Journal de Théorie des Nombres
de Bordeaux **13** (2001), 275–285

Fields of definition of $\mathbb{Q}$-curves

par Jordi QUER

Résumé. Soit C une $\mathbb{Q}$-courbe sans multiplication complexe. Dans cet article, nous caractérisons les corps de nombres K pour lesquels il existe une courbe C' isogène à C dont toutes les isogénies entre les conjuguées par le groupe de Galois sont définies sur K. Nous caractérisons également les courbes C' isogènes à C définies sur un corps de nombres K telles que la variété abélienne $\mathrm{Res}_{K/\mathbb{Q}}$ déduite de C' par restriction des scalaires est un produit de variétés abéliennes de type GL_2.

Abstract. Let C be a $\mathbb{Q}$-curve with no complex multiplication. In this note we characterize the number fields K such that there is a curve C' isogenous to C having all the isogenies between its Galois conjugates defined over K, and also the curves C' isogenous to C defined over a number field K such that the Abelian variety $\mathrm{Res}_{K/\mathbb{Q}}(C'/K)$ obtained by restriction of scalars is a product of Abelian varieties of GL_2-type.

1. Definitions, notation and basic facts

We work in the category of Abelian varieties up to isogeny. $\mathrm{End}_k(A)$ will denote the $\mathbb{Q}$-algebra of endomorphisms defined over a field k of an Abelian variety A.

For a Galois (profinite) group G all the G-modules are discrete and we always assume that the corresponding cohomological objects are continuous.

A $\mathbb{Q}$-curve is an elliptic curve defined over a number field that is isogenous to all of its Galois conjugates. An Abelian variety of GL_2-type is an Abelian variety A defined over $\mathbb{Q}$ whose $\mathbb{Q}$-algebra of endomorphisms $\mathrm{End}_{\mathbb{Q}}(A)$ is a number field of degree equal to its dimension (these are the *primitive* Abelian varieties of GL_2-type of Ribet's definition in 1.1).

Both families appear in generalizations of the Shimura-Taniyama conjecture: the $\mathbb{Q}$-curves are conjecturally the elliptic curves $C/\overline{\mathbb{Q}}$ for which there is a nontrivial morphism $X_1(N) \to C$; the Abelian varieties of GL_2-type are

Manuscrit reçu le 28 octobre 1999.
Research partially supported by DGICYT PB96-0970-C02-02 grant.

conjecturally the varieties $\mathbb{Q}$-isogenous to a $\mathbb{Q}$-simple factor of some $J_1(N)$. The two conjectures are equivalent as a consequence of the following

Theorem 1.1 (Ribet [4]). *An elliptic curve over $\overline{\mathbb{Q}}$ is a $\mathbb{Q}$-curve if, and only if, it is a quotient of some Abelian variety of* GL_2*-type.*

We will only consider $\mathbb{Q}$-curves with no complex multiplication, the study of the complex multiplication case requiring different techniques.

Let $C/\overline{\mathbb{Q}}$ be a $\mathbb{Q}$-curve. We will say that C is *completely defined* over a number field K if all the Galois conjugates of C and the isogenies between them are defined over K.

Let $K/\mathbb{Q}$ be a Galois extension such that C is completely defined over K. For every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ choose an isogeny $\phi_\sigma : {}^\sigma C \to C$. The map

$$c_K(\sigma, \tau) = \phi_\sigma {}^\sigma\phi_\tau \phi_{\sigma\tau}^{-1}, \qquad \sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q}),$$

is a two-cocycle of the group $\mathrm{Gal}(K/\mathbb{Q})$ with values in the group $\mathbb{Q}^*$, identified with the nonzero elements of $\mathrm{End}(C)$, and viewed as a Galois module with trivial action. Another choice of isogenies between Galois conjugates or the change of C by a curve K-isogenous to it modifies the two-cocycle c_K by a coboundary. Hence, the cohomology class $[c_K] \in H^2(K/\mathbb{Q}, \mathbb{Q}^*)$ depends only on the K-isogeny class of the curve C.

Fix an invariant differential ω defined over K for the curve C/K, and take its conjugates as invariant differentials for the conjugate curves. For every isogeny $\phi_\sigma : {}^\sigma C \to C$, defined over K, let $\lambda_\sigma \in K^*$ be determined by

$$\phi_\sigma^*(\omega) = \lambda_\sigma {}^\sigma\omega. \tag{1}$$

Then

$$\lambda_\sigma {}^\sigma\lambda_\tau \lambda_{\sigma\tau}^{-1} = \phi_\sigma {}^\sigma\phi_\tau \phi_{\sigma\tau}^{-1} = c_K(\sigma, \tau).$$

This shows that the cocycle c_K, viewed with images in the $\mathrm{Gal}(K/\mathbb{Q})$-module K^*, is a coboundary. In other words, the image of the cocycle class $[c_K]$ in the group $H^2(K/\mathbb{Q}, K^*) = \mathrm{Br}(K/\mathbb{Q})$ is trivial.

Let c be the inflation of the two-cocycle c_K to $G_\mathbb{Q}$. The cohomology class $[c] \in H^2(G_\mathbb{Q}, \mathbb{Q}^*)$ depends only on the isogeny class of C and has trivial image in the Brauer group $H^2(G_\mathbb{Q}, \overline{\mathbb{Q}}^*) = \mathrm{Br}(\mathbb{Q})$. In [5] Ribet used the two-cocycle class $[c]$ for giving a characterization of the smallest field of definition for $\mathbb{Q}$-curves up to isogeny:

Theorem 1.2 (Ribet [5]). *A $\mathbb{Q}$-curve is isogenous to a curve defined over a number field K if, and only if, the cocycle class $[c]$ is in the kernel of the restriction map*

$$\mathrm{Res} : H^2(G_\mathbb{Q}, \mathbb{Q}^*) \to H^2(G_K, \mathbb{Q}^*).$$

This result can also be deduced from results by Elkies using a completely different argument. Our aim in the next section is to investigate the analogous situation for fields of complete definition.

2. Minimal fields of complete definition

Theorem 2.1. *A $\mathbb{Q}$-curve is isogenous to a curve completely defined over a Galois number field K if, and only if, the cocycle class $[c]$ is in the image of the inflation map*

$$\mathrm{Inf} : H^2(K/\mathbb{Q}, \mathbb{Q}^*) \to H^2(G_{\mathbb{Q}}, \mathbb{Q}^*).$$

Moreover, if $[c] = \mathrm{Inf}\,\xi$ for an element $\xi \in H^2(K/\mathbb{Q}, \mathbb{Q}^*)$ then there is such an isogenous curve having $[c_K] = \xi$.

Proof. The if part being obvious, let C be a $\mathbb{Q}$-curve whose attached two-cocycle $[c]$ is the inflation of some element $\xi \in H^2(K/\mathbb{Q}, \mathbb{Q}^*)$. Then $[c]$ is also in the kernel of the restriction map to $H^2(G_K, \mathbb{Q}^*)$ and, applying Ribet's theorem 1.2, we may assume, up to isogeny, that the curve C is defined over K.

Let c be the two-cocycle constructed from a locally constant set of isogenies $\phi_\sigma : {}^\sigma C \to C$ between the conjugates of C and let $\lambda_\sigma \in \overline{\mathbb{Q}}^*$ be such that $\phi_\sigma^*(\omega) = \lambda_\sigma {}^\sigma\omega$ for an invariant differential ω defined over K of C/K.

Consider the commutative diagram

$$\begin{tikzcd}
 & & 1 \arrow[d] \\
H^1(K/\mathbb{Q}, K^*/\mathbb{Q}^*) \arrow[r, "\delta"] & H^2(K/\mathbb{Q}, \mathbb{Q}^*) \arrow[r, "\iota_*"] \arrow[d, "\mathrm{Inf}"] & \mathrm{Br}(K/\mathbb{Q}) \arrow[d, "\mathrm{Inf}"] \\
 & H^2(G_{\mathbb{Q}}, \mathbb{Q}^*) \arrow[r, "\iota_*"] & \mathrm{Br}(\mathbb{Q})
\end{tikzcd}$$

where the first row is the cohomology exact sequence corresponding to the Galois module exact sequence

$$1 \longrightarrow \mathbb{Q}^* \xrightarrow{\iota} K^* \longrightarrow K^*/\mathbb{Q}^* \longrightarrow 1.$$

Since $\mathrm{Inf}(\xi) = [c]$ and $\iota_*([c])$ is trivial, then $\mathrm{Inf}\,\iota_*(\xi)$ is trivial and $\iota_*(\xi)$ is trivial. Hence ξ is in the image of the boundary map δ and there is a one-cocycle $\sigma \mapsto \mu_\sigma : \mathrm{Gal}(K/\mathbb{Q}) \to K^*/\mathbb{Q}^*$ with $\xi = \delta([\mu])$. Let us denote also by μ any lift with values in K^* of the one-cocycle $G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q}) \to K^*/\mathbb{Q}^*$ obtained by inflation.

Let $b_\sigma = \mu_\sigma \lambda_\sigma^{-1}$. The map $(\sigma, \tau) \mapsto b_\sigma {}^\sigma b_\tau b_{\sigma\tau}^{-1}$ is a two-cocycle of $G_{\mathbb{Q}}$ with values in $\mathbb{Q}^*$ whose cohomology class in $H^2(G_{\mathbb{Q}}, \mathbb{Q}^*)$ is $(\mathrm{Inf}\,\xi)[c]^{-1} = 1$, hence it is a coboundary; changing the choice of isogenies ϕ_σ according to this coboundary we may assume that this two-cocycle is in fact the trivial map. Then the map $\sigma \mapsto b_\sigma$ is a one-cocycle of $G_{\mathbb{Q}}$ with values in $\overline{\mathbb{Q}}^*$. By Hilbert's Theorem 90 there is an element of $\overline{\mathbb{Q}}^*$, that we may write as $\sqrt{\gamma}$ for some $\gamma \in \overline{\mathbb{Q}}^*$, such that $b_\sigma = {}^\sigma\sqrt{\gamma}\sqrt{\gamma}^{-1}$ for every $\sigma \in G_{\mathbb{Q}}$. If $\sigma \in G_K$

then both λ_σ and μ_σ are rational numbers, b_σ is also a rational number, and ${}^\sigma\gamma\gamma^{-1} = b_\sigma^2$ is a positive rational number; taking the norm from a number field containing γ it follows that it is a root of unity, hence it must be 1. Then ${}^\sigma\gamma = \gamma$ for every $\sigma \in G_K$ and $\gamma \in K^*$.

Let C' be the K-twist of the curve C corresponding to the field $K(\sqrt{\gamma})$, and let $\phi : C' \to C$ be an isomorphism. The kernel of the map $\sigma \mapsto {}^\sigma\phi\phi^{-1} : G_K \to \{\pm 1\}$ has the field $K(\sqrt{\gamma})$ as its fixed field and we may choose an invariant differential ω' for C'/K such that $\phi^*(\omega) = \sqrt{\gamma}\,\omega'$.

We claim that the curve C' is completely defined over K and has attached two-cocycle class $[c_K] = \xi$. Choose $\psi_\sigma = \phi^{-1}\phi_\sigma{}^\sigma\phi$ as isogenies between the conjugates of C'. Then

$$\psi_\sigma^*(\omega') = (\phi^{-1}\phi_\sigma{}^\sigma\phi)^*(\omega') = \sqrt{\gamma}^{-1}\lambda_\sigma{}^\sigma\sqrt{\gamma}\ {}^\sigma\omega' = \mu_\sigma\ {}^\sigma\omega'.$$

The isogenies ψ_σ are defined over the field $K(\mu_\sigma) = K$ and the two-cocycle $c_K(\sigma,\tau) = \psi_\sigma{}^\sigma\psi_\tau\psi_{\sigma\tau}^{-1}$ is $\mu_\sigma{}^\sigma\mu_\tau\mu_{\sigma\tau}^{-1}$, hence $[c_K] = \xi$. □

3. Restriction of scalars and GL_2-type

In his proof of Theorem 1.1 Ribet starts with an arbitrary $\mathbb{Q}$-curve C and he shows the existence of a Galois extension $K/\mathbb{Q}$ over which the curve is completely defined, and such that the Abelian variety $B = \mathrm{Res}_{K/\mathbb{Q}}(C/K)$ obtained by restriction of scalars has some $\mathbb{Q}$-simple factor of GL_2-type.

In this section we find necessary and sufficient conditions on the curve C and the field K for the variety B being a product of Abelian varieties of GL_2-type. We remark that, since the zeta functions of the curve C/K and of the variety $B/\mathbb{Q}$ are the same, the curves having this property are, assuming the generalized Shimura-Taniyama conjecture, the elliptic curves over a number field whose zeta functions are products of L-series of classical modular forms for congruence subgroups $\Gamma_1(N)$.

Let C/K be a $\mathbb{Q}$-curve defined over a number field K of degree $[K:\mathbb{Q}] = n$ and let $B = \mathrm{Res}_{K/\mathbb{Q}}(C/K)$ be the Abelian variety obtained by restriction of scalars. Let Σ be a set of representatives of right cosets of $G_\mathbb{Q}$ modulo G_K, $G_\mathbb{Q} = \bigcup_{\sigma\in\Sigma}\sigma G_K$. The elements of Σ correspond to the embeddings $K \to \overline{\mathbb{Q}}$. Over $\overline{\mathbb{Q}}$ the variety B is isomorphic to the product $\prod_{\sigma\in\Sigma}{}^\sigma C$. The full endomorphism algebra of B is

$$\mathrm{End}(B) = \bigoplus_{(\sigma,\tau)\in\Sigma^2} \mathrm{Hom}({}^\sigma C, {}^\tau C),$$

which is a $\mathbb{Q}$-algebra of dimension n^2 since every $\mathrm{Hom}({}^\sigma C, {}^\tau C)$ is a one-dimensional $\mathbb{Q}$-vector space.

Let $S \subset \Sigma$ be a set of representatives of double cosets of $G_\mathbb{Q}$ modulo G_K,

$$G_\mathbb{Q} = \bigcup_{s\in S} G_K s G_K$$

and, for every $s \in S$, let $\Sigma_s \subset \Sigma$ be the representatives of a decomposition of the double coset of s as a disjoint union of right cosets $G_K s G_K = \bigcup_{t\in\Sigma_s} tG_K$, and let $\Sigma'_s \subset G_K$ be a corresponding set of elements $\tau \in G_K$ with $\tau s G_K = tG_K$. For every $s \in S$ choose an isogeny $\phi_s : {}^sC \to C$; then the set

$$\{\ {}^{\sigma\tau}\phi_s,\ |\ s \in S,\ \tau \in \Sigma'_s,\ \sigma \in \Sigma\ \}$$

is a basis of the endomorphism algebra $\mathrm{End}(B)$. The orbit of an isogeny ϕ_s by the action of $G_{\mathbb{Q}}$ contains isogenies in $\mathrm{Hom}({}^{\sigma\tau s}C, {}^{\sigma}C)$ for $\tau \in \Sigma'_s$ and $\sigma \in \Sigma$. Then, the homomorphisms

$$\varphi_s = \sum_{\sigma\in\Sigma}\sum_{\tau\in\Sigma'_s} {}^{\sigma\tau}\phi_s$$

for all elements $s \in S$ such that the isogeny $\phi_s : {}^sC \to C$ is defined over the field ${}^sKK$ are a $\mathbb{Q}$-basis of $\mathrm{End}_{\mathbb{Q}}(B)$, since the elements of $G_{\mathbb{Q}}$ fixing $\mathrm{Hom}({}^{\sigma\tau s}C, {}^{\sigma}C)$ are those in $G_K \cap G_{{}^sK}$.

In particular, $\dim_{\mathbb{Q}} \mathrm{End}_{\mathbb{Q}}(B) \le n$ with equality if, and only if, $K/\mathbb{Q}$ is Galois and all the isogenies between Galois conjugates of the curve C are defined over K. In this case the set $\Sigma = S$ may be identified with $\mathrm{Gal}(K/\mathbb{Q})$ and one checks the formula

$$\varphi_\sigma\varphi_\tau = c(\sigma,\tau)\varphi_{\sigma\tau}, \quad \sigma,\tau \in \mathrm{Gal}(K/\mathbb{Q}),$$

showing that the endomorphism algebra $\mathrm{End}_{\mathbb{Q}}(B)$ is isomorphic to the twisted group algebra $\mathbb{Q}^{[c_K]}[G]$.

Theorem 3.1. *Let C/K be a $\mathbb{Q}$-curve defined over a number field K. Then, $\mathrm{Res}_{K/\mathbb{Q}}(C/K)$ is $\mathbb{Q}$-isomorphic to a product of Abelian varieties of GL_2-type if, and only if, $K/\mathbb{Q}$ is Galois Abelian, C is completely defined over K, and $[c_K]$ is in the kernel of the map*

$$\iota_* : H^2(K/\mathbb{Q}, \mathbb{Q}^*) \to H^2(K/\mathbb{Q}, \overline{\mathbb{Q}}^*)$$

induced by the embedding $\iota : \mathbb{Q}^* \to \overline{\mathbb{Q}}^*$, with $\overline{\mathbb{Q}}^*$ viewed as a module with trivial action.

Proof. If an Abelian variety $B/\mathbb{Q}$ is a product of varieties of GL_2-type over $\mathbb{Q}$ then $\dim_{\mathbb{Q}} \mathrm{End}_{\mathbb{Q}}(B) \ge \dim B$ with equality if, and only if, all the varieties in the decomposition are pairwise non-isogenous or, equivalently, the algebra $\mathrm{End}_{\mathbb{Q}}(B)$ is commutative. In case that B is obtained from a $\mathbb{Q}$-curve by restriction of scalars we have seen that $\dim_{\mathbb{Q}} \mathrm{End}_{\mathbb{Q}}(B) \le \dim B$ with equality if, and only if, $K/\mathbb{Q}$ is Galois and the curve is completely defined over K.

Then, if $B = \mathrm{Res}_{K/\mathbb{Q}}(C/K)$ is a product of Abelian varieties of GL_2-type we must have $\dim_{\mathbb{Q}} \mathrm{End}_{\mathbb{Q}}(B) = \dim B$, $K/\mathbb{Q}$ is Galois, C is completely defined over K, and $\mathrm{End}_{\mathbb{Q}}(B)$ is a commutative algebra. Conversely, if $K/\mathbb{Q}$ is Galois, C is completely defined over K and $\mathrm{End}_{\mathbb{Q}}(B)$ is a commutative algebra (of dimension equal to n) then the decomposition of this algebra as a product of number fields induces a $\mathbb{Q}$-decomposition of B as a product of Abelian varieties of GL_2-type.

Then the proof of the theorem comes from a general fact about twisted group algebras. Namely, that given a cohomology class $\xi \in H^2(G,\mathbb{Q}^*)$ the twisted group algebra $\mathbb{Q}^\xi[G]$ is commutative if, and only if, the group G is Abelian and the element ξ has trivial image in the Schur multiplier group $H^2(G,\overline{\mathbb{Q}}^*)$ (see proposition 5.2 of [3]). □

4. Galois cohomological computations

Let C be a $\mathbb{Q}$-curve and let $\{\phi_\sigma\}_{\sigma\in G_\mathbb{Q}}$ be a (locally constant) set of isogenies between its Galois conjugates. For every $\sigma \in G_\mathbb{Q}$ let $d(\sigma) = \deg(\phi_\sigma) \pmod{\mathbb{Q}^{*2}}$ be the degree of the isogeny ϕ_σ up to squares of rational numbers. The map $d : G_\mathbb{Q} \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ is a group homomorphism that depends only on the isogeny class of the curve C. We call it the *degree map* corresponding to the curve C.

Let K_d be the fixed field of $\ker d$. It is a compositum of quadratic fields.

Lemma 4.1. *Let C be a $\mathbb{Q}$-curve with associated $[c] \in H^2(G_\mathbb{Q},\mathbb{Q}^*)$ and let d be the corresponding degree map. The map*

$$(\sigma,\tau) \mapsto \sqrt{d(\sigma)}^\sigma \sqrt{d(\tau)}\sqrt{d(\sigma\tau)}^{-1}, \qquad \sigma,\tau \in G_\mathbb{Q},$$

is a two-cocycle of $G_\mathbb{Q}$ with values in $\mathbb{Q}^*$ whose cohomology class is $[c]$.

Proof. Let $\{\phi_\sigma\}$ be a locally constant set of isogenies between the conjugates of C and let $\lambda_\sigma \in \overline{\mathbb{Q}}^*$ be the elements as in (1) corresponding to an invariant differential of $C/\overline{\mathbb{Q}}$. The map $\sigma \mapsto \lambda_\sigma^2/\deg(\phi_\sigma)$ is a one-cocycle of $G_\mathbb{Q}$ with values in $\overline{\mathbb{Q}}^*$. By Hilbert's Theorem 90 there is an element $\gamma \in \overline{\mathbb{Q}}^*$ such that $\lambda_\sigma^2 = \deg(\phi_\sigma)^\sigma\gamma\gamma^{-1}$ for every $\sigma \in G_\mathbb{Q}$. Fix a square root $\sqrt{\gamma} \in \overline{\mathbb{Q}}^*$. For every $\sigma \in G_\mathbb{Q}$ one has $\lambda_\sigma = \pm\sqrt{\deg(\phi_\sigma)}\ {}^\sigma\sqrt{\gamma}\sqrt{\gamma}^{-1}$. Hence, the two maps $\sigma \mapsto \lambda_\sigma$ and $\sigma \mapsto \sqrt{d(\sigma)}$, viewed as one-cocycles with values in $\overline{\mathbb{Q}}^*/\mathbb{Q}^*$, are cohomologous, and determine the same element of $H^1(G_\mathbb{Q},\overline{\mathbb{Q}}^*/\mathbb{Q}^*)$. The image of this element in $H^2(G_\mathbb{Q},\mathbb{Q}^*)$ by the coboundary map is equal to $[c]$ and is also equal to the cohomology class of the two-cocycle of the statement. □

Taking degrees in the definition of the two-cocycle c_K one sees that its square is a coboundary, hence $[c_K]$ belongs to the 2-torsion subgroup $H^2(K/\mathbb{Q},\mathbb{Q}^*)[2]$. Let G be the group $\mathrm{Gal}(K/\mathbb{Q})$ or $G_\mathbb{Q}$ (or any profinite group). There is a natural decomposition

$$H^2(G,\mathbb{Q}^*)[2] \simeq H^2(G,\{\pm 1\}) \times \mathrm{Hom}(G,P/P^2) \tag{2}$$

where P denotes the subgroup of positive numbers of $\mathbb{Q}^*$. Under this decomposition a cocycle class $[c]$ corresponds to the pair $([c^{\pm}], d)$, where $c^{\pm}$ is the two-cocycle with values in $\{\pm 1\}$ giving the sign of c and d is determined by the identity $c(\sigma,\tau)^2 = d(\sigma)d(\tau)d(\sigma\tau)^{-1}$. We will call $[c^{\pm}]$ the *sign component* and d the *degree component* of the cohomology class $[c]$. We identify as usual the group $H^2(G_{\mathbb{Q}}, \{\pm 1\})$ with the 2-torsion subgroup $\mathrm{Br}(\mathbb{Q})[2]$.

We say that two sets of elements $a_1, \dots, a_m, d_1, \dots, d_m \in \mathbb{Q}^*/\mathbb{Q}^{*2}$ such that $K = \mathbb{Q}(\{\sqrt{a_i}\})$ and the d_i generate the image of the degree map are *dual bases with respect to the degree map* d if there are elements $\sigma_1, \dots, \sigma_m \in G_{\mathbb{Q}}$ with $d(\sigma_i) = d_i$ and ${}^{\sigma_i}\sqrt{a_j} = \delta_{ij}\sqrt{a_j}$.

Proposition 4.2. *Let C be a $\mathbb{Q}$-curve and let $a_1, \dots, a_n$ and $d_1, \dots, d_n$ be dual bases with respect to the corresponding degree map. Then the cohomology class $[c^{\pm}] \in \mathrm{Br}(\mathbb{Q})[2]$ is the product of quaternion algebras*

$$\prod (a_i, d_i). \tag{3}$$

Proof. By lemma 4.1 the sign component $[c^{\pm}]$ of the cohomology class $[c]$ is the class of the two-cocycle

$$(\sigma,\tau) \mapsto \frac{{}^{\sigma}\sqrt{d(\tau)}}{\sqrt{d(\tau)}}, \quad \sigma,\tau \in G_{\mathbb{Q}},$$

and the formula follows by straightforward computation (see [3] for details). □

Using the results of this section we can give a lot of information about the fields satisfying theorems 1.2, 2.1 and 3.1.

Fields of definition. The restriction map $\mathrm{Res} : H^2(G_{\mathbb{Q}}, \mathbb{Q}^*) \to H^2(K/\mathbb{Q}, \mathbb{Q}^*)$ has a sign and a degree components corresponding to the decomposition (2). To trivialize the degree component it is necessary and sufficient that the field K contains the field K_d. The sign component is also trivialized by the field K_d as it is obvious from the formula of proposition 4.2.

Hence the field K_d is the smallest possible field of definition for the curve C up to isogeny.

Fields of complete definition. The inflation map $\mathrm{Inf} : H^2(K/\mathbb{Q}, \mathbb{Q}^*) \to H^2(G_{\mathbb{Q}}, \mathbb{Q}^*)$ has a sign and a degree components corresponding to the decomposition (2). The degree component of $[c]$ belongs to the image of the inflation map if, and only if, the field K contains the field K_d. The condition for the sign component is more complicated: the group $H^2(K/\mathbb{Q}, \{\pm 1\})$ must contain an element ξ whose inflation to $H^2(G_{\mathbb{Q}}, \{\pm 1\})$ is the product of quaternion algebras (3). This condition can be interpreted in terms of embedding problems in Galois theory: the elements of $H^2(K/\mathbb{Q}, \{\pm 1\})$ classify the double covers of the group $\mathrm{Gal}(K/\mathbb{Q})$ and the inflation of each element to $H^2(G_{\mathbb{Q}}, \{\pm 1\})$ is the obstruction to the solvability of the corresponding embedding problem.

Hence the Galois number fields K over which the curve C can be completely defined up to isogeny are the fields containing K_d as a subfield and such that there is a double cover of $\mathrm{Gal}(K/\mathbb{Q})$ whose corresponding embedding problem has obstruction given by (3).

An example of a field having this property is the field $K_d(\{\sqrt{d(\sigma)}\})$ obtained adjoining to K_d the square roots of the degrees of the isogenies between Galois conjugates of the curve. It is a compositum of at most $2m$ quadratic fields if K_d is a compositum of m quadratic fields. In some cases the curve C can be completely defined up to isogeny over a smaller field; for example, if the product of quaternion algebras (3) is trivial in the Brauer group then the curve can be completely defined up to isogeny over the field K_d.

In general there is no smallest field over which C can be completely defined up to isogeny, but many different minimal fields having that property. Restriction of scalars a product of GL_2-type. Let $K/\mathbb{Q}$ be Galois Abelian and let C be completely defined over K. Then K must contain K_d as a subfield. The element $\iota_*([c_K])$ in $H^2(K/\mathbb{Q}, \overline{\mathbb{Q}}^*)$ is the product of the images of the sign component and of the degree component. The image of the degree component is obviously always trivial. As for the image of the sign component triviality is equivalent to the existence of a map $\sigma \mapsto \beta(\sigma) : \mathrm{Gal}(K/\mathbb{Q}) \to \overline{\mathbb{Q}}^*$ with

$$c_K^{\pm}(\sigma, \tau) = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1}.$$

The square of such a map must be a character $\varepsilon = \beta^2 : \mathrm{Gal}(K/\mathbb{Q}) \to \overline{\mathbb{Q}}^*$ and the map β can be recovered (up to a coboundary) from the character just defining $\beta(\sigma) = \sqrt{\varepsilon(\sigma)}$. Let K_ε be the field fixed by the kernel of the character ε.

What we have seen is that the triviality of $\iota_*([c_K])$ is equivalent to the existence of a character ε of $\mathrm{Gal}(K/\mathbb{Q})$ such that $[c_K^{\pm}]$ is the cohomology class of the two-cocycle

$$c_\varepsilon(\sigma, \tau) = \sqrt{\varepsilon(\sigma)}\sqrt{\varepsilon(\tau)}\sqrt{\varepsilon(\sigma\tau)}^{-1}. \tag{4}$$

Such a two-cocycle can be inflated from a two-cocycle of the group $\mathrm{Gal}(K_\varepsilon, \{\pm 1\})$ and the corresponding element of $H^2(K_\varepsilon/\mathbb{Q}, \{\pm 1\})$ is associated to the problem of embedding the cyclic extension $K_\varepsilon/\mathbb{Q}$ into a cyclic extension of double degree.

From the previous remarks and using theorems 2.1 and 3.1 one obtains the following

Corollary 4.3. *Let C be a $\mathbb{Q}$-curve. There is a $\mathbb{Q}$-curve C' isogenous to C, completely defined over an Abelian number field K such that* $\mathrm{Res}_{K/\mathbb{Q}}(C'/K)$

is a product of Abelian varieties of of GL_2*-type if, and only if, the field* K *contains the field* K_d *and also contains a cyclic extension* $K_\varepsilon/\mathbb{Q}$ *such that the obstruction to embedding* K_ε *into a cyclic extension of double degree is the product of quaternion algebras (3).*

Every element of $H^2(G_\mathbb{Q}, \{\pm 1\})$ can be realized as the obstruction to embedding cyclic extensions of $\mathbb{Q}$ into cyclic extensions of double degree. Hence it is always possible to find fields satisfying the properties of the corollary and elliptic curves isogenous to a given one with restriction of scalars a product of varieties of GL_2-type. For more details about the fields satisfying the properties of the corollary and for the splitting of the varieties B as a product of varieties of GL_2-type see [3].

5. Examples: quadratic $\mathbb{Q}$-curves of degree 2

In this section we give some examples illustrating the results of previous sections. For a non-square rational number t the elliptic curve with Weierstrass equation

$$C_t : Y^2 = X^3 - 6(5 + 3\sqrt{t})X + 8(7 + 9\sqrt{t})$$

is a $\mathbb{Q}$-curve defined over the field $K_d = \mathbb{Q}(\sqrt{t})$ with an isogeny $\phi_\sigma : {}^\sigma C_t \to C_t$ of degree 2. Here σ denotes the nontrivial automorphism of K_d. Moreover, every elliptic curve defined over a quadratic field and having an isogeny of degree 2 to its Galois conjugate is isogenous to a curve C_t for some value of t. This is because the curves C_t have been obtained by parametrizing the rational points of the genus zero curve $X_0(2)/W_2$ quotient of the modular curve classifying isogenies of degree 2 between elliptic curves by the Atkin-Lehner involution W_2; see [1] for a description of the parametrization of $\mathbb{Q}$-curves by rational points of modular curves. The curve C_t has no complex multiplication except for ten values of t

$$t = \frac{5}{4}, \frac{8}{9}, \frac{49}{48}, \frac{80}{81}, \frac{325}{324}, \frac{2400}{2401}, \frac{9800}{9801}, \frac{25921}{25920}, \frac{777925}{777924}, \frac{96059600}{96059601},$$

where it has complex multiplications, respectively, by the order of discriminant

$$D = -20, -24, -36, -40, -52, -72, -88, -100, -148, -232.$$

From now on, we assume that C_t has no complex multiplication, *i.e.*, that t is a non-square rational number not among the ten values listed above. If K is a number field containing K_d and $\gamma \in K^*$ we denote by $C_{t,\gamma}$ the K-twist of the curve C_t over the field $K(\sqrt{\gamma})$; it may be given by the Weierstrass equation

$$C_{t,\gamma} : Y^2 = X^3 - 6(5 + 3\sqrt{t})\gamma^2 X + 8(7 + 9\sqrt{t})\gamma^3.$$

Using proposition 4.2 one computes the sign component of the cohomology class $[c]$ attached to the curve C_t to be

$$[c^{\pm}] = (t, 2).$$

Let ω be an invariant differential defined over K_d for C_t/K_d. Using Vélu's explicit formulas for isogenies between elliptic curves given by Weierstrass equations it is easy to compute

$$\phi_\sigma^*(\omega) = \sqrt{-2}\ ^\sigma\omega,$$

and deduce that the isogeny ϕ_σ is defined over the field $\mathbb{Q}(\sqrt{t}, \sqrt{-2})$. The K_d-twist $C_{t,\sqrt{t}}$ has the isogeny to its conjugate defined over the field $\mathbb{Q}(\sqrt{t}, \sqrt{2})$.

The curve C_t is isomorphic to a curve completely defined over the field K_d if, and only if, the cohomology group $H^2(K_d/\mathbb{Q}, \{\pm 1\})$ contains an element whose inflation to $\mathrm{Br}(\mathbb{Q})[2]$ is the class of the quaternion algebra $(t, 2)$. The group $H^2(K_d/\mathbb{Q}, \{\pm 1\})$ has two elements, the nontrivial one corresponds to the double cover of the group $\mathrm{Gal}(K_d/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ by a cyclic group of order 4, and its inflation to $\mathrm{Br}(\mathbb{Q})[2]$ is the class of the quaternion algebra $(t, -1)$. Hence, the curve C_t can be completely defined over K_d up to isogeny if, and only if, one of the quaternion algebras $(t, 2)$ or $(t, -2)$ is a matrix algebra.

Assume that $(t, 2) = 1$ in $\mathrm{Br}(\mathbb{Q})[2]$. Let a, b rational numbers such that $a^2 - tb^2 = 2$. Then the K_d-twist $C_{t,\gamma}$ of C_t with $\gamma = tb + a\sqrt{t}$ is completely defined over K_d and $B = \mathrm{Res}_{K_d/\mathbb{Q}}(C_{t,\gamma})$ is an Abelian surface of GL_2-type with $\mathrm{End}_{\mathbb{Q}}(B) \simeq \mathbb{Q}(\sqrt{2})$. Analogously, if $(t, -2) = 1$ in $\mathrm{Br}_2(\mathbb{Q})[2]$ and a, b are rational numbers with $a^2 - tb^2 = -2$, then the K_d-twist $C_{t,\gamma}$ with $\gamma = a + b\sqrt{t}$ is completely defined over K_d and $B = \mathrm{Res}_{K_d/\mathbb{Q}}(C_{t,\gamma})$ is an Abelian surface of GL_2-type with $\mathrm{End}_{\mathbb{Q}}(B) \simeq \mathbb{Q}(\sqrt{-2})$.

Let $t = 5$. Since $(5, 2)$ and $(5, -2)$ are (isomorphic) division algebras there is no curve isogenous to C_5 completely defined over K_d. Let $K = K_\varepsilon = \mathbb{Q}(\sqrt{\frac{5+\sqrt{5}}{2}})$ be the cyclic extension of $\mathbb{Q}$ of degree 4 and conductor 20, which is a quadratic extension of K_d. Then K_ε can not be embedded into a cyclic extension of degree 8 and the obstruction to such an embedding is precisely $(5, -2)$. In other words, if $\varepsilon : \mathrm{Gal}(K_\varepsilon/\mathbb{Q}) \to \overline{\mathbb{Q}}^*$ is a character of order 4, then the two-cocycle c_ε defined by (4) has $\mathrm{Inf}([c_\varepsilon]) = (5, -2)$. By corollary 4.3 we know that the curve C_5 is isogenous to a curve completely defined over the field K whose restriction of scalars is a product of varieties of GL_2-type. In order to find such a curve we proceed as follows: let $L = K(\sqrt{-2})$, the curve C_5 is completely defined over L, let $[c_L^{\pm}]$ be the corresponding two-cocycle class, and let $[c_\varepsilon]$ denote the inflation to $\mathrm{Gal}(L/\mathbb{Q})$ of the element of $H^2(K/\mathbb{Q}, \{\pm 1\})$ defined by (4). Then, the element $[c_\varepsilon][c_L^{\pm}]^{-1} \in H^2(L/\mathbb{Q}, \{\pm 1\})$ has trivial image in the Brauer group $\mathrm{Br}(\mathbb{Q})[2]$ and hence determines a solvable embedding problem over the extension $L/\mathbb{Q}$; one finds the following solution

$$\gamma = 2\sqrt{5} + \sqrt{2(5-\sqrt{5})} \in K^*.$$

Then, the K-twist $C_{5,\gamma}$ is completely defined over the field K. Moreover, the Abelian variety $\mathrm{Res}_{K/\mathbb{Q}}(C_{5,\gamma}/K)$ of dimension 4 splits over $\mathbb{Q}$ as a product $A_1 \times A_2$ of two Abelian surfaces of GL_2-type with $\mathrm{End}_{\mathbb{Q}}(A_i) \simeq \mathbb{Q}(\sqrt{-1})$. There are cyclic extensions $K/\mathbb{Q}$ of degree 8 containing K_d such that there is a K-twist $C_{5,\gamma}$ of the curve C_5 completely defined over K such that $B = \mathrm{Res}_{K/\mathbb{Q}}(C_{5,\gamma}/K)$ is a $\mathbb{Q}$-simple Abelian variety of GL_2-type with $\mathrm{End}_{\mathbb{Q}}(B) \simeq \mathbb{Q}(e^{\pi i/8}\sqrt{2})$, but I have not been able to compute an element γ producing such an example.

Let $t = -5$. Then $(-5,2)$ and $(-5,-2)$ are both division algebras and there is no curve isogenous to C_{-5} and completely defined over K_d. Let K_ε be the same cyclic field of the previous paragraph; now K_d is not a subfield of K_ε and the compositum $K = K_d K_\varepsilon$ is an Abelian number field with Galois group isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The cocycle class $[c_\varepsilon] \in H^2(K_\varepsilon/\mathbb{Q}, \{\pm 1\})$ has inflation to $\mathrm{Br}(\mathbb{Q})[2]$ equal to the quaternion algebra $(-5,2)$. Solving the appropriate embedding problem over the field $L = K(\sqrt{2})$ one finds an element

$$\gamma = (1+i)\left(10 + 10\sqrt{5} - 5\sqrt{2(5-\sqrt{5})} - \sqrt{10(5-\sqrt{5})}\right) \in K^*$$

such that the K-twist $C_{-5,\gamma}$ is completely defined over the field K. Moreover, $\mathrm{Res}_{K/\mathbb{Q}}(C_{-5,\gamma})$ splits over $\mathbb{Q}$ as a product $A_1 \times A_2$ of two Abelian varieties of GL_2-type of dimension 4 with $\mathrm{End}_{\mathbb{Q}}(A_i) \simeq \mathbb{Q}(\sqrt{2}, \sqrt{-2})$. In this case it can be shown that there does not exist a field K and a curve C'/K isogenous to C_{-5} with $\mathrm{Res}_{K/\mathbb{Q}}(C'/K)$ being a ($\mathbb{Q}$-simple) Abelian variety of GL_2-type.

References

[1] N. Elkies, *Remarks on elliptic k-curves.* Preprint, 1992.

[2] E. Pyle, *Abelian varieties over $\mathbb{Q}$ with large endomorphism algebras and their simple components over $\overline{\mathbb{Q}}$.* Ph.D. Thesis, Univ. of California at Berkeley, 1995.

[3] J. Quer, *Q-curves and Abelian varieties of* GL_2*-type.* Proc. London Math. Soc. (3) **81** (2000), 285–317.

[4] K. Ribet, *Abelian varieties over $\mathbb{Q}$ and modular forms.* Proceedings of KAIST Mathematics Workshop (1992), 53–79.

[5] K. Ribet, *Fields of definition of Abelian varieties with real multiplication.* Contemp. Math. **174** (1994), 107–118.

Jordi Quer
Dept. Matemàtica Aplicada II
Universitat Politècnica de Catalunya
Pau Gargallo, 5
08028-Barcelona
España
E-mail : quer@ma2.upc.es