Invariants des quotients de la Jacobienne d'une courbe de genre 2

P. Gaudry et É. Schost

7 avril 2000

Introduction

Parmi les courbes de genre 2, celles dont la Jacobienne est décomposable présentent un intérêt particulier. Par exemple, les records actuels de rang ou de torsion sont obtenus pour des courbes de ce type [2]. C'est aussi dans ce cadre que la méthode de Dem'janenko-Manin permet de déterminer tous les points rationnels d'une courbe [6].

Le but du présent article est de rendre explicite le théorème suivant :

Théorème 1 *Soit $\mathcal{C}$ une courbe de genre 2 admettant une involution non triviale. Alors il existe au plus deux courbes elliptiques quotients de degré 2 de sa Jacobienne à isomorphisme près.*

Dans ce cas, nous donnons des formules algébriques reliant les modules de $\mathcal{C}$ au j-invariant des courbes elliptiques dont la Jacobienne de $\mathcal{C}$ est le produit.

Les modules des courbes de genre 2 forment une variété de dimension 3 qui a été décrite pour la première fois par Igusa dans [3]. La construction repose sur des covariants notés A, B, C, D de la forme sextique associée pour lesquels nous adoptons la définition de [3], et les modules s'obtiennent en prenant des quotients de ces covariants.

Nous supposerons que A est non nul, et prendrons les coordonnées locales proposées dans [4] :

$$\begin{aligned} j_1 &= 144\frac{B}{A^2}, \\ j_2 &= -1728\frac{AB-3C}{A^3}, \\ j_3 &= 486\frac{D}{A^5}. \end{aligned}$$

Le cas $A = 0$ sera traité en annexe.

Le corps de base est supposé de caractéristique différente de 2, 3 et 5.

Remerciements

Les calculs nécessaires pour obtenir les formules de cet article ont été faits sur les machines de l'UMS Medicis n° 658 (CNRS – École polytechnique). Nous remercions aussi François Morain pour ses encouragements durant ces travaux.

Préliminaires

Définition 1 *La Jacobienne d'une courbe $\mathcal{C}$ de genre 2 est dite (2,2)-décomposable s'il existe une (2,2)-isogénie entre $Jac(\mathcal{C})$ et un produit de courbes elliptiques $\mathcal{E}_1 \times \mathcal{E}_2$. On dit alors que $\mathcal{E}_1$ est un quotient de degré 2 de $Jac(\mathcal{C})$.*

Le lemme suivant est en substance dans [3].

Lemme 1 *Soit $\mathcal{C}$ une courbe de genre 2. Il existe une surjection de l'ensemble des involutions non hyperelliptiques de $\mathcal{C}$ sur les classes d'isomorphismes des courbes elliptiques quotients de degré 2 de la Jacobienne de $\mathcal{C}$. En particulier, la Jacobienne de $\mathcal{C}$ est (2,2)-décomposable si et seulement si $\mathcal{C}$ admet une involution autre que l'involution hyperelliptique.*

Démonstration Soit τ une involution de $\mathcal{C}$ non hyperelliptique. La courbe $\mathcal{C}$ quotientée par τ est une courbe $\mathcal{E}$ de genre 1 [3]. Alors $\mathcal{E}$ est un quotient de la Jacobienne de $\mathcal{C}$, et on construit ainsi une application qui à chaque involution non triviale de $\mathcal{C}$ associe une classe d'isomorphisme de courbes elliptiques.

Cette application est surjective. En effet, soit $\mathcal{E}$ une courbe de genre 1 quotient de degré 2 de $\mathrm{Jac}(\mathcal{C})$. Il existe alors un morphisme φ de degré 2 de $\mathcal{C}$ sur $\mathcal{E}$. Pour p un point générique de $\mathcal{C}$, la fibre $\varphi^{-1}(\varphi(p))$ est de la forme $\{p, q(p)\}$, où q est une fraction rationnelle de p. On définit alors l'involution τ, qui à p associe $q(p)$. La courbe $\mathcal{E}$ est de genre 1, donc τ n'est pas l'involution hyperelliptique. Cette construction est l'inverse de la précédente. Le morphisme φ n'est pas unique, aussi l'application que l'on construit n'est-elle pas injective. $\square$

Bolza [1], puis Igusa [3] et Lange [7] ont classifié les courbes admettant des automorphismes, en particulier les involutions. Les modules des courbes de genre 2 admettant une involution non triviale forment une sous-variété de dimension 2 de la variété des modules ; à la suite de Lange, nous la noterons $\mathcal{M}_2$. Dans nos coordonnées locales, une équation de cette hypersurface est donnée par la formule ci-dessous, la construction explicite est donnée dans [9].

$$\begin{aligned}
&8393900389396594682757 12 j_3^2 + 92114133216972232458240000 0 j_3^3 + 32983576347223130112000 j_1^2 j_3^2 \\
&+ 182200942574622720 j_3 j_1 j_2^2 - 374813367582081024 j_3 j_1^2 j_2 + 9995023135522160640000 j_3^2 j_1 j_2 \\
&+ 94143178827 j_2^4 - 562220051373121536 j_3 j_2^2 - 562220051373121536 j_3 j_1^3 + 43381176803481600 j_3 j_2^3 \\
&- 719641665757595566080 00 j_3^2 j_2 - 3886064995091016056832 00 j_3^2 j_1 - 1156831381426176 j_1^5 j_3 \\
&- 31381059609 j_1^7 + 62762119218 j_1^4 j_2^2 + 13947137604 j_1^3 j_2^3 - 31381059609 j_1 j_2^4 - 188286357654 j_1^3 j_2^2 \\
&- 6973568802 j_1^6 j_2 + 192612425007458304 j_1^4 j_3 + 94143178827 j_1^6 - 6973568802 j_2^5 \\
&+ 28920784535654400 j_1^2 j_3 j_2^2 + 164848471853230080 j_1^3 j_3 j_2 = 0.
\end{aligned}$$

Une courbe $\mathcal{C}$ de genre 2 admet toujours l'involution hyperelliptique ι, qui commute avec tous ses autres automorphismes. On appellera *groupe réduit d'automorphismes de $\mathcal{C}$* le quotient de son groupe d'automorphismes par $\{1, \iota\}$. On peut alors classifier les points de $\mathcal{M}_2$ par leur groupe réduit d'automorphismes $\mathcal{G}$. On a les 5 possibilités suivantes :

- Le groupe $\mathcal{G}$ est le groupe dihédral D_6, ce qui correspond au point de $\mathcal{M}_2$ associé à la courbe $y^2 = x^6 + 1$.
- Le groupe $\mathcal{G}$ est le groupe symétrique $\mathfrak{S}_4$, ce qui correspond à la courbe $y^2 = x^5 - x$.
- Le groupe $\mathcal{G}$ est le groupe dihédral D_3. Les points correspondants forment une courbe $\mathcal{D}$ de $\mathcal{M}_2$ privée des 2 points précédents.
- Le groupe $\mathcal{G}$ est le groupe de Klein V_4. Les points forment une courbe $\mathcal{V}$ de $\mathcal{M}_2$ privée des 2 points précédents ; ces points sont les seules intersections de $\mathcal{D}$ et $\mathcal{V}$.
- Le groupe $\mathcal{G}$ est $\mathbb{Z}/2\mathbb{Z}$, ce qui correspond à l'ouvert dense $\mathcal{U}$ formé de $\mathcal{M}_2$ privé des courbes précédentes. On appellera ce cas le cas générique.

Dans le dernier cas le théorème 1 est immédiat et il ne nous reste qu'à expliciter les j-invariants des quotients de degré 2 de $\mathcal{C}$.

1 Le cas générique

1.1 Le polynôme minimal à partir d'une forme de Rosenhain

Notre but est d'obtenir explicitement un polynôme de degré 2 donnant les j-invariants en fonction des modules (j_1, j_2, j_3). Le premier pas consiste à obtenir les j-invariants à partir d'une forme de Rosenhain. Nous prenons comme point de départ [3] où l'on trouve la forme de Rosenhain d'une courbe (2,2)-décomposable.

Théorème 2 *Soit $\mathcal{C}$ une courbe de genre 2 (2,2)-décomposable. Alors, sur une clôture algébrique de son corps de définition, $\mathcal{C}$ est isomorphe à une courbe d'équation*

$$y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu), \text{ où } \mu = \nu\frac{1-\lambda}{1-\nu},$$

avec λ, ν, μ deux à deux distincts et différents de 0 et 1. La Jacobienne de $\mathcal{C}$ est alors isogène au produit des courbes elliptiques dont les formes de Legendre sont $y^2 = x(x-1)(x-\Lambda)$, avec Λ racine de l'équation

$$\nu^2\lambda^2\Lambda^2 + 2\nu\mu(-2\nu+\lambda)\Lambda + \mu^2 = 0. \tag{1}$$

Démonstration La courbe $\mathcal{C}$ a 6 points de Weierstraß, et un isomorphisme de $\mathcal{C}$ vers une autre courbe sera entièrement déterminé par les images de 3 de ces points. Notons τ une involution non triviale sur $\mathcal{C}$. Soient P_1, P_2, P_3 des points de Weierstraß de $\mathcal{C}$ représentant chaque orbite sous l'action de τ. La courbe $\mathcal{C}'$ obtenue en envoyant P_1, P_2, P_3 sur respectivement 0, 1, ∞ a une équation de la forme

$$y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu).$$

La courbe n'est pas singulière, donc λ, ν, μ sont deux à deux distincts et différents de 0 et 1. On note encore τ l'image par l'isomorphisme de l'involution. Celle-ci permute les nouveaux points de Weierstraß, et quitte à échanger les noms de λ, μ, ν, on a $\tau(0) = \lambda$, $\tau(1) = \mu$ et $\tau(\infty) = \nu$. D'autre part τ est de la forme

$$\tau(x,y) = \left(\frac{ax+b}{cx+d}, \frac{wy}{(cx+d)^3}\right),$$

et le fait que c'est une involution impose $a = -d$ et $w = \pm(ad-bc)^{3/2}$. L'involution τ peut ainsi être déterminée à l'aide des deux images $\tau(0) = \lambda$ et $\tau(\infty) = \nu$. On obtient alors

$$\tau(x,y) = \left(\nu\frac{x-\lambda}{x-\nu}, \frac{u^3y}{(x-\nu)^3}\right),$$

où

$$u = \pm\sqrt{\nu(\nu-\lambda)}.$$

La relation $\tau(1) = \mu$ fournit alors la première assertion

$$\mu = \nu\frac{1-\lambda}{1-\nu}.$$

L'étape suivante est de trouver une courbe isomorphe à $\mathcal{C}'$ pour laquelle l'involution sera $(x,y) \mapsto (-x,y)$. Pour cela on cherche de nouveau les coefficients d'une transformation du type $\varphi : x \mapsto (ax+b)/(cx+d)$ telle que $\varphi(0) = -\varphi(\lambda)$, $\varphi(1) = -\varphi(\mu)$, $\varphi(\infty) = -\varphi(\nu)$. On vérifie que la transformation

$$\varphi(x) = \frac{x-\nu-u}{x-\nu+u},$$

convient ainsi que tous ses multiples. La courbe $\mathcal{C}$ est donc isomorphe à la courbe $\mathcal{C}''$ d'équation $y^2 = (x^2-x_1^2)(x^2-x_2^2)(x^2-x_3^2)$, où

$$x_1 = \varphi(\infty) = 1, \quad x_2 = \varphi(0) = \frac{\nu-u}{\nu+u}, \quad x_3 = \varphi(1) = \frac{1-(\nu-u)}{1-(\nu+u)}.$$

Par la suite, le morphisme $(x,y) \mapsto (x^2,y)$ envoie $\mathcal{C}''$ sur la courbe elliptique $\mathcal{E}$ d'équation

$$y^2 = (x-1)(x-x_2^2)(x-x_3^2),$$

dont une forme de Legendre est donnée par $y^2 = x(x-1)(x-\Lambda)$ avec

$$\Lambda = \frac{x_2^2-x_3^2}{1-x_3^2} = \frac{\mu}{\left(\nu \pm \sqrt{\nu(\nu-\lambda)}\right)^2}.$$

On obtient ainsi le résultat. Remarquons qu'aucun dénominateur ne peut s'annuler et que la courbe $\mathcal{E}$ est bien non singulière, d'après les conditions sur λ, μ, ν. $\square$

Corollaire 1 *Soient $\mathcal{C}$ une courbe dont les modules appartiennent à $\mathcal{U}$, et λ, μ, ν définis comme dans le théorème précédent. Alors les j-invariants des courbes elliptiques quotients de la Jacobienne de $\mathcal{C}$ sont les solutions d'une équation*

$$j^2 + c_1(\lambda, \nu)j + c_0(\lambda, \nu) = 0, \tag{2}$$

où c_0 et c_1 sont des fractions rationnelles en deux variables.

Démonstration Le j-invariant d'une courbe elliptique est relié à une forme de Legendre par la relation

$$\Lambda^2(\Lambda - 1)^2 j - 2^8(\Lambda^2 - \Lambda + 1)^3 = 0. \tag{3}$$

Le théorème précédent donne deux courbes elliptiques quotients de la Jacobienne de $\mathcal{C}$, et sur $\mathcal{U}$ ce sont les seules. Le polynôme attendu s'obtient ainsi par le calcul du résultant entre les équations 3 et 1 et en tenant compte de la relation $\mu = \nu\frac{1-\lambda}{1-\nu}$. $\square$

On n'écrira pas ici les valeurs de $c_0(\lambda, \nu)$ et $c_1(\lambda, \nu)$. On connaît l'expression des modules en fonction de λ et ν, on pourrait donc obtenir les coefficients c_0 et c_1 en fonction des modules de $\mathcal{C}$ par un calcul d'élimination. L'approche suivante est moins directe, mais produit des formules plus concises.

1.2 Le groupe agissant sur les formes de Rosenhain

Nous introduisons dans cette partie deux invariants caractéristiques des classes d'isomorphismes de courbes (2,2)-décomposables. Ces grandeurs sont invariantes pour l'action du groupe décrit ci-dessous :

Théorème 3 *Soit $\mathcal{C}$ une courbe dont les modules appartiennent à $\mathcal{M}_2$. Alors il existe 24 triplets $(\lambda, \mu = \nu\frac{1-\lambda}{1-\nu}, \nu)$ pour lesquels la courbe d'équation $y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$ est isomorphe à $\mathcal{C}$. L'ensemble de ces triplets est muni de l'action transitive d'un groupe isomorphe à l'unique sous-groupe d'ordre 24 de $PGL(2,5)$.*

Démonstration Le théorème 2 fournit un triplet $(\lambda_1, \mu_1, \nu_1)$ satisfaisant les conditions requises. On peut donc supposer que $\mathcal{C}$ est la courbe correspondant à ce triplet. Toute courbe isomorphe à $\mathcal{C}$ est obtenue par une transformation birationnelle

$$x \mapsto \frac{ax+b}{cx+d}.$$

On exige de plus que la courbe soit mise sous forme de Rosenhain, donc la transformation doit envoyer 3 des 6 points de Weierstraß de $\mathcal{C}$ $(0, 1, \infty, \lambda_1, \mu_1, \nu_1)$ sur les points $(0, 1, \infty)$. L'ensemble des transformations homographiques correspondantes forment un groupe d'ordre 120 et le test exhaustif montre que seules 24 des formes obtenues vérifient la condition supplémentaire liant les nouveaux λ, μ et ν.

Notons $(\lambda_i, \mu_i, \nu_i)_{i=1,\dots,24}$ les triplets solutions. On passe de la forme de Rosenhain donnée par $\{0, 1, \infty, \lambda_i, \mu_i, \nu_i\}$ à une forme donnée par $\{0, 1, \infty, \lambda_j, \mu_j, \nu_j\}$ par applications successives aux 6 éléments des transformations $\sigma_1(x) = 1/x$, $\sigma_2(x) = 1 - x$, $\sigma_3(x) = \frac{x-\lambda_i}{1-\lambda_i}$, $\sigma_4(x) = x/\mu_i$. Ces éléments engendrent un groupe isomorphe à l'unique sous-groupe d'ordre 24 de $PGL(2,5)$, qui agit sur les triplets (λ, μ, ν) selon le tableau suivant :

Transformation	σ_1	σ_2	σ_3	σ_4
λ_i	$\frac{1}{\nu_i}$	$1-\mu_i$	$\frac{\lambda_i}{\lambda_i-1}$	$\frac{\lambda_i}{\mu_i}$
μ_i	$\frac{1}{\mu_i}$	$1-\lambda_i$	$\frac{\mu_i-\lambda_i}{1-\lambda_i}$	$\frac{1}{\mu_i}$
ν_i	$\frac{1}{\lambda_i}$	$1-\nu_i$	$\frac{\nu_i-\lambda_i}{1-\lambda_i}$	$\frac{\nu_i}{\mu_i}$

$\square$

Les fonctions symétriques en les 24 triplets $(\lambda_i, \mu_i, \nu_i)$ sont des invariants de la classe d'isomorphisme de $\mathcal{C}$; il est donc naturel d'y chercher 2 invariants caractérisant ces classes.

Définition 2 *Soient $\mathcal{C}$ une courbe dont les modules appartiennent à $\mathcal{M}_2$, et les triplets λ_i, μ_i, ν_i définis comme précédemment. On appelle Ω et Υ les deux grandeurs suivantes :*

$$\begin{array}{rcl} \Omega & = & \sum_{i=1}^{24} \nu_i^2 \\ \Upsilon & = & \sum_{i=1}^{24} \lambda_i \nu_i, \end{array}$$

Ces grandeurs ne dépendent que de la classe d'isomorphisme de $\mathcal{C}$.

Nous allons relier les modules (j_1, j_2, j_3) à ces nouveaux invariants d'un côté, puis écrire le polynôme minimal des j-invariants en fonction de ces invariants. La proposition suivante prouve que Ω et Υ caractérisent les classes d'isomorphisme de ces courbes.

Proposition 1 *Soient $\mathcal{C}$ une courbe dont les modules sont dans $\mathcal{M}_2$, et Ω et Υ. Sous réserve qu'elles soient définies, on a alors les égalités suivantes :*

$$\begin{array}{rcl} j_1 & = & \dfrac{36(\Omega-2)\Upsilon^2}{(\Omega-8)(2\Upsilon-3\Omega)^2}, \\ j_2 & = & -\dfrac{216\Upsilon^2(\Omega\Upsilon+\Upsilon-27\Omega)}{(\Omega-8)(2\Upsilon-3\Omega)^3}, \\ j_3 & = & -\dfrac{243\Omega\Upsilon^4}{64(\Omega-8)^2(2\Upsilon-3\Omega)^5}. \end{array}$$

Le système surdéterminé précédent n'est consistant que pour (j_1, j_2, j_3) sur $\mathcal{M}_2$. Dans ce cas, Ω et Υ sont donnés par la proposition suivante :

Proposition 2 *Soient $\mathcal{C}$ une courbe dont les modules appartiennent à $\mathcal{M}_2$. Alors les invariants Ω et Υ sont donnés en fonction des modules (j_1, j_2, j_3) par les formules suivantes, lorsqu'elles ont un sens :*

$$\begin{array}{rcl} \Omega & = & (349360128 j_1 j_3 - 29859840 j_3 j_2 + 1911029760000 j_3^2 + 972 j_1^2 j_2 - 110730240 j_1^2 j_3 - 45 j_1 j_2^2 \\ & & -12441600 j_1 j_3 j_2 + 6 j_2^3 + 45 j_1^4 - 330 j_1^3 j_2 - 56 j_1^2 j_2^2 - 16 j_1^5) \,/ \\ & & (-26873856 j_1 j_3 - 14929920 j_3 j_2 + 955514880000 j_3^2 + 3732480 j_1^2 j_3 - 9 j_1 j_2^2 + 4147200 j_1 j_3 j_2 \\ & & +3 j_2^3 + 9 j_1^4 - 3 j_1^3 j_2 + 2 j_1^2 j_2^2 - 2 j_1^5), \\ \\ \Upsilon & = & 3/4(162 j_1^4 - 483729408 j_1 j_3 + 17199267840000 j_3^2 + 67184640 j_1^2 j_3 - 36 j_1^5 - 134369280 j_3 j_2 \\ & & +162 j_1 j_2^2 + 45 j_2^3 + 35251200 j_1 j_3 j_2 - 45 j_1^3 j_2 - 72 j_1^2 j_2^2 - 6912000 j_3 j_2^2 - 20 j_1 j_2^3 - 4 j_1^4 j_2) \\ & & (349360128 j_1 j_3 - 29859840 j_3 j_2 + 1911029760000 j_3^2 + 972 j_1^2 j_2 - 110730240 j_1^2 j_3 - 45 j_1 j_2^2 \\ & & -12441600 j_1 j_3 j_2 + 6 j_2^3 + 45 j_1^4 - 330 j_1^3 j_2 - 56 j_1^2 j_2^2 - 16 j_1^5) \,/ \\ & & \big((27 j_1^4 + 161243136 j_1 j_3 + 1433272320000 j_3^2 - 53498880 j_1^2 j_3 - 9 j_1^5 + 44789760 j_3 j_2 + 486 j_1^2 j_2 \\ & & +135 j_1 j_2^2 - 23846400 j_1 j_3 j_2 - 162 j_1^3 j_2 - 81 j_1^2 j_2^2 - 3456000 j_3 j_2^2 - 10 j_1 j_2^3 - 2 j_1^4 j_2) \\ & & (-26873856 j_1 j_3 - 14929920 j_3 j_2 + 955514880000 j_3^2 + 3732480 j_1^2 j_3 - 9 j_1 j_2^2 + 4147200 j_1 j_3 j_2 \\ & & +3 j_2^3 + 9 j_1^4 - 3 j_1^3 j_2 + 2 j_1^2 j_2^2 - 2 j_1^5)\big). \end{array}$$

Démonstration Les formules se vérifient en exprimant j_1, j_2, j_3 ainsi que Ω et Υ en fonction de λ et ν. $\square$

Remarque Les invariants Ω et Υ sont des fractions rationnelles définies sur la variété $\mathcal{M}_2$. Les formules que nous donnons ne sont pas forcément les plus simples.

Proposition 3 *Soit $\mathcal{C}$ une courbe dont les modules sont dans $\mathcal{U}$. Les j-invariants des courbes elliptiques quotients de la Jacobienne de $\mathcal{C}$ sont les racines de $j^2 + c_1 j + c_0$, où c_0 et c_1 sont donnés par les formules suivantes, lorsqu'elles ont un sens :*

$$\begin{array}{rcl} c_0 & = & \dfrac{4096\Upsilon^2(\Omega-32)^3}{\Omega^2(\Omega-8)}, \\ \\ c_1 & = & -\dfrac{128\Upsilon(\Omega^2-4\Omega\Upsilon+56\Omega-512)}{\Omega(\Omega-8)}. \end{array}$$

Démonstration Les coefficients c_0 et c_1 sont déterminés en fonction de λ et ν dans le corollaire 1. De même, Ω et Υ sont définis à partir de λ et ν. On vérifie alors l'égalité des deux membres. □

Les deux dernières propositions permettent de réécrire le polynôme minimal 2 sous la forme

$$j^2 + c_1(j_1, j_2, j_3)j + c_0(j_1, j_2, j_3) = 0,$$

où $c_1(j_1, j_2, j_3)$ et $c_0(j_1, j_2, j_3)$ sont des fractions rationnelles à trois indéterminées que l'on se garde bien de développer.

Remarque Les cas d'annulation des dénominateurs sont traités en annexe.

2 Étude de la courbe $\mathcal{D}$

Nous rappelons sans démonstration ce résultat dû à Igusa [3].

Théorème 4 *Soit $\mathcal{C}$ une courbe de genre 2. Le groupe réduit d'automorphismes de $\mathcal{C}$ est D_3 si et seulement si $\mathcal{C}$ est isomorphe à une courbe d'équation*

$$y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu), \text{ où } \mu = \frac{1}{1-\lambda}, \text{ et } \nu = 1 - \frac{1}{\lambda}, \tag{4}$$

avec λ différent de 0, de 1 et de $(1 \pm \sqrt{3})/2$.

En termes d'invariants d'Igusa, $\mathcal{C}$ est (2,2)-décomposable de groupe réduit d'automorphismes D_3 si et seulement si ses modules appartiennent à la courbe $\mathcal{D}$ d'équations :

$$\begin{aligned}
j_1 j_2^2 - 297 j_1 j_2 - 90 j_2^2 - 725760 j_1 j_3 + 172800 j_2 j_3 & \\
-2187 j_1 - 243 j_2 + 169641216 j_3 &= 0,\\
7 j_2^3 - 57600 j_3 j_1 j_2 + 8991 j_1 j_2 + 2646 j_2^2 - 34774272 j_3 j_1 - 22394880 j_3 j_2 & \\
-9953280000 j_3^2 + 65610 j_1 + 7290 j_2 - 4901119488 j_3 &= 0,\\
-81 j_1 + 21 j_1^2 - 9 j_2 + 5 j_1 j_2 + 864000 j_3 &= 0.
\end{aligned}$$

Ce résultat s'obtient par un calcul d'élimination, puisque 4 peremt d'exprimer les modules de $\mathcal{C}$ en fonction de λ. Le résultat suivant montre le théorème 1 dans le cas où les modules sont sur $\mathcal{D}$.

Théorème 5 *Soit $\mathcal{C}$ une courbe dont les modules sont sur $\mathcal{D}$. Alors les j-invariants des courbes elliptiques quotients de la Jacobienne de $\mathcal{C}$ sont les racines de $j^2 + c_1 j + c_0$, où c_0 et c_1 sont donnés par les formules suivantes :*

$$\begin{aligned}
c_1 &= \frac{3}{8}\,\frac{-85221 j_1 j_2 - 69228 j_1^2 - 6621 j_2^2 + 6054374400 j_3 j_1 + 692576000 j_3 j_2 - 5952061440 j_3}{j_3(4705 j_2 + 21492 j_1 - 129816)},\\
c_0 &= -81\,\frac{2373 j_1^2 + 1412 j_1 j_2 + 210 j_2^2 + 33696000 j_3 j_1 + 4320000 j_3 j_2 - 246067200 j_3}{j_3(5 j_2 + 27 j_1 - 108)}.
\end{aligned}$$

Démonstration Quand la courbe $\mathcal{C}$ est sous la forme 4, les automorphismes réduits peuvent être explicités. Dans le tableau suivant, u désigne $\pm\sqrt{\lambda^2 - \lambda + 1}$.

	transformation	ordre
Id	$(x, y) \mapsto (x, y)$	1
τ_1	$(x, y) \mapsto \left(\frac{\lambda - x}{(\lambda-1)x+1}, \frac{u^3 y}{((\lambda-1)x+1)^3}\right)$	2
τ_2	$(x, y) \mapsto \left(\frac{(\lambda-1)x+1}{\lambda x+1-\lambda}, \frac{u^3 y}{(\lambda x+1-\lambda)^3}\right)$	2
τ_3	$(x, y) \mapsto \left(\frac{\lambda x+1-\lambda}{x-\lambda}, \frac{u^3 y}{(x-\lambda)^3}\right)$	2
ρ_1	$(x, y) \mapsto \left(1 - \frac{1}{x}, \frac{y}{x^3}\right)$	3
ρ_2	$(x, y) \mapsto \left(\frac{1}{1-x}, \frac{y}{(1-x)^3}\right)$	3

On mime la construction effectuée lors de la démonstration du théorème 2 : à chaque involution τ_i non triviale de $\mathcal{C}$ on associe une paire de courbes elliptiques. Pour cela, on détermine un isomorphisme φ de $\mathcal{C}$ vers une courbe pour laquelle l'involution τ_i devient $(x, y) \mapsto (-x, y)$. On note $x_1 = 1$, x_2 et x_3 les valeurs prises par φ en 0, 1 et ∞. Les courbes elliptiques sont alors de la forme $y^2 = (x-1)(x-x_2^2)(x-x_3^2)$. Leurs formes de Legendre sont $y^2 = x(x-1)(x-\Lambda)$, où $\Lambda = (x_2^2 - x_3^2)/(1-x_3^2)$ et leurs j-invariants s'en déduisent. Tout ceci est résumé dans le tableau suivant :

involution	isomorphisme	action sur les points de Weierstraß	x_2	x_3	Λ
τ_1	$x \mapsto \frac{(-1-u)x+\lambda}{(-1+u)x+\lambda}$	$(0, \lambda), (1, \nu), (\infty, \mu)$	$\frac{-1-u+\lambda}{-1+u+\lambda}$	$\frac{u+1}{u-1}$	$\Lambda_1 = \lambda(\lambda - 1 - u)^2$
τ_2	$x \mapsto \frac{(\lambda-1-u)x+1}{(\lambda-1+u)x+1}$	$(0, \mu), (1, \lambda), (\infty, \nu)$	$\frac{-1-u+\lambda}{-1+u+\lambda}$	$\frac{\lambda-u}{\lambda+u}$	$\Lambda_2 = \frac{1}{\lambda(\lambda-1+u)^2}$
τ_3	$x \mapsto \frac{x-\lambda+u}{x-\lambda-u}$	$(0, \nu), (1, \mu), (\infty, \lambda)$	$\frac{-1-u+\lambda}{-1+u+\lambda}$	$\frac{\lambda-u}{\lambda+u}$	$\Lambda_3 = \frac{1}{\lambda(\lambda-1+u)^2}$

On note Λ'_i le conjugué de Λ_i obtenu en remplaçant u par $-u$. Alors on a les égalités $\Lambda_2 = \Lambda_3 = 1/\Lambda'_1$, et les j-invariants associés sont les mêmes. Il n'y a donc que deux classes d'isomorphismes de courbes quotients.

Les formules donnant c_0 et c_1 se vérifient en exprimant les modules (j_1, j_2, j_3) en fonction de λ. $\square$

Remarque On traite dans l'annexe en 2.(c) le cas d'annulation des dénominateurs.

Théorème 6 *Soit $\mathcal{C}$ une courbe dont les modules sont sur $\mathcal{D}$. Alors les deux courbes elliptiques quotients sont 3-isogènes l'une à l'autre.*

Démonstration Reprenons les notations de la démonstration précédente. Soit $\mathcal{E}_1$ la courbe elliptique associée à l'involution τ_1 mise sous forme de Legendre $y^2 = x(x-1)(x-\Lambda_1)$. Son polynôme de 3-division est alors

$$\psi_3(x) = 3x^4 + (-4\Lambda_1 - 4)x^3 + 6\Lambda_1 x^2 - \Lambda_1^2.$$

On vérifie que le polynôme linéaire suivant divise $\psi_3(x)$:

$$S_3(x) = 3x + \lambda - 2(u+1).$$

Il lui correspond un sous-groupe de $\mathcal{E}_1$ d'ordre 3. Les formules de Vélu [10] permettent alors de déterminer explicitement une courbe 3-isogène à $\mathcal{E}_1$ qui est donnée par

$$y^2 = x^3 + a_2 x^2 + a_4 x + a_6,$$

où a_2, a_4, a_6 sont définis par la suite de calculs suivants :

$$x_0 = \frac{2(u+1) - \lambda}{3}, \quad t = 6x_0^2 - 4(\Lambda_1 + 1)x_0 + 2\Lambda_1, \quad u = 4x_0^3 - 4(\Lambda_1 + 1)x_0^2 + 4\Lambda_1 x_0.$$

$$\begin{array}{rcl} a_2 & = & -(\Lambda_1 + 1), \\ a_4 & = & \Lambda_1 - 5t, \\ a_6 & = & 4(\Lambda_1 + 1)t - 7(u + x_0 t). \end{array}$$

On vérifie que le j-invariant de cette courbe est le conjugué du j-invariant de $\mathcal{E}_1$. $\square$

Corollaire 2 *Soit $\mathcal{C}$ une courbe de genre 2 admettant D_3 comme groupe réduit d'automorphismes. Alors l'anneau d'endomorphisme de la Jacobienne de $\mathcal{C}$ contient un ordre dans l'algèbre de quaternions $(\frac{3,1}{\mathbb{Q}})$. En particulier elle est à multiplication réelle par $\sqrt{3}$.*

Démonstration Soit $\mathcal{C}$ une courbe de genre 2 admettant D_3 comme groupe d'automorphismes. Alors $\mathrm{Jac}(\mathcal{C})$ est isogène à $\mathcal{E}_1 \times \mathcal{E}_2$, où $\mathcal{E}_1$ et $\mathcal{E}_2$ sont deux courbes elliptiques 3-isogènes. Notons $I : \mathcal{E}_1 \to \mathcal{E}_2$ une isogénie de degré 3, et $\hat{I}$ son isogénie duale.

Soit $\mathcal{O}$ l'anneau

$$\mathcal{O} = \left\{ \begin{pmatrix} a & \sqrt{3}b \\ \sqrt{3}c & d \end{pmatrix}, \text{ où } a, b, c, d \in \mathbb{Z} \right\}.$$

Alors l'application qui à $\begin{pmatrix} a & \sqrt{3}b \\ \sqrt{3}c & d \end{pmatrix}$ associe l'endomorphisme de $\mathcal{E}_1 \times \mathcal{E}_2$

$$\begin{array}{rcl} \mathcal{E}_1 \times \mathcal{E}_2 & \to & \mathcal{E}_1 \times \mathcal{E}_2 \\ (P,Q) & \mapsto & ([a]P + [b]\hat{I}Q, [c]IP + [d]Q). \end{array}$$

est un homomorphisme injectif d'anneaux.

La multiplication par $\sqrt{3}$ est représentée par exemple par l'endomorphisme

$$(P,Q) \mapsto (\hat{I}Q, IP).$$

□

3 Groupe d'automorphismes V_4

Comme dans le cas précédent, on commence par rappeler un résultat dû à Igusa.

Théorème 7 *Soit $\mathcal{C}$ une courbe de genre 2. Le groupe réduit d'automorphismes de $\mathcal{C}$ est V_4 si et seulement si $\mathcal{C}$ est isomorphe à une courbe d'équation*

$$y^2 = x(x-1)(x+1)(x-\lambda)(x-1/\lambda), \tag{5}$$

avec λ différent de 0, de -1 et de 1.

En termes d'invariants d'Igusa, $\mathcal{C}$ admet pour groupe d'automorphismes V_4 si et seulement si ses modules appartiennent à la courbe $\mathcal{V}$ d'équations

$$\begin{array}{rcl} 32j_1j_2^2 - 27j_1j_2 - 54j_2^2 + 4423680j_1j_3 + 14745600j_2j_3 - 13436928j_3 & = & 0, \\ 64j_2^3 - 78643200j_1j_2j_3 + 243j_1j_2 - 378j_2^2 + 31850496j_1j_3 - 8847360j_2j_3 & & \\ -36238786560000j_3^2 + 120932352j_3 & = & 0, \\ 3j_1^2 - 10j_1j_2 + 18j_2 - 4608000j_3 & = & 0. \end{array}$$

Ce résultat s'obtient par un calcul d'élimination.

Théorème 8 *Soit $\mathcal{C}$ une courbe de genre 2 admettant V_4 comme groupe réduit d'automorphismes. Alors la Jacobienne de $\mathcal{C}$ est isogène à deux carrés de courbes elliptiques. Ces courbes elliptiques sont 2-isogènes l'une à l'autre. Leurs j-invariants sont les racines de $j^2 + c_1 j + c_0$, où c_0 et c_1 sont donnés par les formules suivantes :*

$$\begin{array}{rcl} c_1 & = & \dfrac{9}{4}\dfrac{3j_1j_2 - 2j_2^2 + 1866240j_3 + 211200j_3j_1 + 64000j_3j_2}{j_3(-243 + 78j_1 + 20j_2)}, \\ c_0 & = & 108\dfrac{2560000j_3j_2 + 51j_1j_2 + 30j_2^2 + 768000j_3j_1 + 18662400j_3}{j_3(-243 + 78j_1 + 20j_2)}. \end{array}$$

Démonstration Quand la courbe $\mathcal{C}$ est sous la forme 5, les automorphismes réduits peuvent être explicités. Dans le tableau suivant, u désigne $\pm\sqrt{1-\lambda^2}$ et $\overline{u}$ désigne $\pm\sqrt{\lambda^2 - 1}$.

	transformation	ordre
Id	$(x,y) \mapsto (x,y)$	1
τ_1	$(x,y) \mapsto \left(\frac{x-\lambda}{\lambda x - 1}, \frac{u^3 y}{(\lambda x-1)^3}\right)$	2
τ_2	$(x,y) \mapsto \left(\frac{\lambda x - 1}{x-\lambda}, \frac{\overline{u}^3 y}{(x-\lambda)^3}\right)$	2
ρ	$(x,y) \mapsto \left(\frac{1}{x}, \frac{iy}{x^3}\right)$	4

On applique la même démarche que dans la démonstration du théorème 5. Cela nous mène au tableau suivant, qui nous donne les j-invariants des courbes quotients.

involution	isomorphisme	action sur les points de Weierstraß	x_2	x_3	Λ	j
τ_1	$\varphi_1(x) = \frac{(1-u)x-\lambda}{(1+u)x-\lambda}$	$(0,\lambda),(1,-1),(\infty,\frac{1}{\lambda})$	$\frac{\lambda+u-1}{\lambda-u-1}$	$\frac{1-u}{1+u}$	$\Lambda_1 = \frac{\lambda^2(1-\lambda)}{(\lambda-1-u)^2}$	$J_1 = 64\frac{(4-l^2)^3}{l^4}$
τ_2	$\varphi_2(x) = \frac{(-\lambda-\bar{u})x+1}{(-\lambda+\bar{u})x+1}$	$(0,\frac{1}{\lambda}),(1,-1),(\infty,\lambda)$	$\frac{\lambda+\bar{u}-1}{\lambda-\bar{u}-1}$	$\frac{\lambda+\bar{u}}{\lambda-\bar{u}}$	$\Lambda_2 = \frac{\lambda-1}{\lambda(\lambda-1-\bar{u})^2}$	$J_2 = 64\frac{(4l^2-1)^3}{l^2}$

Notons Λ_i' les valeurs conjuguées des Λ_i obtenues en remplaçant u par $-u$ et $\bar{u}$ par $-\bar{u}$. Alors $\Lambda_1 + \Lambda_1' = 1$ et $\Lambda_2 + \Lambda_2' = 1$, ce qui explique que les j-invariants des courbes correspondantes sont inchangés. Ainsi la Jacobienne de $\mathcal{C}$ est (2,2)-isogène à des produits $\mathcal{E}_1 \times \mathcal{E}_1$ et $\mathcal{E}_2 \times \mathcal{E}_2$, donc aussi à $\mathcal{E}_1 \times \mathcal{E}_2$. Enfin, les courbes $\mathcal{E}_1$ et $\mathcal{E}_2$ sont 2-isogènes l'une à l'autre car le couple (J_1, J_2) annule l'équation modulaire de degré 2.

4 Exemples

4.1 Cas génerique

Soit la courbe $\mathcal{C}$ définie sur $\mathbb{Q}$ par l'équation

$$y^2 = x^6 - x^5 + x^4 - x^2 - x - 1.$$

Ses invariants d'Igusa sont

$$j_1 = \frac{2^3 \times 3^2 \times 5 \times 13}{37^2},\ j_2 = -\frac{2^3 \times 3^3 \times 11 \times 13}{37^3},\ j_3 = \frac{3^5 \times 53^2}{2^8 \times 37^5}.$$

On vérifie qu'ils sont dans l'ouvert $\mathcal{U}$, et donc $\mathrm{Jac}(\mathcal{C})$ est isogène au produit de deux courbes elliptiques. Sur cet exemple, trouver ces courbes en passant par une forme de Rosenhain nécessiterait de passer dans une extension de $\mathbb{Q}$ de degré 24. Les propositions 2 et 3 permettent de calculer directement

$$c_0 = \frac{2^{14} \times 5^6 \times 37^3}{53^2},\ c_1 = \frac{2^8 \times 3^4 \times 47}{53},$$

et les j-invariants des courbes elliptiques sont définis sur le corps $\mathbb{Q}(i)$ par

$$j = -\frac{2^7 \times 3^4 \times 47}{53} \pm \frac{2^8 \times 7 \times 11 \times 181}{53} i.$$

Notons que 53 est un facteur du discriminant de la courbe. Il n'est donc pas surprenant de le retrouver au dénominateur des valeurs de j et dans l'expression de j_3.

4.2 Courbe $\mathcal{D}$

L'exemple suivant est tiré de l'article [5], où Kulesz construit une courbe ayant de nombreux points rationnels. Soit la courbe $\mathcal{C}$ définie sur $\mathbb{Q}$ par l'équation

$$y^2 = 1412964(x^2 - x + 1)^3 - 8033507x^2(x-1)^2.$$

Ses invariants d'Igusa sont

$$\begin{aligned} j_1 &= \frac{3^2 \times 149 \times 167 \times 239^2 \times 3618470803 \times 33613^2}{757^2 \times 768321547757^2}, \\ j_2 &= -\frac{3^3 \times 239^2 \times 33613^2 \times 195593 \times 3142231650748541037325 7}{757^3 \times 768321547757^3}, \\ j_3 &= -\frac{2^{22} \times 3^17 \times 5^9 \times 7^6 \times 47^3 \times 89^3 \times 239^4 \times 33613^4}{757^5 \times 768321547757^5}. \end{aligned}$$

On vérifie qu'ils sont $\mathcal{D}$, et donc le groupe d'automorphismes réduit de la courbe est D_3. En fait la manière dont cette courbe est construite dans [5] implique directement ce résultat. Là encore, écrire une forme de Rosenhain pour cette courbe nécessiterait de passer dans une extension de $\mathbb{Q}$. Nos formules donnent directement les j-invariants des courbes elliptiques quotients :

$$j = -\frac{239 \times 33613 \times 84333563^3}{2^{24} \times 3^4 \times 5^9 \times 7^2 \times 47^3 \times 89}, \quad \text{et} \quad j' = \frac{19^3 \times 67^3 \times 239 \times 349^3 \times 33613}{2^8 \times 3^{12} \times 5^3 \times 7^6 \times 47 \times 89^3}.$$

4.3 Courbe $\mathcal{V}$

Dans [8], Leprévost et Morain ont étudié la courbe $\mathcal{C}_\theta$ définie sur $\mathbb{Q}(\theta)$ par

$$y^2 = x(x^4 - \theta x^2 + 1),$$

avec comme objectif des calculs de sommes de caractères. Ses invariants d'Igusa sont

$$j_1 = 144\frac{9\theta^2 - 20}{(3\theta^2+20)^2}, \quad j_2 = -3456\frac{27\theta^2 - 140}{(3\theta^2+20)^3}, \quad j_3 = 243\frac{\theta^2 - 4}{(3\theta^2+20)^5}.$$

On vérifie qu'ils annulent les polynômes définissant $\mathcal{V}$, et donc le groupe d'automorphismes réduit de la courbe est V_4. On trouve alors les j-invariants des courbes elliptiques quotients :

$$j = 64\frac{(3\theta-10)^3}{(\theta-2)(\theta+2)^2} \quad \text{et} \quad j' = 64\frac{(3\theta+10)^3}{(\theta+2)(\theta-2)^2}.$$

Notons que les courbes E_θ et E'_θ données dans [8] :

$$y^2 = x(x^2 \pm 4x + 2 - \theta),$$

ont toutes les deux le même j-invariants j'. Les autres courbes quotients, d'invariant j sont les courbes d'équations :

$$y^2 = x(x^2 \pm 4x + 2 + \theta).$$

Annexe : formulaire

Nous complétons l'étude précédente par les formules traitant des cas suivants :

- Le groupe réduit d'automorphismes $\mathcal{G}$ n'est ni $\mathcal{D}$, ni $\mathcal{V}$, ni $\mathbb{Z}/2\mathbb{Z}$: ce sont les deux points traités en 2.(a) et 2.(b) ci-dessous.
- Un dénominateur s'annule. Sur la courbe $\mathcal{D}$ cela se produit en un point traité en 2.(c), dans le cas générique, deux courbes doivent être étudiées, en 2.(f) et 2.(g).
- Le covariant A est nul, et les invariants choisis ne sont plus adaptés. On en choisit deux autres, et on procède à la même étude exhaustive.

Nous regroupons ces formules sous forme d'un algorithme prenant en entrée une courbe quelconque de genre 2, dont la Jacobienne est (2,2)-décomposable, et qui retourne le polynôme minimal des j-invariants des courbes elliptiques quotients de la Jacobienne.

1. Calculer les covariants A, B, C, D de la courbe, et vérifier que $R = 0$.
2. Cas où A est non nul : calculer j_1, j_2, j_3.
   (a) Si $(j_1, j_2, j_3) = (\frac{81}{20}, -\frac{729}{200}, \frac{729}{25600000})$, alors le groupe d'automorphismes est D_6 et retourner $j(j - 54000)$.
   (b) Si $(j_1, j_2, j_3) = (-\frac{36}{5}, \frac{1512}{25}, \frac{243}{200000})$, alors le groupe d'automorphismes est $\mathfrak{S}_4$, et retourner $j - 8000$.

(c) Si $(j_1, j_2, j_3) = (\frac{24297228}{885481}, -\frac{81449284536}{833237621}, -\frac{57798021931029}{47220229240364864})$, alors le groupe d'automorphismes est D_3 et retourner $j^2 + \frac{471690263168}{658503} j - \frac{8094076887461888}{57289761}$.

(d) Si (j_1, j_2, j_3) annulent les polynômes définissant $\mathcal{D}$, alors le groupe d'automorphismes est D_3, et retourner les j calculés en section 2.

(e) Si (j_1, j_2, j_3) annulent les polynômes définissant $\mathcal{V}$, alors le groupe d'automorphismes est V_4, et retourner les j calculés en section 3.

(f) Si (j_1, j_2, j_3) vérifient

$$\begin{aligned} 331776 j_3 - j_2^2 - 24 j_1 j_2 - 144 j_1^2 &= 0, \\ 9 j_1 + j_2 &= 0, \end{aligned}$$

alors le groupe d'automorphismes est $\mathbb{Z}/2\mathbb{Z}$ et retourner

$$j^2 + \frac{150994944 j_3}{j_2 + 12 j_1} j - \frac{260919263232 j_3}{j_2 + 12 j_1}.$$

(g) Si (j_1, j_2, j_3) vérifient

$$\begin{aligned} j_2^5 + 54 j_2^4 - 322486272 j_2^2 j_3 + 481469424205824 j_3^2 &= 0, \\ 18 j_1 + 5 j_2 &= 0, \end{aligned}$$

alors le groupe d'automorphismes est $\mathbb{Z}/2\mathbb{Z}$ et retourner $j^2 + c_1 j + c_0$, où

$$\begin{aligned} c_0 &= -\frac{125}{9559130112} \frac{(-j_2^2 - 24 j_1 j_2 - 144 j_1^2 + 16257024 j_3)^2}{j_3^2} \\ c_1 &= \frac{(-j_2^2 - 24 j_1 j_2 - 144 j_1^2 + 16257024 j_3)(2723051520 j_3 - 289 j_2^2 - 6936 j_1 j_2 - 41616 j_1^2)}{2064772104192 j_3^2}, \end{aligned}$$

(h) Sinon on est dans le cas “générique”, et retourner les j calculés en section 1

3. Cas où $A = 0$

(a) Si $B = 0$ et $C^5 = 4050000 D^3$, alors le groupe d'automorphismes est $\mathbb{Z}/2\mathbb{Z}$, retourner $(j - 4800)(j - 8640)$.

(b) Si $C = 0$ et $B^5 = 3037500 D^2$, alors le groupe d'automorphismes est $\mathbb{Z}/2\mathbb{Z}$, retourner $(j - 160)(j + 21600)$.

Calculer les invariants

$$t_1 = \frac{3}{512} \frac{CD}{B^4} \quad \text{et} \quad t_2 = 1536 \frac{BC}{D}.$$

(c) Si $(t_1, t_2) = (1/576000, -460800)$, alors le groupe d'automorphismes est V_4, et retourner $j^2 + 7200 j + 13824000$.

(d) Si $(t_1, t_2) = (-1/864000, -172800)$, alors le groupe d'automorphismes est D_3, et retourner $j^2 + 55200 j - 69984000$.

(e) On est dans le cas “générique” pour $A = 0$. Calculer

$$\begin{aligned} \Omega &= -4 \frac{-238878720000 t_1 + 1555200 t_2 t_1 + 7 t_2^2 t_1 + 2 t_2}{477757440000 t_1 + 2073600 t_2 t_1 + t_2^2 t_1 - t_2}, \\ \Upsilon &= \frac{3}{4} \frac{(20 t_1^4 t_2^4 + 6912000 t_2^3 t_1^4 + 4 t_2^3 t_1^3)(1911029760000 t_1^3 t_2 - 12441600 t_2^2 t_1^3 - 56 t_2^3 t_1^3 - 16 t_2^2 t_1^2)}{(10 t_1^4 t_2^4 + 3456000 t_2^3 t_1^4 + 2 t_2^3 t_1^3)(955514880000 t_1^3 t_2 + 4147200 t_2^2 t_1^3 + 2 t_2^3 t_1^3 - 2 t_2^2 t_1^2)}. \end{aligned}$$

puis c_0 et c_1 par les formules de la section 1. Retourner $j^2 + c_1 j + c_0$.

Références

[1] O. Bolza. On binary sextics with linear transformations onto themselves. *Amer. J. Math.*, 10:47–70, 1888.

[2] E. Howe, F. Leprevost, and B. Poonen. Large torsion subgroups of split Jacobians of curves of genus two or three. To appear in *Forum Math.*

[3] J. Igusa. Arithmetic variety of moduli for genus two. *Ann. of Math. (2)*, 72:612–649, 1960.

[4] J. Igusa. On siegel modular forms of genus two. *Amer. J. Math.*, 84:175–200, 1962.

[5] L. Kulesz. Courbes algébriques de genre 2 possédant de nombreux points rationnels. *C. R. Acad. Sci. Paris Sér. I Math.*, 321:91–94, 1995.

[6] L. Kulesz. Application de la méthode de Dem'janenko-Manin à certaines familles de courbes de genre 2 et 3. *J. Number Theory*, 76:130–146, 1999.

[7] H. Lange. Über die Modulvarietät der Kurven vom Geschlecht 2. *J. Reine Angew. Math.*, 281:80–96, 1976.

[8] F. Leprévost and F. Morain. Revêtements de courbes elliptiques à multiplication complexe par des courbes hyperelliptiques et sommes de caractères. *J. Number Theory*, 64:165–182, 1997.

[9] J.-F. Mestre. Construction de courbes de genre 2 à partir de leurs modules. In T. Mora and C. Traverso, editors, *Effective methods in algebraic geometry*, volume 94 of *Progr. Math.*, pages 313–334. Birkhäuser, 1991. Proc. Congress in Livorno, Italy, April 17–21, 1990.

[10] Jacques Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. I Math.*, 273:238–241, July 1971. Série A.