein $\mathcal{C}$ en une équation de $\mathcal{C}_E$, de la forme $\Phi(x, y, z) = 0$, où $\Phi$ est un polynôme homogène de degré 4 à coefficients dans le corps des fonctions $\mathbb{C}(X(14))$. Il nous suffit de vérifier que, pour tout $\tau \in \mathfrak{h}$, le polynôme $\Phi$ évalué en $\tau$ est égal, à un coefficient multiplicatif non nul près, au polynôme $Q$ défini en (2–4), à partir des valeurs de $a, b, c$ données par les formules (4–2). Pour cela, considérons sur $X(14)$ la fonction méromorphe $\lambda$ définie par

$$\lambda \;=\; \left(\frac{c-a}{b-a}\right) \circ \pi_2\,.$$

Il s'agit donc de vérifier que $\Phi$ est produit du polynôme suivant:

$$\Psi(x, y, z) \;=\; (\lambda - 1)\mathfrak{q}(x, y, z) - \lambda\mathfrak{q}(y, z, x) + \mathfrak{q}(z, x, y)$$

par une fonction méromorphe sur $X(14)$, holomorphe et non nulle sur $Y(14)$. On obtient le $q$-développement de $\lambda$ à la pointe $\infty$ à partir des développements classiques de $a, b, c$, cf. le théorème I.6.2 de [Silverman 94], ou directement à partir des formes de Klein:

$$\lambda(\tau) \;=\; \left[\prod_{n=0}^{+\infty} \left(1 - q^{7(2n+1)}\right)^8\right] \Bigg/ \left[\prod_{n=0}^{+\infty} \left(1 + q^{7(2n+1)}\right)^8\right], \qquad q = \exp\left(2\pi i\tau/14\right).$$

Soit finalement $\alpha$ le coefficient de $x^3y$ dans $\Phi$. On vérifie que la fonction $\alpha$ est holomorphe et non nulle sur $Y(14)$. On établit ensuite l'égalité suivante, dont le théorème 2.2 est une conséquence:

$$\Phi/\alpha \;=\; \Psi/(\lambda-1)\,. \tag{4–7}$$

Pour ce faire, notons $f \in \mathbb{C}(X(14))$ l'un des coefficients de la différence entre les deux membres de cette égalité, différence qui est un polynôme en $x, y, z$. On commence par majorer le degré du diviseur des pôles de $f$, soit $M$ un tel majorant. Pour voir que $f = 0$, il suffit de démontrer que l'ordre de $f$ à la pointe $\infty$ est au moins $M+1$. Le $q$-développement de $f$ en $\infty$ est obtenu en utilisant tous les développements intermédiaires évoqués plus haut (ceux de $X, Y, X_0, X_a, \ldots, D_0, D_a, \lambda_a, \lambda, \ldots$). À titre d'exemple (le moins favorable), si $f$ est le coefficient de $y^3z$ dans la différence ci-dessus, il suffit de montrer que l'ordre de $f$ en $\infty$ est au moins 742, i.e., que $f(\tau) = O(q^{742})$, où $q = \exp(2i\pi\tau/14)$.

**Remarque 4.2.** Les détails de la démonstration de l'égalité (4–7) ne peuvent être donnés ici, faute de place. Le lecteur intéressé pourra trouver à l'adresse suivante: http://www.math.jussieu.fr/~halberst/xe7.txt un texte donnant les détails en question. Il trouvera aussi un programme appelé xe7.prog permettant notamment d'obtenir, à un ordre donné, les différents $q$-développements nécessaires. Ce programme utilise le logiciel de calcul GP.Pari (cf. [Batut et al. 97]).

### 4.4 Passage du théorème 2.2 au théorème 2.1

Soient $E$ une courbe elliptique sur un corps $k$ de caractéristique 0. On suppose $E$ donnée par l'équation

$$y^2 \;=\; x^3 + a_4x + a_6\,. \tag{4–8}$$

Soit $L$ le sous-corps de $\overline{k}$ engendré sur $k$ par les abscisses $a, b, c$ des points d'ordre 2 de $E$. Appliquons le théorème 2.2 à la courbe elliptique $E$ sur $L$. Reprenons les notations introduites en 4.1, en remplaçant le corps $k$ par $L$. On dispose ainsi d'un $L$-plongement $\psi$ de $X_E(7)$ dans $\mathbb{P}^2$ appliquant les points $\xi, \xi_a, \xi_b, \xi_c$ sur $[1,1,1], [1,0,0], [0,1,0], [0,0,1]$, respectivement. Observons que $\xi$ est défini sur $k$, alors que $\xi_a, \xi_b, \xi_c$ sont a priori définis sur $L$. Soit $r$ l'homographie de $\mathbb{P}^2(L)$ appliquant les points $[1,1,1], [1,0,0], [0,1,0], [0,0,1]$, respectivement sur les points

$$N = [0,1,0]\ ,\ N_a \;=\; [a, a^2, 1]\ ,$$
$$N_b = [b, b^2, 1]\ ,\ N_c \;=\; [c, c^2, 1]\,.$$

Soit $\psi' = r \circ \psi$. On vérifie d'abord que $\psi'$ est défini sur $k$. Soit en effet $\sigma$ un élément de $G_k$. Notons que $\sigma$ laisse stable $\{a, b, c\}$. On a $\xi_a^\sigma = \xi_{\sigma(a)}$. En effet, $\xi_a$ correspond à la classe d'isomorphisme du couple $(E_a, 2\varphi_a)$ donc, par fonctorialité de la bijection signalée dans la propriété (a) de la section 3, $\xi_a^\sigma$ correspond à la classe du couple $(E_a^\sigma, 2\varphi_a^\sigma)$. Les formules de [Vélu 71] montrent que $E_a^\sigma = E_{\sigma(a)}$ et $\varphi_a^\sigma = \varphi_{\sigma(a)}$, d'où l'égalité annoncée. De même on a $\xi_b^\sigma = \xi_{\sigma(b)}$ et $\xi_c^\sigma = \xi_{\sigma(c)}$. Par ailleurs on a $N^\sigma = N$ et $N_a^\sigma = N_{\sigma(a)}$, de même pour $b$ et $c$. Puisque $(N, N_a, N_b, N_c)$ est un repère projectif de $\mathbb{P}^2$, on en déduit, par le même argument qu'en 4.1, que $\psi'^\sigma = \psi'$, i.e., que $\psi'$ est un $k$-plongement de $X_E(7)$ dans $\mathbb{P}^2$.

L'homographie $r^{-1}$ est représentée par la matrice suivante:

$$B \;=\; \begin{pmatrix} b+c & -1 & -bc \\ c+a & -1 & -ca \\ a+b & -1 & -ab \end{pmatrix}\,.$$

Le théorème 2.2 fournit une équation $Q(x, y, z) = 0$ de $X_E(7)$ sur $L$. Pour en déduire une équation de $X_E(7)$ sur $k$, il suffit, puisque $\psi'$ est défini sur $k$, d'effectuer le changement de variables donné par

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \;=\; B \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}\,.$$

On obtient, à un coefficient multiplicatif près, l'équation

$$\begin{aligned} a_4X^4 + 7a_6X^3 + 3(Y^2 - a_4^2)X^2 - a_6(6Y + 5a_4)X \\ + (2Y^3 + 3a_4Y^2 + 2a_4^2Y - 4a_6^2) = 0 \end{aligned} \tag{4–9}$$

homogénéisée. D'où le théorème 2.1.

## 5. INTERPRÉTATION MODULAIRE

Soit $E$ une courbe elliptique sur un corps $k$ de caractéristique 0. À partir d'une équation de Weierstrass de $E$, le théorème 2.1 fournit un modèle de $X_E(7)$: on dispose d'un $k$-isomorphisme $\psi$ de $X_E(7)$ sur une certaine quartique projective plane $\mathcal{C}_E$. Soit $M = [x, y, z]$ un point de $\mathcal{C}_E(k)$. On suppose que $M$ n'est pas un point de Weierstrass (point d'inflexion) de $\mathcal{C}_E$, autrement dit que $M$ est l'image par $\psi$ d'un point $\eta$ de $Y_E(7)(k)$. Soit $(E', v)$ un couple correspondant au point $\eta$ comme dans la section 3. Ce couple est unique à isomorphisme près. En particulier l'invariant modulaire $j(E')$ ne dépend que de $E$ et $M$. L'interprétation modulaire de $\mathcal{C}_E$ consiste d'abord à expliciter $j(E')$ en fonction de $x, y, z$ et des

coefficients de $E$. Soit $P$ l'homogénéisé du premier membre de l'égalité (2–2):

$$P = ax^4 + 7bx^3z + 3(y^2 - a^2z^2)x^2 - b(6y + 5az)xz^2 + z(2y^3 + 3ay^2z + 2a^2yz^2 - 4b^2z^3)\,. \tag{5–1}$$

**Théorème 5.1.** *Avec les notations précédentes, l'invariant modulaire $j(E')$ est donné, en fonction des invariants $\nabla, C, K$ de $P$ calculés en $(x, y, z)$, par la formule*

$$j(E') \;=\; \frac{-4\,C^3}{\Delta_{\scriptscriptstyle E}\,\nabla^7}\,, \tag{5–2}$$

*en notant $\Delta_{\scriptscriptstyle E} = -16(4a^3 + 27b^2)$ le discriminant du modèle (2–1) de $E$, et en posant $\nabla = \nabla(P)(x, y, z)$, idem pour $C$ et $K$.*

*Preuve:* Reprenons les notations de la section 3.1. On dispose d'un $k$-isomorphisme $\psi$ de $X_{\scriptscriptstyle E}(7)$ sur $\mathcal{C}_{\scriptscriptstyle E}$, obtenu À l'aide d'une certaine homographie $h$ de $\mathcal{C}$ sur $\mathcal{C}_{\scriptscriptstyle E}$. Cette homographie est définie par une certaine matrice $B \in \mathrm{GL}_3(\overline{k})$. Soit $N = h^{-1}(M) \in \mathcal{C}(\overline{k})$. On a donc $N = [X, Y, Z]$, où $X, Y, Z$ se déduisent de $x, y, z$ à l'aide du changement de variables (3–6). Il existe ainsi un élément $\lambda$ de $\overline{k}^*$ tel que, en notant toujours $F$ le premier membre de (3–1), on ait:

$$P(x, y, z) \;=\; \lambda\,F(X, Y, Z)\,.$$

Écrivons par exemple $C(F)$ au lieu de $C(F)(X, Y, Z)$ et $C(P)$ au lieu de $C(P)(x, y, z)$. On déduit des formules (3–7) à (3–9) les relations suivantes:

$$\begin{aligned}(\det B)^2\,\nabla(P) &= \lambda^3\,\nabla(F)\,,\\ (\det B)^6\,C(P) &= \lambda^8\,C(F)\,,\\ (\det B)^9\,K(P) &= \lambda^{12}\,K(F)\,.\end{aligned}$$

Par ailleurs, vu la construction de $\psi$, le couple correspondant au point $N \in \mathcal{C}(\overline{k})$ est $(E', v \circ u)$, cf. la propriété (b) en 4.1. On déduit alors des formules précédentes et des formules (3–10) les égalités suivantes:

$$j(E') \;=\; \alpha\,\frac{C(P)^3}{\nabla(P)^7}\,,\quad j(E') - 1728 \;=\; \alpha\,\frac{K(P)^2}{\nabla(P)^7}\,, \tag{5–3}$$

où $\alpha = -(\det B)^4\lambda^{-3}$ est indépendant du point $M = [x, y, z]$ considéré. Pour déterminer $\alpha$, prenons $(x, y, z) = (0, 1, 0)$. En ce point, on constate que l'on a:

$$\nabla(P) \;= -4\,,\quad C(P) \;=\; -768\,a\,,\quad K(P) \;=\; 55296\,b\,.$$

De plus, dans ce cas $E' = E$, et donc les formules (5–3) s'écrivent ainsi:

$$j(E) \;=\; \alpha\,\frac{768^3a^3}{4^7},\quad j(E) - 1728 \;=\; -\alpha\,\frac{55296^2b^2}{4^7}\,.$$

Par ailleurs, on a:

$$\begin{aligned}j(E) \;&=\; \frac{c_4(E)^3}{\Delta_{\scriptscriptstyle E}} \;=\; \frac{-(48a)^3}{\Delta_{\scriptscriptstyle E}},\\ j(E) - 1728 &= \frac{c_6(E)^2}{\Delta_{\scriptscriptstyle E}} \;=\; \frac{(864b)^2}{\Delta_{\scriptscriptstyle E}}\,.\end{aligned}$$

On en déduit que $\alpha = -4/\Delta_{\scriptscriptstyle E}$, ce qui démontre le théorème, compte tenu de (5–3). □

Le théorème 5.1 détermine $E'$ à un $\overline{k}$-isomorphisme près. Le théorème suivant donne $E'$ à un $k$-isomorphisme près.

**Théorème 5.2.** *On garde les notations du théorème 5.1. Considérons le polynôme $V$ défini par*

$$V \;=\; ax^2 + 3bxz + 2ayz + 3y^2. \tag{5–4}$$

*Posons aussi*

$$V \;=\; V(x, y, z) \;\;\textit{et}\;\; d \;=\; 2zV. \tag{5–5}$$

*Soit $E''/k$ la courbe elliptique d'équation*

$$y^2 \;=\; x^3 - \frac{Cd^2}{48}\,x - \frac{Kd^3}{864}. \tag{5–6}$$

*Supposons $d \neq 0$ (cf. la remarque 5.3), de sorte que l'équation (4–6) définit effectivement une courbe elliptique $E''$. Alors $E'$ est $k$-isomorphe à $E''$.*

Nous donnerons l'idée de la démonstration de ce théorème à la fin de la section 7. Contentons-nous ici de quelques remarques.

**Remarque 5.3.** Soit $\mathcal{D}$ la conique d'équation $V = 0$. Cette conique est non-dégénérée, parce que $4a^3 + 27b^2 \neq 0$. Soit $\mathcal{L}$ la tangente à $\mathcal{C}_{\scriptscriptstyle E}$ au point-base $[0, 1, 0]$, i.e., la droite d'équation $z = 0$. Cette tangente recoupe $\mathcal{C}_{\scriptscriptstyle E}$ en deux points $M', M''$ distincts du point-base. Noter que $M' = M''$, i.e., $\mathcal{L}$ est l'une des 28 bitangentes à $\mathcal{C}_{\scriptscriptstyle E}$, si et seulement si $a = 0$, soit $j(E) = 0$. On constate que $\mathcal{D}$ passe par les points $M', M''$ (elle est tangente à $\mathcal{L}$ en $M'$ lorsque $j(E) = 0$). Par ailleurs, $\mathcal{D}$ est tangente à $\mathcal{C}_{\scriptscriptstyle E}$ en chacun des trois points (que l'on notera abusivement $M_a, M_b, M_c$) de $\mathcal{C}_{\scriptscriptstyle E}(\overline{k})$ correspondant à $\xi_a, \xi_b, \xi_c$. Pour le voir, on se place dans un modèle de Legendre (2-3) de $E$. Dans ce modèle, l'équation de $\mathcal{D}$ s'écrit $xy + yz + zx = 0$, d'où la conclusion, puisqu'alors

$$M_a \;=\; [1, 0, 0]\,,\quad M_b \;=\; [0, 1, 0]\,,\quad M_c \;=\; [0, 0, 1]\,.$$

Revenons aux notations du théorème. Si $M$ correspond au point $\xi_0$, $E'$ est isomorphe à $E$. Si $M$ correspond à

l'un des points $\xi_a, \xi_b, \xi_c$, $E'$ est liée à $E$ par une isogénie de degré 2 (définie sur $k$ par hypothèse), les formules de Vélu permettent donc d'expliciter $E'$. Si $M$ est l'un des points $M', M''$ ci-dessus, on peut expliciter $E'$ avec les formules de [Halberstadt and Kraus 99], cf. la remarque 6.2. Dans tous les autres cas, $d \neq 0$, et donc le théorème 5.2 s'applique.

**Remarque 5.4.** D'abord $c_4(E'') = Cd^2$ et $c_6(E'') = Kd^3$. Si l'on multiplie $(x, y, z)$ par $\lambda(x, y, z), \lambda \in k^*$, $c_4(E'')$ et $c_6(E'')$ sont remplacés par $\lambda^{20}c_4(E'')$ et $\lambda^{30}c_6(E'')$, respectivement, ce qui ne change pas $E''$, à un $k$-isomorphisme près. Comme dans la preuve du théorème 5.1, on obtient ensuite:

$$\begin{aligned} C^3 - K^2 &= \lambda^{24}(\det B)^{-18}\big(C(F)^3 - K(F)^2\big) \\ &= -1728\,\lambda^{24}(\det B)^{-18}\,\nabla(F)^7 \;=\; 1728\frac{\nabla^7}{\alpha}, \end{aligned}$$

d'où en tous cas

$$j(E'') \;=\; \frac{1728C^3}{C^3 - K^2} \;=\; \alpha\,\frac{C^3}{\nabla^7} \;=\; j(E')\,.$$

**Remarque 5.5.** La formule (5–2) donnant $j(E')$ n'est pas intrinsèque: elle est valable dans le modèle (2–2) de $\mathcal{C}_E$. Il est facile d'en déduire une formule valable dans n'importe quel modèle de $\mathcal{C}_E$, donné par une équation $Q = 0$. Dans un tel modèle, si $M_0$ est le point-base de $\mathcal{C}_E$ et $M$ un point quelconque de $\mathcal{C}_E$ (pas un point d'inflexion), on a:

$$j(E') \;=\; j(E)\left(\frac{C(Q)(M)^3}{\nabla(Q)(M)^7}\right)\Big/\left(\frac{C(Q)(M_0)^3}{\nabla(Q)(M_0)^7}\right),$$

ceci si $j(E) \neq 0$. Si $j(E) = 0$, on a une formule analogue donnant $j(E') - 1728$ en fonction de $j(E) - 1728$, en remplaçant $C^3$ par $K^2$. On peut faire de même pour le théorème 5.2.

## 6. EXEMPLES

Soit $E$ une courbe elliptique sur $\mathbb{Q}$. Le fait de connaître une équation de $X_E(7)$ ne semble pas faciliter la détermination de tous les points rationnels de $X_E(7)$. En revanche, à partir d'une telle équation de $X_E(7)$, on peut souvent exhiber des points non triviaux de $X_E(7)$. Dans les tables de [Cremona 97], prenons par exemple pour $E$ la courbe $105A2$, d'équation

$$y^2 + xy + y \;=\; x^3 - 8x - 7\,.$$

La courbe $E$ a trois points d'ordre 2 sur $\mathbb{Q}$, un autre modèle de $E$ est le suivant:

$$y^2 \;=\; (x+9)(x+4)(x-12)\,.$$

Appliquons le théorème 2.2 avec $(a, b, c) = (-9, -4, 12)$. La courbe $X_E(7)$ est $\mathbb{Q}$-isomorphe à la quartique $\mathcal{C}_E$ d'équation:

$$\begin{aligned} 16\big[x^3(y+z) - 3x^2yz\big] - 21\big[y^3(z+x) - 3y^2zx\big] \\ + 5\big[z^3(x+y) - 3z^2xy\big] \;=\; 0\,. \end{aligned}$$

Hormis les quatre points triviaux, correspondant aux courbes elliptiques $E, E_a, E_b, E_c$, i.e., aux courbes 105A2, 105A1, 105A4, 105A3 des tables de [Cremona 97], on obtient sept points $M_1, \ldots, M_7$ de $\mathcal{C}_E(\mathbb{Q})$, à savoir:

$$\begin{aligned} &[-2, -1, 1],\ [-15, -10, 6],\ [-5, 30, 74],\ [7, 42, 74], \\ &[-1, -6, 2],\ [-1, -6, 6],\ [-7, 8, 56]\,. \end{aligned}$$

À chaque point $M_i$ correspond une courbe elliptique $E_i$, donnée par une équation minimale du type

$$y^2 + xy + y \;=\; x^3 + A_ix + B_i\,.$$

Voici les coefficients $A_i, B_i$, ainsi que les conducteurs $N(E_i)$:

$A_1 = 15\,684\,182,\ B_1 = 150\,979\,941\,971,\ N(E_1) = 105 \times 547$
$A_2 = 98\,426\,072,\ B_2 = -118\,058\,290\,177,\ N(E_2) = 105 \times 199$
$A_3 \;=\; 151\,862\,712\,344\,018\,927\,072,$
$N(E_3) \;=\; 105 \times 71\,323\,237$
$B_3 \;=\; 324\,025\,834\,222\,116\,840\,088\,628\,456\,381$
$A_4 \;=\; -110\,687\,109\,739\,114\,274\,754\,378,$
$N(E_4) = 105 \times 756\,324\,133$
$B_4 \;=\; 31\,996\,388\,741\,731\,654\,555\,310\,050\,009\,671\,673$
$A_5 \;=\; 658\,313\,627,\ B_5 \;=\; 62\,672\,650\,864\,103,$
$N(E_5) \;=\; 105 \times 31 \times 47$
$A_6 \;=\; -13\,067\,234\,953,\ B_6 \;=\; 579\,095\,758\,519\,181,$
$N(E_6) \;=\; 105 \times 19 \times 349$
$A_7 \;=\; -623\,567\,947\,331\,673,\ N(E_7) \;=\; 105 \times 103 \times 5\,021$
$B_7 \;=\; -6\,949\,399\,992\,965\,765\,557\,397\,.$

Les huit courbes elliptiques $E, E_1, \ldots, E_7$ sont deux à deux non isogènes sur $\mathbb{Q}$, mais les représentations de Galois modulo 7 associées sont symplectiquement isomorphes.

Voici deux autres courbes elliptiques fournissant chacune un huituplet comme ci-dessus:

(a) la courbe elliptique notée 106B1 dans les tables de [Cremona 97], ayant pour équation: $y^2 + xy = x^3 + x^2 - 7x + 5$;

(b) la courbe de conducteur 1785 ayant pour équation: $y^2 + xy = x^3 + x^2 - 2x - 9$.

**Remarque 6.1.** Sans le théorème 2.2, il n'est pas évident de montrer directement, par exemple, que les représentations de Galois dans $E[7]$ et $E_4[7]$ sont isomorphes. En appliquant la proposition 4 de [Kraus et Oesterlé 92], il faudrait vérifier que, pour tout nombre premier $p < 24\,202\,372\,256$ ne divisant pas $N(E_4)$, $a_p(E)$ et $a_p(E_4)$ sont congrus modulo 7! Une autre solution consisterait à déterminer deux corps de nombres $k, k'$ de degré 8 sur $\mathbb{Q}$ tels que $E$ (resp. $E_4$) possède sur $k$ (resp. $k'$) un sous-groupe cyclique d'ordre 7 stable par Galois, puis à vérifier que $k$ et $k'$ sont isomorphes.

**Remarque 6.2.** Reprenons les notations du théorème 2.1, fournissant un modèle $\mathcal{C}_E$ pour $X_E(7)$. Le point-base $\xi$ de $Y_E(7)$ correspond, on l'a vu, au point $P = [0,1,0]$ de $\mathcal{C}_E$. La tangente en $P$ à $\mathcal{C}_E$ est la droite $z = 0$, elle recoupe $\mathcal{C}_E$ en deux points, qui sont rationnels sur $k$ si et seulement si $-3a$ est un carré dans $k$, i.e., si $c_4(E)$ est un carré dans $k$. On obtient ainsi une explication géométrique du fait signalé dans [Halberstadt and Kraus 99], à savoir que, dès que $c_4(E)$ est un carré, la courbe $X_E(7)$ possède un point rationnel autre que le point-base, et en général c'est un point non trivial de $Y_E(7)$. Dans l'exemple ci-dessus, on obtiendrait ainsi les points $M_2, M_7$ de $\mathcal{C}_E$.

Voici deux questions naturelles, auxquelles nous ne savons pas répondre. Quels sont les entiers $k > 1$ pour lesquels il existe un $k$-uplet de courbes elliptiques sur $\mathbb{Q}$, deux à deux non isogènes sur $\mathbb{Q}$, dont les représentations de Galois modulo 7 sont symplectiquement isomorphes? Plus précisément, quelle est la borne supérieure $K_1$ de l'ensemble de ces entiers $k$? Si l'on admet la conjecture uniforme (cf. [Caporaso et al 95]), cette borne est finie. On peut poser la même question en exigeant cette fois qu'il existe une infinité (en un sens évident) de tels $k$-uplets, d'où une autre borne supérieure $K_2$. Evidemment $K_2 \leq K_1$. D'après l'exemple ci-dessus, $K_1 \geq 8$. La minoration $K_2 \geq 5$ résulte du théorème 2 de [Halberstadt and Kraus 99]. On peut en fait améliorer cette minoration, grâce au théorème 2.1:

**Proposition 6.3.** *Avec les notations ci-dessus, on a* $K_2 \geq 6$.

*Preuve:* Soit $k$ un corps de caractéristique 0. Pour tout $u \in k$ distinct de $\pm 2$, soit $A_u$ la courbe elliptique d'équation

$$y^2 = x^3 - 3x + u\,.$$

D'après le théorème 2.1, la courbe $X_{A_u}(7)$ est $k$-isomorphe à la quartique $\mathcal{A}_u$, complétée projective de la courbe d'équation

$$\begin{aligned} 3x^4 - 7ux^3 - 3(y^2-9)x^2 + 3u(2y-5)x \\ - (2y^3 - 9y^2 + 18y - 4u^2) = 0\,. \end{aligned} \tag{6–1}$$

On dispose déjà de trois points de $\mathcal{A}_u(k)$ (la remarque 6.2 s'applique, car $c_4(A_u) = 144$): $M_1 = [0,1,0]$, correspondant à la courbe $A_u$, et $M_2 = [1,1,0]$, $M_3 = [-1,1,0]$. Cela étant, considérons l'équation (6–1) comme une équation du second degré en $u$. Son discriminant est:

$$\begin{aligned} D(x,y) = 49x^6 + (162 - 84y)x^4 + (84y^2 - 180y - 207)x \\ + (32y^3 - 144y^2 + 288y)\,. \end{aligned} \tag{6–2}$$

On constate que $D(x,x^2) = \Big[9x(x^2-1)\Big]^2$. Si l'on remplace $y$ par $x^2$ dans l'équation (6–1), cette équation en $u$ a deux solutions, l'une d'elles étant: $(5x^3 + 3x)/4$. Ceci suggère de considérer la courbe elliptique $E$ sur $\mathbb{Q}(T)$ définie par l'équation

$$y^2 = x^3 - 3x + (5T^3 + 3T)/4\,.$$

La quartique correspondante possède sur $\mathbb{Q}(T)$ quatre points rationnels, à savoir les points $M_1, M_2, M_3$ ci-dessus, et le point $[T, T^2, 1]$. Soit $t \neq \pm 1$ un nombre rationnel. Spécialisons $E$ en $t$. On obtient une courbe elliptique $E_t$ telle que $X_{E_t}(\mathbb{Q})$ possède au moins quatre points: la quartique $\mathcal{C}_t$ correspondante passe par les points $M_1, M_2, M_3$ et $M_4 = [t, t^2, 1]$. La droite $M_1M_4$, d'équation $x = tz$, recoupe $\mathcal{C}_t$ en deux points $M_5, M_6$, qui sont rationnels sur $\mathbb{Q}$ si et seulement si $(t^2-1)(5t^2+7)$ est un carré. Considérons donc la courbe d'équation

$$v^2 = (t^2-1)(5t^2+7). \tag{6–3}$$

La compactifiée lisse de cette courbe est $\mathbb{Q}$-isomorphe à la courbe elliptique d'équation $y^2 = x^3 - x^2 + 9x$, i.e., à la courbe 840E1 des tables de [Cremona 97]. Cette courbe elliptique étant de rang 1 sur $\mathbb{Q}$, l'équation (6–3) possède une infinité de solutions sur $\mathbb{Q}$. Soit $(t,v)$ l'une de ces solutions, $t \neq \pm 1, \pm 2$. Les six points $M_1, \ldots, M_6$ de $\mathcal{C}_t$ correspondants sont alors distincts. Ces points correspondent à six courbes elliptiques $F_1, \ldots, F_6$ sur $\mathbb{Q}$, bien définies à $\mathbb{Q}$-isomorphisme près, $F_1 = E_t$. Prenons par exemple $(t,v) = (43/11,\, 4176/11^2)$. On vérifie dans ce

cas que les six courbes elliptiques $F_i$ obtenues sont deux à deux non isogènes sur $\mathbb{Q}$. Par des arguments standard on en déduit que, pour presque tous les couples $(t,v) \in \mathbb{Q}^2$ solutions de l'équation (6–3), les six courbes elliptiques $F_i$ correspondantes sont deux à deux non isogènes sur $\mathbb{Q}$. La proposition 6.3 en résulte aussitôt. □

## 7. UN CAS PARTICULIER DU THÉORÈME 2.1

On se place ici sous les hypothèses du théorème 2.1. On suppose de plus que $E[7]$ possède un $\mu_7$, i.e., un sous-module galoisien $C$ isomorphe à $\mu_7$. Avec les notations de 4.1, choisissons un isomorphisme symplectique $u$ de $A(\overline{k})$ sur $E[7]$ tel que $u(\mu_7) = C$, et associons à $u$ un $\overline{k}$-isomorphisme $t$ de $X_E(7)$ sur $X(7)$. Les images par $t^{-1}$ des pointes $P_1, P_2, P_3$ de $X(7)$ sont alors rationnelles sur $k$. On en déduit aisément que $X_E(7)$ possède sur $k$ un modèle ternaire, i.e, une équation de la forme $\alpha X^3Y + \beta Y^3Z + \gamma Z^3X = 0$, où $\alpha, \beta, \gamma$ sont des éléments de $k$ convenables. On va montrer ci-dessous comment expliciter un tel modèle.

Tout d'abord, on sait paramétrer les courbes elliptiques possédant un $\mu_7$ (cf. [Kraus 96]). à tout $s \in k$ associons la cubique $E(s)$ d'équation

$$y^2 + a_1(s)xy + a_3(s)y \;=\; x^3 + a_2(s)x^2 + a_4(s)x + a_6(s)\,,$$

où

$$\begin{aligned}
a_1(s) &= 1 + s - s^2,\\
a_2(s) = a_3(s) &\;=\; s^2 - s^3,\\
a_4(s) &= 5s(1-s)(s^2 - s + 1)(s^3 + 2s^2 - 5s + 1),\\
a_6(s) &= s(1-s)(s^9 + 9s^8 - 37s^7 + 70s^6 - 132s^5\\
&\qquad + 211s^4 - 182s^3 + 76s^2 - 18s + 1).
\end{aligned}$$

Les invariants standard associés à $E(s)$ sont:

$$\begin{aligned}
c_4(s) &= (s^2 - s + 1)(s^6 + 229s^5 + 270s^4\\
&\qquad - 1695s^3 + 1430s^2 - 235s + 1),\\
c_6(s) &= -s^{12} + 522s^{11} + 8955s^{10} - 37950s^9 + 70998s^8\\
&\qquad - 131562s^7 + 253239s^6 - 316290s^5\\
&\qquad + 218058s^4 - 80090s^3 + 14631s^2 - 510s - 1,\\
\Delta(s) &= s(s-1)D(s)^7, \text{ où } \; D(s) \;=\; s^3 - 8s^2 + 5s + 1.
\end{aligned}$$

Lorsque $\Delta(s) \neq 0$, $E(s)$ est une courbe elliptique sur $k$; d'après loc. cit., elle possède un $\mu_7$ et l'on obtient ainsi, à $k$-isomorphisme près, toutes les courbes elliptiques sur $k$ possédant un $\mu_7$. L'équation ternaire cherchée est alors la suivante (cf. aussi [Kraus 91]):

**Théorème 7.1.** *Avec les notations ci-dessus, soit $s \in k$ tel que $\Delta(s) \neq 0$. La courbe $X_{E(s)}(7)$ est $k$-isomorphe à la courbe d'équation*

$$X^3Y + Y^3Z + s(s-1)^2\,Z^3X \;=\; 0\,. \qquad (7\text{–}1)$$

*Preuve:* Posons $a(s) = -c_4(s)/48$ et $b(s) = -c_6(s)/864$. Notons $\mathcal{C}_s$ la quartique projective obtenue dans le théorème 2.1, lorsqu'on remplace $a, b$ par $a(s), b(s)$, respectivement. Soit d'autre part $\mathcal{C}'_s$ la quartique définie par l'équation (7–1). Considérons la matrice $H = (a_{ij}) \in \mathrm{GL}_3(k)$ donnée par

$$\begin{aligned}
a_{11} &= 6s^5 - 294s^4 + 306s^3 + 174s^2 - 222s + 30,\\
a_{12} &= 72(s-1),\\
a_{13} &= -s^9 - 110s^8 - 1065s^7 + 5054s^6 - 7798s^5 + 5894s^4\\
&\qquad - 3031s^3 + 1440s^2 - 381s - 2,\\
a_{21} &= 102s^5 - 714s^4 + 1422s^3 - 1074s^2 + 258s + 6,\\
a_{22} &= 72(1-s),\\
a_{23} &= 28s^9 + 32s^8 - 186s^7 - 2261s^6 + 8512s^5 - 11690s^4\\
&\qquad + 7546s^3 - 2100s^2 + 120s - 1,\\
a_{31} &= -30s^4 - 72s^3 + 414s^2 - 204s - 102,\\
a_{32} &= 72,\\
a_{33} &= 2s^8 - 399s^7 + 1680s^6 - 3787s^5 + 3640s^4 - 315s^3\\
&\qquad - 1078s^2 + 284s - 28.
\end{aligned}$$

On vérifie que l'homographie $f$ de $\mathbb{P}^2$ définie par $H$ applique $\mathcal{C}_s$ sur $\mathcal{C}'_s$, d'où le théorème. On notera au passage que, dans le modèle (7–1), le point-base de $Y_{E(s)}(7)$ est le point $[s-1, 1-s, 1]$, comme il résulte de la présente démonstration. □

### 7.1 Démonstration abrégée du théorème 5.2.

En passant par le cas générique, puis en spécialisant, on peut supposer d'une part que $j(E') \neq 0, 1728$, d'autre part que, une base de $E[7]$ sur $\mathbb{F}_7$ étant choisie, la représentation $\rho$ de $G_k$ dans $\mathrm{GL}_2(\mathbb{F}_7)$ associée à $E$ est surjective. Supposons $d \neq 0$, avec les notations du théorème. Il s'agit de montrer que $E'$ et $E''$ sont $k$-isomorphes. On sait déjà que $j(E'') = j(E')$. Il existe donc un $\delta \in k^*$ tel que $E''$ soit $k$-isomorphe à la tordue de $E'$ par le caractère associé à l'extension $k(\sqrt{\delta})/k$. Tout revient à montrer que $\delta$ est un carré dans $k$. Soit $k'$ le corps des invariants de l'image réciproque par $\rho$ du sous-groupe de $\mathrm{GL}_2(\mathbb{F}_7)$ formé des matrices diagonales du type $\begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix}$. Le corps $k'$ ne contient pas la seule extension quadratique de $k$ contenue dans $k(E[7])$, à savoir $k(\sqrt{-7})$. Ainsi

$\delta$ est un carré dans $k$ si et seulement si c'est un carré dans $k'$. En remplaçant $k$ par $k'$, on peut donc désormais supposer que $E$ possède un sous-$G_k$-module isomorphe à $(\mathbb{Z}/7\mathbb{Z})\times\mu_7$. Puisque $E$ possède un $\mu_7$, on peut supposer que $E = E(s)$, pour un $s \in k$ tel que $\Delta(s) \neq 0$. Du fait que $E$ possède un $(\mathbb{Z}/7\mathbb{Z}) \times \mu_7$, on déduit que $s(s-1)^2$ est une puissance septième dans $k$. Soit donc $\sigma \in k$ tel que $s(s-1)^2 = \sigma^7$.

Reprenons les notations de la preuve du théorème 7.1. Au point $M = [x, y, z] \in \mathcal{C}_s(k)$ correspond un point $[X, Y, Z] \in \mathcal{C}'_s(k)$, de sorte que

$$\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \;=\; H \begin{pmatrix} x \\ y \\ z \end{pmatrix} \tag{7–2}$$

Le point $N = [\sigma X, Y, \sigma^3 Z]$ appartient alors à $\mathcal{C}(k)$. Il résulte de plus des définitions qu'il existe un isomorphisme symplectique de $k$-schémas en groupes $u'$ de $A$ sur $E'[7]$ tel que le couple $(E', u')$ corresponde au point $N$, comme dans la section 3. Appliquons maintenant la formule (3–12). Notons $Q$ le premier membre de (7–1). À l'aide des formules (3–8) et (3–9), on voit que, dans un modèle de $E'$ sur $k$ convenable, on a:

$$\begin{aligned} c_4(E') &= C(Q)(X, Y, Z)(-XYZ)^2, \\ c_6(E') &= K(Q)(X, Y, Z)(-XYZ)^3. \end{aligned} \tag{7–3}$$

Notons $P$ le polynôme défini en (5–1), dans lequel on a remplacé $a$ par $a(s)$ et $b$ par $b(s)$. Modulo le changement de variables (7–2), on vérifie que l'on a:

$$Q(X, Y, Z) = 2^{10}\, 3^8\, (s-1)^3 D(s)^3\, P(x, y, z). \tag{7–4}$$

Par ailleurs

$$\det(H) \;=\; -2^7\, 3^6\, (s-1)^2 D(s)^4. \tag{7–5}$$

Posons maintenant

$$C = C(P)(x, y, z) \quad \text{et} \quad C' = C(Q)(X, Y, Z),$$

de même pour $K, K'$. En vertu des formules (3–8), (3–9), (7–4) et (7–5), il vient:

$$C' = 2^{38}3^{28}(s-1)^{12}C, \quad K' = -2^{57}3^{42}(s-1)^{18}K. \tag{7–6}$$

Compte tenu des formules (7–3) et (7–6), $E'$ a un modèle sur $k$ dans lequel on a:

$$c_4(E') = C(2XYZ)^2, \quad c_6(E') = K(2XYZ)^3. \tag{7–7}$$

Notons enfin $L$ (resp., $W$) le poylynôme en $X, Y, Z$ se déduisant du polynôme $z$ (resp., $V$) via le changement de variables (7–2). Pour conclure, vu les formules (7–7), il suffit de voir que la fonction $g = LW/(XYZ)$ sur $\mathcal{C}'_s$ est un carré dans le corps de fonctions $k(\mathcal{C}'_s)$. On constate que, si l'on pose

$$\begin{aligned} r \;&= \frac{(s+2)X^2Y + (3s-1)Y^2Z}{XYZ} + \frac{s(s-1)(2s-3)Z^2X}{XYZ} \\ &\quad + \frac{(s^2-s+1)XYZ}{XYZ}, \end{aligned} \tag{7–8}$$

on a l'égalité suivante:

$$r^2 \;=\; 2^8\, 3^6\, (s-1)^2\, D(s)^4\, g\,.$$

Le théorème 5.2 est ainsi démontré.

## 8. COMPLÉMENTS

Considérons une courbe elliptique $E$ sur $\mathbb{Q}$, et notons $\rho$ la représentation de Galois dans $E[7]$. Une question naturelle se pose: peut-on déterminer effectivement tous les points rationnels de $X_E(7)$? Comme nous l'avons signalé, il semble que le fait de connaître une équation de $X_E(7)$ ne soit pas ici d'un grand secours. Nous donnons dans ce paragraphe deux exemples de courbes $E$ pour lesquelles on peut répondre à la question ci-dessus.

Notons simplement $J_E$ la jacobienne de $X_E(7)$ sur $\mathbb{Q}$. Si par hasard $J_E$ a un quotient elliptique de rang 0 sur $\mathbb{Q}$, on peut évidemment déterminer $X_E(7)(\mathbb{Q})$ effectivement. Malheureusement, on va voir que ce cas ne se présente pas souvent. On a tout d'abord le résultat suivant:

**Théorème 8.1.** *Soit $E$ une courbe elliptique sur $\mathbb{Q}$. Pour que $J_E$ possède un quotient elliptique sur $\mathbb{Q}$, il faut et il suffit que l'image de $\rho$ soit contenue dans le normalisateur d'un sous-groupe de Cartan de* $\mathrm{GL}(E[7])$.

Nous ne pouvons ici qu'esquisser la démonstration, les détails seront publiés ultérieurement. Puisque $X_E(7)$ est une tordue galoisienne de $X(7)$, $J_E$ est une tordue de la jacobienne de $X(7)$, i.e., de la jacobienne $J(\mathcal{C})$ de la quartique de Klein. La structure de $J(\mathcal{C})$ est connue depuis longtemps, au moins sur $\mathbb{C}$. Plus précisément, soit $A$ la courbe elliptique définie par l'équation

$$y^2 + xy \;=\; x^3 - x^2 - 2x - 1\,.$$

C'est la courbe 49A1 des tables de [Cremona 97]. On sait aussi que $A$ est un modèle de $X_0(49)$ sur $\mathbb{Q}$ (cf. [Ligozat 75]). Alors $J(\mathcal{C})$ est isogène sur $\mathbb{C}$ (et déjà sur $\mathbb{Q}(\mu_7)$) à $A^3$. La structure de $J(\mathcal{C})$ sur $\mathbb{Q}$ a été étudiée dans [Coleman 89] et [Prapavessi 94], mais, pour prouver le

théorème 8.1, il est nécessaire d'approfondir les résultats des articles cités. En tous cas, $J(\mathcal{C})$ est isogène sur $\mathbb{Q}$ au produit de $A$ par une variété abélienne simple de dimension 2. Si $J_E$ a un quotient elliptique $B$ (sur $\mathbb{Q}$), il est clair que $B$ est une tordue de $A$: $B$ est $\mathbb{Q}$-isomorphe à la tordue $A_d$ de $A$ par le caractère associé à une extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, où $d$ est un entier non nul libre de carrés. Une étude détaillée des différents 1-cocycles du groupe de Galois de $\overline{\mathbb{Q}}/\mathbb{Q}$ intervenant ici permet de montrer que l'ordre de l'image de $\rho$ n'est alors pas multiple de 7. On en déduit aussitôt la nécessité de la condition de l'énoncé. La suffisance est plus facile.

Supposons maintenant que l'image de $\rho$ soit contenue dans le normalisateur $N$ d'un sous-groupe de Cartan $C$ de $\mathrm{GL}(E[7])$. D'après le théorème 8.1, il existe un entier $d$, comme ci-dessus, tel que $A_d$ soit un quotient de $J_E$. Il existe donc un morphisme (défini sur $\mathbb{Q}$) non constant de $X_E(7)$ sur $A_d$. Si l'image par ce morphisme du point-base de $Y_E(7)$ est d'ordre infini, la méthode envisagée ne permettra pas de conclure. En fait c'est presque toujours le cas, comme le montrent les deux propositions ci-après, que nous ne pouvons que signaler ici sans démonstration.

**Proposition 8.2.** *Il n'y a qu'un nombre fini (à $\overline{\mathbb{Q}}$-isomorphisme près) de courbes elliptiques $E/\mathbb{Q}$ ayant la propriété suivante: il existe un morphisme non constant, défini sur $\mathbb{Q}$, de $X_E(7)$ sur une courbe elliptique, tel que l'image par ce morphisme du point-base de $Y_E(7)$ soit d'ordre fini.*

**Proposition 8.3.** *Considérons les courbes elliptiques $E/\mathbb{Q}$ ayant la propriété indiquée dans la proposition 8.2. Restreignons-nous au cas déployé, i.e. au cas où, avec les notations ci-dessus, $C$ est un sous-groupe de Cartan déployé de $\mathrm{GL}(E[7])$. Il n'y a en fait, à un $\overline{\mathbb{Q}}$-isomorphisme près, qu'une seule telle courbe elliptique, à savoir la courbe elliptique $E$ de conducteur 2450 définie par l'équation suivante:*

$$y^2 + xy \;=\; x^3 - x^2 - 107x - 379\,.$$

*De plus, $X_E(7)$ possède alors un seul point rationnel sur $\mathbb{Q}$: le point-base de $Y_E(7)$.*

Voici un autre exemple, de nature totalement différente.

**Proposition 8.4.** *Soit $E$ la courbe 26B2 des tables de [Cremona 97], d'équation*

$$y^2 + xy + y \;=\; x^3 - x^2 - 213x - 1257\,.$$

*Cette courbe possède un $\mu_7$, elle est en fait isomorphe à la courbe elliptique $E(2)$, avec les notations de la section 7. La courbe $X_E(7)$ possède exactement quatre points rationnels sur $\mathbb{Q}$, à savoir le point-base et trois pointes (cf. la section 7).*

*Preuve:* Compte tenu du théorème 7.1, il s'agit de démontrer que les seules solutions $(X, Y)$ sur $\mathbb{Q}$ de l'équation

$$X^3Y + Y^3 + 2X \;=\; 0$$

sont $(0, 0)$ et $(1, -1)$. Via la transformation birationnelle définie par les formules

$$x = -X^3/Y^2, \quad y = X/Y; \quad X = -x/y^2, \quad Y = -x/y^3,$$

il revient au même de montrer que les seules solutions $(x, y)$ sur $\mathbb{Q}$ de l'équation

$$2y^7 \;=\; x^2(x-1) \tag{8–1}$$

sont $(0, 0), (1, 0)$ et $(-1, -1)$. La résolution de l'équation (8–1) sur $\mathbb{Q}$ se ramène facilement à celle des équations suivantes:

$$a^7 + b^7 \;=\; 2^k c^7 \quad (k = 1, 2, 4)\,.$$

L'étude de ces équations (cf. [Dénes 52]) permet d'achever la preuve de la proposition. □

## Bibliographie


[Batut et al. 97] C. Batut, K. Belabas, D. Bernardi, H. Cohen, et M. Olivier. "User's Guide to PARI-GP (Version 2.0). Bordeaux: Lab A2X, Université de Bordeaux I, 1997.

[Caporaso et al 95] L. Caporaso, J. Harris, and B. Mazur. "Uniformity of Rational Points." *J. Amer. Math. Soc.* 10 (1995), 1–35.

[Coleman 89] R. Coleman. "Torsion Points on Abelian Etale Coverings of $\mathbb{P}^1$ - $\{0, 1, \infty\}$." *Trans. Amer. Math. Soc.* 311 (1989), 185–208.

[Cremona 97] J. E. Cremona. *Algorithms for Modular Elliptic Curves*, Second edition. Cambridge, UK: Cambridge University Press, 1997.

[Deligne et Rapoport 73] P. Deligne et M. Rapoport. "Les schémas de modules de courbes elliptiques," pp. 14-316 dans *Modular functions of one variable*, II (Antwerp, 1972), édité par P. Deligne et W. Kuyk, pp. 14–316, Lecture Notes in Math. 349, Berlin: Springer, 1973.

[Dénes 52] P. Dénes. "Über die Diophantische Gleichung $x^\ell + y^\ell = cz^\ell$." *Acta Math.* 88 (1952), 241–251.

[Elkies 99] N. Elkies. "The Klein Quartic in Number Theory." In *The Eightfold Way*, edited by S. Lévy, pp. 51–102. Cambridge, UK: Cambridge University Press, 1999.

[Halberstadt and Kraus 99] E. Halberstadt and A. Kraus. "On the Modular Curves $Y_E(7)$." *Math. of Computation* 69:231 (1999), 1193–1206.

[Klein 1878] F. Klein. "Über die transformation siebenter Ordnung der elliptischen Funktionen." *Math. Annalen* 14 (1878), 428–471.

[Kraus 90] A. Kraus. "Sur les modules galoisiens des courbes elliptiques." *Sém. de théorie des nombres de Caen*, Caen, France: Université de Caen, 1990.

[Kraus 91] A. Kraus. "Sur des courbes de genre 3 associées aux courbes elliptiques." *Journées arithmétiques de Caen*, Caen, France: Université de Caen, 1991.

[Kraus 96] A. Kraus. "Sur les modules des points de 7-torsion d'une famille de courbes elliptiques." *Ann. Inst. Fourier* 46 (1996), 899–907.

[Kraus et Oesterlé 92] A. Kraus et J. Oesterlé. "Sur une question de B. Mazur." *Math. Ann.* 293 (1992), 259–275.

[Lang 87] S. Lang. *Elliptic Functions*, Second edition, Graduate Texts in Math. 112. New York: Springer, 1987.

[Ligozat 75] G. Ligozat. "Courbes modulaires de genre 1." *Bull. Soc. Math. France, Supplément*, mémoire 43 (1975), 1–80.

[Ligozat 77] G. Ligozat, "Courbes modulaires de niveau 11." In *Modular Functions of One Variable V*, edited by J. P. Serre et D. B. Zagier, pp. 149–237, Lecture Notes in Math. 601. Berlin: Springer, 1977.

[Mazur 78] B. Mazur. "Rational Isogenies of Prime Degree." *Invent. Math.* 44:2 (1978), 129–162.

[Prapavessi 94] D. T. Prapavessi. "On the Jacobian of the Klein Curve." *Proc. of the Amer. Math. Soc.* 122:4 (1994), 971–978.

[Silverman 86] J. H. Silverman. *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. 106. New York: Springer, 1986.

[Silverman 94] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Math. 151. New York: Springer, 1994.

[Vélu 71] J. Vélu. "Isogénies entre courbes elliptiques." *C.R. Acad. Sci. Paris, Sér. A* 273 (1971), 238–241.

Emmanuel Halberstadt, Université de Paris VI, Institut de Mathématiques, UMR 7586 du CNRS, Équipe de Théorie des Nombres, 175 Rue du Chevaleret Paris, 75013 France (halberst@math.jussieu.fr)

Alain Kraus, Université de Paris VI, Institut de Mathématiques, UMR 7586 du CNRS, Équipe de Théorie des Nombres, 175 Rue du Chevaleret Paris, 75013 France (kraus@math.jussieu.fr)

Received December 21, 2001; accepted in revised form April 18, 2003.