ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 30, Number 3, Fall 2000

GALOIS REPRESENTATIONS ATTACHED TO THE PRODUCT OF TWO ELLIPTIC CURVES

AMADEU REVERTER AND NÚRIA VILA

ABSTRACT. We study the images of mod p Galois representations attached to the abelian variety product of two elliptic curves. The case of two nonisogenous elliptic curves without complex multiplication has been considered by Serre [**3**]. In this paper we examine the case of two isogenous elliptic curves.

Let E_1, E_2 be two elliptic curves defined over a number field K. Let p be a prime number, and let $E_1[p]$ and $E_2[p]$ denote the group of p-torsion points of E_1 and E_2. The action of the absolute Galois group G_K of K on the p-torsion points of E_1 and E_2 defines the Galois representations

$$\rho_{E_1,p} : G_K \longrightarrow \mathrm{Aut}\,(E_1[p]), \quad \rho_{E_2,p} : G_K \longrightarrow \mathrm{Aut}\,(E_2[p])$$

and the homomorphism

$$\psi_p : G_K \longrightarrow \mathrm{Aut}\,(E_1[p]) \times \mathrm{Aut}\,(E_2[p]).$$

Let us denote

$$M_p := \{(s, s') \in \mathrm{Aut}\,(E_1[p]) \times \mathrm{Aut}\,(E_2[p]) : \det s = \det s'\}.$$

Let χ_p be the mod p cyclotomic character. We have that $\det \rho_{E_1,p} = \det \rho_{E_2,p} = \chi_p$, by the Weil pairing. Then the image $\psi_p(G_K)$ is contained in M_p.

Serre [**3**] studies the image $\psi_p(G_K)$ whenever the elliptic curves are without complex multiplication and not $\overline{K}$-isogenous. Using Falting's results [**2**] on the Tate conjecture, we have

Received by the editors on April 5, 1999, and in revised form on May 11, 1999.
This research has been partially supported by DGES grant PB96-0970-C02-01.

Theorem [**3**]. *Let E_1/K and E_2/K be two elliptic curves without complex multiplication and nonisogenous. Then $\psi_p(G_K) = M_p$, for all but finitely many primes p.*

From now on we will consider elliptic curves defined over K and K-isogenous. First we need some results concerning the relationship between the image of mod p Galois representation attached to elliptic curves, K-isogenies and p-torsion points.

1. Images and isogenies. Let K be a number field and let E/K be an elliptic curve defined over K. Let p be a prime number, and let χ_p be the mod p cyclotomic character. Let $\rho_{E,p}$ be the mod p Galois representation associated to the p-torsion points $E[p]$ of the elliptic curve E. Observe that the elliptic curve E/K admits an isogeny of degree p defined over K if and only if the image $\rho_{E,p}(G_K)$ is contained in a Borel subgroup. If E_1/K and E_2/K are related by an isogeny defined over K of degree prime to p, then this isogeny induces a G_K-module isomorphism from $E_1[p]$ to $E_2[p]$, which identifies the images $\rho_{E_1,p}(G_K)$ and $\rho_{E_2,p}(G_K)$. Moreover, we have

Lemma 1.1. *Let E_1/K and E_2/K be two elliptic curves and $\phi : E_1 \to E_2$ be a K-isogeny of degree p. Then the following conditions are equivalent*:

(i) *There exists a one-dimensional G_K-stable subspace of $E_1[p]$ not annihilated by ϕ.*

(ii) *$\rho_{E_1,p}(G_K)$ is contained in a split Cartan subgroup of* $\mathrm{Aut}\,(E_1[p])$.

(iii) *There exists an elliptic curve E_3/K non-K-isomorphic to E_2 and a K-isogeny $\phi' : E_1 \to E_3$ of degree p.*

Lemma 1.2. *Let E/K be an elliptic curve with nontrivial p-torsion points defined over K. Then a basis of $E[p]$ exists such that*

$$\rho_{p,E}(G_K) = \begin{cases} \begin{pmatrix} 1 & * \\ 0 & \chi_p(G_K) \end{pmatrix} & \textit{if } E \textit{ has only one } K\textit{-isogeny} \\ & \textit{of degree } p, \\ \begin{pmatrix} 1 & 0 \\ 0 & \chi_p(G_K) \end{pmatrix} & \textit{otherwise.} \end{cases}$$

Proof. Let $P \in E(K)[p]\backslash\{0\}$ and $Q \in E[p]$ such that $\{P, Q\}$ is an $\mathbf{F}_p$-basis of $E[p]$. Let $\sigma_0 \in G_K$ such that $P^{\sigma_0} = P$, $Q^{\sigma_0} = c_{\sigma_0}P + d_{\sigma_0}Q$ and d_{σ_0} generate the cyclic group $\det \rho_{E,p}(G_K) = \chi_p(G_K) \subseteq \mathbf{F}_p^*$. If $d_{\sigma_0} \neq 1$, take $\{P, Q'\}$ as a basis, where $Q' = c_{\sigma_0}P + (d_{\sigma_0} - 1)Q$. Then

$$\begin{pmatrix} 1 & 0 \\ 0 & \chi_p(G_K) \end{pmatrix} \subseteq \rho_{E,p}(G_K) \subseteq \begin{pmatrix} 1 & * \\ 0 & \chi_p(G_K) \end{pmatrix}.$$

Therefore, using Lemma 1.1 we obtain the result. □

Lemma 1.3. *Let E_1/K and E_2/K be two elliptic curves, and let $\phi : E_1 \to E_2$ be a K-isogeny of degree p. Assume that,*

(i) $\chi_p(G_K) \neq \{1\}$.

(ii) *E_1 and E_2 have nontrivial K defined p-torsion points.*

(iii) *The image $\rho_{E_1,p}(G_K)$ is conjugate to $\left(\begin{smallmatrix} 1 & * \\ 0 & \chi_p(G_K) \end{smallmatrix}\right)$.*

Then the image $\rho_{E_2,p}(G_K)$ is conjugate to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \chi_p(G_K) \end{smallmatrix}\right)$.

Proof. $\phi(E_1[p])$ is a G_K-stable line in $E_2[p]$ on which G_K acts via χ_p, and $E_2[p]$ also contains a G_K-stable line on which G_K acts trivially, by assumption (ii). The result follows from (i). □

Lemma 1.4. *Let E_1/K and E_2/K be two elliptic curves and $\phi : E_1 \to E_2$ be a K-isogeny of degree $p \neq 2$. Assume that $E_2(K)[p] = \{0\}$. Then the curve E_1 has nontrivial K-rational p-torsion points if and only if $\rho_{E_2,p}(G_K)$ is conjugate to $\left(\begin{smallmatrix} \chi_p(G_K) & * \\ 0 & 1 \end{smallmatrix}\right)$.*

Proof. Assume that $E_1(K)[p] \neq \{0\}$. $\phi(E_1[p])$ is a G_K-stable line in $E_2[p]$ on which G_K acts via χ_p. As in Lemma 1.2, we see that there exists a basis of $E_2[p]$ such that $\rho_{E_2,p}(G_K) = \left(\begin{smallmatrix} \chi_p(G_K) & * \\ 0 & 1 \end{smallmatrix}\right)$. Conversely, by Lemma 1.1, $\hat{\phi}(E_2[p])$ is a G_K-stable line in $E_1[p]$ on which G_K acts trivially, where $\hat{\phi}$ is the dual isogeny to ϕ. □

Definition. Let E/K be an elliptic curve and let $p \neq 2$ be a prime number. We will say that E is a p-exceptional elliptic curve over K if it satisfies the following conditions:

(i) The elliptic curve E has no nontrivial K-rational p-torsion points.

(ii) There exist an elliptic curve E'/K and a K-isogeny $\phi : E \to E'$ of degree p.

(iii) Every elliptic curve E' K-isogenous to E with isogeny of degree p has no nontrivial K-rational p-torsion points.

We remark that, from the 722 elliptic curves without complex multiplication listed in the Antwerp tables [**1**], only 39 are 3-exceptional over $\mathbf{Q}$, 27 are 5-exceptional over $\mathbf{Q}$, 8 are 7-exceptional over $\mathbf{Q}$, 4 are 11-exceptional over $\mathbf{Q}$ and 4 are 13-exceptional over $\mathbf{Q}$; if $p > 13$, all elliptic curves are non-p-exceptional over $\mathbf{Q}$. More precisely, the p-exceptional elliptic curves over $\mathbf{Q}$ without complex multiplication, with conductor less than or equal to 200 are:

$$\begin{aligned}
p = \ 3 :\ & 50A,\ 50B,\ 50C,\ 50D;\ 80A,\ 80B,\ 80C,\ 80D;\\
& 98A,\ 98B,\ 98C,\ 98D,\ 98E,\ 98F;\ 100A,\ 100B,\ 100C,\ 100D;\\
& 112E,\ 112F,\ 112G,\ 112H,\ 112I,\ 112J;\\
& 150I,\ 150J,\ 150K,\ 150L,\ 150M,\ 150N,\ 150O,\ 150P;\\
& 175C,\ 175D,\ 175E;\ 176A,\ 176B;\ 196A,\ 196B\\
p = \ 5 :\ & 50E,\ 50F,\ 50G,\ 50H;\ 75A,\ 75B;\\
& 99C,\ 99D,\ 99E;\ 121A,\ 121B,\ 121C;\\
& 150E,\ 150F,\ 150G,\ 150H;\ 171I,\ 171J;\\
& 175F,\ 175G;\ 176D,\ 176E,\ 176F;\ 198Q,\ 198R,\ 198S,\ 198T\\
p = \ 7 :\ & 162A,\ 162B,\ 162C,\ 162D,\ 162G,\ 162H,\ 162I,\ 162J\\
p = 11 :\ & 121F,\ 121G,\ 121H,\ 121I\\
p = 13 :\ & 147A,\ 147B,\ 147I,\ 147J.
\end{aligned}$$

Using Lemmas 1.2 and 1.4 we can give the images of the mod p Galois representation attached to non-p-exceptional elliptic curves which admit a K-isogeny of degree p.

Lemma 1.5. *Let E/K be a non-p-exceptional elliptic curve over K. Assume that E admits a K-isogeny of degree p, then*

(i) *If $E(K)[p] \neq \{0\}$ and E admits only one K-isogeny of degree p,* *then there exists a basis of* $E[p]$ *such that*

$$\rho_{E,p}(G_K) = \begin{pmatrix} 1 & * \\ 0 & \chi_p(G_K) \end{pmatrix}.$$

(ii) *If* $E(K)[p] \neq \{0\}$ *and* E *admits more than one* K*-isogeny of degree* p*, then there exists a basis of* $E[p]$ *such that*

$$\rho_{E,p}(G_K) = \begin{pmatrix} 1 & 0 \\ 0 & \chi_p(G_K) \end{pmatrix}.$$

(iii) *If* $E(K)[p] = \{0\}$*, then there exists a basis of* $E[p]$ *such that*

$$\rho_{E,p}(G_K) = \begin{pmatrix} \chi_p(G_K) & * \\ 0 & 1 \end{pmatrix}.$$

2. Product of two K-isogenous elliptic curves. Let E_1 and E_2 be two elliptic curves defined over K and K-isogenous. If we fix a basis of $E_1[p]$ and a basis of $E_2[p]$, we can identify $\mathrm{Aut}\,(E_1[p])$ and $\mathrm{Aut}\,(E_2[p])$ with $\mathrm{GL}_2(\mathbf{F}_p)$, and $\mathrm{Aut}\,(E_1[p] \times E_2[p])$ with $\mathrm{GL}_4(\mathbf{F}_p)$. We have a natural injection $\mathrm{Aut}\,(E_1[p]) \times \mathrm{Aut}\,(E_2[p]) \hookrightarrow \mathrm{Aut}\,(E_1[p] \times E_2[p])$.

We consider the homomorphism

$$\psi_p : G_K \longrightarrow \mathrm{Aut}\,(E_1[p]) \times \mathrm{Aut}\,(E_2[p]).$$

We remark that, in the case of K-isogenous elliptic curves, we have a strict inclusion $\psi_p(G_K) \subset M_p$ for all prime numbers p not dividing the degree of the isogeny. In fact we have $\psi_p(G_K) = \{(s,s) \in M_p : s \in \rho_{E_1,p}(G_K)\}$ in this case.

Let us denote $N_p := M_p \cap (\rho_{E_1,p}(G_K) \times \rho_{E_2,p}(G_K))$. Clearly, we have that the image $\psi_p(G_K) \subseteq N_p$.

Theorem 2.1. *Let* E_1/K *and* E_2/K *be two elliptic curves. Let* p *be a prime number, and let* $\phi : E_1 \to E_2$ *be a* K*-isogeny of degree* p*.*

Suppose that the pth cyclotomic character χ_p over K is nontrivial and that E_1 is a non-p-exceptional elliptic curve, then $\psi_p(G_K) = N_p$.

Proof. By Lemmas 1.5, 1.2, 1.3 and 1.4, we can find a basis of $E_1[p] \times E_2[p]$ such that N_p has, matricially, one of the following expressions:

$$\text{(i)} \left\{ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & d & 0 & 0 \\ 0 & 0 & 1 & c \\ 0 & 0 & 0 & d \end{pmatrix} \right\}_{\substack{d \in \chi_p(G_K) \\ c \in \mathbf{F}_p}} \qquad \text{(ii)} \left\{ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & d & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & d \end{pmatrix} \right\}_{d \in \chi_p(G_K)}$$

$$\text{(iii)} \left\{ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & d & 0 & 0 \\ 0 & 0 & d & c \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\}_{\substack{d \in \chi_p(G_K) \\ c \in \mathbf{F}_p}} \qquad \text{(iv)} \left\{ \begin{pmatrix} a & c & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & c' \\ 0 & 0 & 0 & a \end{pmatrix} \right\}_{\substack{a \in \chi_p(G_K) \\ c \in \mathbf{F}_p \\ c' \in \mathbf{F}_p}}.$$

In cases (i), (ii) and (iii), if $(s, s') \in N_p$, let $\sigma \in G_K$ such that $s' = \rho_{E_2,p}(\sigma)$. Since $\det s = \det s'$, then $\rho_{E_1,p}(\sigma) = s$ and $(s, s') = \psi_p(\sigma) \in \psi_p(G_K)$.

In case (iv), if $(s, s') \in N_p$, with $s = \left(\begin{smallmatrix} a & c \\ 0 & 1 \end{smallmatrix}\right)$ and $s' = \left(\begin{smallmatrix} 1 & c' \\ 0 & a \end{smallmatrix}\right)$, let $\sigma \in G_K$ such that $\rho_{E_1,p}(\sigma) = s$. Then $\rho_{E_2,p}(\sigma) = \left(\begin{smallmatrix} 1 & c_\sigma \\ 0 & a \end{smallmatrix}\right)$. There exists $\sigma'' \in G_K$ such that $\rho_{E_2,p}(\sigma'') = \left(\begin{smallmatrix} 1 & c' - c_\sigma \\ 0 & 1 \end{smallmatrix}\right)$ and $\rho_{E_1,p}(\sigma'') = \mathrm{id}$. Therefore, $(s, s') = \psi_p(\sigma) \circ \psi_p(\sigma'') = \psi_p(\sigma \circ \sigma'') \in \psi_p(G_K)$.

Remark. In the case of p-exceptional elliptic curves, we have a strict inclusion $\psi_p(G_K) \subset N_p$. Let $\phi : E_1 \to E_2$ be a K-isogeny of degree p. Let $\varphi_1^{E_1}$ and $\varphi_2^{E_1}$, respectively $\varphi_1^{E_2}$ and $\varphi_2^{E_2}$, be the two characters $G_K \to \mathbf{F}_p^*$, giving the action of G_K on the stable line L and on the quotient $E_1[p]/L$, respectively on $\phi(L)$ and $E_2[p]/\phi(L)$. Then $\varphi_1^{E_1} = \varphi_2^{E_2}$ and $\varphi_2^{E_1} = \varphi_1^{E_2}$, which are nontrivial, since E_1 and E_2 are p-exceptional.

REFERENCES

1. B. Birch and W. Kuyk (eds.), *Modular functions of one variable* IV, Lecture Notes in Math. **476**, Springer-Verlag, New York, 1972.

2. G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.

3. J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

4. J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Math. 106, Springer-Verlag, New York, 1986.

Seminari de Matemàtiques, I.B. Bellvitge., Avda. Amèrica, 99, E-08907 L'Hospitalet de Llobregat, Spain
E-mail address: areverte@pie.xtec.es

Departament d'Àlgebra i Geometria, Facultat de Matemàtiques, Universitat de Barcelona, Gran Via de les Corts Catalanes, 585, E-08007 Barcelona, Spain
E-mail address: vila@cerber.mat.ub.es