UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION
INTERNATIONAL ATOMIC ENERGY AGENCY
INTERNATIONAL CENTRE FOR THEORETICAL PHYSICS
I.C.T.P., P.O. BOX 586, 34100 TRIESTE, ITALY, CABLE: CENTRATOM TRIESTE

SMR.1004/10

SUMMER SCHOOL ON ELLIPTIC CURVES

(11- 29 August 1997)

Splitting 2-cocycles related to $\mathbb{Q}$-curves

J. Quer
Departamento Matematica Aplicada II
Universitat Politecnica de Catalunya
Pau Gargallo 5
08028 Barcelona
Spain

Splitting 2-cocycles related to $\mathbb{Q}$-curves

Jordi Quer

August, 1997

These are notes for a talk to be given in the Summer School on Elliptic Curves (Trieste, August 1997). Some aspects of the theory of elliptic $\mathbb{Q}$-curves are discussed. We find the dimensions and the endomorphism algebras of the abelian varieties of GL_2-type associated to them by explicitly splitting some related 2-cocycles. We also discuss the parametrization of $\mathbb{Q}$-curves by quotients of the modular curve $X_0(N)$, and their fields of definition.

The results are joint work with J. González and J.C. Lario, partially supported by Spanish DGICYT grants PB93-0034 and PB93-0815.

1 $\mathbb{Q}$-curves, abelian varieties of GL_2-type, and modularity

A $\mathbb{Q}$-curve is an elliptic curve defined over $\overline{\mathbb{Q}}$ that is isogenous to all its Galois conjugates. Every elliptic curve isogenous to a $\mathbb{Q}$-curve is also a $\mathbb{Q}$-curve.

Examples:

- Elliptic curves defined over $\mathbb{Q}$, and the curves isogenous to them.
- Elliptic curves with complex multiplication (Shimura, [15]).

Parametrization of $\mathbb{Q}$-curves. Let N be a squarefree integer, and let $X^*(N)$ be the quotient curve of the modular curve $X_0(N)$ by the grup of Atkin-Lehner involutions $\{w_d\}$ for $d \mid N$. Let $X_0(N) \to X^*(N)$ be the corresponding covering. The coordinates of every noncusp point $(j, j_N) \in X_0(N)(\overline{\mathbb{Q}})$ projecting onto a point in $X^*(N)(\mathbb{Q})$ are j-invariants of $\mathbb{Q}$-curves.

In [1] and, using different techniques, in [10], it is proved that every $\mathbb{Q}$-curve without complex multiplication is isogenous to some $\mathbb{Q}$-curve obtained in that way.

In [3] it is shown that:

- There are 43 values of N for which $X^*(N)$ has genus zero. They are products of one, two or three primes.
- There are 38 values of N for which $X^*(N)$ has genus one. They are products of one, two, three or four primes. For all 38 curves, the rank of the Mordell-Weil group over $\mathbb{Q}$ is one.

A general method for computing the j-invariants of the $\mathbb{Q}$-curves parametrized by those 81 curves $X^*(N)$ of genus zero or one is also given in [3].

Elkies [1] conjectured that, for N large enough, all the rational points of $X^*(N)$ should come from cusps and complex multiplication points. Hence, the previous 81 modular curves would parametrize the j-invariants of all the $\mathbb{Q}$-curves without complex multiplication except for a finite number of them.

Abelian varieties of GL_2-type. An abelian variety A defined over $\mathbb{Q}$ is of GL_2-type if the $\mathbb{Q}$-algebra $E = \mathbb{Q} \otimes \mathrm{End}_{\mathbb{Q}}(A)$ of endomorphisms of A defined over $\mathbb{Q}$ is a number field of degree

$$[E : \mathbb{Q}] = \dim A.$$

In particular, such a variety must be $\mathbb{Q}$-simple.

The reason for the name is that for abelian varieties of GL_2-type the Tate module $V_\ell(A) = \mathbb{Q} \otimes T_\ell(A)$ is a free module of rank 2 over the algebra $\mathbb{Q}_\ell \otimes E$, and the Galois action on the ℓ-power torsion of A induces a 2-dimensional representation $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Q}_\ell \otimes E)$.

The correspondence. In [9], Ribet proves that an elliptic curve defined over $\overline{\mathbb{Q}}$ is a quotient of some abelian variety of GL_2-type if, and only if, it is a $\mathbb{Q}$-curve.

In [6], Pyle introduces the "building blocks", higher dimensional analogues of $\mathbb{Q}$-curves, and characterizes them as the factors over $\overline{\mathbb{Q}}$ of abelian varieties of GL_2-type.

Modularity of abelian varieties of GL_2-type. Let $f \in S_2(\Gamma_1(N))$ be a normalized newform, and let $E_f = \mathbb{Q}(\ldots, a_n, \ldots)$ be the number field generated over $\mathbb{Q}$ by its Fourier coefficients. Shimura [14, 16] associates to f an abelian variety A_f with the following properties:

- A_f is defined over $\mathbb{Q}$ and is a $\mathbb{Q}$-simple quotient of $J_1(N)$,
- $\dim A_f = [E_f : \mathbb{Q}]$, and
- $\mathbb{Q} \otimes \mathrm{End}_{\mathbb{Q}}(A_f) = E_f$.

In particular the abelian varieties A_f are of GL_2-type.

In fact, as Ribet shows in [8], the jacobian $J_1(N)$ factors over $\mathbb{Q}$, up to isogeny, as a product of varieties A_f for newforms f of levels dividing N.

In [9] Ribet proves that Serre's conjecture [13, (3.2.4?)] on mod p Galois representations implies that all the abelian varieties of GL_2-type are obtained, up to isogeny, from the Shimura construction; i.e., that every abelian variety of GL_2-type is a $\mathbb{Q}$-simple quotient of some $J_1(N)$.

Modularity of $\mathbb{Q}$-curves. In [5] Mazur says that an elliptic curve C, defined over the field of the complex numbers, possesses a "hyperbolic uniformization of arithmetic type" if there is a non-constant analytic map $X_1(N)_{\mathbb{C}} \to C_{\mathbb{C}}$ for some N. Any such curve must be defined over $\overline{\mathbb{Q}}$ and the existence of a uniformization of that type is equivalent to $C_{\overline{\mathbb{Q}}}$ being a factor of the jacobian $J_1(N)_{\overline{\mathbb{Q}}}$. In that case we just say that C "is modular".

As a consequence of the characterization of $\mathbb{Q}$-curves as the one-dimensional factors over $\overline{\mathbb{Q}}$ of abelian varieties of GL_2-type, and of his results on the modularity of those varieties, Ribet obtains in [9] that

- every modular elliptic curve is a $\mathbb{Q}$-curve, and,
- modulo Serre's conjecture, every $\mathbb{Q}$-curve is modular.

2 Isogenies, 2-cocycles, and twisting

We work in the category of abelian varieties up to isogeny; i.e., we consider the morphisms to be elements of $\mathbb{Q} \otimes \mathrm{Hom}(A, B)$, where $\mathrm{Hom}(A, B)$ are "true" morphisms between abelian varieties. This makes the isogenies invertible.

From now on we will only consider $\mathbb{Q}$-curves without complex multiplication. In particular, for our curves we can identify $\mathbb{Q} \otimes \mathrm{End}(C) = \mathbb{Q}$.

In this section, after some remarks on isogenies between elliptic curves, we introduce the 2-cocycle associated to a $\mathbb{Q}$-curve by Ribet. We will also study the effect of twisting and show that, after twisting the curve, the isogenies between conjugate curves can be defined over the field obtained adjoining the square root of the degree.

Isogenies between elliptic curves. Let $\phi : C' \to C$ be an isogeny between two elliptic curves over $\overline{\mathbb{Q}}$. Then, fixing Weierstrass models for C and C', we can write an equation for ϕ of the form

$$\phi(X, Y) = (F(X), \frac{1}{\lambda} Y\, F'(X))$$

for some rational function $F(X) \in \overline{\mathbb{Q}}(X)$ and a nonzero $\lambda \in \overline{\mathbb{Q}}$. The constant λ is also determined by the identity

$$\phi^*(w_C) = \lambda \cdot w_{C'},$$

where $w_C = (dX)/(2Y)$ is the differential invariant. The following properties are easily seen:

- the constants λ are muliplicative for the composition of isogenies,
- the constant for the isogeny ${}^\sigma\phi$ is ${}^\sigma\lambda$,
- if $m \in \mathbb{Z}$, the constant for the multiplication-by-m isogeny is $\lambda = m$,
- if $\widehat{\phi}$ is the dual isogeny, and $\widehat{\lambda}$ is the corresponding constant, $\widehat{\lambda}\lambda = d = \deg \phi$.

Fields of definition of isogenies. Assume that the two curves C and C' are defined over a number field k. Then, for every $\sigma \in G_k$, ${}^\sigma\phi : C' \to C$ is an isogeny of the same degree and, since we assume no complex multiplication, ${}^\sigma\phi = \pm\phi$. We have in this way an action of G_k on the set $\{\pm\phi\}$. The isogeny ϕ is defined over k if, and only if, that action is trivial and, if not, it is defined over a quadratic extension of that field.

In particular, since

$${}^\sigma\phi(X, Y) = ({}^\sigma F(X), \frac{1}{{}^\sigma\lambda} Y\, {}^\sigma F'(X)) = (F(X), \pm\frac{1}{\lambda} Y\, F'(X)) = \pm\phi(X, Y),$$

we see that the rational function F is always defined over k, and that the isogeny is defined over the field $k(\lambda)$, with $\lambda^2 \in k^*$.

Locally constant sets of isogenies. Let C be a $\mathbb{Q}$-curve. For every $\sigma \in G_\mathbb{Q}$ we choose an isogeny $\mu_\sigma : {}^\sigma C \to C$ in such a way that the set $\{\mu_\sigma\}$ is locally constant; i.e., there is a finite Galois extension $k/\mathbb{Q}$ such that $\mu_\sigma = \mu_\tau$ whenever σ and τ restrict to the same automorphism of k. The smallest possible field k is the Galois closure of the field of definition of the curve C.

2-cocycles. For every pair σ, τ, the two maps $\mu_\sigma \circ {}^\sigma\mu_\tau$ and $\mu_{\sigma\tau}$ are isogenies ${}^{\sigma\tau}C \to C$ and, in absence of complex multiplication, they must differ by a nonzero rational number $c(\sigma,\tau)$,

$$\mu_\sigma \circ {}^\sigma\mu_\tau = c(\sigma,\tau) \circ \mu_{\sigma\tau}.$$

Then, the map $c : G_\mathbb{Q} \times G_\mathbb{Q} \to \mathbb{Q}^*$ is a 2-cocycle for the trivial action of $G_\mathbb{Q}$ on $\mathbb{Q}^*$. A change in the choice of the isogenies μ_σ modifies the cocycle c by a coboundary. Hence, the cohomology class $[c] \in H^2(G_\mathbb{Q}, \mathbb{Q}^*)$ depends only on the curve C, and not on the isogenies.

If λ_σ is the constant associated to μ_σ, we have the corresponding formula

$$\lambda_\sigma \, {}^\sigma\lambda_\tau = c(\sigma,\tau)\, \lambda_{\sigma\tau}.$$

Let K denote a finite Galois extension of $\mathbb{Q}$, containing k, such that all the isogenies μ_σ are defined over K. Then c is the inflation of some cocycle defined over $\mathrm{Gal}(K/\mathbb{Q})$. The smallest possible K is $k(\{\lambda_\sigma\})$, that is an extension of type $(2,\ldots,2)$ of k. From the identity ${}^\sigma\lambda_\tau = c(\sigma,\tau)\lambda_{\sigma\tau}\lambda_\sigma^{-1}$ we see that this field is Galois over $\mathbb{Q}$.

The degree map. For every $\sigma \in G_\mathbb{Q}$ let $d_\sigma \in \mathbb{Q}^*$ denote the degree of the isogeny μ_σ. Then from the formula defining the 2-cocycle, we get

$$d_\sigma \, d_\tau = c(\sigma,\tau)^2 \, d_{\sigma\tau}$$

and the map

$$\delta : G_\mathbb{Q} \to \mathbb{Q}^*/\mathbb{Q}^{*2}, \qquad \sigma \mapsto d_\sigma \pmod{\mathbb{Q}^{*2}},$$

is a group homomorphism. This map does not depend on the locally constant set of isogenies chosen, but only on the curve C.

Its kernel fixes a subfield of the field k of type $(2,\ldots,2)$. We denote it k_0.

Isogenous $\mathbb{Q}$-curves. Let $\phi : C' \to C$ be an isogeny between $\mathbb{Q}$-curves. Then we have isogenies

$${}^\sigma C' \xrightarrow{{}^\sigma\phi} {}^\sigma C \xrightarrow{\mu_\sigma} C \xrightarrow{\phi^{-1}} C'$$

giving a correspondence

$$\{\mu_\sigma\} \leftrightarrow \{\mu'_\sigma = \phi^{-1} \circ \mu_\sigma \circ {}^\sigma\phi\}$$

between the locally constant sets of isogenies for C and for C'. If $\lambda'_\sigma, \lambda_\sigma, \lambda$ are the constants associated to μ'_σ, μ_σ and ϕ,

$$\lambda'_\sigma = \lambda_\sigma \, {}^\sigma\lambda \, \lambda^{-1}.$$

The 2-cocycle associated to the curve C from the locally constant set $\{\mu_\sigma\}$ is the same than that associated to C' from the set $\{\mu'_\sigma\}$. Hence, the cohomology class $[c] \in H^2(G_\mathbb{Q}, \mathbb{Q}^*)$ is an invariant of the isogeny class of the curve.

Since $\deg \mu'_\sigma = \deg \mu_\sigma$, the previous correspondence maintains the degrees of the isogenies. In particular, the map $\delta : G_\mathbb{Q} \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ and the field k_0 are also invariants of the isogeny class.

Note that in the tower of fields

$$\mathbb{Q} \subseteq k_0 \subseteq k \subseteq K,$$

the field k_0 depends on the isogeny class of C, the field k on the curve C, and the field K on the locally constant set of isogenies $\{\mu_\sigma\}$.

A consequence of results in [1] or [9] is that every $\mathbb{Q}$-curve is isogenous to one already defined over the field k_0.

The effect of twisting. Let γ be a nonzero element of k. We denote by C_γ the twisted curve over $k(\sqrt{\gamma})$, and by $\phi_\gamma : C_\gamma \to C$ an isomorphism.

If C is given by a Weierstrass equation $Y^2 = X^3 + AX + B$, then C_γ has equation $Y^2 = X^3 + \gamma^2 AX + \gamma^3 B$, and $\phi_\gamma(X, Y) = (X\gamma^{-1}, Y\gamma^{-3/2})$. Hence, the constant λ associated to ϕ_γ is $\sqrt{\gamma}$ and, under the previous correspondence for locally constant sets of isogenies, we have

$$\lambda'_\sigma = \lambda_\sigma \, {}^\sigma\sqrt{\gamma}\,\sqrt{\gamma}^{-1}.$$

The twisted curve. Let C be a $\mathbb{Q}$-curve. Choose a locally constant set of isogenies $\{\mu_\sigma\}$. Dividing the two equalities

$$d_\sigma \, d_\tau = c(\sigma,\tau)^2 \, d_{\sigma\tau}, \quad \text{and} \quad \lambda_\sigma^2 \, {}^\sigma\lambda_\tau^2 = c(\sigma,\tau)^2 \, \lambda_{\sigma\tau}^2,$$

we obtain

$$\frac{d_\sigma}{\lambda_\sigma^2} \, {}^\sigma\left(\frac{d_\tau}{\lambda_\tau^2}\right) = \frac{d_{\sigma\tau}}{\lambda_{\sigma\tau}^2},$$

and the map $\sigma \mapsto d_\sigma/\lambda_\sigma^2$ is a 1-cocycle on $G_\mathbb{Q}$ with values in k^*. In fact, it comes by inflation from a 1-cocycle defined in $\mathrm{Gal}(k/\mathbb{Q})$. By Hilbert's 90 theorem there exist an element $\gamma \in k^*$ such that

$$\frac{d_\sigma}{\lambda_\sigma^2} = {}^\sigma\gamma\,\gamma^{-1}.$$

Then for the twisted curve C_γ we have

$$\lambda_\sigma'^{\,2} = \lambda_\sigma^2 \, {}^\sigma\gamma\,\gamma^{-1} = d_\sigma$$

and we have proved the:

Theorem 1 *Let C be a $\mathbb{Q}$-curve defined over a Galois extension $k/\mathbb{Q}$. Then, there is a $\gamma \in k^*$ and a locally constant set of isogenies $\{\mu'_\sigma\}$ for the twisted curve C_γ such that every μ'_σ is defined over $k(\sqrt{d_\sigma})$ and has $\lambda'_\sigma = \sqrt{d_\sigma}$.*

In particular, the field K for the twisted curve is the composition of k and the field $\mathbb{Q}(\{\sqrt{d_\sigma}\})$ generated over $\mathbb{Q}$ by the square roots of the degrees of the isogenies between conjugates. Combining this with the results of Elkies and Ribet on the fields of definition of $\mathbb{Q}$-curves, we see that evey $\mathbb{Q}$-curve is isogenous to a curve for which the field K of definition of the curve and the isogenies is of type $(2, \ldots, 2)$.

3 Splitting the cocycles

The abelian varieties of GL_2-type having as a quotient a given $\mathbb{Q}$-curve are in correspondence with the splitting functions of the cocycle c. In this section we describe that correspondence and reduce the splitting of the cocycles to an equality between Brauer classes.

Splitting functions. A splitting function for the 2-cocycle c is a locally constant map

$$\beta : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$$

such that

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

A theorem by Tate [12] shows that these splitting functions must always exist. It is clear that two splitting functions β and β' for the same cocycle c must differ in a Galois character

$$\beta' = \chi\beta, \qquad \chi : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*.$$

If we start with another cocycle c' corresponding to a different choice of isogenies for the same curve, the splitting functions for both cocycles differ in a locally constant map $G_{\mathbb{Q}} \to \mathbb{Q}^*$.

Normalization. Consider the locally constant map $\sigma \mapsto \sqrt{d_\sigma}$, and let c_1 be the cocycle differing from c on its coboundary; i.e.,

$$c_1(\sigma, \tau) = c(\sigma, \tau)\frac{\sqrt{d_{\sigma\tau}}}{\sqrt{d_\sigma}\sqrt{d_\tau}}.$$

The new, normalized 2-cocycle c_1, takes its values into $\{\pm 1\}$. We define the splitting functions β_1 for it in the same way, $c_1(\sigma, \tau) = \beta_1(\sigma)\beta_1(\tau)\beta_1(\sigma\tau)^{-1}$. Then the splitting functions β for c and β_1 for c_1 are related by the identity

$$\beta(\sigma) = \beta_1(\sigma)\sqrt{d_\sigma}.$$

Splitting characters. Let β_1 be a splitting function for the normalized 2-cocycle c_1. Since

$$\beta_1(\sigma)\beta_1(\tau)\beta_1(\sigma\tau)^{-1} = c_1(\sigma, \tau) \in \{\pm 1\},$$

the following map is a Galois character

$$\varepsilon = \beta_1^2, \qquad \varepsilon : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*.$$

A character of the form $\varepsilon = \beta_1^2$ for some splitting function will be called a splitting character for the cocycle c_1.

Let $L/\mathbb{Q}$ be the cyclic extension fixed by the kernel of ε. We will call it a splitting field for the cocycle c_1. The degree $[L : \mathbb{Q}]$ is the order of ε.

Since a splitting function is determined by c_1 only up to multiplying by a Galois character, a splitting character is determined only up to the square of some Galois character.

Minimality. If the character ε has order n, the splitting function β_1 take its values into the $2n$-th roots of unity. We define the index of β_1 as the maximum order of the roots of unity in its image.

It is easy to see that the minimal index for a splitting function β_1 is a power of 2, hence the minimal splitting characters ε (resp. splitting fields L) have order (resp. degree) a power of 2.

There exist splitting functions with odd index if, and only if, the cocycle c is trivial, $c(\sigma, \tau) = 1$. If c is nontrivial, then the index of a minimal splitting function is 2^m for some $m \geqslant 1$ and the order of a minimal splitting character is 2^{m-1}. Moreover, in this case, the index of any β_1 is always twice the order of $\varepsilon = \beta_1^2$.

Endomorphism algebras of abelian varieties of GL_2-type. If β is a splitting function for c, let

$$E_\beta = \mathbb{Q}(\{\beta(\sigma)\})$$

be the field obtained adjoining to $\mathbb{Q}$ the values taken by β. In Ribet [9] and, with a more general and precise formulation, in the thesis of Pyle [6], they show that:

- For every β there exists an abelian variety A_β of GL_2-type, having C as a quotient, with endomorphism algebra $\mathbb{Q} \otimes \mathrm{End}_{\mathbb{Q}}(A_\beta) = E_\beta$.
- Every abelian variety of GL_2-type having C as a quotient is isogenous over $\mathbb{Q}$ to one of the varieties A_β.

Proposition 2 *Let L be a splitting field of degree n corresponding to a splitting function β. Let ζ_{2n} denote a primitive $2n$-th root of unity.*

- *If $L \cap k_0 = \mathbb{Q}$, let $\{d_1, \ldots, d_r\}$ be a basis of $\delta(G_{\mathbb{Q}})$. Then,*

$$E_\beta = \mathbb{Q}(\zeta_{2n}, \sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_r}).$$

- *If $L \cap k_0$ is a quadratic field, let $\sigma \in G_{\mathbb{Q}}$ be any element restricting to a generator of $\mathrm{Gal}(L/\mathbb{Q})$, $d_1 = \deg \mu_\sigma$, and $d_2, \ldots, d_r$ a basis of $\delta(G_L)$. Then,*

$$E_\beta = \mathbb{Q}(\zeta_{2n}\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_r}).$$

PROOF: Consider the equality

$$\beta(\sigma) = \beta_1(\sigma)\sqrt{d_\sigma}.$$

The value of $\sqrt{d_\sigma}$ up to rational numbers depends only on the restriction of σ to k_0, and the value of $\beta_1(\sigma)$ is, up to $\{\pm 1\}$, determined by its square $\varepsilon(\sigma)$, that depends only on the restriction of σ to L.

Then we just write the abelian extension $k_0 L$ as a product of L and of linearly disjoint quadratic extensions. From the corresponding decomposition of $\mathrm{Gal}(k_0 L/\mathbb{Q})$ as a product of cyclic groups, it is then easy to compute the values of $\beta(\sigma)$. □

This proposition shows that the endomorphism algebras E_β depend only on the splitting field L or, what amounts the same, on the splitting character ε. In particular, if 2^s denotes the degree of a minimal splitting character, then the smallest dimension of an abelian variety of GL_2-type having C as a quotient is

$$2^{r+s-1} \quad \text{or} \quad 2^{r+s}$$

depending on whether there exist splitting fields L of degree 2^s with $L \cap k_0 \neq \mathbb{Q}$ or not, and also on whether one of the isogenies between conjugate curves has degree 2, since $\mathbb{Q}(\zeta_{2n})$ contains $\sqrt{2}$ for n large enough.

Characterization of splitting characters. In order to determine the abelian varieties of GL_2-type attached to a given elliptic curve, we must know which characters are splitting characters for a given cocycle c_1.

Let $\varepsilon : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$ be any Galois character whose kernel fixes the field L. Consider the diagram

$$\begin{array}{ccccccccc} & & & & & & G_{\mathbb{Q}} & & \\ & & & & & \swarrow^{\widetilde{\varepsilon}?} & \downarrow{\scriptstyle \varepsilon} & & \\ 1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \overline{\mathbb{Q}}^* & \longrightarrow & \overline{\mathbb{Q}}^* & \longrightarrow & 1. \end{array}$$

Where the map $\overline{\mathbb{Q}}^* \to \overline{\mathbb{Q}}^*$ in the exact sequence is $a \mapsto a^2$.

Let $\sqrt{\varepsilon} \in H^2(G_{\mathbb{Q}}, \{\pm 1\})$ be the element corresponding to the pullback of the exact sequence by ε. It can be interpreted as the obstruction to the existence of a Galois character $\widetilde{\varepsilon}$ commuting the diagram (a square root of the character ε) or also as the obstruction to embedding the cyclic extension $L/\mathbb{Q}$ into a cyclic extension of twice its degree.

Theorem 3 *A Galois character ε is a splitting character for the cocycle c_1 if, and only if,*

$$\sqrt{\varepsilon} = [c_1] \quad in \quad H^2(G_{\mathbb{Q}}, \{\pm 1\}).$$

PROOF: Let $\mathrm{Gal}(K/\mathbb{Q}) = G$, and denote by $\pi : G_{\mathbb{Q}} \to G$ the natural projection. Then the 2-cocycle c_1 is obtained by inflation from a 2-cocycle defined over $\mathrm{Gal}(K/\mathbb{Q})$ that, abusing of the notation, we also call c_1. Consider the cohomology class $[c_1] \in H^2(G, \overline{\mathbb{Q}}^*)$, where $\overline{\mathbb{Q}}^*$ is considered as a G-module with trivial action, and let $\widetilde{G}$ be the corresponding central group extension. Then we have a diagram

$$\begin{array}{ccccccccc} & & & & & & G_{\mathbb{Q}} & & \\ & & & & & \swarrow^{\widetilde{\pi}} & \downarrow{\scriptstyle \pi} & & \\ 1 & \longrightarrow & \overline{\mathbb{Q}}^* & \longrightarrow & \widetilde{G} & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

where the (continuous) group homomorphisms $\widetilde{\pi}$ commuting the diagram are called liftings of π. An easy computation shows that:

Lemma 4 *Let $s : G \to \widetilde{G}, g \mapsto s_g$ be a section of the epimorphism in the previous exact sequence such that $s_g s_h = c(g,h) s_{gh}$ $\forall g, h \in G$. Then*

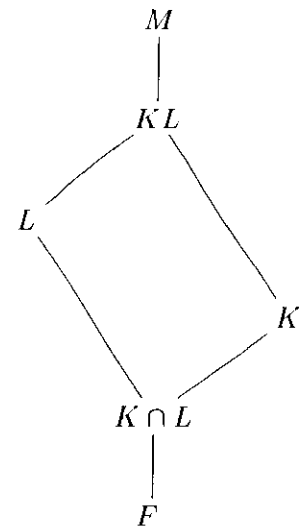
$$\widetilde{\pi}(\sigma) = \beta_1(\sigma)^{-1} s_{\pi(\sigma)}$$

gives a correspondence between splitting functions for c_1 and liftings of π.

The cohomology class $[c_1] \in H^2(G_{\mathbb{Q}}, \{\pm 1\})$ is then the obstruction to the existence of some lifting $\widetilde{\pi}$ whose β_1 has trivial character. The situation is analogous to that in the computation by Tate [12, Sections 6.1, 6.3, and 6.4] of the obstruction to the existence of linear liftings of projective Galois representations, and the proof given there can be adapted to our case.

There is also an alternative approach that works over any base field F, and not only over $\mathbb{Q}$, based in the theory of Galois embedding problems and its cohomological obstructions. If M

denotes the field fixed by the kernel of a lifting $\widetilde{\pi}$, we have a diagram of field extensions



Where the extension M/KL is of degree 1 or 2. Then one identifies the obstructions for the two embedding problems corresponding to the two exact sequences

$$1 \longrightarrow \mathrm{Gal}(M/K) \longrightarrow \mathrm{Gal}(M/F) \longrightarrow \mathrm{Gal}(K/F) \longrightarrow 1,$$

and

$$1 \longrightarrow \mathrm{Gal}(M/KL) \longrightarrow \mathrm{Gal}(M/F) \longrightarrow \mathrm{Gal}(KL/F) \longrightarrow 1.$$

It can be proved that the obstruction to the solvability of the second embedding problem for a given cyclic extension L/F is the product of the cohomology class $[c_1] \in H^2(G_F, \{\pm 1\})$ and the obstruction to embedding L/F into a cyclic extension of twice its degree. □

Local components and Brauer group. The restriction to the decomposition groups give a monomorphism

$$H^2(G_{\mathbb{Q}}, \{\pm 1\}) \to \prod H^2(G_{\mathbb{Q}_p}, \{\pm 1\})$$

For every $\xi \in H^2(G_{\mathbb{Q}}, \{\pm 1\})$ and a (finite or infinite) prime p, we denote by ξ_p its local components. Then, global equality is equivalent to local equality for every p.

We recall the usual identification of $H^2(G_{\mathbb{Q}}, \{\pm 1\})$ with the 2-component of the Brauer group $\mathrm{Br}_2(\mathbb{Q})$, corresponding to central simple algebras that are split under quadratic extension.

If $a, b \in \mathbb{Q}^*$, we denote by $(a, b) \in \mathrm{Br}_2(\mathbb{Q})$ the corresponding quaternion algebra. For a local field $\mathbb{Q}_p$, if we identify $\mathrm{Br}_2(\mathbb{Q}_p) = \{\pm 1\}$, then the local component $(a, b)_p$ is given by the Hilbert symbol.

4 Galois characters with given $\sqrt{\varepsilon}$

For general fields F the obstruction to embedding a cyclic extension L/F into a cyclic extension of twice its degree can be very difficult to compute. There are known formulas giving it as a product of quaternion algebras in the Brauer group $\mathrm{Br}_2(F)$ only for L of small degree. Fortunately, class field theory enables a very easy computation for the case of $F = \mathbb{Q}$.

Local components of $\sqrt{\varepsilon}$. Let $\varepsilon : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$ be a Galois character. Via class field theory we identify it with an idele class character or with a Dirichlet character. Denote by ε_p its restriction to $\mathbb{Q}_p^*$ or to $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ if p^α is the p-power factor of the conductor of ε.

Then, the local component $(\sqrt{\varepsilon})_p$ is the obstruction to the existence of a square root of the character ε_p, and it is given by its parity; i.e.,

$$(\sqrt{\varepsilon})_p = \varepsilon_p(-1).$$

For every finite prime p we define

$$u(p) = \begin{cases} 1, & p = 2, \\ \mathrm{ord}_2(p-1), & p \neq 2. \end{cases}$$

The number of roots of unity of order a power of 2 contained in the field $\mathbb{Q}_p$ is $2^{u(p)}$. For odd p, a character of $\mathbb{Q}_p^*$ is odd if, and only if, it has order divisible by $2^{u(p)}$. For $p = 2$ there exist odd characters of any even order.

Global characters with given local conditions. Given $\xi \in \mathrm{Br}_2(\mathbb{Q})$, let

$$u(\xi) = \max\{\, u(p) \mid \xi_p = -1 \,\}$$

where we consider the local components ξ_p for all finite primes p. We define $u(\xi) = 0$ in case that $\xi = 1$ in $\mathrm{Br}_2(\mathbb{Q})$. The following proposition can be found in [7]:

Proposition 5 *Let $\xi \in \mathrm{Br}_2(\mathbb{Q})$. There exist Galois characters ε of order n with*

$$\sqrt{\varepsilon} = \xi$$

if, and only if, n is a multiple of $2^{u(\xi)}$.

Let $k_1/\mathbb{Q}$ be a quadratic extension, corresponding to a Galois character ε_1. Then, there exist Galois characters ε of order n with

$$\sqrt{\varepsilon} = \xi \quad \textit{and} \quad k_1 \subseteq L$$

if, and only if, the following conditions are satisfied:

- *For every odd prime p,*
  - $\xi_p = -1$ *and* p *ramified in* k_1 $\Rightarrow$ $u(p) = \mathrm{ord}_2(n)$,
  - $\xi_p = -1$ *and* p *unramified in* k_1 $\Rightarrow$ $u(p) < \mathrm{ord}_2(n)$,
  - $\xi_p = 1$ *and* p *ramified in* k_1 $\Rightarrow$ $u(p) > \mathrm{ord}_2(n)$,
- *and, for $p = 2$,*
  - $\xi_2 = -1$ *and* $\varepsilon_1(-1) = -1$ $\Rightarrow$ $\mathrm{ord}_2(n) = 1$,
  - $\xi_2 = -1$ *and* $\varepsilon_1(-1) = 1$ $\Rightarrow$ $\mathrm{ord}_2(n) > 1$,
  - $\xi_2 = 1$ $\Rightarrow$ $\varepsilon_1(-1) = 1$.

For some ξ and k_1, there are no characters satisfying the two conditions $\sqrt{\varepsilon} = \xi$ and $k_1 \subseteq L$ but, when some such character does exist, then there are two possibilities for the orders of the set of characters satisfying them:

- their orders are the numbers n with $\mathrm{ord}_2(n) = u(\xi)$, or
- their orders are the numbers n with

$$u(\xi) < \mathrm{ord}_2\, n < m = \begin{cases} \infty, & \text{only 2 ramifies in } k_1, \\ \min\{u(p) \mid p \text{ odd, ramified in } k_1\}, & \text{otherwise.} \end{cases}$$

5 Computation of $[c_1]$

In this section we compute the element $[c_1] \in \mathrm{Br}_2(\mathbb{Q})$. The computation is done step by step, starting from the easiest case of $\mathbb{Q}$-curves over quadratic fields, until we arrive to the general case, for which an extra auxiliary twisting is nedded in order to do the computation.

Theorem 6 *Let C be a $\mathbb{Q}$-curve. Let $k_0 = \mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_r})$ be the field fixed by the kernel of the δ map. For every i, let $\sigma_i \in G_{\mathbb{Q}}$ be an element acting on k_0 by*

$${}^{\sigma_i}\sqrt{a_j} = \begin{cases} -\sqrt{a_j}, & j = i, \\ \sqrt{a_j}, & j \neq i, \end{cases}$$

and let d_i be the degree of the corresponding isogeny μ_{σ_i}. Then,

$$[c_1] = (a_1, d_1)(a_2, d_2) \cdots (a_r, d_r) \in \mathrm{Br}_2(\mathbb{Q}).$$

PROOF: We may change our curve by an isogenous curve that is already defined over $k = k_0$ and for which the constants λ_σ are $\sqrt{d_\sigma}$, since the a_i, σ_i and d_i are the same for booth curves, and also $[c_1]$ is the same.

Quadratic $\mathbb{Q}$-curves. Assume first that k is a quadratic field, $k = \mathbb{Q}(\sqrt{a})$.

Let d be the degree of a nontrivial isogeny $\mu : {}^{\sigma}C \to C$, with $\lambda = \sqrt{d}$. Let $K = \mathbb{Q}(\sqrt{a}, \sqrt{d})$ denote, as always, the field of definition of the isogeny.

As locally constant set of isogenies for the curve C we may take:

$$\mu_\sigma = \begin{cases} \mu, & \sigma|_k \neq 1, \\ 1, & \sigma|_k = 1. \end{cases}$$

The case $d = a$. In this case $K = k$ is a quadratic field. Let s denote the nontrivial automorphism. Then, the 2-cocycles are given in the following tables

c	1	s
1	1	1
s	1	$-d$

c_1	1	s
1	1	1
s	1	-1

The element $[c_1] \in H^2(G_{\mathbb{Q}}, \{\pm 1\})$ is well known to be the obstruction to embedding the quadratic field $K/\mathbb{Q}$ into a cyclic quartic extension, and this obstruction is equal to

$$(a, -1) = (a, a) = (a, d) \in \mathrm{Br}_2(\mathbb{Q}).$$

The case $d \neq a$. In this case $K/\mathbb{Q}$ is a quartic extension of Klein type. Let s and t denote the generators of $\mathrm{Gal}(K/\mathbb{Q})$ defined by

$$s: \begin{cases} \sqrt{a} \mapsto -\sqrt{a}, \\ \sqrt{d} \mapsto \sqrt{d}, \end{cases} \quad \text{and} \quad t: \begin{cases} \sqrt{a} \mapsto \sqrt{a}, \\ \sqrt{d} \mapsto -\sqrt{d}. \end{cases}$$

Then, the 2-cocycles are given in the following tables

c	1	s	t	st
1	1	1	1	1
s	1	d	1	d
t	1	-1	1	-1
st	1	$-d$	1	$-d$

c_1	1	s	t	st
1	1	1	1	1
s	1	1	1	1
t	1	-1	1	-1
st	1	-1	1	-1

The element $[c_1] \in H^2(G_{\mathbb{Q}}, \{\pm 1\})$ is well known to be the obstruction to embedding the field $K/\mathbb{Q}$ into a dihedral extension of degree 8 cyclic over the quadratic field $\mathbb{Q}(\sqrt{ad})$. This obstruction is given by the quaternion algebra

$$(a, d) \in \mathrm{Br}_2(\mathbb{Q}).$$

The case of k linearly disjoint from $\mathbb{Q}(\{\sqrt{d_s}\})$. We assume in this paragraph that

$$\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_r}) \cap \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_r}) = \mathbb{Q}$$

Then $K/\mathbb{Q}$ is an extension of type $(2, \ldots, 2)$ of degree 2^{2r} and we can choose a basis for

$$\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{Gal}(k/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\{\sqrt{d_\sigma}\})/\mathbb{Q})$$

in the following way:

First, we choose $s_1, \ldots, s_r$ that are a basis for $\mathrm{Gal}(k/\mathbb{Q})$ and are trivial on the other component of the group $\mathrm{Gal}(K/\mathbb{Q})$. Let

$$k = \mathbb{Q}(\sqrt{a_1}) \cdots \mathbb{Q}(\sqrt{a_r})$$

be the corresponding decomposition as a product of linearly disjoint quadratic extensions; i.e., each s_i restricts to the nontrivial automorphism on the component $\mathbb{Q}(\sqrt{a_i})$ and to the identity on the others.

For every i, let $d_i = \deg \mu_{s_i}$, and let t_i be the automorphism of K that acts trivially on the field k and by $\sqrt{d_i} \mapsto -\sqrt{d_i}$ on the field $\mathbb{Q}(\{\sqrt{d_s}\})$. In fact, we have:

$$s_i: \begin{cases} \sqrt{a_i} \mapsto -\sqrt{a_i}, & \\ \sqrt{a_j} \mapsto \sqrt{a_j}, & j \neq i, \\ \sqrt{d_j} \mapsto \sqrt{d_j}, & \forall j, \end{cases} \quad \text{and} \quad t_i: \begin{cases} \sqrt{a_j} \mapsto \sqrt{a_j}, & \forall j, \\ \sqrt{d_i} \mapsto -\sqrt{d_i}, & \\ \sqrt{d_j} \mapsto \sqrt{d_j}, & j \neq i. \end{cases}$$

Now, let's compute the cocycle. Every element $x \in \mathrm{Gal}(K/\mathbb{Q})$ is uniquely written as

$$x = s_1^{x(s_1)} \cdots s_r^{x(s_r)} t_1^{x(t_1)} \cdots t_r^{x(t_r)}, \qquad x(s_i), x(t_i) \in \{0, 1\}.$$

Then, the element λ_x satisfies

$$\lambda_x = \sqrt{d_x} \equiv \prod_{i=1}^{r} \sqrt{d_i}^{x(s_i)} \pmod{\mathbb{Q}^*}$$

and the Galois action of an element $y \in G$ on it is given by

$${}^y\lambda_x = \big(\prod_{i=1}^{r}(-1)^{x(s_i)y(t_i)}\big)\lambda_x.$$

The values of the cocycle c are

$$c(x,y) = \lambda_x {}^x\lambda_y \lambda_{xy}^{-1} = \big(\prod_{i=1}^{r}(-1)^{x(s_i)y(t_i)}\big)\frac{\sqrt{d_x}\sqrt{d_y}}{\sqrt{d_{xy}}},$$

and the cocycle c_1 is given by the formula

$$c_1(x,y) = \prod_{i=1}^{r}(-1)^{x(s_i)y(t_i)}.$$

Define $K_i = \mathbb{Q}(\sqrt{a_i}, \sqrt{d_i})$. The fields K_i are of Klein type, linearly disjoint, and $K = K_1 \cdots K_r$. It is clear from the last expression that c_1 is a product of cocycles defined over the K_i, each of which is equal to the cocycle we already encountered in the quadratic case, corresponding to embedding a Klein extension into a dihedral extension of degree 8 in a certain way, whose obstruction is equal to (a_i, d_i). Then, the obstruction we are computing is the product of quaternion algebras

$$[c_1] = (a_1, d_1)(a_2, d_2)\cdots(a_r, d_r) \in \mathrm{Br}_2(\mathbb{Q}).$$

The general case (last twist). For computing the obstruction in the general case, we will work in a different twist of the curve in order to avoid the "mixing" between the field of definition of the curve and the field of the square roots of the degrees of the isogenies.

We start with a curve and a locally constant set of isogenies $\{\mu_\sigma\}$ as before. Let $s_1, \ldots, s_r$ be a basis of $\mathrm{Gal}(k/\mathbb{Q})$, and let

$$k = k_1 \cdots k_r = \mathbb{Q}(\sqrt{a_1}) \cdots \mathbb{Q}(\sqrt{a_r})$$

be the corresponding decomposition as a product of linearly disjoint quadratic extensions. For every i, choose a rational prime number p_i that is a norm of the extension $k_i/\mathbb{Q}$, and $z_i \in k_i$ an element with

$$N_{k_i/\mathbb{Q}}(z_i) = z_i {}^{s_i} z_i = p_i.$$

We may, and do, choose the prime numbers p_i to be different of each other and relatively prime to the product $a_1 \cdots a_r$.

For every $x \in \mathrm{Gal}(k/\mathbb{Q})$, written as $x = s_1^{x_1} \cdots s_r^{x_r}$, $x_i \in \{0, 1\}$, let

$$p_x = \prod_{i=1}^{r} p_i^{x_i}, \quad \text{and} \quad z_x = \prod_{i=1}^{r} z_i^{x_i}.$$

Then, since for every pair $x_i, y_i \in \{0,1\}$

$$\frac{\sqrt{p_i}^{x_i}\sqrt{p_i}^{y_i}}{\sqrt{p_i}^{x_i+y_i \pmod 2}} = \frac{z_i^{x_i}\, s_i^{x_i}\, z_i^{y_i}}{z_i^{x_i+y_i \pmod 2}} = \begin{cases} p_i, & x_i = y_i = 1, \\ 1, & \text{otherwise,} \end{cases}$$

we obtain the following equality for every $x, y \in \mathrm{Gal}(k/\mathbb{Q})$

$$\sqrt{p_x}\,\sqrt{p_y}\,\sqrt{p_{xy}}^{-1} = {z_x}^{x} z_y\, z_{xy}^{-1}.$$

Let $\gamma = \prod_{i=1}^{r} z_i$. Consider the twisted curve C_γ and the locally constant set of isogenies $\{\mu'_x\}$ obtained from the $\{\mu_\sigma\}$ as explained in Section 2. Let λ_x be the constants associated to the μ'_x. Then, for every $x \in \mathrm{Gal}(k/\mathbb{Q})$,

$$\lambda_x^2 = {d_x}^{x}\gamma\,\gamma^{-1} = {d_x}^{x} z_x\, z_x^{-1} = d_x\, p_x\, z_x^{-2}$$

hence

$$\lambda_x = \frac{\sqrt{d_x p_x}}{z_x}$$

and the field of definition of the isogenies μ'_x is

$$K = k(\{\sqrt{d_x p_x}\}) = k \cdot \mathbb{Q}(\{\sqrt{d_x p_x}\}).$$

Now, the fields k and $\mathbb{Q}(\{\sqrt{d_x p_x}\})$ are linearly disjoint and we proceed as in the previous paragraph: We fix a basis $\{s_1, \ldots, s_r, t_1, \ldots, t_r\}$ for $\mathrm{Gal}(K/\mathbb{Q})$ in the same way, and denote by $x(s_i), x(t_i) \in \{0,1\}$ the coordinates of an element x.

Now, the element λ_x satisfies

$$\lambda_x = \frac{\sqrt{d_x p_x}}{z_x} \equiv \frac{\prod_{i=1}^{r} \sqrt{d_i p_i}^{x(s_i)}}{z_x} \pmod{\mathbb{Q}^*}$$

and the Galois action of an element $y \in G$ on it is given by

$${}^{y}\lambda_x = \Big(\prod_{i=1}^{r}(-1)^{x(s_i)y(t_i)}\Big)\frac{\sqrt{d_x p_x}}{{}^{y}z_x}.$$

Then, the values of the cocycle c are

$$c(x,y) = \lambda_x\,{}^{x}\lambda_y\,\lambda_{xy}^{-1} = \Big(\prod_{i=1}^{r}(-1)^{x(s_i)y(t_i)}\Big)\frac{\sqrt{d_x p_x}\sqrt{d_y p_y}}{\sqrt{d_{xy} p_{xy}}}\frac{z_{xy}}{z_x\,{}^{y}z_x} = \Big(\prod_{i=1}^{r}(-1)^{x(s_i)y(t_i)}\Big)\frac{\sqrt{d_x}\sqrt{d_y}}{\sqrt{d_{xy}}},$$

the cocycle c_1 is given by the same formula

$$c_1(x,y) = \prod_{i=1}^{r}(-1)^{x(s_i)y(t_i)},$$

and the obstruction is

$$[c_1] = \prod_{i=1}^{r}(a_i, d_i\, p_i).$$

From the choice of the primes p_i, each (a_i, p_i) is trivial and the obstruction is, in fact, given by the same formula than before. □

6 Quadratic $\mathbb{Q}$-curves

Let N be a squarefree integer $\geqslant 2$. We say that a $\mathbb{Q}$-curve is quadratic of degree N when the image of the δ map is generated by N. We also assume that C is defined over a quadratic field; i.e., that its field of definition is $k_0 = k$.

Endomorphism algebras. Let A denote an abelian variety of GL_2-type having the quadratic $\mathbb{Q}$-curve C as a quotient, and let E denote the algebra of its $\mathbb{Q}$-endomorphisms. Let $[c_1] = (a, N) \in \mathrm{Br}_2(\mathbb{Q})$, and $u = u((a, N))$ as defined in Section 4. Then,

- The smallest dimension for A is 2^u or 2^{u+1}, depending on the existence of a splitting field L with special properties (see end of Section 4), and also on whether $N = 2$ or not.
- The smallest dimension for A is 2 if, and only if, one of (a, N) or $(a, -N)$ is trivial in $\mathrm{Br}_2(\mathbb{Q})$.
  - There exist A with $E = \mathbb{Q}(\sqrt{N})$ if, and only if, $(a, N) = 1$.
  - There exist A with $E = \mathbb{Q}(\sqrt{-N})$ if, and only if, $(a, -N) = 1$.
- For every n with $\mathrm{ord}_2(n) \geqslant u$ there exist A with $E = \mathbb{Q}(\zeta_{2n}, \sqrt{N})$.
- Given n, there exist A with $E = \mathbb{Q}(\zeta_{2n}\sqrt{N})$ if, and only if, there is a splitting field L of degree n containing k as a subfield.

Parametrization of quadratic $\mathbb{Q}$-curves. The quadratic $\mathbb{Q}$-curves of degree N can be parametrized by the rational points of the curve X_N quotient of $X_0(N)$ by the Atkin-Lehner involution W_N.

Using the ideas of [3] one can compute the corresponding j-invariants in case that X_N has genus zero or one. For example, consider the case $N = 2$. Then, $G = (\eta(z)/\eta(2z))^{24}$ is a function on $X_0(2)$ and $t = G + 2^{12}/G$ is a rational hauptmodul on X_2. We can express the symmetric functions $j + j_2$ and $j \cdot j_2$ as polynomials on t, and compute

$$j = \frac{1}{2}\left(-6656 + 49\,t + t^2 + (47 + t)\,\sqrt{(-128 + t)(128 + t)}\right).$$

Fields of definition when X_N has genus zero. Suppose that X_N has genus zero, and let g denote the genus of $X_0(N)$. Then, the fields of definition of the quadratic $\mathbb{Q}$-curves of degree N are the quadratic fields in the set

$$\mathbb{Q}\left(\sqrt{P(t)}\right), \qquad t \in \mathbb{Q}$$

for some squarefree polynomial $P(t) \in \mathbb{Q}[t]$ of degree $2g + 2$.

If $X_0(N)$ has genus zero, one computes the following polynomials

N	2	3	5	6	7	10	13
$P(t)$	$t^2 - 1$	$t^2 - 1$	$t^2 - 5$	$t^2 - 2$	$t^2 - 1$	$t^2 - 5$	$t^2 - 13$

The other cases correspond to $X_0(N)$ elliptic or hyperelliptic with hyperelliptic involution W_N. The corresponding values of N are

$$N = 11, 17, 19, 23, 29, 31, 41, 47, 59, 71, \quad 14, 15, 21, 26, 35, 39,$$

and we can take as polynomials $P(t)$ the polynomials $P(F)$ in the tables of [2] (warning: for $N = 31$ the coefficient of F^5 must be $+4$ instead of -4). For example,

$$\begin{aligned} N = 19, \quad P(t) &= -48 - 76\,t - 32\,t^2 + t^4, \\ N = 29, \quad P(t) &= -4 - 32\,t - 83\,t^2 - 66\,t^3 - 17\,t^4 + 2\,t^5 + t^6, \\ N = 35, \quad P(t) &= 1 + 4\,t - 6\,t^2 + 4\,t^3 - 9\,t^4 - 4\,t^5 - 6\,t^6 - 4\,t^7 + t^8. \end{aligned}$$

Fields of definition when $X_0(N)$ has genus zero. The fields of definition of quadratic $\mathbb{Q}$-curves of degrees $N = 2, 3, 5, 6, 7, 10, 13$ are the $k = \mathbb{Q}(\sqrt{a})$ with

- any a for $N = 2, 3, 7$,
- $(a, N) = 1$ for $N = 5, 13$,
- $(a, 2) = 1$ for $N = 6$, and,
- $(a, 5) = 1$ for $N = 10$.

This conditions affect the endomorphism algebras of the abelian varieties of GL_2-type attached to the curves. In particular,

- There exist quadratic $\mathbb{Q}$-curves of degrees $N = 3, 6$ and 7 for which the smallest abelian variety A has dimension bigger than any given number. For example if p is a prime number $\equiv 2 \pmod 3$ and $\equiv 1 \pmod{2^u}$, then the smallest A corresponding to a $\mathbb{Q}$-curve of degree 3 defined over $\mathbb{Q}(\sqrt{p})$ is 2^u.
- For $N = 2$ [illegible], every quadratic $\mathbb{Q}$-curve of degree N is the quotient of some abelian variety of GL_2-type of dimension 2 or 4 with endomorphism algebra

$$\mathbb{Q}(\sqrt{2}), \quad \mathbb{Q}(\sqrt{-2}) \quad \text{or} \quad \mathbb{Q}(i, \sqrt{2}).$$

- For $N = 5$ and 13, every quadratic $\mathbb{Q}$-curve of degree N is the quotient of an abelian variety of dimension 2 with endomorphism algebra $\mathbb{Q}(\sqrt{N})$.

Assuming the modularity of the $\mathbb{Q}$-curves, the examples of degrees 3, 6 and 7 imply the existence of modular forms with many inner twists (see [8]) in a strong sense; i.e., all the twists of the modular form by Dirichlet characters have more inner twists than any given number.

Restrictions to the existence of quadratic $\mathbb{Q}$-curves. The conditions on the quadratic fields for the existence of a $\mathbb{Q}$-curve of given degree that we observed in the case that $X_0(N)$ has genus zero can be generalized to necessary conditions for general N as follows:

Proposition 7 *If there exists a quadratic $\mathbb{Q}$-curve of degree N defined over the quadratic field k, then every divisor $N_1 \mid N$ such that*

$$N_1 \equiv 1 \pmod 4 \qquad \text{or} \qquad N_1 \text{ even and } N/N_1 \equiv 3 \pmod 4$$

is a norm of k.

PROOF: Let $N = N_1 N_2$ be a nontrivial factorization of N (when it exists).

It is known (see [2],[3]) that the following three functions G are functions on $X_0(N)$. In fact they belong to the Newman group of functions on the curve $X_0(N)$. It is also known that the action of the involution W_N on them is as given:

$$G(z) = \left(\frac{\eta(z)}{\eta(Nz)}\right)^{24/(12,N-1)}, \qquad G|_{W_N} = N^{12/(12,N-1)}\frac{1}{G},$$

$$G(z) = \left(\frac{\eta(z)\,\eta(N_2 z)}{\eta(N_1 z)\,\eta(Nz)}\right)^{24/(24,(N_1-1)(N_2+1))}, \qquad G|_{W_N} = N_1^{24/(24,(N_1-1)(N_2+1))}\frac{1}{G},$$

and, if $d = (N-1, N_2 - N_1)$, $\alpha = (N-1)/d$, $\beta = (N_2 - N_1)/d$,

$$G(z) = \frac{\eta(z)^\alpha\,\eta(N_1 z)^\beta}{\eta(N_2 z)^\beta\,\eta(Nz)^\alpha}, \qquad G|_{W_N} = N_1^{(\alpha+\beta)/2} N_2^{(\alpha-\beta)/2}\frac{1}{G}.$$

Now, let z be a point on the upper half plane such that $j(z)$ is the invariant of a $\mathbb{Q}$-curve of degree N defined over k. Then, $G(z)$ is an element of k whose conjugate is $G|_{W_N}(z)$, and has norm

$$N^{12/(12,N-1)}, \quad N_1^{24/(24,(N_1-1)(N_2+1))}, \quad \text{or} \quad N_1^{(\alpha+\beta)/2} N_2^{(\alpha-\beta)/2}$$

depending on the function G we use. The result is then consequence of that:

- If $N \equiv 1 \pmod 4$, the exponent in $N^{12/(12,N-1)}$ is odd.
- If $N = N_1 N_2$ and $N_1 \equiv 1 \pmod 4$, then:
  - If N_2 is odd, the exponent in $N_1^{24/(24,(N_1-1)(N_2+1))}$ is odd.
  - If N_2 is even, d is odd, $(\alpha+\beta)/2 = (N_1+1)(N_2-1)/2d$ is odd and $(\alpha-\beta)/2 = (N_1-1)(N_2+1)/2d$ is even.
- If $N = N_1 N_2$, N_1 is even and $N_2 \equiv 3 \pmod 4$, d is odd, $(\alpha+\beta)/2 = (N_1+1)(N_2-1)/2d$ is odd and $(\alpha-\beta)/2 = (N_1-1)(N_2+1)/2d$ is even.

□

As an immediate corollary we obtain that every quadratic $\mathbb{Q}$-curve of degree $N \equiv 1 \pmod 4$ is the quotient of an abelian variety of GL_2-type of dimension 2 with algebra of $\mathbb{Q}$-endomorphisms equal to $\mathbb{Q}(\sqrt{N})$.

7 Examples over bigger fields

In this section we just give some examples of $\mathbb{Q}$-curves with more than one nontrivial isogeny.

Biquadratic $\mathbb{Q}$-curves of degrees dividing 6. Consider the functions

$$G = \left(\frac{\eta(z)\,\eta(3z)}{\eta(2z)\,\eta(6z)}\right)^4, \qquad t = G + 3^4/G.$$

Then, t is a rational hauptmodul of $X^*(6)$, and we can express any symmetric polynomial on j, j_2, j_3 and j_6 as a polynomial on t. After some computations, we obtain the following expression for the j-invariants of the $\mathbb{Q}$-curves parametrized by $X^*(6)$.

$$\begin{aligned} j = \frac{1}{4}\big(& (1730592 + 472644\,t - 19412\,t^2 - 8415\,t^3 - 234\,t^4 + 24\,t^5 + t^6) + \\ & (-2+t)\,(9+t)\,(-3416 - 169\,t + 19\,t^2 + t^3)\,\sqrt{(-18+t)(14+t)} + \\ & (-2+t)\,(9+t)\,(14+t)\,(-215 + 3\,t + t^2)\,\sqrt{(-18+t)(18+t)} + \\ & (109116 + 22868\,t - 2673\,t^2 - 360\,t^3 + 8\,t^4 + t^5)\,\sqrt{(14+t)(18+t)}\,\big). \end{aligned}$$

And the fields of definition of these curves are the biquadratic

$$k = \mathbb{Q}\left(\sqrt{(t+14)(t-18)}, \sqrt{(t+18)(t-18)}\right).$$

Moreover, the involutions W_2 and W_3 correspond to change the sign of one root and leave the other fixed, in the given order. We write down the information about the abelian varieties of GL_2-type associated to the $\mathbb{Q}$-curves corresponding to some values of $t \in \mathbb{Q}$:

- $t = 0$, $\quad k = \mathbb{Q}(\sqrt{-7}, \sqrt{-1})$,

  $$j = 54\left(8012 + 4515\,i + (3031 + 1708\,i)\,\sqrt{7}\right),$$

  $E = \mathbb{Q}(\zeta_{2n}, \sqrt{2}, \sqrt{3})$ for $\mathrm{ord}_2(n) \geqslant 1$,
  minimal A of dimension 8 with $E = \mathbb{Q}(i, \sqrt{2}, \sqrt{3})$.

- $t = -1$, $\quad k = \mathbb{Q}(\sqrt{-247}, \sqrt{-323})$,

  $$j = \frac{1}{4}\left(1246694 + 83942\,\sqrt{221} + 77496\,\sqrt{-247} + 67704\,\sqrt{-323}\right),$$

  $E = \mathbb{Q}(\zeta_{2n}, \sqrt{2}, \sqrt{3})$ for $\mathrm{ord}_2(n) \geqslant 4$,
  minimal A of dimension 32 with $E = \mathbb{Q}(\zeta_{32}, \sqrt{3})$.

- $t = -2$, $\quad k = \mathbb{Q}(\sqrt{-15}, \sqrt{-5})$,

  $$j = 8\left(24079 + 13916\,\sqrt{3} + 18228\sqrt{-5} + 10535\,\sqrt{-15}\right),$$

  $E = \mathbb{Q}(\zeta_{2n}, \sqrt{2}, \sqrt{3})$ for $\mathrm{ord}_2(n) \geqslant 1$, and also $\mathbb{Q}(\zeta_{2n}\sqrt{2}, \sqrt{6})$ for $\mathrm{ord}_2(n) = 1$,
  minimal A of dimension 4 with $E = \mathbb{Q}(\sqrt{-2}, \sqrt{6})$.

- $t = 14$, $\quad k = \mathbb{Q}(\sqrt{-7}, \sqrt{-2})$,

  $$j = -8\left(221873 - 44436\sqrt{-2} - 23667\sqrt{-7} + 59332\,\sqrt{14}\right),$$

  $E = \mathbb{Q}(\zeta_{2n}, \sqrt{2}, \sqrt{3})$ for all n, and also $\mathbb{Q}(\zeta_{2n}\sqrt{3}, \sqrt{2})$ for $\mathrm{ord}_2(n) \geqslant 1$,
  minimal A of dimension 4 with $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Assuming modularity of $\mathbb{Q}$-curves, only the last one is a quotient of $J_0(N)$ for some N. The other three come from $\mathbb{Q}$-simple factors of $J_1(N)$ corresponding to newforms with nontrivial nebentypus.

Triquadratic $\mathbb{Q}$-curves of degrees dividing 30. Consider the functions

$$G = \frac{\eta(z)\,\eta(3z)\,\eta(5z)\,\eta(15z)}{\eta(2z)\,\eta(6z)\,\eta(10z)\,\eta(30z)}, \qquad t = G + 4/G.$$

Then, t is a rational hauptmodul of $X^*(30)$, and we can express any symmetric polynomial on the j_d for $d \mid 30$ as a polynomial on t. After some computations, we obtain the j-invariants of the $\mathbb{Q}$-curves parametrized by $X^*(30)$ as an algebraic expression in t. The fields of definition for the corresponding $\mathbb{Q}$-curves are the triquadratic

$$k = \mathbb{Q}\left(\sqrt{(t+4)(t-4)},\, \sqrt{(t+5)(t+1)(t+4)(t-4)},\, \sqrt{(t+5)(t+1)(t)(t-4)}\right),$$

and the involutions W_2, W_3 and W_5 correspond to changing the sign of one of the three square roots, leaving fixed the other two, in the given order. We make some computations for a couple of examples:

- $t = 1$, $\quad k = \mathbb{Q}(\sqrt{-15}, \sqrt{-5}, \sqrt{-1})$,

$$j = \frac{-3}{4}(1+i)\,\big((1520448042 + 9908421603\,i) + (877849349 + 5720577044\,i)\,\sqrt{3} + (679965303 + 4431181206\,i)\,\sqrt{5} + (392585740 + 2558319455)\,\sqrt{15}\big).$$

  $E = \mathbb{Q}(\zeta_{2n}, \sqrt{2}, \sqrt{3}, \sqrt{5})$ for $\mathrm{ord}_2(n) \geqslant 1$, $\mathbb{Q}(\zeta_{2n}\sqrt{2}, \sqrt{5}, \sqrt{6})$ for $\mathrm{ord}_2(n) = 1$,
  and $\mathbb{Q}(\zeta_{2n}\sqrt{2}, \sqrt{3}, \sqrt{10})$ for $\mathrm{ord}_2(n) = 1$,
  minimal A of dimension 8 with $E = \mathbb{Q}(\sqrt{-2}, \sqrt{5}, \sqrt{6})$ or $\mathbb{Q}(\sqrt{-2}, \sqrt{3}, \sqrt{10})$.

- $t = 8$, $\quad k = \mathbb{Q}(\sqrt{3}, \sqrt{39}, \sqrt{26})$,

$$j = 1728\,\big(5307866332334849883878 41 + 3753228277225653606488 68\,\sqrt{2} + 3064498055796005639155 80\,\sqrt{3} + 2166927356186397058737 60\,\sqrt{6} + 1472137248041679848506 20\,\sqrt{13} + 1040958230927598655718 40\,\sqrt{26} + 8499388364409585793752 0\,\sqrt{39} + 6009975148411916715800 4\,\sqrt{78}\big),$$

  $E = \mathbb{Q}(\zeta_{2n}, \sqrt{2}, \sqrt{3}, \sqrt{5})$ for $\mathrm{ord}_2(n) \geqslant 2$, $\mathbb{Q}(\zeta_{2n}\sqrt{5}, \sqrt{2}, \sqrt{3})$ for $\mathrm{ord}_2(n) = 2$,
  $\mathbb{Q}(\zeta_{2n}\sqrt{2}, \sqrt{5}, \sqrt{6})$ for $\mathrm{ord}_2(n) = 2$ and, finally, $\mathbb{Q}(\zeta_{2n}\sqrt{2}, \sqrt{6}, \sqrt{10})$ for $\mathrm{ord}_2(n) \geqslant 3$,
  minimal A of dimension 16 with
  $E = \mathbb{Q}(\zeta_8\sqrt{5}, \sqrt{2}, \sqrt{3})$ or $\mathbb{Q}(\zeta_8\sqrt{2}, \sqrt{5}, \sqrt{6})$, or also $\mathbb{Q}(\zeta_8, \sqrt{3}, \sqrt{5})$.

References

[1] N. Elkies, *Remarks on elliptic k-curves*, preprint (May 1993).

[2] J. González, *Equations of hyperelliptic modular curves*, Ann. Inst. Fourier 41, 4 (1991), 779–795.

[3] J. González and J.C. Lario, *Rational and elliptic parametrizations of $\mathbb{Q}$-curves*, preprint (1997).

[4] Y. Hasegawa, *$\mathbb{Q}$-curves over quadratic fields*, preprint (1996).

[5] B. Mazur, *Number theory as gadfly*, Amer. Math. Monthly 98 (1991), 593–610.

[6] 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).

[7] J. Quer, *Liftings of projective 2-dimensional galois representations and embedding problems*, J. Algebra 171 (1995), 541–566.

[8] K. Ribet, *Twists of modular forms and endomorphisms of abelian varieties*, Math. Ann. 253 (1980), 43–62.

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

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

[11] B. Roberts, *$\mathbb{Q}$-curves over quadratic fields*, Ph.D. Thesis, Univ. of Maryland (1995).

[12] J.-P. Serre, *Modular forms of weight one and Galois representations*, Algebraic Number Fields (A. Frölich Ed.), Academic Press (1977), 193–268.

[13] J.-P. Serre, *Sur les représentations modulaires de degrée 2 de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. 54 (1987), 179–230.

[14] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Publ. Mat. Soc. Japan 11 (1971).

[15] G. Shimura, *On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields*, Nagoya Math. J. 43 (1971), 199–208.

[16] G. Shimura, *On the factors of the jacobian variety of a modular function field*, J. Math. Soc. Japan 25 (1973), 523–544.