MATHEMATICS OF COMPUTATION
Volume 78, Number 265, January 2009, Pages 537–554
S 0025-5718(08)02132-7
Article electronically published on May 13, 2008

FIELDS OF DEFINITION OF BUILDING BLOCKS

JORDI QUER

Abstract. We investigate the fields of definition up to isogeny of the abelian varieties known as *building blocks*. These varieties are defined as the $\mathbb{Q}$-varieties admitting real or quaternionic multiplications of the maximal possible degree allowed by their dimensions (cf. Pyle (2004)). The Shimura-Taniyama conjecture predicts that every such variety is isogenous to a non-CM simple factor of a modular Jacobian $J_1(N)$.

The obstruction to descend the field of definition of a building block up to isogeny is given by Ribet in 1994 as an element in a Galois cohomology group. In this paper we begin by studying these elements from an abstract Galois-cohomological point of view, and obtain results and formulas for the computation of invariants related to them. When considered for the element attached to a building block, these invariants give the structure of its endomorphism algebra, and also complete information on the possible fields of definition up to isogeny of this building block.

We implemented these computations in `Magma` for building blocks given as $\overline{\mathbb{Q}}$-simple factors up to isogeny of the Jacobian of the modular curve $X_1(N)$. Using this implementation we computed a table for conductors $N \leq 500$, which is described in the last section. This table is a source of examples of building blocks with different behaviors and of statistical information; in particular, it contains many examples that answer a question posed by Ribet in 1994 on the existence of a smallest field of definition up to isogeny for RM-building blocks of even dimension.

1. Building blocks

Let $\overline{\mathbb{Q}}$ be an algebraic closure of the rationals and let $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group. All number fields will be seen as subfields of $\overline{\mathbb{Q}}$. The action of $G_{\mathbb{Q}}$ will be denoted exponentially on the left. All $G_{\mathbb{Q}}$-modules are assumed to be discrete, and group cohomology is always (continuous) Galois cohomology.

We work in the category of abelian varieties up to isogeny, in which all isogenies are formally inverted, and denote as usual $\mathrm{End}^0(A) := \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(A)$ the endomorphism algebra of an abelian variety in that category; $\mathrm{End}^0_K(A)$ will denote the subalgebra of endomorphisms defined over a given field K.

In this section we recall the basic theory of the abelian varieties known as *building blocks*. The main references are the thesis of E. Pyle, published in [1], and the papers [5] and [4] by K. Ribet. Most results quoted as Ribet-Pyle in the present paper appear in [5] or [4] for building blocks with real multiplications and then in [1] are given for the general case of real or quaternionic multiplication.

Received by the editor June 1, 2006 and, in revised form, December 26, 2007.
2000 *Mathematics Subject Classification.* Primary 11F11, 11G18.
This research was supported by grants MTM2006-15038-C02-01 and 2005SGR-00443.

An abelian variety $B/\overline{\mathbb{Q}}$ defined over $\overline{\mathbb{Q}}$ is a $\mathbb{Q}$-*variety* if it is $G_{\mathbb{Q}}$-equivariantly isogenous to all its conjugates: for every $\sigma \in G_{\mathbb{Q}}$ there exists an isogeny $\mu_\sigma \colon {}^\sigma B \to B$ that is compatible with the Galois action in the sense that

$$\mu_\sigma \circ {}^\sigma\psi = \psi \circ \mu_\sigma \qquad \forall\ \psi \in \mathrm{End}^0(B).$$

A *building block* is a $\mathbb{Q}$-variety that is simple and has endomorphism algebra $\mathcal{D} = \mathrm{End}^0(B)$ either a totally real field F of degree $[F : \mathbb{Q}] = \dim B$ or a (necessarily totally indefinite) quaternion algebra over a totally real field F of degree $[F : \mathbb{Q}] = \frac{1}{2}\dim B$. In other words, the Rosati involution is an involution of the first kind on the division algebra $\mathcal{D}$, and the dimension of this algebra is the largest possible allowed by the dimension of B. We will call them RM-building blocks or QM-building blocks depending on whether $\mathcal{D} = F$ (real multiplication) or $\mathcal{D}$ is a quaternion algebra over F (quaternionic multiplication).

The class γ. Let B be a building block. For every $\sigma \in G_{\mathbb{Q}}$ pick a compatible isogeny $\mu_\sigma \colon {}^\sigma B \to B$ in such a way that the set $\{\mu_\sigma\}$ is locally constant. For every pair $\sigma, \tau \in G_{\mathbb{Q}}$ let $c(\sigma,\tau)$ denote the map $\mu_\sigma \circ {}^\sigma\mu_\tau \circ \mu_{\sigma\tau}^{-1}$; it is an endomorphism of B that belongs to the center F of the endomorphism algebra $\mathcal{D}$, and c is a 2-cocycle of $G_{\mathbb{Q}}$ with values in F^* viewed as a module with trivial action. The cohomology class of c is an element $\gamma = [c] \in H^2(G_{\mathbb{Q}}, F^*)$ that does not depend on the choice of compatible isogenies between the Galois conjugates of B, and is in fact an invariant of the isogeny class of the variety B.

Let K be a number field. A building block B is said to be *a building block over* K if the abelian variety B and all the endomorphisms of $\mathcal{D}$ are defined over the field K. If a building block B is isogenous to a building block over K, we say that B *descends to* K (up to isogeny), and also that K is *a field of definition up to isogeny* of the building block B. The cohomology class γ turns out to be the obstruction to descend the field of definition of a building block; indeed, one has the

Theorem 1.1 (Ribet-Pyle, cf. [1, Proposition 5.2])**.** *A building block B is isogenous to a building block over the number field K if, and only if, the cohomology class γ lies in the kernel of the restriction map $H^2(G_{\mathbb{Q}}, F^*) \to H^2(G_K, F^*)$.*

The degree map. The "degree" $\delta(\mu_\sigma)$ of compatible isogenies is defined and studied in [4, p. 114] in the case of real multiplication and in [1, pp. 218-220] for the general case. After fixing a polarisation $\theta \colon B \to \widehat{B}$ of the building block B, the "degree" of a compatible isogeny μ_σ is defined as

$$\delta(\mu_\sigma) = \mu_\sigma \circ {}^\sigma\theta^{-1} \circ \widehat{\mu}_\sigma \circ \theta;$$

it is a totally positive element of the field F (cf. [1, Proposition 5.4]) and from the fact that the endomorphism algebra of B is of the first kind one deduces that

$$c(\sigma,\tau)^2 = \delta(\mu_\sigma)\delta(\mu_\tau)\delta(\mu_{\sigma\tau})^{-1}.$$

This equality implies that γ belongs to the 2-torsion subgroup $H^2(G_{\mathbb{Q}}, F^*)[2]$. The name "degree" is due to the fact that the degree of an isogeny $\mu_\sigma \colon {}^\sigma B \to B$, in the usual sense of the degree of a homomorphism between abelian varieties, is the reduced norm over $\mathbb{Q}$ of the element $\delta(\mu_\sigma)$ of the simple algebra $\mathcal{D}$ (cf. [1, Proposition 5.5]). Since the compatible isogenies μ_σ are determined only up to multiplication by an element of F^*, the degree map δ viewed with values in F^*/F^{*2} is an invariant of (the isogeny class of) the variety B.

Decomposition of γ (*cf.* [4, p. 115]). The group F^* has a (noncanonical) decomposition as the cartesian product $P \times \{\pm 1\}$ of the group $\{\pm 1\}$ and the free group $P = F^*/\{\pm 1\}$. This induces a decomposition (also noncanonical) of the second cohomology groups, which restricted to the two-torsion subgroups gives a decomposition

$$H^2(G_{\mathbb{Q}}, F^*)[2] \simeq H^2(G_{\mathbb{Q}}, P)[2] \times H^2(G_{\mathbb{Q}}, \{\pm 1\}). \tag{1}$$

The exact sequence $1 \to P \overset{x \mapsto x^2}{\to} P \to P/P^2 \to 1$ induces an isomorphism in cohomology:

$$H^2(G_{\mathbb{Q}}, P)[2] \simeq \mathrm{Hom}(G_{\mathbb{Q}}, P/P^2). \tag{2}$$

Note that $P/P^2 = F^*/\{\pm 1\}F^{*2}$. Under the decomposition (1) and the isomorphism (2) the element $\gamma \in H^2(G_{\mathbb{Q}}, F^*)[2]$ is split into two pieces: an element $\overline{\gamma} \in \mathrm{Hom}(G_{\mathbb{Q}}, P/P^2)$ canonically determined by γ and an element $\gamma_{\pm} \in H^2(G_{\mathbb{Q}}, \{\pm 1\}) \simeq \mathrm{Br}(\mathbb{Q})[2]$ that does depend on the choice of decomposition $F^* \simeq P \times \{\pm 1\}$. The condition of Theorem 1.1 can now be translated into the corresponding conditions for the components $\overline{\gamma}$ and $\gamma_{\pm}$: a field K trivializes γ if, and only if, it trivializes both components $\overline{\gamma}$ and $\gamma_{\pm}$.

Fields of definition up to isogeny. Let K_P be the extension of $\mathbb{Q}$ fixed by the kernel of $\overline{\gamma}$. It is a polyquadratic extension of $\mathbb{Q}$ (we will use the word *polyquadratic* for extensions that are abelian of exponent two, i.e. a composition of quadratic extensions). A given field K trivializes $\overline{\gamma}$ if, and only if, it contains the field K_P. On the other hand, every nontrivial element of $\mathrm{Br}(\mathbb{Q})[2]$ has splitting fields that are quadratic fields, hence every building block B is always isogenous to a building block over some polyquadratic extension of $\mathbb{Q}$ (this is Theorem 1.2 of [4] for the real multiplication case and Theorem 5.1 of [1] for the general case).

Let $\mathrm{res}_{\mathbb{Q}}^{K_P}(\gamma_{\pm})$ denote the image of the sign component $\gamma_{\pm}$ by the restriction map

$$\mathrm{res}_{\mathbb{Q}}^{K_P} \colon H^2(G_{\mathbb{Q}}, \{\pm 1\}) \to H^2(G_{K_P}, \{\pm 1\}) \simeq \mathrm{Br}(K_P)[2].$$

If $\mathrm{res}_{\mathbb{Q}}^{K_P}(\gamma_{\pm})$ is trivial, then K_P is the smallest possible field of definition up to isogeny for the building block B. Otherwise, if $\mathrm{res}_{\mathbb{Q}}^{K_P}(\gamma_{\pm}) \neq 1$, then there is no such smallest possible field: all fields of definition up to isogeny must strictly contain K_P, and they are the extensions of K_P that are splitting fields for the division quaternion algebra with center K_P corresponding to the element $\mathrm{res}_{\mathbb{Q}}^{K_P}(\gamma_{\pm})$.

In [4, Corollary 4.5] Ribet proves that for RM-building blocks of odd dimension we are always in the first case: $\mathrm{res}_{\mathbb{Q}}^{K_P}(\gamma_{\pm})$ is trivial. This fact was proven previously by N. Elkies for the case $F = \mathbb{Q}$, the situation in which the building blocks are also known by the name of $\mathbb{Q}$-*curves*. In [4, p. 109] Ribet asks whether the hypothesis on the parity of $\dim B$ is really necessary in his result. In the table of building blocks that we describe in the last section we will find examples of RM-building blocks of even dimension (2 and 4) with nontrivial $\mathrm{res}_{\mathbb{Q}}^{K_P}(\gamma_{\pm})$, hence the hypothesis is necessary; the table also contains examples of QM-building blocks with trivial and nontrivial values of this element.

The study of the existence of building blocks with no smallest field of definition up to isogeny was in fact our main motivation to program the computations described in the present paper.

The Brauer class of $\mathcal{D}$. Every element $\gamma \in H^2(G_{\mathbb{Q}}, F^*)$ determines an element $\mathrm{brc}_F(\gamma) \in \mathrm{Br}(F)$, defined as the image of γ under the natural maps

$$H^2(G_{\mathbb{Q}}, F^*) \to H^2(G_F, F^*) \to H^2(G_F, \overline{F}^*), \tag{3}$$

of which the first is the restriction to the subgroup $G_F \subseteq G_{\mathbb{Q}}$ and the second is the map induced by the embedding $F^* \hookrightarrow \overline{F}^*$ as G_F-modules with the natural Galois action. When γ is the element obtained from a building block B by the construction described above, then $\mathrm{brc}_F(\gamma)$ is just the class of the algebra $\mathcal{D} = \mathrm{End}^0(B)$ in the Brauer group $\mathrm{Br}(F)$ (cf. [1, Theorem 2.1]).

2. Some computations in Galois cohomology

Let F be a totally real number field. We consider F^* as a $G_{\mathbb{Q}}$-module with trivial action. Let $\gamma \in H^2(G_{\mathbb{Q}}, F^*)[2]$ be a cohomology class of order dividing 2. Let $\overline{\gamma} \in \mathrm{Hom}(G_{\mathbb{Q}}, P/P^2)$ and let $\gamma_{\pm} \in H^2(G_{\mathbb{Q}}, \{\pm 1\})$ be the two components corresponding to γ under a decomposition (1) and the isomorphism (2).

In this section we study this element γ just as an element of the abstract cohomology group considered. The results and formulas obtained will be later applied to the case of our interest, in which $\gamma = \gamma_B$ is obtained as in Section 1 from a building block B. We first compute the homomorphism $G_{\mathbb{Q}} \to P/P^2$ corresponding to the component $\overline{\gamma}$. As for the *sign component* $\gamma_{\pm}$, we study its dependence on the chosen decomposition $F^* \simeq P \times \{\pm 1\}$, and also show how to compute it as an element of $\mathrm{Br}(\mathbb{Q})[2]$. We will then study the Brauer class $\mathrm{brc}_F(\gamma) \in \mathrm{Br}(F)[2]$ corresponding to γ under the maps (3), and give a formula for computing it explicitly.

Two torsion of the Brauer group. We will need explicit descriptions of elements belonging to the 2-torsion $\mathrm{Br}(k)[2] \simeq H^2(G_k, \{\pm 1\})$ of the Brauer group of a field k (we are interested in number fields but these descriptions work for any field of characteristic different from 2). Here we recall a couple of basic constructions of such elements (see [2, Section 2] for more details) and also introduce notation. For every pair of elements $a, b \in k^*$ we denote, as it is customary, by $(a, b) \in \mathrm{Br}(k)[2]$ the Brauer class of the quaternion algebra with basis $\{1, \imath, \jmath, \kappa\}$ and multiplication determined by $\imath^2 = a, \jmath^2 = b, \imath\jmath = -\jmath\imath = \kappa$. The class (a, b) can also be constructed as a cup product in $H^2(G_k, \{\pm 1\})$ as follows. Let $\chi_a, \chi_b \colon G_k \to \mathbb{Z}/2\mathbb{Z}$ be additive characters of order dividing 2 whose kernels have as fixed fields $k(\sqrt{a})$ and $k(\sqrt{b})$, respectively. Then the map

$$(\sigma, \tau) \mapsto (-1)^{\chi_a(\sigma)\chi_b(\tau)} \colon G_k \times G_k \to \{\pm 1\}$$

is a two-cocycle of G_k with values in $\{\pm 1\}$ whose cohomology class is that of (a, b).

For every Galois character $\chi \colon G_k \to \overline{k}^*$ we will denote by $\gamma_\chi \in \mathrm{Br}(k)[2]$ the Brauer class of the two-cocycle of G_k with values in $\{\pm 1\}$ defined by

$$(\sigma, \tau) \mapsto \frac{\sqrt{\chi(\sigma)}\sqrt{\chi(\tau)}}{\sqrt{\chi(\sigma\tau)}}$$

after a choice of a square root $\sqrt{\chi(\sigma)}$ for each $\sigma \in G_k$. This element represents the obstruction to embed the cyclic extension of k fixed by $\ker \chi$ into a cyclic extension of k of double degree; equivalently, it is the obstruction to the existence of a square root of the Galois character χ. If χ is quadratic with kernel having fixed field $k(\sqrt{a})$, then one easily checks that the element γ_χ coincides with (a, a), which is also equal to $(a, -1)$.

The degree splitting maps. Let c be a cocycle representing the class γ. Since c^2 is a coboundary, there exists a splitting map for it; i.e. a map $\sigma \mapsto \delta_\sigma \colon G_{\mathbb{Q}} \to F^*$ such that

$$c^2(\sigma,\tau) = \delta_\sigma \delta_\tau \delta_{\sigma\tau}^{-1}. \tag{4}$$

Motivated by the fact that in the situation of interest to us the maps δ_σ are provided by the "degrees" $\delta(\mu_\sigma)$ of isogenies between conjugates of building blocks, we define

Definition 2.1 (Degree splitting map)**.** A map $\sigma \mapsto \delta_\sigma \colon G_{\mathbb{Q}} \to F^*$ satisfying (4) will be called a *degree splitting map* for the two-cocycle c.

Two degree splitting maps for the same cocycle differ in a group homomorphism $G_{\mathbb{Q}} \to F^*$ that, by continuity, must take values in the torsion subgroup $\{\pm 1\}$ of F^*, i.e., two degree splitting maps differ in a quadratic Galois character. Taking its values modulo squares, we obtain from any degree splitting map a group homomorphism

$$\delta \colon G_{\mathbb{Q}} \to F^*/F^{*2}, \qquad \sigma \mapsto \delta_\sigma \pmod{F^{*2}}, \tag{5}$$

and the set of all these homomorphisms modulo quadratic Galois characters only depends on the cohomology class γ and not on the cocycle c representing it. We can also take the values of a degree splitting map modulo elements of $\{\pm 1\}F^{*2}$, and in this way we obtain a group homomorphism

$$\overline{\delta} \colon G_{\mathbb{Q}} \to F^*/\{\pm 1\}F^{*2} = P/P^2, \qquad \sigma \mapsto \delta_\sigma \pmod{\{\pm 1\}F^{*2}},$$

that only depends on the cohomology class γ. One has the following:

Proposition 2.2. *The map $\overline{\delta} \colon G_{\mathbb{Q}} \to P/P^2$ is the first component $\overline{\gamma}$ of γ under any decomposition* (1) *and the isomorphism* (2)*.*

Proof. The proof given by Pyle in [1, Proposition 5.6] for the case when $\gamma = \gamma_B$ is attached to a building block works in the general situation. We repeat here the argument.

Let c be a cocycle representing γ. The class $\overline{\gamma} \in H^2(G_{\mathbb{Q}}, P)[2]$ under the decomposition (1) is the class of the cocycle $\overline{c} = c \pmod{\{\pm 1\}}$ with values in $P = F^*/\{\pm 1\}$.

Given any degree splitting map for c, consider the corresponding map $\overline{\delta}$. The image of this map in $H^2(G_{\mathbb{Q}}, P)[2]$ under the isomorphism (2), which is the connecting homomorphism of group cohomology, is computed in the following way: one chooses representatives in P of the values of $\overline{\delta}$ in P/P^2; for example, one may take $\delta_\sigma \pmod{\{\pm 1\}}$ as a representative of $\overline{\delta}(\sigma)$. Then the element $\delta_\sigma \delta_\tau \delta_{\sigma\tau}^{-1}$ is a square in the group P, and taking its (unique) square root in P we obtain a map $(\sigma,\tau) \mapsto \sqrt{\delta_\sigma \delta_\tau \delta_{\sigma\tau}^{-1}}$ which is a two-cocycle of $G_{\mathbb{Q}}$ with values in P whose class in $H^2(G_{\mathbb{Q}}, P)[2]$ is the required image. But since $\overline{c}^2(\sigma,\tau) = \delta_\sigma \delta_\tau \delta_{\sigma\tau}^{-1}$, the square roots $\sqrt{\delta_\sigma \delta_\tau \delta_{\sigma\tau}^{-1}}$ coincide with the values $\overline{c}(\sigma,\tau)$ of the cocycle $\overline{c}$. □

The quadratic degree characters. Let K_P denote the fixed field of the kernel of the homomorphism $\overline{\gamma}$. It is a polyquadratic extension of $\mathbb{Q}$. A quadratic character ψ of $G_{\mathbb{Q}}$ will be called a *quadratic degree character* if its restriction to the subgroup G_{K_P} is trivial; equivalently, if it factors through the group $\mathrm{Gal}(K_P/\mathbb{Q})$. The group of all quadratic degree characters will be denoted by Ψ. In the future we will also often make use of the additive versions (with values in $\mathbb{Z}/2\mathbb{Z}$) of the quadratic degree

characters, i.e., of the homomorphisms $G_{\mathbb{Q}} \to \mathbb{Z}/2\mathbb{Z}$ factoring through the group $\mathrm{Gal}(K_P/\mathbb{Q})$.

Let $\sigma_1, \dots, \sigma_r$ be elements of $G_{\mathbb{Q}}$ whose restrictions to K_P give a basis of $\mathrm{Gal}(K_P/\mathbb{Q})$ as a vector space over the field of two elements, and let $\psi_1, \dots, \psi_r$ be the dual basis of the space of additive characters $\mathrm{Hom}(\mathrm{Gal}(K_P/\mathbb{Q}), \mathbb{Z}/2\mathbb{Z})$ with respect to the basis $\{\sigma_i\}$; we consider the characters ψ_i as defined in all elements of $G_{\mathbb{Q}}$ by inflation. Given a degree splitting map $\sigma \mapsto \delta_\sigma$, let $\delta_i = \delta_{\sigma_i}$ be the corresponding values for $i = 1, \dots, r$.

Definition 2.3 (Dual bases)**.** The characters $\psi_i \colon G_{\mathbb{Q}} \to \mathbb{Z}/2\mathbb{Z}$ and the elements $\delta_i \in F^*$ constructed in this way from any basis $\sigma_1, \dots, \sigma_r$ of $\mathrm{Gal}(K_P/\mathbb{Q})$ will be called dual bases with respect to the degree splitting map δ.

Lemma 2.4. *There exist degree splitting maps such that the corresponding map* (5) *factors through the group* $\mathrm{Gal}(K_P/\mathbb{Q})$*. These degree splitting maps will be called* reduced*.*

Proof. Let $\delta \mapsto \delta_\sigma \colon G_{\mathbb{Q}} \to F^*$ be any degree splitting map, and let $\{\psi_i\}$ and $\{\delta_i\}$ be dual bases with respect to it.

For every $\sigma \in G_{\mathbb{Q}}$ its action on the field K_P coincides with that of the element $\sigma_1^{\psi_1(\sigma)} \cdots \sigma_r^{\psi_r(\sigma)}$, hence $\overline{\gamma}(\sigma) = \overline{\gamma}(\sigma_1)^{\psi_1(\sigma)} \cdots \overline{\gamma}(\sigma_r)^{\psi_r(\sigma)}$ and there exists a unique sign $\chi_\delta(\sigma) \in \{\pm 1\}$ such that

$$\delta_\sigma = \chi_\delta(\sigma) \delta_1^{\psi_1(\sigma)} \cdots \delta_r^{\psi_r(\sigma)} \pmod{F^{*2}}. \tag{6}$$

From this identity and the observation that $\delta_i^{\psi_i(\sigma)} \delta_i^{\psi_i(\tau)} = \delta_i^{\psi_i(\sigma\tau)} \pmod{F^{*2}}$ for every $\sigma, \tau \in G_{\mathbb{Q}}$ it follows that the map $\sigma \mapsto \chi_\delta(\sigma)$ is a quadratic Galois character (this character depends not only on the degree map δ as the notation employed might suggest, but also on the basis σ_i of the Galois group $\mathrm{Gal}(K_P/\mathbb{Q})$ chosen).

Let us consider the new splitting map δ' obtained multiplying δ by the character χ_δ, and perform the same construction with this new map. Since $\chi_\delta(\sigma_i) = 1$, as it is clear from (6), we have $\delta'_i = \delta_i$, and then for every $\sigma \in G_{\mathbb{Q}}$ we have

$$\delta'_\sigma = \chi_\delta(\sigma)\delta_\sigma = \chi_\delta(\sigma)^2 \delta_1^{\psi_1(\sigma)} \cdots \delta_r^{\psi_r(\sigma)} = {\delta'_1}^{\psi_1(\sigma)} \cdots {\delta'_r}^{\psi_r(\sigma)} \pmod{F^{*2}}.$$

From this expression it follows that the values of the degree splitting map δ' on an element $\sigma \in G_{\mathbb{Q}}$ depend only on the restriction of this element to the field K_P, because the exponents $\psi_i(\sigma)$ only depend on it. □

It is clear that among the (infinitely many) degree splitting maps for a given cocycle c, which differ from each other by the multiplication by any quadratic Galois character, the reduced ones are finite in number, and differ from each other by the multiplication by a quadratic degree character.

When B is a building block and $c(\sigma, \tau) = \mu_\sigma \circ {}^\sigma\mu_\tau \circ \mu_{\sigma\tau}^{-1}$ is the 2-cocycle computed from a locally constant set of compatible isogenies, then the "degree" map $\sigma \mapsto \delta(\mu_\sigma)$ defined in Section 1 is a reduced degree splitting map for the cocycle c. This is an immediate consequence of the fact that the values $\delta(\mu_\sigma)$ are totally positive: in the identity (6) the sign $\chi_\delta(\sigma)$ always has to be positive since the elements on both sides are totally positive elements of F^*.

For every degree splitting map δ we denote by Δ_δ the subgroup of F^*/F^{*2} generated by the values δ_σ for $\sigma \in G_{\mathbb{Q}}$, and by $F_\delta = F(\{\sqrt{\delta_\sigma}\}) = F(\sqrt{\Delta_\delta})$ the field obtained by adjoining to F the square roots of these values, which is a polyquadratic

extension of F. Let Δ be the subgroup of F^*/F^{*2} generated by all the values $\pm\delta_\sigma$, or equivalently by the values δ_σ and by -1. The group Δ no longer depends on the degree splitting map δ but only on the class γ. When the degree splitting map δ is not reduced, then $\Delta_\delta = \Delta$; when δ is reduced, then Δ_δ is a subgroup of index 2 of Δ with $\Delta = \Delta_\delta \oplus \langle -1\rangle$. In fact, every complement of $\langle -1\rangle$ in Δ as an $\mathbb{F}_2$-vector space is of the form Δ_δ for a reduced degree splitting map δ.

Let $\sigma \mapsto \delta_\sigma$ be a degree splitting map. For each $s \in G_F$ we define

$$\psi_s(\sigma) = \frac{\sqrt[s]{\delta_\sigma}}{\sqrt{\delta_\sigma}}, \qquad \sigma \in G_{\mathbb{Q}}, \tag{7}$$

which is a quadratic Galois character that depends only on the action of s on the field F_δ. Then one has the following:

Lemma 2.5. *If δ is a reduced degree splitting map, then the map $s \mapsto \psi_s$ induces an isomorphism between the group $\mathrm{Gal}(F_\delta/F)$ and the group Ψ of the quadratic degree characters.*

Proof. If δ is reduced, then for every $\sigma \in G_{K_P}$ the value δ_σ is a square of an element of F^* and hence $\psi_s(\sigma) = 1$. This means that in this case all the quadratic characters ψ_s are quadratic degree characters. One immediately checks that the map $s \mapsto \psi_s \colon G_F \to \Psi$ is a group homomorphism. The character ψ_s is trivial if, and only if, the automorphism s leaves every square root $\sqrt{\delta_\sigma}$ fixed, and by definition this is equivalent to $s \in G_{F_\delta}$. This means that the map $s \mapsto \psi_s$ induces an injective homomorphism from $\mathrm{Gal}(F_\delta/F)$ to Ψ. But these two groups have the same number of elements, namely, the number of elements of the group $\mathrm{Gal}(K_P/\mathbb{Q})$, since $\delta \colon G_{\mathbb{Q}} \to F^*/F^{*2}$ factors through that Galois group and has image the group Δ_δ that, by Kummer theory, is isomorphic to the Galois group of F_δ over F. □

Decompositions of F^*. To give an isomorphism

$$F^* \simeq P \times \{\pm 1\} \tag{8}$$

is equivalent to giving a *sign map*: a group homomorphism $\mathrm{sgn} \colon F^* \to \{\pm 1\}$ such that $\mathrm{sgn}(-1) = -1$. Since such a map always factors through the quotient group F^*/F^{*2}, it is completely determined by a homomorphism $F^*/F^{*2} \to \{\pm 1\}$ sending -1 to -1. Equivalently, to giving a sign map amounts to giving a nontrivial linear form of F^*/F^{*2} as a vector space over the field of two elements, such that -1 has nontrivial image.

If the degree $[F : \mathbb{Q}]$ is odd, then a canonical choice is possible: one may take as the sign of an element of F^* the sign of its absolute norm in $\mathbb{Q}$, or equivalently to identify P with the subgroup of F^* consisting of elements of positive norm. For fields of even degree such a canonical choice does not exist.

Proposition 2.6. *The sign component $\gamma_\pm$ attached to an element γ relative to a given sign map only depends on the values of this sign map in the finite subgroup $\Delta \subset F^*/F^{*2}$.*

The sign components attached to γ for all possible sign maps differ from each other by the multiplication by elements γ_ψ, for $\psi \in \Psi$ ranging over all the quadratic degree characters.

Proof. Let c be any cocycle representing γ and let $\sigma \mapsto \delta_\sigma$ be a reduced degree splitting map for c. Fix a square root $\sqrt{\delta_\sigma}$ for every $\sigma \in G_{\mathbb{Q}}$. Then we can write

$$c(\sigma, \tau) = c_\pm(\sigma, \tau)\sqrt{\delta_\sigma}\sqrt{\delta_\tau}\sqrt{\delta_{\sigma\tau}}^{\,-1} \tag{9}$$

for some sign $c_\pm(\sigma,\tau) \in \{\pm 1\}$. Now the class $\gamma_\pm$ is the cohomology class of the cocycle $\mathrm{sgn}(c)$, that is the product of the cocycles $\mathrm{sgn}(c_\pm) = c_\pm$ (since $c_\pm$ takes values in ± 1), which does not depend on the sign map, and of the cocycle $\mathrm{sgn}(\sqrt{\delta_\sigma}\sqrt{\delta_\tau}\sqrt{\delta_{\sigma\tau}}^{-1})$. The cohomology class of this second cocycle does not depend on the choice of square roots since a change of signs in the choices only would modify it by a coboundary. Now we describe a choice of square roots from which we will compute its cohomology class.

Let $\{\psi_i\}$ and $\{\delta_i\}$ be dual bases for the degree splitting map δ, as defined in Definition 2.3. As in (6), for every $\sigma \in G_\mathbb{Q}$, its restriction to the field K_P is completely determined by $\psi_i(\sigma)$ and every δ_σ can be written as

$$\delta_\sigma = \chi_\delta(\sigma)\delta_1^{\psi_1(\sigma)} \cdots \delta_r^{\psi_r(\sigma)} x_\sigma^2$$

with sign $\chi_\delta(\sigma) = 1$ since δ is reduced, for some element $x_\sigma \in F^*$. We can now define a square root for every δ_σ writing

$$\sqrt{\delta_\sigma} = \sqrt{\delta_1}^{\psi_1(\sigma)} \cdots \sqrt{\delta_r}^{\psi_r(\sigma)} x_\sigma$$

for any choice x_σ of the square root of x_σ^2. Using this choice of square roots, and noticing that for every $i = 1, \ldots, r$ one has

$$\frac{\sqrt{\delta_i}^{\psi_i(\sigma)}\sqrt{\delta_i}^{\psi_i(\tau)}}{\sqrt{\delta_i}^{\psi_i(\sigma\tau)}} = \delta_i^{\psi_i(\sigma)\psi_i(\tau)},$$

one obtains from (9) the following identity

$$c(\sigma,\tau) = c_\pm(\sigma,\tau)\ \delta_1^{\psi_1(\sigma)\psi_1(\tau)}\ \cdots\ \delta_r^{\psi_r(\sigma)\psi_r(\tau)}\ x_\sigma x_\tau x_{\sigma\tau}^{-1}.$$

Now applying the sign map sgn we have

$$\mathrm{sgn}(c)(\sigma,\tau) = c_\pm(\sigma,\tau)\ \mathrm{sgn}(\delta_1)^{\psi_1(\sigma)\psi_1(\tau)} \cdots\ \mathrm{sgn}(\delta_r)^{\psi_r(\sigma)\psi_r(\tau)}\ \mathrm{sgn}(x_\sigma)\mathrm{sgn}(x_\tau)\mathrm{sgn}(x_{\sigma\tau})^{-1}.$$

From this expression, and observing that the last part made of the $\mathrm{sgn}(x_\sigma)$ is a coboundary, it follows that the class of $\mathrm{sgn}(c)$ depends only on the values of the sign map in the δ_i, and these elements belong to Δ, which is the first part of the statement.

For each $i = 1, \ldots, r$, if $\mathrm{sgn}(\delta_i) = 1$, then the factor $\mathrm{sgn}(\delta_i)^{\psi_i(\sigma)\psi_i(\tau)}$ is trivial, and if $\mathrm{sgn}(\delta_i) = -1$, then this factor is the cohomology class of the cup product of $\psi_i \in \mathrm{Hom}(G_\mathbb{Q}, \mathbb{Z}/2\mathbb{Z})$ by itself, which is the class γ_ψ for the quadratic character $\psi = (-1)^{\psi_i}$. If we define $\epsilon_i \in \mathbb{Z}/2\mathbb{Z}$ by the identity $\mathrm{sgn}(\delta_i) = (-1)^{\epsilon_i}$, then we obtain the cohomology class of $\mathrm{sgn}(c)$ as the product of the class $[c_\pm]$ by the class γ_ψ attached to a quadratic degree character

$$[\mathrm{sgn}(c)] = [c_\pm] \cdot \gamma_\psi, \qquad \psi = (-1)^{\epsilon_1\psi_1 + \cdots + \epsilon_r\psi_r}.$$

Every (multiplicative) degree character $\psi \in \Psi$ can be written in a unique way as $\psi(\sigma) = (-1)^{\epsilon_1\psi_1(\sigma) + \cdots + \epsilon_r\psi_r(\sigma)}$ for $\epsilon_i \in \mathbb{Z}/2\mathbb{Z}$. To finish the proof of the statement we only need to show that every quadratic degree character $\psi \in \Psi$ will be obtained from some sign map; in other words, that any choice of values of $\epsilon_i \in \mathbb{Z}/2\mathbb{Z}$ is realized by some sign map. Indeed, the δ_i are a basis of Δ_δ as a vector space over $\mathbb{F}_2$, and since δ is reduced adding -1, one has a basis of Δ. Given an arbitrary choice of signs $\mathrm{sgn}(\delta_i) = (-1)^{\epsilon_i} \in \{\pm 1\}$ for the δ_i, and defining $\mathrm{sgn}(-1) = -1$, one

gets by linearity a nontrivial linear form $\Delta \to \{\pm 1\}$. This form can be extended to linear forms of the full space F^*/F^{*2} which are the sign maps required. □

The characters ε. For computing the cohomology class $\gamma_\pm \in H^2(G_\mathbb{Q}, \{\pm 1\})$ we need to compute the cohomology class of the sign factor $c_\pm$ in (9) for some cocycle c representing γ and some reduced degree splitting map for it.

Let $\overline{\mathbb{Q}}^*$ be viewed as a discrete module over the group $G_\mathbb{Q}$ with trivial action. A theorem of Tate (cf. [6, Theorem 4]) says that the group $H^2(G_\mathbb{Q}, \overline{\mathbb{Q}}^*)$ is trivial.

Let $\gamma \in H^2(G_\mathbb{Q}, F^*)$ be represented by the cocycle c. By Tate's theorem this cocycle is a coboundary when we consider it as taking its images in $\overline{\mathbb{Q}}^*$. Let $\sigma \mapsto \alpha_\sigma \colon G_\mathbb{Q} \to \overline{\mathbb{Q}}^*$ be a (continuous) splitting map for it, i.e., a map with

$$c(\sigma, \tau) = \alpha_\sigma \alpha_\tau \alpha_{\sigma\tau}^{-1}. \tag{10}$$

Let $\sigma \mapsto \delta_\sigma$ be a reduced degree splitting map for c. Then squaring the previous identity and dividing by (4) we see that the map $\varepsilon \colon G_\mathbb{Q} \to \overline{\mathbb{Q}}^*$ defined by

$$\varepsilon(\sigma) = \frac{\alpha_\sigma^2}{\delta_\sigma}, \qquad \sigma \in G_\mathbb{Q} \tag{11}$$

is a continuous homomorphism, i.e., a Galois character with values in the roots of unity.

Notice that this Galois character ε depends on choices of a splitting map $\sigma \mapsto \alpha_\sigma$ and a reduced degree splitting map $\sigma \mapsto \delta_\sigma$ for a given cocycle c representing γ. One may easily check that a change of α (with the same δ) amounts to multiplying ε by the square of some Galois character, and a change of δ (same α) amounts to multiplying ε by the corresponding quadratic degree character ψ. Hence, ε is determined by the cohomology class γ only up to multiplication by squares of Galois characters and by quadratic degree characters.

Theorem 2.7. *Let ε be a Galois character defined by* (11) *from some splitting map $\sigma \mapsto \alpha_\sigma$ and reduced degree splitting map $\sigma \mapsto \delta_\sigma$. There exists a sign map such that the sign component $\gamma_\pm$ corresponding to it is the element $\gamma_\varepsilon \in H^2(G_\mathbb{Q}, \{\pm 1\})$.*

Proof. For every $\sigma \in G_\mathbb{Q}$ choose square roots $\sqrt{\delta_\sigma}$ and $\sqrt{\varepsilon(\sigma)}$ in such a way that $\alpha_\sigma = \sqrt{\delta_\sigma}\sqrt{\varepsilon(\sigma)}$. Then we have

$$c(\sigma, \tau) = \alpha_\sigma \alpha_\tau \alpha_{\sigma\tau}^{-1} = \sqrt{\varepsilon(\sigma)}\sqrt{\varepsilon(\tau)}\sqrt{\varepsilon(\sigma\tau)}^{-1} \ \sqrt{\delta_\sigma}\sqrt{\delta_\sigma}\sqrt{\delta_{\sigma\tau}}^{-1},$$

and for a given sign map sgn we have

$$\operatorname{sgn}(c)(\sigma, \tau) = \operatorname{sgn}(\sqrt{\varepsilon(\sigma)}\sqrt{\varepsilon(\tau)}\sqrt{\varepsilon(\sigma\tau)}^{-1}) \operatorname{sgn}(\sqrt{\delta_\sigma}\sqrt{\delta_\sigma}\sqrt{\delta_{\sigma\tau}}^{-1}).$$

The first cocycle in this product (in which the sign map acts as the identity since it is applied to elements of F^* that are equal to ± 1) has cohomology class γ_ε. As for the second, in the proof of Proposition 2.6 we have seen that its cohomology class ranges over all values γ_ψ for quadratic characters $\psi \in \Psi$ when the sign map ranges over all possible such maps. Hence for the sign map corresponding to the trivial character $\psi = 1$ (which is in fact the sign map that defines every element of Δ_δ to be positive), the cohomology class of this second part is trivial, and we have proved the result. □

Computation of $\mathrm{brc}_F(\gamma)$. Now we find a formula for the element $\mathrm{brc}_F(\gamma) \in \mathrm{Br}(F)[2]$ determined by a given element $\gamma \in H^2(G_{\mathbb{Q}}, F^*)$ under the maps (3). Let $\sigma \mapsto \delta_\sigma$ be a reduced degree splitting map for a cocycle c representing γ, and let $\psi_i \in \mathrm{Hom}(G_{\mathbb{Q}}, \mathbb{Z}/2\mathbb{Z})$ and $\delta_i \in F^*$, for $i = 1, \ldots, r$, be dual bases with respect to it.

For every $i = 1, \ldots, r$ let $t_i \in \mathbb{Q}^*$ be a rational number such that the quadratic field $\mathbb{Q}(\sqrt{t_i})$ is the fixed field of $\ker \psi_i$. Let $\sigma \mapsto \alpha_\sigma$ be a splitting map for c considered with values in $\overline{\mathbb{Q}}^*$, and let ε be the Galois character defined by (11) in terms of α and δ. Then we have the following:

Theorem 2.8. *The class* $\mathrm{brc}_F(\gamma) \in \mathrm{Br}(F)[2]$ *is given by the formula*

$$\mathrm{brc}_F(\gamma) = \mathrm{res}^F_{\mathbb{Q}}(\gamma_\varepsilon) \cdot (t_1, \delta_1) \cdots (t_r, \delta_r).$$

Proof. This proof is essentially the same as given in [3, Théorème 3] for the case of cohomology classes attached to building blocks. We consider the cocycle c as a 2-cocycle of the group $G_F \subseteq G_{\mathbb{Q}}$ with values in $\overline{F}^* = \overline{\mathbb{Q}}^*$, but now with the natural Galois action instead of the trivial action. We recall that we have $c(\sigma, \tau) = \alpha_\sigma \alpha_\tau \alpha_{\sigma\tau}^{-1}$. We choose square roots of $\varepsilon(\sigma)$ and of δ_σ in such a way that $\alpha_\sigma = \sqrt{\varepsilon(\sigma)}\sqrt{\delta_\sigma}$. Multiplying and dividing by $\sqrt{\delta_\sigma}^{\,\sigma}\sqrt{\delta_\tau}\sqrt{\delta_{\sigma\tau}}^{\,-1}$, which is a coboundary of G_F with values in $\overline{\mathbb{Q}}^*$ under the Galois action, we have

$$c(\sigma, \tau) = \alpha_\sigma \alpha_\tau \alpha_{\sigma\tau}^{-1} = \sqrt{\varepsilon(\sigma)}\sqrt{\varepsilon(\tau)}\sqrt{\varepsilon(\sigma\tau)}^{\,-1} \; \frac{\sqrt{\delta_\tau}}{{}^{\sigma}\sqrt{\delta_\tau}} \; \sqrt{\delta_\sigma}^{\,\sigma}\sqrt{\delta_\tau}\sqrt{\delta_{\sigma\tau}}^{\,-1}.$$

From this expression we obtain the Brauer class of the cocycle c as the product of the class γ_ε by the class of the two-cocycle $(\sigma, \tau) \mapsto \sqrt{\delta_\tau}/{}^{\sigma}\sqrt{\delta_\tau}$. Using the assumption made of δ being reduced we can write $\delta_\tau = \prod_{i=1}^r \delta_i^{\psi_i(\tau)} \cdot x_\tau^2$ for some $x_\tau \in F^*$, and the chosen square roots satisfy

$$\sqrt{\delta_\tau} = \sqrt{\delta_1}^{\psi_1(\tau)} \; \cdots \; \sqrt{\delta_r}^{\psi_r(\tau)} \cdot x_\tau$$

for the appropriate choice of square root x_τ of x_τ^2.

Let $\sigma_1', \ldots, \sigma_r'$ be the basis of the group $\mathrm{Gal}(F_\delta/F)$ consisting of the automorphisms determined by ${}^{\sigma_i'}\sqrt{\delta_j} = \sqrt{\delta_j}$ if $i \neq j$ and ${}^{\sigma_i'}\sqrt{\delta_i} = -\sqrt{\delta_i}$. Let $\psi_1', \ldots, \psi_r'$ be the basis of the group $\mathrm{Hom}(\mathrm{Gal}(F_\delta/F), \mathbb{Z}/2\mathbb{Z})$ which is the dual of the basis $\{\sigma_i'\}$. We also view the characters ψ_i' as defined in all the elements of G_F by inflation. Then, for every element $\sigma \in G_F$ and $1 \leq i \leq r$ we have $\sqrt{\delta_i}/{}^{\sigma}\sqrt{\delta_i} = (-1)^{\psi_i'(\sigma)}$. Since $x_\tau \in F$, we obtain

$$\frac{\sqrt{\delta_\tau}}{{}^{\sigma}\sqrt{\delta_\tau}} = \frac{\sqrt{\delta_1}^{\psi_1(\tau)} \; \cdots \; \sqrt{\delta_r}^{\psi_r(\tau)} \cdot x_\tau}{{}^{\sigma}\sqrt{\delta_1}^{\psi_1(\tau)} \; \cdots \; {}^{\sigma}\sqrt{\delta_r}^{\psi_r(\tau)} \cdot {}^{\sigma}x_\tau} = (-1)^{\psi_1'(\sigma)\psi_1(\tau)} \; \cdots \; (-1)^{\psi_r'(\sigma)\psi_r(\tau)},$$

and this expression shows that the cohomology class of the cocycle $(\sigma, \tau) \mapsto \sqrt{\delta_\tau}/{}^{\sigma}\sqrt{\delta_\tau}$ is the product of all the cup products of every pair of a character ψ_i' and (the restriction to G_F of) the character ψ_i, as characters of G_F, for $i = 1, \ldots, r$, from which we obtain the formula for $\mathrm{brc}_F(\gamma)$ given in the statement. □

Hilbert symbols. Now applying Theorems 2.7 and 2.8 we can compute the invariants $\gamma_\varepsilon \in \mathrm{Br}(\mathbb{Q})[2]$ and $\mathrm{brc}_F(\gamma) = \gamma_\varepsilon \prod(t_i, \delta_i) \in \mathrm{Br}(F)[2]$. By class field theory, giving an element of the Brauer group of a number field K is equivalent to giving all its local invariants; for elements of two-torsion, and using the exact sequence

$$0 \longrightarrow \mathrm{Br}(K)[2] \longrightarrow \bigoplus_{v \in \Sigma_K} \mathrm{Br}(K_v)[2] \overset{(\xi_v) \mapsto \prod_v \xi_v}{\longrightarrow} \{\pm 1\} \longrightarrow 1,$$

where Σ_K denotes the set of (Archimedean and non-Archimedean) places of K, and for every completion K_v of K we identify $\mathrm{Br}(K_v)[2]$ with the group $\{\pm 1\}$, to giving an element $\xi \in \mathrm{Br}(K)[2]$ is equivalent to giving its local components ξ_v for every completion, and in practice one needs only to list the (finite, of even cardinality) set of places with $\xi_v = -1$.

In our formulas appear elements given in two ways: either of the form γ_χ for Galois characters of $G_{\mathbb{Q}}$, or of the form (t, δ), with $t \in \mathbb{Q}^*$ and $\delta \in F^*$. For the convenience of the reader we describe here how their local components can be computed in practice, using basic well-known facts about Brauer groups and Hilbert symbols.

Let $\chi\colon G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$ be a Galois character, identified in the usual way with a primitive Dirichlet character of conductor m. For every prime number p, let χ_p be the component of χ modulo to the largest power of p dividing m. Then the local components of $\gamma_\chi \in \mathrm{Br}(\mathbb{Q})[2]$ are given by

$$(\gamma_\chi)_p = \chi_p(-1) \qquad \text{for every (finite) prime } p, \qquad \text{and} \quad (\gamma_\chi)_\infty = \chi(-1).$$

For a quaternion algebra over the rationals, given as (a, b) for rational numbers $a, b \in \mathbb{Q}^*$, the usual formulas for computing Hilbert symbols $(a, b)_p \in \{\pm 1\}$ (see for example Serre's Course d'Arithmétique) are enough for determining $(a, b) \in \mathrm{Br}(\mathbb{Q})[2]$. If we want to perform analogous computations over number fields, for infinite places and places of odd residual characteristic we have similar formulas, but in general there are no such formulas for the dyadic places. The computations we are interested in are simplified by the fact that on the elements $(t, \delta) \in \mathrm{Br}(F)[2]$ appearing in our formula one of its components is always a rational number $t \in \mathbb{Q}^*$; in this case the computation is reduced to the computation of Hilbert symbols over $\mathbb{Q}$ by using the formula

$$(t, \delta)_w = (t, N_{L_w/K_v}(\delta))_v,$$

which holds in the following general situation: L/K is an extension of number fields, $t \in K$, $\delta \in L$, and w is a place of L lying over a place v of K.

Finally, when we need to consider the restriction of an element $\xi \in \mathrm{Br}(K)[2]$ to $\mathrm{Br}(L)[2]$ for an extension L/K (for example we need the restriction $\mathrm{res}^F_{\mathbb{Q}}(\gamma_\pm)$ in order to compute $\mathrm{brc}_F(\gamma)$ using the formula of Theorem 2.8 and also the restriction $\mathrm{res}^{K_P}_{\mathbb{Q}}(\gamma_\pm)$ in order to decide whether K_P is a field of definition or not), we can just use the local restriction maps $\mathrm{Br}(K_v)[2] \to \mathrm{Br}(L_w)[2]$ for every place w of L over a place v of K; these maps send the element $\xi_v \in \mathrm{Br}(K_v)[2] \simeq \{\pm 1\}$ to the element $\xi_v^{[L_w:K_v]} \in \mathrm{Br}(L_w)[2]$, and everything is reduced to just computing the parity of each extension $[L_w : K_v]$.

3. Varieties of GL_2-type

An abelian variety $A/\mathbb{Q}$ defined over $\mathbb{Q}$ is *of* GL_2*-type* if the subalgebra $\mathrm{End}^0_{\mathbb{Q}}(A) \subseteq \mathrm{End}^0(A)$ is a number field of degree $[E : \mathbb{Q}] = \dim A$; in this paper we will also add the condition that A has no complex multiplication, which is equivalent to the fact that E is a maximal subfield of $\mathrm{End}^0(A)$. One has the following:

Theorem 3.1 (Pyle-Ribet, cf. [1, Propositions 1.3, 1.4 and 4.5])**.** *An abelian variety over $\mathbb{Q}$ is of GL_2-type if, and only if, it factors over $\overline{\mathbb{Q}}$ as a power of a building block.*

Let A be an abelian variety of GL_2-type with simple factor B. Then $\mathcal{X} = \mathrm{End}^0(A)$ is a matrix algebra over the division algebra $\mathcal{D}$, hence a central simple F-algebra. Let $E = \mathrm{End}^0_{\mathbb{Q}}(A)$, which is a maximal subfield of $\mathcal{X}$, and has a canonical complex conjugation given by the Rosati involution induced by any polarization on A. The Galois action on $\mathcal{X}$ induces an endomorphism on it, and applying the Noether-Skolem theorem we obtain for every $\sigma \in G_{\mathbb{Q}}$ an element $\alpha(\sigma) \in E^*$ such that ${}^{\sigma}\psi = \alpha(\sigma) \circ \psi \circ \alpha(\sigma)^{-1}$ for every $\psi \in \mathcal{X}$, only determined up to elements of F^*.

The field E is generated over F by the elements $\alpha(\sigma)$ ([1, Proposition 1.5]) and the extension E/F is Galois and abelian ([1, Proposition 1.7]). The Rosati involution induced by any polarization of $A/\mathbb{Q}$ induces a canonical involution $a \mapsto \overline{a}$ of E, giving rise to the complex conjugation on every complex embedding of the field E, and for every $\sigma \in G_{\mathbb{Q}}$ one has $\alpha(\sigma)\overline{\alpha(\sigma)} \in F^*$ ([1, Lemma 1.6]).

The map $c'(\sigma, \tau) \mapsto \alpha(\sigma)\alpha(\tau)\alpha(\sigma\tau)^{-1}$ is a 2-cocycle of $G_{\mathbb{Q}}$ with values in F^*, considered as a module with trivial action. By the method explained in Section 1 we can construct another cocycle of the same type $c(\sigma, \tau) = \mu_\sigma \circ {}^{\sigma}\mu_\tau \circ \mu_{\sigma\tau}^{-1}$ from compatible isogenies between the conjugates of the building block B. In fact, one has the following:

Theorem 3.2 (Pyle-Ribet, cf. [1, Theorem 4.6])**.** *The cocycles c and c' are cohomologous.*

We remark here that the cocycle c' we are using is the same cocycle used by Ribet in [5], but Pyle in [1] uses its inverse; since its cohomology class belongs to the 2-torsion of the group $H^2(G_{\mathbb{Q}}, F^*)$ both choices are equally useful for our purposes.

By the previous theorem, and since the elements $\alpha(\sigma)$ are defined only up to multiplication by elements of F^*, we may always make a choice of these $\alpha(\sigma)$ such that the cocycle c' coincides with any given cocycle c computed from the building block B, and in the following we will always assume that we choose the $\alpha(\sigma)$ in this way. Then, the theorem above says that the map $\sigma \mapsto \alpha(\sigma) \in E^*$ is a splitting map with values in $E^* \subset \overline{\mathbb{Q}}^*$ for the cocycle c, and it can be used for the computation of the sign component $\gamma_\pm$ and of the Brauer class $\mathrm{brc}_F(\gamma)$ using Theorems 2.7 and 2.8. Moreover, the cocycle c admits the reduced degree splitting map $\sigma \mapsto \delta(\mu_\sigma)$. Then, by formula (11) we obtain a Galois character defined by

$$\varepsilon(\sigma) = \frac{\alpha(\sigma)^2}{\delta(\mu_\sigma)}. \tag{12}$$

This Galois character is completely determined by the abelian variety A, and clearly does not depend on the isogenies between the conjugates of its absolutely simple factor B used in its computation.

Inner twists. To every element $s \in G_F$ we can also attach a Galois character, which we call an *inner twist character* of the GL_2-type variety $A/\mathbb{Q}$, defined by

$$\chi_s(\sigma) = \frac{{}^{s}\alpha(\sigma)}{\alpha(\sigma)}. \tag{13}$$

The fact that this is a Galois character is a consequence of the fact that $c'(\sigma, \tau) \in F^*$. Obviously, the character χ_s does only depend on the action of s on E and in

fact we have as many such characters as the degree $[E : F]$. When s is the complex conjugation one obtains the character

$$\chi_{\mathrm{conj}}(\sigma) = \frac{\overline{\alpha(\sigma)}}{\alpha(\sigma)} = \frac{\alpha(\sigma)\overline{\alpha(\sigma)}}{\alpha(\sigma)^2}.$$

Multiplying it by the character ε we obtain a Galois character sending the element $\sigma \in G_{\mathbb{Q}}$ to $\alpha(\sigma)\overline{\alpha(\sigma)}/\delta(\mu_\sigma)$, which is an element of F^*, and hence must be ± 1; moreover, since $\delta(\mu_\sigma)$ and $\alpha(\sigma)\overline{\alpha(\sigma)}$ are both totally positive, this character must be trivial, from which we deduce (see also [1, Theorem 5.2] for an equivalent result) that the character ε attached to A by (12) is the inverse of χ_{conj},

$$\varepsilon = \chi_{\mathrm{conj}}^{-1}.$$

Hence, we also obtain as a consequence that, with the choice we made of the elements $\alpha(\sigma)$, imposing the cocycle c' to be the same as c, we have $\delta(\mu_\sigma) = \alpha(\sigma)\overline{\alpha(\sigma)}$ for every $\sigma \in G_{\mathbb{Q}}$.

The quadratic degree characters. Let $F_\delta = F(\sqrt{\delta(\mu_\sigma)})$ be the extension obtained by adjoining to F the square roots of the degrees of all the μ_σ, which is a finite polyquadratic extension of the same degree as $K_P/\mathbb{Q}$. From Lemma 2.5 we know that there is an isomorphism between the Galois group $\mathrm{Gal}(F_\delta/F)$ and the group Ψ of quadratic degree characters obtained by sending every $s \in G_F$ to the character

$$\psi_s(\sigma) = \frac{{}^s\sqrt{\delta(\mu_\sigma)}}{\sqrt{\delta(\mu_\sigma)}}. \tag{14}$$

Since $\sqrt{\delta(\mu_\sigma)} = \alpha(\sigma)\sqrt{\varepsilon(\sigma)}$ we obtain the following relation between the inner twist characters and the quadratic degree characters, where we denote by $\sqrt{\varepsilon}^{s-1}$ the Galois character of $G_{\mathbb{Q}}$ defined by $\sigma \mapsto {}^s\sqrt{\varepsilon(\sigma)}/\sqrt{\varepsilon(\sigma)}$ for every $\sigma \in G_{\mathbb{Q}}$.

Proposition 3.3. *For every element $s \in G_F$ one has the identity of Galois characters*

$$\psi_s = \chi_s \cdot \sqrt{\varepsilon}^{s-1}.$$

This proposition can be useful for the computation of the quadratic degree characters from the knowledge of the inner twist characters, and vice versa. In fact, the inner twist characters χ_s depend only on the action of s on the field E, and the quadratic degree characters ψ_s depend on its action on the field F_δ. Hence the identity of the proposition can be stated for elements s of the (finite) Galois group of the field $E \cdot F_\delta$ over F. Notice that since $\sqrt{\delta(\mu_\sigma)} = \alpha_\sigma\sqrt{\varepsilon(\sigma)}$, the field $E \cdot F_\delta$ is obtained by adjoining to E the square roots of the values of the character ε, and it must be either equal to E or to a quadratic extension of E.

ℓ-adic representations [*cf.* [5, Section 3 and 5]]. Let $A/\mathbb{Q}$ be an abelian variety of GL_2-type. For every prime number ℓ the ℓ-adic Tate module $V_\ell(A)$ is free of rank two over $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. For every prime λ of E dividing ℓ let E_λ be the completion of E at λ, and let $V_\lambda = V_\ell \otimes_{E \otimes \mathbb{Q}_\ell} E_\lambda$. For each prime p of good reduction let

$$a_p = \mathrm{tr}_{E_\lambda}(\mathrm{Frob}_p \,|V_\lambda) \tag{15}$$

with λ any prime dividing some prime $\ell \neq p$. This trace of Frobenius a_p is an element of $E \subset E_\lambda$ that does not depend on the prime λ chosen.

Then, the field E is generated by the numbers a_p ([5, Proposition 1.5]), the field F is generated by the numbers $a_p^2/\varepsilon(p)$ ([5, Theorem 5.3]; notice that the character

ε in this theorem coincides with ours due to [1, Theorem 5.12]). Moreover, for every prime p of good reduction such that $a_p \neq 0$ one has

$$\alpha(\mathrm{Frob}_p) \equiv a_p \pmod{F^*}, \tag{16}$$

and one can obtain the values of the splitting map α from the knowledge of the traces of Frobenius a_p.

4. Computations, examples and tables

In this section we describe an implementation in `Magma` of a package that computes the main invariants described in previous sections for modular abelian varieties. We also give statistical information on the data of a table computed using this implementation, containing building blocks that are simple factors up to isogeny of the Jacobians $J_1(N)$ of levels $N \leq 500$. The table contains many examples of RM-building blocks of even dimension that cannot be descended to the field K_P, showing that the hypothesis of the degree $[F : \mathbb{Q}]$ being odd cannot be avoided in Ribet's result [4, Corollary 4.5]; the smallest such example occurs in level $N = 33$ and will be described at the end of this section. The package will be included in forthcoming versions of `Magma` and the complete table (which may be extended in the future to bigger bounds) can be downloaded at `http://www-ma2.upc.es/~quer/Recerca`.

We begin by recalling some basic facts about modular forms and modular abelian varieties. Let $f = \sum a_n q^n \in S_2(N, \varepsilon)$ be a (normalized) newform of weight 2, level N and Nebentypus character ε. Let $E = \mathbb{Q}(\{a_n\})$ be the number field generated by its Fourier coefficients. Shimura attached to f an abelian variety A_f defined over $\mathbb{Q}$, of dimension $\dim A_f = [E : \mathbb{Q}]$, that can be constructed up to $\mathbb{Q}$-isogeny either as a subvariety or a quotient of the Jacobian of the modular curve $X_1(N)$. The action of the Hecke operators on $J_1(N)$ induces an isomorphism between the field E and $\mathrm{End}^0_{\mathbb{Q}}(A_f)$. Hence A_f is an abelian variety of GL_2-type. By the Eichler-Shimura correspondence, the Fourier coefficients a_p of the modular form f are the traces of Frobenius (15) acting on the λ-adic Tate modules $V_\lambda(A_f)$. Let A_f be isogenous to a power of an abelian variety B_f simple over $\overline{\mathbb{Q}}$. The varieties A_f and B_f (considered up to $\mathbb{Q}$-isogeny and up to $\overline{\mathbb{Q}}$-isogeny, respectively), are called *modular abelian varieties*. In ([5, Theorem 4.4]) it was shown that Serre's conjecture on the modularity of two-dimensional mod p Galois representations of $G_{\mathbb{Q}}$ would imply that every abelian variety of GL_2-type (equivalently, every building block) is modular. Due to the recent proof by Khare-Winterberger of Serre's modularity conjecture, the modularity of all building blocks is now a theorem.

The modular form f is said to have complex multiplication when there exists a (necessarily unique and odd) Dirichlet character χ such that $a_p = \chi(p)a_p$ for every prime $p \nmid N$. This is equivalent to the fact that B_f is an elliptic curve with complex multiplication by an order of the imaginary quadratic field fixed by the kernel of the character χ.

We assume from now on that f has no complex multiplication, and hence that B_f is a building block. In this case the field F which is the center of $\mathrm{End}^0(B_f)$ is the subfield of E generated by the numbers $a_p^2/\varepsilon(p)$ for all primes $p \nmid N$.

The *inner twists* of the non-CM modular form f are Dirichlet characters χ_s attached to every element $s \in G_F$ and determined by the identities

$$^s a_p = \chi_s(p) a_p \qquad \text{for every} \quad p \nmid N. \tag{17}$$

We can also define the *quadratic degree characters* of the non-CM modular form f as the quadratic Dirichlet characters ψ_s attached to every $s \in G_F$ and determined by

$$\sqrt[s]{a_p^2/\varepsilon(p)} = \psi_s(p)\sqrt{a_p^2/\varepsilon(p)} \qquad \text{for every} \quad p \nmid N. \tag{18}$$

Then we have the following:

Proposition 4.1. *The inner twists and the quadratic degree characters of a modular form are the same as the corresponding characters for the* GL_2*-type variety* A_f *and the building block* B_f*, defined in the previous section by the identities* (13) *and* (14).

Proof. Let χ_s be an inner twist for A_f. Then for every prime p not dividing N, the identity (13) for $\sigma = \mathrm{Frob}_p$ and the congruence (16) when $a_p \neq 0$ imply the identity (17) in this case; when $a_p = 0$ this is also trivially satisfied. Conversely, assume the identity (17) satisfied. The identity (13) for an automorphism $\sigma \in G_{\mathbb{Q}}$ depends only on the action of σ on the field K_P. Then, using the well-known fact that for non-CM modular forms the set of primes for which $a_p \neq 0$ is of density one into the set of all primes, by the Cebotarev density theorem every element of $\sigma|_{K_p} \in \mathrm{Gal}(K_P/\mathbb{Q})$ is of the form Frob_p for some prime p with $a_p \neq 0$, and the identity (17) and the congruence (16) for this prime p imply the identity (13) for σ. The same argument can be used for proving the property for the quadratic degree characters. □

Implementation. The best implementation available for doing computations with modular symbols, modular forms, and modular abelian varieties are the packages written by William Stein for the computer system `Magma`. Based on these packages, we implemented several functions for computing some of the invariants described in this paper. The main functions are `DegreeMap`, `BrauerClass`, and `ObstructionDescentBuildingBlock`. The three functions have as input a space of modular symbols of level an integer N and Nebentypus a Dirichlet character ε modulo N that is new and irreducible, and hence it determines a newform f.

The main function `DegreeMap` gives as output a sequence of $r \geq 0$ pairs (t_i, δ_i) with $t_i \in \mathbb{Q}^*$ and $\delta_i \in F^*$, such that the field K_P is the polyquadratic extension of $\mathbb{Q}$ obtained by adjoining the square roots of the numbers t_i, the group Ψ of quadratic degree characters is the group generated by the r characters corresponding to the quadratic fields $\mathbb{Q}(\sqrt{t_i})$, and if we denote $\psi_i \colon G_{\mathbb{Q}} \to \mathbb{Z}/2\mathbb{Z}$ the additive versions of these characters, then the degree map corresponding to the abelian variety B_f is determined modulo squares by the formula $\delta(\mu_\sigma) = \prod_{i=1}^r \delta_i^{\psi_i(\sigma)} \pmod{F^{*2}}$. The function `BrauerClass` uses the output of `DegreeMap` to compute the Brauer class of the endomorphism algebras of the varieties A_f and B_f from the formula in Theorem 2.8; the Brauer class is in practice given as the list of primes of F that are ramified in that quaternion algebra. The function `ObstructionDescentBuildingBlock` uses the function `DegreeMap` to compute the field K_P, and gives as output the obstruction to descend the building block B_f over the field K_P; this obstruction is an element of $\mathrm{Br}(K_P)$, given again as a list of ramified places of this field. The computation of Hilbert symbols needed for obtaining these obstructions has been programmed using the remarks at the end of Section 2.

An important ingredient needed by `DegreeMap` is the computation of the inner twists of a modular form. For this we use W. Stein's implementation. We remark

that for the unconditional computation of the inner twists one has to test the equality (17) for enough primes; the best proved bound on the number of primes to be tested grows as N^2 (see the `Magma` documentation on inner twists), and this makes the computation too expensive even for moderate values of N. In general, a conjectural bound linear on N is used in W. Stein's implementation, that should be enough, although there is no proof of that fact. For the elaboration of the table described below we used the proved bound for all forms of level $N \leq 100$ and the linear bound $15 + N/2$ for larger levels.

A table. We elaborated a table with the output data of the three functions just described for all the newforms of level $N \leq 500$ and Nebentypus characters ε whose orders satisfy $\varphi(\mathrm{ord}(\varepsilon)) \leq 12$ (i.e. such that the number field generated by the values of ε has degree over $\mathbb{Q}$ bounded by 12), and such that the corresponding field F has degree $[F : \mathbb{Q}] \leq 4$. In fact we are quite confident that our table contains all the newforms in the given level range $N \leq 500$ for which the corresponding field F has degree up to 4, with no restriction on the Nebentypus character. Indeed, for characters whose values generate extensions of degree larger than 12 we performed the computations using modular symbols over finite fields instead of working over number fields, and we did not find any modular form with $[F : \mathbb{Q}] \leq 4$ for these characters of large degree; even though this reduction process seems to always produce the right answers, we do not have a complete theoretical justification for it.

From our computations we obtained

$$\#\{\ f \in S_2(N, \varepsilon) \text{ newform} \mid N \leq 500,\ \varphi(\mathrm{ord}(\varepsilon)) \leq 12,\ [F : \mathbb{Q}] \leq 4\} = 5609.$$

The number of such forms that are newforms for $\Gamma_0(N)$, i.e., forms with trivial Nebentypus character, is

$$\#\{\ f \in S_2(N) \text{ newform} \mid N \leq 500,\ [F : \mathbb{Q}] \leq 4\} = 1750.$$

In the tables below we give some statistical information on properties of the forms of the table and of the corresponding modular abelian varieties. The first table gives the number of forms for each degree of F over $\mathbb{Q}$, and also the number of cases in which the algebra $\mathcal{D} = \mathrm{End}^0(B_f)$ is equal to F or is a quaternion division algebra over F.

$[F : \mathbb{Q}]$	total	$\mathcal{D} = F$	$\mathcal{D} \neq F$
1	2610	2426	184
2	1613	1555	58
3	739	695	44
4	647	619	28
total	5609	5295	314

The next table gives the number of occurrences for every possible dimension r of the group Ψ of quadratic degree characters found in the range of the tables. We recall that this dimension corresponds to the size of the field K_P, which is of degree $[K_P : \mathbb{Q}] = 2^r$. The data are also given in separate rows depending on the values of the degree $[F : \mathbb{Q}]$.

$[F:\mathbb{Q}]$	$r=0$	$r=1$	$r=2$	$r=3$
1	1767	663	172	8
2	1031	475	102	5
3	548	131	53	7
4	378	186	73	10
total	3724	1455	400	30

Finally, we tabulate the number of occurrences of trivial and nontrivial obstruction to descend the building block B_f to the field K_P up to isogeny, separated for RM-building blocks and for QM-building blocks.

$[F:\mathbb{Q}]$	$\mathcal{D}=F$ and obs $\neq 0$	$\mathcal{D}\neq F$ and obs $\neq 0$
1	0	21
2	121	1
3	0	0
4	42	0

The two zeros occurring at odd degree in the column corresponding to RM-building blocks are due to Ribet's result [4, Corollary 4.5]. The fact that the other two entries at this same column are nonzero is an answer to the question posed by Ribet asking whether the hypothesis of the degree $[F:\mathbb{Q}]$ being odd is really necessary in his result.

An example. The example of this behavior with smallest level N occurs at level $N=33$. Let ε be an even Dirichlet character of order 10 and conductor 33, which is uniquely determined up to Galois conjugation. There is a unique newform $f=\sum a_n q^n$ in the space $S_2(33,\varepsilon)$ up to Galois conjugation. It has coefficients in the cyclotomic field $E=\mathbb{Q}(e^{2\pi i/20})$, of degree 8. The form has four inner twists, given by the characters $1, \chi_3, \varepsilon^{-1}$ and $\varepsilon^{-1}\chi_3$, with χ_3 being the nontrivial character modulo 3. The field F is $\mathbb{Q}(\sqrt{5})$ and the field K_P is $\mathbb{Q}(\sqrt{-11})$.

The $\mathbb{Q}$-simple abelian variety A_f is of dimension 8 and it is isogenous to the fourth power of a $\overline{\mathbb{Q}}$-simple abelian surface B_f, which is an RM-building block with multiplications by $\mathbb{Q}(\sqrt{5})$. The obstruction to descend this building block to K_P up to isogeny is the nontrivial element of $\mathrm{Br}(K_P)[2]$ ramified at the two primes of K_P of norm 3. The smallest degree of a field over which this variety can be defined up to isogeny is 4; for example, $\mathbb{Q}(\sqrt{-11},\sqrt{-3})$ is such a field.

References

[1] E. Pyle, *Abelian varieties over $\mathbb{Q}$ with large endomorphism algebras and their simple components over $\overline{\mathbb{Q}}$.* Modular curves and abelian varieties, 189–239, Progr. Math., **224**, Birkhäuser, Basel, 2004. MR2058652 (2005f:11119)

[2] J. Quer, *Embedding problems over abelian groups and an application to elliptic curves.* J. Algebra **237** (2001), no. 1, 186–202. MR1813898 (2002b:12008)

[3] J. Quer, *La classe de Brauer de l'algèbre d'endomorphismes d'une variété abélienne modulaire.* C. R. Acad. Sci. Paris Sér. I Math. **327** (1998), no. 3, 227–230. MR1650241 (99j:14045)

[4] K. Ribet, *Fields of definition of abelian varieties with real multiplication.* Arithmetic geometry (Tempe, AZ, 1993), 107–118, Contemp. Math., **174**, Amer. Math. Soc., Providence, RI, 1994. MR1299737 (95i:11057)

[5] K. Ribet, *Abelian varieties over $\mathbb{Q}$ and modular forms.* Modular curves and abelian varieties, 241–261, Progr. Math., **224**, Birkhäuser, Basel, 2004 MR2058653 (2005k:11120)

[6] 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), pp. 193–268. Academic Press, London, 1977. MR0450201 (56:8497)

Universitat Politècnica de Catalunya, Departament Matemàtica Aplicada II, Campus Nord, Edifici Omega, Despatx 438, Jordi Girona 1–3, 08034-Barcelona, Spain
E-mail address: Jordi.Quer@upc.edu