

BULLETIN DE LA S. M. F.

PIERRE LE DUFF

**Représentations galoisiennes associées aux
points d'ordre ℓ des jacobiniennes de certaines
courbes de genre 2**

Bulletin de la S. M. F., tome 126, n° 4 (1998), p. 507-524

http://www.numdam.org/item?id=BSMF_1998__126_4_507_0

© Bulletin de la S. M. F., 1998, tous droits réservés.

L'accès aux archives de la revue « Bulletin de la S. M. F. » (<http://smf.emath.fr/Publications/Bulletin/Presentation.html>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

**REPRÉSENTATIONS GALOISIENNES ASSOCIÉES AUX
POINTS D'ORDRE ℓ DES JACOBIENNES DE
CERTAINES COURBES DE GENRE 2**

PAR PIERRE LE DUFF (*)

RÉSUMÉ. — Soit J la jacobienne d'une courbe C de genre 2 définie sur \mathbb{Q} . Soit p un nombre premier. On suppose que la réduction du modèle de Néron de J sur \mathbb{Q}_p est une extension d'une courbe elliptique par un tore. Soit $\bar{\mathbb{Q}}$ une clôture algébrique de \mathbb{Q} ; le groupe de Galois $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ agit sur les points de ℓ -division de J . On note ρ_ℓ la représentation associée. De plus, on suppose qu'il existe un nombre premier de bonne réduction q tel que le groupe de Galois sur \mathbb{Q} du polynôme caractéristique de l'endomorphisme de Frobenius en q est le groupe diédral à 8 éléments (ce qui implique que J est absolument simple). On peut alors déterminer une infinité de nombres premiers ℓ pour lesquels l'image de ρ_ℓ est $\text{GSp}(4, \mathbb{F}_\ell)$. Deux exemples sont traités à la fin de l'article.

ABSTRACT. — POINTS OF ORDER ℓ OF THE JACOBIAN OF SPECIAL CURVES OF GENUS 2. — Let J be the Jacobian of a curve C of genus 2, defined over \mathbb{Q} . Let p be a prime number. Assume that the reduction of the Néron model of J over \mathbb{Q}_p is an extension of an elliptic curve by a torus. We denote by $\bar{\mathbb{Q}}$ an algebraic closure of \mathbb{Q} ; the Galois group $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on the ℓ -division points of J . We denote by ρ_ℓ the associated representation. Let q be a prime number where J has good reduction such that the Galois group over \mathbb{Q} of the characteristic polynomial of the Frobenius endomorphism associated to q is the dihedral group with 8 elements (this implies that J is absolutely simple). Then an infinite set of prime numbers can be found such that the image of ρ_ℓ is $\text{GSp}(4, \mathbb{F}_\ell)$. Two examples will be given at the end of this article.

0. Introduction

Soit J une variété abélienne de dimension g , définie sur K un corps de nombres. Fixons \bar{K} une clôture algébrique de K et notons G_K le groupe

(*) Texte reçu le 29 juillet 1997, révisé le 28 avril 1998.

P. LE DUFF, Département de Mathématiques, Université de Caen, Esplanade de la Paix, 14032 Caen CEDEX (France). Email Leduff@math.unicaen.fr.

Classification AMS : 14H40, 14G05.

Mots clés : groupe symplectique, variété abélienne, représentation galoisienne.

de Galois $\text{Gal}(\bar{K}/K)$. Pour m un nombre entier, on note

$$J_m = \text{Hom}(\mathbb{Z}/m\mathbb{Z}, J(\bar{K}))$$

le groupe des points d'ordre divisant m de J . Le groupe G_K agit sur J_ℓ et on note ρ_ℓ la représentation Galoisienne associée :

$$\rho_\ell : \text{Gal}(\bar{K}/K) \longrightarrow \text{GL}(2g, \mathbb{F}_\ell).$$

Dans le cas des courbes elliptiques, l'étude de l'image de ρ_ℓ est faite dans [S1]. Ainsi, si E est une courbe elliptique sans multiplication complexe sur \bar{K} , alors, pour tout nombre premier suffisamment grand,

$$\rho_\ell(G_K) = \text{GL}(2, \mathbb{F}_\ell).$$

On peut être plus précis et affirmer qu'il existe une constante ℓ_0 qui dépend de manière effective de la hauteur de E , du degré et du discriminant du corps de nombres tel que, pour tout nombre premier $\ell > \ell_0$, on a (cf. [MW])

$$\rho_\ell(G_K) = \text{GL}(2, \mathbb{F}_\ell).$$

Ribet dans [R] a étudié le cas des variétés abéliennes à multiplications réelles. Il considère J une variété abélienne telle que $E = \text{End}_K J \otimes \mathbb{Q}$ est un corps totalement réel de degré la dimension de J . L'image de ρ_ℓ est incluse, pour presque tout ℓ , dans $\text{GL}(2, \mathcal{O}/\ell\mathcal{O})$ où \mathcal{O} est l'anneau des entiers de E . Dans le cas où J n'a pas partout potentiellement bonne réduction, il démontre que pour presque tout ℓ ,

$$\text{Im } \rho_\ell = \{u \in \text{GL}(2, \mathcal{O}/\ell\mathcal{O}) : \det u \in \mathbb{F}_\ell^*\}.$$

Serre a généralisé dans [S2] certains de ses résultats sur les courbes elliptiques au cas des variétés de dimension supérieure. Notons $\text{GSp}(2g, \mathbb{F}_\ell)$ le groupe des similitudes symplectiques et supposons que J possède une polarisation de degré d^2 sur K . Si ℓ ne divise pas d , l'image de ρ_ℓ est incluse dans $\text{GSp}(2g, \mathbb{F}_\ell)$. On suppose qu'il existe $\ell_0 > 3$ tel que l'image de ρ_{ℓ_0} soit $\text{GSp}(2g, \mathbb{F}_{\ell_0})$. Il résulte d'un théorème de Serre (voir [S2]) qu'il existe un nombre C (non effectif) tel que, pour tout $\ell > C$, le groupe de Galois en ℓ soit $\text{GSp}(2g, \mathbb{F}_\ell)$. Il semble pour le moment très difficile de rendre ce résultat effectif.

Le but de cet article est de donner des exemples de variétés abéliennes de dimension 2 pour lesquelles on sait déterminer un ensemble infini explicite de nombres premiers ℓ pour lesquels l'image de ρ_ℓ est $\text{GSp}(2g, \mathbb{F}_\ell)$.

Soient \bar{v} une valuation discrète de \bar{K} et $I_{\bar{v}}$ le groupe d'inertie relatif à \bar{v} . On étudie dans le § 1 l'action de $I_{\bar{v}}$ sur les points d'ordre divisant ℓ de J . Dans le cas où la variété abélienne a mauvaise réduction, on en déduit l'existence d'un élément d'ordre ℓ , noté σ , qui appartient à l'image de ρ_{ℓ} et on sait calculer $\dim(\ker(\sigma - 1))$. On s'intéresse au cas des variétés de dimension 2 définie sur \mathbb{Q} dont la fibre spéciale du modèle de Néron est une extension d'une courbe elliptique par un tore. L'élément d'ordre ℓ obtenu est alors une *transvection* :

$$\dim(\ker(\sigma - 1)) = 3.$$

On démontre ensuite dans le § 2 que le groupe des isométries symplectiques $\mathrm{Sp}(4, \mathbb{F}_{\ell})$ est engendré par n'importe quel couple formé d'une transvection et d'un élément dont le polynôme caractéristique est irréductible. Lorsque J est la jacobienne d'une courbe de genre deux, on sait calculer les polynômes caractéristiques des images par ρ_{ℓ} des éléments de Frobenius (§ 3). Supposons déterminé un nombre premier q de bonne réduction tel que le groupe de Galois sur \mathbb{Q} du polynôme caractéristique de l'élément de Frobenius en q est le groupe diédral à 8 éléments (ce qui implique que J est absolument simple). On peut alors déterminer une infinité de nombres premiers ℓ pour lesquels l'image de ρ_{ℓ} est $\mathrm{GSp}(4, \mathbb{F}_{\ell})$ (§ 4). Une version condensée des §§ 1, 3, 4 est déjà parue dans [LD1]. Deux exemples numériques sont traités à la fin de cet article.

Notations. — Dans tout ce qui suit,

- K est un corps de nombres algébriques,
- \bar{K} est une clôture algébrique de K ,
- v est une valuation discrète de K et \bar{v} une extension de v à \bar{K} ,
- O_v est l'anneau de valuation de v , le corps résiduel est noté k_v et p_v désigne sa caractéristique,
- $I_{\bar{v}}$ désigne le groupe d'inertie relatif à \bar{v} .

1. Étude de l'action du groupe d'inertie

Soit J une variété abélienne de dimension g définie sur K . Pour m un nombre entier non nul, on note

$$J_m = \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, J(\bar{K})).$$

On sait que J_m est un $\mathbb{Z}/m\mathbb{Z}$ -module libre de rang $2g$. Dans cette partie, on s'intéresse à l'action du groupe d'inertie sur ce module. On rappelle

que J a bonne réduction s'il existe un schéma abélien J_v sur $\text{Spec}(O_v)$ tel que

$$J \simeq J_v \times_{O_v} K.$$

Soit J_v le modèle de Néron de J relatif à v (cf. [BLR, p. 12]). On note

$$\tilde{J}_v = J_v \times_{O_v} k$$

la fibre spéciale de J ; c'est un groupe algébrique commutatif sur k_v . Soit \tilde{J}_v^0 la composante connexe contenant l'élément neutre de \tilde{J}_v ; c'est l'extension d'une variété abélienne par un groupe linéaire. Fixons \bar{k}_v une clôture algébrique de k_v et notons

$$\tilde{J}_\ell = \text{Hom}(\mathbb{Z}/\ell\mathbb{Z}, \tilde{J}_v(\bar{k}_v))$$

le groupe des points d'ordre divisant ℓ de la fibre spéciale. Enfin, soit J_ℓ^I le sous-groupe de J_ℓ qui est fixé par $I_{\bar{v}}$. Le groupe des composantes connexes est un groupe fini d'ordre noté $(\tilde{J}_v : \tilde{J}_v^0)$.

PROPOSITION 1.1. — *Soit J une variété abélienne sur K ayant mauvaise réduction en v et soit ℓ un nombre premier différent de la caractéristique de k . Si ℓ ne divise pas $(\tilde{J}_v : \tilde{J}_v^0)$, alors l'extension $K(J_\ell)/K$ est ramifiée en v .*

Démonstration. — La composante connexe \tilde{J}_v^0 est une extension d'une variété abélienne B par un groupe linéaire H tel que $H = S \times U$ où S est un tore et U est unipotent. On sait [ST, lemme 1, p. 494] que \tilde{J}_ℓ est l'extension d'un groupe d'ordre divisant $(\tilde{J}_v : \tilde{J}_v^0)$ par un $\mathbb{Z}/\ell\mathbb{Z}$ -module libre de rang $\dim(S) + 2 \dim(B)$. De plus, \tilde{J}_ℓ est isomorphe à $J_\ell^{I_v}$ [ST, lemme 2]. La condition sur ℓ impose que $J_\ell^{I_v}$ est de rang $\dim(S) + 2 \dim(B)$. La variété a mauvaise réduction en v , donc

$$\dim(S) + 2 \dim(B) < 2 \dim(J).$$

Donc J_ℓ^I n'est pas de rang $2 \dim(J)$; autrement dit l'extension $K(J_\ell)/K$ est ramifiée en v . \square

Supposons maintenant que J a une polarisation de degré d^2 et que ℓ est un nombre premier ne divisant pas d . La polarisation munit J_ℓ d'une forme bilinéaire alternée non dégénérée

$$W : J_\ell \times J_\ell \longrightarrow \mu_\ell,$$

appelée *accouplement de Weil*. Notons μ_ℓ additivement, et soit

$$\epsilon_\ell : \text{Gal}(\bar{K}/K) \longrightarrow \mathbb{F}_\ell^*$$

le caractère cyclotomique. Lorsque $(P, Q) \in J_\ell \times J_\ell$ et $\sigma \in \text{Gal}(\bar{K}/K)$, on a :

$$W(\sigma(P), \sigma(Q)) = \epsilon_\ell(\sigma) W(P, Q).$$

Autrement dit, l'application $P \mapsto \sigma(P)$ est une similitude symplectique de J_ℓ de multiplicateur $\epsilon_\ell(\sigma) \in \mathbb{F}_\ell^*$. On obtient ainsi une représentation galoisienne

$$\rho_\ell : \text{Gal}(\bar{K}/K) \longrightarrow \text{GSp}(2g, \mathbb{F}_\ell),$$

où GSp désigne le groupe des similitudes symplectiques. Il existe dans $\text{GSp}(2g, \mathbb{F}_\ell)$ des éléments d'ordre ℓ auquel on s'intéressera plus particulièrement dans le § 2.

DÉFINITION 1.2. — *Une similitude symplectique d'ordre ℓ qui laisse stable un hyperplan est appelée transvection.*

Lorsque la variété abélienne a un certain type de mauvaise réduction, on peut en déduire l'existence d'une transvection dans l'image de ρ_ℓ .

PROPOSITION 1.3. — *Soit J une variété abélienne sur K dont la réduction \tilde{J}_v en v est une extension d'une variété abélienne de dimension $\dim(J) - 1$ par un tore de dimension 1. Soit ℓ un nombre premier différent de la caractéristique de k_v et qui ne divise pas $(\tilde{J}_v : \tilde{J}_v^0)$. Il existe alors un élément du groupe d'inertie de v dont l'image par ρ_ℓ est une transvection.*

Démonstration. — En effet, \tilde{J}_v^0 est alors un $\mathbb{Z}/\ell\mathbb{Z}$ -module libre de rang $2 \dim(J) - 1$. Le groupe d'inertie laisse fixe un sous-espace de dimension $2 \dim(J) - 1$; l'extension $K(J_\ell)/K$ est ramifiée en v donc il existe α appartenant au groupe d'inertie tel que $\rho_\ell(\alpha) \neq \text{Id}$. Cet élément est une transvection. \square

REMARQUE. — On peut se demander ce qui se passe lorsque ℓ divise $(\tilde{J}_v : \tilde{J}_v^0)$. Considérons J la jacobienne d'une courbe de genre 2 à réduction totalement dégénérée. On sait, par la proposition 1.1, que pour ℓ qui ne divise pas $(\tilde{J}_v : \tilde{J}_v^0)$, il existe $\sigma \in I_{\bar{v}}$ tel que

$$\dim(\ker(\rho_\ell(\sigma) - 1)) = 2.$$

On peut montrer que, si $(\tilde{J}_v : \tilde{J}_v^0)$ est divisible par ℓ mais pas par ℓ^2 , il existe $\sigma \in I_{\bar{v}}$ tel que $\rho_\ell(\sigma)$ est une transvection. Dans le cas où ℓ^2 divise $(\tilde{J}_v : \tilde{J}_v^0)$, on ne peut rien affirmer, sans autres hypothèses, sur la ramification en v de l'extension $K(J_\ell)/K$.

2. Sous-groupes de $\mathrm{Sp}(4, \mathbb{F}_\ell)$

2.1. Définitions générales.

Sauf mention contraire dans toute cette partie, ℓ désignera un nombre premier impair. Pour les résultats généraux sur la géométrie symplectique on renvoie à [A]. Les sous-groupes maximaux des groupes finis classiques ont été étudiés dans [As] puis dans [KL]. Cependant, ces travaux ne traitent pas les cas de petites dimensions qui ont été étudiés précédemment. Le but de cette partie est de démontrer que $\mathrm{Sp}(4, \mathbb{F}_\ell)$ est engendré par n'importe quel couple formé d'une transvection et d'un élément dont le polynôme caractéristique est irréductible (voir théorème 2.7). On utilise la liste des sous-groupes maximaux de $\mathrm{Sp}(4, \mathbb{F}_\ell)$ donnée par Mitchell [M] dont on redonne une démonstration.

Soit V un \mathbb{F}_ℓ -espace vectoriel de dimension 4 muni d'une forme bilinéaire alternée non dégénérée w . Une base (e_1, e_2, e_3, e_4) de V est dite *symplectique* si elle vérifie :

$$\begin{aligned} \forall i, \quad w(e_1, e_i) &= \delta_{i3}, \\ \forall j, \quad w(e_2, e_j) &= \delta_{j4}, \\ w(e_3, e_4) &= 0. \end{aligned}$$

Le sous-espace vectoriel engendré par v_1, v_2, \dots, v_k est noté

$$\langle v_1, v_2, \dots, v_k \rangle.$$

Dans tout ce qui suit, a_1, a_2, a_3, a_4 désignent des éléments de \mathbb{F}_ℓ ; on écrit

$$v = {}^t(a_1, a_2, a_3, a_4)$$

le vecteur $v = a_1e_1 + a_2e_2 + a_3e_3 + a_4e_4$. Un sous-espace H de V est dit *isotrope* si $H \cap H^\perp \neq \{0\}$ et *totalement isotrope* si $H \subset H^\perp$. Les plus grands sous-espaces totalement isotropes sont de dimension 2. Ainsi, $P_{12} = \langle e_1, e_2 \rangle$ est totalement isotrope tandis que $P_{13} = \langle e_1, e_3 \rangle$ ne l'est pas car $w(e_1, e_3) = 1$.

Si H est un hyperplan de V , alors $\dim H = 3$ et $\dim H^\perp = 1$. De plus, une forme alternée est toujours dégénérée sur un espace de dimension impaire; donc $H \cap H^\perp \neq \{0\}$ et donc $H^\perp \subset H$. Le sous-espace H^\perp s'appelle le *centre* de l'hyperplan H . Tous les plans d'un hyperplan passant par son centre sont totalement isotropes. Ainsi $H = \langle e_1, e_3, e_4 \rangle$ a pour centre $\langle e_4 \rangle$ et pour tout $(a_1, a_3, a_4) \in \mathbb{F}_\ell^3$ avec $a_1 \neq 0$ ou $a_3 \neq 0$; le plan $\langle e_4, a_1e_1 + a_3e_3 + a_4e_4 \rangle$ est totalement isotrope. On désigne par $\mathrm{Sp}(4, \mathbb{F}_\ell)$ le groupe des isométries symplectiques de V . Autrement dit, ce sont les

éléments M de $GL(4, \mathbb{F}_\ell)$ vérifiant, pour tout $(v_1, v_2) \in V^2$,

$$w(M(v_1), M(v_2)) = w(v_1, v_2)$$

C'est un groupe d'ordre $\ell^4(\ell^4 - 1)(\ell^2 - 1)$.

Si σ est une transvection, on appelle *axe* (resp. *centre*) de σ l'hyperplan qu'elle fixe (resp. la droite $\text{Im}(\sigma - 1)$). Soient $v_1 = (\sigma - 1)(u)$ un élément de $\text{Im}(\sigma - 1)$ et $v_2 \in \ker(\sigma - 1)$. On a :

$$w(v_1, v_2) = w((\sigma - 1)(u), \sigma(v_2)) = -w(u, v_2) + w(u, \sigma(v_2)) = 0.$$

Autrement dit, $\text{Im}(\sigma - 1)$ est égal à $\ker(\sigma - 1)^\perp$. Tous les plans et les hyperplans coupant le centre d'une transvection sont stables par cette transvection. Par exemple, on notera dans toute cette partie :

$$T_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Le centre de T_4 est $\langle e_4 \rangle$, son axe est $\langle e_1, e_3, e_4 \rangle$.

2.2. Sous-groupes de $Sp(4, \mathbb{F}_\ell)$ contenant des transvections.

THÉORÈME 2.2. — Soit G un sous-groupe propre de $Sp(4, \mathbb{F}_\ell)$ contenant une transvection. L'une au moins des trois assertions suivantes est vérifiée :

- (1) G laisse stable un hyperplan de V et une droite de cet hyperplan,
- (2) G laisse stable un plan totalement isotrope,
- (3) les éléments de G stabilisent ou échangent deux plans non totalement isotropes supplémentaires orthogonaux.

Démonstration. — Soit G un groupe de $Sp(4, \mathbb{F}_\ell)$ contenant une transvection et qui ne vérifie aucune des propriétés (1), (2) et (3). On va montrer l'existence dans G de quatre transvections particulières qui engendrent $Sp(4, \mathbb{F}_\ell)$. Quitte à faire un changement de base on peut supposer que la transvection contenue dans $Sp(4, \mathbb{F}_\ell)$ est T_4 dont le centre est $\langle e_4 \rangle$. On va utiliser plusieurs fois le résultat suivant :

LEMME 2.3. — On suppose que $v \notin \langle e_1, e_3, e_4 \rangle$. Il existe alors $k \in \mathbb{N}^*$ tel que $T_4^k(v) \in \langle e_1, e_2, e_3 \rangle$.

Démonstration. — En effet, v est de la forme ${}^t(a_1, a_2, a_3, a_4)$ avec $a_2 \neq 0$. Or

$$T_4^k(v) = {}^t(a_1, a_2, a_3, a_4 + ka_2).$$

En prenant $k = \frac{a_4}{a_2}$ on obtient le résultat. \square

Étape 1. — On montre que, quitte à changer de base, G contient une transvection de centre $\langle e_2 \rangle$.

LEMME 2.4. — *Il existe $g \in G$ tel que $g(e_4) \notin \langle e_1, e_3, e_4 \rangle$.*

Démonstration. — Comme, par hypothèse, le groupe G ne vérifie pas la propriété (1), il existe donc $g_1 \in G$ tel que $g_1(e_4) \notin \langle e_4 \rangle$. Lorsque $g_1(e_4) \notin \langle e_1, e_3, e_4 \rangle$, on choisit $g = g_1$. Dans le cas contraire, considérons le plan $\langle g_1(e_4), e_4 \rangle$. Comme on l'a remarqué précédemment, c'est un plan totalement isotrope. La deuxième assertion n'étant pas vérifiée par G , il existe $g_2 \in G$ qui ne laisse pas stable ce plan. On peut supposer que $g_2(e_4) \notin \langle g_1(e_4), e_4 \rangle$. Si $g_2(e_4) \notin \langle e_1, e_3, e_4 \rangle$, on choisit $g = g_2$. Sinon $\langle g_2(e_4), g_1(e_4), e_4 \rangle$ est un hyperplan contenu dans $\langle e_1, e_3, e_4 \rangle$; il lui est donc égal. Cet hyperplan n'est pas stable; donc il existe $g \in G$ tel que $g(e_4) \notin \langle e_1, e_3, e_4 \rangle$. \square

Écrivons $g(e_4) = {}^t(b_1, b_2, b_3, b_4)$ où $b_2 \neq 0$ et appliquons le lemme 2.3. Il existe k tel que

$$z = T_4^k \circ g(e_4) = {}^t(b_1, b_2, b_3, 0).$$

Il existe donc une transvection de centre $\langle z \rangle$ appartenant à $\langle e_1, e_2, e_3 \rangle$ mais pas à $\langle e_1, e_3 \rangle$. Il existe un changement de base symplectique qui laisse stable l'axe et le centre de T_4 et qui envoie $\langle z \rangle$ sur $\langle e_2 \rangle$. Par exemple, on peut prendre comme matrice de passage :

$$P = \begin{pmatrix} b_2 & b_1 & 0 & 0 \\ 0 & b_2 & 0 & 0 \\ 0 & b_3 & 1/b_2 & 0 \\ b_3 & 0 & -b_1/b_2^2 & 1/b_2 \end{pmatrix}.$$

On peut donc supposer que G contient deux transvections T_4 et T_2 de centre $\langle e_4 \rangle$ et $\langle e_2 \rangle$. L'élément T_2 est représenté par la matrice :

$$T_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Étape 2. — On montre que, quitte à changer de base, G contient une transvection de centre $\langle e_2 + e_3 \rangle$. Le groupe G contient les deux transvections T_4 et T_2 .

Notons G_1 le groupe engendré par T_2 et T_4 . Ce groupe agit transitivement sur les droites de $P_{24} = \langle e_2, e_4 \rangle$, donc G_2 contient toutes les transvections de centre appartenant à P_{24} . De plus, G_2 laisse stable P_{24} et P_{13} . Puisque G ne vérifie pas l'assertion 2, il existe un élément de G qui ne laisse pas stable ces deux plans et qui ne les échange pas. Soient $v_0 \in P_{24}$ et $g_0 \in G$ tels que $g_0(v_0) \notin P_{24} \cup P_{13}$.

Si $g(v_0) \notin \langle e_1, e_3, e_4 \rangle$, en appliquant le lemme 2.3, on déduit qu'il existe k tel que $v_1 = T_4^k \circ g(v_0) \in \langle e_1, e_2, e_3 \rangle$ et $v_1 \notin P_{13} \cup P_{24}$. Finalement, quitte à échanger e_2 et e_4 , on peut supposer que $g(v_0) \in \langle e_1, e_2, e_3 \rangle$ et $g(v_0) \notin P_{13} \cup P_{24}$. Il existe une transvection de centre v_0 dans G_2 , donc il existe une transvection de centre $\langle g(v_0) \rangle$. Pour finir, on fait un changement de base symplectique qui laisse stable les centres de T_2 et T_4 et qui envoie $\langle g(v_0) \rangle$ sur $\langle e_2 + e_3 \rangle$ (ce changement de base est possible car $g(v_0)$ est convenablement situé). On peut donc supposer que G contient T_4, T_2 et T_{23} où

$$T_{23} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & -1 \\ 1 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Étape 3. — On montre que G contient une transvection de centre e_1 .

Soit G_2 le sous-groupe de G engendré par les trois transvections déjà déterminée. Ce groupe agit transitivement sur les droites de l'hyperplan $H = \langle e_2, e_3, e_4 \rangle$. Pour le montrer, il suffit de calculer pour $i = 2, 4$, l'image de e_i par $T_{23}^{k_3} \circ T_2^{k_2} \circ T_4^{k_1}$. Le groupe G_2 contient donc toutes les transvections de centre appartenant à H . Le groupe G_2 laisse stable $\langle e_3 \rangle$ et H . Puisque G ne vérifie pas l'assertion 1, il existe $v \in H$ et $g \in G$ tel que $g(v) \notin H$. Le calcul de $T_4^{k_4} \circ T_2^{k_3} \circ T_4^{k_2} \circ T_{23}^{k_1}(e_1)$ montre qu'il existe $\tilde{g} \in G$ tel que $g(v) = \tilde{g}(e_1)$ (l'image de la droite $\langle e_1 \rangle$ par G_2 est l'ensemble des droites n'appartenant pas à H). Le groupe G contient la transvection T_1 :

$$T_1 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Étape 4. — On montre que T_4, T_2, T_{23}, T_1 engendrent $\text{Sp}(4, \mathbb{F}_\ell)$.

On va calculer l'orbite et le stabilisateur de $\langle e_3 \rangle$ par G . Le stabilisateur de $\langle e_3 \rangle$ est au moins égal au sous-groupe G_2 engendré par T_{23}, T_2 et T_4 . Il suffit donc de calculer l'ordre de G_2 . Le sous-groupe G_1 engendré par T_4 et T_2 stabilise e_1 . L'ordre de G_1 est $\ell(\ell^2 - 1)$. De plus, pour tout $\lambda \in \mathbb{F}_\ell^*$, il existe $g \in G_2$ tel que $g(e_1) = \lambda e_1$. L'orbite de $\langle e_1 \rangle$ par G_2 est l'ensemble des droites n'appartenant pas à H . Il y a ℓ^3 droites n'appartenant pas à un hyperplan. L'ordre du stabilisateur de $\langle e_3 \rangle$ est donc au moins égal à $\ell^4(\ell^2 - 1)(\ell - 1)$.

Soit $D = \langle v \rangle$ une droite de V . Dans le cas où cette droite est incluse dans H , on a déjà vu qu'il existe $g \in G$ tel que $g(\langle e_3 \rangle) = D$. Dans

le cas contraire écrivons alors $D = \langle {}^t(1, a_2, a_3, a_4) \rangle$. On applique le lemme 2.4 pour montrer qu'il existe k_1 tel que $T_1^{k_1}(\langle e_3 \rangle) = {}^t\langle (1, 0, a_3, 0) \rangle$. Finalement il existe $g \in G_2$ tel que $g({}^t(1, 0, a_3, 0)) = {}^t(1, a_2, a_3, a_4)$ donc $g \circ T_1^{k_1}(\langle e_3 \rangle) = D$. On en déduit que G_2 agit transitivement sur l'ensemble des droites de V qui est de cardinal $\ell^3 + \ell^2 + \ell + 1$.

L'ordre de $\mathrm{Sp}(4, \mathbb{F}_\ell)$ étant $\ell^4(\ell^4 - 1)(\ell^2 - 1)$, on en déduit que l'on a $G = \mathrm{Sp}(4, \mathbb{F}_\ell)$. \square

On peut donc maintenant écrire les sous-groupes maximaux de $\mathrm{Sp}(4, \mathbb{F}_\ell)$ contenant une transvection.

• Il y a les sous-groupes qui laissent stables un hyperplan $H = \langle e_1, e_3, e_4 \rangle$. Dans une base symplectique formée à partir de $\langle e_1, e_3, e_4 \rangle$ ils s'écrivent :

$$\begin{pmatrix} a_1 & x & a_2 & 0 \\ 0 & k & 0 & 0 \\ a_3 & y & a_4 & 0 \\ a_5 & z & a_6 & k^{-1} \end{pmatrix}$$

où

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in \mathrm{SL}(2, \mathbb{F}_\ell) \quad \text{et} \quad \begin{cases} ka_5 = -a_3x + a_1y, \\ ka_6 = -a_4x + a_2y. \end{cases}$$

Ces groupes sont d'ordre $\ell^4(\ell^2 - 1)(\ell - 1)$.

• Il y a les sous-groupes qui laissent stables un plan P totalement isotrope. Dans une base symplectique obtenue en complétant une base symplectique de P ils s'écrivent :

$$\begin{pmatrix} {}^tA^{-1} & 0 \\ C & A \end{pmatrix} \quad \text{avec} \quad A \in \mathrm{SL}(2, \mathbb{F}_\ell) \quad \text{et} \quad A^tC = C^tA.$$

Ces groupes sont également d'ordre $\ell^4(\ell^2 - 1)(\ell - 1)$.

• Il y a les sous-groupes dont les éléments laissent stables ou échangent deux plans non totalement isotropes orthogonaux supplémentaires. Dans une base symplectique formée à partir de ces deux plans ils s'écrivent :

$$\begin{pmatrix} \star & 0 & \star & 0 \\ 0 & \star & 0 & \star \\ \star & 0 & \star & 0 \\ 0 & \star & 0 & \star \end{pmatrix} \cup \begin{pmatrix} 0 & \star & 0 & \star \\ \star & 0 & \star & 0 \\ 0 & \star & 0 & \star \\ \star & 0 & \star & 0 \end{pmatrix}.$$

Ces groupes sont d'ordre $2\ell^2(\ell^2 - 1)^2$. On remarque que les éléments de ces groupes laissent stables un plan ou ont une trace nulle.

2.3. Résultat principal sur $\mathrm{Sp}(4, \mathbb{F}_\ell)$.

Pour montrer le théorème principal sur $\mathrm{Sp}(4, \mathbb{F}_\ell)$, on a besoin de deux lemmes.

LEMME 2.5. — *Le polynôme caractéristique d'une isométrie symplectique est de la forme $P(X) = X^4 + aX^3 + bX^2 + aX + 1$.*

Démonstration. — C'est une conséquence immédiate de la conservation de la forme alternée. \square

LEMME 2.6. — *Le polynôme $X^4 + bX^2 + 1$, où $b \in \mathbb{F}_\ell$, est réductible sur \mathbb{F}_ℓ .*

Démonstration. — Soit α une racine de ce polynôme; alors $-\alpha$, α^{-1} et $-\alpha^{-1}$ sont aussi des racines. Supposons au contraire que $X^4 + bX^2 + 1$ est irréductible; les racines sont alors conjuguées dans \mathbb{F}_{ℓ^4} et sont donc α , α^ℓ , α^{ℓ^2} , α^{ℓ^3} . Si $\alpha^{-1} = \alpha$, alors $\alpha = \pm 1$ ce qui est exclu. Supposons que $\alpha^{-1} = \alpha^{\ell^3}$; alors $\alpha^{\ell^3+1} = 1$. Or le pgcd de $\ell^3 + 1$ et $\ell^4 - 1$ est $\ell + 1$; on en déduit que $\alpha^{\ell+1} = 1$ et donc $\alpha \in \mathbb{F}_{\ell^2}$, ce qui est une contradiction. Reste le cas où $\alpha^{-1} = \alpha^{\ell^2}$; alors $-\alpha$ ne peut être égal qu'à α^ℓ ou α^{ℓ^3} . Dans les deux cas, compte tenu de $\alpha^{\ell^4-1} = 1$, on a $(\alpha^2)^{\ell-1} = 1$ donc $\alpha^2 \in \mathbb{F}_\ell$; autrement dit, $\alpha \in \mathbb{F}_{\ell^2}$ ce qui est exclu. \square

THÉORÈME 2.7. — *Une transvection et un élément dont le polynôme caractéristique est irréductible engendrent $\mathrm{Sp}(4, \mathbb{F}_\ell)$.*

Soit H le sous-groupe engendré par ces deux éléments et supposons que H est différent de $\mathrm{Sp}(4, \mathbb{F}_\ell)$. On peut appliquer le théorème 2.2. Le groupe H contient un élément dont le polynôme caractéristique est irréductible, donc il ne laisse stable aucun sous-espace de V . Les éléments de H qui ne laissent pas stables un sous-espace vectoriel échangent deux plans supplémentaires orthogonaux non totalement isotopes. Leur trace est nulle et grâce au lemme 2.6, leur polynôme caractéristique est réductible. \square

On en déduit grâce à la proposition 1.3 le résultat suivant :

COROLLAIRE 2.8. — *Soit J une variété abélienne sur K de dimension 2 dont la réduction \tilde{J}_v en v est une extension d'une courbe elliptique par un tore de dimension 1. Soit ℓ un nombre premier différent de la caractéristique de k_v et qui ne divise pas $(\tilde{J}_v : \tilde{J}_v^0)$. Si $\mathrm{Im}(\rho_\ell)$ contient une isométrie symplectique dont le polynôme caractéristique est irréductible, alors $\mathrm{Im}(\rho_\ell)$ contient $\mathrm{Sp}(4, \mathbb{F}_\ell)$.*

REMARQUE 1. — Le théorème 2.7 ne se généralise pas de manière immédiate à $\mathrm{Sp}(2g, \mathbb{F}_\ell)$ pour $g \geq 3$. Par exemple, soit H le sous-groupe de $\mathrm{Sp}(6, \mathbb{F}_\ell)$ formé des éléments qui laissent stables ou permutent trois plans totalement isotropes supplémentaires. Le groupe H contient des transvections et des éléments dont le polynôme caractéristique est irréductible.

REMARQUE 2. — Il y a des sous-groupes de $\mathrm{Sp}(4, \mathbb{F}_\ell)$ qui contiennent des éléments d'ordre ℓ et des éléments dont le polynôme caractéristique est irréductible. Par exemple, $\mathrm{SL}(2, \mathbb{F}_{\ell^2})$ se plonge dans $\mathrm{Sp}(4, \mathbb{F}_\ell)$ et l'image contient une transvection et un élément dont le polynôme caractéristique est irréductible.

3. Éléments de Frobenius

Plaçons-nous dans le cas où $K = \mathbb{Q}$ et J est la jacobienne d'une courbe C de genre 2 définie sur \mathbb{Q} . Soit q un nombre premier de bonne réduction et \bar{q} une extension de q à $\overline{\mathbb{Q}}$. On désigne par $I_{\bar{q}}$ et $D_{\bar{q}}$ les groupes d'inertie et de décomposition relatif à \bar{q} . Lorsque J a bonne réduction en q , on sait que si ℓ est différent de q , alors $\rho_\ell(I_{\bar{q}}) = \{1\}$ (cf. § 1). On note $\mathcal{F}_{\bar{q}}$ l'élément de Frobenius. La classe de conjugaison de l'image de $\mathcal{F}_{\bar{q}}$ par ρ_ℓ ne dépend que de q et de ℓ . Soit $T_\ell(J) = \varprojlim_{\nu} J_{\ell^\nu}$ le module de Tate et ρ_{ℓ^∞} la représentation galoisienne attachée. On note respectivement $P_{q,\ell}^\infty(X)$ et $P_{q,\ell}(X)$ les polynômes caractéristiques de $\rho_{\ell^\infty}(\mathcal{F}_{\bar{q}})$ et de $\rho_\ell(\mathcal{F}_{\bar{q}})$. Il est bien connu que les coefficients de $\rho_{\ell^\infty}(\mathcal{F}_{\bar{q}})$ sont indépendants de ℓ . Plus précisément (cf. [CF, p. 80]) :

THÉORÈME 3.1. — *Pour $n \geq 1$, soit N_n le nombre de points de C sur le corps \mathbb{F}_{q^n} . On a :*

$$P_{q,\ell}^\infty(X) = X^4 - tX^3 + sX^2 - qtX + q^2,$$

où

$$t = q + 1 - N_1 \quad \text{et} \quad s = \frac{1}{2}(N_1^2 + N_2) + q - (q + 1)N_1;$$

en particulier, $P_{q,\ell}^\infty(X) \in \mathbb{Z}[X]$. \square

On obtient les coefficients de $P_{q,\ell}(X)$ en réduisant modulo ℓ ceux de $P_{q,\ell}^\infty(X) \in \mathbb{Z}[X]$. Supposons déterminé un nombre premier q tel que $P_{q,\ell}^\infty(X)$ est irréductible. On peut alors déterminer les ℓ pour lesquels $P_{q,\ell}^\infty(X)$ modulo ℓ demeure irréductible. Le groupe de Galois de $P_{q,\ell}^\infty(X)$ est un sous-groupe de D_4 et lui est égal le plus souvent.

PROPOSITION 3.2. — *Soit*

$$P(X) = X^4 + aX^3 + bX^2 + aqX + q^2$$

un polynôme irréductible de $\mathbb{Z}[X]$ tel que le groupe de Galois de P est D_4 . On note

$$Q(X) = X^2 + aX + (b - 2q)$$

et Δ_P, Δ_Q les discriminants de ces deux polynômes. Si ℓ est un nombre premier qui vérifie $\left(\frac{\Delta_P}{\ell}\right) = -1$ et $\left(\frac{\Delta_Q}{\ell}\right) = -1$, alors la réduction de P modulo ℓ est irréductible sur \mathbb{F}_ℓ .

Démonstration. — Il suffit d'appliquer le théorème de Stickelberger (cf. [C, p. 288]). \square

L'image d'un élément de Frobenius par ρ_ℓ est un élément de $\mathrm{GSp}(4, \mathbb{F}_\ell)$. Cependant, pour appliquer les résultats du § 2, on voudrait obtenir un élément de $\mathrm{Sp}(4, \mathbb{F}_\ell)$. Pour cela, considérons l'image de $\mathcal{F}_{\tilde{q}}^{\ell-1}$ par ρ_ℓ . Il est nécessaire de pouvoir contrôler l'irréductibilité de son polynôme caractéristique que l'on note $P_{q,\ell}^{(\ell-1)}(X)$.

LEMME 3.3. — *Lorsque $P_{q,\ell}(X)$ est irréductible sur \mathbb{F}_ℓ , $P_{q,\ell}^{(\ell-1)}(X)$ est irréductible sur \mathbb{F}_ℓ .*

Démonstration. — Supposons au contraire que $P_{q,\ell}^{(\ell-1)}(X)$ est réductible. Soit $\alpha \in \overline{\mathbb{F}}_\ell$ une racine de $P_{q,\ell}(X)$ de sorte que $\alpha^{\ell-1}$ est une racine de $P_{q,\ell}^{(\ell-1)}(X)$. Alors $\alpha^{\ell-1} \in \mathbb{F}_{\ell^2}^*$ et donc $\alpha^{(\ell-1)(\ell^2-1)} = 1$. Notons \tilde{q} la classe de q modulo ℓ . Les racines de $P_{q,\ell}(X)$ dans $\overline{\mathbb{F}}_\ell$ sont de la forme $\alpha, \tilde{q}/\alpha, \beta, \tilde{q}/\beta$. Ces racines sont conjuguées et $P_{q,\ell}(X)$ est supposé irréductible. On a alors $\alpha^{\ell^2} = \tilde{q}/\alpha$.

En effet si, par exemple, $\tilde{q}/\alpha = \alpha^\ell$, on a $\alpha^{\ell^2-1} = 1$ et donc $\alpha \in \mathbb{F}_{\ell^2}$, ce qui n'est pas possible. Les autres cas sont semblables. On a donc $\alpha^{(\ell-1)(\ell^2+1)} = 1$ dont on déduit que $\alpha^{2(\ell-1)} = 1$ et donc que $\alpha^2 \in \mathbb{F}_\ell$ et $\alpha \in \mathbb{F}_{\ell^2}$ ce qui est une contradiction. \square

4. Applications aux jacobiniennes de courbes de genre 2

Dans cette partie on applique les résultats obtenus précédemment aux jacobiniennes J de courbes C de genre 2 définie sur \mathbb{Q} ayant un certain type de réduction stable. Il faut donc relier les types de réduction stable de la courbe et la fibre spéciale du modèle de Néron de J . On garde les notations du § 1. On note \mathcal{X} le modèle minimal régulier de C sur $\mathrm{Spec}(O_v)$ et $\tilde{\mathcal{X}}$ sa fibre spéciale. On sait [BLR, § 9.5, th. 4] que :

$$\tilde{J}_v^0 = \mathrm{Pic}_{\tilde{\mathcal{X}}/k_v}^0.$$

En suivant les notations de [Liu], on dira qu'une courbe de genre 2 a une réduction stable de type (II) si la fibre spéciale géométrique est une courbe de genre 1 avec un point double ordinaire. La réduction est de type (VI) si la fibre spéciale géométrique est composée d'une courbe elliptique et d'une courbe de genre 0 avec un point double ordinaire.

LEMME 4.1 (cf. [BLR, exemple 8, p. 246]). — Soit C une courbe de genre 2 dont la réduction stable en v est de type (II) ou (VI). La composante connexe contenant l'élément neutre de la fibre spéciale du modèle de Néron de J est alors une extension d'une courbe elliptique par un tore.

Démonstration. — La courbe C est semi-stable au sens de [BLR]. Notons $\tilde{\mathcal{X}}_n$ la normalisation de $\tilde{\mathcal{X}}$. Il suffit de vérifier que $\text{Pic}_{\tilde{\mathcal{X}}_n/k_v}^0$ est une variété abélienne de dimension 1. \square

Considérons enfin le diagramme commutatif suivant :

$$\begin{array}{ccccccc}
 1 & \rightarrow & \text{Gal}(\mathbb{Q}(J_\ell)/\mathbb{Q}(\mu_\ell)) & \rightarrow & \text{Gal}(\mathbb{Q}(J_\ell)/\mathbb{Q}) & \rightarrow & \text{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q}) \rightarrow 1 \\
 & & \downarrow \tilde{\rho}_\ell & & \downarrow \rho_\ell & & \downarrow \wr \\
 1 & \longrightarrow & \text{Sp}(4, \mathbb{F}_\ell) & \longrightarrow & \text{GSp}(4, \mathbb{F}_\ell) & \longrightarrow & (\mathbb{Z}/\ell\mathbb{Z})^* \longrightarrow 1.
 \end{array}$$

On en déduit que, si $\tilde{\rho}_\ell$ est surjectif, ρ_ℓ l'est aussi. On peut alors résumer les différents résultats obtenus dans le théorème suivant :

THÉORÈME 4.2. — Soit (C) une courbe de genre 2 définie sur \mathbb{Q} ayant une réduction de type (II) ou (VI) en un nombre premier p . Soit c l'ordre du groupe des composantes connexes de la fibre spéciale du modèle de Néron en p . On suppose qu'il existe un nombre premier q de bonne réduction tel que le groupe de Galois du corps des racines $P_{q,\ell}(X)$ est le groupe diédral à 8 éléments D_4 . Posons

$$\begin{aligned}
 P_{q,\ell}(X) &= X^4 + aX^3 + bX^2 + aqX + q^2, \\
 Q_{q,\ell}(X) &= X^2 + aX + (b - 2q),
 \end{aligned}$$

et soient Δ_P, Δ_Q , les discriminants de ces polynômes. Soit ℓ un nombre premier qui ne divise pas $2pqc$ et tel que :

$$\left(\frac{\Delta_P}{\ell}\right) = -1 \quad \text{et} \quad \left(\frac{\Delta_Q}{\ell}\right) = -1.$$

Alors l'image de ρ_ℓ est $\text{GSp}(4, \mathbb{F}_\ell)$. En particulier, il existe une infinité de nombres premiers vérifiant cette propriété.

On donne deux exemples qui illustrent le théorème précédent. Les calculs numériques ont été effectués en utilisant le système PARI.

EXEMPLE 1. — On considère la courbe d'équation

$$y^2 = x^5 - x + 1$$

définie sur \mathbb{Q} qui a réduction de type (II) en $p = 19$ et $p = 151$. Les deux groupes de composantes du modèle de Néron en $p = 19$ et $p = 151$ sont d'ordre 1. On en déduit que pour tout ℓ impair il existe un élément d'ordre ℓ qui est une transvection. On calcule par exemple le polynôme caractéristique de l'élément de Frobenius en $p = 11$:

$$P_{F_{11}}(X) = X^4 + 8X^3 + 39X^2 + 88X + 121.$$

Il est irréductible sur \mathbb{Z} de groupe de Galois D_4 . On a :

$$\Delta_P = 2^4 \cdot 5 \cdot 11^2 \cdot 181 \quad \text{et} \quad \Delta_Q = 2^2 \cdot 3 \cdot 11.$$

On obtient donc un premier type de résultat : si $\left(\frac{905}{\ell}\right) = -1$ et $\left(\frac{33}{\ell}\right) = -1$ et ℓ est différent de 2 et de 11, alors

$$\text{Im}(\rho_\ell) = \text{GSp}(4, \mathbb{F}_\ell).$$

En calculant plusieurs polynômes caractéristiques d'éléments de Frobenius et en appliquant plusieurs fois le théorème 4.2, on déduit que pour $2 < \ell < 500\,000$ on a $\text{Im}(\rho_\ell) = \text{GSp}(4, \mathbb{F}_\ell)$.

On traite le cas $\ell = 2$ à part. Le groupe de Galois de $X^5 - X + 1$ étant S_5 , on en déduit que l'image de ρ_2 est S_5 .

EXEMPLE 2. — On considère la courbe C_{29} d'équation

$$y^2 = (2x - 1)(2x^5 - x^4 - 4x^2 + 8x - 4)$$

donnée dans [Le] qui possède un point rationnel d'ordre 29. La courbe admet une réduction stable de type (II) dans \mathbb{Q}_{61} . Le cardinal du groupe des composantes connexes du modèle de Néron est 1. On calcule $P_{q,\ell}(X)$ en $q = 3$:

$$P_{F_3}(X) = X^4 + 3X^3 + 7X^2 + 9X + 9.$$

En appliquant le théorème 4.2, on trouve que pour $\ell \neq 2, 3, 61$ vérifiant

$$\left(\frac{61}{\ell}\right) = -1 \quad \text{et} \quad \left(\frac{5}{\ell}\right) = -1,$$

l'image de ρ_ℓ est $\text{GSp}(4, \mathbb{F}_\ell)$. Si on calcule 40 polynômes caractéristiques d'éléments de Frobenius, on montre que, si ℓ est un nombre premier inférieur à 500 000, différent de 2, 29, 61, ρ_ℓ est surjective.

Pour $\ell = 29$, on sait *a priori* que $\text{Im } \rho_{29}$ est incluse dans le sous-groupe Γ de $\text{GSp}(4, \mathbb{F}_{29})$ laissant stable le vecteur correspondant au point rationnel d'ordre 29. On en déduit que :

$$\text{Im } \rho_{29} \subset \Gamma = \left\{ \begin{pmatrix} a_1 & x & a_2 & 0 \\ 0 & k & 0 & 0 \\ a_3 & y & a_4 & 0 \\ a_5 & z & a_6 & 1 \end{pmatrix} ; M = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in \text{GL}(2, \mathbb{F}_{29}), \right. \\ \left. \begin{cases} ka_5 = -a_3x + a_1y, \\ ka_6 = -a_4x + a_2y, \end{cases} \text{ et } \det(M) = k \right\}.$$

PROPOSITION 4.3. — *L'image de ρ_{29} est le groupe Γ dont l'ordre est $29^4(29 - 1)(29^2 - 1)$.*

Démonstration. — On considère p le morphisme de groupes :

$$p : \quad \Gamma \quad \longrightarrow \quad \text{GL}(2, \mathbb{F}_{29}),$$

$$\begin{pmatrix} a_1 & x & a_2 & 0 \\ 0 & k & 0 & 0 \\ a_3 & y & a_4 & 0 \\ a_5 & z & a_6 & 1 \end{pmatrix} \quad \longmapsto \quad \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}.$$

Le noyau de p , noté N , est un groupe d'ordre 29^3 qui est isomorphe à un produit semi-direct de $\mathbb{Z}/29\mathbb{Z}$ par $(\mathbb{Z}/29\mathbb{Z})^2$. Notons $M(x, y, z)$ les éléments de ce groupe. La loi de groupe s'écrit :

$$M(x, y, z) \star M(x', y', z') = M(x + x', y + y', z + z' + yx' - xy').$$

On a donc la suite exacte suivante :

$$1 \rightarrow N \rightarrow \Gamma \xrightarrow{p} \text{GL}(2, \mathbb{F}_{29}) \rightarrow 1.$$

Notons $\tilde{\Gamma} = \text{Im } \rho_{29}$. Le calcul de quelques polynômes caractéristiques d'éléments de Frobenius montre que $p|_{\tilde{\Gamma}}$ est surjective. Soit \tilde{N} le noyau de $p|_{\tilde{\Gamma}}$, de sorte que l'on a la suite exacte :

$$1 \rightarrow \tilde{N} \rightarrow \tilde{\Gamma} \xrightarrow{p} \text{GL}(2, \mathbb{F}_{29}) \rightarrow 1.$$

Le groupe \tilde{N} est un sous-groupe de N qui est distingué dans $\tilde{\Gamma}$. Les trois seuls sous-groupes possibles (c'est-à-dire compatible avec la surjectivité de $p|_{\tilde{\Gamma}}$) sont :

$$\{\text{Id}\}, \left\langle \left(\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \right) \right\rangle, N.$$

De plus, le polynôme caractéristique de l'élément de Frobenius en $q = 8527$ (qui est congru à 1 modulo 29) est $(X - 1)^4$ et le nombre de points de la réduction de la jacobienne en $q = 29$ n'est pas divisible par 29^2 . On en déduit que $\text{Im } \rho_{29}$ n'est pas incluse dans le sous-groupe H défini par :

$$H = \left\{ \left(\begin{array}{cccc} a_1 & 0 & a_2 & 0 \\ 0 & k & 0 & 0 \\ a_3 & 0 & a_4 & 0 \\ 0 & z & 0 & 1 \end{array} \right) ; M = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in \text{GL}(2, \mathbb{F}_{29}), \right. \\ \left. z, k \in \mathbb{F}_{29}^* \det(M) = k \right\}.$$

Le noyau de $p|\tilde{\Gamma}$ est donc N ; le groupe $\tilde{\Gamma}$ est égal à Γ . \square

Pour $\ell = 2$, on trouve que $\text{Im } \rho_2 = S_5$.

BIBLIOGRAPHIE

- [A] ARTIN (E.). — *Algèbre géométrique*. — Cahiers Scientifiques XXVII, Gauthiers Villars.
- [As] ASCHBACHER (M.). — *On the maximal subgroups of the finite classical groups*, Invent. Math., t. **76**, 1984, p. 469–514.
- [BLR] BOSCH (S.), LÜTKEBOHMERT (W.), M Raynaud (M.). — *Néron Models*. — Springer Verlag, 1990.
- [CF] CASSELS (J.W.S.), FLYNN (E.V.). — *Prolegomena to a middlebrow arithmetic of curves of genus 2*, L.M.S. Lecture Note Series, Cambridge University Press, t. **230**, 1996.
- [C] CHILDS (L.). — *A concrete introduction to higher algebra*. — Springer Verlag, 1979.
- [Le] LEPRÉVOST (F.). — *Jacobienues de certaines courbes de genre 2 : torsion et simplicité*, J. théorie des nombres de Bordeaux, t. **7**, 1995, p. 283–306.
- [LD1] LE DUFF (P.). — *Points d'ordre ℓ des jacobienues de certaines courbes de genre 2*, C. R. Acad. Sci. Paris, Série I t. **325**, 1997, p. 243–246.
- [LD2] LE DUFF (P.). — *Thèse*, Université de Caen, 1997; C. R. Acad. Sci. Paris, Série I t. **325**, 1997, p. 243–246.
- [Liu] LIU (Q.). — *Courbes stables de genre 2 et leur schéma de modules*, Math. Annalen, t. **295**, 1993, p. 201–222.

- [KL] KLEIDMAN (P.), LIEBECK (M.). — *The subgroups structure of the finite classical groups*, L.M.S. Lecture Note Series, Cambridge University Press, t. **129**, 1990.
- [MW] MASSER (D.), WÜSTHOLZ (G.). — *Galois properties of division fields of elliptic curves*, Bull. London Math. Soc., t. **25**, 1993, p. 247–254.
- [M] MITCHELL (H.). — *The subgroups of the quaternary abelian linear group*, Trans. Amer. Math. Soc., t. **15**, 1914, p. 379–396.
- [R] RIBET (K.). — *Galois action on division points of abelian varieties with real multiplications*, Amer. J. of Math., t. **98**, n° 3, 1976, p. 751–804.
- [ST] SERRE (J.-P.), TATE (J.). — *Good reduction of abelian varieties*, Ann. of Math., t. **88**, 1968, p. 492–516.
- [S1] SERRE (J.-P.). — *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math., t. **15**, 1972, p. 259–331.
- [S2] SERRE (J.-P.). — *Résumé de cours*. — Annuaire du Collège de France, 1985–1986.