Artin representations attached to pairs of isogenous abelian varieties

Francesc Fité

December 16, 2010

Abstract

Given a pair of abelian varieties defined over a number field k and isogenous over a finite Galois extension L/k, we define a rational Artin representation of the group $\mathrm{Gal}(L/k)$ that shows a global relation between the L-functions of each variety and provides certain information about their decomposition up to isogeny over L. We study several properties of these Artin representations. As an application, for each curve C' in a family of twists of a certain genus 3 curve C, we explicitly compute the Artin representation attached to the Jacobians of C and C' and show how this Artin representation can be used to determine the L-function of the curve C' in terms of the L-function of C.

1 Introduction

Let A be an abelian variety of dimension g defined over a number field k. Fix an algebraic closure $\overline{k}$ of k. All the extensions of k that we will consider will be contained in $\overline{k}$. For a prime ℓ, denote by $T_\ell(A)$ the ℓ-adic Tate module of A and write $V_\ell(A) = T_\ell(A) \otimes \mathbb{Q}$. There is an action of the absolute Galois group $G_k = \mathrm{Gal}(\overline{k}/k)$ on $V_\ell(A)$, which gives an ℓ-adic representation of dimension $2g$

$$\varrho_A \colon G_k \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A)) \simeq \mathrm{GL}_{2g}(\mathbb{Q}_\ell)\,.$$

As ℓ varies, the family $\{\varrho_A\}$ constitutes a strictly compatible system of rational ℓ-adic representations in the sense of [Ser89]. Let $\overline{\mathfrak{p}}$ be a prime of $\overline{k}$ lying over a prime $\mathfrak{p}$ of k not dividing ℓ, let $I_{\overline{\mathfrak{p}}}$ be its inertia group and let $\mathrm{Frob}_{\overline{\mathfrak{p}}}$ be a Frobenius element over $\mathfrak{p}$. The polynomial

$$L_{\mathfrak{p}}(A/k, T) = \det(1 - \varrho_A(\mathrm{Frob}_{\overline{\mathfrak{p}}})T; V_\ell(A)^{I_{\overline{\mathfrak{p}}}})$$

has integer coefficients and does not depend on ℓ. A prime $\mathfrak{p}$ of k is a prime of good reduction for A if and only if the action of $I_{\overline{\mathfrak{p}}}$ through ϱ_A is trivial on $V_\ell(A)$ (see [ST68]). In this case, one has $L_{\mathfrak{p}}(A/k, T) = \prod_{i=1}^{g}(1-\alpha_i T)(1-\overline{\alpha}_i T)$, where the α_i are complex numbers such that $\alpha_i\overline{\alpha}_i = N\mathfrak{p}$. Here $N\mathfrak{p}$ stands for the norm of $\mathfrak{p}$, i.e., the size of the residue field of $\mathfrak{p}$. The L-function of A/k is defined as

$$L(A/k, s) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(A/k, N\mathfrak{p}^{-s})^{-1}\,,$$

where the product runs over all primes in k.

Let A' be an abelian variety defined over k and assume that there exists an isogeny $\phi\colon A \to A'$ defined over a finite Galois extension L/k. By functoriality, ϕ induces an isomorphism $V_\ell(A) \to V_\ell(A')$ of $\mathbb{Q}_\ell[G_L]$-modules. Let $\mathfrak{P}$ be a non-ramified prime of L of norm $N\mathfrak{P} = (N\mathfrak{p})^f$. Consider

$$L_{\mathfrak{p}}(A/k,T) = \prod_i (1-\alpha_i T)\,, \qquad L_{\mathfrak{p}}(A'/k,T) = \prod_i (1-\beta_i T)\,.$$

Recall that the local factors $L_{\mathfrak{P}}(A/L,T)$ and $L_{\mathfrak{P}}(A'/L,T)$ coincide. Since $\mathfrak{P}$ is a non-ramified prime of L, $V_\ell(A)^{I_{\overline{\mathfrak{p}}}} = V_\ell(A)^{I_{\overline{\mathfrak{P}}}}$ and $V_\ell(A')^{I_{\overline{\mathfrak{p}}}} = V_\ell(A')^{I_{\overline{\mathfrak{P}}}}$. Moreover, since a Frobenius element $\mathrm{Frob}_{\overline{\mathfrak{P}}}$ over $\mathfrak{P}$ equals the f-power of a Frobenius element $\mathrm{Frob}_{\overline{\mathfrak{p}}}$ over $\mathfrak{p}$, we have

$$\prod_i (1-\alpha_i^f T) = L_{\mathfrak{P}}(A/L,T) = L_{\mathfrak{P}}(A'/L,T) = \prod_i (1-\beta_i^f T)\,.$$

By reordering the roots, if necessary, we obtain that for $i = 1,\dots,\dim V_\ell(A)^{I_{\overline{\mathfrak{p}}}}$ it holds that $\alpha_i^f = \beta_i^f$, i.e., the roots α_i and β_i differ by a root of unity. The aim of this article is to study to what extent these roots of unity can be seen as the eigenvalues of the images of a certain Artin representation of the group $\mathrm{Gal}(L/k)$. We will make this idea more precise below. For this aim, it will be helpful to give an alternative argument of the existence of these roots of unity.

Let G denote $\mathrm{Gal}(L/k)$ until the end of this section. For every prime $\mathfrak{p}$ of k the following remarkable identity holds

$$L_{\mathfrak{p}}(\mathrm{Res}_k^L A/k,T) = \prod_{\varrho} L_{\mathfrak{p}}(A/k,\varrho,T)^{\dim \varrho}\,, \tag{1.1}$$

where the product on the right hand-side of the equality runs through all absolutely irreducible representations of G. For $\mathfrak{p}$ a prime of k which is non-ramified in L, the Rankin-Selberg polynomial $L_{\mathfrak{p}}(A/k,\varrho,T)$ is the polynomial whose roots are all the products of roots of $L_{\mathfrak{p}}(A/k,T)$ and roots of $\det(1-\varrho(\mathrm{Frob}_{\mathfrak{p}})T)$. Since $L_{\mathfrak{p}}(\mathrm{Res}_k^L A/k,T)$ and $L_{\mathfrak{p}}(\mathrm{Res}_k^L A'/k,T)$ coincide, we deduce that $L_{\mathfrak{p}}(A'/k,T)$ divides $\prod_\varrho L_{\mathfrak{p}}(A/k,\varrho,T)^{\dim\varrho}$ and we thus recover the existence of the already mentioned roots of unity.

Moreover, identity (1.1) can be understood in terms of the Tate modules, asserting that $V_\ell(\mathrm{Res}_k^L A)$ and $\bigoplus_\varrho \dim\varrho\cdot\varrho\otimes V_\ell(A)$ are isomorphic as $\mathbb{Q}_\ell[G_k]$-modules. Since $V_\ell(\mathrm{Res}_k^L A)$ and $V_\ell(\mathrm{Res}_k^L A')$ are isomorphic, the previous conclusion can now be rephrased by saying that $V_\ell(A')$ is a sub-$\mathbb{Q}_\ell[G_k]$-module of $\bigoplus_\varrho \dim\varrho\cdot\varrho\otimes V_\ell(A) \simeq \mathrm{Reg}_G\otimes V_\ell(A)$, where Reg_G denotes the regular representation of G. It now arises the question of wether a rational representation θ of G of dimension smaller than $|G|$ can be defined satisfying

$$V_\ell(A') \subseteq \theta\otimes V_\ell(A) \tag{1.2}$$

as $\mathbb{Q}_\ell[G_k]$-modules.

We now present a situation, where such a representation always exists. The semisimple module $\mathbb{Q}[G]$ decomposes as a direct sum $\bigoplus_\varrho \mathbb{Q}[G]_\varrho$ indexed by the rational irreducible representations of G, where $\mathbb{Q}[G]_\varrho \simeq n_\varrho\cdot\varrho$ denotes the ϱ-isotypic component of $\mathbb{Q}[G]$. Let $\mathcal{I}_\varrho$ be $\mathbb{Q}[G]_\varrho\cap\mathbb{Z}[G]$. In [MRS07], for every rational irreducible representation ϱ, an abelian variety

$$A_\varrho := \mathcal{I}_\varrho\otimes_{\mathbb{Z}} A$$

defined over k is constructed. This construction is given in the context of commutative algebraic groups, but we will only be concerned with abelian varieties (for several explicit examples of this construction we refer the reader to [Sil08]). It is shown that A_ϱ is isomorphic over L to $A^{n_\varrho \cdot \dim \varrho}$. Now property (1.2) holds if one takes $\theta = \varrho$. Indeed, one has

$$V_\ell(A_\varrho) \simeq n_\varrho \cdot \varrho \otimes V_\ell(A) \subseteq \varrho \otimes V_\ell(A^{n_\varrho \cdot \dim \varrho}),$$

where for the first isomorphism we have applied theorem 2.2 in [MRS07]. In particular, for E an elliptic curve and E_χ the twist given by the quadratic character χ of a quadratic extension L/k, one can take $\theta = \chi$.

In section 2, we define a rational Artin representation $\theta(A, A'; L/k)$ and, for every prime ℓ, a $\mathbb{Q}_\ell[G_k]$-module W_ℓ such that the representation $\theta_\ell(A, A'; L/k)$ that affords satisfies that $\theta_\ell(A, A'; L/k) \simeq \mathbb{Q}_\ell \otimes \theta(A, A'; L/k)$.

We start section 3 proving that $\theta(A, A'; L/k)$ satisfies property (1.2) as a consequence of the fact that $V_\ell(A')$ is a submodule of $W_\ell \otimes V_\ell(A)$. Besides, we investigate several properties of $\theta(A, A'; L/k)$, such as its behavior under the change of the field extension, a characterization of its faithfulness, etc. In particular, we show that when we consider the representation $\theta(A_\varrho, A^{n_\varrho \cdot \dim \varrho}; L/k)$ corresponding to the particular case of the twisted abelian varieties $A^{n_\varrho \cdot \dim \varrho}$ and A_ϱ, one recovers a multiple of the original representation ϱ.

Finally, in section 4 we use this Artin representation to compute the L-functions of a family of twists of a certain modular genus 3 curve.

Acknowledgements. I want to thank J.-C. Lario for providing many inspiring ideas, and offering constant help and support. I am also grateful to X. Guitart and J. Quer for carefully reading a preliminary version of this article.

2 Definition and rationality

The representation ϱ_A endows $V_\ell(A)$ with a structure of $\mathbb{Q}_\ell[G_k]$-module, as we have already mentioned. We will denote by $V_\ell(A)^*$ its dual, that is the $\mathbb{Q}_\ell[G_k]$-module with underlying $\mathbb{Q}_\ell$-vector space $\mathrm{Hom}_{\mathbb{Q}_\ell}(V_\ell(A), \mathbb{Q}_\ell)$ endowed with the action given by ϱ_A^*, the contragredient representation of ϱ_A.

Let G be a group, F a field and V an F-vector space of dimension n. For a representation $\varrho\colon G \to \mathrm{Aut}_F(V)$, its contragredient representation ϱ^* satisfies $(\varrho^*(\sigma)\lambda)(v) = \lambda(\varrho(\sigma^{-1})v)$ for any $\sigma \in G$, $\lambda \in \mathrm{Hom}_F(V, F)$ and $v \in V$. By choosing a basis in V, we have $\mathrm{Aut}_F(V) \simeq \mathrm{GL}_n(F)$ and we can see $\varrho(\sigma)$ as a matrix with coefficients in F. By taking the dual basis in $\mathrm{Hom}_F(V, F)$ of the taken basis in V, one has that $\varrho^*(\sigma) = (\varrho(\sigma)^{-1})^t$, where ^{t} indicates transposition of matrices.

Consider now the $\mathbb{Q}_\ell[G_k]$-module $V_\ell(A)^* \otimes V_\ell(A')$, where the action of G_k is given by $\varrho_A^* \otimes \varrho_{A'}$ and denote by

$$W_\ell = (V_\ell(A)^* \otimes V_\ell(A'))^{G_L}$$

the subspace of the elements invariant under the action of the subgroup $G_L = \mathrm{Gal}(\overline{k}/L)$. In general, for F a field, G a group, H a normal subgroup of G, and V an $F[G]$-module (with the action of G on V denoted by left exponentiation) and $v \in V^H$, $h \in H$, and $g \in G$, we have ${}^h({}^g v) = {}^g({}^{g^{-1}hg} v) = {}^g({}^{h'} v) = {}^g v$, where $h' = g^{-1}hg$ is an element of H. That is, V^H is endowed with a structure of $F[G/H]$-module. As a consequence, we have the following lemma.

Lemma 2.1. *The space W_ℓ acquires a structure of $\mathbb{Q}_\ell[\mathrm{Gal}(L/k)]$-module.*

We will denote by $\theta_\ell(A, A'; L/k)$ the representation of $\mathrm{Gal}(L/k)$ afforded by the module W_ℓ. Observe that for every prime $\mathfrak{p}$ of good reduction for A and A', the eigenvalues of $\theta_\ell(A, A'; L/k)(\mathrm{Frob}_\mathfrak{p})$ are roots of unity obtained as quotients of roots of $L_\mathfrak{p}(A'/k, T)$ and roots of $L_\mathfrak{p}(A/k, T)$.

To investigate the properties of this representation, we need to recall some basic properties of tensor products, duals and morphisms of modules. We summarize them in the auxiliary result below. For G a group and F a field, let V and W be $F[G]$-modules. The F-vector space $\mathrm{Hom}_F(V, W)$ becomes an $F[G]$-module via the action defined as follows: for $g \in G$, $\lambda \in \mathrm{Hom}_F(V, W)$ and $v \in V$, we have

$$({}^g\lambda)(v) = {}^g\lambda({}^{g^{-1}}v)\,. \tag{2.1}$$

Note that by taking $W = F$ with the trivial action of G, the module $\mathrm{Hom}_F(V, W)$ is just the dual module of V.

Lemma 2.2. *Let V, W, W_1 and W_2 be $F[G]$-modules, which are of finite dimension as F-vector spaces. Let H be a normal subgroup of G. We have the following isomorphisms:*

i) $V^* \otimes W \simeq \mathrm{Hom}_F(V, W)$ *as $F[G]$-modules.*

ii) $\mathrm{Hom}_F(V, W_1 \otimes W_2) \simeq \mathrm{Hom}_F(V \otimes W_1^*, W_2)$ *as $F[G]$-modules.*

iii) $(V^H)^* \simeq (V^*)^H$ *as $F[G/H]$-modules.*

Proof. For i) we refer to lemma 3.12 of [Kar92]. Although throughout this reference G is always taken to be finite, we emphasize that the proof of this fact makes no use of this condition. Assertion ii) follows from i) and the fact that $(V \otimes W)^* \simeq V^* \otimes W^*$ (see lemma 3.11 of [Kar92]):

$$\begin{aligned}\mathrm{Hom}_F(V, W_1 \otimes W_2) &\simeq V^* \otimes (W_1 \otimes W_2)\\ &\simeq (V \otimes W_1^*)^* \otimes W_2\\ &\simeq \mathrm{Hom}_F(V \otimes W_1^*, W_2)\,.\end{aligned}$$

For iii) we need a new description of the subspace of invariants. Let $\alpha\colon G \to K$ be a morphism of groups. Denote $\mathrm{Ind}_G^K V$ the $F[G]$-module $F[K] \otimes_{F[G]} V$, where we can view $F[K]$ as an $F[G]$-module thanks to the morphism α. If α is injective, the $F[K]$-module $\mathrm{Ind}_G^K W$ coincides with usual notion of induced module from the subgroup G to K. If α is surjective, the $F[K]$-module $\mathrm{Ind}_G^K V$ is isomorphic to the subspace of V consisting of the elements invariant under $\mathrm{Ker}(\alpha)$ (see [Ser77], exercise 7.1). Let K be G/H and let α denote the natural projection. Since the operations of inducing and taking duals commute, we have

$$(V^H)^* \simeq \mathrm{Ind}_G^{G/H}(V)^* \simeq \mathrm{Ind}_G^{G/H}(V^*) \simeq (V^*)^H\,.$$

□

Remark 2.1. *With the notation of the previous lemma, let* $\mathrm{Hom}_{F[H]}(V, W)$ *denote the F-vector space of homomorphisms from V to W which commute with*

the actions of H on V and W. Equivalently, $\mathrm{Hom}_{F[H]}(V,W)$ *can be characterized as the space* $(\mathrm{Hom}_F(V,W))^H$ *of the invariant elements in* $\mathrm{Hom}_F(V,W)$ *under the action (2.1) and so, as justified before lemma 2.1, it acquires a structure of $F[G/H]$-module. It follows that* $\mathrm{Hom}_{F[H]}(V,W)$ *is isomorphic to* $(V^*\otimes W)^H$ *and that* $\mathrm{Hom}_{F[H]}(V,W_1\otimes W_2)$ *is isomorphic to* $\mathrm{Hom}_{F[H]}(V\otimes W_1^*,W_2)$.

Lemma 2.3. *The module W_ℓ is selfdual.*

Proof. First, we claim that the module $V_\ell(A)^*\otimes V_\ell(A')$ is selfdual. Since $\mathbb{Q}_\ell$ has characteristic zero and $V_\ell(A)^*\otimes V_\ell(A')$ is semisimple, it suffices to check that for every $\sigma\in G_k$ it holds $\mathrm{Tr}\,\varrho_A^*\otimes\varrho_{A'}(\sigma)=\mathrm{Tr}\,\varrho_A\otimes\varrho_{A'}^*(\sigma)$ (see [Ser89], chapter 1, section 2.1). Since Tr is a continuous function, by the Cebotarev Density Theorem, it is enough to check it for the Frobenius elements corresponding to primes of good reduction for A and A'. Let $\sigma=\mathrm{Frob}_{\mathfrak{p}}$ be such an element. Note that if $\mathrm{Tr}\,\varrho_A(\sigma)=\sum_i\alpha_i+\overline{\alpha}_i$, then

$$\mathrm{Tr}\,\varrho_A^*(\sigma)=\sum_i\frac{1}{\alpha_i}+\frac{1}{\overline{\alpha}_i}=\sum_i\frac{\overline{\alpha}_i}{N\mathfrak{p}}+\frac{\alpha_i}{N\mathfrak{p}}=\frac{1}{N\mathfrak{p}}\,\mathrm{Tr}\,\varrho_A(\sigma)\,.$$

The claim then follows from the formula

$$\mathrm{Tr}\,(\varrho_A^*\otimes\varrho_{A'}(\sigma))=\frac{1}{N\mathfrak{p}}\,(\mathrm{Tr}\,\varrho_A(\sigma)\cdot\mathrm{Tr}\,\varrho_{A'}(\sigma))\ .$$

We deduce that $W_\ell=(V_\ell(A)^*\otimes V_\ell(A'))^{G_L}$ is selfdual by applying *iii)* of lemma 2.2. □

As a consequence of the fact that $V_\ell(A)^*\otimes V_\ell(A')$ is selfdual, we deduce that $\theta_\ell(A,A';L/k)$ and $\theta_\ell(A',A;L/k)$ are isomorphic.

Let m be the exponent of $\mathrm{Gal}(L/k)$. Observe that $\mathrm{Tr}\,\theta_\ell(A,A';L/k)$ belongs to $\mathbb{Q}(\zeta_m)$, where ζ_m stands for a primitive m-th root of unity. Then, a theorem of Brauer (see [Ser77], theorem 24), conjectured by Schur, guarantees that the representation $\theta_\ell(A,A';L/k)$ can be realized over $\mathbb{Q}(\zeta_m)$, that is, there exists a representation $\tilde{\theta}_\ell(A,A';L/k)$ with matrices having coefficients in $\mathbb{Q}(\zeta_m)$ (thus, an Artin representation) such that

$$\theta_\ell(A,A';L/k)\otimes\overline{\mathbb{Q}}_\ell\simeq\tilde{\theta}_\ell(A,A';L/k)\otimes\overline{\mathbb{Q}}_\ell\,.$$

It follows from lemma 2.3, that $\mathrm{Tr}\,\theta_\ell(A,A';L/k)$ belongs to $\mathbb{R}\cap\mathbb{Q}(\zeta_m)$. Next, we shall see that in fact $\mathrm{Tr}\,\theta_\ell(A,A';L/k)$ belongs to $\mathbb{Q}$. Even more, we shall prove that $\theta_\ell(A,A';L/k)$ can be realized over $\mathbb{Q}$.

Let $\mathrm{Hom}_L(A,A')$ stand for the $\mathbb{Z}$-module of homomorphisms from A to A' which are defined over L and denote the $\mathbb{Q}$-vector space $\mathrm{Hom}_L(A,A')\otimes\mathbb{Q}$ by $\mathrm{Hom}_L^0(A,A')$. Write $\mathrm{End}_L(A)$ for the ring $\mathrm{Hom}_L(A,A)$ and $\mathrm{End}_L^0(A)$ for $\mathrm{End}_L(A)\otimes\mathbb{Q}$. Observe that, since A and A' are defined over k, the group $\mathrm{Gal}(L/k)$ acts on $\mathrm{Hom}_L^0(A,A')$. Call $\theta(A,A';L/k)$ the rational representation afforded by the $\mathbb{Q}[\mathrm{Gal}(L/k)]$-module $\mathrm{Hom}_L^0(A,A')$.

Proposition 2.1. *The representation $\theta_\ell(A,A';L/k)$ is realizable over $\mathbb{Q}$. More precisely, one has*

$$\theta_\ell(A,A';L/k)\simeq\mathbb{Q}_\ell\otimes\theta(A,A';L/k)\,.$$

Proof. The results of Faltings (see [Fal83]) ensure that

$$\mathrm{Hom}_L^0(A, A') \otimes \mathbb{Q}_\ell \simeq \mathrm{Hom}_{\mathbb{Q}_\ell[G_L]}(V_\ell(A), V_\ell(A')) \tag{2.2}$$

as $\mathbb{Q}_\ell[\mathrm{Gal}(L/k)]$-modules. Remark 2.1 together with equation (2.2) gives that $\theta_\ell(A, A'; L/k)$ is isomorphic over $\mathbb{Q}_\ell$ to $\theta(A, A'; L/k)$. □

Corollary 2.1. *The family $\{\theta_\ell(A, A'; L/k)\}_\ell$ constitutes a strictly compatible system of rational ℓ-adic representations of the group $\mathrm{Gal}(L/k)$, where the exceptional set of primes consists on the primes of k ramified in L. In particular, $\mathrm{Tr}\,\theta_\ell(A, A'; L/k)$ is a rational character of $\mathrm{Gal}(L/k)$ which does not depend on the prime ℓ.*

Proof. For $\mathfrak{p}$ a prime of k non-ramified in L, proposition 2.1 implies

$$\det(1 - \theta_\ell(A, A'; L/k)(\mathrm{Frob}_\mathfrak{p})T) = \det(1 - \theta(A, A'; L/k)(\mathrm{Frob}_\mathfrak{p})T)\,,$$

which is a polynomial with rational coefficients. In particular, for every prime ℓ, one has that $\mathrm{Tr}\,\theta_\ell(A, A'; L/k)$ equals $\mathrm{Tr}\,\theta(A, A'; L/k)$, which is a rational character of $\mathrm{Gal}(L/k)$ which does not depend on the prime ℓ. □

Remark 2.2. *Since A and A' are isogenous over L, we have that*

$$\dim \theta(A, A'; L/k) = \dim_{\mathbb{Q}} \mathrm{Hom}_L^0(A, A') = \dim_{\mathbb{Q}} \mathrm{End}_L^0(A) > 0\,.$$

We will refer to $\theta(A, A'; L/k)$ as the Artin representation attached to the isogenous abelian varieties A and A' over L/k.

3 Properties of $\theta(A, A'; L/k)$

In the previous section, a rational Artin representation $\theta(A, A'; L/k)$ has been attached to a pair of isogenous abelian varieties $A \sim_L A'$ over a finite Galois extension L/k. We show that this representation satisfies property (1.2) in the Introduction.

Theorem 3.1. *$V_\ell(A')$ is a sub-$\mathbb{Q}_\ell[G_k]$-module of $\theta(A, A'; L/k) \otimes V_\ell(A)$.*

Proof. By proposition 2.1, we have $\theta(A, A'; L/k) \otimes V_\ell(A) \simeq W_\ell \otimes V_\ell(A)$. Suppose that $V_\ell(A') \simeq \bigoplus n_i \cdot V_i$ as a sum of simple $\mathbb{Q}_\ell[G_k]$-modules V_i. We want to show that V_i appears with multiplicity at least n_i in $W_\ell \otimes V_\ell(A)$. Since

$$W_\ell \otimes V_\ell(A) \simeq \bigoplus_j n_j \cdot (V_\ell(A)^* \otimes V_j)^{G_L} \otimes V_\ell(A)\,,$$

it suffices to see that V_i is a constituent of $(V_\ell(A)^* \otimes V_i)^{G_L} \otimes V_\ell(A)$. Since V_i is simple, this is equivalent to prove that $\dim_{\mathbb{Q}_\ell} \mathrm{Hom}_{\mathbb{Q}_\ell[G_k]}(V_i, (V_\ell(A)^* \otimes V_i)^{G_L} \otimes V_\ell(A)) > 0$. Now, *ii)* of lemma 2.2 provides an isomorphism

$$\mathrm{Hom}_{\mathbb{Q}_\ell[G_k]}(V_i, (V_\ell(A)^* \otimes V_i)^{G_L} \otimes V_\ell(A)) \simeq \mathrm{Hom}_{\mathbb{Q}_\ell[G_k]}(V_\ell(A)^* \otimes V_i, (V_\ell(A)^* \otimes V_i)^{G_L})\,,$$

from which the result follows provided that $(V_\ell(A)^* \otimes V_i)^{G_L}$ is a nontrivial sub-$\mathbb{Q}_\ell[G_k]$-module of $V_\ell(A)^* \otimes V_i$. Indeed, since $V_\ell(A) \simeq \bigoplus n_i \cdot V_i$ as $\mathbb{Q}_\ell[G_L]$-modules, one has

$$\begin{aligned}\dim_{\mathbb{Q}_\ell}(V_\ell(A)^* \otimes V_i)^{G_L} &= \dim_{\mathbb{Q}_\ell} \mathrm{Hom}_{\mathbb{Q}_\ell[G_L]}(V_\ell(A), V_i) \\ &= \sum_j n_j \dim_{\mathbb{Q}_\ell} \mathrm{Hom}_{\mathbb{Q}_\ell[G_L]}(V_j, V_i) \\ &\geq \dim_{\mathbb{Q}_\ell} \mathrm{End}_{\mathbb{Q}_\ell[G_L]}(V_i)\,.\end{aligned}$$

□

Corollary 3.1. *Suppose that A' is simple over k and that $A \sim_k E^g$, for E an elliptic curve defined over k such that $\mathrm{End}_k^0(E) \simeq \mathbb{Q}$. Then, $V_\ell(A') \simeq \varrho \otimes V_\ell(E)$, where ϱ is a representation of $\mathrm{Gal}(L/k)$ such that $\theta(A, A'; L/k) = g \cdot \varrho$.*

Proof. Observe that the hypothesis $A \sim_k E^g$ implies that $\theta(A, A'; L/k) = g \cdot \varrho$, for a certain rational representation ϱ. By theorem 3.1, we have

$$V_\ell(A') \subseteq \theta(A, A'; L/k) \otimes V_\ell(E^g) \simeq g^2 \cdot \varrho \otimes V_\ell(E)\,.$$

Since $V_\ell(A')$ is simple, $V_\ell(A') \subseteq \varrho \otimes V_\ell(E)$. Since $\dim \varrho \leq g$ (as a consequence of $\mathrm{End}_k^0(E) \simeq \mathbb{Q}$), the inclusion is an isomorphism and the proposition follows. □

Proposition 3.1. *Let ϱ be an irreducible rational representation of $\mathrm{Gal}(L/k)$. If $\mathrm{End}_L^0(A) \simeq \mathbb{Q}$, then $\theta(A^{n_\varrho \cdot \dim \varrho}, A_\varrho; L/k) \simeq n_\varrho^2 \cdot \dim \varrho \cdot \varrho$.*

Proof. Observe that on the one hand, we have

$$(V_\ell(A^{n_\varrho \cdot \dim \varrho})^* \otimes V_\ell(A_\varrho))^{G_L} \simeq n_\varrho^2 \cdot \dim \varrho \cdot \varrho \otimes (V_\ell(A)^* \otimes V_\ell(A))^{G_L}\,.$$

On the other hand, $\mathrm{End}_L^0(A) \simeq \mathbb{Q}$ implies that $(V_\ell(A)^* \otimes V_\ell(A))^{G_L}$ is the trivial representation. □

In particular, if χ is the quadratic character of a quadratic extension L/k, E is an elliptic curve defined over k such that $\mathrm{End}_L^0(E) \simeq \mathbb{Q}$ and E_χ the quadratic twist of E given by χ, then $\theta(E, E_\chi; L/k) \simeq \chi$.

So far we have not paid much attention to the extension L/k. We do this in the following, where we are concerned with the problem of relating the distinct representations attached to the pair A and A' obtained when we let the field of definition of the isogeny between them vary. First we remind some notations. Let G be a group and H be a subgroup of G. If ϱ is a representation of G, we denote by $\mathrm{Res}_H^G \varrho$ the representation ϱ restricted to the subgroup H. If ϱ is a representation of H, we denote by $\mathrm{Ind}_H^G \varrho$ the induced representation from H to G. If H is normal in G, ϱ is a representation of G/H and π is the canonical projection from G to G/H, we denote by $\mathrm{Inf}_{G/H}^G \varrho$ the representation $\varrho \circ \pi$. If F/F'' is a Galois extensions of fields, F'/F'' a subextension of F/F'' and $G = \mathrm{Gal}(F/F'')$ and $H = \mathrm{Gal}(F/F')$, we will simply write $\mathrm{Res}_{F'}^F$, $\mathrm{Ind}_{F'}^F$ and $\mathrm{Inf}_{F'}^F$ for Res_H^G, Ind_H^G and $\mathrm{Inf}_{G/H}^G$, respectively.

Proposition 3.2. *It holds:*

i) Let L'/k be a Galois subextension of L/k over which A and A' are isogenous. Then, the representation $\theta(A, A'; L/k)$ is isomorphic to a subrepresentation of $\mathrm{Ind}_{L'}^L \theta(A, A'; L/L')$.

ii) Let L'/k be a Galois extension containing L/k. Then, the representation $\mathrm{Inf}_L^{L'}\,\theta(A,A';L/k)$ is isomorphic to a subrepresentation of $\theta(A,A';L'/k)$.

Proof. For the first statement, observe that $\theta(A,A';L/L') = \mathrm{Res}^L_{L'}\,\theta(A,A';L/k)$. Now we obtain the result from the fact that any complex representation ϱ of a finite group G is a subrepresentation of $\mathrm{Ind}_H^G \mathrm{Res}_H^G \varrho$, for any subgroup H of G. Indeed, let χ_ϱ denote the character of ϱ. By Frobenius reciprocity, for any irreducible character χ of G, one has

$$(\chi,\chi_\varrho)_G \leq (\mathrm{Res}^G_H\,\chi, \mathrm{Res}^G_H\,\chi_\varrho)_H = (\chi, \mathrm{Ind}^G_H \mathrm{Res}^G_H\,\chi_\varrho)_G,$$

where $(\cdot,\cdot)_G$ and $(\cdot,\cdot)_H$ denote the scalar products on complex-valued functions on G and H, respectively. The second statement is due to the fact that for every $F[G]$-module V and normal subgroup H of G, $\mathrm{Inf}^G_H\,V^H$ is a sub-$F[G]$-module of V. □

Proposition 3.3. *The representation $\theta(A,A';L/k)$ is faithful if and only if for every proper Galois subextension L'/k of L/k it holds*

$$\dim_{\mathbb{Q}} \mathrm{Hom}^0_{L'}(A,A') < \dim_{\mathbb{Q}} \mathrm{Hom}^0_L(A,A')\,.$$

Proof. Indeed, $\theta(A,A';L/k)$ is not faithful if and only if there exists a proper Galois subextension L'/k of L/k such that

$$\mathrm{Hom}^0_{L'}(A,A') = \mathrm{Hom}^0_L(A,A')\,.$$

Since the space on the left-hand side of the equality is always included into the one on the right-hand side, asking for equality of the spaces amounts to asking for equality of their dimensions. □

As a corollary of this proposition, we obtain that if there does not exist a Galois subextension of L/k over which A and A' are isogenous, then $\theta(A,A';L/k)$ is faithful. Therefore, a subextension L'/k of L/k can always be taken so that $\theta(A,A';L'/k)$ is faithful. We give an elementary result, which will be useful to determine the irreducible constituents of $\theta(A,A';L/k)$.

Proposition 3.4. *Suppose that $\theta(A,A';L/k) \simeq \bigoplus n_\varrho \cdot \varrho$, where the sum runs over the absolutely irreducible representations of $\mathrm{Gal}(L/k)$ and the n_ϱ are non-negative integers. Let L'/k be a subextension of L/k. Then we have*

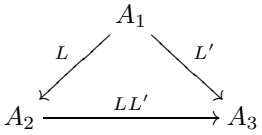
$$\sum_{\mathrm{Ker}\,\varrho \supseteq \mathrm{Gal}(L/L')} n_\varrho \cdot \dim \varrho = \dim_{\mathbb{Q}} \mathrm{Hom}^0_{L'}(A,A')\,.$$

In particular, $\dim_{\mathbb{Q}} \mathrm{Hom}^0_k(A,A')$ is the multiplicity of the trivial representation of $\mathrm{Gal}(L/k)$ in $\theta(A,A';L/k)$.

Proof. It is enough to observe that the space $\mathrm{Hom}^0_{L'}(A,A')$ is isomorphic to the direct sum of those constituents ϱ of $\theta(A,A';L/k)$ such that $\mathrm{Ker}\,\varrho$ contains $\mathrm{Gal}(L/L')$. □

To close this section, we turn to discuss a kind of transitivity property satisfied by $\theta(A,A';L/k)$. It will turn out to be a very useful tool, as shown in the next section. Let A_1, A_2 and A_3 be abelian varieties defined over a number

field k, such that A_1 and A_2 are isogenous over the finite Galois extension L/k and A_1 and A_3 are isogenous over the finite Galois extension L'/k. Notice that A_2 and A_3 are isogenous over the composition LL'.



Next proposition shows how the Artin representations attached to the three pairs of isogenous varieties are related.

Proposition 3.5. *The representation $\theta(A_2, A_3; LL'/k)$ is isomorphic to a sub-representation of*

$$\theta(A_1, A_2; LL'/k) \otimes \theta(A_1, A_3; LL'/k)\,.$$

Proof. Since $\theta(A_1, A_2; LL'/k)$ is selfdual, by $i)$ of lemma 2.2, it suffices to prove that there is an inclusion of $\mathbb{Q}[\mathrm{Gal}(LL'/k)]$-modules

$$\mathrm{Hom}_{LL'}(A_2, A_3) \subseteq \mathrm{Hom}_{\mathbb{Q}}(\mathrm{Hom}_{LL'}(A_1, A_2), \mathrm{Hom}_{LL'}(A_1, A_3))\,.$$

Denote $\mathrm{Hom}_{LL'}(A_i, A_j)$ by F_{ij}. For each $\varphi \in F_{23}$, define $\tilde{\varphi} \in \mathrm{Hom}_{LL'}(F_{12}, F_{13})$ in the following way: for each $\lambda \in F_{12}$, let $\tilde{\varphi}(\lambda) = \varphi \circ \lambda \in F_{13}$. The map $\varphi \mapsto \tilde{\varphi}$ gives an inclusion that respects the action of $\mathrm{Gal}(LL'/k)$. Indeed, one has

$$(\widetilde{{}^{\sigma}\varphi})(\lambda) = {}^{\sigma}\varphi \circ \lambda = {}^{\sigma}(\varphi \circ {}^{\sigma^{-1}}\lambda) = {}^{\sigma}(\tilde{\varphi}({}^{\sigma^{-1}}\lambda)) = ({}^{\sigma}\tilde{\varphi})(\lambda)\,,$$

for any $\sigma \in \mathrm{Gal}(LL'/k)$, $\varphi \in F_{23}$ and $\lambda \in F_{12}$. □

4 Example

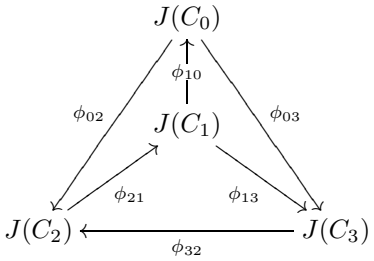
In [BFGL07], the modular genus 3 curve $C_0 = X^+(7,3)$ is defined. Moreover, for each polynomial $f(x) \in \mathbb{Q}[x]$ of degree 4 such that its splitting field L is an $\mathcal{S}_4$-extension containing $\mathbb{Q}(\sqrt{-3})$ a way to produce a twist $X^+(7,3)_\varrho$ is shown. Here, ϱ stands for a surjective Galois representation of $G_{\mathbb{Q}}$ onto $\mathrm{PGL}_2(\mathbb{F}_3)$ determined up to conjugation by its splitting field L. In the same article, the curve C_0 is shown to be isomorphic over $\mathbb{Q}(\sqrt{-3})$ to the plane quartic C_1 given by the following equation

$$X^4 + Y^4 + Z^4 + \frac{2}{7}\left(X^2Z^2 + Y^2Z^2 + X^2Y^2\right) = 0\,.$$

The Jacobian $J(C_0)$ of the curve C_0 happens to be $\mathbb{Q}$-isogenous to $E_{21}^2 \times E_{63}$, where E_{21} and E_{63} stand for the elliptic curves of conductor 21 and label $A1$, and conductor 63 and label $A2$ in the Cremona's Tables (see [Cre97]). It can be checked that the curves E_{21} and E_{63} do not have complex multiplication and are isomorphic over $\mathbb{Q}(\sqrt{-3})$, but not over $\mathbb{Q}$. The Jacobian of the curve C_1 is $\mathbb{Q}$-isogenous to E_{21}^3.

Let $C_2 = X^+(7,3)_\varrho$ and $C_3 = X^+(7,3)_{\varrho'}$ be the curves attached to any two Galois representations ϱ and ϱ' from $G_{\mathbb{Q}}$ onto $\mathrm{PGL}_2(\mathbb{F}_3)$, with splitting fields L and L' satisfying $L \cap L' = \mathbb{Q}(\sqrt{-3})$. Let f and f' be defining polynomials

of L and L', respectively. Let ϕ_{ij} stand for a fixed isomorphism from C_i to C_j, and use the same notation to refer to the induced isomorphism between the Jacobians. It follows from the definition of $X^+(7,3)_\varrho$ that ϕ_{21} and ϕ_{13} are respectively defined over $L_{21} = L$ and $L_{31} = L'$. The isomorphism ϕ_{32} is clearly defined over the composition $L_{32} = LL'$, which is an extension of degree 288 over $\mathbb{Q}$. As mentioned above, the isomorphism ϕ_{01} can be defined over $L_{01} = \mathbb{Q}(\sqrt{-3})$. Since both L and L' contain $\mathbb{Q}(\sqrt{-3})$, it follows that ϕ_{02} and ϕ_{03} are defined over $L_{02} = L$ and $L_{03} = L'$, respectively.



One of the aims of this section is to compute the Artin representations $\theta_{ij} = \theta(J(C_i), J(C_j); L_{ij}/\mathbb{Q})$ for $(i,j) = (0,1)$, $(0,2)$, $(0,3)$, $(2,1)$, $(1,3)$, and $(3,2)$. Since $J(C_1)$ and $J(C_2)$ are L-isogenous to E_{21}^3, it follows from proposition 2.2 that θ_{21} has dimension 9. The same argument proves that θ_{13} and θ_{32} have dimension 9. We fix the following notation:

i) Let $1a_L$, $2a_L$,... stand for the conjugacy classes of $\mathrm{Gal}(L/\mathbb{Q})$, and χ_1, χ_2,... for its irreducible characters (see Table 1). Note that the traces in the entries of Table 1 are given as sums of eigenvalues of the corresponding irreducible representations. Analogously, denote by $1a_{L'}$, $2a_{L'}$,... the conjugacy classes of $\mathrm{Gal}(L'/\mathbb{Q})$, and by χ'_1, χ'_2,... its irreducible characters. Moreover, let ϱ_i be the irreducible representation associated to χ_i.

ii) Let χ_t and χ_q be the trivial and the quadratic characters of $\mathrm{Gal}(\mathbb{Q}(\sqrt{-3})/\mathbb{Q})$, respectively.

iii) Let $1A$, $2A$,... stand for the conjugacy classes of $\mathrm{Gal}(LL'/\mathbb{Q})$ and ψ_1, ψ_2,... for its irreducible characters (see Table 2).

Class	$1a_L$	$2a_L$	$2b_L$	$3a_L$	$4a_L$
Size	1	3	6	8	6
χ_1	1	1	1	1	1
χ_2	1	1	-1	1	-1
χ_3	2	$1+1$	$1-1$	$\zeta_3+\overline{\zeta}_3$	$1-1$
χ_4	3	$1-1-1$	$1-1-1$	$1+\zeta_3+\overline{\zeta}_3$	$1+i-i$
χ_5	3	$1-1-1$	$1+1-1$	$1+\zeta_3+\overline{\zeta}_3$	$-1+i-i$

Table 1: Character table of $\mathrm{Gal}(L/\mathbb{Q})$

Consider the subfields L_3 and L_4 of L defined in [BFGL07]. We recall that $L_4/\mathbb{Q}$ denotes a quartic extension generated by a root of the polynomial f and L_3 denotes a cubic extension generated by a root of the resolvent of f. In

Class	$1A$	$2A$	$2B$	$2C$	$2D$	$3A$	$3B$	$3C$	$3D$	$4A$	$4B$	$4C$	$6A$	$6B$
Size	1	2	2	2	2	3	3	3	3	4	4	4	6	6
ψ_1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
ψ_2	1	1	1	1	−1	1	1	1	1	−1	−1	−1	1	1
ψ_3	2	2	2	2	0	−1	2	−1	−1	0	0	0	−1	2
ψ_4	2	2	2	2	0	2	−1	−1	−1	0	0	0	2	−1
ψ_5	2	2	2	2	0	−1	−1	2	−1	0	0	0	−1	−1
ψ_6	2	2	2	2	0	−1	−1	−1	2	0	0	0	−1	−1
ψ_7	3	3	−1	−1	1	0	3	0	0	−1	1	−1	0	−1
ψ_8	3	3	−1	−1	−1	0	3	0	0	1	−1	1	0	−1
ψ_9	3	−1	3	−1	1	3	0	0	0	−1	−1	1	−1	0
ψ_{10}	3	−1	3	−1	−1	3	0	0	0	1	1	−1	−1	0
ψ_{11}	6	−2	6	−2	0	−3	0	0	0	0	0	0	1	0
ψ_{12}	6	6	−2	−2	0	0	−3	0	0	0	0	0	0	1
ψ_{13}	9	−3	−3	1	1	0	0	0	0	1	−1	−1	0	0
ψ_{14}	9	−3	−3	1	−1	0	0	0	0	−1	1	1	0	0

Table 2: Character table of $\mathrm{Gal}(LL'/\mathbb{Q})$

page 375 of the mentioned reference, it is shown that there exist elliptic curves E_R defined over L_3 and E_S defined over $\mathbb{Q}$ such that

$$J(C_2) \sim_{\mathbb{Q}} \mathrm{Res}_{\mathbb{Q}}^{L_3} E_R \qquad \text{and} \qquad J(C_2) \times E_S \sim_{\mathbb{Q}} \mathrm{Res}_{\mathbb{Q}}^{L_4} E_S \,. \tag{4.1}$$

Moreover, one can check that $E_S \sim_{\mathbb{Q}} E_{63}$.

Lemma 4.1. *Let p be a prime of good reduction for both $J(C_1)$ and $J(C_2)$. Let $(1-\alpha T)(1-\overline{\alpha}T)$ be the local factor $L_p(E_{21}/\mathbb{Q},T)$. Then, the local factor $L_p(J(C_2)/\mathbb{Q},T)$ equals*

$$\begin{cases} L_p(E_{21}/\mathbb{Q},T)(1-\zeta_3\alpha T)(1-\overline{\zeta}_3\overline{\alpha}T)(1-\overline{\zeta}_3\alpha T)(1-\zeta_3\overline{\alpha}T) & \text{if } f_{L_3}=3 \\ L_p(E_{21}/\mathbb{Q},T)(1-i\alpha T)(1+i\overline{\alpha}T)(1+i\alpha T)(1-i\overline{\alpha}T) & \text{if } f_{L_4}=4, \end{cases}$$

where f_{L_3} and f_{L_4} denote the residue class degrees of p in L_3 and L_4, respectively, and ζ_3 a primitive cubic root of unity.

Proof. Recall that for an abelian variety A defined over a number field extension L/k and a prime $\mathfrak{p}$ of k, we have the equality

$$L_{\mathfrak{p}}(\mathrm{Res}_k^L A/k,T) = \prod_{\mathfrak{P}|\mathfrak{p}} L_{\mathfrak{P}}(A/L,T^{f_{\mathfrak{P}}})\,,$$

where $f_{\mathfrak{P}}$ denotes the residue class degree of the prime $\mathfrak{P}$ of L. Thus, if $f_{L_3}=3$ and $\mathfrak{P}_3$ denotes the prime of L_3 over p, relation (4.1) gives

$$L_p(J(C_2)/\mathbb{Q},T) = L_{\mathfrak{P}_3}(E_R/L_3,T^3) = 1-(1+p^3-\#\tilde{E}_R(\mathbb{F}_{p^3}))T+p^3T^6\,, \tag{4.2}$$

where $\tilde{E}_R$ denotes the reduction of E_R modulo the prime $\mathfrak{P}_3$. Since $E_R \simeq_L E_{21}$ and $f_{L_3}=3$ implies $f_L=3$, one has that $\#\tilde{E}_R(\mathbb{F}_{p^3}) = \#\tilde{E}_{21}(\mathbb{F}_{p^3})$. Write

$L_p(E_{21}/\mathbb{Q},T) = 1 - aT + pT^2$. By differentiating the function

$$\mathrm{Log}\left(\frac{1-aT+pT^2}{(1-T)(1-pT)}\right) = \sum_{n\geq 1} \#\tilde{E}_{21}(\mathbb{F}_{p^n})\frac{T^n}{n}\,,$$

one easily obtains that $\#\tilde{E}_{21}(\mathbb{F}_{p^3}) = 1 + p^3 - a^3 + 3ap$. Substituting in equation (4.2) and factoring, we get to

$$L_p(J(C_2)/\mathbb{Q},T) = (1 - aT + pT^2)(1 + aT + (a^2 - p)T^2 + apT^3 + p^2T^4)\,.$$

Now, a straightforward calculation of the roots of the second factor in the above expression leads us to the first statement of the lemma. For the second, if $\mathfrak{P}_4$ denotes the prime of L_4 over p, relation (4.1) implies

$$L_p(J(C_2)/\mathbb{Q},T)L_p(E_{63}/\mathbb{Q},T) = L_{\mathfrak{P}_4}(E_S/L_4,T^4)\,.$$

Applying an analogous argument to the previous case, one arrives at

$$L_{\mathfrak{P}_4}(E_S/L_4,T^4) = (1 + aT + pT^2)(1 - aT + pT^2)(1 + (a^2 - 2p)T^2 + p^2T^4)\,.$$

Now use that, for primes with $f_L = 4$, one has $L_p(E_{63}/\mathbb{Q},T) = 1 + aT + pT^2$ and then the lemma follows by computing the roots of the last factor of the above expression. □

Lemma 4.2. *The curves E_{21} and E_{63} do not appear in the decomposition up to isogeny over $\mathbb{Q}$ of $J(C_2)$.*

Proof. Suppose that $J(C_2) \sim_{\mathbb{Q}} E_{21} \times A$ or $J(C_2) \sim_{\mathbb{Q}} E_{63} \times A$, for some abelian surface A defined over $\mathbb{Q}$ and we will reach a contradiction. Then $A \sim_L E_{21}^2$. As explained in the previous sections, we can consider the Artin representation $\theta(A, E_{21}^2; L/\mathbb{Q})$ and it has dimension 4. Let p be a non-supersingular prime for E_{21} of good reduction for both E_{21} and A with residue class degree $f_{L_3} = 3$. If we write $L_p(E_{21}/\mathbb{Q},T) = (1 - \alpha T)(1 - \overline{\alpha}T)$, the condition of p being non-supersingular guarantees that $\overline{\alpha}/\alpha$ has infinite order (see for example [Tat66], theorem 2). From lemma 4.1, it follows that the only possible values for a quotient of a root of $L_p(E_{21}/\mathbb{Q},T)$ and a root of $L_p(A/\mathbb{Q},T)$ that have finite order are ζ_3 and $\overline{\zeta}_3$. Thus, $\theta(A, E_{21}^2; L/\mathbb{Q}) \simeq 2 \cdot \varrho_3$ (see Table 1). Let p be a non-supersingular prime for E_{21} of good reduction for both E_{21} and A with residue class degree $f_{L_4} = 4$. Lemma 4.1 shows that the only possible values for a quotient of a root of $L_p(E_{21}/\mathbb{Q},T)$ and a root of $L_p(A/\mathbb{Q},T)$ that have finite order are i and $-i$. We reach a contradiction by observing that the eigenvalues of ϱ_3 on the class $4a_L$ are are 1 and -1 (see Table 1). □

We have seen that E_{21} is not a $\mathbb{Q}$-factor of $J(C_2)$. Nevertheless, as we will prove later, for every prime p of good reduction for both $J(C_2)$ and E_{21}, the polynomial $L_p(E_{21}/\mathbb{Q},T)$ divides $L_p(J(C_2)/\mathbb{Q},T)$. Another example where this curious phenomenon occurs is the following one. Let E denote an elliptic curve over $\mathbb{Q}$ and let d_1 and d_2 be nonsquare rational numbers such that d_1d_2 is also a nonsquare. Consider the product $A = E_{d_1} \times E_{d_2} \times E_{d_1d_2}$ of the quadratic twists of E by d_1, d_2 and d_1d_2. Then, for every prime p of good reduction for both E and A, it is clear that $L_p(E/\mathbb{Q},T)$ divides $L_p(A/\mathbb{Q},T)$, even though E is not a $\mathbb{Q}$-factor of A.

Corollary 4.1. *The Jacobian $J(C_2)$ is simple over $\mathbb{Q}$.*

Proof. Assume $J(C_2)$ decomposes, i.e., $J(C_2) \sim_{\mathbb{Q}} E \times A$, for some elliptic curve E and some abelian surface A, both defined over $\mathbb{Q}$. It follows that $E_{21} \sim_L E$. Let θ stand for $\theta(E, E_{21}; L/\mathbb{Q})$. Since $\dim \theta = 1$ (E does not have complex multiplication), we have that either $\operatorname{Tr}\theta = \chi_1$ or χ_2. In any case, θ factors through $\mathbb{Q}(\sqrt{-3})$, the only quadratic extension of L. Then, theorem 3.1 implies that $V_\ell(E) \simeq \theta \otimes V_\ell(E_{21})$, from which we deduce that either $E \sim_{\mathbb{Q}} E_{21}$ or $E \sim_{\mathbb{Q}} E_{63}$. But this is a contradiction with the previous lemma. □

We now compute all the Artin representations θ_{ij} involved in the above graph of isogenies. As for θ_{32}, it will be computed in proposition 4.2 from θ_{21} and θ_{13} and the transitivity property stated in proposition 3.5.

Proposition 4.1. *We have:*

i) $\operatorname{Tr}(\theta_{21}) = 3 \cdot \chi_4$

ii) $\operatorname{Tr}(\theta_{13}) = 3 \cdot \chi_4'$

iii) $\operatorname{Tr}(\theta_{10}) = 6 \cdot \chi_t + 3 \cdot \chi_q$

iv) $\operatorname{Tr}(\theta_{02}) = 2 \cdot \chi_4 + \chi_5$

v) $\operatorname{Tr}(\theta_{03}) = 2 \cdot \chi_4' + \chi_5'$.

Proof. By proposition 3.4 and lemma 4.2, the representation ϱ_1 is not a constituent of θ_{21}. Let p be a non-supersingular prime for E_{21} of good reduction for both E_{21} and $J(C_2)$ with residue class degree $f_{L_4} = 4$. By lemma 4.1, the only possible values for a quotient of a root of $L_p(E_{21}^3/\mathbb{Q}, T)$ and a root of $L_p(J(C_2)/\mathbb{Q}, T)$ of finite order are $1, i$ and $-i$. Since $\varrho_2(4a_L)$, $\varrho_3(4a_L)$ and $\varrho_5(4a_L)$ have -1 as an eigenvalue, the representations ϱ_2, ϱ_3 and ϱ_5 are not constituents of θ_{21}, neither. Proceeding analogously, one obtains that $\operatorname{Tr}(\theta_{13}) = 3 \cdot \chi_4'$.

To prove that $\operatorname{Tr}(\theta_{10}) = 6 \cdot \chi_t + 3 \cdot \chi_q$ it is enough to observe that

$$\dim_{\mathbb{Q}} \operatorname{Hom}_{\mathbb{Q}}(J(C_1), J(C_0)) = \dim_{\mathbb{Q}} \operatorname{Hom}_{\mathbb{Q}}(E_{21}^3, E_{21}^2 \times E_{63}) = 6$$

and then apply proposition 3.4.

Proposition 3.2 tells us that $\operatorname{Inf}_{\mathbb{Q}(\sqrt{-3})}^{L} \theta_{10} \simeq 6 \cdot \varrho_1 \oplus 3 \cdot \varrho_2$ is isomorphic to a subrepresentation of $\theta(J(C_1), J(C_0); L/\mathbb{Q})$. But since they both have the same dimension, they are in fact isomorphic. Proposition 3.5 tells us that θ_{02} is isomorphic to a subrepresentation of

$$\theta_{21} \otimes \theta(J(C_1), J(C_0); L/\mathbb{Q}) \simeq 3 \cdot \varrho_4 \otimes (6 \cdot \varrho_1 \oplus 3 \cdot \varrho_2) = 18 \cdot \varrho_4 \oplus 9 \cdot \varrho_5 \,.$$

Hence, $\operatorname{Tr}(\theta_{02}) = n \cdot \chi_4 + m \cdot \chi_5$, for certain integers $0 \leq n,\, m \leq 3$. Applying again proposition 3.5, we have that $\theta(J(C_1), J(C_0); L/\mathbb{Q})$ is isomorphic to a subrepresentation of

$$\begin{aligned} \theta_{02} \otimes \theta_{21} &\simeq (3n \cdot \varrho_4 \otimes \varrho_4) \oplus (3m \cdot \varrho_5 \otimes \varrho_4) \\ &\simeq 3n(\varrho_1 \oplus \varrho_3 \oplus \varrho_4 \oplus \varrho_5) \oplus 3m(\varrho_2 \oplus \varrho_3 \oplus \varrho_4 \oplus \varrho_5) \\ &\simeq 3n \cdot \varrho_1 \oplus 3m \cdot \varrho_2 \oplus 9 \cdot \varrho_3 \oplus 9 \cdot \varrho_4 \oplus 9 \cdot \varrho_5 \,. \end{aligned}$$

Hence, $n \geq 2$ and $m \geq 1$, which implies $n = 2$ and $m = 1$ as desired. Proceeding analogously, one obtains that $\operatorname{Tr}(\theta_{03}) = 2 \cdot \chi_4' + \chi_5'$. □

Now we can prove that for every prime p of good reduction for both E_{21} and $J(C_2)$, the polynomial $L_p(E_{21}/\mathbb{Q},T)$ divides $L_p(J(C_2)/\mathbb{Q},T)$. The image of any element in $\mathrm{Gal}(L/\mathbb{Q})$ by ϱ_4 has 1 as an eigenvalue. This means that the polynomials $L_p(E_{21}^3/\mathbb{Q},T)$ and $L_p(J(C_2)/\mathbb{Q},T)$ have a common root for every such p. Since $L_p(E_{21}/\mathbb{Q},T)$ is irreducible, it must divide $L_p(J(C_2)/\mathbb{Q},T)$.

Proposition 4.2. *We have* $\mathrm{Tr}(\theta_{32}) = \psi_{13}$.

Proof. First we need to know how the conjugacy classes of $\mathrm{Gal}(LL'/\mathbb{Q})$ project onto the conjugacy classes of the quotients $\mathrm{Gal}(L/\mathbb{Q})$ and $\mathrm{Gal}(L'/\mathbb{Q})$. Denote by π_L and $\pi_{L'}$ the canonical projections from $\mathrm{Gal}(LL'/\mathbb{Q})$ to $\mathrm{Gal}(L/\mathbb{Q})$ and $\mathrm{Gal}(L'/\mathbb{Q})$, respectively. With the help of Magma (see [Mag]), we obtain:

$1a_L = \pi_L(1A \cup 2B \cup 3A)$	$1a_{L'} = \pi_{L'}(1A \cup 2A \cup 3B)$
$2a_L = \pi_L(2A \cup 2C \cup 6A)$	$2a_{L'} = \pi_{L'}(2B \cup 2C \cup 6B)$
$2b_L = \pi_L(2D \cup 4C)$	$2b_{L'} = \pi_{L'}(2D \cup 4B)$
$3a_L = \pi_L(3B \cup 3C \cup 3D \cup 6D)$	$3a_{L'} = \pi_{L'}(3A \cup 3C \cup 3D \cup 6A)$
$4a_L = \pi_L(4A \cup 4B)$	$4a_{L'} = \pi_{L'}(4A \cup 4C)$

It is now easy to compute that $\mathrm{Tr}\,\mathrm{Inf}_L^{LL'}(\varrho_4) = \psi_{10}$ and that $\mathrm{Tr}\,\mathrm{Inf}_{L'}^{LL'}(\varrho_4') = \psi_8$. Proposition 3.2 says that $\mathrm{Inf}_L^{LL'}\theta_{21}$ and $\mathrm{Inf}_L^{LL'}\theta_{13}$ are respectively subrepresentations of $\theta(J(C_2),J(C_1);LL'/\mathbb{Q})$ and $\theta(J(C_1),J(C_3);LL'/\mathbb{Q})$. In fact, since they have the same dimension, they coincide. Proposition 3.5 states that θ_{32} is a subrepresentation of

$$\theta(J(C_2),J(C_1);LL'/\mathbb{Q}) \otimes \theta(J(C_1),J(C_3);LL'/\mathbb{Q})\,.$$

This representation has trace $9\cdot\psi_{10}\cdot\psi_8 = 9\cdot\psi_{13}$ and now the fact that θ_{32} has dimension 9 ensures that $\mathrm{Tr}(\theta_{32}) = \psi_{13}$. □

We have seen that $\theta(J(C_1),J(C_2);L/\mathbb{Q}) \simeq 3\cdot\varrho_4$. Applying cororllary 3.1, we obtain that $V_\ell(J(C_2)) \simeq \varrho_4 \otimes V_\ell(E_{21})$, from which the next corollary follows.

Corollary 4.2. *For every prime p which is non-ramified in L, the local factor $L_p(J(C_2)/\mathbb{Q},T)$ coincides with the Rankin-Selberg polynomial $L_p(E_{21}/\mathbb{Q},\varrho_4,T)$.*

Corollary 4.3. *For every prime p of good reduction for both E_{21} and $J(C_2)$, we have*

$$\#\tilde{C}_2(\mathbb{F}_{p^r}) = (1+p^r)(1-\mathrm{Tr}\,\varrho_4(\mathrm{Frob}_p^r)) + \mathrm{Tr}\,\varrho_4(\mathrm{Frob}_p^r)\#\tilde{E}_{21}(\mathbb{F}_{p^r})\,.$$

Proof. Let α and $\overline{\alpha}$ be the reciprocals of the roots of $L_p(E_{21}/\mathbb{Q},T)$ and let λ_i denote the reciprocals of the roots of $\det(1-\varrho_4(\mathrm{Frob}_p)T)$. Then, we have

$$\begin{aligned}\#\tilde{C}_2(\mathbb{F}_{p^r}) &= 1+p^r-\sum_i(\lambda_i\alpha)^r+(\lambda_i\overline{\alpha})^r\\ &= 1+p^r-\mathrm{Tr}\,\varrho_4(\mathrm{Frob}_p^r)(\alpha^r+\overline{\alpha}^r)\\ &= 1+p^r-\mathrm{Tr}\,\varrho_4(\mathrm{Frob}_p^r)(1+p^r-\#\tilde{E}_{21}(\mathbb{F}_{p^r}))\,.\end{aligned}$$

□

References

[BFGL07] N. Bruin, J. Fernández, J. González, J.-C. Lario, *Rational Points on twists of* $X_0(63)$, Acta Arithmetica, 126.4, 2007.

[Cre97] J. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, 1997. Available online at www.warwick.ac.uk/∼masgaj/book/fulltext/index.html.

[CR62] C. W. Curtis, I. Reiner, *Representation theory of finite groups and associative algebras*, American Mathematical Society, 1962.

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73, 349-366, 1983.

[Kar92] G. Karpilovsky, *Group representations. Volume* 1. *Part B: Introduction to group representations and characters*, Elsevier Science Publishers B.V., 1992.

[Mag] Magma, *The magma computational algebra system*, available from http://magma.maths.usyd.edu.au/magma/.

[MRS07] B. Mazur, K. Rubin, A. Silverberg, *Twisting commutative algebraic groups*, Journal of Algebra 314, 419-438, 2007.

[Ser77] J.-P. Serre, *Linear representations of finite groups*, Springer-Verlag, New York, 1977.

[Ser89] J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, Addison-Wesley Publ. Co., Redding, Mass., 1989.

[Sil08] A. Silverberg, *Applications to cryptography of twisting commutative algebraic groups*, Discrete Applied Mathematics 156, 3122-3138, 2008.

[ST68] J.-P. Serre, J. Tate, *Good reduction of abelian varieties*, The Annals of Mathematics, Vol. 88, No. 3, 492-517, 1968.

[Tat66] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. 2, 134-144, 1966.