JULIO FERNÁNDEZ

On octahedral extensions of $\mathbb{Q}$ and quadratic $\mathbb{Q}$-curves

On octahedral extensions of $\mathbb{Q}$
and quadratic $\mathbb{Q}$-curves

par JULIO FERNÁNDEZ

RÉSUMÉ. On donne une condition nécessaire pour qu'une représentation surjective $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{F}_3)$ provienne de la 3-torsion d'une $\mathbb{Q}$-courbe. Nous étudions plus particulièrement le cas des $\mathbb{Q}$-courbes quadratiques.

ABSTRACT. We give a necessary condition for a surjective representation $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{F}_3)$ to arise from the 3-torsion of a $\mathbb{Q}$-curve. We pay a special attention to the case of quadratic $\mathbb{Q}$-curves.

1. Introduction

Let C be a $\mathbb{Q}$-curve defined over a number field k, that is an elliptic curve over k without complex multiplication and isogenous to all its Galois conjugates. Throughout, we will denote by G_k and $\mathrm{G}_{\mathbb{Q}}$ the absolute Galois groups $\mathrm{Gal}(\overline{\mathbb{Q}}/k)$ and $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, respectively. Let

$$\rho_C : \mathrm{G}_k \longrightarrow \mathrm{GL}_2(\mathbb{F}_3)$$

be the representation given by the Galois action on the 3-torsion points of C. Then, there exists an odd representation

$$\varrho_C : \mathrm{G}_{\mathbb{Q}} \longrightarrow \mathrm{PGL}_2(\mathbb{F}_3)$$

whose restriction to G_k is lifted to $\mathrm{GL}_2(\mathbb{F}_3)$ by ρ_C. The representation ϱ_C comes from the Galois action on the 3-torsion of the abelian varieties of GL_2-type having the curve C as a quotient (see the proof of Theorem 2.1).

The fixed field of ϱ_C, which we will denote by K_C, has Galois group over $\mathbb{Q}$ inside the symmetric group $\mathcal{S}_4$, since this last group is isomorphic to $\mathrm{PGL}_2(\mathbb{F}_3)$. The behaviour of the restriction of ϱ_C to G_k implies the following property for the field K_C: its compositum with k is the extension

generated by the x-coordinates of the 3-torsion points of C, with respect to any Weierstrass equation for C over k. Whenever $k/\mathbb{Q}$ is Galois and ρ_C is surjective, K_C is the only $\mathcal{S}_4$-extension of $\mathbb{Q}$ satisfying that property; a proof of this claim is given in the appendix. We recall that ϱ_C being odd amounts to K_C not being real.

We will say that a representation

$$\varrho : \ \mathrm{G}_\mathbb{Q} \longrightarrow \mathrm{PGL}_2(\mathbb{F}_3)$$

arises from a $\mathbb{Q}$-curve C if $\varrho = \varrho_C$, where this last equality is considered up to conjugation inside $\mathrm{PGL}_2(\mathbb{F}_3)$. Any such representation ϱ must be odd.

In section 2 we give a necessary condition for a surjective representation ϱ as above to arise from a given $\mathbb{Q}$-curve, in terms of the trace quadratic form attached to any quartic subextension of the fixed field of ϱ. In section 3 we focus on the case of elliptic curves defined over quadratic fields.

2. The sign component in $\mathrm{Br}_2(\mathbb{Q})$ attached to a $\mathbb{Q}$-curve

Let C/k be a $\mathbb{Q}$-curve. From any locally constant set of isogenies from C to its $\mathrm{G}_\mathbb{Q}$-conjugates, one can attach to C an invariant $\xi_C \in H^2(\mathrm{G}_\mathbb{Q}, \overline{\mathbb{Q}}^*)$ of its isogeny class (see [5], Proposition 2.1, and also [7], section 6). The sign component of ξ_C, denoted by $\xi_C^\pm$, is an element in $\mathrm{Br}_2(\mathbb{Q})$, the 2-torsion of the Brauer group of $\mathbb{Q}$. This element is related to the *complete definition* of the $\mathbb{Q}$-curve (cf. [5] and [6]): assuming k to be the minimal field of definition for C up to isogeny, which is a polyquadratic extension of $\mathbb{Q}$, the existence of a k-twist C' of C with all the isogenies

$$^\sigma C' \longrightarrow C' \qquad \sigma \in \mathrm{Gal}(k/\mathbb{Q})$$

defined over k amounts to the existence of a double cover of the group $\mathrm{Gal}(k/\mathbb{Q})$ whose corresponding embedding problem has obstruction given by $\xi_C^\pm$.

The sign component $\xi_C^\pm$ is explicitly given in [5], Theorem 3.1, as a product of quaternion algebras in terms of the minimal field of definition for C up to isogeny and the degrees of the isogenies between C and its Galois conjugates. Our first result gives another expression for $\xi_C^\pm$ depending only on the octahedral extension $K_C/\mathbb{Q}$ in the introduction.

Theorem 2.1. *Assume that ϱ_C is surjective, and let K_C be defined as in section 1. Then, the sign component of ξ_C is given by the following product in $\mathrm{Br}_2(\mathbb{Q})$:*

$$\xi_C^\pm \ = \ w_C \, (-2, \, d_C) \, (-1, -3) \, ,$$

where d_C and w_C are, respectively, the discriminant and the Witt invariant of the trace quadratic form attached to any quartic subextension of $K_C/\mathbb{Q}$.

Proof. For any character $\eta \colon G_\mathbb{Q} \to F^*$, with F an algebraically closed field, let $[\eta]$ be the element in $\mathrm{Br}_2(\mathbb{Q})$ giving the obstruction to the existence of a character $\psi \colon G_\mathbb{Q} \to F^*$ such that $\psi^2 = \eta$. Let us consider these two particular cases:

- For the mod 3 cyclotomic character

$$\chi \colon G_\mathbb{Q} \longrightarrow \mathrm{Gal}\left(\mathbb{Q}(\sqrt{-3})/\mathbb{Q}\right) \simeq \{\pm 1\},$$

  $[\chi]$ is given by the quaternion algebra $(-1, -3)$.
- For any lifting

$$\rho \colon G_\mathbb{Q} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_3)$$

  of the projective representation ϱ_C, the element $[\det \rho]$ gives, by Theorem 6 in [8] and Proposition 1.2 in [4], the obstruction to the solvability of the embedding problem

$$2\,\mathcal{S}_4^- \longrightarrow \mathcal{S}_4 \simeq \mathrm{Gal}\left(K_C/\mathbb{Q}\right),$$

  where $2\,\mathcal{S}_4^-$ is the only double cover of $\mathcal{S}_4$ which can be embedded into $\mathrm{SL}_2(\overline{\mathbb{F}}_3)$. That obstruction can be expressed (see [9], Théorème 1, and [10], section 2) in terms of the trace quadratic form attached to any quartic subextension of $K_C/\mathbb{Q}$, so that we have the equality

$$[\det \rho] \;=\; w_C\left(-2,\, d_C\right)$$

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

Every lifting of ϱ_C into $\mathrm{GL}_2(\overline{\mathbb{F}}_3)$ is obtained, up to isomorphism, as follows. Let $A/\mathbb{Q}$ be an abelian variety having the $\mathbb{Q}$-curve C as a quotient and with $\mathbb{Q}$-endomorphism algebra $\mathbb{Q} \otimes \mathrm{End}_\mathbb{Q}(A)$ a number field of degree $\dim(A)$. By [7], Theorem 6.1, such an abelian variety exists, and we can also assume, replacing A by a $\mathbb{Q}$-isogenous abelian variety if necessary, that the $\mathbb{Q}$-endomorphism ring of A is the maximal order in $\mathbb{Q} \otimes \mathrm{End}_\mathbb{Q}(A)$. For every prime ideal $\mathfrak{p}$ over 3 in that order, the intersection $A[\mathfrak{p}]$ of the kernels of all the endomorphisms in $\mathfrak{p}$ becomes then a 2-dimensional vector space over $\overline{\mathbb{F}}_3$, and the representation

$$\rho_{A,\mathfrak{p}} \colon G_\mathbb{Q} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_3)$$

given by the Galois action on $A[\mathfrak{p}]$ is a lifting of ϱ_C; for another description of the representations $\rho_{A,\mathfrak{p}}$, we refer to [2], section 2.

From [1], Proposition 2.15 (see also [5], Theorem 4.2), we have the identity

$$[\chi \det \rho_{A,\mathfrak{p}}] = \xi_C^\pm.$$

By combining it with the above equalities, we obtain

$$\xi_C^\pm \;=\; [\det \rho_{A,\mathfrak{p}}]\,[\chi] \;=\; w_C\left(-2,\, d_C\right)(-1, -3)$$

in $\mathrm{Br}_2(\mathbb{Q})$, as desired. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Remark 2.1. Given an octahedral extension $K/\mathbb{Q}$, let $d \in \mathbb{Q}^*/\mathbb{Q}^{*\,2}$ and $w \in \mathrm{Br}_2(\mathbb{Q})$ be, respectively, the discriminant and the Witt invariant of the quadratic form $\mathrm{Tr}_{K_1/\mathbb{Q}}(x^2)$ attached to a quartic subextension $K_1/\mathbb{Q}$ of $K/\mathbb{Q}$. Then, w can easily be computed from any *reduced* polynomial $f(X) = X^4 + a\,X^2 + b\,X + c$ defining the extension $K_1/\mathbb{Q}$ (cf. [2], Remark 4.2, and [3], section 2):

- If $a = 0$ or $a = 2\,d$ up to squares, then $w = (-1, -d)$.
- Otherwise, $\delta = 2\,a^3 + 9\,b^2 - 8\,a\,c$ is non-zero, and then $w = (-1, -d)\,(2\,a\,d, \delta)$.

Notice also that d is the discriminant of f up to squares.

The following corollary, which is just a restatement of Theorem 2.1, gives the necessary condition announced in the introduction.

Corollary 2.1. *Let $\varrho : \mathrm{G}_\mathbb{Q} \longrightarrow \mathrm{PGL}_2(\mathbb{F}_3)$ be a surjective representation, and let d and w be the invariants defined by the fixed field of ϱ (as in Remark 2.1). If ϱ arises from a $\mathbb{Q}$-curve C, with attached sign component $\xi_C^\pm$ in $\mathrm{Br}_2(\mathbb{Q})$, then the equality*

$$\xi_C^\pm \;=\; w\,(-2,\,d)\,(-1,\,-3)$$

must hold.

3. Ellipticity over quadratic fields of projective mod 3 Galois representations

Given a projective representation

$$\varrho : \mathrm{G}_\mathbb{Q} \longrightarrow \mathrm{PGL}_2(\mathbb{F}_3)\,,$$

we will say that ϱ is *elliptic* over a quadratic field k if its restriction to G_k is given by

$$\varrho_{\,|\,\mathrm{G}_k} \;=\; \overline{\rho}_E$$

for some elliptic curve E defined over k. Here ρ_E denotes as above the representation of G_k attached to the 3-torsion points of E, and $\overline{\rho}_E$ stands for its associated projective representation. It is clear from the definitions that ellipticity is a necessary condition for the representation ϱ to arise from a $\mathbb{Q}$-curve defined over k.

Whenever $\det \varrho : \mathrm{G}_\mathbb{Q} \to \mathbb{F}_3^*$ is the cyclotomic character χ, the representation ϱ arises from an elliptic curve defined over $\mathbb{Q}$ (and hence it is elliptic over any quadratic field) if and only if it can be lifted to $\mathrm{GL}_2(\mathbb{F}_3)$ [3]. If this last condition is not fulfilled, there are still a priori infinitely many quadratic fields k over which ϱ could be elliptic.

On the other hand, the quadratic field k is uniquely determined by ϱ provided that $\det \varrho \neq \chi$: it corresponds necessarily to the quadratic character $\chi \det \varrho$, so that the restriction $\det \varrho_{\,|\,\mathrm{G}_k}$ becomes cyclotomic. In this

case, the following result gives a characterization of those surjective representations ϱ which are elliptic over k.

Theorem 3.1. *Let* $\varrho : G_{\mathbb{Q}} \to \mathrm{PGL}_2(\mathbb{F}_3)$ *be a surjective representation with non-cyclotomic determinant, and let* d *and* w *be, respectively, the discriminant and the Witt invariant of the trace quadratic form attached to any quartic subextension of the fixed field of* ϱ. *The following conditions are equivalent:*

(1) *The representation* ϱ *is elliptic over a quadratic field.*

(2) *For every prime* p *that splits in* $\mathbb{Q}(\sqrt{-3\,d}\,)$, *the local component at* p *of the quaternion algebra* $w\,(-1, -d)$ *is trivial.*

(3) *Every prime* p *for which* $w_p \neq (-1, -d)_p$ *in* $\mathrm{Br}_2(\mathbb{Q}_p)$ *satisfies the following (where we regard* d *and* $-3\,d$ *as squarefree integers):*

  • *If* p *is odd, then the Legendre symbol* $\left(\frac{-3\,d}{p}\right)$ *is not* 1.
  • *If* $p = 2$, *then* $d \not\equiv 5 \,(\mathrm{mod}\ 8)$.

(4) *The fixed field of* ϱ *is the splitting field of a polynomial of the form* $X^4 - 6\,X^2 + b\,X + c$, *for some* $b, c \in \mathbb{Q}$.

Proof. The hypothesis on $\det \varrho$ amounts to saying that $d \neq -3$ in $\mathbb{Q}^*/\mathbb{Q}^{*\,2}$. As we have noticed above, the only quadratic field k over which ϱ can be elliptic is the fixed field of $\chi \det \varrho$, namely $\mathbb{Q}\left(\sqrt{-3\,d}\,\right)$.

Let $K_1/\mathbb{Q}$ be a quartic subextension of the fixed field of ϱ. Consider the quadratic form $\mathrm{Tr}_{K_1/\mathbb{Q}}(x^2)$ on K_1, with invariants $d \in \mathbb{Q}^*/\mathbb{Q}^{*\,2}$ and $w \in \mathrm{Br}_2(\mathbb{Q})$, and denote by $\mathcal{T}$ its restriction to the 3-dimensional subspace

$$\left\{\, x \in K_1 \mid \mathrm{Tr}_{K_1/\mathbb{Q}}(x) = 0 \,\right\}.$$

The quadratic form $\mathcal{T}$ has also discriminant d and Witt invariant w. Regarded as a real quadratic form, its signature is $(r_1 + r_2 - 1, r_2)$, where r_1 (resp. $2\,r_2$) is the number of real (resp. non-real) embeddings of K_1 into $\overline{\mathbb{Q}}$ (see [9], 3.4) ; in particular, it represents any positive real number, which in terms of Hilbert symbols means that $w_\infty = (-1, -d)_\infty$ in $\mathrm{Br}_2(\mathbb{R})$ whenever d is negative.

Condition (4) amounts to the existence of an element $\alpha \in K_1$ with $\mathrm{Tr}_{K_1/\mathbb{Q}}(\alpha) = 0$ and $\mathrm{Tr}_{K_1/\mathbb{Q}}(\alpha^2) = 3$, i.e. to the representability of 3 by $\mathcal{T}$. In terms of Hilbert symbols, the obstruction to that is given by the equality

$$w_p \,=\, (-1, -d)_p$$

in $\mathrm{Br}_2(\mathbb{Q}_p)$ for every prime p such that $-3\,d$ is a square in $\mathbb{Q}_p^*$. This is in turn equivalent to condition (2), whose translation into Legendre-Kronecker symbols is given by (3).

Consider now the natural morphisms

$$\mathbb{Q}^*/\mathbb{Q}^{*\,2} \to k^*/k^{*\,2} \qquad \mathrm{Br}_2(\mathbb{Q}) \to \mathrm{Br}_2(k)\,.$$

The discriminant and the Witt invariant of the quadratic form (over k) $\mathrm{Tr}_{K_1 k/k}(x^2)$ are the image of d and w, respectively, by these maps. By Theorem 3 in [3] and Theorem 4.2, Lemma 4.1 in [2], ϱ is elliptic over k if and only if $w = (-1,-d)$ in $\mathrm{Br}_2(k)$. Since k is imaginary whenever $w_\infty \neq (-1,-d)_\infty$ in $\mathrm{Br}_2(\mathbb{R})$, this amounts again to condition (2).   □

Remark 3.1. The representation ϱ need not be odd to satisfy the equivalent conditions in the proposition. Also, the surjectivity assumption can be relaxed by only asking the fixed field of ϱ to be the normal closure of a quartic extension of $\mathbb{Q}$, and the result remains the same.

Let us now apply the above result, along with the one in the previous section, to $\mathbb{Q}$-curves of degree N, that is to $\mathbb{Q}$-curves defined over a quadratic field, with non-rational j-invariant, and having an isogeny of degree N to its conjugate curve.

Proposition 3.1. *Let ϱ, d and w be as in Theorem 3.1. If ϱ arises from a $\mathbb{Q}$-curve of degree N, then the following two equivalent conditions are satisfied:*

  (i) *The Witt invariant $w \in \mathrm{Br}_2(\mathbb{Q})$ is given by*

$$w = (-1,-d)(2N,-3d).$$

  (ii) *For every polynomial $X^4 - 6X^2 + bX + c \in \mathbb{Q}[X]$ having the fixed field of ϱ as splitting field, $\delta = 3(16c + 3b^2 - 144)$ is non-zero and the quaternion algebra $(2\delta N, -3d)$ is trivial in $\mathrm{Br}_2(\mathbb{Q})$.*

Proof. The existence of polynomials as in (ii) is ensured by Theorem 3.1, and the equivalence between the two conditions is a straightforward consequence of Remark 2.1. Let C be a $\mathbb{Q}$-curve of degree N attached to ϱ. Since the quadratic field of definition for C is $\mathbb{Q}(\sqrt{-3d})$, the sign component $\xi_C^\pm$ is given by the quaternion algebra $(N, -3d)$ [5]. Condition (i) follows then from Corollary 2.1.   □

Appendix

We look closer here at the uniqueness of the octahedral extension $K_C/\mathbb{Q}$ attached in the introduction to a $\mathbb{Q}$-curve C defined over a Galois number field k, in the case of surjective 3-torsion. The precise statement amounts to the following *octahedral exercise*. Its proof is obtained directly from Galois theory and the lemma below.

Proposition. *Let $K/\mathbb{Q}$ and $k/\mathbb{Q}$ be normal extensions such that the Galois groups $\mathrm{Gal}(K/\mathbb{Q})$ and $\mathrm{Gal}(Kk/k)$ are isomorphic to the symmetric group S_4. Then, there are no other S_4-extensions of $\mathbb{Q}$ having the same compositum with k as K.*

Lemma. *Let* G_1 *and* G_2 *be groups, and identify them with their respective canonical images inside the product group* $G_1 \times G_2$. *Assume the center of* G_2 *to be trivial. Let* H *be a normal subgroup of* $G_1 \times G_2$ *with the same order as* G_1 *and having trivial intersection with* G_2. *Then,* H *must be equal to* G_1.

Proof. From the assumptions on H, this subgroup must be of the form

$$\left\{ (g, \sigma_g) \,\big|\, g \in G_1 \right\} .$$

All we must see then is that $\sigma_g = 1$ for all g in G_1. Assume that $\sigma_g \neq 1$ for some g. Since G_2 has trivial center, there must be some τ in G_2 such that $\tau^{-1} \sigma_g \tau \neq \sigma_g$. Then, the element

$$(g, \tau^{-1} \sigma_g \tau) = (1, \tau)^{-1} (g, \sigma_g) (1, \tau)$$

lies in H and is different from (g, σ_g), which yields a contradiction. $\square$

References

[1] J. S. ELLENBERG, C. SKINNER, *On the modularity of* $\mathbb{Q}$-*curves*. Duke Math. J. **109** (2001), no. 1, 97–122.

[2] J. FERNÁNDEZ, J. C. LARIO, A. RIO, *Octahedral Galois representations arising from* $\mathbb{Q}$-*curves of degree* 2. Canad. J. Math. **54** (2002), 1202–1228.

[3] J. C. LARIO, A. RIO, *An octahedral-elliptic type equality in* $\mathrm{Br}_2(k)$. C. R. Acad. Sci. Paris Sér. I Math. **321** (1995), no. 1, 39–44.

[4] J. QUER, *Liftings of projective* 2-*dimensional Galois representations and embedding problems*. J. Algebra **171** (1995), no. 2, 541–566.

[5] J. QUER, $\mathbb{Q}$-*curves and abelian varieties of* GL_2-*type*. Proc. London Math. Soc. (3) **81** (2000), no. 2, 285–317.

[6] J. QUER, *Fields of definition of* $\mathbb{Q}$-*curves*. J. Théor Nombres Bordeaux **13** (2001), no. 1, 275–285.

[7] K. A. RIBET, *Abelian varieties over* $\mathbb{Q}$ *and modular forms*. Algebra and topology 1992 (Taejŏn), Korea Adv. Inst. Sci. Tech., Taejŏn, 1992, pp. 53–79.

[8] J.-P. SERRE, *Modular forms of weight one and Galois representations*. Algebraic number fields: *L*-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 193–268.

[9] J.-P. SERRE, *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$. Comment. Math. Helv. **59** (1984), no. 4, 651–676.

[10] N. VILA, *On stem extensions of* $\mathcal{S}_n$ *as Galois group over number fields*. J. Algebra **116** (1988), 251–260.

Julio FERNÁNDEZ
Departament de Matemàtica Aplicada 2
Universitat Politècnica de Catalunya
Pau Gargallo 5, E-08028 Barcelona
Spain
E-mail : julio.fernandez@upc.es