Arithmetic properties of abelian varieties under Galois conjugation

Xavier Guitart Morales

2010 *Mathematics Subject Classification.* 11G10, 11G18.

Arithmetic properties of abelian varieties under Galois conjugation

Tesi doctoral
Autor: Xavier Guitart Morales
Director: Jordi Quer Bosor
Departament de Matemàtica Aplicada II
Universitat Politècnica de Catalunya

A la meva àvia.

Contents

Notation

If k is a field then $\overline{k}$ denotes an algebraic closure of k, k_s a separable closure of k and $G_k = \mathrm{Gal}(k_s/k)$. All rings we consider are associative and with unity. If R is a ring then $\mathrm{M}_n(R)$ is the ring of $n \times n$ matrices with coefficients in R, and $\mathrm{GL}_n(R)$ is the group of invertible elements of $\mathrm{M}_n(R)$. When working with equivalence relations we will usually denote by $[x]$ the equivalence class of x. The dimension of an F-vector space E is denoted either by $\dim_F E$ or by $[E : F]$ if $F \subseteq E$.

For an algebraic variety V defined over k and a field K containing k we write V_K for the extension of scalars $V \times_{\mathrm{Spec}\, k} \mathrm{Spec}\, K$. If A is an abelian variety over k, $\mathrm{End}_k(A)$ denotes its ring of endomorphisms defined over k. If k is clear by the context, this ring is sometimes denoted by $\mathrm{End}(A)$. We mainly work in the category of abelian varieties up to isogeny, and the notation $\mathrm{End}^0_k(A)$ stands for the endomorphism algebra $\mathrm{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Introduction

This thesis is concerned with several arithmetic properties of abelian varieties that are isogenous to their Galois conjugates. To be more precise, the central object of study are *abelian k-varieties*, especially in the case where k is a number field. That is, we discuss abelian varieties B over $\overline{k}$ such that for each $\sigma \in \mathrm{Gal}(\overline{k}/k)$ there exists an isogeny $\mu_\sigma \colon {}^\sigma B \to B$ satisfying $\varphi \circ \mu_\sigma = \mu_\sigma \circ {}^\sigma\varphi$ for all $\varphi \in \mathrm{End}_{\overline{k}}(B)$. We study their simple factors, their endomorphism algebras and their fields of definition.

In the case $k = \mathbb{Q}$, an interesting type of abelian $\mathbb{Q}$-varieties are the so-called *building blocks*: those whose endomorphism algebra is a central division algebra over a totally real number field F, with Schur index $t = 1$ or $t = 2$ and reduced degree $t[F : \mathbb{Q}]$ equal to the dimension of the variety. The interest in these geometric objects arose in connection with the Shimura-Taniyama conjecture about modularity of elliptic curves over $\mathbb{Q}$, and its generalizations to higher dimensional varieties over $\mathbb{Q}$ as well as to varieties over number fields. Indeed, building blocks are known to be the $\overline{\mathbb{Q}}$-simple factors up to isogeny of non-CM abelian varieties over $\mathbb{Q}$ of GL_2-type. As Ribet showed in [**Ri92**], the recently proven Serre's conjecture on 2-dimensional mod p Galois representations (now a theorem of Khare and Wintenberger [**KW09**]) implies that the GL_2-type varieties are precisely the $\mathbb{Q}$-simple factors of modular Jacobians $J_1(N)$. As a consequence, building blocks are the modular abelian varieties over $\overline{\mathbb{Q}}$, in the sense that they are the $\overline{\mathbb{Q}}$-simple factors of the modular Jacobians $J_1(N)_{\overline{\mathbb{Q}}}$.

The modularity of building blocks is a key property that can be exploited for the study of their arithmetic or for applications to other problems. For instance, the theory of Heegner points and Gross-Zagier type formulas can be used to prove partial results in the direction of the Birch and Swinnerton-Dyer conjecture. On the other hand, the modularity of $\mathbb{Q}$-curves has been exploited to solve some diophantine equations of Fermat-type; cf. the work of Ellenberg [**Ell04**] or Dieulefait and Jiménez [**DJ09**]. It is worth noting that the $\mathbb{Q}$-curves C/K that are suitable for this application are those whose L-series $L(C/K; s)$ are a product of L-series of modular forms.

In spite of this, many of the interesting arithmetic properties of building blocks were established before they were known to be modular, being just a consequence of the existence of compatible isogenies to their Galois conjugates and of the structure of their endomorphism algebras. Indeed, a lot of research has been done on the subject since the seminal work of

Ribet. For instance, Ribet himself proved in [**Ri92**] that every elliptic $\mathbb{Q}$-curve arises as the $\overline{\mathbb{Q}}$-simple factor of some GL_2-type variety over $\mathbb{Q}$. Elkies [**El02**] showed that non-CM elliptic k-curves are parametrized up to isogeny by k-rational points on modular curves $X^*(N)$ for squarefree integers N. As a consequence, he obtained results on the possible fields of definition of such k-curves up to isogeny. Shortly after, and motivated by Elkies's work, Ribet studied in [**Ri94**] the relation between the field of moduli and the field of definition of abelian k-varieties with real multiplication. Quer [**Qu00**] performed a similar study for the possible fields of definition of a $\mathbb{Q}$-curve C together with the corresponding isogenies between Galois conjugates. In addition, he characterized the fields K with the property that the restriction of scalars $\mathrm{Res}_{K/\mathbb{Q}}(C)$ is isogenous over $\mathbb{Q}$ to a product of GL_2-type varieties. After the validity of Serre's conjecture, this property guarantees that $L(C/K;s)$ is a product of L-series of modular forms.

Many of the results of Ribet for $\mathbb{Q}$-curves or for building blocks with real multiplication were generalized to the case of arbitrary building blocks by his student Elizabeth Pyle in her 1995 PhD thesis [**Py02**]. In particular, she completed the characterization of building blocks as the $\overline{\mathbb{Q}}$-simple factors of non-CM GL_2-type varieties, establishing a correspondence between the two kinds of objects: every such GL_2-type variety is isogenous over $\overline{\mathbb{Q}}$ to the power of a building block, and every building block appears as the $\overline{\mathbb{Q}}$-simple factor of some GL_2-type variety. In the last section of [**Py02**] some questions were posed about how this correspondence could be generalized to GL_2-type varieties over other fields k. This was the starting point of the present thesis, which naturally led us to investigate other related properties of abelian k-varieties.

We focus on three different aspects of the arithmetic of abelian k-varieties. First, we aim to give a practical method for computing their possible fields of definition up to isogeny. Second, we provide an answer to the question in Pyle's thesis, by characterizing the absolutely simple factors of GL_2-type varieties over number fields k. A generalization of the Shimura-Taniyama conjecture for Hilbert modular forms predicts that GL_2-type varieties are precisely the modular abelian varieties when k is totally real (cf. [**Da00**, Conjecture 2.4] for a precise statement). Third, we characterize the abelian k-varieties B/K such that their restriction of scalars $\mathrm{Res}_{K/k}(B)$ is isogenous over k to a product of GL_2-type varieties. Observe that this implies that $L(B/K;s)$ is then a product of L-series of GL_2-type varieties over k.

On the other hand, as we said above, many good arithmetic properties of building blocks come from the structure of their endomorphism algebra and from the existence of isogenies to their Galois conjugates. In view of this, it seems natural to consider also the problem of extending the techniques applied to building blocks to as wide a class of abelian varieties as possible. For this reason, the strategy that we follow in this thesis is the following. First of all, we abstract the properties of building blocks that provide them with good arithmetic behavior. Then we consider the most general abelian

varieties with these properties, and we study if analogous results for the arithmetic of these varieties hold in the more general situation. In this way we address the three concrete above mentioned problems, but stating some results in greater generality whenever possible.

Outline of the main results. In order to identify the widest setting to which each part of the building block theory can be extended, the chapters follow a somewhat decreasing level of generality. After Chapter 1, which is devoted to standard background material, in Chapter 2 we begin by considering an arbitrary field k, and by looking into abelian varieties with field of moduli k up to isogeny: that is, varieties B/k_s that are k_s-isogenous to their Galois conjugates. A descent theorem of Ribet characterizes under what conditions such a variety is isogenous to a variety defined over k. However, in concrete cases it is sometimes difficult to verify whether such conditions are satisfied or not. The main result of this chapter is Theorem 2.16, in which Ribet's theorem is used in order to identify two obstructions to descend the field of definition. Such a characterization of the descent property is more suitable for practical computations, as it will be clear from the examples provided in Section 4.3.

After Chapter 2, we gradually consider more restricted settings. In Chapter 3 we deal with abelian k-varieties, which are a special type of varieties with field of moduli k. In Proposition 3.16 we use the results of the previous chapter to characterize their fields of definition up to isogeny, in terms of certain cohomology classes canonically attached to them. Moreover, in Proposition 3.18 we characterize their fields of complete definition (that is, where the endomorphisms and the isogenies to the Galois conjugates are defined), also in terms of those cohomology classes.

The results of Chapter 3 concerning fields of definition can be made very explicit for abelian k-varieties of the first kind, due to the particularly simple structure of the cohomology groups involved in this case. This is what we do in Chapter 4. In it we perform the technical computations that are necessary in order to determine in practice the minimal fields of definition up to isogeny. In the particular case $k = \mathbb{Q}$, this method can be seen as a complement to Ribet and Pyle's study of the field of definition of building blocks. Indeed, they dealt with fields of definition of building blocks together with their endomorphisms. In the case of quaternionic multiplication, the varieties can sometimes be defined over smaller fields than their endomorphisms, and this is what our approach permits to detect. In Section 4.3 we illustrate this phenomenon in concrete examples of building blocks with quaternionic multiplication. For them we apply the techniques developed through the chapter to explicitly compute their minimal fields of definition, which are sometimes smaller than the minimal fields of definition of the endomorphisms.

In Chapter 5 we put ourselves in the case where k is a number field. One of the main goals is to prove Proposition 5.29, which provides the

correspondence between GL_2-type varieties over k and certain k-varieties. However, the key property of GL_2-type varieties that permits to establish such a correspondence is that they are k-varieties defined over k, for which the algebra $\mathrm{End}_k^0(A)$ is a maximal subfield of $\mathrm{End}_{\overline{k}}^0(A)$. Thus, we identify the varieties satisfying this property as the more general class for which a similar correspondence holds. We call them *Ribet-Pyle varieties*. In Proposition 5.2 we see that every Ribet-Pyle variety is $\overline{k}$-isogenous to a power of a k-variety, and in Theorem 5.3 we prove the converse: every abelian k-variety is the $\overline{k}$-simple factor of some Ribet-Pyle variety. From this we deduce the above mentioned correspondence for GL_2-varieties over k. We also study restrictions of scalars of k-varieties. To be more precise, we compute their algebra of endomorphisms defined over k (Proposition 5.32), and we characterize when they are isogenous to products of Ribet-Pyle varieties over k (Propositions 5.35 and 5.36).

In the final two chapters we take $k = \mathbb{Q}$, and we study some properties of abelian $\mathbb{Q}$-varieties related to their modularity. The main result of this part of the thesis is Theorem 6.17. It is a characterization of the abelian varieties over a number field K with the property that $L(B/K; s)$ is a product of L-series of classical elliptic modular forms over $\mathbb{Q}$. The varieties satisfying this property, which we have called *strongly modular*, are the ones that are useful in most of the applications of modularity. For instance, as we mentioned above this is the property needed for their use in solving diophantine equations. Another important consequence is that their L-series $L(B/K; s)$ are known to satisfy the Hasse conjecture.

Finally, in Chapter 7 we present some explicit examples of strongly modular abelian varieties. They are surfaces with quaternionic multiplication, constructed as Jacobians of genus 2 curves given by explicit equations over number fields. Thus they are constructed without any use of modular forms. By applying the results of Chapter 6 we deduce their strong modularity just as a consequence of their geometric and arithmetic properties. As an illustration of our results, in some cases we are able to explicitly identify the corresponding modular forms, which give the L-series of the varieties as products of L-series of modular forms.

Agraïments. Voldria agrair molt sincerament al meu director, en Jordi Quer, tota la seva ajuda i la seva generositat a l'hora de compartir les idees matemàtiques, sense les quals aquesta tesi no hauria estat possible.

Faig extensiu l'agraïment als companys del grup de teoria de nombres de Barcelona i de la UPC. Entre ells, i de manera molt especial, a aquells amb qui he compartit aventura: en Francesc Fité, en Santi Molina, en Juanjo Rué, en Francesc Creixell i en Luis Emilio Garcia. També a l'Enrique González-Jiménez, amb qui he tingut l'oportunitat i el plaer de treballar, i a en Víctor Rotger, de qui també és sempre un plaer aprendre matemàtiques. No em puc oblidar tampoc d'agrair a en Josep Grané tot el seu ajut i el seu guiatge, ja des que vaig començar la carrera.

També vull donar les gràcies als amics que, més sovint del que potser imaginen, en certa manera han contribuït a fer possible aquest treball. Entre ells hi ha els companys de dinars i tertúlies: en Miquel, l'Oriol, en Felipe i l'Alex; els companys de pis: la Mari, l'Aina i l'Eneko; els amics d'abans de venir a Barcelona: l'Isa, en Marc i la Irene; algunes persones que han estat importants per mi però potser mai llegiran aquestes línies: la Núria i la Sandra; i algunes que ho són i segur que les llegiran, en especial la Maria.

Finalment, dono les gràcies als meus pares i al meu germà, que en tot moment han estat al meu costat.

CHAPTER 1

Background

The first chapter is devoted to summarize the material that constitutes the background for the rest of the thesis. The aim is twofold: first, to present in a concise and in a (as much as possible) self-contained way the definitions and results that will play a role later on; second, to settle the notation and terminology related to the algebraic and geometric objects that we will use throughout the thesis.

The contents of sections 1.1 to 1.4 are well-known facts about group cohomology, simple algebras and abelian varieties, that can be found in the standard references for these topics. Because of this, we will not give explicitly a reference for each of the results that we state; instead, we will give some general references at the beginning of each section, providing a citation for a particular statement only if it cannot be found in the general references. Section 1.5 is a brief review of the definitions and properties of abelian varieties of GL_2-type over $\mathbb{Q}$ and their simple factors over $\overline{\mathbb{Q}}$.

1.1. Galois cohomology

A standard reference for the basic facts on group and Galois cohomology is [**Se79**, Chapter VII], and this section is largely based on it. Another excellent reference is [**Mi08**, Chapter II].

Definitions and basic properties. The case of interest to us is that of a Galois group, endowed with the Krull topology, which acts naturally on some algebro-geometric object. For this reason, we will mainly consider the case of profinite groups acting continuously on discrete modules. Let G be a profinite group and let M be a discrete abelian G-module, written multiplicatively. We write the continuous G-action on M exponentially on the left

$$\begin{array}{ccc} G \times M & \longrightarrow & M \\ (\sigma, m) & \longmapsto & {}^{\sigma}m, \end{array}$$

so that ${}^{\sigma}(mn) = {}^{\sigma}m\,{}^{\sigma}n$ and ${}^{(\sigma\tau)}m = {}^{\sigma}({}^{\tau}m)$ for all $\sigma, \tau \in G$, $m, n \in M$. A continuous action of G on M is the same as a continuous group homomorphism $G \to \mathrm{Aut}(M)$. Let M^G be the submodule of fixed elements

$$M^G = \{m \in M \,|\, {}^{\sigma}m = m \text{ for all } \sigma \in G\}.$$

The functor $M \mapsto M^G$ is left exact. Its right derived functors are the *cohomology groups of G with coefficients in M*, denoted $H^r(G, M)$ for $r \geqslant 0$.

Next we recall how they can be computed in terms of continuous cochains, cocycles and coboundaries.

The set $C^r(G,M)$ of continuous maps $G^r \to M$ is a group, called the *group of r-cochains* of G with values in M (here G^0 is taken to be $\{1\}$). Let $d^r\colon C^r(G,M) \to C^{r+1}(G,M)$ be the homomorphism given by

$$(d^r c)(\sigma_1,\dots,\sigma_{r+1}) = \\ {}^{\sigma_1}c(\sigma_2,\dots,\sigma_{r+1}) \left(\prod_{i=1}^{r} c(\sigma_1,\dots,\sigma_i\sigma_{i+1},\dots,\sigma_{r+1})^{(-1)^i}\right) c(\sigma_1,\dots,\sigma_r)^{(-1)^{r+1}}.$$

The group of *r-cocycles* of G with values in M is defined to be $Z^r(G,M) = \ker(d^r)$, and the group of *r-coboundaries* is $B^r(G,M) = \mathrm{im}(d^{r-1})$. By direct computation one sees that $d^{r+1}\circ d^r = 1$, so that $B^r(G,M) \subseteq Z^r(G,M)$. The *$r$-th cohomology group of G with coefficients in M* can be then computed as

$$H^r(G,M) = Z^r(G,M)/B^r(G,M).$$

If c belongs to $Z^r(G,M)$ we will denote by $[c]$ its class in $H^r(G,M)$. Two r-cocycles are said to be *cohomologous* if they differ by a coboundary.

Remark 1.1. The groups $H^r(G,M)$ depend not only on G and M, but also on the action $\Theta\colon G \to \mathrm{Aut}(M)$. We will write $H^r(G,M;\Theta)$ if we need to make it explicit. The notation $H^r(G,M;1)$ means that the action considered is the *trivial* one (i.e. the one such that ${}^\sigma m = m$ for all $\sigma \in G$, $m \in M$). Moreover, if the group G is the Galois group of a finite extension $K/\mathbb{Q}$ and its action on M is clear by the context, we will often write $H^r(K/\mathbb{Q},M)$ instead of $H^r(\mathrm{Gal}(K/\mathbb{Q}),M)$.

It follows from the definition of cohomology groups as derived functors that given an exact sequence of discrete G-modules

$$1 \to M \to N \to P \to 1,$$

there exist *connecting homomorphisms* $\delta^r\colon H^r(G,P) \to H^{r+1}(G,M)$ giving rise to the cohomology long exact sequence

$$\cdots \to H^r(G,N) \to H^r(G,P) \xrightarrow{\delta^r} H^{r+1}(G,M) \to H^{r+1}(G,N) \to \cdots.$$

In fact, if c is an element in $Z^r(G,P)$ one can compute a representative for $\delta^r([c])$ in the following way: lift the map $c\colon G^r \to P$ to a map $\tilde{c}\colon G^r \to N$; then, since $d^r(c) = 1$, necessarily $d^r(\tilde{c})$ takes values in M so that $d^r(\tilde{c}) \in Z^{r+1}(G,M)$, and one defines $\delta^r([c])$ to be the class of $d^r(\tilde{c})$.

An important property of the continuous cohomology groups $H^r(G,M)$ is that they are torsion groups for all $r > 0$.

Inflation and restriction. If H is a subgroup of G then M is a discrete H-module. Composing the inclusion $H^r \to G^r$ with a cocycle $c\colon G^r \to M$ one obtains a cocycle $H^r \to M$. This induces the so-called *restriction homomorphism*

$$\mathrm{Res}\colon H^r(G,M) \longrightarrow H^r(H,M).$$

Similarly, if H is a normal subgroup of G then M^H is a G/H-module. Composing the natural map $G^r \to (G/H)^r$ with cocycles $c\colon (G/H)^r \to M^H$ gives the *inflation homomorphism*

$$\mathrm{Inf}\colon H^r(G/H, M^H) \longrightarrow H^r(G, M).$$

Particular cases: $H^1(G,M)$ and $H^2(G,M)$. Since we will only work with first and second cohomology groups in this thesis, we particularize the above definitions to these cases. A 1-cocycle is a continuous map $c\colon G \to M$ such that

$$c(\sigma\tau) = c(\sigma)^\sigma c(\tau)$$

for all $\sigma, \tau \in G$. A 1-coboundary is a map $G \to M$ of the form $\sigma \mapsto m^{-1\sigma}m$ for some $m \in M$. Then $H^1(G,M)$ is the group of 1-cocycles modulo the subgroup of 1-coboundaries. In particular, if the action of G on M is trivial then $H^1(G,M)$ can be identified with $\mathrm{Hom}(G,M)$, the group of continuous homomorphisms from G to M.

A 2-cocycle is a continuous map $c\colon G \times G \to M$ such that

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

for all $\rho, \sigma, \tau \in G$, and a 2-coboundary is a map $G \times G \to M$ of the form $(\sigma,\tau) \mapsto s(\sigma)^\sigma s(\tau)s(\sigma\tau)^{-1}$ for some continuous map $s\colon G \to M$.

A 2-cocycle c is said to be *normalized* if $c(1,1) = 1$. Every 2-cocycle is cohomologous to a normalized one. Indeed, if $c(1,1) = m$ consider the constant map $\lambda_m\colon G \to M$ such that $\lambda_m(\sigma) = m^{-1}$; then $d^1(\lambda_m)c$ is normalized.

An application of H^2: group extensions. Let G be a group and let A be an abelian group. An *extension* of G by A is an exact sequence of groups

$$1 \longrightarrow A \xrightarrow{\iota} \tilde{G} \xrightarrow{\pi} G \longrightarrow 1.$$

Two such extensions are said to be equivalent if there exists an isomorphism $\phi\colon \tilde{G}_1 \to \tilde{G}_2$ such that the following diagram commutes:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{\iota_1} & \tilde{G}_1 & \xrightarrow{\pi_1} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{Id}} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \mathrm{Id}} & & \\ 1 & \longrightarrow & A & \xrightarrow{\iota_2} & \tilde{G}_2 & \xrightarrow{\pi_2} & G & \longrightarrow & 1. \end{array}$$

We remark that the isomorphism class of $\tilde{G}$ does not determine the equivalence class of the extension in general, because it is necessary to specify the epimorphism $\tilde{G} \xrightarrow{\pi} G$. In particular, there might exist non-equivalent extensions with isomorphic groups $\tilde{G}_1$ and $\tilde{G}_2$.

We can make G act on A in the following way: for each $\sigma \in G$ choose a preimage $\tilde{\sigma}$ for it in $\tilde{G}$, and define ${}^\sigma a = \tilde{\sigma}a\tilde{\sigma}^{-1}$ (for simplicity in the notation it is convenient to identify A with a subgroup of G via ι). This gives a group

homomorphism $\Theta\colon G \to \mathrm{Aut}(A)$, and we will denote by $H^2(G, A; \Theta)$ the second cohomology group with respect to this action Θ.

The action Θ defined above only depends on the equivalence class of the extension. From now on we fix an action Θ and we consider extensions of G by A with associated action Θ. A (set theoretic) *section* for π is a map $s\colon G \to \tilde{G}$ such that $\pi \circ s = \mathrm{Id}$. Given a section s, the map $c_s\colon G \times G \to A$ defined by $c_s(\sigma, \tau) = s(\sigma)s(\tau)s(\sigma\tau)^{-1}$ belongs to $Z^2(G, A; \Theta)$. For a different choice of the section for π, one obtains a 2-cocycle cohomologous to c_s. In this way one can associate to each extension of G by A (with action Θ) an element of $H^2(G, A; \Theta)$.

Proposition 1.2. *The above construction gives a one-to-one correspondences between the set of equivalence classes of extensions of G by A with action Θ and $H^2(G, A; \Theta)$.*

In the next section we will see another example where 2-cohomology groups are used to classify equivalence classes of certain objects, in that case of central simple algebras.

Non-abelian cohomology. If M is non-abelian, the above definitions can be adapted to define $H^0(G, M)$ and $H^1(G, M)$, in such a way that these objects satisfy some analogous properties to the ones of the corresponding cohomology groups in the abelian case. Let M be a discrete non-abelian G-module. $H^0(G, M)$ is defined as M^G. A 1-*cocycle* is a continuous map $c\colon G \to M$ such that $c(\sigma\tau) = c(\sigma)^\sigma c(\tau)$ for all $\sigma, \tau \in G$. Two 1-cocycles c and c' are *cohomologous* if $c'(\sigma) = m^{-1}c(\sigma)^\sigma m$ for some $m \in M$. This defines an equivalence relation in the set $Z^1(G, M)$ of 1-cocycles, and $H^1(G, M)$ is the quotient set. We remark that $H^1(G, M)$ does not have in general a natural group structure; instead, it is regarded as a pointed set (i.e. as a set with a distinguished element), with the distinguished element being the class of the map $\sigma \mapsto 1$.

If $1 \to M \to N \to P \to 1$ is an exact sequence of non-abelian G-modules there is a morphism of pointed sets $\Delta\colon H^0(G, P) \to H^1(G, M)$ such that the sequence

$$1 \to M^G \to N^G \to P^G \xrightarrow{\Delta} H^1(G, M) \to H^1(G, N) \to H^1(G, P) \tag{1.1}$$

is exact (the kernel of a morphism of pointed sets is the preimage of the distinguished element). Moreover, if M lies in the center of N then there is a morphism of pointed sets $\delta\colon H^1(G, P) \to H^2(G, M)$ such that (1.1) can be extended to an exact sequence

$$\cdots \to P^G \xrightarrow{\Delta} H^1(G, M) \to H^1(G, N) \to H^1(G, P) \xrightarrow{\delta} H^2(G, M).$$

The definition of δ goes as follows. Let c be an element of $Z^1(G, P)$. For each $\sigma \in G$ take a preimage $\tilde{c}(\sigma)$ of $c(\sigma)$ in N. Then $\delta([c])$ is represented by the class of the map $(\sigma, \tau) \mapsto \tilde{c}(\sigma)^\sigma \tilde{c}(\tau)\tilde{c}(\sigma\tau)^{-1}$.

An application of H^1: Twists of varieties. An interpretation of the first cohomology group that will be important for us is that it classifies twists of some geometric objects. Next we recall the case of projective varieties.

Let X be a quasiprojective variety over a separable field k. A *twist* of X is a variety Y over k which is isomorphic to X over $\overline{k}$ (that is, $X_{\overline{k}}$ and $Y_{\overline{k}}$ are isomorphic). Let $\mathrm{Aut}_{\overline{k}}(X)$ denote the group of automorphisms of $X_{\overline{k}}$. Since X is defined over k, the Galois group $G = \mathrm{Gal}(\overline{k}/k)$ acts in a natural way on the automorphisms of $X_{\overline{k}}$, so that $\mathrm{Aut}_{\overline{k}}(X)$ is a discrete G-module (the continuity of the action being a consequence of the fact that every endomorphism of X is defined over a finite extension of k).

Given a twist Y of X and a $\overline{k}$-isomorphism $\phi\colon Y \to X$, the map $c_Y : G \to \mathrm{Aut}_{\overline{k}}(X)$ given by $c_Y(\sigma) = {}^{\sigma}\phi \circ \phi^{-1}$ is easily checked to be a 1-cocycle of G with values in $\mathrm{Aut}_{\overline{k}}(X)$. With another choice of the isomorphism ϕ one obtains a cohomologous cocycle, and if Z is k-isomorphic to Y then $[c_Z] = [c_Y]$. This gives therefore a well defined map between the set of k-isomorphism classes of twists of X and $H^1(G, \mathrm{Aut}_{\overline{k}}(X))$.

Proposition 1.3. *If X is a quasiprojective variety over k then the above construction is a natural one-to-one correspondence*

$$\frac{\{\textit{Twists of } X\}}{k\textit{-isomorphism}} \overset{1:1}{\longleftrightarrow} H^1(G, \mathrm{Aut}_{\overline{k}}(X)).$$

The fact that to each cohomology class corresponds a twist of X is a consequence of the results of Weil [**We56**] on Galois descent of varieties. However, what we will use throughout the thesis is an analogous correspondence in the category of abelian varieties up to isogeny, which is a consequence of the results of Ribet on Galois descent in this category (cf [**Ri92**, §8] or Remark 2.6 below).

1.2. Central simple algebras

There are many excellent sources describing the theory of central simple algebras. For instance, [**Pi82**] gives a detailed exposition of it, and this is the book we will use in subsequent chapters as a reference for some specific results. However, the brief review of the basic material we present in this section is more similar to Chapter IV of [**Mi08**], which provides a very concise introduction to this topic.

Simple and semisimple algebras. Let F be a field. A *F-algebra* is a ring A whose center contains F; it is called *central* F-algebra if its center is equal to F. A *subalgebra* of a F-algebra is a subring that contains F; in particular, a *subfield* of A is a field $E \subseteq A$ such that $F \subseteq E$. A *F-algebra homomorphism* $\phi\colon A \to B$ is a F-linear ring homomorphism such that $\phi(1_A) = 1_B$. All F-algebras we consider throughout this section are assumed to be of finite dimension over F.

A F-algebra is *simple* if it has no two-sided ideals other that 0 and A, and it is *semisimple* if it is a direct sum of simple algebras. A *division*

algebra is an algebra such that every nonzero element x has an inverse, i.e. an element x^{-1} such that $xx^{-1} = x^{-1}x = 1$. A division algebra D is obviously simple; in fact, the algebra $\mathrm{M}_n(D)$ is simple as well. The following celebrated theorem states that these matrix algebras over division algebras are essentially all simple algebras up to isomorphism.

Theorem 1.4 (Wedderburn)**.** *Let A be a finite dimensional simple F-algebra. Then there exists a division F-algebra D, which is uniquely determined up to isomorphism, and a positive integer n such that A is isomorphic to $\mathrm{M}_n(D)$.*

Since the center of a division algebra is a field, Wedderburn's Theorem implies that the center of a simple algebra is also a field (because the center of $\mathrm{M}_n(D)$ is isomorphic to the center of D). Hence, any simple algebra is central over its center. Moreover, the center of a semisimple algebra is a product of fields.

Next we state another famous theorem that characterizes the automorphisms of a central simple algebra.

Theorem 1.5 (Skolem-Noether)**.** *Let B be a simple F-algebra and let A be a central simple F-algebra. If $\phi, \psi \colon B \to A$ are F-algebra homomorphisms, then there exists an element $a \in A^\times$ such that $\phi(b) = a\psi(b)a^{-1}$ for all $b \in B$. In particular, every F-algebra automorphism of A is inner.*

An element of $A^\times$ acts trivially on A by conjugation if and only if it belongs to the center of A. Therefore the group of automorphisms of a central simple F-algebra A is isomorphic to $A^\times/F^\times$.

Centralizers and maximal subfields. Let B be a subalgebra of a F-algebra A. The *centralizer* of B in A is

$$C_A(B) = \{a \in A \mid ba = ab \text{ for all } b \in B\}.$$

Theorem 1.6 (Double Centralizer Theorem)**.** *Let A be a central simple F-algebra and let $B \subseteq A$ be a simple subalgebra. Then $C_A(B)$ is simple, $C_A(C_A(B)) = B$ and*

$$[B : F][C_A(B) : F] = [A : F].$$

A subfield E of A is called a *maximal subfield* if it is maximal with respect to inclusion. The following is a useful characterization of maximal subfields, in the case where F is a number field.

Proposition 1.7. *Let A be a central simple algebra over a number field F, and let E be a subfield of A. Then E is a maximal subfield of A if and only if $C_A(E) = E$.*

Let D be a central division F-algebra. The dimension $[D : F]$ turns out to be a perfect square and the integer $t = [D : F]^{1/2}$ is called the *Schur index* of D. In general, if A is a central simple algebra, by Wedderburn's Theorem $A \simeq \mathrm{M}_n(D)$ for some n and for some division algebra D; in this situation,

the Schur index of A is defined to be the Schur index of D. We see that $[A : F]$ is also a perfect square, and as a consequence of the Double Centralizer Theorem and Proposition 1.7 we have the following characterization of maximal subfields in algebras over number fields.

Proposition 1.8. *Let A be a central simple algebra over a number field F. A subfield E of A is maximal if and only if $[A : F] = [E : F]^2$.*

The Brauer group. Let A and B be two central simple F-algebras. By Wedderburn's Theorem there exist division algebras D_A and D_B such that $A \simeq \mathrm{M}_n(D_A)$ and $B \simeq \mathrm{M}_m(D_B)$ for some positive integers n and m. The algebras A and B are said to be *similar* if $D_A \simeq D_B$. An equivalent condition for similarity is that $A \otimes_F \mathrm{M}_r(F) \simeq B \otimes \mathrm{M}_s(F)$ for some r, s. Similarity is an equivalence relation; let $\mathrm{Br}(F)$ denote the set of equivalence classes.

The fact that the tensor product of two central simple F-algebras is again a central simple F-algebra is used to define an operation in $\mathrm{Br}(F)$ by means of $[A][B] = [A \otimes_F B]$. This is well defined and it induces in $\mathrm{Br}(F)$ a structure of abelian group; $\mathrm{Br}(F)$ is called the *Brauer group* of F. The identity is the class of F, and the inverse of $[A]$ is the class of the opposite algebra A^{opp} (this is an algebra isomorphic to A as F-vector space, but with product $x \cdot y = yx$). The Brauer group is known explicitly for some types of fields. In the following theorem we collect some of these results.

Theorem 1.9. *The Brauer group of an algebraically closed field is trivial. The Brauer group of $\mathbb{R}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, and the class of Hamilton's quaternions $\mathbb{H}$ is the only nontrivial element. The Brauer group of a finite field is trivial. The Brauer group of a nonarchimedean local field is canonically isomorphic to $\mathbb{Q}/\mathbb{Z}$.*

If A is a central simple F-algebra and L is a field containing F, then $A \otimes_F L$ is a central simple L-algebra. Then, the map $A \mapsto A \otimes_F L$ induces a group homomorphism

$$\mathrm{Br}(F) \longrightarrow \mathrm{Br}(L).$$

The kernel of this map is denoted $\mathrm{Br}(L/K)$. A field L is said to *split* A, or it is said to be a *splitting field* of A, if A belongs to $\mathrm{Br}(L/F)$; that is, if $A \otimes_F L$ is isomorphic to a matrix algebra over L. If E is a maximal subfield of A then it *splits* A. It is a well known fact that every central simple F-algebra has a maximal subfield separable over F, and this has the following consequence.

Proposition 1.10. $\mathrm{Br}(F) = \cup \mathrm{Br}(L/F)$ *where L runs over the finite Galois extensions of F in $\overline{F}$.*

Galois cohomology and Brauer Groups. Suppose that F is a perfect field. Let L/F be a finite Galois extension and consider $L^\times$ as a discrete $\mathrm{Gal}(L/F)$ module with the Galois action. Let c be an element in

$Z^2(L/F, L^\times)$, and let A_c be the free L-module with basis $\{e_\sigma\}_{\sigma\in\mathrm{Gal}(L/F)}$. Define a product operation in A_c by the rules

- $e_\sigma x = {}^\sigma x e_\sigma$ for $x \in L$ and $\sigma \in \mathrm{Gal}(L/F)$,
- $e_\sigma e_\tau = c(\sigma,\tau)e_{\sigma\tau}$.

The cocycle condition ensures that the defined product is associative, so that A_c is a ring. Moreover, it is a central simple F-algebra and it contains L as a maximal subfield. If c' is a cocycle cohomologous to c, then $A_{c'}$ and A_c are isomorphic as F-algebras. Hence, there is a well defined map

$$\begin{array}{ccc} H^2(L/F, L^\times) & \longrightarrow & \mathrm{Br}(L/F) \\ [c] & \longmapsto & [A_c]. \end{array}$$

Theorem 1.11. *The above map is in fact a group isomorphism between* $\mathrm{Br}(L/F)$ *and* $H^2(L/F, L^\times)$*. By taking direct limits over* L *one gets a group isomorphism* $H^2(\mathrm{Gal}(\overline{F}/F), \overline{F}^\times) \simeq \mathrm{Br}(F)$*. Finally, if* $F \subseteq M \subseteq \overline{F}$ *then the natural map* $\mathrm{Br}(F) \to \mathrm{Br}(M)\colon [A] \mapsto [A \otimes_F M]$ *corresponds under this isomorphism to* $\mathrm{Res}\colon H^2(\mathrm{Gal}(\overline{F}/F), \overline{F}^\times) \to H^2(\mathrm{Gal}(\overline{F}/M), \overline{F}^\times)$*.*

A consequence of this theorem is that $\mathrm{Br}(F)$ is a torsion group, since the same is true for cohomology groups.

Brauer groups of number fields. Let F be a number field and let A be a central simple F-algebra. If v is a (finite or infinite) place of F then F_v denotes the completion of F at v, and A_v denotes $A \otimes_F F_v$ which is a central simple F_v-algebra. If v is a finite place, then $\mathrm{Br}(F_v)$ is canonically isomorphic to $\mathbb{Q}/\mathbb{Z}$. Hence, there exists a homomorphism $\mathrm{Inv}_v\colon \mathrm{Br}(F) \to \mathbb{Q}/\mathbb{Z}$ sending each A to the element in $\mathbb{Q}/\mathbb{Z}$ that corresponds to A_v under the isomorphism $\mathrm{Br}(F_v) \simeq \mathbb{Q}/\mathbb{Z}$. If v is a real infinite place then $\mathrm{Br}(F_v) \simeq \mathbb{Z}/2\mathbb{Z} \simeq \frac{1}{2}\mathbb{Z}/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z}$. Hence in this case there is also a homomorphism $\mathrm{Inv}_v\colon \mathrm{Br}(F) \to \mathbb{Q}/\mathbb{Z}$. Finally, if v is a complex infinite place, the map $\mathrm{Inv}_v\colon \mathrm{Br}(F) \to \mathrm{Br}(F_v)$ sends each A to 1, since then $\mathrm{Br}(F_v) \simeq \mathrm{Br}(\mathbb{C})$ is trivial. Thus we get a homomorphism $\mathrm{Inv}\colon \mathrm{Br}(F) \to \prod_v \mathbb{Q}/\mathbb{Z}$ as the product of Inv_v for all places v of F. The following deep theorem is a fundamental result in the theory of Brauer groups over number fields.

Theorem 1.12. *Let* F *be a number field. The image of the homomorphism* $\mathrm{Inv}\colon \mathrm{Br}(F) \to \prod_v \mathbb{Q}/\mathbb{Z}$ *lies in* $\bigoplus_v \mathbb{Q}/\mathbb{Z}$*, and the sequence*

$$1 \longrightarrow \mathrm{Br}(F) \xrightarrow{\mathrm{Inv}} \bigoplus_v \mathbb{Q}/\mathbb{Z} \xrightarrow{\Sigma} \mathbb{Q}/\mathbb{Z} \longrightarrow 1$$

is exact.

A central simple algebra A is said to be *split* at a place v of F if $\mathrm{Inv}_v(A) = 0$ or, equivalently, if $A \otimes_F F_v$ is isomorphic to a matrix algebra over F_v. Otherwise, A is said to *ramify* in v. The first part of the previous theorem states that a central simple algebra ramifies only at a finite number of places.

Another important property of Brauer groups over number fields, which is a consequence of Theorem 1.12 and of a study of the Brauer groups of

local fields, is that the order of $[A]$ if $\mathrm{Br}(F)$ is equal to the Schur index of A.

Quaternion algebras. Let F be a field with $\mathrm{char}(F) \neq 2$. A *quaternion algebra* over F is a central simple F-algebra of dimension 4 over F. Every quaternion algebra over F can be described as a free F-module with F-basis $\{1, i, j, k\}$ and multiplication rules $i^2 = a$, $j^2 = b$ and $ij = -ji = k$, for some $a, b \in F^\times$. We will use the symbol $(a, b)_F$ to denote such a quaternion algebra. In particular, $(-1, -1)_{\mathbb{R}}$ is isomorphic to Hamilton's quaternions $\mathbb{H}$.

A quaternion algebra $(a, b)_F$ is either isomorphic to $M_2(F)$ or it is a division algebra; in particular it is a central simple algebra. Its class in $\mathrm{Br}(F)$ has order 1 or 2, and a theorem of Merkur'ev states that the 2-torsion of $\mathrm{Br}(F)$ is generated by the classes of quaternion algebras.

Now suppose that F is a number field, and let $\mathcal{Q}$ be a quaternion algebra over F. For each place v we have that $\mathrm{Inv}_v(\mathcal{Q})$ is equal to 0 or to $1/2$; that is, the knowledge of $\mathrm{Inv}_v(\mathcal{Q})$ is equivalent to know if $\mathcal{Q}$ splits or ramifies in v. The injectivity of the map Inv in Theorem 1.12 implies that the isomorphism class of $\mathcal{Q}$ is determined by the places where $\mathcal{Q}$ ramifies. The exactness at the central group implies that there exists a quaternion algebra that exactly ramifies in a set S of places of F if and only if S is finite of even cardinality and it does not contain any complex place of F.

Reduced norms and traces. Let A be a central simple F-algebra, and let E be a splitting field of A (for instance a maximal subfield, or an algebraically closed field containing F). Then we can find an isomorphism of E-algebras $\phi\colon A \otimes_F E \to \mathrm{M}_n(E)$ for some n. For each $a \in A$, the determinant and the trace of the matrix $\phi(a)$ belong to F, and their values do not depend on E nor on the chosen isomorphism ϕ. The determinant of $\phi(a)$ is called the *reduced norm* of a, and the trace of $\phi(a)$ is called the *reduced trace* of a. They are denoted by $\mathrm{N}_{A/F}(a)$ and $\mathrm{Tr}_{A/F}(a)$ respectively.

Suppose now that F is a finite separable extension of a field k. The *reduced norm of A over k* is defined to be $\mathrm{N}_{A/k} = \mathrm{N}_{F/k} \circ \mathrm{N}_{A/F}$, where $\mathrm{N}_{F/k}$ is the usual norm of field extensions. The *reduced trace of A over k* is defined to be $\mathrm{Tr}_{A/k} = \mathrm{Tr}_{F/k} \circ \mathrm{Tr}_{A/F}$, where $\mathrm{Tr}_{F/k}$ is the usual trace of field extensions.

1.3. Abelian varieties

This section contains a brief review of some of the basic facts on abelian varieties that we will need in the thesis. The main references used are [**Mu70**], [**Mi86**] and [**MoGe**].

Definition and basic properties. Let k be a field. A *group variety* over k is a variety V over k together with two morphisms

$$m\colon V \times V \to V, \quad i\colon V \to V$$

defined over k, and an element $e \in V(k)$ such that m and i define a group structure on $V(\overline{k})$ with identity element e. The quadruple (V, m, i, e) is then a group in the category of varieties over k, so that for any k-algebra S the maps m and i induce a group structure on $V(S)$.

Definition 1.13. An *abelian variety over* k is a complete group variety over k.

Although only completeness is required in the definition, an important property is that there exists an ample divisor on an abelian variety, which implies that every abelian variety is projective. Moreover, abelian varieties are always nonsingular (in fact this is true for all group varieties). The group law on an abelian variety A is necessarily commutative; accordingly it is usually denoted by $+$, and the identity element by 0.

Homomorphisms. If A and B are abelian varieties over k, a regular morphism of algebraic varieties $A \to B$ over k is a *homomorphism* if the map that it induces on points $A(\overline{k}) \to B(\overline{k})$ is a group homomorphism. The notation $\mathrm{Hom}_k(A, B)$ stands for the set of all such homomorphisms. The set $\mathrm{End}_k(A) = \mathrm{Hom}_k(A, A)$ has a natural group structure given by the addition in A; it is torsion-free and finitely generated as $\mathbb{Z}$-module. What is more, $\mathrm{End}_k(A)$ admits a natural ring structure, with the product being the composition of endomorphisms.

Remark 1.14. The subscript k in the notation for the homomorphisms and endomorphisms emphasizes the fact that they are morphisms defined over k, but it is often suppressed in the modern literature. If the ground field k is clear, we will also follow this convention sometimes, so $\mathrm{Hom}(A, B)$ and $\mathrm{End}(A)$ will denote homomorphisms and endomorphisms defined over k. However, in many situations it will be convenient for us to preserve the subscript for the field of definition, in order to avoid confusions with homomorphism defined over other fields. Indeed, if K is a field containing k we will often consider the set $\mathrm{Hom}_K(A_K, B_K)$ of homomorphisms defined over K. For simplicity we will write $\mathrm{Hom}_K(A, B)$ instead of $\mathrm{Hom}_K(A_K, B_K)$ and $\mathrm{End}_K(A)$ instead of $\mathrm{End}_K(A_K)$. Note that $\mathrm{Hom}_k(A, B) \subseteq \mathrm{Hom}_K(A, B)$, but the inclusion is strict in general. The following property gives some control on the possible fields of definition for the homomorphisms.

Proposition 1.15. *If A and B are abelian varieties over k, then there exists a finite extension K/k (with $K \subset k_s$) such that K is the smallest field of definition of all the endomorphisms from A to B. That is to say, for any field extension $K \subseteq L$ we have that $\mathrm{Hom}_K(A, B) = \mathrm{Hom}_L(A, B)$, and for any field extension $k \subseteq L$ such that $\mathrm{Hom}_L(A, B) \simeq \mathrm{Hom}_{k_s}(A, B)$ then necessarily $K \subseteq L$.*

The Galois group $\mathrm{Gal}(k_s/k)$ acts naturally on $A(k_s)$. For instance, if we consider an embedding of A into $\mathbb{P}^n_k$ and $x = [x_0 : \cdots : x_n] \in A(k_s)$ then for each $\sigma \in \mathrm{Gal}(k_s/k)$ we have that ${}^\sigma x = [{}^\sigma x_0 : \cdots : {}^\sigma x_n]$. The group $\mathrm{Gal}(k_s/k)$

also acts on $\mathrm{Hom}_{k_s}(A,B)$ in the following way: for $f \in \mathrm{Hom}_{k_s}(A,B)$, then ${}^{\sigma}f$ is the homomorphism that on points is given by ${}^{\sigma}f(x) = {}^{\sigma}(f({}^{\sigma^{-1}}x))$. We have a characterization of $\mathrm{Hom}_K(A,B)$ as

$$\mathrm{Hom}_K(A,B) = \{f \in \mathrm{Hom}_{k_s}(A,B) \,|\, {}^{\sigma}f = f \text{ for all } \sigma \in \mathrm{Gal}(k_s/K)\}.$$

Isogenies. Let $f : A \to B$ be a homomorphism of abelian varieties. The *kernel* of f, $\ker(f)$, is the scheme theoretic fibre over $0 \in B$. Such an f is called an *isogeny* if it is exhaustive and it has finite kernel. The *degree* of f is $\deg(f) = [k(A) : k(B)]$, the degree of the extension of function fields given by $f^* : k(B) \to k(A)$. If $g : B \to C$ is another isogeny, then $\deg(g \circ f) = \deg(g)\deg(f)$.

An important example of isogenies are the 'multiplication by n maps': for a positive integer n, the map $n_A \colon A \to A$ given on points by $x \mapsto nx$ is an isogeny of degree n^{2g}, where g is the dimension of A. The kernel of n_A is denoted by $A[n]$, and its points over k_s form a group whose structure is as follows:

$$A[n](k_s) \simeq (\mathbb{Z}/n\mathbb{Z})^{2g} \text{ if } \mathrm{char}(k) \nmid n,$$
$$A[p^m](k_s) \simeq (\mathbb{Z}/p^m\mathbb{Z})^{i} \text{ if } p = \mathrm{char}(k),$$

for some i in the range $0, \ldots, g$. Since n_A is defined over k, if x belongs to $A[n](k_s)$ then for any σ in $\mathrm{Gal}(k_s/k)$ the conjugate point ${}^{\sigma}x$ belongs to $A[n](k_s)$ as well. This gives an action of $\mathrm{Gal}(k_s/k)$ on $A[n](k_s)$.

Abelian varieties up to isogeny. We will mainly work in the category of *abelian varieties up to isogeny*: its objects are abelian varieties, and the homomorphisms from A to B are the elements of $\mathrm{Hom}_k^0(A,B) = \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{Hom}_k(A,B)$. The 0 superscript will be also used to indicate 'tensor product with $\mathbb{Q}$' in similar contexts. For instance, $\mathrm{End}_k^0(A)$ stands for $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_k(A)$, which is a $\mathbb{Q}$-algebra called the *endomorphism algebra* of A; this terminology differentiates it from the *endomorphism ring* $\mathrm{End}_k(A)$.

Given an isogeny $f \colon A \to B$ there exists an isogeny $g \colon B \to A$ such that $f \circ g = n_B$ for some $n > 0$. This property implies that the isogenies are isomorphisms in this category, and from now on if $f \colon A \to B$ is an isogeny f^{-1} will denote its inverse in $\mathrm{Hom}_k^0(A,B)$. Observe that, since the isogenies 'multiplication by n' are defined over k, there is a natural extension of the action of $\mathrm{Gal}(k_s/k)$ on $\mathrm{Hom}_k(A,B)$ to an action on $\mathrm{Hom}_k^0(A,B)$, given by ${}^{\sigma}(r \otimes f) = r \otimes {}^{\sigma}f$ for all $r \in \mathbb{Q}$. By abuse of terminology we will also refer to the elements $r \otimes f$ as isogenies.

Finally, two abelian varieties A and B are *isogenous* if there exists an isogeny from A to B. As we said above, in this case there exists also an isogeny from B to A, so that the property of being isogenous is an equivalence relation. We will write $A \sim_k B$ to indicate that A and B are isogenous.

Remark 1.16. The subindex k indicates that the varieties are isogenous with an isogeny defined over k. As with homomorphisms, if the ground field of A and B is clear to be k we will just write $A \sim B$, and this shall be

understood as $A \sim_k B$. As usual, if K is a field containing k we will write $A \sim_K B$ instead of $A_K \sim_K B_K$, and we will say in this case that A and B are isogenous over K.

Tate modules and ℓ-adic representations. Let ℓ be a prime number. The *ℓ-adic Tate module* of A is defined to be $T_\ell(A) = \varprojlim A[\ell^n](k_s)$, where the inverse system is given by the multiplication by ℓ maps. An element $a = (a_n)$ of $T_\ell(A)$ is a sequence of points $a_n \in A(k_s)$ such that $\ell a_1 = 0$ and $\ell a_n = a_{n-1}$ for all $n > 1$. If ℓ is different from the characteristic of k then $T_\ell(A)$ is a free $\mathbb{Z}_\ell$-module of rank $2g$. Let $V_\ell(A) = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(A)$. Then $V_\ell(A)$ is a $\mathbb{Q}_\ell$-vector space of dimension $2g$. If E is a subfield of $\mathrm{End}_k^0(A)$, then E acts on $V_\ell(A)$ by giving an $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-module structure on $V_\ell(A)$. In fact, we have the following result.

Proposition 1.17. *Let E be a subfield of $\mathrm{End}_k^0(A)$. Then $V_\ell(A)$ is a free $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-module of rank $2g/[E : \mathbb{Q}]$.*

A homomorphism $f\colon A \to B$ gives rise to a group homomorphism $A[n](k_s) \to A[n](k_s)$, and therefore it induces a $\mathbb{Z}_\ell$-homomorphism

$$T_\ell(f)\colon T_\ell(A) \longrightarrow T_\ell(B).$$

In fact, for any ℓ different from the characteristic of k the map

$$\mathrm{Hom}_k(A, B) \longrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(A), T_\ell(B))$$

obtained in this way is injective, and it extends to a map

$$\mathrm{Hom}_k^0(A, B) \longrightarrow \mathrm{Hom}_{\mathbb{Q}_\ell}(V_\ell(A), V_\ell(B)).$$

In the particular case where $A = B$ we have a ring injection

$$T_\ell\colon \mathrm{End}_k(A) \longrightarrow \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A)) \simeq \mathrm{M}_{2g}(\mathbb{Z}_\ell),$$

where the isomorphism is obtained by choosing a $\mathbb{Z}_\ell$-basis of $T_\ell(A)$. If ϕ belongs to $\mathrm{End}_k(A)$ and ℓ is different from $\mathrm{char}(k)$, then the characteristic polynomial $P_\phi(X)$ of $T_\ell(\phi)$ has coefficients in $\mathbb{Z}$ and it does not depend on the prime ℓ; it is called the *characteristic polynomial* of ϕ. The degree 0 coefficient of P_ϕ is equal to $\deg(\phi)$, and the *trace* of ϕ is defined by the identity

$$P_\phi(X) = X^{2g} - \mathrm{Tr}(\phi)X^{2g-1} + \cdots + \deg(\phi).$$

The notions of characteristic polynomial, degree and trace can be extended in the obvious way to elements ϕ in $\mathrm{End}_k^0(A)$ by using the ℓ-adic representation of $\mathrm{End}_k^0(A)$

$$V_\ell\colon \mathrm{End}_k^0(A) \longrightarrow \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A)) \simeq \mathrm{M}_{2g}(\mathbb{Q}_\ell). \tag{1.2}$$

There is a continuous action of $\mathrm{Gal}(k_s/k)$ on $T_\ell(A)$, since it acts on each $A[\ell^n](k_s)$. This gives a *ℓ-adic representation* of $\mathrm{Gal}(k_s/k)$, i.e. a continuous homomorphism

$$\rho_\ell\colon \mathrm{Gal}(k_s/k) \longrightarrow \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A)) \simeq \mathrm{GL}_{2g}(\mathbb{Z}_\ell),$$

where the isomorphism is obtained again by choosing a $\mathbb{Z}_\ell$-basis of $T_\ell(A)$.

L-series. Let K be a number field. For a prime $\mathfrak{p}$ of K we denote by $I_\mathfrak{p} \subseteq G_K$ the inertia group at $\mathfrak{p}$, by $N_\mathfrak{p}$ the number of elements of the residue field and by $\mathrm{Frob}_\mathfrak{p} \in G_K$ a Frobenius element at $\mathfrak{p}$. Let A/K be an abelian variety of dimension g, and let S be the finite set of primes of K that are primes of bad reduction of A. The family of ℓ-adic representations

$$\{\rho_\ell \colon G_K \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A)) \simeq \mathrm{GL}_{2g}(\mathbb{Q}_\ell)\}$$

satisfies the following properties.

(1) If $\mathfrak{p}$ is a prime of K such that $\mathfrak{p}$ does not belong to S and $\mathfrak{p}$ does not divide ℓ, then ρ_ℓ is unramified at $\mathfrak{p}$ (i.e. $\rho_\ell(I_\mathfrak{p}) = \{1\}$).
(2) For every prime $\mathfrak{p}$ of K the polynomial

$$P_\mathfrak{p}(T) = \det(1 - \rho_\ell(\mathrm{Frob}_\mathfrak{p})T)_{V_\ell(A)^{I_\mathfrak{p}}}$$

belongs to $\mathbb{Z}(T)$, and it does not depend on ℓ if $\mathfrak{p} \nmid \ell$.

The *L-series* of A over K is defined to be

$$L(A/K; s) = \prod_\mathfrak{p} P_\mathfrak{p}(N_\mathfrak{p}^{-s})^{-1},$$

where the product runs over all primes of K. The factor $L_\mathfrak{p}(A/K; s) = P_\mathfrak{p}(N_\mathfrak{p}^{-s})^{-1}$ is called the local factor at $\mathfrak{p}$. The following theorem was proved by Faltings in the paper where he also proved the Mordell Conjecture [**Fa86**].

Theorem 1.18 (Faltings Isogeny Theorem)**.** *Let A and A' be abelian varieties defined over $\mathbb{Q}$. They are $\mathbb{Q}$-isogenous if and only if $L_p(A/\mathbb{Q}; s)$ is equal to $L_p(A'/\mathbb{Q}; s)$ for all but finitely many primes p.*

Dual abelian variety and Rosati involution. Now we recall the basic properties that we will need concerning duals of abelian varieties. Let A be an abelian variety over k, and let $\mathrm{Pic}(A)$ be the group of invertible sheaves on A. Let $\mathrm{Pic}^0(A)$ be the group of invertible sheaves invariant under translation

$$\mathrm{Pic}^0(A) = \{\mathcal{L} \in \mathrm{Pic}(A) \mid t_a^*\mathcal{L} \simeq \mathcal{L} \text{ on } A_{\overline{k}} \text{ for all } a \in A(\overline{k})\}.$$

The dual of A is an abelian variety $\hat{A}$ over k such that $\hat{A}(\overline{k}) = \mathrm{Pic}^0(A_{\overline{k}})$, where this identification is given by an invertible sheaf on $A \times \hat{A}$. That is, there exists an invertible sheaf $\mathcal{P}$ on $A \times \hat{A}$ such that for all $a \in \hat{A}(\overline{k})$ the restriction $\mathcal{P}_{|A\times\{a\}}$ represents a in $\mathrm{Pic}^0(A_{\overline{k}})$. It satisfies the properties that are natural to expect of a dual: it is of the same dimension as A, every homomorphism $f \colon A \to B$ over k induces a homomorphism $\hat{f} \colon \hat{B} \to \hat{A}$ over k and $\hat{\hat{A}}$ is canonically isomorphic to A.

Every invertible sheaf $\mathcal{L}$ on $A_{\overline{k}}$ induces a homomorphism $\varphi_\mathcal{L} \colon A_{\overline{k}} \to \hat{A}_{\overline{k}}$ by means of $\varphi_\mathcal{L}(a) = t_a^*(\mathcal{L}) \otimes \mathcal{L}^{-1}$. A *polarization* of A is an isogeny $\lambda \colon A \to \hat{A}$ over k such that, over $\overline{k}$ it is of the form $\varphi_\mathcal{L}$ for some ample sheaf $\mathcal{L}$ on $A_{\overline{k}}$. The pair (A, λ) is called a *polarized abelian variety.*

The *Rosati involution* of $\mathrm{End}_k^0(A)$ associated to a polarization λ is defined to be the map

$$\begin{array}{ccc} \mathrm{End}_k^0(A) & \longrightarrow & \mathrm{End}_k^0(A) \\ \phi & \longmapsto & \phi' = \lambda^{-1} \circ \hat{\phi} \circ \lambda. \end{array}$$

It is easily checked that $(\phi+\alpha)' = \phi' + \alpha'$, $(a\phi)' = a\phi'$ and $(\phi\circ\alpha)' = \alpha' \circ \phi'$ for all $\phi, \alpha \in \mathrm{End}_k^0(A)$, $a \in \mathbb{Q}$. In addition, it is indeed an involution, i.e. $\phi'' = \phi$. A key property of the Rosati involution is that it is positive definite, in the sense that for each nonzero $\phi \in \mathrm{End}_k^0(A)$ the rational number $\mathrm{Tr}(\phi \circ \phi')$ is positive.

Jacobians. Let k be an algebraically closed field and let C/k be a smooth projective curve of genus g. The Jacobian of C is an abelian variety $\mathrm{Jac}(C)$ over k of dimension g, provided with an embedding $C \hookrightarrow \mathrm{Jac}(C)$. When extended linearly to divisors on C, this embedding induces a group isomorphism between $\mathrm{Pic}^0(C)$ and $\mathrm{Jac}(C)(k)$. Moreover, the curve C induces a principal polarization on $\mathrm{Jac}(C)$ (i.e. a polarization $\mathrm{Jac}(C) \to \widehat{\mathrm{Jac}(C)}$ which is an isomorphism); it is called the *canonical polarization* of $\mathrm{Jac}(C)$.

All the above properties of Jacobians also hold when the field k is not algebraically closed, provided that C has at least one k-rational point.

Representations of the endomorphism algebra. In addition to the ℓ-adic representation (1.2), we will often use two other representations of $\mathrm{End}_k^0(A)$. First of all, we recall the space of *tangent vectors* $\mathrm{Lie}(A/k)$, which is a k-vector space of dimension equal to the dimension of A. Since $\mathrm{End}_k^0(A)$ acts on $\mathrm{Lie}(A/k)$ as k-endomorphisms, $\mathrm{Lie}(A/k)$ is indeed a $\mathrm{End}_k^0(A)$-module. See [**Mu70**, §11] for the details about $\mathrm{Lie}(A/k)$.

If k is a subfield of $\mathbb{C}$, then the variety $A_{\mathbb{C}}$ is a complex manifold. It turns out that the first homology group $H_1(A_{\mathbb{C}}, \mathbb{Z})$ is a free abelian group of rank $2\dim(A)$. The homology with coefficients in $\mathbb{Q}$, $H_1(A_{\mathbb{C}}, \mathbb{Q})$, is then a $\mathbb{Q}$-vector space of dimension equal to $2\dim(A)$ with an action of $\mathrm{End}_k^0(A)$.

Restriction of scalars. This paragraph is based on [**We82**, §1.3]. Let K/k be a finite separable field extension and let V/K be an algebraic variety. A variety W/k together with a K-morphism $p\colon W_K \to V$ is called *the restriction of scalars* of V from K to k if it has the following universal property: for every variety X/k and K-morphism $\varphi\colon X_K \to V$, there exists a unique k-morphism $\varphi'\colon X \to W$ such that $p \circ \varphi'_K = \varphi$. The restriction of scalars, if it exists, is unique up to k-isomorphism and we will denote it by $\mathrm{Res}_{K/k}(V)$. Another property, which in fact could be taken as the definition of restriction of scalars (see [**We82**, p. 5]), is the following: if $\sigma_1, \ldots, \sigma_d$ are the distinct k-embeddings of K in $\overline{k}$, then

$$({}^{\sigma_1}p, \ldots, {}^{\sigma_d}p)\colon W \to {}^{\sigma_1}V \times \cdots \times {}^{\sigma_d}V$$

is a $\overline{k}$-isomorphism. As for its existence, we are only concerned with the case where V is quasiprojective, and then it is another consequence of the results of Weil on Galois descent [**We56**].

Theorem 1.19. *If V/K is quasiprojective then $\mathrm{Res}_{K/k}(V)$ exists.*

In particular, if B/K is an abelian variety then $\mathrm{Res}_{K/k}(B)$ exists. Moreover, in this case $\mathrm{Res}_{K/k}(B)$ acquires a structure of abelian variety.

Proposition 1.20. *If B/K is an abelian variety then $A = \mathrm{Res}_{K/k}(B)$ is also an abelian variety, and $p\colon A_K \to B$ is a homomorphism. If C is an abelian variety over k, as a consequence of the universal property p induces an isomorphism $\mathrm{Hom}_K(C, B) \simeq \mathrm{Hom}_k(C, A)$.*

1.4. Endomorphism algebras of abelian varieties

Decomposition into simple varieties up to isogeny. An abelian variety A over k is called *simple* (or simple over k, or k-simple) if there does not exist any abelian variety $B \subseteq A$ over k except 0 and A. If K is a field containing k, we will say that A is simple over K if A_K is simple over K; we remark that a simple variety over k can be non-simple over K. If A is simple over $\overline{k}$ then it is said to be *absolutely simple*. We will also say that A is *isotypical* if it is isogenous to a power of a simple variety.

Theorem 1.21. *Let A be an abelian variety over k. There exist k-simple and pairwise non-isogenous abelian varieties $A_1, \ldots, A_r$, and positive integers $n_1, \ldots, n_r$ such that*

$$A \sim_k A_1^{n_1} \times \cdots \times A_r^{n_r}. \tag{1.3}$$

The varieties A_i are unique up to k-isogeny (and up to permutation) and the associated multiplicities n_i are uniquely determined.

Let A be a simple variety over k, and let $\phi \in \mathrm{End}_k(A)$ be an endomorphism. The connected component of $\ker(\phi)$ containing 0 is an abelian variety, so that it is either 0 or A. Hence, any nonzero endomorphism is an isogeny, and therefore it has an inverse in $\mathrm{End}_k^0(A)$. This shows that $\mathrm{End}_k^0(A)$ is a division algebra, which is of finite dimension over $\mathbb{Q}$. The endomorphism algebra of A^n is then isomorphic to $\mathrm{M}_n(\mathrm{End}_k^0(A))$. In addition, if A and B are non-isogenous then $\mathrm{Hom}_k^0(A, B) = 0$ and $\mathrm{End}_k^0(A \times B) \simeq \mathrm{End}_k^0(A) \times \mathrm{End}_k^0(B)$. Using these properties one can prove the following standard consequence of Theorem 1.21.

Proposition 1.22. *Let A be an abelian variety and let* (1.3) *be its decomposition into k-simple varieties up to isogeny. Then we have that*

$$\mathrm{End}_k^0(A) \simeq \mathrm{M}_{n_1}(D_1) \times \cdots \times \mathrm{M}_{n_r}(D_r),$$

where D_i is the division algebra $\mathrm{End}_k^0(A_i)$.

We see that the endomorphism algebra of an abelian variety is therefore a semisimple finite dimensional algebra over $\mathbb{Q}$.

Classification of endomorphism algebras. Let A be a k-simple abelian variety with endomorphism algebra $D = \mathrm{End}_k^0(A)$. The Rosati involution $'$ on D (associated to a certain polarization) is positive; that is, it satisfies that $\mathrm{Tr}_{D/\mathbb{Q}}(\phi\phi') > 0$ for all $\phi \neq 0$, where $\mathrm{Tr}_{D/\mathbb{Q}}$ is the reduced trace of D over $\mathbb{Q}$ (in fact, we have stated this property before for Tr, the trace of an endomorphism, but Tr is a positive multiple of $\mathrm{Tr}_{D/\mathbb{Q}}$). There is a classification due to Albert of all possible pairs $(D, ')$, with D a finite dimensional division algebra over $\mathbb{Q}$ and $'$ an involution such that $\mathrm{Tr}_{D/\mathbb{Q}}(\phi\phi') > 0$ for all $\phi \neq 0$. This classification applied to $\mathrm{End}_k^0(A)$ gives the following structure theorem for endomorphism algebras of simple abelian varieties.

Theorem 1.23. *Let A be a k-simple abelian variety of dimension g. Let F be the center of $D = \mathrm{End}_k^0(A)$, and let $F_0 = \{x \in D \,|\, x' = x\}$ be the subfield fixed by the Rosati involution $'$. Define the following quantities: $d = [D : F]^{1/2}$, $e = [F : \mathbb{Q}]$ and $e_0 = [F_0 : \mathbb{Q}]$. Then D is isomorphic to an algebra of one of the following four types:*

- *TYPE I. $D = F = F_0$ is a totally real number field and the Rosati involution is the identity. In this case, $e \,|\, g$.*
- *TYPE II. $F = F_0$ is a totally real number field and D is a totally indefinite quaternion division algebra over F. That is, for any embedding $\sigma\colon F \to \mathbb{R}$ one has that $D \otimes_\sigma \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R})$. In this case $2e \mid g$.*
- *TYPE III. $F = F_0$ is a totally real number field and D is a totally definite quaternion division algebra over F. That is, for any embedding $\sigma\colon F \to \mathbb{R}$ one has that $D \otimes_\sigma \mathbb{R} \simeq \mathbb{H}$, where $\mathbb{H}$ denotes Hamilton's quaternions. In this case $e^2 \mid g$.*
- *TYPE IV. F_0 is a totally real number field, F is a CM extension of F_0 (i.e a totally imaginary quadratic extension of F_0) and D is a a division algebra with center F. In this case $e_0 d^2 \mid g$ if $\mathrm{char}(k) = 0$, and $e_0 d \mid g$ if $\mathrm{char}(k) > 0$.*

Observe that F_0 is a totally real number field and that F is equal either to F_0 or to a CM extension of F_0. The variety A is said to be *of the first kind* if $F = F_0$ and *of the second kind* if F is a CM extension of F_0.

Complex multiplication. An abelian variety A over k of dimension g is said to have *complex multiplication* (or CM for short) over k if $\mathrm{End}_k^0(A)$ contains a commutative semisimple algebra of dimension $2g$ over $\mathbb{Q}$. This is the maximal dimension that such a subalgebra can have. If k is a field of characteristic 0, then a k-simple variety has complex multiplication over k if and only if $\mathrm{End}_k^0(A)$ is a CM number field of degree $2g$ over $\mathbb{Q}$.

For simplicity, if we just say that A has CM (without specifying over which field) we mean that A has CM over $\overline{k}$.

1.5. Abelian varieties of GL_2-type and $\mathbb{Q}$-varieties

Ribet introduced in [**Ri92**] the notion of abelian variety over $\mathbb{Q}$ of GL_2-*type*. The initial interest on these varieties relied on its relation with the (at that time conjectural) generalization of the Shimura-Taniyama conjecture (see [**Ri92**, §4] or Section 6.1 of this thesis for more details). In that seminal article, Ribet characterized the 1-dimensional absolutely simple factors up to isogeny of abelian varieties of GL_2-type without CM. This characterization was completed in E. Pyle's thesis [**Py02**], in which the absolutely simple factors up to isogeny of abelian varieties of GL_2-type without CM were characterized (without any dimensional restriction). These absolutely simple factors are known as *building blocks*, and they are a special type of so-called *abelian* $\mathbb{Q}$*-varieties*.

As a motivation for this thesis, we briefly recall in this section the definitions of abelian variety of GL_2-type over $\mathbb{Q}$, of building block and of abelian $\mathbb{Q}$-variety, and we state the relation between these types of varieties.

Definition 1.24. An abelian variety A over $\mathbb{Q}$ is of GL_2-*type* if $\mathrm{End}^0_{\mathbb{Q}}(A)$ is a number field E of degree $[E:\mathbb{Q}] = \dim A$.

Remark 1.25. Since E acts on A as endomorphisms defined over $\mathbb{Q}$, each $\sigma \in G_{\mathbb{Q}}$ acts $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-linearly on $V_\ell(A)$. Then the ℓ-adic representation of $G_{\mathbb{Q}}$ in fact takes values in $\mathrm{Aut}_{E\otimes\mathbb{Q}_\ell}(V_\ell(A))$. Since $V_\ell(A)$ is a free $E\otimes_{\mathbb{Q}}\mathbb{Q}_\ell$-module of rank $2\dim A/[E:\mathbb{Q}] = 2$, by taking a basis one obtains a ℓ-adic representation

$$\rho_\ell \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(E\otimes\mathbb{Q}_\ell).$$

This is the reason why these varieties are called of GL_2-type.

The abelian varieties over $\mathbb{Q}$ of GL_2-type and dimension one are the elliptic curves defined over $\mathbb{Q}$. Indeed, any elliptic curve C over $\mathbb{Q}$ satisfies that $\mathrm{End}^0_{\mathbb{Q}}(C) \simeq \mathbb{Q}$ (even if C has complex multiplication over $\overline{\mathbb{Q}}$).

Definition 1.26. An *abelian* $\mathbb{Q}$*-variety* is an abelian variety $B/\overline{\mathbb{Q}}$ which is $\mathrm{End}^0_{\overline{\mathbb{Q}}}(B)$-equivariantly isogenous to all of its Galois conjugates. That is, for each $\sigma \in G_{\mathbb{Q}}$ there exists an isogeny $\mu_\sigma \colon {}^\sigma B \to B$ such that the following diagram

$$\begin{array}{ccc} {}^\sigma B & \xrightarrow{\mu_\sigma} & B \\ {\scriptstyle {}^\sigma\varphi}\downarrow & & \downarrow{\scriptstyle \varphi} \\ {}^\sigma B & \xrightarrow{\mu_\sigma} & B. \end{array} \tag{1.4}$$

commutes for all $\varphi \in \mathrm{End}^0_{\overline{\mathbb{Q}}}(B)$.

Equivalently, B is an abelian $\mathbb{Q}$-variety if and only if the pair $(B, \mathrm{End}^0_{\overline{\mathbb{Q}}}(B))$ has field of moduli $\mathbb{Q}$.

Definition 1.27. A *building block* is an abelian variety $B/\overline{\mathbb{Q}}$ such that

(1) B is an abelian $\mathbb{Q}$-variety, and
(2) $\mathrm{End}^0_{\overline{\mathbb{Q}}}(B)$ is a central division algebra over a totally real number field F, with Schur index $t = 1$ or $t = 2$ and $t[F : \mathbb{Q}] = \dim B$.

Remark 1.28. Ribet introduced in [**Ri92**] the term $\mathbb{Q}$-*curve* to denote an elliptic curve $C/\overline{\mathbb{Q}}$ that is isogenous to all of its Galois conjugates. If a $\mathbb{Q}$-curve does not have CM, then diagram (1.4) automatically commutes for all $\varphi \in \mathrm{End}^0_{\overline{\mathbb{Q}}}(C)$. Hence, a building block of dimension 1 is the same as a $\mathbb{Q}$-curve without complex multiplication.

Many interesting things can be said about the arithmetic of abelian varieties of GL_2-type and of $\mathbb{Q}$-varieties. For instance, in [**Ch87**] the Brauer class of the algebra of endomorphisms over $\overline{\mathbb{Q}}$ of the varieties of GL_2-type was computed, and in [**Ri94**] the possible fields of definition of $\mathbb{Q}$-varieties were characterized. Moreover, the two kinds of varieties are related by the following theorem, which is [**Py02**, Propositions 1.4 and 4.5].

Theorem 1.29 (Ribet-Pyle)**.** *Let $A/\mathbb{Q}$ be an abelian variety of GL_2-type without complex multiplication. Then $A \sim_{\overline{\mathbb{Q}}} B^n$ for some building block B and some $n > 0$. Conversely, given a building block B there exists an abelian variety $A/\mathbb{Q}$ of GL_2-type such that $A \sim_{\overline{\mathbb{Q}}} B^n$ for some $n > 0$.*

CHAPTER 2

Field of moduli and field of definition up to isogeny

In this chapter we study the field of moduli of an abelian variety up to isogeny. We begin with Section 2.1, containing definitions and some basic properties. In Section 2.2 we introduce the main theme we study in this chapter and also in the next two: the relation between the field of moduli and the field of definition up to isogeny of an abelian variety. In this direction, a theorem of Ribet characterizes completely under what conditions a variety can be defined up to isogeny over its field of moduli. What we do in Section 2.2 is to restate Ribet's result in a convenient way for subsequent computations. More concretely, we state it in terms of the splitting of an exact sequence of topological groups. This leads us to treat in Section 2.3 the splitting of group extensions with non-abelian kernel, and to apply the results obtained to the problem of determining the field of definition up to isogeny of an abelian variety in Section 2.4. The main result of this chapter is Theorem 2.17, which will be the base for our further study of fields of definition up to isogeny. Finally, in Section 2.5 we put the contents of the chapter in a more general framework, and we observe that they can be also used in other situations. This shall be seen as an attempt to identify the most general situation in which the formalism described in this chapter applies, but it will not be used in the rest of the thesis.

2.1. Field of moduli up to isogeny

Let Ω/k be a Galois extension and let G be its Galois group $G = \mathrm{Gal}(\Omega/k)$. Recall that the Krull topology on G has as a basis of open sets around the identity the subgroups of the form $\mathrm{Gal}(\Omega/K)$, with K a finite extension of k. We will be mostly interested in the cases where Ω/k is a finite extension (hence the topology on G is discrete) or where Ω is a separable closure k_s of k. Let B/Ω be an abelian variety.

Definition 2.1. The *field of moduli up to isogeny of B relative to Ω/k* is Ω^H, the subfield of Ω fixed by the subgroup H of G defined as:

$$H = \{\sigma \in \mathrm{Gal}(\Omega/k) \,|\, {}^{\sigma}B \sim B\}.$$

Although B is defined over Ω, it has a model defined over some finite extension L of k; that is, there exists an abelian variety A defined over L such that $B \simeq A_{\Omega}$. For such an L we have that $\mathrm{Gal}(\Omega/L) \subseteq H$, and therefore H

is an open (hence also closed) subgroup of G. By the fundamental theorem of Galois theory, if K is the field of moduli up to isogeny of B relative to Ω/k then $\mathrm{Gal}(\Omega/K) = H$, and K has the property that ${}^{\sigma}B \sim B$ for all $\sigma \in \mathrm{Gal}(\Omega/K)$. In fact, it is the smallest subfield of Ω containing k that has this property, since for any field M such that ${}^{\sigma}B \sim B$ for all $\sigma \in \mathrm{Gal}(\Omega/M)$ we have that $\mathrm{Gal}(\Omega/M) \subseteq H$, and $K = \Omega^H \subseteq M$. In particular, we see that the field of moduli K is a finite extension of k which is included in all possible fields of definition of B.

Observe that the definition of field of moduli we have given depends on the extension Ω/k. Replacing k by the finite extension K if necessary, we can always suppose that k is the field of moduli of B relative to Ω/k, and this is the situation we will consider from now on, because all fields of interest of the theory must contain the field of moduli. We also fix the extension Ω/k and, to simplify the terminology, we will just say that B/Ω has *field of moduli k up to isogeny*. This will indicate that k is the field of moduli up to isogeny of B relative to Ω/k, and by the definitions this is equivalent to the existence, for each $\sigma \in G$, of an isogeny $\phi_\sigma \colon {}^{\sigma}B \to B$. The collection of isogenies $\{\phi_\sigma\}_{\sigma\in G}$ can be taken to be locally constant. This means that there exists a finite extension L/k such that $\phi_\sigma = \phi_\tau$ whenever $\sigma_{|L} = \tau_{|L}$. Indeed, one can take L to be a finite extension of k such that B has a model defined over L (with all the endomorphisms defined over L), which by abusing notation we denote again by B. One can consider compatible isogenies $\mu_s \colon {}^{s}B \to B$ for all $s \in \mathrm{Gal}(L/k)$, and then for $\sigma \in G_k$ define $\phi_\sigma = \mu_s$, where $s = \sigma_{|L}$. In view of this, we make the following definition.

Definition 2.2. Let B/Ω be an abelian variety with field of moduli k up to isogeny. A *system of isogenies for B* is a locally constant set of isogenies $\{\phi_\sigma \colon {}^{\sigma}B \to B\}_{\sigma\in G}$.

Let $\mathcal{B} = \mathrm{End}^0(B)$ be the endomorphism algebra of B. Since $\mathcal{B}$ is semisimple, its center F is a product of number fields, and a system of isogenies for B can be used to define an action $\star$ of G on F: for $\sigma \in G$ and $\varphi \in F$ we define $\sigma \star \varphi = \phi_\sigma \circ {}^{\sigma}\varphi \circ \phi_\sigma^{-1}$. It is easy to check that $\sigma \star \varphi$ belongs to F and that $\star$ is indeed an action. We remark that in verifying the property $\sigma \star (\tau \star \varphi) = (\sigma\tau) \star \varphi$ it is crucial to use the fact that φ belongs to the center of $\mathcal{B}$, and therefore $\star$ will not define in general an action on the whole algebra $\mathcal{B}$, but only on its center F. Moreover, the action on F does not depend on the system of isogenies used: if $\{\mu_\sigma\}_{\sigma\in G}$ is another system of isogenies then

$$\begin{aligned} \mu_\sigma \circ {}^{\sigma}\varphi \circ \mu_\sigma^{-1} &= \mu_\sigma \circ \phi_\sigma^{-1} \circ \phi_\sigma \circ {}^{\sigma}\varphi \circ \phi_\sigma^{-1} \circ \phi_\sigma \circ \mu_\sigma^{-1} \\ &= (\mu_\sigma \circ \phi_\sigma^{-1}) \circ (\sigma \star \varphi) \circ (\mu_\sigma \circ \phi_\sigma^{-1})^{-1} = \sigma \star \varphi, \end{aligned}$$

because $\sigma \star \varphi$ lies in F and it commutes with the elements of $\mathcal{B}$.

If B is isotypical, that is, if $B \sim C^n$ for some simple variety C, then B has field of moduli k if and only if C has field of moduli k. Indeed, if C has field of moduli k then ${}^{\sigma}C \sim C$ and therefore ${}^{\sigma}B \sim {}^{\sigma}C^n \sim C^n \sim B$. On the

other hand, if B has field of moduli k then ${}^{\sigma}B \sim B$ implies that ${}^{\sigma}C^n \sim C^n$, and by the uniqueness of the decomposition of abelian varieties into simple factors up to isogeny we see that ${}^{\sigma}C \sim C$ and B has field of moduli k.

In the general case we have that B decomposes up to isogeny as a product $B_1 \times \cdots \times B_r$, where the B_i's are isotypical varieties with non-isogenous simple factors. If each B_i has field of moduli k, clearly B has also field of moduli k. However, B having field of moduli k does not imply that each B_i has field of moduli k. For instance, consider a simple variety B/M defined over a finite Galois extension M of k but not having field of moduli k. Then $A = \prod_{\tau \in \mathrm{Gal}(K/k)} {}^{\tau}B$ has field of moduli k, but its isotypical factors do not. The problem in this case is that there exist isogenies ${}^{\sigma}A \to A$, but they do not come from isogenies ${}^{\sigma\tau}B \to {}^{\tau}B$ on each isotypical factor. This phenomenon can be detected by means of the action induced by the isogenies ${}^{\sigma}A \to A$ on the center of the endomorphism algebra: the isogenies respect each isotypical factor if and only if the action they define restrict to an action on each simple factor of the center of the endomorphism algebra. In this direction, the following proposition asserts that the only obstruction for an abelian variety with field of moduli k to have all of it simple factors with field of moduli k is precisely this one.

Proposition 2.3. *Let B/Ω be an abelian variety with field of moduli k up to isogeny with isotypical decomposition $B \sim B_1 \times \cdots \times B_r$, and let $F \simeq F_1 \times \cdots \times F_r$ be the associated decomposition of the center of its endomorphism algebra as a product of number fields. Then each B_i has field of moduli k if and only if the action $\star$ on F restricts to an action on each F_i.*

Proof. If each B_i has field of moduli k up to isogeny then for each $\sigma \in G$ there exists an isogeny $\phi_\sigma^i \colon {}^{\sigma}B_i \to B_i$. Define $\phi_\sigma \colon {}^{\sigma}B \to B$ to be the isogeny that is ϕ_σ^i on each component. Let λ_i be an element in F_i, and let λ be the element in F which is λ_i in the i-th component and 0 in the other ones. Then $\sigma \star \lambda$ is equal to $\phi_\sigma^i \circ {}^{\sigma}\lambda_i \circ {\phi_\sigma^i}^{-1}$ in the i-th component and 0 in the others, so the action of G on F restricts to an action of G on F_i.

Suppose now that $\star$ restricts to an action on each F_i. Since B has field of moduli k, for each $\sigma \in G$ there exists an isogeny between ${}^{\sigma}B$ and B, and by the uniqueness of the isotypical decomposition this implies that there exists an isogeny $\phi_{\sigma,i} \colon {}^{\sigma}B_i \to B_{\epsilon(i)}$, for some index $\epsilon(i)$. For λ_i in F_i, let λ be the element in F whose i-th coordinate is λ_i and the others are 0. Then $\sigma \star \lambda$ is the isogeny whose $\epsilon(i)$-th coordinate is $\phi_{\sigma,i} \circ {}^{\sigma}\lambda_i \circ \phi_{\sigma,i}^{-1}$, and the others are 0. Since $\star$ restricts to an action on F_i, we have that $\epsilon(i) = i$ for each i, and each B_i has field of moduli k. □

2.2. Field of moduli versus field of definition

Let B be an abelian variety defined over Ω. If A is an abelian variety defined over k such that A_Ω is isogenous to B, then B has field of moduli k up to isogeny. The converse of this property does not hold in general: if

B/Ω has field of moduli k up to isogeny, there does not necessarily exist an abelian variety A/k with A_Ω isogenous to B. Indeed, if A is defined over k and $\lambda\colon B \to A_\Omega$ is an isogeny, for each σ in G one can define an isogeny $\phi_\sigma = \lambda^{-1} \circ {}^\sigma\lambda\colon {}^\sigma B \to B$, and these isogenies satisfy the relation $\phi_\sigma \circ {}^\sigma\phi_\tau = \phi_{\sigma\tau}$. Therefore, the existence of these ϕ_σ's is a necessary condition for the existence of a variety defined over k and isogenous to B. The following theorem of Ribet, which is [**Ri92**, Theorem 8.2], states that it is also a sufficient condition.

Theorem 2.4 (Ribet)**.** *Let Ω/k be a Galois extension and let B/Ω be an abelian variety. Suppose that there exist isogenies $\{\phi_\sigma\colon {}^\sigma B \to B\}_{\sigma\in G}$ satisfying the compatibility condition*

$$\phi_\sigma \circ {}^\sigma\phi_\tau = \phi_{\sigma\tau}. \tag{2.1}$$

Then there exists an abelian variety A/k and an isogeny $\lambda\colon B \to A_\Omega$ such that $\phi_\sigma = \lambda^{-1} \circ {}^\sigma\lambda$.

Remark 2.5. As we remarked after Proposition 1.3, this theorem is the analogous in the category of abelian varieties up to isogeny of the famous Galois descent results of Weil in other categories of algebro-geometric objects. More precisely, Weil studied the fields of definition of quasiprojective varieties up to (regular) isomorphism and also up to birrational equivalence. See [**We56**] for more details.

Remark 2.6. Let A/k be an abelian variety. A twist of A in the category of abelian varieties up to isogeny is an abelian variety A'/k that is $\overline{k}$-isogenous to A. Ribet's theorem implies that twists of A are classified by $H^1(G_k, \mathrm{Aut}_{\overline{k}}^0(A))$, meaning that there is a natural one-to-one correspondence

$$\frac{\{\text{Twists of } A\}}{k\text{-isogeny}} \overset{1:1}{\longleftrightarrow} H^1(G, \mathrm{Aut}_{\overline{k}}^0(A)).$$

Definition 2.7. We will say that a field K is a *field of definition of B up to isogeny*, or that B *can be defined over K up to isogeny*, if there exists an abelian variety A/K such that A_Ω and B are isogenous over Ω.

The previous theorem completely characterizes the fields of definition up to isogeny of an abelian variety B with field of moduli k up to isogeny: they are the fields K such that for each σ in $\mathrm{Gal}(\Omega/K)$ there exists an isogeny $\phi_\sigma\colon {}^\sigma B \to B$, and these ϕ_σ's satisfy (2.1). However, in practice it is usually difficult to prove the existence or non-existence of such ϕ_σ's. The goal of this section is to restate Theorem 2.4 but with the condition on the existence of compatible isomorphisms up to isogeny replaced by an equivalent condition more suitable for computations in practice. This new condition will involve the splitting of an exact sequence of groups.

For $\sigma \in G$ denote by $\mathrm{Isog}^0({}^\sigma B, B)$ the isogenies between ${}^\sigma B$ and B. Let E be the disjoint union of the sets $\mathrm{Isog}^0({}^\sigma B, B)$ for σ in G, that is

$$E = \bigsqcup_{\sigma \in G} \mathrm{Isog}^0({}^\sigma B, B).$$

The elements in E are of the form ϕ_σ, with ϕ_σ an element in $\mathrm{Isog}^0({}^\sigma B, B)$. Observe that, since E is defined as a disjoint union, ϕ_σ belongs to a unique subset of E of the form $\mathrm{Isog}^0({}^\sigma B, B)$, even if ϕ_σ can be interpreted in a natural way as an element of $\mathrm{Isog}^0({}^\tau B, B)$ for some τ different from σ (for instance because ${}^\tau B = {}^\sigma B$).

We can make E into a group by defining the product $\cdot$ of an element ϕ_σ in $\mathrm{Isog}^0({}^\sigma B, B)$ and an element ϕ_τ in $\mathrm{Isog}^0({}^\tau B, B)$ as $\phi_\sigma \cdot \phi_\tau = \phi_\sigma \circ {}^\sigma \phi_\tau$. It is immediately checked that $\phi_\sigma \cdot \phi_\tau$ belongs to $\mathrm{Isog}^0({}^{\sigma\tau} B, B)$, and that $(E, \cdot)$ is a group, where the neutral is the identity morphism $\mathrm{Id} \in \mathrm{Isog}^0(B, B)$ and the inverse of ϕ_σ is ${}^{\sigma^{-1}}\phi_\sigma^{-1} \in \mathrm{Isog}^0({}^{\sigma^{-1}} B, B)$.

Since $\mathrm{Isog}^0(B, B)$ is the same as $\mathcal{B}^\times = \mathrm{End}^0(B)^\times$, there is an injective group homomorphism $\iota \colon \mathcal{B}^\times \to E$. We can also define a group homomorphism $\pi \colon E \to G$ by sending each element $\phi_\sigma \in \mathrm{Isog}^0({}^\sigma B, B)$ to σ. If B has field of moduli k, then π is exhaustive. Therefore, in this case we have an exact sequence of groups

$$1 \longrightarrow \mathcal{B}^\times \xrightarrow{\iota} E \xrightarrow{\pi} G \longrightarrow 1. \tag{2.2}$$

We will consider this as an exact sequence of topological groups, with the discrete topology on E. Recall that an exact sequence of groups is said to be *split* if there exists a (set-theoretic) section s for π that is also a group homomorphism. When working with topological groups, it is natural to require such sections to be continuous homomorphisms. Our reformulation of Theorem 2.4 is the following statement.

Proposition 2.8. *Let B/Ω be an abelian variety with field of moduli k. The variety B can be defined over k up to isogeny if and only if the exact sequence* (2.2) *splits with a continuous section.*

Proof. A set-theoretic section for π is a map $\sigma \mapsto \phi_\sigma \colon G \to E$ such that ϕ_σ belongs to $\mathrm{Isog}^0({}^\sigma B, B)$. By the definition of the group law in E, it is a homomorphism if and only if $\phi_\sigma \circ {}^\sigma \phi_\tau = \phi_{\sigma\tau}$ for all σ, τ in G, which is precisely (2.1).

Now if there exists such a variety A/k with an isogeny $\lambda \colon B \to A_\Omega$, then $\{\phi_\sigma = \lambda^{-1} \circ {}^\sigma \lambda\}_{\sigma \in G}$ is a section of π that is a homomorphism; and it is continuous since λ is defined over a finite extension of k. Conversely, if (2.2) splits with a continuous section, then Theorem 2.4 implies the existence of A/k and $\lambda \colon B \to A_\Omega$. □

In this way, the problem of determining whether an abelian variety B/Ω with field of moduli k up to isogeny can be defined over a field K up to isogeny translates into the problem of determining whether an exact sequence of topological groups (with non-abelian kernel in general) is split.

2.3. Group extensions with non-abelian kernel

The problem of determining whether an exact sequence of groups is split is well known and it has been vastly studied in the case of abelian kernel. However, we are interested in the sequence (2.2) even if $\mathcal{B}$ is not a commutative algebra, and then the kernel is non-abelian. For this reason, in this section we consider exact sequences of groups

$$1 \longrightarrow H \xrightarrow{\iota} E \xrightarrow{\pi} G \longrightarrow 1, \tag{2.3}$$

where we do not require H to be commutative. We will identify H with its isomorphic image in E. Recall that a (set-theoretic) *section* of π is a map $s\colon G \to E$ such that $\pi \circ s = \mathrm{Id}$, and that the sequence (2.3) is said to be *split* if there exists a section s that is a group homomorphism. For each section s of π we define c_s to be the map

$$\begin{array}{rccc} c_s\colon & G \times G & \longrightarrow & H \\ & (\sigma, \tau) & \longmapsto & s(\sigma)s(\tau)s(\sigma\tau)^{-1}. \end{array}$$

Let Z be the center of H. A key role in the study of the splitting of non-abelian extensions is played by the so-called central sections.

Definition 2.9. We say that s is a *central section* if $c_s(\sigma, \tau)$ lies in Z for all $\sigma, \tau \in G$.

A central section s can be used to define an action Θ_s of G in H, by defining

$$\Theta_s(\sigma)(h) = s(\sigma)hs(\sigma)^{-1}, \quad \text{for all } \sigma \in G, h \in H.$$

It is easily checked that this is indeed a group action that depends, in general, on the central section s used. However, when restricted to Z it gives rise to an action of G on Z that is independent of the central section s.

Let $\theta\colon G \to \mathrm{Aut}(Z)$ be the action defined on Z by any central section and denote by $Z^2(G, Z; \theta)$ the group of (non-necessarily continuous) 2-cocycles of G with values in Z with respect to the action θ. One easily checks that $c_s \in Z^2(G, Z; \theta)$. In the commutative kernel case, i.e. when $H = Z$, the cohomology class $[c_s]$ does not depend on the section s, and the exact sequence (2.3) is split if and only if $[c_s]$ is trivial. However, if the kernel is non-abelian the cohomology class $[c_s]$ does depend in general on the central section s. Even in this case, the splitting of the extension is characterized in terms of the cohomology classes attached to central sections.

Proposition 2.10. *The exact sequence* (2.3) *is split if and only if there exists a central section s such that its cohomology class $[c_s] \in H^2(G, Z; \theta)$ is trivial.*

Proof. If the sequence splits there exists a section s that is also a group homomorphism, and therefore $c_s(\sigma, \tau) = s(\sigma)s(\tau)s(\sigma\tau)^{-1} = 1$. That is, s is a central section and $[c_s] = 1$.

Suppose now that s is a central section with $[c_s] = 1$. This means that there exists a map $\sigma \mapsto \eta_\sigma$ from G with values in Z such that

$$\begin{aligned} c_s(\sigma,\tau) &= s(\sigma)s(\tau)s(\sigma\tau)^{-1} = \eta_\sigma\theta(\sigma)(\eta_\tau)\eta_{\sigma\tau}^{-1} \\ &= \eta_\sigma s(\sigma)\eta_\tau s(\sigma)^{-1}\eta_{\sigma\tau}^{-1} = \eta_{\sigma\tau}^{-1}s(\sigma)\eta_\tau s(\sigma)^{-1}\eta_\sigma. \end{aligned}$$

Then, the map $t(\sigma) = \eta_\sigma^{-1}s(\sigma)$ is also a section, and it is indeed a group homomorphism:

$$\begin{aligned} t(\sigma)t(\tau)t(\sigma\tau)^{-1} &= \eta_\sigma^{-1}s(\sigma)\eta_\tau^{-1}s(\tau)s(\sigma\tau)^{-1}\eta_{\sigma\tau} \\ &= \eta_\sigma^{-1}s(\sigma)\eta_\tau^{-1}s(\sigma)^{-1}s(\sigma)s(\tau)s(\sigma\tau)^{-1}\eta_{\sigma\tau} \\ &= \eta_\sigma^{-1}s(\sigma)\eta_\tau^{-1}s(\sigma)^{-1}\eta_{\sigma\tau}s(\sigma)s(\tau)s(\sigma\tau)^{-1} \\ &= \eta_\sigma^{-1}s(\sigma)\eta_\tau^{-1}s(\sigma)^{-1}\eta_{\sigma\tau}c(\sigma,\tau) = 1. \end{aligned}$$

□

Hence, deciding whether an exact sequence is split is equivalent to deciding whether the set of all cohomology classes associated to central sections contains the trivial class. Now we show how to compute the set of all cohomology classes associated to central extensions from the knowledge of one particular class $[c_s]$ in this set.

Let s be a central section; we denote by Θ_s the action it defines on H and by θ the action it defines on Z. The following exact sequence of G-groups

$$1 \longrightarrow Z \longrightarrow H \longrightarrow H/Z \longrightarrow 1 \tag{2.4}$$

gives rise to the cohomology exact sequence of pointed sets (cf. Section 1.1)

$$\cdots \longrightarrow H^1(G,Z;\theta) \longrightarrow H^1(G,H;\Theta_s) \longrightarrow H^1(G,H/Z;\Theta_s) \xrightarrow{\delta} H^2(G,Z;\theta).$$

The explicit description of the connecting map δ is given in terms of cocycles by

$$\begin{array}{rccc} \delta\colon & H^1(G,H/Z;\Theta_s) & \longrightarrow & H^2(G,Z;\theta) \\ & [\sigma \mapsto \psi_\sigma Z] & \longmapsto & [(\sigma,\tau) \mapsto \psi_\sigma\Theta_s(\sigma)(\psi_\tau)\psi_{\sigma\tau}^{-1}]. \end{array} \tag{2.5}$$

Proposition 2.11. *The set of all cohomology classes associated to central sections is* $[c_s]\,\mathrm{im}(\delta) \subseteq H^2(G,Z;\theta)$.

Proof. Let $\psi\colon \sigma \mapsto \psi_\sigma Z$ be an element in $Z^1(G,H/Z;\Theta_s)$. Then

$$\begin{aligned} c_s(\sigma,\tau)\delta(\psi)(\sigma,\tau) &= c_s(\sigma,\tau)\psi_\sigma s(\sigma)\psi_\tau s(\sigma)^{-1}\psi_{\sigma\tau}^{-1} \\ &= c_s(\sigma,\tau)\psi_\sigma s(\sigma)\psi_\tau s(\tau)s(\sigma\tau)^{-1}s(\sigma\tau)s(\tau)^{-1}s(\sigma)^{-1}\psi_{\sigma\tau}^{-1} \\ &= c_s(\sigma,\tau)\psi_\sigma s(\sigma)\psi_\tau s(\tau)s(\sigma\tau)^{-1}c_s(\sigma,\tau)^{-1}\psi_{\sigma\tau}^{-1} \\ &= \psi_\sigma s(\sigma)\psi_\tau s(\tau)s(\sigma\tau)^{-1}\psi_{\sigma\tau}^{-1}, \end{aligned}$$

which is the 2-cocycle associated to the central section $\sigma \mapsto \psi_\sigma s(\sigma)$.

Let t be an arbitrary central section. For each $\sigma \in G$ we define $\psi_\sigma = t(\sigma)s(\sigma)^{-1}$. The map $\psi\colon \sigma \mapsto \psi_\sigma Z$ satisfies that

$$\begin{aligned}\delta(\psi)(\sigma,\tau) &= \psi_\sigma s(\sigma)\psi_\tau s(\sigma)^{-1}\psi_{\sigma\tau}^{-1}\\ &= t(\sigma)s(\sigma)^{-1}s(\sigma)t(\tau)s(\tau)^{-1}s(\sigma)^{-1}s(\sigma\tau)t(\sigma\tau)^{-1}\\ &= t(\sigma)t(\tau)t(\sigma\tau)^{-1}t(\sigma\tau)s(\tau)^{-1}s(\sigma)^{-1}s(\sigma\tau)t(\sigma\tau)^{-1}\\ &= c_t(\sigma,\tau)t(\sigma\tau)s(\sigma\tau)^{-1}s(\sigma\tau)s(\tau)^{-1}s(\sigma)^{-1}s(\sigma\tau)t(\sigma\tau)^{-1}\\ &= c_t(\sigma,\tau)c_s(\sigma,\tau)^{-1},\end{aligned}$$

and we see that $[c_t] \in [c_s]\operatorname{im}(\delta)$. □

As a consequence of Proposition 2.10 and Proposition 2.11 we have the following characterization of the splitting of exact sequences.

Corollary 2.12. *The exact sequence* (2.3) *is split if and only if the following conditions hold:*

1. *There exists a central section s.*
2. *The set $[c_s]\operatorname{im}(\delta) \subseteq H^2(G, Z; \theta)$ contains the trivial cohomology class.*

Remark 2.13. In this section we have stated all the results for arbitrary group extensions, and this has led us to use cohomology groups constructed with non-necessarily continuous cocycles. If one uses continuous cohomology groups instead, then one obtains a characterization of exact sequences of topological groups splitting with continuous sections. This was our original aim in view of Proposition 2.8, and from now on all cohomology groups we consider are continuous cohomology groups.

2.4. Field of definition up to isogeny

Now we particularize the results of the previous section to the exact sequence (2.2). Let Ω/k be a Galois extension with Galois group G. Let B/Ω be an abelian variety with field of moduli k, $\mathcal{B} = \operatorname{End}^0(B)$, $F = Z(\mathcal{B})$ and let $\{\phi_\sigma\colon {}^\sigma B \to B\}_{\sigma\in G}$ be a system of isogenies. The exact sequence (2.4) particularized to our current setting is

$$1 \longrightarrow F^\times \longrightarrow \mathcal{B}^\times \longrightarrow \mathcal{B}^\times/F^\times \longrightarrow 1. \tag{2.6}$$

The system of isogenies $\{\phi_\sigma\}_{\sigma\in G}$ is a set-theoretic section for π, and as we have seen it defines an action θ of G on $F^\times$: for $\sigma \in G$ and $\varphi \in F^\times$ then $\theta(\sigma)(\varphi) = \phi_\sigma \circ {}^\sigma\varphi \circ \phi_\sigma^{-1}$. The action θ on $F^\times$ does not depend on the system of isogenies chosen, and in fact it coincides with the action $\star$ that we defined in Section 2.1. The only difference is that in Section 2.1 the action was on F (as a $\mathbb{Q}$-algebra), and now is on $F^\times$ (as a group); however, the action on $F^\times$ determines a unique action on F because F has a $\mathbb{Q}$-basis consisting of invertible elements. We denote by c_ϕ the map $(\sigma,\tau) \mapsto \phi_\sigma \circ {}^\sigma\phi_\tau \circ \phi_{\sigma\tau}^{-1}\colon G \times G \to \mathcal{B}^\times$.

Definition 2.14. The system of isogenies $\{\phi_\sigma\}_{\sigma\in G}$ is *central* if $c_\phi(\sigma,\tau)$ takes values in $F^\times$.

As we have seen in Section 2.3, when $\{\phi_\sigma\}_{\sigma\in G}$ is central then c_ϕ is a continuous 2-cocycle of G with values in $F^\times$ (equipped with the G-action θ), and its cohomology class $[c_\phi]$ belongs to the group $H^2(G,F^\times;\theta)$. Moreover, we can extend the action θ to an action Θ_ϕ of G on $\mathcal{B}^\times$ in the obvious manner: $\Theta_\phi(\sigma)(\varphi)=\phi_\sigma\circ{}^\sigma\varphi\circ\phi_\sigma^{-1}$. Actually by the results in Section 2.3 we know that this is an action on $\mathcal{B}^\times$, but again since $\mathcal{B}$ has a basis formed by invertible elements it is in fact a well defined action on the whole $\mathcal{B}$.

We denote by $\Delta(B)$ the set of cohomology classes $[c_\phi]$ in $H^2(G,F^\times;\theta)$ associated to central systems of isogenies. Note that $\Delta(B)$ only depends on the Ω-isogeny class of B. Indeed, if $\{\phi_\sigma\}_{\sigma\in G}$ is a central system of isogenies and $\lambda\colon B\to B'$ is an isogeny, then $\{\psi_\sigma=\lambda\circ\phi_\sigma\circ{}^\sigma\lambda^{-1}\}_{\sigma\in G}$ is a central system of isogenies for B' and $c_\psi(\sigma,\tau)=\lambda\circ c_\phi(\sigma,\tau)\circ\lambda^{-1}$, so the cocycles c_ψ and c_ϕ coincide under the identification of $Z(\mathrm{End}^0(B'))$ and $Z(\mathrm{End}^0(B))$ given by λ.

The connecting map δ corresponding to (2.6) is given by:

$$\begin{array}{rccl}\delta\colon & H^1(G,\mathcal{B}^\times/F^\times;\Theta_\phi) & \longrightarrow & H^2(G,F^\times;\theta)\\ & \{\sigma\mapsto\psi_\sigma F^\times\} & \longmapsto & \{(\sigma,\tau)\mapsto\psi_\sigma\circ(\phi_\sigma\circ{}^\sigma\psi_\tau\circ\phi_\sigma^{-1})\circ\psi_{\sigma\tau}^{-1}\}.\end{array}$$

Proposition 2.15. *Let $[c_\phi]$ be the cohomology class attached to a central system of isogenies. Then $\Delta(B)=[c_\phi]\,\mathrm{im}(\delta)$.*

Proof. This is Proposition 2.11. □

Theorem 2.16. *Let B/Ω be an abelian variety with field of moduli k up to isogeny. The variety B can be defined over k up to isogeny if and only if the following conditions hold:*

1. *There exists a central system of isogenies $\{\phi_\sigma\}_{\sigma\in G}$ for B.*
2. *The set $\Delta(B)=[c_\phi]\,\mathrm{im}(\delta)$ contains the trivial class.*

Proof. This is Corollary 2.12. □

Finally, we can use the above result to give a method for determining whether a certain field K is a field of definition of B up to isogeny.

Theorem 2.17. *Let B/Ω be an abelian variety with field of moduli k, and let $[c_\phi]$ be the cohomology class attached to a central system of isogenies for B. There exists a variety A/K such that B and A_Ω are Ω-isogenous if and only if there exists an element $\psi\in H^1(\mathrm{Gal}(\Omega/K),\mathcal{B}^\times/F^\times;\Theta_\phi)$ such that*

$$\delta(\psi)\,\mathrm{Res}_k^K[c_\phi]=1, \tag{2.7}$$

where Res_k^K is the usual restriction map

$$\mathrm{Res}_k^K\colon H^2(G,F^\times;\theta)\to H^2(\mathrm{Gal}(\Omega/K),F^\times;\theta).$$

Proof. This is an application of Theorem 2.16, since B has field of moduli K with respect to Ω/K and $\mathrm{Res}_k^K[c_\phi]$ is the cohomology class attached to the central system $\{\phi_\sigma\}_{\sigma\in\mathrm{Gal}(\Omega/K)}$. □

In Chapter 4 we will use the above theorem to explicitly compute fields of definition of abelian k-varieties of the first kind.

2.5. Weil descent

We devote this last section to a digression on the possibility of adapting the scheme we followed so far in this chapter to a more general setting, allowing the use of our techniques to a pool of different but somehow related situations. As we have already noted in Remark 2.5, Ribet's theorem is one instance of a more general framework of results relating fields of moduli and fields of definition in other categories of interest in arithmetic geometry, being the theorems of Weil on the field of definition of quasiprojective varieties the most prominent examples. The categories where the analogous of Weil's theorems hold will be said to admit *Weil descent*.

To be more precise, let $\mathcal{C}$ be a category on which the Galois group G of a certain extension Ω/k operates. By this we mean that G acts on the objects and on the morphisms of $\mathcal{C}$. Thus, if σ is an element of G then for each object C there is an object ${}^{\sigma}C$, and for each morphism $\phi\colon C_1 \to C_2$ there is a morphism ${}^{\sigma}\phi\colon {}^{\sigma}C_1 \to {}^{\sigma}C_2$. Moreover, we assume that all properties that are natural to expect for such an action are satisfied. For instance

$$ {}^{\mathrm{Id}}C = C,\ {}^{\tau}({}^{\sigma}C) = {}^{\tau\sigma}C,\ {}^{\mathrm{Id}}\phi = \phi\ \ {}^{\tau}({}^{\sigma}\phi) = {}^{\tau\sigma}\phi,\ \ {}^{\sigma}(\phi\circ\psi) = {}^{\sigma}\phi\circ{}^{\sigma}\psi. $$

We say that an object C *is defined over a field* K if ${}^{\sigma}C = C$ for all $\sigma \in \mathrm{Gal}(\Omega/K)$; similarly, a morphism ϕ is defined over K if ${}^{\sigma}\phi = \phi$ for all $\sigma \in \mathrm{Gal}(\Omega/K)$. Note that all objects and morphisms of $\mathcal{C}$ are defined over Ω. From now on, we assume that for each object or morphism of $\mathcal{C}$, there exists a finite extension K of k where it is defined. In this way, the action of G on $\mathcal{C}$ is discrete. There are many examples of this kind of categories; for instance, the category of algebraic varieties defined over Ω with regular morphisms would be a prototypical one.

As in Definition 2.1, the *field of moduli relative to* Ω/k of an object C is defined to be the fixed field of Ω by the elements $\sigma \in G$ such that ${}^{\sigma}C \simeq C$. If C is isomorphic to an object B defined over K, then K contains the field of moduli of C. Indeed, if $\lambda\colon C \to B$ is an isomorphism then $\phi_\sigma = \lambda^{-1}\circ{}^{\sigma}\lambda$ for $\sigma \in \mathrm{Gal}(\Omega/K)$ is an isomorphism $\phi_\sigma\colon {}^{\sigma}C \to C$. Obviously these isomorphisms satisfy the condition $\phi_\sigma\circ{}^{\sigma}\phi_\tau = \phi_{\sigma\tau}$, and the set $\{\phi_\sigma\colon {}^{\sigma}C \to C\}_{\sigma\in\mathrm{Gal}(\Omega/K)}$ is locally constant.

Definition 2.18. We say that $\mathcal{C}$ satisfies *Weil's descent criterion* if each object C of $\mathcal{C}$ satisfies the following property: for every locally constant set of isomorphisms $\{\phi_\sigma\colon {}^{\sigma}C \to C\}_{\sigma\in\mathrm{Gal}(\Omega/k)}$ such that $\phi_\sigma\circ{}^{\sigma}\phi_\tau = \phi_{\sigma\tau}$, there exists an object B defined over k and an isomorphism $\lambda\colon C \to B$ such that $\phi_\sigma = \lambda^{-1}\circ{}^{\sigma}\lambda$.

Among the categories satisfying Weil's descent criterion we can find, for example:

- Quasiaffine and quasiprojective varieties with regular morphisms; quasiaffine and quasiprojective varieties with rational morphisms. This is in [**We56**].
- Abelian varieties up to isogeny (as we said this is [**Ri92**, Theorem 8.2]).
- Coverings of curves (cf. [**DD97**]).

Now, following the same line of reasoning as in Section 2.2, we can interpret Weil's descent condition of Definition 2.18 in terms of the splitting of an exact sequence of groups. More precisely, the set

$$\bigsqcup_{\sigma\in G} \mathrm{Isom}({}^{\sigma}C, C)$$

can be given a group structure by defining $\phi_\sigma \cdot \phi_\tau = \phi_\sigma \circ {}^{\sigma}\phi_\tau$ for $\phi_\sigma \in \mathrm{Isom}({}^{\sigma}C, C)$ and $\phi_\tau \in \mathrm{Isom}({}^{\tau}C, C)$. In this way we have a group monomorphism

$$\iota\colon \mathrm{Aut}(C) \to \bigsqcup_{\sigma\in G} \mathrm{Isom}({}^{\sigma}C, C),$$

consisting on viewing each $\phi \in \mathrm{Aut}(C)$ as an element of $\mathrm{Isom}({}^{\mathrm{Id}}C, C)$. There is also a group homomorphism

$$\pi\colon \bigsqcup_{\sigma\in G} \mathrm{Isom}({}^{\sigma}C, C) \to G$$

sending an element $\phi_\sigma \in \mathrm{Isom}({}^{\sigma}C, C)$ to σ. An object C has field of moduli k if and only if π is an epimorphism. In that case we have the following exact sequence

$$1 \longrightarrow \mathrm{Aut}(C) \xrightarrow{\iota} \bigsqcup_{\sigma\in G} \mathrm{Isom}({}^{\sigma}C, C) \xrightarrow{\pi} G \longrightarrow 1.$$

Exactly the same argument we used in proving Proposition 2.8 leads us to the following statement.

Proposition 2.19. *Let $\mathcal{C}$ be a category with a discrete action of $G = \mathrm{Gal}(\Omega/k)$. Then $\mathcal{C}$ satisfies Weil's descent criterion if for each object C in $\mathcal{C}$ the following conditions are equivalent:*

(1) *There exists an object B defined over k that is isomorphic to C.*
(2) *The object C has field of moduli k with respect to Ω/k and the exact sequence*

$$1 \longrightarrow \mathrm{Aut}(C) \xrightarrow{\iota} \bigsqcup_{\sigma\in \mathrm{Gal}(\Omega/k)} \mathrm{Isom}({}^{\sigma}C, C) \xrightarrow{\pi} \mathrm{Gal}(\Omega/k) \longrightarrow 1,$$

splits with continuous sections.

Therefore, by Corollary 2.12 we see that in categories with Weil descent there are two obstructions to an object with field of moduli k to being isomorphic to an object defined over k. The first one is the existence of some central section s for π; that is, such that $c_s(\sigma, \tau) = s(\sigma) \cdot s(\tau) \cdot s(\sigma\tau)^{-1}$

lies in $Z = Z(\mathrm{Aut}(C))$ for all $\sigma, \tau \in G$. The second one is the existence of an element $\psi \in H^1(G, \mathrm{Aut}(C)/Z; \Theta_s)$ such that $[c_s] \cdot \delta(\psi) = 1$. When $\mathrm{Aut}(C)$ is abelian the condition reduces to the more familiar case where the obstruction is a unique element of a cohomology group.

CHAPTER 3

Abelian k-varieties

In Chapter 2 we have seen that for an abelian variety with field of moduli k there is a natural action of the Galois group $G_k = \mathrm{Gal}(k_s/k)$ on the center of its endomorphism algebra. This chapter is devoted to the study of the particular case of abelian varieties with field of moduli k where this action is trivial: we call them abelian k-varieties. Actually, one of the main themes of this thesis is to characterize the field of definition up to isogeny of abelian k-varieties of the first kind.

In Section 3.1 we give the definition and some basic properties of abelian k-varieties; in particular we describe their behavior under the decomposition up to isogeny into absolutely simple varieties, and we canonically attach to them a cohomology class that will constitute one of the basic tools for their study. In Section 3.2 we start investigating their field of definition up to isogeny, and we give the general results that will be used in Chapter 4 to give a concrete characterization of these fields for varieties of the first kind. Precisely, as a preparation for Chapter 4, in Section 3.3 we present the background material that is necessary for giving a detailed description of the field of definition up to isogeny of abelian k-varieties of the first kind.

3.1. Definition and basic properties

Let k be a field, k_s a separable closure of k and $G_k = \mathrm{Gal}(k_s/k)$. From now on we will use the terminology of the previous chapter particularized to the case where $\Omega = k_s$. So we say that an abelian variety B/k_s has field of moduli k (relative to the extension k_s/k) if for each $\sigma \in G_k$ the varieties ${}^\sigma B$ and B are isogenous. As usual, we denote by $\mathcal{B}$ the endomorphism algebra of B and by F its center. Recall that a system of isogenies $\{\phi_\sigma \colon {}^\sigma B \to B\}_{\sigma \in G_k}$ defines an action θ of G_k on $F^\times$: if $\varphi \in F^\times$ then $\theta(\sigma)(\varphi) = \phi_\sigma \circ {}^\sigma\varphi \circ \phi_\sigma^{-1}$. The abelian k-varieties are characterized as those for which this action is the simplest one.

Definition 3.1. An *abelian k-variety* is an abelian variety B/k_s with field of moduli k such that the action θ of G_k on $F^\times$ is trivial.

Note that if the action of G_k on $F^\times$ is trivial, the action on F (as $\mathbb{Q}$-vector space) is trivial as well, because F has a basis formed by invertible elements. The property of being an abelian k-variety is preserved by the decomposition into simple abelian varieties up to isogeny.

Proposition 3.2. *B/k_s is an abelian k-variety if and only if all of its simple factors up to isogeny are.*

PROOF. Suppose first that B is isotypical and $B \sim C^n$. Since we can identify the field $Z(\mathrm{End}^0(C))$ with $Z(\mathrm{End}^0(B))$, the action of G_k is trivial on one of these fields if and only if it is trivial on the other one.

In the general case, let $B \sim B_1 \times \cdots \times B_r$ be the decomposition of B into isotypical varieties, and let $F \simeq F_1 \times \cdots \times F_r$ be the corresponding decomposition of F into a product of number fields. If each B_i is an abelian k-variety, then the action of G_k of $F^\times$ is trivial since it is trivial on each $F_i^\times$. If B is an abelian k-variety, then by Proposition 2.3 each B_i has field of moduli k, and the action of G_k on $F_i^\times$ is trivial since it is the restriction of the action of G_k on $F^\times$, which is trivial by hypothesis. □

Definition 3.3. We say that an isogeny $\mu_\sigma \colon {}^\sigma B \to B$ is *compatible with the endomorphisms of B*, or for simplicity just *compatible*, if $\varphi \circ \mu_\sigma = \mu_\sigma \circ {}^\sigma\varphi$ for all $\varphi \in \mathrm{End}^0(B)$. That is, if for all $\varphi \in \mathrm{End}^0(B)$ the following diagram commutes:

$$\begin{array}{ccc} {}^\sigma B & \xrightarrow{\mu_\sigma} & B \\ {\scriptstyle {}^\sigma\varphi}\downarrow & & \downarrow{\scriptstyle \varphi} \\ {}^\sigma B & \xrightarrow{\mu_\sigma} & B. \end{array}$$

Remark 3.4. If μ_σ is compatible and λ belongs to the center of $\mathrm{End}^0(B)$ then $\lambda \circ \mu_\sigma$ is also a compatible isogeny. Conversely, if μ_σ is compatible then every compatible isogeny ϕ_σ is of the form $\phi_\sigma = \lambda \circ \mu_\sigma$ for some λ in the center of $\mathrm{End}^0(B)$.

Proposition 3.5. *An abelian variety B/k_s is an abelian k-variety if and only if for all σ in G_k there exists a compatible isogeny $\mu_\sigma \colon {}^\sigma B \to B$.*

PROOF. If there exists a set of compatible isogenies $\{\mu_\sigma \colon {}^\sigma B \to B\}_{\sigma \in G_k}$ then for all $\varphi \in F$ we have that $\mu_\sigma \circ {}^\sigma\varphi \circ \mu_\sigma^{-1} = \varphi$, and then the action θ of G_k on F is trivial and B is an abelian k-variety.

Suppose now that B is an isotypical abelian k-variety. Then $\mathcal{B}$ is a simple F-algebra, and for each σ in G_k there exists an isogeny $\phi_\sigma \colon {}^\sigma B \to B$ such that $\phi_\sigma \circ {}^\sigma\varphi \circ \phi_\sigma^{-1} = \varphi$ for all $\varphi \in F$. This means that the map $\varphi \mapsto \phi_\sigma \circ {}^\sigma\varphi \circ \phi_\sigma^{-1} \colon \mathcal{B} \to \mathcal{B}$ is an automorphism of F-algebras. By the Skolem-Noether Theorem it is an inner automorphism: there exists an element α_σ belonging to $\mathcal{B}$ such that $\phi_\sigma \circ {}^\sigma\varphi \circ \phi_\sigma^{-1} = \alpha_\sigma \circ \varphi \circ \alpha_\sigma^{-1}$ for all φ in $\mathcal{B}$. Then $\mu_\sigma = \alpha_\sigma^{-1} \circ \phi_\sigma$ satisfies that $\mu_\sigma \circ {}^\sigma\varphi \circ \mu_\sigma^{-1} = \varphi$ for every $\varphi \in \mathcal{B}$, and therefore it is a compatible isogeny. In the general case, we have that $B \sim B_1 \times \cdots \times B_r$, where each B_i is isotypical. If B is an abelian k-variety, then by 3.2 each B_i is a k-variety, and by the previous case for each σ in G_k there exists a compatible isogeny for B_i. By taking the product of these isogenies we obtain a compatible isogeny for B. □

Remark 3.6. We could equivalently give the condition on the existence of a system of compatible isogenies by saying that the pair $(B, \mathrm{End}^0(B))$ has field of moduli k.

Remark 3.7. We could have taken the existence of a compatible system of isogenies as the definition of abelian k-variety, and this would have been a natural generalization of the definition of abelian $\mathbb{Q}$-variety given by Ribet and Pyle (cf. Definition 1.26). Instead, we have chosen a different (but equivalent) approach, in order to emphasize the paper that plays the natural action of G_k on F in a variety with field of moduli k; from this point of view, it seems natural to study those varieties where this action is the simplest possible. However, the useful property when working with k-varieties, and the one we will more often use, is the existence of compatible isogenies.

Every system of compatible isogenies $\{\mu_\sigma \colon {}^\sigma B \to B\}_{\sigma \in G_k}$ is central. Indeed, for φ in $\mathcal{B}$ we have that

$$\mu_\sigma \circ {}^\sigma\mu_\tau \circ \mu_{\sigma\tau}^{-1} \circ \varphi = \mu_\sigma \circ {}^\sigma\mu_\tau \circ {}^{\sigma\tau}\varphi \circ \mu_{\sigma\tau}^{-1} = \mu_\sigma \circ {}^\sigma\varphi \circ {}^\sigma\mu_\tau \circ \mu_{\sigma\tau}^{-1} = \varphi \circ \mu_\sigma \circ {}^\sigma\mu_\tau \circ \mu_{\sigma\tau}^{-1},$$

and therefore $c_\mu(\sigma,\tau) = \mu_\sigma \circ {}^\sigma\varphi \circ \mu_\sigma^{-1}$ belongs to $F^\times$. Recall that c_μ belongs to $Z^2(G_k, F^\times)$, where now the action of G_k on $F^\times$ is the trivial one. In the rest of the thesis all cohomology groups appearing will be with the trivial action, unless otherwise stated; hence we drop the mention of the action in the notation for the cohomology groups.

Lemma 3.8. *The cohomology class $[c_\mu] \in H^2(G_k, F^\times)$ does not depend on the system of compatible isogenies $\{\mu_\sigma\}$, and it is an invariant of the isogeny class of B.*

Proof. Let $\{\phi_\sigma\}$ be another system of compatible isogenies. Then $\phi_\sigma = \lambda_\sigma \circ \mu_\sigma$ for some λ_σ belonging to $F^\times$ (see Remark 3.4), and we have that

$$\begin{aligned} c_\phi(\sigma,\tau) &= (\lambda_\sigma \circ \mu_\sigma) \circ {}^\sigma(\lambda_\tau \circ \mu_\tau) \circ (\lambda_{\sigma\tau} \circ \mu_{\sigma\tau}^{-1}) = \lambda_\sigma \circ \mu_\sigma \circ {}^\sigma\lambda_\tau \circ {}^\sigma\mu_\tau \circ \mu_{\sigma\tau}^{-1} \circ \lambda_{\sigma\tau}^{-1} \\ &= \lambda_\sigma \circ \lambda_\tau \circ \mu_\sigma \circ {}^\sigma\mu_\tau \circ \mu_{\sigma\tau}^{-1} \circ \lambda_{\sigma\tau}^{-1} = \lambda_\sigma \circ \lambda_\tau \circ c_\mu(\sigma,\tau) \circ \lambda_{\sigma\tau}^{-1} \\ &= c_\mu(\sigma,\tau) \circ \lambda_\sigma \circ \lambda_\tau \circ \lambda_{\sigma\tau}^{-1}, \end{aligned}$$

which shows that c_ϕ and c_μ are cohomologous.

Now let $\kappa \colon B' \to B$ be an isogeny. Then it is easy to check that $\{\nu_\sigma = \kappa^{-1} \circ \mu_\sigma \circ {}^\sigma\kappa\}_{\sigma \in G_k}$ is a system of compatible isogenies for B' and

$$c_\nu(\sigma,\tau) = \kappa^{-1} \circ c_\mu(\sigma,\tau) \circ \kappa.$$

Hence, under the identification of $Z(\mathrm{End}^0(B'))$ with $Z(\mathrm{End}^0(B))$ given by κ, the two cocycles coincide. □

As we have seen the cohomology class attached to a compatible system of isogenies only depends on the variety B, and we will reflect this fact in our notation.

Definition 3.9. We will denote by $[c_B]$ the cohomology class $[c_\mu]$ associated to any system of compatible isogenies.

In the next section we will work with cohomology classes $[c_\phi]$ attached to central systems of isogenies not necessarily compatible. In this case, $[c_\phi]$ depends in general on the particular system $\{\phi_\sigma\}_{\sigma\in G_k}$ used, and it does not need to coincide with $[c_B]$. As we will see, this will be one of the main points to be exploited when studying fields of definition up to isogeny of abelian k-varieties. For the moment, we give two more properties of $[c_B]$. The first one refers to its good behavior with respect to the decomposition of B into simple factors.

Proposition 3.10. *Let $B \sim B_1^{n_1} \times \cdots \times B_r^{n_r}$ be the decomposition of B into simple abelian varieties, and let $F \simeq F_1 \times \cdots \times F_r$ be the corresponding decomposition of the centers of the endomorphism algebras. Then $[c_B] = ([c_{B_1}], \ldots, [c_{B_r}])$, under the identification $H^2(G_k, F^\times) \simeq \prod_{i=1}^r H^2(G_k, F_i^\times)$.*

PROOF. This is a straightforward verification. □

From now on we will usually consider absolutely simple abelian k-varieties, since the general case can be reduced to this one using Proposition 3.10. We finish this section of basic properties of k-varieties with a lemma that we will use in Proposition 3.18.

Lemma 3.11. *Every 2-cocycle representing the cohomology class of $[c_B]$ can be obtained as the cocycle associated to a system of compatible isogenies.*

PROOF. Let c_μ be the cocycle associated to a system of compatible isogenies $\{\mu_\sigma\}$. If c is a cocycle cohomologous to c_μ, then

$$c(\sigma,\tau) = c_\mu(\sigma,\tau)\circ\lambda_\sigma\circ\lambda_\tau\circ\lambda_{\sigma\tau}^{-1},$$

where the λ's belong to $F^\times$. Then the cocycle associated to the system of compatible isogenies $\{\lambda_\sigma\circ\mu_\sigma\}_{\sigma\in G_k}$ is c. □

3.2. Fields of definition of abelian k-varieties

Let B/k_s be a simple abelian k-variety. Ribet proved that the cohomology class $[c_B]$ contains all the information concerning the possible fields of definition up to isogeny of an abelian k-variety together with its endomorphisms. More precisely, we have the following

Proposition 3.12 (Ribet-Pyle)**.** *Let B be an abelian k-variety and let K be a field containing k. There exists an abelian variety B_0 defined over K, k_s-isogenous to B and with all its endomorphisms defined over K if and only if $[c_B]$ lies in the kernel of the restriction map* $\mathrm{Res}_k^K : H^2(G_k, F^\times) \to H^2(G_K, F^\times)$.

PROOF. This is proved in [**Py02**, proposition 5.2] for the particular case of building blocks (i.e. abelian $\mathbb{Q}$-varieties satisfying certain conditions on the dimensions of their endomorphism algebras). But neither the fact that $k = \mathbb{Q}$ nor the extra conditions on the endomorphism algebras play any role in the proof, so exactly the same argument proves what is stated here. □

Remark 3.13. We can interpret this result as a characterization of the fields of definition up to isogeny of the pair $(B, \mathrm{End}^0(B))$; that is, of the fields of definition of the variety and of its endomorphisms.

Remark 3.14. If we say that the endomorphisms of B are defined over K, it is of course implicitly assumed that B itself is defined over K. Therefore, for simplicity we will just say in this case that K is a field of definition of the endomorphisms of B. Accordingly, if we say that K is a field of definition of B, we are not giving any information about the field of definition of the endomorphisms of B, except that it is a certain field containing K.

Proposition 3.12 does not characterize completely the fields of definition up to isogeny of B, since it may occur that for a certain field K there exists a B_0 defined over K and isogenous to B, but that there is no such B_0 with all of its endomorphisms defined over K. However, this situation is only possible if the endomorphism algebra of B is non-commutative, as we can see in the following

Proposition 3.15. *If a k-variety B is defined over a field K, then the endomorphisms in the center of its endomorphism algebra are also defined over K.*

Proof. Since B is defined over K, for each $\sigma \in G_K$ we have that ${}^\sigma B = B$, and a compatible isogeny $\mu_\sigma \colon {}^\sigma B \to B$ belongs to $\mathrm{End}^0(B)$. If λ is an element in the center of the endomorphism algebra, then ${}^\sigma\lambda = \mu_\sigma^{-1} \circ \lambda \circ \mu_\sigma = \lambda$, so λ is defined over K. □

Hence, if B has a non-commutative endomorphism algebra it is natural to ask for a characterization of its fields of definition up to isogeny. In this case the information is not all contained in $[c_B]$, but also in all the other cohomology classes $[c_\phi]$ attached to central systems of isogenies. This is the content of Theorem 2.17, which we now particularize to abelian k-varieties. Note that, since in this case the action of G_K of $F^\times$ is trivial, the cohomology pointed set $H^1(G_K, \mathcal{B}^\times/F^\times)$ coincides with $\mathrm{Hom}(G_K, \mathcal{B}^\times/F^\times)$, the set of continuous group homomorphisms from G_K to $\mathcal{B}^\times/F^\times$. Hence, the connecting map δ is given by

$$\begin{array}{rccc} \delta\colon & \mathrm{Hom}(G_K, \mathcal{B}^\times/F^\times) & \longrightarrow & H^2(G_K, F^\times) \\ & \{\sigma \mapsto \psi_\sigma F^\times\} & \longmapsto & \{(\sigma,\tau) \mapsto \psi_\sigma \circ \psi_\tau \circ \psi_{\sigma\tau}^{-1}\}. \end{array} \tag{3.1}$$

Proposition 3.16. *Let B be an abelian k-variety and let $[c_B]$ be the cohomology class associated to a compatible system of isogenies for B. There exists a variety B_0 defined over K and isogenous to B if and only if there exists a group homomorphism $\psi\colon G_K \to \mathcal{B}^\times/F^\times$ such that $\delta(\psi)\,\mathrm{Res}_k^K[c_B] = 1$.*

Proof. This is Theorem 2.17 in the setting of abelian k-varieties. □

In Chapter 4 we will expand on this result by studying, for abelian varieties of the first kind with quaternionic multiplication, to what extent the

fields of definition of the variety can be smaller than the fields of definition of the endomorphisms.

Now we turn our attention to the field of definition of the compatible isogenies between the variety and its Galois conjugates. First of all, we observe that if B is defined over K and $\mu_\sigma\colon {}^\sigma B \to B$ is a compatible isogeny defined over K, then all compatible isogenies ${}^\sigma B \to B$ are also defined over K. This is because any other compatible isogeny is of the form $\mu'_\sigma = \lambda_\sigma \circ \mu_\sigma$, with λ_σ belonging to $F^\times$. By Proposition 3.15 the map λ_σ is defined over K, and so μ'_σ is defined over K as well.

Definition 3.17. Let K/k be a Galois extension. We say that an abelian k-variety is *completely defined over* K if the variety, all of its endomorphisms and all its compatible isogenies are defined over K.

Let B be an abelian k-variety completely defined over K, and for each $s \in \mathrm{Gal}(K/k)$ let $\mu_s\colon {}^s B \to B$ be a compatible isogeny. It is easily checked that the map

$$c_{B/K}\colon \mathrm{Gal}(K/k) \times \mathrm{Gal}(K/k) \longrightarrow F^\times, \qquad c_{B/K}(s,t) = \mu_s \circ {}^s\mu_t \circ \mu_{st}^{-1}$$

is a well defined 2-cocycle of $\mathrm{Gal}(K/k)$ with values in the trivial $\mathrm{Gal}(K/k)$-module $F^\times$. Moreover, its cohomology class $[c_{B/K}] \in H^2(K/k, F^\times)$ is an invariant of the K-isogeny class of B, and the inflation of $[c_{B/K}]$ to $H^2(G_k, F^\times)$ is equal to $[c_B]$. This last property has a converse in the following proposition, which is a generalization of [**Qu00**, Theorem 2.4].

Proposition 3.18. *An abelian k-variety B is k_s-isogenous to an abelian k-variety completely defined over K if and only if the cohomology class $[c_B]$ belongs to the image of the inflation map* $\mathrm{Inf}\colon H^2(K/k, F^\times) \to H^2(G_k, F^\times)$. *Moreover, if $[c_B] = \mathrm{Inf}([c])$ for some $[c] \in H^2(K/k, F^\times)$, then there exists such a variety B_0/K with $[c_{B_0/K}] = [c]$.*

Proof. Assume that $[c_B] = \mathrm{Inf}([c])$. Since the image of the inflation lies in the kernel of the restriction, by Proposition 3.12 we can suppose that B and all of its endomorphisms are defined over K.

Modifying the 2-cocycle c by a coboundary we can assume that it is normalized, i.e. that it takes the value $c(1,1) = 1$, and as a consequence of the cocycle condition this implies that also $c(s,1) = c(1,s) = 1$ for all $s \in \mathrm{Gal}(K/k)$. Moreover, by Lemma 3.11 we can suppose that $\mathrm{Inf}(c)$ coincides with the cocycle c_B. This implies that $c_B(\sigma,\tau) = 1$ whenever σ or τ belong to the subgroup G_K. It follows that the map $\sigma \mapsto \mu_\sigma$ is a 1-cocycle of G_K with values in the group $\mathrm{Aut}^0(B)$, viewed as a module with the natural Galois action of G_K, which is in fact the trivial action since all the elements of $\mathrm{End}^0(B)$ are defined over K.

Let B_0 be the twist of B by this 1-cocycle: it is an abelian variety B_0 defined over K together with an isogeny $\kappa\colon B \to B_0$ such that $\mu_\sigma = \kappa^{-1} \circ {}^\sigma\kappa$ for all $\sigma \in G_K$ (see Remark 2.6). We will see that this variety satisfies the conditions of the proposition.

Every endomorphism of B_0 is of the form $\kappa\circ\psi\circ\kappa^{-1}$ for some $\psi\in\mathrm{End}^0(B)$. Since all endomorphisms of B are defined over K and the isogenies μ_σ are compatible, for every $\sigma\in G_K$ one has

$$^\sigma(\kappa\circ\psi\circ\kappa^{-1}) = {}^\sigma\kappa\circ{}^\sigma\psi\circ{}^\sigma\kappa^{-1} = \kappa\circ\mu_\sigma\circ{}^\sigma\psi\circ\mu_\sigma^{-1}\circ\kappa^{-1} = \kappa\circ\psi\circ\kappa^{-1}$$

and the endomorphisms of B_0 are defined over K as well.

A calculation shows that the maps $\nu_\sigma = \kappa\circ\mu_\sigma\circ{}^\sigma\kappa^{-1}$ are compatible isogenies ${}^\sigma B_0\to B_0$ for every $\sigma\in G_k$, and the relation $\mu_\sigma=\kappa^{-1}\circ{}^\sigma\kappa$ for elements $\sigma\in G_K$ shows that $\nu_\sigma=1$ for σ fixing the field K. The cocycle c_{B_0} computed from this set of isogenies is related to c_B by $c_{B_0}(\sigma,\tau) = \kappa\circ c_B(\sigma,\tau)\circ\kappa^{-1}$ for all $\sigma,\tau\in G_k$. Since c_B is the inflation of c and this cocycle is normalized, one deduces that $c_{B_0}(\sigma,\tau)=1$ if either σ or τ belong to the subgroup G_K. Applying this fact to a pair $\sigma\in G_k$ and $\tau\in G_K$ one deduces that

$$1 = c_{B_0}(\sigma,\tau) = \nu_\sigma\circ{}^\sigma\nu_\tau\circ\nu_{\sigma\tau}^{-1} = \nu_\sigma\circ\nu_{\sigma\tau}^{-1},$$

and so that $\nu_{\sigma\tau}=\nu_\sigma$. This means that ν_σ only depends on the action of σ on K (i.e. on the class of σ modulo the normal subgroup G_K). Now, applying the identity to a pair $\sigma\in G_K$ and $\tau\in G_k$ one has

$$1 = c_{B_0}(\sigma,\tau) = \nu_\sigma\circ{}^\sigma\nu_\tau\circ\nu_{\sigma\tau}^{-1} = {}^\sigma\nu_\tau\circ\nu_{\sigma\tau}^{-1} = {}^\sigma\nu_\tau\circ\nu_\tau^{-1},$$

and so ${}^\sigma\nu_\tau=\nu_\tau$ proving that the compatible isogenies ν_τ are also defined over K for every $\tau\in G_k$.

Finally, for every element $s\in\mathrm{Gal}(K/k)$ let ν_s be the isogeny ν_σ for any $\sigma\in G_k$ whose action on K is given by the element s. In this way one obtains a set of compatible isogenies for B_0 defined over the field K and the cocycle $c_{B_0/K}$ computed using this set is the cocycle $c_{B_0/K}(s,t)=\kappa\circ c(s,t)\circ\kappa^{-1}$. Hence, under the isomorphism between the centers of the endomorphisms of the varieties B_0 and B given by conjugation by the isogeny κ between them, the cohomology class $[c_{B_0/K}]$ is the class $[c]$ we started with. □

If B is a variety of the first kind, then the previous proof actually gives us slightly more information than the stated in the proposition. Indeed, we have the following result.

Proposition 3.19. *Let B be a simple abelian k-variety of the first kind, defined over K and such that $[c_B]=\mathrm{Inf}([c])$ for some $[c]\in H^2(K/k,F^\times)$. Then there exists a B_0 completely defined over K with $[c_{B_0/K}]=[c]$, and such that B_0 is isomorphic to B with an isomorphism defined over a quadratic extension of K.*

Proof. In the proof of 3.18 we constructed the variety B_0 as the χ-twist of B, where χ is a homomorphism $G_K\to F^\times$. Since B is simple of the first kind we have that F is a totally real number field, so the only roots of unity it contains are $\{\pm1\}$. Therefore χ takes values in $\{\pm1\}$, which can be identified in a canonical way with true isomorphisms of B, and χ factors through a quadratic extension L of K. This implies that B is L-isomorphic to B_0. □

3.3. Varieties of the first kind

Let B/k_s be a simple abelian k-variety of the first kind. Recall that this means that $\mathcal{B} = \mathrm{End}^0(B)$ is either a totally real number field F, or a quaternion division algebra over a totally real number field F. In this section we give a precise description of the fields of definition up to isogeny of the endomorphisms of B. This description was first given by Ribet and Pyle for the particular case of building blocks. Our aim is to show that their arguments and results are also valid in the more general case of abelian k-varieties of the first kind.

The degree map and the structure of $H^2(G_k, F^\times)[2]$. Let B_1 and B_2 be simple abelian varieties of the first kind, and fix $\lambda_1\colon B_1 \to \hat{B}_1$, $\lambda_2\colon B_2 \to \hat{B}_2$ polarizations of B_1 and B_2 respectively. An isogeny $\mu\colon B_1 \to B_2$ is said to be *Rosati compatible* if the isomorphism $\mathrm{End}^0(B_1) \simeq \mathrm{End}^0(B_2)$ induced by μ is compatible with the Rosati involutions defined by λ_1 and λ_2. Writing down this condition, it is easy to see that μ is Rosati compatible if and only if the element $\mu \circ \lambda_1^{-1} \circ \hat{\mu} \circ \lambda_2$ belongs to the center of $\mathrm{End}^0(B_2)$. In this case, we say that $d(\mu) = \mu \circ \lambda_1^{-1} \circ \hat{\mu} \circ \lambda_2 \in Z(\mathrm{End}^0(B_2))$ is the *degree* of μ. An important property of $d(\mu)$ is that it is a totally positive element of the totally real field $Z(\mathrm{End}(B_2))$. The justification for the name degree comes from the following property.

Proposition 3.20. *Let B_1 and B_2 be simple k-varieties of the first kind. Let $\lambda_1\colon B_1 \to \hat{B}_1$ and $\lambda_2\colon B_2 \to \hat{B}_2$ be polarizations with $\deg(\lambda_1) = \deg(\lambda_2)$ and let $\mu\colon B_1 \to B_2$ be a Rosati compatible isogeny. Then we have that $\deg \mu = \mathrm{N}_{\mathcal{B}/\mathbb{Q}}(d(\mu))^n$, where $\mathcal{B} = \mathrm{End}^0(B_2)$, $\mathrm{N}_{\mathcal{B}/\mathbb{Q}}$ is the reduced norm on $\mathcal{B}$ and $n = \dim B_2/(t \cdot [F : \mathbb{Q}])$.*

Proof. The proof is the same as in [**Py02**, Proposition 5.5]. □

If $\psi\colon B_2 \to B_3$ is another isogeny then $d(\psi \circ \mu) = (\psi \circ d(\mu) \circ \psi^{-1}) \circ d(\psi)$. Hence, if we call $F = Z(\mathrm{End}(B_3))$, and we use ψ to identify $Z(\mathrm{End}(B_2))$ with F, we can write $d(\psi \circ \mu) = d(\psi) \cdot d(\mu)$ as elements in F. Moreover, it is easy to check that if α belongs to $\mathrm{End}^0(B_1)$ then $d(\alpha) = \alpha \circ \alpha'$, where the $'$ denotes the Rosati involution defined by λ_1.

Now let B be a simple abelian k-variety of the first kind, and let $\lambda\colon B \to \hat{B}$ be a polarization. It is straightforward to check that compatible isogenies $\mu_\sigma\colon {}^\sigma B \to B$ are Rosati compatible. By taking ${}^\sigma\lambda\colon {}^\sigma B \to {}^\sigma\hat{B}$ as polarizations for ${}^\sigma B$ we have that $d(\mu_\sigma) = \mu_\sigma \circ {}^\sigma\lambda^{-1} \circ \hat{\mu}_\sigma \circ \lambda$ belongs to $F = Z(\mathrm{End}(B))$. The following is a key property of the cohomology class $[c_B]$, and its proof is an application of the degree map.

Proposition 3.21. *The cohomology class $[c_B]$ has order dividing 2.*

Proof. Applying d to the expression $c_B(\sigma, \tau) = \mu_\sigma \circ {}^\sigma\mu_\tau \circ \mu_{\sigma\tau}^{-1}$ we find that $c_B(\sigma, \tau) \cdot c_B(\sigma, \tau)' = d(\mu_\sigma) \cdot d(\mu_\tau) \cdot d(\mu_{\sigma\tau})^{-1}$. Since B is of the first kind and any Rosati involution fixes F we can replace $c_B(\sigma, \tau)'$ by $c_B(\sigma, \tau)$, and this gives an expression for the cocycle c_B^2 as a coboundary. □

Now we describe the structure of $H^2(G_k, F^\times)[2]$, which turns out to be particularly simple. As we will see in the next chapter, this fact gives a lot of information about the field of definition of the endomorphisms of abelian k-varieties of the first kind.

A *sign map* for F is a group homomorphism $\mathrm{sign}\colon F^\times \to \{\pm 1\}$ such that $\mathrm{sign}(-1) = -1$. A sign map gives a group isomorphism $F^\times \simeq P \times \{\pm 1\}$, where $P = F^\times/\{\pm 1\}$. From now on we fix a sign map for F by fixing an embedding of F in $\mathbb{R}$, and then taking the usual sign. The corresponding isomorphism $F^\times \simeq P \times \{\pm 1\}$ gives then a decomposition of $H^2(G_k, F^\times)[2]$.

Proposition 3.22. *Let F be a totally real number field, and let P be the group $F^\times/\{\pm 1\}$. There exists a (non-canonical) isomorphism of groups*

$$H^2(G_k, F^\times)[2] \simeq H^2(G_k, \{\pm 1\}) \times \mathrm{Hom}(G_k, P/P^2). \tag{3.2}$$

If γ belongs to $H^2(G_k, F^\times)[2]$ we denote by $\gamma_\pm \in H^2(G_k, \{\pm 1\})$ and $\overline{\gamma} \in \mathrm{Hom}(G_k, P/P^2)$ its two components under the isomorphism (3.2)*. They can be computed, in terms of a representative c for γ, in the following way:*

1. *The cohomology class $\gamma_\pm$ is represented by the cocycle $(\sigma, \tau) \mapsto \mathrm{sign}(c(\sigma, \tau))$.*
2. *If $c(\sigma, \tau)^2 = d_\sigma d_\tau d_{\sigma\tau}^{-1}$ is an expression of c^2 as a coboundary, the map $\overline{\gamma}$ is given by $\sigma \mapsto d_\sigma \bmod \{\pm 1\}(F^\times)^2$.*

Proof. This is essentially the content of the propositions 5.3 and 5.6 in [**Py02**]. □

Remark 3.23. We will say that $\overline{\gamma}$ is the *degree component of* γ, and that $\gamma_\pm$ is the *sign component of* γ. If k has characteristic 2 then $H^2(G_k, \{\pm 1\}) = \{1\}$. From now on we assume that the characteristic of k is different from 2. In this case $H^2(G_k, \{\pm 1\})$ is isomorphic to the 2-torsion of the Brauer group of k, which is generated by the quaternion algebras over k. As it is usual, we will use the notation $(a, b)_k$ for the quaternion algebra generated over k by elements i, j such that $i^2 = a$, $j^2 = b$ and $ij + ji = 0$. As for the elements in $\mathrm{Hom}(G_k, P/P^2)$ we will use the notation $(t, d)_P$ with $t \in k$ and $d \in F^\times$, to denote (the inflation of) the homomorphism that sends the non-trivial automorphism of $\mathrm{Gal}(k(\sqrt{t})/k)$ to the class of d in P/P^2. Every element in $\mathrm{Hom}(G_k, P/P^2)$ is the product of morphisms of this kind, and therefore it can be expressed in the form $(t_1, d_1)_P \cdot (t_2, d_2)_P \cdots (t_n, d_n)_P$ for some $t_i \in k$, $d_i \in F^\times$. We remark that, although they are convenient for their compactness, these expressions for the elements of $\mathrm{Hom}(G_k, P/P^2)$ are not unique.

Minimal abelian extensions of exponent 2. Elkies proved in [**El02**] that every elliptic k-curve without CM is k_s-isogenous to some elliptic curve defined over an abelian extension of k of exponent 2 (also called a $(2, \ldots, 2)$-extension of k). He obtained this result as a consequence of the fact that elliptic k-curves are parametrized by k-rational points of curves of the form

$X_0(N)/W(N)$. Here $X_0(N)$ is the modular curve associated with the moduli problem of classifying elliptic curves together with a cyclic subgroup of order N, and $W(N)$ is the group of Atkin-Lehner involutions of $X_0(N)$. In fact, starting from a k-rational point in $X_0(N)/W(N)$ and taking a preimage of it in $X_0(N)$ one obtains a point P in $X_0(N)$ that represents an elliptic curve C defined over k_s; the point ${}^\sigma P$ corresponds to ${}^\sigma C$, and since P and ${}^\sigma P$ are related by an Atkin-Lehner involution, by the moduli interpretation of these involutions one obtains that ${}^\sigma C$ and C are isogenous. Thus C is a k-curve, and since $W(N)$ is a group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}$ we see that C is defined over an abelian extension of k of exponent 2. The point is that Elkies showed that every elliptic k-curve is isogenous to one obtained by this process applied to some k-rational point in $X_0(N)/W(N)$, for some N. A similar argument works also for abelian k-surfaces with quaternionic multiplication, as it is explained in [**GM09**], but in this case they are parametrized by k-rational points of curves of the form $X_0(D,N)/W(D,N)$, where $X_0(D,N)$ is a Shimura curve.

Ribet proved in [**Ri94**, Theorem 1.2] with a different approach that any abelian k-variety of the first kind is k_s-isogenous to some variety defined over an abelian extension of k of exponent 2. Actually more is true, because such an extension can also be taken to be the field of definition of the endomorphisms of the variety.

Theorem 3.24 (Ribet)**.** *Let B be an abelian k-variety of the first kind. There exists a variety k_s-isogenous to B and with all the endomorphisms defined over a $(2,\dots,2)$-extension of k.*

Proof. Let $\gamma = [c_B]$ be the cohomology class in $H^2(G_k, F^\times)[2]$ associated to a compatible system of isogenies for B, and let $\overline{\gamma}$ and $\gamma_\pm$ be its degree and sign components respectively. Since P/P^2 is an abelian group of exponent 2, the fixed field of k_s by $\ker\overline{\gamma}$ is a $(2,\dots,2)$-extension K_P of k, and the restriction of $\overline{\gamma}$ to K_P is trivial. The component $\gamma_\pm$ can be identified with a product of quaternion algebras, and each quaternion algebra is split by a quadratic field. Hence, $\gamma_\pm$ is split by a $(2,\dots,2)$-extension $K_\pm$. Therefore, the field $K = K_\pm K_P$ is a $(2,\dots,2)$-extension of k such that $\mathrm{Res}^K_k(\gamma)$ is trivial. The result follows now from Proposition 3.12. □

Since the restriction map respects the decomposition (3.2), a field K trivializes γ if and only if it trivializes the two components $\overline{\gamma}$ and $\gamma_\pm$. A field K trivializes $\overline{\gamma}$ if and only if it contains K_P, the fixed field of k_s by $\ker\overline{\gamma}$. As we have seen, the map $\overline{\gamma}$ is given by the degree; that is $\overline{\gamma}(\sigma) \equiv d(\mu_\sigma) \mod \{\pm 1\}(F^\times)^2$. The field K_P is of the form $K_P = k(\sqrt{t_1},\dots,\sqrt{t_n})$ for certain elements $t_i \in k$, and if we denote by σ_i the generator of $\mathrm{Gal}(k(\sqrt{t_i})/k)$ and $d_i = d(\mu_{\sigma_i})$, then in the notation described in Remark 3.23 we have that $\overline{\gamma} = (t_1,d_1)_P \cdots (t_n,d_n)_P$.

If the field K_P already trivializes $\gamma_\pm$, then K_P is the minimal field of definition of the endomorphisms of B up to isogeny. Ribet proved in [**Ri94**]

that if k has characteristic 0 then this is always the case for abelian k-varieties with real multiplication and odd dimension. However, for varieties with quaternionic multiplication, or of even dimension in general, it does not need to be the case, as the counterexamples given by Quer in [**Qu09**] show. In general, the fields of definition of the endomorphisms of B up to isogeny are the composition of K_P with a field splitting the algebra represented by $\gamma_\pm$. If K_P does not split $\gamma_\pm$ there does not exist a minimum field of definition for the endomorphisms of B, but only minimal $(2,\dots,2)$-extensions: they are the composition of K_P with any $(2,\dots,2)$-extension of k splitting $\gamma_\pm$.

Of course a main source of abelian k-varieties for the particular case $k=\mathbb{Q}$ are modular abelian varieties. For these varieties, the fields K_P and $K_\pm$ can be explicitly computed. Jordi Quer has programmed several routines in `Magma` to perform such computations, based on the packages for modular abelian varieties by William Stein. In [**Qu09**] these routines are explained, as well as the theory behind them. Moreover, in the appendix of [**Qu09**] we find tables with the fields K_P and the rational quaternion algebras $\gamma_\pm$ corresponding to the modular abelian varieties of small conductor.

CHAPTER 4

Fields of definition of k-varieties of the first kind

In the last section of Chapter 3 we have seen that given a k-variety B of the first kind, there always exist abelian extensions K/k of exponent 2 such that that B is k_s-isogenous to some variety whose endomorphisms are defined over K. Moreover, we have also given a detailed characterization of the minimal extensions having this property. This gives a fairly complete picture of the fields of definition of $\mathrm{End}^0_{k_s}(B)$ up to isogeny.

In this chapter we deal with the fields of definition of B up to isogeny. In particular, we are interested in the case where there exist fields of definition of the variety that are strictly smaller that the minimal fields of definition of the endomorphisms. In Section 4.3 we will provide examples where this situation does occur. However, as a result of our study we will see that there is a restriction in this phenomenon: if K is a minimal $(2,\dots,2)$-extension where the endomorphisms of B are defined, and $L \subseteq K$ is a field of definition of B up to isogeny, then $[K:L] \leqslant 8$.

Most of our analysis of the possible fields of definition of B up to isogeny will be based on the results of Chapter 3. In particular, in Proposition 3.16, which we now restate for convenience in a slightly modified version.

Proposition 4.1. *Let B be an abelian k-variety of the first kind and let $\gamma = [c_B]$ be the cohomology class associated to a compatible system of isogenies for B. There exists a variety B_0 defined over K and isogenous to B if and only if $\mathrm{Res}^K_k(\gamma)$ belongs to $\mathrm{im}(\delta)$, where the connecting map δ is given by:*

$$\begin{array}{rccc} \delta\colon & \mathrm{Hom}(G_K, \mathcal{B}^\times/F^\times) & \longrightarrow & H^2(G_K, F^\times) \\ & \{\sigma \mapsto \psi_\sigma F^\times\} & \longmapsto & \{(\sigma,\tau) \mapsto \psi_\sigma \circ \psi_\tau \circ \psi_{\sigma\tau}^{-1}\}. \end{array} \tag{4.1}$$

Proof. By Proposition 3.16 we know that B is defined over K up to isogeny if and only if there exists $\psi \in \mathrm{Hom}(G_K, \mathcal{B}^\times/F^\times)$ such that $\delta(\psi)\,\mathrm{Res}^K_k(\gamma) = 1$. By Proposition 3.21 the cohomology class γ has order dividing two, and then the condition is equivalent to $\mathrm{Res}^K_k(\gamma) = \delta(\psi)$. □

In view of this proposition, a key step in computing the fields of definition up to isogeny of B is to describe precisely what possibilities for the image of the connecting map δ we have. Section 4.1 is devoted to this task: we compute all possible cohomology classes of the form $\delta(\psi)$ for $\psi \in \mathrm{Hom}(G_K, \mathcal{B}^\times/F^\times)$. We use these results in Section 4.2, where we analyze to what extent it is possible to *descend* the field of definition of

the variety, starting from a minimal field of definition for the endomorphisms. Finally, is Section 4.3 we apply our study to some concrete abelian $\mathbb{Q}$-varieties.

4.1. The image of δ

Let B/k_s be a simple abelian k-variety of the first kind. This corresponds, according to the usual classification of simple abelian varieties in terms of their endomorphism algebras, to varieties of type I, II and III (see Section 1.4). The variety is of type I if $\mathcal{B} = \mathrm{End}^0(B)$ is isomorphic to a totally real number field F; it is of type II if $\mathcal{B}$ is a division totally indefinite quaternion algebra over a totally real number field F; finally, it is of type III if $\mathcal{B}$ is a division totally definite quaternion algebra over a totally real number field F. Recall that $\mathcal{B}$ is totally indefinite if $\mathcal{B} \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R}) \times \cdots \times \mathrm{M}_2(\mathbb{R})$. Equivalently, if $\mathcal{B} \simeq (a,b)_F$ then either $\sigma(a) > 0$ or $\sigma(b) > 0$ for each embedding $\sigma\colon F \to \mathbb{R}$. Similarly, $\mathcal{B}$ is totally definite if $\mathcal{B} \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{H} \times \cdots \times \mathbb{H}$, where $\mathbb{H}$ is the algebra of Hamilton quaternions, and in this case for any expression $\mathcal{B} \simeq (a,b)_F$ we have that a and b are totally negative. From now on we will consider only varieties of types II and III since, as we know from Proposition 3.15, the field of definition of the variety up to isogeny can be smaller than the field of definition of the endomorphisms only if the endomorphism algebra is noncommutative.

Let $\mathcal{B}$ be a division quaternion algebra over a totally real number field F. As we said, the goal of this section is to compute all the elements in $H^2(G_K, F^\times)[2]$ that are of the form $\delta(\psi)$ for some continuous morphism $\psi\colon G_K \to \mathcal{B}^\times/F^\times$, and to determine their components $\delta(\psi)_\pm$ and $\overline{\delta(\psi)}$ under the isomorphism $H^2(G_K, F^\times)[2] \simeq H^2(G_K, \{\pm 1\}) \times H^2(G_K, P/P^2)$. Recall that this isomorphism depends on the choice of an embedding $F \hookrightarrow \mathbb{R}$; hence, we fix such an embedding and from now on we view F as a subfield of $\mathbb{R}$.

The image of a continuous homomorphism $\psi\colon G_K \to \mathcal{B}^\times/F^\times$ is a finite subgroup of $\mathcal{B}^\times/F^\times$. In [**CF00**, §2] these subgroups are classified. In the following proposition we collect some of the results from this article that are relevant to us.

Proposition 4.2 (Chinburg-Friedman)**.** *Let $\mathcal{B}$ be a quaternion algebra over a number field F. Each finite subgroup of $\mathcal{B}^\times/F^\times$ is isomorphic to one of the following groups: a cyclic group C_n of order n, a dihedral group D_{2n} of order $2n$, the symmetric groups S_4 and S_5, or the alternating group A_4. Moreover we have that*

- *$\mathcal{B}^\times/F^\times$ always contains subgroups isomorphic to C_2.*
- *$\mathcal{B}^\times/F^\times$ always contains subgroups isomorphic to $C_2 \times C_2 \simeq D_4$.*
- *Let $n > 2$ be an integer and let ζ_n be a primitive n-th root of unity in $\overline{F}$. There exists a subgroup of $\mathcal{B}^\times/F^\times$ isomorphic to C_n if and only if $\zeta_n + \zeta_n^{-1}$ belongs to F and $F(\zeta_n)$ is isomorphic to a maximal subfield of $\mathcal{B}$.*

- *If $\mathcal{B}^\times/F^\times$ contains a subgroup isomorphic to C_n, then it also contains a subgroup isomorphic to D_{2n}.*
- *$\mathcal{B}^\times/F^\times$ contains a subgroup isomorphic to A_4 if and only if $\mathcal{B} \simeq (-1,-1)_F$.*
- *If $\mathcal{B}^\times/F^\times$ contains a subgroup isomorphic to A_4, then it contains a subgroup isomorphic to S_4 as well.*
- *$\mathcal{B}^\times/F^\times$ contains a subgroup isomorphic to A_5 if and only if $\mathcal{B} \simeq (-1,-1)_F$ and $\sqrt{5}$ belongs to F.*

In addition, when proving that this is a complete classification of finite subgroups of $\mathcal{B}^\times/F^\times$, explicit generators for subgroups of each isomorphism class are given in [**CF00**]. We will describe these generators when we need them.

Observe that if $\mathcal{B}$ is totally indefinite then A_4, S_4 and A_5 never occur as subgroups of $\mathcal{B}^\times/F^\times$, and then the only finite subgroups possible are cyclic or dihedral. The case $\mathcal{B}$ totally indefinite is specially important, since it is the case of building blocks. For these reasons we split our study into two separate cases: totally indefinite and totally definite quaternion algebras.

Totally indefinite quaternion algebras. Let $\mathcal{B}$ be a division totally indefinite quaternion algebra over a totally real number field F. In this case the only possible finite subgroups of $\mathcal{B}^\times/F^\times$ are cyclic or dihedral. In order to compute the cohomology classes $\delta(\psi)$ we will consider four separate cases, depending on whether $\operatorname{im}\psi$ is isomorphic to C_2, $C_2\times C_2$, C_n or D_{2n} for some $n>2$. We will use the following notation: if G is a group, then Δ_G will denote the set of elements $\gamma\in H^2(G_K,F^\times)[2]$ that are of the form $\gamma=\delta(\psi)$, for some morphism $\psi\colon G_K\to\mathcal{B}^\times/F^\times$ such that $\operatorname{im}\psi\simeq G$. In addition, we will make use of the notation introduced in Remark 3.23.

Proposition 4.3. *An element $\gamma\in H^2(G_K,F^\times)[2]$ belongs to Δ_{C_2} if and only if*

- *$\overline{\gamma}=(t,b)_P$, for some $t\in K^\times\setminus K^{\times 2}$ and $b\in F^\times$ such that $F(\sqrt{b})$ is isomorphic to a maximal subfield of $\mathcal{B}$.*
- *$\gamma_\pm=(t,\operatorname{sign}(b))_K$.*

Proof. Let ψ be a morphism whose image is isomorphic to C_2. Then the fixed field of $\ker\psi$ is $K(\sqrt{t})$ for some $t\in K^\times\setminus K^{\times 2}$, and ψ is the inflation of a morphism (that we also call ψ) from $\operatorname{Gal}(K(\sqrt{t})/K)$, which is determined by the image of a generator σ of the Galois group. If $\psi(\sigma)=\overline{y}$ (here $\overline{y}$ denotes the class of y in $\mathcal{B}^\times/F^\times$), then $b=y^2$ belongs to $F^\times$ and y does not belong to $F^\times$. That is, $F(\sqrt{b})$ is isomorphic to a maximal subfield of $\mathcal{B}$. From the explicit description of δ given in (4.1), a straightforward computation shows that a cocycle c representing $\delta(\psi)$ is given by

$$c(1,1)=c(1,\sigma)=c(\sigma,1)=1,\quad c(\sigma,\sigma)=b.$$

By taking the sign of this cocycle we obtain a representative for $\delta(\psi)_\pm$, and it corresponds to the quaternion algebra $(t,\operatorname{sign}(b))_K$. The cocycle c^2

is the coboundary of the map $1 \mapsto 1$, $\sigma \mapsto b$, and by Proposition 3.22 the component $\overline{\delta(\psi)}$ is $(t,b)_P$.

Now, for $t \in K^\times \setminus K^{\times 2}$ and $b \in F^\times$ such that $F(\sqrt{b})$ is isomorphic to a maximal subfield of $\mathcal{B}$, take $y \in \mathcal{B}$ with $y^2 = b$. Then the morphism $\psi\colon \mathrm{Gal}(K(\sqrt{t})/K) \to \mathcal{B}^\times/F^\times$ that sends a generator σ to $\overline{y}$ has image isomorphic to C_2, and by the previous argument the components of $\delta(\psi)$ are $\delta(\psi)_\pm = (t, \mathrm{sign}(b))_K$ and $\overline{\delta(\psi)} = (t,b)_P$. □

Proposition 4.4. *An element $\gamma \in H^2(G_K, F^\times)[2]$ lies in $\Delta_{C_2\times C_2}$ if and only if*

- *$\overline{\gamma} = (s,a)_P \cdot (t,b)_P$ for some $s,t \in K^\times \setminus K^{\times 2}$ and $a,b \in F^\times$ such that a is positive and $\mathcal{B} \simeq (a,b)_F$.*
- *$\gamma_\pm = (\mathrm{sign}(b)s, t)_K$.*

Proof. If ψ is a morphism with image isomorphic to $C_2 \times C_2$, it factors through a finite Galois extension M/K with $\mathrm{Gal}(M/K) \simeq C_2 \times C_2$. We write M as $M = K(\sqrt{s}, \sqrt{t})$, and let σ, τ be the generators of the Galois group such that $M^{\langle\sigma\rangle} = K(\sqrt{t})$ and $M^{\langle\tau\rangle} = K(\sqrt{s})$. If $\overline{x} = \psi(\sigma)$ and $\overline{y} = \psi(\tau)$, we know that $a = x^2$ belongs to $F^\times$, $b = y^2$ belongs to $F^\times$ and $xy = \varepsilon yx$ for some $\varepsilon \in F^\times$. In fact, multiplying this expression on the left by x we see that necessarily $\varepsilon = -1$, hence $\mathcal{B} \simeq (a,b)_F$.

Let $\gamma_{s,a}$ be the element in $Z^2(M/K, F^\times)$ defined as the inflation of the cocycle

$$\gamma_{s,a}(1,1) = \gamma_{s,a}(\sigma,1) = \gamma_{s,a}(1,\sigma) = 1, \quad \gamma_{s,a}(\sigma,\sigma) = a,$$

and in a similar way we define the cocycle $\gamma_{t,b}$ by means of

$$\gamma_{t,b}(1,1) = \gamma_{t,b}(\tau,1) = \gamma_{t,b}(1,\tau) = 1, \quad \gamma_{t,b}(\tau,\tau) = b.$$

Let χ_s and χ_t be the elements in $\mathrm{Hom}(\mathrm{Gal}(M/K), \mathbb{Z}/2\mathbb{Z})$ defined by the formulas ${}^\rho\sqrt{s}/\sqrt{s} = (-1)^{\chi_s(\rho)}$ and ${}^\rho\sqrt{t}/\sqrt{t} = (-1)^{\chi_t(\rho)}$, and let $\gamma_{s,t}$ be the 2-cocycle belonging to $Z^2(M/K, \{\pm 1\})$ defined by

$$\gamma_{s,t}(\rho,\mu) = (-1)^{\chi_s(\mu)\chi_t(\rho)}.$$

Then, a direct computation gives that a cocycle c representing $\delta(\psi)$ is the product of these three 2-cocycles: $c = \gamma_{s,t} \cdot \gamma_{s,a} \cdot \gamma_{t,b}$. The cocycle $\gamma_{s,t}$ represents the quaternion algebra $(s,t)_K$, and then we have that

$$\delta(\psi)_\pm = (s,t)_K \cdot (s, \mathrm{sign}(a))_K \cdot (t, \mathrm{sign}(b))_K. \tag{4.2}$$

Since $\mathcal{B}$ is totally indefinite, we can suppose that a is positive, and then $\delta(\psi)_\pm = (\mathrm{sign}(b)\, s, t)_K$. Arguing as in the proof of Proposition 4.3, the component $\overline{\delta(\psi)}$ is easily seen to be $(s,a)_P \cdot (t,b)_P$.

Finally, suppose that $\mathcal{B} \simeq (a,b)_F$ where the element a is positive. Let s,t be in $K^\times \setminus K^{\times 2}$, and let $x, y \in \mathcal{B}$ be such that $x^2 = a$, $y^2 = b$ and $xy = -yx$. With the same notations as before for $\mathrm{Gal}(K(\sqrt{s}, \sqrt{t})/K)$, the map ψ that sends σ to $\overline{x}$ and τ to $\overline{y}$ satisfies that $\delta(\psi)_\pm = (\mathrm{sign}(b)\, s, t)_K$ and $\overline{\delta(\psi)} = (s,a)_P \cdot (t,b)_P$. □

Proposition 4.5. *Suppose that $\mathcal{B}^\times/F^\times$ contains a subgroup isomorphic to C_n for some $n > 2$; let ζ_n be a primitive n-th root of unity in $\overline{F}$ and let $\alpha = 2+\zeta_n+\zeta_n^{-1}$. An element $\gamma \in H^2(G_K, F^\times)[2]$ lies in Δ_{C_n} if and only if there exists a cyclic extension M/K, with $\mathrm{Gal}(M/K) = \langle\sigma\rangle$ such that*

- *$\overline{\gamma} = (t, \alpha)$, where $K(\sqrt{t}) = M^{\langle\sigma^2\rangle}$.*
- *$\gamma_\pm$ is represented by the cocycle*

$$c_\pm(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{if } i+j < n, \\ -1 & \text{if } i+j \geqslant n. \end{cases} \tag{4.3}$$

We note that if n is odd then $\Delta_{C_n} = \{1\}$.

Proof. Let ψ be a morphism with image isomorphic to C_n. Then the fixed field for $\ker\psi$ is a cyclic extension M/K with $\mathrm{Gal}(M/K) = \langle\sigma\rangle$. The element $x \in \mathcal{B}^\times$ such that $\psi(\sigma) = \overline{x}$ has the property that $a = x^n$ lies in $F^\times$. Since $\psi(\sigma^i) = \overline{x^i}$, a straightforward computation shows that $\delta(\psi)$ is given by

$$c(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{if } i+j < n, \\ a & \text{if } i+j \geqslant n. \end{cases} \tag{4.4}$$

By [**CF00**, Lemma 2.1] we can suppose that $x = 1+\zeta$ with $\zeta \in \mathcal{B}^\times$ an element of order n. We identify ζ with ζ_n and then by Proposition 4.2 we see that $\zeta + \zeta^{-1} \in F^\times$. From $(1+\zeta)^2\zeta^{-1} = 2+\zeta+\zeta^{-1}$ we see that $(1+\zeta)^{2n} = (2+\zeta+\zeta^{-1})^n$, and if we define $\alpha = (2+\zeta+\zeta^{-1}) \in F^\times$ we have that $a^2 = x^{2n} = (1+\zeta)^{2n} = \alpha^n$. Therefore, the cocycle c^2 is the coboundary of the map $\sigma^i \mapsto \alpha^i$, $0 \leqslant i < n$, and by Proposition 3.22 the component $\overline{\delta(\psi)}$ is the map that sends σ to the class of α in P/P^2. Clearly σ^2 is in the kernel of this map, and since $\langle\sigma\rangle = \langle\sigma^2\rangle$ if n is odd, then $\overline{\delta(\psi)}$ is trivial in this case, while if n is even and $K(\sqrt{t})$ is the fixed field of M by $\langle\sigma^2\rangle$, then $\overline{\delta(\psi)} = (t, \alpha)_P$.

A cocycle representing $\delta(\psi)_\pm$ is the sign of (4.4). If n is odd, the cohomology class of this cocycle is always trivial (it is the coboundary of the map $\sigma^i \mapsto (\operatorname{sign} a)^i$ for $0 \leqslant i < n$). If n is even then a is negative because

$$a = x^n = (1+\zeta)^n = (2+\zeta+\zeta^{-1})^{n/2}\zeta^{n/2} = -(2+\zeta+\zeta^{-1})^{n/2},$$

and $2+\zeta+\zeta^{-1}$ is positive due to the identification of ζ with ζ_n. This gives that $\delta(\psi)_\pm$ is given by (4.3).

Finally, if t, M, σ and α are as in the statement of the proposition, the map ψ sending σ to $\overline{(1+\zeta)}$ with $\zeta \in B^\times$ an element of order n gives a $\delta(\psi)$ with the predicted components. □

Proposition 4.6. *Suppose that $\mathcal{B}^\times/F^\times$ contains a subgroup isomorphic to D_{2n} for some $n > 2$. Let ζ_n be a primitive n-th root of unity in $\overline{F}$, $\alpha = 2+\zeta_n+\zeta_n^{-1}$ and $d = (\zeta_n+\zeta_n^{-1})^2-4$. A cohomology class $\gamma \in H^2(G_K, F^\times)[2]$ lies in $\Delta_{D_{2n}}$ if and only if there exists a dihedral extension M/K, with $\mathrm{Gal}(M/K) = \langle\sigma,\tau \mid \sigma^n = 1, \tau^2 = 1, \sigma\tau = \tau\sigma^{-1}\rangle$ such that*

- $\overline{\gamma} = (s,\alpha)_P \cdot (t,b)_P$, *where* $L(\sqrt{s}) = M^{\langle\sigma^2,\tau\rangle}$, $L(\sqrt{t}) = M^{\langle\sigma\rangle}$ *and* $b \in F^\times$ *satisfies that* $\mathcal{B} \simeq (d,b)_F$.
- $\gamma_\pm$ *is given by the cocycle*

$$c_\pm(\sigma^i\tau, \sigma^{i'}\tau^{j'}) = \begin{cases} 1 & \text{if} \quad i - i' \geqslant 0 \\ -1 & \text{if} \quad i - i' < 0, \end{cases} \tag{4.5}$$

$$c_\pm(\sigma^i, \sigma^{i'}\tau^{j'}) = \begin{cases} 1 & \text{if} \quad i + i' < n \\ -1 & \text{if} \quad i + i' \geqslant n. \end{cases} \tag{4.6}$$

We note that if n *is odd, then* $\overline{\gamma} = (t,b)_P$ *and* $\gamma_\pm = 1$.

Proof. Let ψ be a morphism with image isomorphic to D_{2n}. It factors through a dihedral extension M with $\mathrm{Gal}(M/K) = \langle\sigma,\tau\rangle$ and relations between the generators as in the proposition. If we call $\overline{x} = \psi(\sigma)$, $\overline{y} = \psi(\tau)$, we know that $a = x^n$ belongs to $F^\times$, that $b = y^2$ belongs to $F^\times$ and that there exists some $\varepsilon \in F^\times$ such that $xy = \varepsilon y x^{-1}$. Multiplying in the left by x^{n-1} we find that $x^n y = \varepsilon^n y x^{-n}$, and so $\varepsilon^n = a^2$. Now we show that, in fact, ε can be identified with α. Indeed, $x = 1 + \zeta$ with $\zeta \in \mathcal{B}^\times$ of order n that we identify with ζ_n, and so $x^{-1} = (1 + \zeta^{-1})(2 + \zeta + \zeta^{-1})^{-1}$. Since $F(\zeta)$ is a maximal subfield of $\mathcal{B}$ different from $F(y)$, the conjugation by y is a non-trivial automorphism of $F(\zeta)/F$. The only such automorphism is complex conjugation, which sends ζ to ζ^{-1}, and therefore $y^{-1}\zeta y = \zeta^{-1}$. This implies that $(1+\zeta)y = y(1+\zeta^{-1})$, and this is $xy = (2+\zeta+\zeta^{-1})yx^{-1}$. Therefore $\varepsilon = (2 + \zeta + \zeta^{-1})$, which is identified with α.

In order to give a compact expression for $\delta(\psi)$ we first define a cocycle γ_b:

$$\gamma_b(\sigma^i\tau^j, \sigma^{i'}\tau^{j'}) = \begin{cases} 1 & \text{if } j + j' < 2, \\ b & \text{if } j + j' = 2, \end{cases} \tag{4.7}$$

and a cocycle e:

$$e(\sigma^i\tau, \sigma^{i'}\tau^{j'}) = \begin{cases} \alpha^{i'} & \text{if } i - i' \geqslant 0 \\ \alpha^{i'}a^{-1} & \text{if } i - i' < 0, \end{cases}$$

$$e(\sigma^i, \sigma^{i'}\tau^{j'}) = \begin{cases} 1 & \text{if } i + i' < n \\ a & \text{if } i + i' \geqslant n. \end{cases}$$

To compute a cocycle that represents $\delta(\psi)$, we take the lift $\tilde{\psi}$ form $\mathcal{B}^\times/F^\times$ to $\mathcal{B}$ given by $\tilde{\psi}(\sigma^i\tau^j) = x^iy^j$ for $0 \leqslant i < n$, $0 \leqslant j < 2$. Then we have that

$$\begin{aligned}
(\delta(\psi))(\sigma^i\tau, \sigma^{i'}\tau^{j'}) &= \tilde{\psi}(\sigma^i\tau)\tilde{\psi}(\sigma^{i'}\tau^{j'})\tilde{\psi}(\sigma^i\tau\sigma^{i'}\tau^{j'})^{-1} \\
&= \tilde{\psi}(\sigma^i\tau)\tilde{\psi}(\sigma^{i'}\tau^{j'})\tilde{\psi}(\sigma^{i-i'}\tau^{1+j'})^{-1} \\
&= \begin{cases} x^iyx^{i'}y^{j'}(x^{i-i'}y^{(1+j')\bmod 2})^{-1} & \text{if } i-i' \geqslant 0 \\ x^iyx^{i'}y^{j'}(x^{n+(i-i')}y^{(1+j')\bmod 2})^{-1} & \text{if } i-i' < 0 \end{cases} \\
&= \begin{cases} \alpha^{i'}x^{i-i'}y^{1+j'}y^{-(1+j')\bmod 2}\ x^{-(i-i')} & i-i' \geqslant 0 \\ \alpha^{i'}x^{i-i'}y^{1+j'}y^{-(1+j')\bmod 2}\ x^{-(i-i')}x^{-n} & i-i' < 0 \end{cases} \\
&= \begin{cases} \gamma_b(\sigma^i\tau, \sigma^{i'}\tau^{j'})\alpha^{i'} & \text{if } i-i' \geqslant 0 \\ \gamma_b(\sigma^i\tau, \sigma^{i'}\tau^{j'})\alpha^{i'}a^{-1} & \text{if } i-i' < 0, \end{cases}
\end{aligned}$$

$$\begin{aligned}
(\delta(\psi))(\sigma^i, \sigma^{i'}\tau^{j'}) &= \tilde{\psi}(\sigma^i)\tilde{\psi}(\sigma^{i'}\tau^{j'})\tilde{\psi}(\sigma^i\sigma^{i'}\tau^{j'})^{-1} \\
&= \tilde{\psi}(\sigma^i)\tilde{\psi}(\sigma^{i'}\tau^{j'})\tilde{\psi}(\sigma^{i+i'}\tau^{j'})^{-1} \\
&= \begin{cases} x^ix^{i'}y^{j'}(x^{i+i'}y^{j'})^{-1} & \text{if } i+i' < n \\ x^ix^{i'}y^{j'}(x^{(i+i')-n}y^{j'})^{-1} & \text{if } i+i' \geqslant n \end{cases} \\
&= \begin{cases} x^{i+i'}y^{j'}y^{-j'}x^{-(i+i')} & \text{if } i+i' < n \\ x^{i+i'}y^{j'}y^{-j'}x^{-(i+i')}x^n & \text{if } i+i' \geqslant n \end{cases} \\
&= \begin{cases} \gamma_b(\sigma^i, \sigma^{i'}\tau^{j'}) & \text{if } i+i' < n \\ \gamma_b(\sigma^i, \sigma^{i'}\tau^j)a & \text{if } i+i' \geqslant n. \end{cases}
\end{aligned}$$

From these expressions we see that $\delta(\psi)$ is represented by the cocycle $\gamma_b \cdot e$. Clearly γ_b is 2-torsion since γ_b^2 is the coboundary of the map $d_\gamma(\sigma^i) = 1$, $d_\gamma(\sigma^i\tau) = b$. The cocycle e is 2-torsion as well, and a coboundary for e^2 is given by the map $d_e(\sigma^i\tau^j) = \alpha^i$. If we view d_γ and d_e as taking values in P/P^2, then by Proposition 3.22 we have that $\overline{\delta(\psi)}$ is the map $d_e \cdot d_\gamma$. Note that $\langle\sigma^2, \tau\rangle \subseteq \ker d_e$. If n is odd, then $\langle\sigma^2, \tau\rangle = \mathrm{Gal}(M/K)$ and the only contribution to $\overline{\delta(\psi)}$ comes from d_γ, and it is the map $(t, b)_P$. If n is even, then the contribution of γ_e is (s, α), and in this case $\overline{\delta(\psi)} = (s, \alpha)_P \cdot (t, b)_P$.

The component $\delta(\psi)_\pm$ comes from taking the sign in the cocycle $\gamma_b \cdot e$. The element b is positive, since by [**CF00**, Lemma 2.3] we have that $\mathcal{B} \simeq (d, b)_F$ and d is negative. To determine the sign of a, note that from $\alpha^n = a^2$, we have that if n is even then $\alpha^{n/2} = \pm a$. The case $\alpha^{n/2} = a$ is not possible since otherwise $F(x^{n/2}, y)$ would be a subfield of $\mathcal{B}$ of dimension 4 over F. Then $\alpha^{n/2} = -a$ and the fact that α is totally positive forces a to be negative. This gives that $\delta(\psi)_\pm$ is represented by the cocycle given by (4.5) and (4.6). If n is odd then $c_\pm$ is the coboundary of the map $\sigma^i\tau^j \mapsto (-1)^i$.

As usual, given an extension M/K, elements $b \in F^\times$, $s, t \in K^\times$ and $c_\pm \in Z^2(M/K, \{\pm 1\})$ with the properties described in the proposition, one

can construct easily a map ψ with the prescribed $\delta(\psi)$ just defining $\psi(\sigma) = \overline{x}$ and $\psi(\tau) = \overline{y}$, where $\overline{x}, \overline{y}$ generate a subgroup of $\mathcal{B}^\times$ isomorphic to D_{2n} and $y^2 = b$. □

Totally definite quaternion algebras. Let $\mathcal{B}$ be a totally definite quaternion algebra over F. The description of Δ_G when G is a cyclic or a dihedral group is very similar to the case of totally indefinite algebras, being the only differences in the sign components; in fact, the proofs are almost the same, with minor changes concerning the sign of some elements in $F^\times$.

Proposition 4.7. *An element $\gamma \in H^2(G_K, F^\times)[2]$ belongs to Δ_{C_2} if and only if*

- *$\overline{\gamma} = (t, b)_P$, with $t \in K^\times \setminus K^{\times 2}$ and $b \in F^\times$ is such that $F(\sqrt{b})$ is isomorphic to a maximal subfield of $\mathcal{B}$.*
- *$\gamma_\pm = (t, -1)_K$.*

Proof. This is proved exactly as Proposition 4.3, but noticing that now b has to be a negative element, hence $\operatorname{sign}(b) = -1$. □

Proposition 4.8. *An element $\gamma \in H^2(G_K, F^\times)[2]$ lies in $\Delta_{C_2 \times C_2}$ if and only if*

- *$\overline{\gamma} = (s, a)_P \cdot (t, b)_P$, where $s, t \in K^\times \setminus K^{\times 2}$ and $\mathcal{B} \simeq (a, b)_F$.*
- *$\gamma_\pm = (s, t)_K \cdot (-1, st)_K$.*

Proof. The only difference with Proposition 4.4 is that in the expression (4.2) both a and b are negative, and this gives that the sign component is $(s, t)_K \cdot (-1, st)_K$. □

Proposition 4.9. *Suppose that $\mathcal{B}^\times/F^\times$ contains a subgroup isomorphic to C_n for some $n > 2$, let ζ_n be a primitive n-th root of unity in $\overline{F}$ and let $\alpha = 2 + \zeta_n + \zeta_n^{-1}$. An element $\gamma \in H^2(G_K, F^\times)[2]$ lies in Δ_{C_n} if and only if there exists a cyclic extension M/K, with $\operatorname{Gal}(M/K) = \langle\sigma\rangle$ such that*

- *$\overline{\gamma} = (t, \alpha)$, where $K(\sqrt{t}) = M^{\langle\sigma^2\rangle}$.*
- *$\gamma_\pm$ is represented by the cocycle*

$$c_\pm(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{if } i + j < n, \\ -1 & \text{if } i + j \geqslant n. \end{cases} \tag{4.8}$$

We note that if n is odd then $\Delta_{C_n} = \{1\}$.

Proof. In this case the result and the proof are exactly the same as in Proposition 4.5, since no use of the fact that the algebra was totally indefinite was made there. □

Proposition 4.10. *Suppose that $\mathcal{B}^\times/F^\times$ contains a subgroup isomorphic to D_{2n} for some $n > 2$. Let ζ_n be a primitive n-th root of unity in $\overline{F}$, $\alpha = 2 + \zeta_n + \zeta_n^{-1}$ and $d = (\zeta_n + \zeta_n^{-1})^2 - 4$. A cohomology class $\gamma \in H^2(G_K, F^\times)[2]$ lies in $\Delta_{D_{2n}}$ if and only if there exists a dihedral extension M/K, with $\operatorname{Gal}(M/K) = \langle\sigma, \tau \mid \sigma^n = 1, \tau^2 = 1, \sigma\tau = \tau\sigma^{-1}\rangle$ such that*

- $\overline{\gamma} = (s,\alpha)_P \cdot (t,b)_P$, *where* $L(\sqrt{s}) = M^{\langle\sigma^2,\tau\rangle}$, $L(\sqrt{t}) = M^{\langle\sigma\rangle}$ *and* $b \in F^\times$ *satisfies that* $\mathcal{B} \simeq (d,b)_F$.
- $\gamma_\pm$ *is given by the cocycle*

$$c_\pm(\sigma^i\tau, \sigma^{i'}\tau^{j'}) = \begin{cases} (-1)^{j'} & \text{if} \quad i - i' \geqslant 0 \\ (-1)^{1+j'} & \text{if} \quad i - i' < 0, \end{cases} \tag{4.9}$$

$$c_\pm(\sigma^i, \sigma^{i'}\tau^{j'}) = \begin{cases} 1 & \text{if} \quad i + i' < n \\ -1 & \text{if} \quad i + i' \geqslant n. \end{cases} \tag{4.10}$$

We note that if n *is odd, then* $\overline{\gamma} = (t,b)_P$ *and* $\gamma_\pm = 1$.

Proof. Again, the argument is as in Proposition 4.6, but now the sign of b in (4.7) is -1, and modifying accordingly the sign component $\gamma_\pm$ we obtain the result. □

Now we turn our attention to the subgroups of $\mathcal{B}^\times/F^\times$ isomorphic to A_4, S_4 and A_5. The precise structure of these subgroups is given in the following proposition, whose proof can be found in [**CF00**, §2].

Proposition 4.11 (Chinburg-Friedman)**.** *The group* $\mathcal{B}^\times/F^\times$ *contains a subgroup isomorphic to* S_4 *if and only if it contains a subgroup isomorphic to* A_4. *This occurs if and only if* $\mathcal{B} \simeq (-1,-1)_F$. *On the other hand,* $\mathcal{B}^\times/F^\times$ *contains a subgroup isomorphic to* A_5 *if and only if* $\mathcal{B} \simeq (-1,-1)_F$ *and* $\sqrt{5}$ *belongs to* F. *Moreover, any two of these subgroups are always conjugated if they are isomorphic as abstract groups.*

Let $\imath, \jmath$ *and* κ *be elements of* $\mathcal{B}^\times$ *such that* $\imath^2 = -1$, $\jmath^2 = -1$, $\imath\jmath = \kappa$ *and* $\jmath\imath = -\kappa$, *and let* $\alpha_2 = (1 + \imath + \jmath + \kappa)/2$. *Then the subgroup of* $\mathcal{B}^\times/F^\times$ *generated by the classes of* $\imath$ *and* α_2 *is isomorphic to* A_4, *and the subgroup generated by the classes of* $1 + \imath$ *and* α_2 *is isomorphic to* S_4. *Suppose that* $\sqrt{5}$ *belongs to* F, *and define* $\tau = (1+\sqrt{5})/2$ *and* $\alpha_4 = (\tau + \tau^{-1}\imath + \jmath)/2$. *The subgroup generated by the classes of* α_2 *and* α_4 *is isomorphic to* A_5.

Proposition 4.12. *Let* $\psi\colon G_K \to \mathcal{B}^\times/F^\times$ *be a continuous morphism with image isomorphic to* A_4. *Then* $\overline{\delta(\psi)}$ *is trivial.*

Proof. The homomorphism ψ can be regarded as the inflation of a homomorphism $\psi\colon \mathrm{Gal}(M/K) \to \mathcal{B}^\times/F^\times$, where M/K is an extension with $\mathrm{Gal}(M/K) \simeq A_4$. We can take the following presentation for $\mathrm{Gal}(M/K)$: $\mathrm{Gal}(M/K) \simeq \langle a, b \,|\, a^2 = 1,\, b^3 = 1, (ab^2)^3 = 1\rangle$, and under this identification its elements are

$$\mathrm{Gal}(M/K) = \{1, a, b, b^2, ab, ab^2, ba, b^2a, bab, b^2ab, bab^2, aba\}.$$

By Proposition 4.11 we know that $\mathrm{im}(\psi)$ is conjugated to the subgroup generated by $\overline{\imath}$ and $\overline{\alpha}_2$. But ψ and a conjugated of ψ have the same image by δ, hence we can assume that $\mathrm{im}(\psi)$ is the group generated by $\overline{\imath}$ and $\overline{\alpha}_2$. These elements of $\mathcal{B}^\times/F^\times$ satisfy that $\overline{\imath}^2 = 1$, $\overline{\alpha}_2^3 = 1$ and $(\overline{\imath}\,\overline{\alpha}_2^2)^3 = 1$, so we

can suppose that $\psi(a) = \overline{\imath}$ and $\psi(b) = \overline{\alpha}_2$. Hence we can take the following lift $\tilde{\psi}$ of ψ in $\mathcal{B}^\times$:

$$\begin{array}{llll} \tilde{\psi}(1) = 1, & \tilde{\psi}(a) = \imath, & \tilde{\psi}(b) = \alpha_2, & \tilde{\psi}(b^2) = \alpha_2^2, \\ \tilde{\psi}(ab) = \imath\alpha_2, & \tilde{\psi}(ab^2) = \imath\alpha_2^2, & \tilde{\psi}(ba) = \alpha_2\imath, & \tilde{\psi}(b^2a) = \alpha_2^2\imath, \\ \tilde{\psi}(bab) = \alpha_2\imath\alpha_2, & \tilde{\psi}(b^2ab) = \alpha_2^2\imath\alpha_2, & \tilde{\psi}(bab^2) = \alpha_2\imath\alpha_2^2, & \tilde{\psi}(aba) = \imath\alpha_2\imath. \end{array}$$

The fact that $\psi(\sigma)\psi(\tau)\psi(\sigma\tau)^{-1}$ is equal to 1 in $\mathcal{B}^\times/F^\times$ means that we can transform the expression $\psi(\sigma)\psi(\tau)\psi(\sigma\tau)^{-1}$ to $1 \in \mathcal{B}^\times/F^\times$ by using the relations $\overline{\imath}^2 = 1$, $\overline{\alpha}_2^3 = 1$ and $(\overline{\imath}\,\overline{\alpha}_2^2)^3 = 1$. Since $\imath^2 = -1$, $\alpha_2^3 = -1$ and $(\imath\alpha_2^2)^3 = 1$, using these relations we can transform the element $\tilde{\psi}(\sigma)\tilde{\psi}(\tau)\tilde{\psi}(\sigma\tau)^{-1}$ into an element of $F^\times$, which necessarily is equal to either 1 or -1. Therefore $\delta(\psi)^2(\sigma,\tau)$ is equal to 1 for all σ and τ in G_K, and then $\overline{\delta(\psi)}$ is trivial. □

Proposition 4.13. *Let $\psi\colon G_K \to \mathcal{B}^\times/F^\times$ be a continuous morphism with image isomorphic to S_4. Let M be the fixed field of k_s by the kernel of ψ, and let t be an element in K such that $\mathrm{Gal}(M/K(\sqrt{t})) \simeq A_4$. Then $\overline{\delta(\psi)} = (t,2)_P$.*

Proof. By the previous proposition the morphism $\overline{\delta(\psi)}$ restricted to the subgroup $\mathrm{Gal}(k_s/K(\sqrt{t}))$ is trivial. Thus $\overline{\delta(\psi)}$ is the inflation of a morphism $\psi\colon \mathrm{Gal}(K(\sqrt{t})/K) \to \mathcal{B}^\times/F^\times$, and this implies that it is of the form $(t,d)_P$ for some d. A presentation of $\mathrm{Gal}(M/K)$ which is isomorphic to S_4 is given by

$$\mathrm{Gal}(M/K) \simeq \langle e, f \,|\, e^4 = 1,\ f^3 = 1,\ (ef)^2 = 1\rangle,$$

and the elements $a = e^2$ and $b = f$ satisfy the relations given in the presentation of A_4 we used in the proof of Proposition 4.12. From Proposition 4.11 we can suppose that $\mathrm{im}(\psi)$ is generated by $\overline{1+\imath}$ and $\overline{\alpha}_2$, and these elements satisfy the same relations as e and f. This means that we can take a lift of ψ such that $\tilde{\psi}(e) = 1 + \imath$ and $\tilde{\psi}(a) = \imath$. Then

$$\tilde{\psi}(e)\tilde{\psi}(e)\tilde{\psi}(a)^{-1} = (1+\imath)(1+\imath)\imath^{-1} = 2,$$

and from this we obtain that $\overline{\delta(\psi)}(e) \equiv 2 \mod \{\pm 1\}F^{\times 2}$. □

Proposition 4.14. *Let $\psi\colon G_K \to \mathcal{B}^\times/F^\times$ be a continuous homomorphism with image isomorphic to A_5. Then $\overline{\delta(\psi)}$ is trivial.*

Proof. The reasoning is the same as in Proposition 4.12. Let M be the field fixed by the kernel of ψ. Then $\mathrm{Gal}(M/K) \simeq A_5$ has a presentation given by

$$\mathrm{Gal}(M/K) \simeq \langle a, b \,|\, a^2 = 1,\ b^3 = 1,\ (ab)^5 = 1\rangle. \tag{4.11}$$

By Proposition 4.11 we can suppose that $\mathrm{im}(\psi)$ is generated by $\overline{\alpha}_2$ and $\overline{\alpha}_4$, and therefore it is also generated by $\overline{\alpha_4\alpha_2}$ and $(\overline{\alpha}_2)^2$. These last two generators satisfy the same relations as a and b in (4.11), that is: $(\overline{\alpha_4\alpha_2})^2 = 1$, $(\overline{\alpha}_2^2)^3 = 1$ and $(\overline{\alpha}_4)^5 = 1$. Hence we can take a lift $\tilde{\psi}$ such that $\tilde{\psi}(a) = \alpha_4\alpha_2$, $\tilde{\psi}(b) = \alpha_2^2$ and $\tilde{\psi}(ab) = \alpha_4$. But $(\alpha_4\alpha_2)^2 = -1$, $(\alpha_2^2)^3 = 1$ and $\alpha_4^5 = -1$, and therefore $\delta(\psi)$ takes values in $\{\pm 1\}$. □

Remark 4.15. Observe that in the proofs of Propositions 4.12, 4.13 and 4.14 we have computed the images (up to conjugation) of the morphism ψ. From this, it is straightforward to derive the explicit expression for the sign component $\delta(\psi)_{\pm}$.

4.2. Descent of the field of definition of the variety

Let B/k_s be a simple abelian k-variety of type II or III, and let $\mathcal{B}$ be its endomorphism algebra with center F. Suppose that the endomorphisms of B are defined over a minimal $(2,\dots,2)$-extension K of k. In this section we investigate the subfields of K that are fields of definition of B up to isogeny.

Proposition 4.16. *Suppose that B is defined up to isogeny over a field L such that $k \subseteq L \subseteq K$. Then $[K:L] \leqslant 8$.*

Proof. Let $\gamma = [c_B]$ be the cohomology class attached to B. By Proposition 4.1 there exists a continuous morphism $\psi\colon G_L \to \mathcal{B}^\times/F^\times$ such that $\mathrm{Res}^L_k(\gamma) = \delta(\psi)$. By the results of the previous section characterizing the elements of the form $\delta(\psi)$ we can always find a field M with $[M:L] \leqslant 8$ (and in fact with $[M:L] \leqslant 4$ if $\mathrm{im}(\delta)$ is not isomorphic to D_{2n} with $n > 2$) such that $\mathrm{Res}^M_L(\delta(\psi)) = 1$. But then $\mathrm{Res}^M_k(\gamma) = 1$ and M is a field of definition of the endomorphisms of B. The minimality of K implies that $[K:L] \leqslant 8$. □

It is clear that if B_0/L is isogenous to B with L strictly contained in K, then $\mathrm{End}^0_L(B_0) \subsetneq \mathrm{End}^0_{k_s}(B_0)$. An interesting case of this situation is when the endomorphisms of B_0 are defined over K, but then the field L cannot be much smaller than K, as we can see in the following proposition.

Proposition 4.17. *Let B be a building block such that B and its endomorphisms are defined over a minimal $(2,\dots,2)$-extension K. There exists a variety B_0 defined over $L \subsetneq K$ that is K-isogenous to B and has all of its endomorphisms defined over K if, and only if, there exists a continuous homomorphism $\psi : G_L \to \mathcal{B}^\times/F^\times$ such that $\mathrm{Res}^L_k(\gamma) = \delta(\psi)$ and $G_K \subseteq \ker(\psi)$. In particular $\mathrm{Gal}(K/L) \simeq C_2$ or $\mathrm{Gal}(K/L) \simeq C_2 \times C_2$.*

Proof. Let $\kappa : B \to B_0$ be an isogeny defined over K, where B_0 is defined over L and $\mathrm{End}^0_{k_s}(B_0) = \mathrm{End}^0_K(B_0)$. For $\sigma \in G_L$ let $\nu_\sigma = \kappa^{-1} \circ {}^\sigma\kappa$, and let $\psi_\sigma = \nu_\sigma \circ \mu_\sigma^{-1}$ where μ_σ is a compatible isogeny for B. Since $\nu_\sigma \circ {}^\sigma\nu_\tau \circ \nu_{\sigma\tau}^{-1} = 1$ for all $\sigma, \tau \in G_L$, we see that $\mathrm{Res}^L_k(\gamma) = \delta(\psi)$. Moreover, for $\sigma \in G_K$ the isogeny μ_σ lies in $F^\times$ and $\nu_\sigma = 1$, so ψ_σ belongs to $F^\times$.

For the other implication, for $\sigma \in G_L$ let $\nu_\sigma = \psi_\sigma \circ \mu_\sigma$, with μ_σ a compatible isogeny. Under the conditions of the proposition, there exists a variety B_0 defined over L and an isogeny $\kappa : B \to B_0$ such that $\nu_\sigma = \kappa^{-1} \circ {}^\sigma\kappa$. Then any endomorphism of B_0 is of the form $\kappa \circ \varphi \circ \kappa^{-1}$ for some $\varphi \in \mathrm{End}^0_{k_s}(B)$.

Then for $\sigma \in G_K$ we have that

$$\begin{aligned} {}^{\sigma}(\kappa\circ\varphi\circ\kappa^{-1}) &= {}^{\sigma}\kappa\circ{}^{\sigma}\varphi\circ{}^{\sigma}\kappa^{-1} = \kappa\circ\psi_\sigma\circ\mu_\sigma\circ{}^{\sigma}\varphi\circ\mu_\sigma^{-1}\circ\psi_\sigma^{-1}\circ\kappa^{-1} \\ &= \kappa\circ\psi_\sigma\circ\varphi\circ\psi_\sigma^{-1}\circ\kappa^{-1} = \kappa\circ\varphi\circ\kappa^{-1}. \end{aligned}$$

Finally, the last statement follows because $\mathrm{Gal}(K/L)$ must be isomorphic to a subgroup of $\mathcal{B}^\times/F^\times$, and all abelian groups of exponent 2 contained in $\mathcal{B}^\times/F^\times$ are isomorphic to either C_2 or $C_2 \times C_2$. □

4.3. Examples: building blocks with quaternionic multiplication

In this section we show in some concrete examples how the techniques developed so far can be used to descend the field of definition of k-varieties, starting from a minimal field of definition for their endomorphisms. Our examples will be abelian $\mathbb{Q}$-varieties and, more concretely, building blocks with quaternionic multiplication arising from modular abelian varieties. In Section 6.1 we will briefly review the theory of modular abelian varieties and its relation with abelian varieties of GL_2-type. At this point, we just recall that to each non-CM newform $f = \sum a_n q^n$ of weight 2 for $\Gamma_1(N)$ one can associate an abelian variety A_f of GL_2-type over $\mathbb{Q}$, such that $\mathrm{End}^0_{\mathbb{Q}}(A_f)$ is isomorphic to $\mathbb{Q}(\{a_n\}_{n\geqslant 1})$. We will denote by B_f the corresponding building block such that $A_f \sim_{\overline{\mathbb{Q}}} (B_f)^n$.

We will use the information provided by the building block table of [**Qu09**, Section 5.1 of the Appendix]. This data can also be obtained directly by means of the `Magma` functions implemented by Jordi Quer, which are based on the packages of William Stein for modular abelian varieties.

Example 4.18. Let f be the unique newform of level 243 and trivial Nebentypus that appears in the table. The variety A_f has dimension 2 and it is absolutely simple, so in this case $A_f \sim_{\overline{\mathbb{Q}}} B_f$. Therefore, we know a priori that $\mathbb{Q}$ is a field of definition of B_f up to isogeny. Let us see how this can also be deduced using our results.

Let $\gamma = [c_{B_f}]$ be the corresponding cohomology class. The components of γ are $\gamma_\pm = 1$ and $\overline{\gamma} = (-3,6)_P$, and $K_P = \mathbb{Q}(\sqrt{-3})$ is a minimum field of definition of B_f and of its endomorphisms up to isogeny. The endomorphism algebra $\mathcal{B}$ is the quaternion algebra over $\mathbb{Q}$ ramified at the primes 2 and 3. The field $\mathbb{Q}(\sqrt{6})$ is isomorphic to a maximal subfield of $\mathcal{B}$, and by Proposition 4.3 there exists a morphism $\psi\colon G_{\mathbb{Q}} \to \mathcal{B}^\times/\mathbb{Q}^\times$ such that $\overline{\delta(\psi)} = (-3,6)_P$ and $\delta(\psi)_\pm = (-3,1)_{\mathbb{Q}}$, which is trivial in $H^2(G_{\mathbb{Q}}, \{\pm 1\})$. Therefore $\gamma \cdot \delta(\psi) = 1$ and we deduce the existence of an abelian variety defined over $\mathbb{Q}$ and isogenous to B_f.

Remark 4.19. In general, if f is a newform of weight two for $\Gamma_1(N)$ such that the variety A_f is absolutely simple and has quaternionic multiplication over $\overline{\mathbb{Q}}$, then the minimal field of definition of all the endomorphisms of A_f will always be strictly larger that $\mathbb{Q}$. However, it is obvious that the variety A_f is defined over $\mathbb{Q}$. This is a rather trivial case where the field of

definition of the variety is strictly smaller than the field of definition of the endomorphisms. We have included one of these trivial examples in order to show that they can also be recovered with our techniques. The following are nontrivial examples, in the sense that it is not clear a priori whether their field of definition can be descended or not, and it is then necessary to use the results of the previous sections.

Example 4.20. Let f be the unique modular form in the table of level 60 and Nebentypus of order 4. In this case the variety A_f is 4-dimensional and $A_f \sim_{\overline{\mathbb{Q}}} (B_f)^2$. The cohomology class associated to B_f has components $\overline{\gamma} = (5,2)_P \cdot (-3,5)_P$, and $\gamma_\pm$ is the quaternion algebra over $\mathbb{Q}$ ramified at the primes 3 and 5. The field $K_P = \mathbb{Q}(\sqrt{5}, \sqrt{-3})$ is the minimum field of definition of the variety and of its endomorphisms up to isogeny, and the algebra $\mathcal{B} = \mathrm{End}^0_{\overline{\mathbb{Q}}}(B_f)$ is the quaternion algebra over $\mathbb{Q}$ ramified at 2 and 5, which is isomorphic to $(-2,5)_\mathbb{Q}$. Hence, by Proposition 4.4 there exists a $\psi\colon G_\mathbb{Q} \to \mathcal{B}^\times/\mathbb{Q}^\times$ such that $\overline{\delta(\psi)} = (5,-2)_P \cdot (-3,5)_P$ and $\delta(\psi)_\pm = (5,3)_\mathbb{Q}$, which is the quaternion algebra ramified at 3 and 5. Hence $\gamma \cdot \delta(\psi) = 1$ and by Proposition 4.17 there exists a variety B_0 defined over $\mathbb{Q}$ and with all its endomorphisms defined over K_P that is isogenous to B_f.

In [**DR05**] there are some equations of genus two curves over $\mathbb{Q}$, whose Jacobian has QM over $\overline{\mathbb{Q}}$. These are explicit examples of the phenomenon described above from the modular point of view.

Example 4.21. Let f be the unique modular form in the table of level 80 and Nebentypus of order 4. The dimension of A_f is 4 and $A_f \sim_{\overline{\mathbb{Q}}} (B_f)^2$. Now $\overline{\gamma} = (5,2)_P \cdot (-4,3)_P$ and $\gamma_\pm$ is the quaternion algebra over $\mathbb{Q}$ ramified at 2 and 5. Again K_P, which in this case is $\mathbb{Q}(\sqrt{5}, \sqrt{-1})$, is the minimum field of definition of B_f and of its endomorphisms up to isogeny.

First, we show that there does not exist a variety B_0 defined over $\mathbb{Q}$ and with all its endomorphisms defined over K_P. By Proposition 4.17 the existence of such variety would be equivalent to the existence of a $\psi\colon G_\mathbb{Q} \to \mathcal{B}^\times/\mathbb{Q}^\times$ with image isomorphic to $C_2 \times C_2$ such that $\overline{\delta(\psi)} = \overline{\gamma}$ and $\delta(\psi)_\pm = \gamma_\pm$. By Proposition 4.4, $\overline{\delta(\psi)} = (s,a)_P \cdot (t,b)_P$ with $\mathcal{B} \simeq (a,b)_\mathbb{Q}$. If we want $\overline{\delta(\psi)} = \overline{\gamma}$, the only possibilities for a, b modulo squares are the following: $a = 2$ and $b = 3$, $a = 2$ and $b = -3$, $a = -2$ and $b = 3$ or $a = -2$ and $b = -3$. Since $\mathcal{B}$ is the quaternion algebra of discriminant 6, only the first two options are possible. But if $\overline{\delta(\psi)} = (5,2)_P \cdot (-4,3)_P$, from Proposition 4.4 we see that $\delta(\psi)_\pm = (5,-4)_\mathbb{Q}$, which is not equal to $\gamma_\pm$, and if $\overline{\delta(\psi)} = (5,2)_P \cdot (-4,-3)_P$ then $\delta(\psi)_\pm = (-5,-4)_\mathbb{Q}$ which is also not equal to $\gamma_\pm$. Hence there does not exist such a ψ.

Now we will see that there exists a $\psi\colon G_\mathbb{Q} \to \mathcal{B}^\times/F^\times$ with image isomorphic to $D_{2\cdot 4}$ such that $\gamma \cdot \delta(\psi) = 1$. This tells us that there exists an abelian variety B_0 defined over $\mathbb{Q}$ that is isogenous to B_f, but that does not have all its endomorphisms defined over K_P. First of all, we observe that $\mathcal{B} \simeq (-1,3)_\mathbb{Q}$, and so $\mathcal{B}$ contains a maximal subfield isomorphic to $\mathbb{Q}(i)$,

where $i = \sqrt{-1}$. This implies that $\mathcal{B}^\times/\mathbb{Q}^\times$ contains subgroups isomorphic to $D_{2\cdot 4}$. More precisely, if x, y are elements in $\mathcal{B}$ such that $x^2 = -1$, $y^2 = 3$, and $xy = -yx$, then the subgroup of $\mathcal{B}^\times/\mathbb{Q}^\times$ generated by $\overline{1+x}$ and $\overline{y}$ is isomorphic to $D_{2\cdot 4}$.

The number field $M = \mathbb{Q}(\sqrt[4]{5}, i)$ has $\mathrm{Gal}(M/\mathbb{Q}) \simeq D_{2\cdot 4}$, generated by the automorphisms $\sigma\colon \sqrt[4]{5} \mapsto i\sqrt[4]{5},\ i \mapsto i$ and $\tau\colon \sqrt[4]{5} \mapsto \sqrt[4]{5},\ i \mapsto -i$. We define $\psi\colon G_\mathbb{Q} \to \mathcal{B}^\times/F^\times$ as the morphism sending σ to $\overline{1+x}$ and τ to $\overline{y}$. From the expressions given in Proposition 4.6 we see that $\overline{\delta(\psi)} = (-1,3)_P \cdot (5,2)_P$, which is equal to $\overline{\gamma}$. It only remains to see that $\delta(\psi)_\pm = \gamma_\pm$. Let D be the quaternion algebra associated to $\delta(\psi)_\pm$. Since $\delta(\psi)_\pm$ belongs to $Z^2(M/\mathbb{Q}, \{\pm 1\})$ and the extension $M/\mathbb{Q}$ only ramifies at the primes 2 and 5, D can only ramify at the places 2, 5 and ∞ (see [**Pi82**, Proposition 18.5]). We will see that $D \otimes_\mathbb{Q} \mathbb{Q}(i)$ is not trivial in the Brauer group (and therefore D ramifies at some prime), and that $D \otimes_\mathbb{Q} \mathbb{Q}(\sqrt{5})$ is trivial (and therefore D does not ramify at ∞). These two conditions imply that D ramifies exactly at 2 and 5.

Since $\mathrm{Gal}(M/\mathbb{Q}(i)) = \langle\sigma\rangle$, a 2-cocycle c representing $D \otimes_\mathbb{Q} \mathbb{Q}(i)$ is the restriction to the subgroup $\langle\sigma\rangle \subseteq \mathrm{Gal}(M/\mathbb{Q})$ of a cocycle representing $\delta(\psi)_\pm$. From (4.5) and (4.6) we obtain that

$$c(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{if } i + j < 4 \\ -1 & \text{if } i + j \geqslant 4. \end{cases}$$

By [**Pi82**, Lemma 15.1] the algebra associated to this cocycle is trivial if and only if -1 belongs to $\mathrm{Nm}_{M/\mathbb{Q}(i)}(M)$, where $\mathrm{Nm}_{M/\mathbb{Q}(i)}$ refers to the norm in the extension $M/\mathbb{Q}(i)$. But -1 is not a norm of this extension, hence $D \otimes_\mathbb{Q} \mathbb{Q}(i)$ is non-trivial in the Brauer group.

Since $\mathrm{Gal}(M/\mathbb{Q}(\sqrt{5})) = \langle\sigma^2, \tau\rangle$, a 2-cocycle c representing $D \otimes_\mathbb{Q} \mathbb{Q}(\sqrt{5})$ is the restriction to $\langle\sigma^2, \tau\rangle \subseteq \mathrm{Gal}(M/\mathbb{Q})$ of a cocycle representing $\delta(\psi)_\pm$. Again from (4.5) and (4.6) we obtain the following:

$$\begin{array}{llll} c(1,1) = 1 & c(\sigma^2,1) = 1 & c(\tau,1) = 1 & c(\sigma^2\tau,1) = 1 \\ c(1,\sigma^2) = 1 & c(\sigma^2,\sigma^2) = -1 & c(\tau,\sigma^2) = -1 & c(\sigma^2\tau,\sigma^2) = 1 \\ c(1,\tau) = 1 & c(\sigma^2,\tau) = 1 & c(\tau,\tau) = 1 & c(\sigma^2\tau,\tau) = 1 \\ c(1,\sigma^2\tau) = 1 & c(\sigma^2,\sigma^2\tau) = -1 & c(\tau,\sigma^2\tau) = -1 & c(\sigma^2\tau,\sigma^2\tau) = 1. \end{array}$$

To see that the cohomology class of this cocycle in $H^2(M/\mathbb{Q}(\sqrt{5}), M^\times)$ is trivial (where now the action is the natural Galois action), we define a map λ by $\lambda(1) = 1$, $\lambda(\sigma^2) = i$, $\lambda(\tau) = i$ and $\lambda(\sigma^2\tau) = -i$. Now a computation shows that $c(\rho, \mu) = \lambda(\rho) \cdot {}^\rho\lambda(\mu) \cdot \lambda(\rho\mu)^{-1}$ for all $\rho, \mu \in \mathrm{Gal}(M/\mathbb{Q}(\sqrt{5}))$.

Example 4.22. Let f be the unique modular form in the table of level 336 and Nebentypus of order 6. The dimension of A_f is 8 and $A_f \sim_{\overline{\mathbb{Q}}} (B_f)^4$. For this variety $\overline{\gamma} = (-3, 11)_P$ and $\gamma_\pm$ is the quaternion algebra ramified at 2 and 3. Hence $K_P = \mathbb{Q}(\sqrt{-3})$ and since $\mathrm{Res}^{K_P}_\mathbb{Q}(\gamma_\pm) = 1$ we have that K_P is the minimum field of definition of B_f and of its endomorphisms up to

isogeny. We will show that B_f is not isogenous to any variety defined over $\mathbb{Q}$.

As K_P is a quadratic number field and $\gamma_\pm \neq 1$, the only morphisms ψ we have to consider are those with image isomorphic to C_2 or to C_n for some even $n > 2$. The only such values of n with $\mathcal{B}^\times/\mathbb{Q}^\times$ containing a subgroup isomorphic to C_n are $n = 4$ and $n = 6$. Since the component $\overline{\delta(\psi)}$ associated to a ψ with image C_n has the form $(t, 2+\zeta_n+\zeta_n^{-1})$, and for $n = 4, 6$ we have that $2+\zeta_n+\zeta_n^{-1}$ is not congruent to 11 modulo $\{\pm 1\}\mathbb{Q}^{*2}$, it turns out that there does not exist any ψ with image C_4 or C_6 such that $\gamma \cdot \overline{\delta(\psi)} = 1$. If ψ has image C_2, the only possibilities are $\overline{\delta(\psi)} = (-3, 11)$ or $\overline{\delta(\psi)} = (-3, -11)$. In the first case we would have $\delta(\psi)_\pm = (-3, 1)_\mathbb{Q}$ and in the second case $\delta(\psi)_\pm = (-3, -1)$. In both cases $\delta(\psi)_\pm \neq \gamma_\pm$, and thus there does not exist a ψ with image C_2 such that $\gamma \cdot \delta(\psi) = 1$.

CHAPTER 5

Varieties defined over k and k-varieties

As we said in Section 1.5 abelian $\mathbb{Q}$-varieties appear in a natural way in [**Py02**] when studying $\overline{\mathbb{Q}}$-simple factors of abelian varieties of GL_2-type over $\mathbb{Q}$. Recall that an abelian variety $A/\mathbb{Q}$ is said to be of GL_2-type if $\mathrm{End}^0_{\mathbb{Q}}(A)$ is a number field of degree equal to $\dim A$. If A does not have complex multiplication, then A decomposes up to $\overline{\mathbb{Q}}$-isogeny as the power of a building block. A building block is a $\mathbb{Q}$-variety $B/\overline{\mathbb{Q}}$ whose endomorphism algebra $\mathcal{B}$ is a central division algebra over a totally real number field F and $t[F:\mathbb{Q}] = \dim B$, where t is the Schur index of $\mathcal{B}$. Every building block is the absolutely simple factor up to isogeny of some abelian variety of GL_2-type over $\mathbb{Q}$. In this way, there is a correspondence between abelian varieties of GL_2-type over $\mathbb{Q}$ and building blocks.

The goal of this chapter is to generalize the above correspondence in two different directions. First of all, we want to consider not only abelian $\mathbb{Q}$-varieties, but also abelian k-varieties for any number field k. This would lead us to consider abelian varieties of GL_2-type over k. That is, abelian varieties A/k whose endomorphism algebra $\mathrm{End}^0_k(A)$ is a number field of degree equal to $\dim A$. But we also would like to drop the condition relating the dimension of the $\overline{k}$-simple factor and its endomorphism algebra that one has in the case of building blocks. In the case $k = \mathbb{Q}$, the main property of abelian varieties of GL_2-type that allows to prove the correspondence with building blocks is, in fact, that $\mathrm{End}^0_{\mathbb{Q}}(A)$ is a maximal subfield of $\mathrm{End}^0_{\overline{\mathbb{Q}}}(A)$. Moreover, this property implies that A itself is an abelian $\mathbb{Q}$-variety (a proof of this fact is given in Proposition 5.26). Therefore, we propose a generalization which consists on considering abelian k-varieties defined over k such that $\mathrm{End}^0_k(A)$ is a maximal subfield of $\mathrm{End}^0_{\overline{k}}(A)$. We call them *Ribet-Pyle varieties*, and we show that there is a correspondence between them and absolutely simple abelian k-varieties, in the same way as it happens with abelian varieties of GL_2-type over $\mathbb{Q}$ and building blocks.

In Section 5.1 we define Ribet-Pyle varieties, and establish the correspondence between them and abelian k-varieties when k is a number field: Ribet-Pyle varieties decompose up to $\overline{k}$-isogeny as a power of an abelian k-variety, and any abelian k-variety is the $\overline{k}$-simple factor of some Ribet-Pyle variety. In Section 5.2 we study the relation between the Ribet-Pyle varieties that have the same simple factor over $\overline{k}$. In Section 5.3 we deal with abelian varieties of GL_2-type over k, and we prove that they are indeed a particular

case of Ribet-Pyle varieties. Finally, in sections 5.4 and 5.5 we study the restriction of scalars of abelian k-varieties. More precisely, in Section 5.4 we compute their algebra of endomorphisms defined over k, and in Section 5.5 we characterize when these restrictions of scalars are isogenous to products of Ribet-Pyle varieties.

5.1. Ribet-Pyle varieties

We begin this section by defining the type of varieties that we will study in the rest of the chapter.

Definition 5.1. A *Ribet-Pyle variety* over a field k is an abelian k-variety A defined over k such that $\mathrm{End}_k^0(A)$ is a maximal subfield of $\mathrm{End}_{\overline{k}}^0(A)$.

One of the directions of the correspondence that we aim to establish is not hard to prove.

Proposition 5.2. *A Ribet-Pyle variety is isotypical over $\overline{k}$. That is, $A \sim_{\overline{k}} B^n$ for some absolutely simple abelian k-variety B.*

Proof. Since A is an abelian k-variety defined over k, by Proposition 3.15 we have that the center of $\mathrm{End}_{\overline{k}}^0(A)$ is contained in $\mathrm{End}_k^0(A)$. By hypothesis $\mathrm{End}_k^0(A)$ is a field, which implies that the center of $\mathrm{End}_{\overline{k}}^0(A)$ is a field as well. Thus $A_{\overline{k}}$ is isotypical, since otherwise the center of $\mathrm{End}_{\overline{k}}^0(A)$ would be a product of fields. Moreover the absolutely simple factor of A is a k-variety by Proposition 3.2. □

The goal of this section is to prove the other direction of the correspondence.

Theorem 5.3. *Let k be a number field, and let $B/\overline{k}$ be a simple abelian k-variety. Then there exists a Ribet-Pyle variety A/k such that $A \sim_{\overline{k}} B^n$ for some n.*

In the rest of this chapter, k will denote a number field and $B/\overline{k}$ will be a simple abelian k-variety. The endomorphism algebra $\mathrm{End}_{\overline{k}}^0(B)$ will be denoted by $\mathcal{B}$, and its center by F. We remark that we are not assuming B to be of the first kind, so F can be either a totally real field or a CM field, and the Schur index t of $\mathcal{B}$ can be greater that 2. We fix an algebraic closure $\overline{F}$ of F, and a system of compatible isogenies $\{\mu_\sigma \colon {}^\sigma B \to B\}_{\sigma \in G_k}$. We recall that c_B, the corresponding cocycle associated to the compatible system, is defined by $c_B(\sigma,\tau) = \mu_\sigma \circ {}^\sigma\mu_\tau \circ \mu_{\sigma\tau}^{-1}$ and it belongs to $Z^2(G_k, F^\times)$, where the action of G_k on $F^\times$ is trivial. As usual $[c_B]$ will denote its cohomology class in $H^2(G_k, F^\times)$.

Splitting maps. As in the work of Ribet and Pyle, the following theorem of Tate will play an important role in our proof of Theorem 5.3.

Theorem 5.4 (Tate)**.** *The group $H^2(G_k, \overline{F}^\times)$ is trivial when we consider the trivial action of G_k on $\overline{F}^\times$.*

PROOF. This theorem appears in [**Ri92**] as Theorem 6.3 in the particular case $k = \mathbb{Q}$, and it is a consequence of a theorem of Tate. The same argument works in general, and we reproduce it here.

Let $W \subseteq \overline{F}^\times$ be the group of roots of unity in $\overline{F}^\times$. The exact sequence

$$1 \longrightarrow W \longrightarrow \overline{F}^\times \longrightarrow \overline{F}^\times/W \longrightarrow 1$$

gives rise to a en exact sequence of cohomology groups

$$\cdots \to H^1(G_k, \overline{F}^\times/W) \to H^2(G_k, W) \to H^2(G_k, \overline{F}^\times) \to H^2(G_k, \overline{F}^\times/W)$$

The group $\overline{F}^\times/W$ is uniquely divisible (that is, for each integer n the map raising to the n-th power is a group isomorphism), and this implies that $H^i(G_k, \overline{F}^\times/W) = \{1\}$ for all i. Therefore the group $H^2(G_k, \overline{F}^\times)$ is isomorphic to $H^2(G_k, W)$. Since the action of G_k on W is trivial, $H^2(G_k, W)$ is isomorphic to $H^2(G_k, \mathbb{Q}/\mathbb{Z})$, and by a theorem of Tate (which is proved in [**Se77**, §6.5]) for any local or global field K the group $H^2(G_K, \mathbb{Q}/\mathbb{Z})$ is trivial. □

The inclusion of trivial G_k-modules $F^\times \hookrightarrow \overline{F}^\times$ induces a homomorphism

$$H^2(G_k, F^\times) \to H^2(G_k, \overline{F}^\times).$$

Theorem 5.4 implies that the image of $[c_B]$ in $H^2(G_k, \overline{F}^\times)$ is trivial. Thus there exist continuous maps $\beta\colon G_k \to \overline{F}^\times$ such that

$$c_B(\sigma, \tau) = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1}, \quad \text{for all } \sigma, \tau \in G_k. \tag{5.1}$$

Definition 5.5. A continuous map $\beta\colon G_k \to \overline{F}^\times$ satisfying (5.1) is called a *splitting map for* c_B.

Note that any map of the form $\beta' = \beta\chi$, with $\chi\colon G_k \to \overline{F}^\times$ a character, is another splitting map for c_B. In fact, as we vary χ through all the characters from G_k on $\overline{F}^\times$ we obtain all the splitting maps for c_B. Moreover if we multiply β by a continuous map $\lambda\colon G_k \to F^\times$ we obtain a splitting map for a cocycle cohomologous to c_B.

For a splitting map β, we will denote by E_β the field $F(\{\beta(\sigma)\}_{\sigma \in G_k})$, which is a subfield of $\overline{F}$. The extension E_β/F is finite, because of the continuity of β. In the proof of Theorem 5.3 we will need to choose β such that the field E_β contains an appropriate root of unity. Now we prove that, in fact, for any root of unity we can find a β such that E_β contains it.

Let m be the order of $[c_B]$ in $H^2(G_k, F^\times)$, and let d be a continuous map $d\colon G_k \to F^\times$ expressing c_B^m as a coboundary; that is, such that

$$c_B(\sigma, \tau)^m = d(\sigma)d(\tau)d(\sigma\tau)^{-1}. \tag{5.2}$$

We define a map

$$\begin{array}{rccc} \varepsilon_\beta\colon & G_k & \longrightarrow & \overline{F}^\times \\ & \sigma & \longmapsto & \beta(\sigma)^m/d(\sigma). \end{array}$$

By (5.1) and (5.2) we see that $\varepsilon_\beta\colon G_k \to \overline{F}^\times$ is a continuous character.

Lemma 5.6. *For each nonnegative integer n there exists a splitting map β such that $F(\zeta_n) \subseteq E_\beta$, where ζ_n is a primitive n-th root of unity in $\overline{F}$.*

PROOF. Let β' be a splitting map for c_B, and let r be the order of $\varepsilon_{\beta'}$. Let $e = \gcd(n, r)$ and let $\chi\colon G_k \to \overline{F}^\times$ be a character of order mn/e, where m is the order of $[c_B]$ in $H^2(G_k, F^\times)$. Then the character $\chi^m\varepsilon_{\beta'}$ is the character that corresponds to the splitting map $\beta = \chi\beta'$ and its order is nr/e, which is a multiple of n. Therefore E_β contains a primitive n-th root of unity ζ_n. □

Cyclic splitting fields of simple algebras. Let $\mathcal{A}$ be a central simple algebra over a field F. A field L containing F is called a *splitting field for* $\mathcal{A}$ if $\mathcal{A}\otimes_F L$ is isomorphic to a matrix algebra over F. An equivalent terminology is to say that $\mathcal{A}$ is split by L.

In order to prove Theorem 5.3 we will use the fact that any division algebra over F is split by a field of the form $F(\zeta_n)$. This result is already known, but we include a proof of it based on a standard theorem of class field theory, the Grunwald-Wang Theorem.

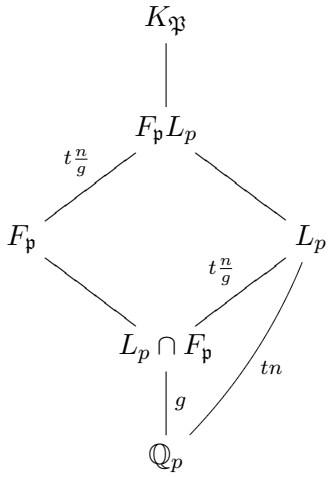
Theorem 5.7 (Grunwald-Wang Theorem)**.** *Let K be a number field, and let $\{(v_1, n_1), \ldots, (v_r, n_r)\}$ be a finite set of pairs, where each v_i is a place of K and each n_i is a positive integer such that $n_i \leqslant 2$ if v_i is a real place, and $n_i = 1$ if v_i is a complex place. Let m be the least common multiple of the n_i's. If m divides n, then there exists a cyclic extension L/K of degree n such that for each i the degree $[L_{v_i} : K_{v_i}]$ is divisible by n_i.*

Proposition 5.8. *Let F be a number field and let $\mathcal{D}$ be a central division algebra over F. There exists a cyclic extension $L/\mathbb{Q}$ such that LF is a splitting field for $\mathcal{D}$.*

PROOF. Let F' be the Galois closure of F. Let $n = [F' : \mathbb{Q}]$ and let t be the Schur index of $\mathcal{D}$. Let $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ be the set of primes of F where $\mathcal{D}$ ramifies, and let $\{p_1, \ldots, p_l\}$ be the set of primes of $\mathbb{Q}$ below $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$. The Grunwald-Wang Theorem, when applied to the primes p_i with $n_i = tn$, and to the infinite place of $\mathbb{Q}$ with $n_\infty = 2$, guarantees the existence of a cyclic extension $L/\mathbb{Q}$ of degree $2tn$ such that $[L_p : \mathbb{Q}_p] = tn$ for all p belonging to $\{p_1, \ldots, p_l\}$ and $L_v = \mathbb{C}$ for all archimedean place v of L. Let $K = LF$.

If $\mathfrak{p}$ is a prime of F dividing p, and $\mathfrak{P}$ is a prime of K dividing $\mathfrak{p}$, the fields L_p and $F_\mathfrak{p}$ can be seen as subfields of $K_\mathfrak{P}$. Then the degree $g = [L_p \cap F_\mathfrak{p} : \mathbb{Q}_p]$

divides n, and in the following diagram



we see that t divides $[K_{\mathfrak{P}} : F_{\mathfrak{p}}]$. Therefore K is a totally imaginary extension of F such that, for any prime $\mathfrak{p}$ of F ramifying in $\mathcal{D}$ and for any prime $\mathfrak{P}$ of K dividing $\mathfrak{p}$, the index $[K_{\mathfrak{P}} : F_{\mathfrak{p}}]$ is a multiple of the Schur index of $\mathcal{D}$. An important property of division algebras over number fields is that, when this happens, the field K is necessarily a splitting field for $\mathcal{D}$ (see [**Pi82**, Corollary 18.4 b and Corollary 17.10 a]). □

Corollary 5.9. *Every central division F-algebra is split by an extension of the form $F(\zeta_n)$.*

Proof. By the previous proposition there exists a cyclic extension $L/\mathbb{Q}$ such that LF splits $\mathcal{D}$. The field L is contained in a field of the form $\mathbb{Q}(\zeta_n)$ by the Kronecker-Weber Theorem, and then $F(\zeta_n)$ splits $\mathcal{D}$. □

Construction of Ribet-Pyle varieties. What we do now is to start with an absolutely simple abelian k-variety B and then to construct a Ribet-Pyle variety over k that has B as its simple factor up to $\overline{k}$-isogeny. Recall that $\mathcal{B}$ denotes $\mathrm{End}_k^0(B)$, F is the center of $\mathcal{B}$ and t denotes the Schur index of $\mathcal{B}$. Besides, c_B is the cocycle attached to a compatible system of isogenies $\{\mu_\sigma \colon {}^\sigma B \to B\}_{\sigma \in G_k}$ and β is a splitting map for c_B.

Let n be the degree $[E_\beta : F]$, which depends on β although we do not make it explicit in the notation. By fixing a F-basis of E_β we have an injective F-algebra homomorphism

$$\phi \colon E_\beta \longrightarrow \mathrm{M}_n(F) \subseteq \mathrm{M}_n(\mathcal{B}) \simeq \mathrm{End}_k^0(B^n).$$

The elements of E_β act as endomorphisms of B^n by means of ϕ. Let $\hat{\mu}_\sigma$ be the isogeny $\hat{\mu}_\sigma \colon {}^\sigma B^n \to B^n$ consisting in μ_σ in each factor.

Proposition 5.10. *Let $\phi \colon E_\beta \to \mathrm{M}_n(F)$ be a F-algebra homomorphism. There exists an abelian variety X_β over k and an isogeny $\kappa \colon B^n \to X_\beta$ over $\overline{k}$ such that $\kappa^{-1} \circ {}^\sigma\kappa = \phi(\beta(\sigma))^{-1} \circ \hat{\mu}_\sigma$ for all $\sigma \in G_k$. In addition, the k-isogeny class of X_β does not depend on ϕ.*

PROOF. Let ν_σ be the isomorphism of abelian varieties up to isogeny defined by $\nu_\sigma = \phi(\beta(\sigma))^{-1} \circ \hat{\mu}_\sigma$. In order to prove the existence of X_β, by Theorem 2.4 we need to check that $\nu_\sigma \circ {}^\sigma\nu_\tau \circ \nu_{\sigma\tau}^{-1} = 1$. Indeed,

$$\begin{aligned}
\nu_\sigma \circ {}^\sigma\nu_\tau \circ \nu_{\sigma\tau}^{-1} &= \phi(\beta(\sigma))^{-1} \circ \hat{\mu}_\sigma \circ {}^\sigma\phi(\beta(\tau))^{-1} \circ {}^\sigma\hat{\mu}_\tau \circ \hat{\mu}_{\sigma\tau}^{-1} \circ \phi(\beta(\sigma\tau)) \\
&= \phi(\beta(\sigma))^{-1} \circ \phi(\beta(\tau))^{-1} \circ \hat{\mu}_\sigma \circ {}^\sigma\hat{\mu}_\tau \circ \hat{\mu}_{\sigma\tau}^{-1} \circ \phi(\beta(\sigma\tau)) \\
&= \phi(\beta(\sigma))^{-1} \circ \phi(\beta(\tau))^{-1} \circ c_B(\sigma,\tau) \circ \phi(\beta(\sigma\tau)) \\
&= \phi(\beta(\sigma)^{-1} \circ \beta(\tau)^{-1} \circ \beta(\sigma\tau)) \circ c_B(\sigma,\tau) \\
&= \phi(c_B(\sigma,\tau)^{-1}) \circ c_B(\sigma,\tau) = c_B(\sigma,\tau)^{-1} \circ c_B(\sigma,\tau) = 1.
\end{aligned}$$

Now suppose that ϕ and ψ are F-algebra homomorphisms $E_\beta \to \mathrm{M}_n(F)$, and let $X_{\beta,\phi}$ and $X_{\beta,\psi}$ denote the varieties constructed by the above procedure using ϕ and ψ respectively to define the action of E_β on B^n. We aim to see that $X_{\beta,\phi}$ and $X_{\beta,\psi}$ are k-isogenous.

Let C denote the image of ϕ. The map $\phi(x) \mapsto \psi(x) \colon C \to \mathrm{M}_n(F)$ is a F-algebra homomorphism. Since C is simple and $\mathrm{M}_n(F)$ is central simple over F, by the Skolem-Noether Theorem there exists an element b belonging to $\mathrm{M}_n(F)^\times$ such that $\phi(x) = b\psi(x)b^{-1}$ for all x in E_β. By the defining property of $X_{\beta,\phi}$ and $X_{\beta,\psi}$ there are isogenies $\kappa \colon B^n \longrightarrow X_{\beta,\phi}$ and $\lambda \colon B^n \longrightarrow X_{\beta,\psi}$ such that

$$\kappa^{-1} \circ {}^\sigma\kappa = \phi(\beta(\sigma))^{-1} \circ \hat{\mu}_\sigma = b \circ \psi(\beta(\sigma))^{-1} \circ b^{-1} \circ \hat{\mu}_\sigma, \tag{5.3}$$

$$\lambda^{-1} \circ {}^\sigma\lambda = \psi(\beta(\sigma))^{-1} \circ \hat{\mu}_\sigma. \tag{5.4}$$

The isogeny $\nu = \kappa \circ b \circ \lambda^{-1} \colon X_{\beta,\psi} \longrightarrow X_{\beta,\phi}$ is defined over k, since for each σ of G_k we have that

$$\begin{aligned}
\nu^{-1} \circ {}^\sigma\nu &= \lambda \circ b^{-1} \circ \kappa^{-1} \circ {}^\sigma\kappa \circ {}^\sigma b \circ {}^\sigma\lambda^{-1} \\
&= \lambda \circ b^{-1} \circ b \circ \psi(\beta(\sigma))^{-1} \circ b^{-1} \circ \hat{\mu}_\sigma \circ {}^\sigma b \circ {}^\sigma\lambda^{-1} \\
&= \lambda \circ \psi(\beta(\sigma))^{-1} \circ \hat{\mu}_\sigma \circ {}^\sigma b^{-1} \circ {}^\sigma b \circ {}^\sigma\lambda^{-1} \\
&= \lambda \circ \lambda^{-1} \circ {}^\sigma\lambda \circ {}^\sigma\lambda^{-1} = 1,
\end{aligned}$$

where we used the compatibility of $\hat{\mu}_\sigma$ with the endomorphisms of B^n in the third equality, and the expressions (5.3) and (5.4) in the second and fourth equality respectively. □

We fix a F-algebra homomorphism $\phi \colon E_\beta \to \mathrm{M}_n(F)$, and we make E_β act on B^n by means of ϕ. If β is a splitting map for c_B, then X_β will denote a variety over k such that there exists a $\overline{k}$-isogeny $\kappa \colon B^n \to X_\beta$ with the property that $\kappa^{-1} \circ {}^\sigma\kappa = \beta(\sigma)^{-1} \circ \hat{\mu}_\sigma$ for all σ in G_k. This variety is unique up to k-isogeny. Observe that, although we have had to make a choice in the homomorphism ϕ, the k-isogeny class of the variety X_β does not depend on this choice. Since $X_\beta \sim_{\overline{k}} B^n$ we have an isomorphism $\mathrm{End}_k^0(X_\beta) \simeq \mathrm{M}_n(\mathcal{B})$. In the following proposition we compute the algebra of endomorphisms of X_β defined over k.

Proposition 5.11. *The algebra* $\mathrm{End}_k^0(X_\beta)$ *is isomorphic to the centralizer of* E_β *in* $\mathrm{M}_n(\mathcal{B})$.

PROOF. As we said, $\mathrm{End}_k^0(X_\beta)$ is isomorphic to $\mathrm{M}_n(\mathcal{B})$ and the isomorphism is given by the isogeny $\kappa\colon B^n \to X_\beta$; that is, any endomorphism of X_β up to $\overline{k}$-isogeny is of the form $\kappa\circ\psi\circ\kappa^{-1}$, for some $\psi \in \mathrm{End}_{\overline{k}}^0(B^n)$. For σ in G_k we have the following:

$$\begin{aligned} {}^\sigma(\kappa\circ\psi\circ\kappa^{-1}) = \kappa\circ\psi\circ\kappa^{-1} \quad &\iff \quad {}^\sigma\kappa\circ{}^\sigma\psi\circ{}^\sigma\kappa^{-1} = \kappa\circ\psi\circ\kappa^{-1} \\ &\iff \quad \kappa^{-1}\circ{}^\sigma\kappa\circ{}^\sigma\psi\circ\kappa\circ({}^{\kappa^{-1}}\circ{}^\sigma\kappa)^{-1} = \psi \\ &\iff \quad \beta(\sigma)\circ\hat{\mu}_\sigma\circ{}^\sigma\psi\circ\hat{\mu}_\sigma^{-1}\circ\beta(\sigma)^{-1} = \psi \\ &\iff \quad \beta(\sigma)\circ\psi = \psi\circ\beta(\sigma). \end{aligned}$$

This means that the endomorphisms of X_β defined over k are exactly the ones coming from endomorphisms ψ that commute with $\beta(\sigma)$, for all σ in G_k. Now the proposition is clear, since the $\beta(\sigma)$'s generate E_β. □

Corollary 5.12. *The algebra* $\mathrm{End}_k^0(X_\beta)$ *is isomorphic to* $E_\beta \otimes_F \mathcal{B}$.

PROOF. This is a well known property of central simple algebras that follows from the Double Centralizer Theorem; for convenience of the reader we include a proof here. Let C be the centralizer of E_β in $\mathrm{M}_n(\mathcal{B})$. In view of Proposition 5.11 we have to prove that $C \simeq E_\beta \otimes_F \mathcal{B}$. It is clear that E_β is contained in C. Moreover, $\mathcal{B}$ is contained in C because the elements of E_β can be seen as $n\times n$ matrices with entries in F, and these matrices commute with $\mathcal{B}$ (which is identified with the diagonal matrices in $\mathrm{M}_n(\mathcal{B})$). Since E_β and $\mathcal{B}$ commute, there exists a subalgebra of C isomorphic to $E_\beta \otimes_F \mathcal{B}$, which has dimension nt^2 over F. By the Double Centralizer Theorem we know that

$$[C : F][E_\beta : F] = [\mathrm{M}_n(\mathcal{B}) : F] = n^2t^2,$$

and from this we obtain that $[C : F] = nt^2$, hence C is isomorphic to $E_\beta \otimes_F \mathcal{B}$. □

At this point we have at our disposal all the tools needed to prove Theorem 5.3.

PROOF OF THEOREM 5.3. By Corollary 5.9 there exists an integer m such that $F(\zeta_m)$ splits $\mathcal{B}$. Let β be a splitting map for c_B with E_β containing $F(\zeta_m)$; the existence of such a β is guaranteed by Lemma 5.6. Consider the variety X_β. By Corollary 5.12 we have that $\mathrm{End}_k^0(X_\beta) \simeq E_\beta \otimes_F \mathcal{B}$, and this later algebra is in turn isomorphic to $M_t(E_\beta)$ because E_β is a splitting field for $\mathcal{B}$. Therefore there exists an abelian variety A_β defined over k such that $X_\beta \sim_k A_\beta^t$ and $\mathrm{End}_k^0(A_\beta) \simeq E_\beta$. Clearly A_β is $\overline{k}$-isomorphic to $B^{n/t}$, where $n = [E_\beta : F]$, and we claim that it is in fact a Ribet-Pyle variety. This follows by a dimension argument: the dimension of the subfield is $\dim_F \mathrm{End}_k^0(A_\beta) = \dim_F(E_\beta) = n$, while the dimension of the ambient

algebra is $\dim_F \mathrm{End}_k^0(A_\beta) = (\frac{n}{t})^2 \dim_F(\mathcal{B}) = n^2$. Hence, by Proposition 1.8 we see that $\mathrm{End}_k^0(A)$ is a maximal subfield of $\mathrm{End}_{\overline{k}}^0(A)$. □

Given an abelian k-variety B there do exist in general infinitely many Ribet-Pyle varieties with $\overline{k}$-simple factor isogenous to B. What is more, they can have arbitrarily large dimension. We have seen in this section how to produce, for each splitting map β for c_B, a Ribet-Pyle variety with this property. In the following proposition we see that, in fact, when we vary β among all possible splitting maps for c_B we obtain by the construction above all Ribet-Pyle varieties whose simple factor is B.

Proposition 5.13. *Any Ribet-Pyle variety with simple factor B is isogenous over k to the variety A_β obtained applying the above procedure to some splitting map β for c_B.*

Proof. Let A/k be a Ribet-Pyle variety and let κ be a $\overline{k}$-isogeny $B^n \to A$. Let E be the maximal subfield $\mathrm{End}_k^0(A)$ of $\mathrm{End}_{\overline{k}}^0(A)$, and fix an embedding of E in $\overline{F}$. We have the relation $[E : F] = nt$, where t is the Schur index of $\mathcal{B} = \mathrm{End}_{\overline{k}}^0(B)$. We also choose a system of compatible isogenies $\{\mu_\sigma \colon {}^\sigma B \to B\}_{\sigma \in G_k}$, and we denote by $\hat{\mu}_\sigma$ the diagonal isogeny ${}^\sigma B^n \to B^n$ given by μ_σ. We define $\beta(\sigma) = \kappa \circ \hat{\mu}_\sigma \circ {}^\sigma\kappa^{-1}$, which is a compatible isogeny $A_{\overline{k}} \to A_{\overline{k}}$. The fact that $\beta(\sigma)$ is compatible implies that $\beta(\sigma) \circ \varphi = {}^\sigma\varphi \circ \beta(\sigma)$ for all σ in G_k and $\varphi \in \mathrm{End}_{\overline{k}}^0(A)$. In particular, when applied to elements φ of E, this property says that $\beta(\sigma)$ lies in the centralizer of E, which is E itself by the maximality of E, and since $c_B(\sigma, \tau) = \beta(\sigma) \circ \beta(\tau) \circ \beta(\sigma\tau)^{-1}$ the map $\sigma \mapsto \beta(\sigma)$ is a splitting map for c_B. We have already seen the inclusion $E_\beta \subseteq E$; moreover, it is clear that $C(E_\beta) \subseteq E$, and taking centralizers and applying the Double Centralizer Theorem we have that $E = C(E) \subseteq C(C(E_\beta)) = E_\beta$. Hence $E = E_\beta$ and so $[E_\beta : F] = nt$.

Now we define a $\overline{k}$-isogeny $\hat{\kappa} \colon (B^n)^t \to A^t$ as the diagonal isogeny associated to κ, and we make E_β act on B^{nt} by means of $\hat{\kappa}$. It is easy to check that $\hat{\kappa}^{-1} \circ {}^\sigma\hat{\kappa} = \hat{\kappa}^{-1} \circ \beta(\sigma)^{-1} \circ \hat{\kappa} \circ \hat{\mu}_\sigma$, so A^t satisfies the property defining X_β. By the uniqueness of X_β we have that $A^t \sim_k X_\beta$, and so $A_\beta \sim_k A$. □

Remark 5.14. During the proof of Theorem 5.3, the fact that k is a number field is only used in Tate's theorem in order to guarantee the existence of splitting maps for c_B. In consequence, Theorem 5.3 is valid for all fields k such that $H^2(G_k, \overline{F}^\times; 1)$ is trivial. In particular, it is valid for all local or global fields, as we have already commented in the proof of Theorem 5.4.

Remark 5.15. For any splitting map β for c_B we have constructed an abelian variety X_β with $\mathrm{End}_k^0(X_\beta) \simeq E_\beta \otimes_F \mathcal{B}$. The key step in proving the existence of a Ribet-Pyle variety with B as its $\overline{k}$-simple factor, is to show that there exist splitting maps β such that the field E_β splits $\mathcal{B}$. Under certain conditions on B and k, all splitting maps β produce a field E_β that splits $\mathcal{B}$. For instance, we have the following result.

Proposition 5.16. *Let $d = 2\dim B/t[F : \mathbb{Q}]$. If t is square-free and $\gcd(t, d[k : \mathbb{Q}]/2) = 1$, then for any splitting map β for c_B the field E_β splits $\mathcal{B}$.*

Proof. Let t_0 be the Schur index of $E_\beta \otimes_F \mathcal{B}$, which is a divisor of t. We know that $\mathrm{End}_k^0(X_\beta) \simeq E_\beta \otimes_F \mathcal{B}$, so $E_\beta \otimes_F \mathcal{B}$ acts on the k-vector space $\mathrm{Lie}(A/k)$. This means that there exists a division algebra of dimension t_0^2 over E_β acting on a vector space of k-dimension equal to $\dim X_\beta = [E_\beta : F]\dim B$. This implies that

$$t_0^2[E_\beta : F][F : \mathbb{Q}] \mid [E_\beta : F]\dim B[k : \mathbb{Q}] = [E_\beta : F]\frac{td}{2}[F : \mathbb{Q}][k : \mathbb{Q}].$$

We see that t_0^2 divides $td[k : \mathbb{Q}]/2$, and if t is square-free then t_0 divides $d[k : \mathbb{Q}]/2$, which forces t_0 to be 1 and E_β splits $\mathcal{B}$. □

Remark 5.17. When $k = \mathbb{Q}$ and B is a building block we are in the situation of Proposition 5.16, since then $d[k : \mathbb{Q}]/2$ is equal to 1, and t is either 1 or 2, hence square-free. This is why in Ribet and Pyle's construction of abelian varieties of GL_2-type associated to a building block, it is not necessary to prove the existence of splitting fields for c_B that are also splitting fields for the algebra $\mathcal{B}$, since all of them are. However, in their proof they did not use an argument similar to the one in Proposition 5.16. They used instead the fact that the image of the cohomology class $[c_B]$ in $H^2(G_F, \overline{F}^\times)$ (where now the action of G_F on $\overline{F}^\times$ is the Galois action) gives the Brauer class of $\mathcal{B}$, under the isomorphism $H^2(G_F, \overline{F}^\times) \simeq \mathrm{Br}(F)$. In the more general situation of abelian k-varieties we do not have this information about the Brauer class of $\mathcal{B}$.

5.2. Ribet-Pyle varieties coming from the same k-variety

In this section we study the relation between Ribet-Pyle varieties that have the same simple factor up to $\overline{k}$-isogeny. As we have seen, any two such varieties are of the form A_β and $A_{\beta'}$, for some splitting maps β and β' for c_B such that E_β and $E_{\beta'}$ split $\mathcal{B}$. The main result of this section is Proposition 5.23, which is an expression relating the ℓ-adic representations of A_β and $A_{\beta'}$ involving the splitting maps β and β'. To be more precise, the traces of the two ℓ-adic representations differ by the character $\chi = \beta/\beta'$. We begin by giving some elementary properties of ℓ-adic representations of twits and isotypical varieties that we will need later.

Isotypical varieties, twists and their ℓ-adic representations. Let A/k be an abelian variety and let E be a number field acting on A over k. More precisely, we suppose given an injection $\iota\colon E \hookrightarrow \mathrm{End}_k^0(A)$ so that the elements of E act on A as endomorphisms over k by means of ι; we consider ι fixed once and for all, so we do not make it explicit in the notation. Let ℓ be a prime number and denote $V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, where $T_\ell(A) = \varprojlim A[\ell^n]$

is the ℓ-adic Tate module of A. The rank of V_ℓ as $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-module is $d = 2 \dim A/[E : \mathbb{Q}]$, and the action of G_k on T_ℓ gives the ℓ-adic representation

$$\rho_A^E \colon G_k \longrightarrow \mathrm{Aut}_{E\otimes\mathbb{Q}_\ell}(V_\ell A) \simeq \mathrm{GL}_d(E \otimes \mathbb{Q}_\ell),$$

where the isomorphism between $\mathrm{Aut}_{E\otimes\mathbb{Q}_\ell}(V_\ell A)$ and $\mathrm{GL}_d(E\otimes\mathbb{Q}_\ell)$ is given by fixing a basis of $V_\ell A$ as $E\otimes\mathbb{Q}_\ell$-module. If $(a_n)_{n\geqslant 1}$ is a sequence representing an element in $T_\ell A$ and σ is an element in G_k, then $\rho_A^E(\sigma)((a_n)) = ({}^\sigma a_n)$.

Now we describe the relation between certain ℓ-adic representation of A and certain ℓ-adic representation of A^r. Let L/E be a field extension of degree r. By fixing an E-algebra embedding $L \hookrightarrow \mathrm{M}_r(E)$ the field L acts on A^r. Then $V_\ell(A^r)$ is a $L \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-module of rank d, so we can consider the ℓ-adic representation

$$\rho_{A^r}^L : G_k \longrightarrow \mathrm{Aut}_{L\otimes\mathbb{Q}_\ell}(V_\ell(A^r)) \simeq \mathrm{GL}_d(L \otimes \mathbb{Q}_\ell).$$

Lemma 5.18. *If ℓ is a prime number that splits completely in L, then there exist $L \otimes \mathbb{Q}_\ell$-basis of $V_\ell(A^r)$ such that $\rho_{A^r}^L$ takes values in $\mathrm{GL}_d(E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)$; moreover, $\rho_{A^r}^L$ is isomorphic to the extension of scalars of ρ_A^E to $L \otimes \mathbb{Q}_\ell$.*

Proof. Let $\{P_1, P_2, \ldots, P_r\}$ be a basis of $V_\ell A$ as $E\otimes\mathbb{Q}_\ell$-module, and for each i let $\mathbf{P}_i = (P_i, \ldots, P_i)$ be the element of $V_\ell(A^r) \simeq (V_\ell A)^r$ obtained by repeating r times P_i. Since ℓ splits completely in E we have that $E \otimes \mathbb{Q}_\ell \simeq \mathbb{Q}_\ell^n$, and therefore

$$\mathbb{Q}_\ell^n \cdot P_1 + \mathbb{Q}_\ell^n \cdot P_2 + \cdots + \mathbb{Q}_\ell^n \cdot P_r = V_\ell(A).$$

Hence we see that

$$(\mathbb{Q}_\ell^n)^r \cdot \mathbf{P}_1 + (\mathbb{Q}_\ell^n)^r \cdot \mathbf{P}_2 + \cdots + (\mathbb{Q}_\ell^n)^r \cdot \mathbf{P}_r = (V_\ell(A))^r.$$

This implies that $\{\mathbf{P}_1, \mathbf{P}_2, \ldots, \mathbf{P}_r\}$ is a $L \otimes \mathbb{Q}_\ell$-basis of $V_\ell(A^r)$, because $(\mathbb{Q}_\ell^n)^r \simeq L \otimes \mathbb{Q}_\ell$. Now for $\sigma \in G_k$ let $(s_j^i) \in \mathrm{GL}_d(E \otimes \mathbb{Q}_\ell)$ be the matrix $\rho_A^E(\sigma)$. By definition this means that ${}^\sigma P_i = \sum s_j^i P_j$, so we also have

$${}^\sigma \mathbf{P}_i = (\sum s_j^i P_j, \sum s_j^i P_j, \ldots, \sum s_j^i P_j) = \sum s_j^i \mathbf{P}_i,$$

since an element of $E \otimes \mathbb{Q}_\ell$ acts on $(V_\ell A)^r$ by acting on each factor $V_\ell(A)$. This means that the matrix of $\rho_{A^r}^L$ in the basis $\{\mathbf{P}_1, \mathbf{P}_2, \ldots, \mathbf{P}_r\}$ is (s_j^i), which is the image in $\mathrm{GL}_2(L \otimes \mathbb{Q}_\ell)$ of the matrix $\rho_A^E(\sigma)$, and this proves the lemma. □

Now we study the effect on the ℓ-adic representation of twisting A by a character. The group G_k acts on $\mathrm{End}_{\overline{k}}^0(A)$, and so it does on E since we view E as a subfield of $\mathrm{End}_{\overline{k}}^0(A)$. Actually, E is a subfield of $\mathrm{End}_k^0(A)$, so G_k acts trivially on E. For this reason, a character $\chi \colon G_k \to E^\times$ can be regarded as an element belonging to $H^1(G_k, \mathrm{End}_{\overline{k}}^0(A))$. Consider the variety A^χ, the twist of A by the cocycle χ. This is a variety defined over k together with a $\overline{k}$-isogeny $\kappa \colon A \to A^\chi$ such that $\kappa^{-1} \circ {}^\sigma\kappa = \chi(\sigma)$ for all $\sigma \in G_k$. Then

we can make E act on A^χ by means of κ: if φ belongs to E, then $\kappa\circ\varphi\circ\kappa^{-1}$ belongs to $\mathrm{End}_k^0(A^\chi)$. Moreover, for each $\sigma\in G_k$ we have that

$$\begin{aligned}{}^\sigma(\kappa\circ\varphi\circ\kappa^{-1}) &= {}^\sigma\kappa\circ{}^\sigma\varphi\circ{}^\sigma\kappa^{-1} = {}^\sigma\kappa\circ\varphi\circ{}^\sigma\kappa^{-1} = \\ &= \kappa\circ\chi(\sigma)\circ\varphi\circ\chi(\sigma)^{-1}\circ\kappa^{-1} = \kappa\circ\varphi\circ\kappa^{-1},\end{aligned}$$

so E can also be seen as a subfield of $\mathrm{End}_k^0(A^\chi)$. Hence, we can consider the ℓ-adic representations attached to A and A^χ respectively:

$$\rho_A^E\colon G_k\longrightarrow \mathrm{Aut}_{E\otimes\mathbb{Q}_\ell}(V_\ell A),$$

$$\rho_{A^\chi}^E\colon G_k\longrightarrow \mathrm{Aut}_{E\otimes\mathbb{Q}_\ell}(V_\ell A^\chi).$$

Lemma 5.19. *The representation $\rho_{A^\chi}^E$ is isomorphic to $\chi\otimes\rho_A^E$.*

Proof. The isogeny $\kappa\colon A\to A^\chi$ gives the following map between the Tate modules, that we also call κ:

$$\begin{array}{rccc}\kappa\colon & V_\ell(A) & \longrightarrow & V_\ell(A^\chi)\\ & (\dots,P_n,\dots) & \longmapsto & (\dots,\kappa(P_n),\dots).\end{array}$$

Being clear that κ is an isomorphism of $\mathbb{Q}_\ell$-modules, we note that it is also a morphism of E-modules: if φ belongs to E and P_n belongs to $A[\ell^n]$, we have to check that $\kappa(\varphi\cdot P_n)=\varphi\cdot\kappa(P_n)$. But φ acts on $A^\chi[\ell^n]$ as $\kappa\circ\varphi\circ\kappa^{-1}$, and therefore

$$\varphi\cdot\kappa(P_n)=\kappa\circ\varphi\circ\kappa^{-1}(\kappa(P_n))=\kappa(\varphi(P_n))=\kappa(\varphi\cdot P_n).$$

Now, for $\sigma\in G_k$ the representations are as follows: $\rho_A^E(\sigma)\colon P_n\mapsto{}^\sigma P_n$ and $\rho_{A^\chi}^E(\sigma)\colon Q_n\mapsto{}^\sigma Q_n$. We have that $\rho_{A^\chi}^E(\sigma)\circ\kappa=\kappa\circ\chi(\sigma)\rho_A^E(\sigma)$, because

$$(\rho_{A^\chi}^E(\sigma)\circ\kappa)(P_n)={}^\sigma(\kappa(P_n)),$$

$$(\kappa\circ\chi(\sigma)\rho_A^E(\sigma))(P_n)=\kappa(\kappa^{-1}\circ{}^\sigma\kappa({}^\sigma P_n))={}^\sigma\kappa({}^\sigma P_n)={}^\sigma(\kappa(P_n)).$$

This, together with the fact that κ is an isomorphism of $E\otimes\mathbb{Q}_\ell$-modules implies that it is an isomorphism between the representations $\rho_{A^\chi}^E$ and $\chi\otimes\rho_A^E$. □

Varieties attached to splitting maps: a generalization. Let β be a splitting map for c_B, and let $E_\beta\subseteq\overline{F}$ be the extension of degree n over F obtained adjoining to F the values of β. Let $L\subseteq\overline{F}$ be an extension of E_β of degree r, and fix an F-algebra embedding $\phi\colon L\hookrightarrow \mathrm{M}_m(F)$, where $m=nr$. Denote by $\hat\mu_\sigma$ the diagonal isogeny ${}^\sigma B^m\to B^m$ given by μ_σ, and define $\nu_\sigma=\phi(\beta(\sigma))^{-1}\circ\hat\mu_\sigma$. Using the same argument as in the proof of Proposition 5.10 one can prove the following statement.

Proposition 5.20. *There exists an abelian variety X_β^L over k and an isogeny $\kappa\colon B^m\to X_\beta^L$ over $\overline{k}$ such that $\kappa^{-1}\circ{}^\sigma\kappa=\phi(\beta(\sigma))^{-1}\circ\hat\mu_\sigma$ for all $\sigma\in G_k$. In addition, the k-isogeny class of X_β^L does not depend on ϕ.*

Obviously, if we take $L = E_\beta$ then X_β^L coincides with the variety X_β defined in Proposition 5.10. In general, the relation between X_β and X_β^L is also very simple, as we see in the next lemma.

Lemma 5.21. *Let L/E_β be an extension of degree r. Then X_β^L and $(X_\beta)^r$ are k-isogenous.*

PROOF. To define the action of L on B^m, where $m = [L : F]$, we take a F-algebra morphism $\phi : L \to \mathrm{M}_m(F)$ compatible with the tower of extensions $L/E_\beta/F$. That is, we construct it as the composition of two morphisms $L \to M_n(E_\beta) \to \mathrm{M}_n(M_r(F))$, where the first morphism is the one obtained by fixing an E_β-basis of L, and the second one is obtained by fixing a F-basis of E_β. Using this ϕ, and since β takes values in $E_\beta \subseteq L$, we see that the elements $\beta(\sigma)$ act on $B^m = (B^n)^r$ independently on each of the r factors of the form B^n. With this action, the variety $(X_\beta)^r$ clearly satisfies the condition that defines X_β^L, and therefore $X_\beta^L \sim_k (X_\beta)^r$. □

Now let β and β' be two splitting maps for c_B, and take $L = E_\beta E_{\beta'}$. These splitting maps take values in L, so we can consider the varieties X_β^L and $X_{\beta'}^L$, that are both $\overline{k}$-isogenous to B^m. Recall that there exist $\overline{k}$-isogenies $\kappa\colon B^m \to X_\beta^L$ and $\lambda\colon B^m \to X_{\beta'}^L$ such that $\kappa^{-1}\circ{}^\sigma\kappa = \beta(\sigma)^{-1}\circ\hat{\mu}_\sigma$ and $\lambda^{-1}\circ{}^\sigma\lambda = \beta'(\sigma)^{-1}\circ\hat{\mu}_\sigma$ respectively. Using these isogenies we can translate the action of L on B^m into an action of L on X_β^L and $X_{\beta'}^L$. In fact, we obtain inclusions $L \hookrightarrow \mathrm{End}_k^0(X_\beta^L)$ and $L \hookrightarrow \mathrm{End}_k^0(X_{\beta'}^L)$. Hence, the character $\chi = \beta/\beta' \colon G_k \to L^\times$ can be identified with an element of $H^1(G_k, \mathrm{End}_{\overline{k}}^0(X_\beta^L))$, and it makes sense to consider the variety $(X_\beta^L)^\chi$, the twist of X_β^L by χ.

Proposition 5.22. *The varieties $X_{\beta'}^L$ and $(X_\beta^L)^\chi$ are k-isogenous.*

PROOF. The variety $X_{\beta'}^L$ is defined over k, and the isogeny

$$\nu = \lambda\circ\kappa^{-1}\colon X_\beta^L \longrightarrow X_{\beta'}^L$$

satisfies that, for $\sigma \in G_k$:

$$\begin{aligned}\nu^{-1}\circ{}^\sigma\nu &= \kappa\circ\lambda^{-1}\circ{}^\sigma\lambda\circ{}^\sigma\kappa^{-1} = \kappa\circ\beta'(\sigma)^{-1}\circ\hat{\mu}_\sigma\circ{}^\sigma\kappa^{-1} = \\ &= \kappa\circ\beta'(\sigma)^{-1}\circ\hat{\mu}_\sigma\circ\hat{\mu}_\sigma^{-1}\circ\beta(\sigma)\circ\kappa^{-1} = \kappa\circ\chi(\sigma)\circ\kappa^{-1}.\end{aligned}$$

The variety $(X_\beta)^\chi$ is the unique (up to k-isogeny) abelian variety satisfying these properties, and hence $X_{\beta'}^L$ and $(X_\beta^L)^\chi$ are k-isogenous. □

Given β and β' two splitting maps for c_B, we can also consider the varieties A_β and $A_{\beta'}$ and their ℓ-adic representations. To simplify the notation, we will call ρ_β and $\rho_{\beta'}$ the ℓ-adic representations of G_k associated to A_β and $A_{\beta'}$ that take values in $\mathrm{GL}_2(E_\beta \otimes \mathbb{Q}_\ell)$ and $\mathrm{GL}_2(E_{\beta'} \otimes \mathbb{Q}_\ell)$ respectively.

Proposition 5.23. *The traces of the ℓ-adic representations ρ_β and $\rho_{\beta'}$ are related by*

$$\mathrm{tr}(\rho_\beta) = \chi \cdot \mathrm{tr}(\rho_{\beta'}),$$

where χ is the character β/β'.

PROOF. Let $L = E_\beta E_{\beta'}$, $r = [L : E_\beta]$ and $r' = [L : E_{\beta'}]$. Since the traces of the ℓ-adic representations are independent of ℓ, we can suppose that ℓ splits completely in L. Consider the varieties X_β^L and $X_{\beta'}^L$. By Proposition 5.22 we have that $X_{\beta'}^L$ and $(X_\beta^L)^\chi$ are k-isogenous, and by Lemma 5.19 we find that $\rho^L_{X^L_{\beta'}} \simeq \chi \otimes \rho^L_{X^L_\beta}$. But by Lemma 5.18 this implies that $\rho^{E_{\beta'}}_{X_{\beta'}} \otimes L \simeq \chi \otimes (\rho^{E_\beta}_{X_\beta} \otimes L)$, and taking traces this gives:

$$\mathrm{tr}(\rho^{E_{\beta'}}_{X_{\beta'}}) = \chi \cdot \mathrm{tr}(\rho^{E_\beta}_{X_\beta}). \tag{5.5}$$

Since $X_\beta \sim (A_\beta)^t$ and $X_{\beta'} \sim (A_{\beta'})^t$ we have that $\mathrm{tr}(\rho^{E_\beta}_{X_\beta}) = t \cdot \mathrm{tr}(\rho^{E_\beta}_{A_\beta})$ and $\mathrm{tr}(\rho^{E_{\beta'}}_{X_{\beta'}}) = t \cdot \mathrm{tr}(\rho^{E_{\beta'}}_{A_{\beta'}})$. When we substitute this in (5.5) we obtain the relation in the statement of the proposition. □

5.3. Abelian varieties of GL_2-type over k

As we said in the introduction of this chapter, one of the goals of introducing Ribet-Pyle varieties is to establish a correspondence between abelian varieties of GL_2-type over k and a particular type of k-varieties. Up to now, this correspondence had only been studied for the case $k = \mathbb{Q}$ in the articles by Ribet and Pyle. In this section we show that abelian varieties of GL_2-type over k without CM are Ribet-Pyle varieties, and then we use Theorem 5.3 to prove the correspondence in this case.

Definition 5.24. An abelian variety of GL_2-type over k is an abelian variety A/k such that $\mathrm{End}^0_k(A)$ is a number field of degree over $\mathbb{Q}$ equal to the dimension of A.

By [**Sh72**, Proposition 1.5] if an abelian variety of GL_2-type over k has some absolutely simple factor with CM, then A itself has CM over $\overline{k}$. Since arithmetic properties of abelian varieties with CM are well studied, and this case requires completely different methods from the ones we are using here, we will suppose from now on that all abelian varieties of GL_2-type over k do not have (any absolutely simple factor with) CM.

Lemma 5.25. *Let A be an abelian variety of GL_2-type over k and let K/k be a Galois extension. Then A decomposes as $A \sim_K B^n$ where B/K is a K-simple abelian variety. If we let $\mathcal{B} = \mathrm{End}^0_K(B)$, $F = Z(\mathcal{B})$ and t the Schur index of $\mathcal{B}$, then $E = \mathrm{End}^0_k(A)$ is a maximal subfield of $\mathrm{End}^0_K(A)$ and $t[F : \mathbb{Q}] = \dim B$.*

PROOF. First we prove that $A \sim_K B^n$ for some K-simple abelian variety B/K. A priori we know that $A \sim_K B_1^{n_1} \times \cdots \times B_r^{n_r}$. Since $E = \mathrm{End}^0_k(A)$ is a field, it acts on each $B_i^{n_i}$. Hence, it acts on $H_1((B_i^{n_i})_{\mathbb{C}}, \mathbb{Q})$, which is a $\mathbb{Q}$-vector space of dimension $2n_i \dim B_i$. This implies that $[E : \mathbb{Q}]$ divides

$2n_i \dim B_i$. On the other hand, $[E : \mathbb{Q}] = \dim A = \sum n_i \dim B_i$, thus $[E : \mathbb{Q}] \geqslant n_i \dim B_i$. This means that, either $[E : \mathbb{Q}] = n_i \dim B_i$ or $[E : \mathbb{Q}] = 2n_i \dim B_i$. But the second option is impossible, since we are assuming that A has no simple factor with CM. Therefore $[E : \mathbb{Q}] = n_i \dim B_i$ and in the K-decomposition of A only appears one simple factor.

Next, we prove that E is a maximal subfield of $\mathrm{End}_K^0(A)$. Since A is isotypical, $\mathrm{End}_K^0(A)$ is a simple algebra, so it is enough to see that $C(E)$, the centralizer of E in $\mathrm{End}_K^0(A)$, is a field. Let φ be an element belonging to $C(E)$. A priori $\varphi(A) \sim_K B^r$ for some $r \leqslant n$, but since E acts on $\varphi(A)$ we have that $[E : \mathbb{Q}] \mid 2r \dim B$, which means that $r = n$ or $r = n/2$. The second option is again impossible, since it would imply that A has a factor with CM, so we have that $r = n$. Thus φ is an isogeny, hence invertible in $\mathrm{End}_K^0(A)$.

Now, since $E = \mathrm{End}_k^0(A)$ is a maximal subfield of $\mathrm{End}_K^0(A) \simeq \mathrm{M}_n(\mathcal{B})$ we have that $[E : F] = nt$. Multiplying this equality by $[F : \mathbb{Q}]$ we have that $[E : \mathbb{Q}] = nt[F : \mathbb{Q}]$, and from $[E : \mathbb{Q}] = \dim A = n \dim B$ we obtain the relation $t[F : \mathbb{Q}] = \dim B$. □

Proposition 5.26. *Let A be an abelian variety of GL_2-type over k without complex multiplication. Then it is a Ribet-Pyle variety over k.*

Proof. By Lemma 5.25 with $K = \overline{k}$ we know that $E = \mathrm{End}_k^0(A)$ is a maximal subfield of $\mathrm{End}_{\overline{k}}^0(A)$. It only remains to prove that A is an abelian k-variety. For each $\sigma \in G_k$ the automorphism of $\mathrm{End}_{\overline{k}}^0(A)$ given by $\varphi \mapsto {}^\sigma\varphi$ fixes E; since E is a maximal subfield, it contains the center F of $\mathrm{End}_{\overline{k}}^0(A)$, and so $\varphi \mapsto {}^\sigma\varphi$ is a F-algebra automorphism. By the Skolem-Noether Theorem there exists an element $\alpha(\sigma)$ belonging to $\mathrm{End}_{\overline{k}}^0(A)$ such that ${}^\sigma\varphi = \alpha(\sigma)\varphi\alpha(\sigma)^{-1}$. This relation implies that $\alpha(\sigma)$ commutes with the elements in E, since they are endomorphisms defined over k. But E is a maximal subfield, so that it coincides with its centralizer. This implies that $\alpha(\sigma)$ belongs to E, and it is a compatible isogeny. □

Remark 5.27. The variety B/K appearing in Lemma 5.25 is an abelian k-variety with a system of compatible isogenies defined over K. Indeed, in the proof of 5.26 we have seen that A is an abelian k-variety with a system of isogenies defined over k. The system of isogenies induced on B by the decomposition $A \sim_K B^n$ gives compatible isogenies for B defined over K.

Lemma 5.25 and Remark 5.27 with $K = \overline{k}$ characterize the $\overline{k}$-simple factors of abelian varieties of GL_2-type over k. Moreover, the divisibility conditions in the classification theorem of endomorphism algebras of abelian varieties (cf. Theorem 1.23), together with the condition $t[F : \mathbb{Q}] = \dim B$ imply that $t = 1$ or $t = 2$. In the case of abelian varieties of GL_2-type over $\mathbb{Q}$, Pyle used the name building blocks for their $\overline{\mathbb{Q}}$-simple factors. Accordingly, we propose the following generalization.

Definition 5.28. A *building block for abelian varieties of* GL_2*-type over* k is an abelian k-variety $B/\overline{k}$ whose endomorphism algebra is a central division algebra over a field F with Schur index $t = 1$ or $t = 2$ and $t[F : \mathbb{Q}] = \dim B$.

Now a straightforward application of Theorem 5.3 implies that, in fact, every building block for abelian varieties of GL_2-type over k occurs as $\overline{k}$-simple factor of some abelian variety of GL_2-type.

Proposition 5.29. *Let B be a building block for abelian varieties of* GL_2*-type over k. There exists an abelian variety of* GL_2*-type over k such that $A \sim_{\overline{k}} B^n$ for some n.*

Proof. By Theorem 5.3 there exists a Ribet-Pyle variety A over k such that $A \sim_{\overline{k}} B^n$ for some n. The field $E = \mathrm{End}^0_k(A)$ is a maximal subfield of $\mathrm{End}^0_{\overline{k}}(A) \simeq \mathrm{M}_n(\mathcal{B})$, which means that $[E : F] = nt$. Multiplying both sides of this equality by $[F : \mathbb{Q}]$ we see that $[E : \mathbb{Q}] = nt[F : \mathbb{Q}] = n \dim B = \dim A$, and so A is a variety of GL_2-type over k. □

5.4. The endomorphism algebra of the restriction of scalars

Let $B/\overline{k}$ be a simple abelian k-variety. In Section 5.1 we have seen the relation of B with certain abelian varieties defined over k: the Ribet-Pyle varieties having B as simple factor. Another way of obtaining an abelian variety defined over k starting from B is by means of restriction of scalars. In this section we compute the endomorphism algebra of the restriction of scalars of B, a result that we will use in the next section in order to see the relation between the restriction of scalars and the Ribet-Pyle varieties associated to B.

It is worth noting that, although restriction of scalars has not appeared explicitly until now in our approach, it has been implicitly used in the construction of Ribet-Pyle varieties from a k-variety we described in Section 5.1. Indeed, we have used Theorem 2.4 as a black box that, given an abelian variety over $\overline{k}$ and a system of isogenies satisfying certain conditions, it produces an abelian variety defined over k, which is the one we have used to construct the Ribet-Pyle varieties. However, in Ribet's proof of this theorem, the variety defined over k is obtained as one of the factors of a restriction of scalars of the variety defined over $\overline{k}$.

Let K/k be a finite Galois extension with Galois group G. Suppose that B is defined over K and that for each $\sigma \in G_k$ there exists a compatible isogeny $\mu_\sigma \colon {}^\sigma B \to B$ defined over K (note that in this case all compatible isogenies ${}^\sigma B \to B$ are also defined over K). This situation is similar to the one where B is completely defined over K (cf. Definition 3.17), except that we do not require now all the endomorphisms of B to be defined over K. In addition, we relax the hypothesis of B being $\overline{k}$-simple, and we only require B to be K-simple. As usual we denote by $\mathcal{B}$ the endomorphism algebra $\mathrm{End}^0_{\overline{k}}(B)$ and by F the center of $\mathcal{B}$. Let also $\mathcal{D}$ be the algebra $\mathrm{End}^0_K(B)$ and

let E be the center of $\mathcal{D}$. Observe that Proposition 3.15 gives an inclusion $F \subseteq E$.

To such a variety B, we can attach a cohomology class $[c_{B/K}]$ belonging to $H^2(G, E^\times)$, where $E^\times$ is seen as a G-module with trivial action. The definition of the cocycle $c_{B/K}$ is very similar to the one given Section 3.2 for the case of varieties completely defined over K. That is, for each $s \in G$ choose a representative $\tilde{s}$ in G_k, and define

$$c_{B/K} \colon G \times G \to E^\times, \qquad c_{B/K}(s,t) = \mu_{\tilde{s}} \circ {}^{\tilde{s}}\mu_{\tilde{t}} \circ \mu_{\widetilde{st}}^{-1}.$$

When all the endomorphisms of B are defined over K this cocycle $c_{B/K}$ takes values in $F^\times$ and coincides with the $c_{B/K}$ defined in Section 3.2, so it can be seen as a generalization of that case; hence the choice of the notation. Since now we are not requiring the field K to be a field of definition of all the endomorphisms of B we can only guarantee that $c_{B/K}(s,t)$ lies in $E^\times$, but not in $F^\times$. In the next lemma we state the main properties of this cocycle.

Lemma 5.30. *The map $c_{B/K}$ is a 2-cocycle of G with values in $E^\times$, considered as a module with trivial action. The cohomology class $[c_{B/K}] \in H^2(G, E^\times)$ does not depend neither on the lift $s \mapsto \tilde{s}$, nor on the choice of the isogenies $\mu_{\tilde{s}}$. Moreover, the inflation of $[c_{B/K}]$ to $H^2(G_k, E^\times)$ coincides with the image of $[c_B]$ by the morphism $H^2(G_k, F^\times) \to H^2(G_k, E^\times)$ induced by the embedding $F^\times \hookrightarrow E^\times$.*

Proof. Let φ be an element of $\mathcal{D}$. Since $\widetilde{st} = \tilde{s}\,\tilde{t}\,\tau$ for some $\tau \in G_K$ we have

$$\begin{aligned} c_{B/K}(s,t) \circ \varphi &= \mu_{\tilde{s}} \circ {}^{\tilde{s}}\mu_{\tilde{t}} \circ \mu_{\widetilde{st}}^{-1} \circ \varphi = \mu_{\tilde{s}} \circ {}^{\tilde{s}}\mu_{\tilde{t}} \circ {}^{\widetilde{st}}\varphi \circ \mu_{\widetilde{st}}^{-1} = \\ &= \mu_{\tilde{s}} \circ {}^{\tilde{s}}\mu_{\tilde{t}} \circ {}^{\tilde{s}\tilde{t}\tau}\varphi \circ \mu_{\widetilde{st}}^{-1} = \mu_{\tilde{s}} \circ {}^{\tilde{s}}\mu_{\tilde{t}} \circ {}^{\tilde{s}\tilde{t}}\varphi \circ \mu_{\widetilde{st}}^{-1} = \\ &= \mu_{\tilde{s}} \circ {}^{\tilde{s}}\varphi \circ {}^{\tilde{s}}\mu_{\tilde{t}} \circ \mu_{\widetilde{st}}^{-1} = \varphi \circ \mu_{\tilde{s}} \circ {}^{\tilde{s}}\mu_{\tilde{t}} \circ \mu_{\widetilde{st}}^{-1} = \varphi \circ c_{B/K}(s,t), \end{aligned}$$

and this shows that $c_B(s,t)$ lies in E. In the same way we can prove the cocycle condition, and the independence on the set $\{\mu_\sigma\}_{\sigma \in G_k}$ is seen in an analogous way than for the case of the cocycle c_B.

Observe that, if $\sigma \in G_k$ is such that $\sigma|_K = \tilde{s}|_K$ then $\mu_\sigma \circ \mu_{\tilde{s}}^{-1}$ commutes with the elements in $\mathcal{D}$; therefore, we can write $\mu_\sigma = \lambda_\sigma \circ \mu_{\tilde{s}}$ for some $\lambda_\sigma \in E^\times$. Now it is immediately seen that using another lift from G to G_k modifies the cocycle $c_{B/K}$ by a coboundary.

It remains to prove the last statement in the lemma. Take $\sigma, \tau \in G_k$ and put $s = \sigma|_K$, $t = \tau|_K$. We use the same name for the cocycles and for their images for the morphisms involved; namely, $c_{B/K}$ is the inflation to G_k of $c_{B/K}$ and c_B is the image of c_B in $Z^2(G_k, E^\times)$. By the definitions $c_B(\sigma,\tau) = \mu_\sigma \circ {}^\sigma\mu_\tau \circ \mu_{\sigma\tau}^{-1}$ and $c_{B/K}(\sigma,\tau) = \mu_{\tilde{s}} \circ {}^{\tilde{s}}\mu_{\tilde{t}} \circ \mu_{\widetilde{st}}^{-1}$. Since $\sigma_{|K} = \tilde{s}_{|K}$ we see that $\mu_\sigma = \mu_{\tilde{s}} \circ \lambda_\sigma$ for some $\lambda_\sigma \in E$. Now $c_B(\sigma,\tau) = c_{B/K}(\sigma,\tau) \circ \lambda_\sigma \circ \lambda_\tau \circ \lambda_{\sigma\tau}^{-1}$ and the two cocycles are cohomologous. □

Remark 5.31. Observe that, since we are not requiring K to be a field of definition of all the endomorphisms of B, now the cohomology class $[c_{B/K}]$ can contain very small information about the variety B. For instance, if B is an abelian variety of GL_2-type over k, we can take $K = k$ and then $[c_{B/K}]$ is trivial, whereas if we take K a field of definition of $\mathrm{End}_k^0(B)$ then $[c_{B/K}]$ will not be trivial in general.

Our objective now is to compute the algebra $\mathrm{End}_k^0(\mathrm{Res}_{K/k}(B))$. What we obtain is a generalization of the expression found by Ribet in [**Ri92**, Lemma 6.4] for the case of $\mathbb{Q}$-curves, giving the algebra as a twisted group algebra. The main difference is that in our case the algebra is obtained by a construction that mimics the standard twisted group algebra definition, which we first describe in abstract terms.

Let $\mathcal{A}$ be any central E-algebra and let $c \in Z^2(G, E^\times)$ be a two-cocycle of a finite group G with values in the multiplicative group $E^\times$ viewed as a module with trivial action. One defines the E-algebra $\mathcal{A}^c[G]$ by just generalizing the usual definition of twisted group algebra: it is the free left $\mathcal{A}$-module $\oplus_{s\in G}\mathcal{A}\cdot\lambda_s$ with basis a set of symbols λ_s indexed by the elements $s \in G$ and multiplication defined by the relations:

$$\begin{aligned} a\cdot\lambda_s &= \lambda_s\cdot a, \qquad \text{for} \quad a\in\mathcal{A},\\ \lambda_s\cdot\lambda_t &= c(s,t)\cdot\lambda_{st}. \end{aligned} \tag{5.6}$$

The cocycle condition for c is used to check that this definition makes sense and produces an associative algebra. Of course its isomorphism class does only depend on the cohomology class of the cocycle c. This algebra is related with the twisted group algebra $E^c[G]$ through the following isomorphism:

$$\mathcal{A}^c[G] \simeq \mathcal{A}\otimes_E E^c[G] \qquad \text{as} \quad E\text{-algebras.}$$

Indeed, if we put $E^c[G] = \oplus_{s\in G} E\cdot\lambda_s$ then the map

$$\begin{array}{ccc} \mathcal{A}\otimes_E E^c[G] & \longrightarrow & \mathcal{A}^c[G] \\ a\otimes\sum x_s\cdot\lambda_s & \longmapsto & \sum(ax_s)\cdot\lambda_s \end{array}$$

is an isomorphism of E-algebras.

Proposition 5.32. *Let B be an abelian k-variety defined over K which is K-simple and has a system of compatible isogenies defined over K. Let $\mathcal{D} = \mathrm{End}_K^0(B)$ and $E = Z(\mathcal{D})$. Then,*

$$\mathrm{End}_k^0(\mathrm{Res}_{K/k}(B)) \simeq \mathcal{D}\otimes_E E^{c_{B/K}}[G]. \tag{5.7}$$

Proof. Call A the variety $\mathrm{Res}_{K/k}(B)$. For each $s \in G$ fix a representative $\tilde{s}$ for s in G_k, but imposing that $\tilde{1} = 1$. Let $\{\mu_\sigma\}_{\sigma\in G_k}$ be a locally constant set of compatible isogenies defined over K in which we have chosen μ_1 to be the identity. We know that $A \sim_K \prod_{s\in G} {}^{\tilde{s}}B$, and that by the universal property of the functor restriction of scalars $\mathrm{End}_k(A) \simeq \mathrm{Hom}_K(A, B)$. Hence,

$$\mathrm{End}_k^0(A) \simeq \mathrm{Hom}_K^0(A,B) \simeq \prod_{s\in G}\mathrm{Hom}_K^0({}^{\tilde{s}}B, B) \simeq \prod_{s\in G}\mathcal{D}\cdot\mu_{\tilde{s}}$$

and we see that $\mathrm{End}_k^0(A)$ is a left $\mathcal{D}$-module of dimension $[K:k]$. We shall determine now its structure as an algebra. Define, for $s \in G$, λ_s to be the endomorphism of A that sends ${}^{\tilde{t}s}B$ to ${}^{\tilde{t}}B$ via ${}^{\tilde{t}}\mu_{\tilde{s}}$. It is fixed by all elements in G_k and so it is an endomorphism of A defined over k. Since we forced $\tilde{1}$ to be 1, we can identify λ_1 with the identity endomorphism of $\mathrm{End}_k(A)$.

We can embed $\mathcal{D}$ in $\mathrm{End}_k^0(A)$ by sending each $d \in \mathcal{D}$ to the morphism whose components are the diagonal maps ${}^{\tilde{s}}d\colon {}^{\tilde{s}}B \to {}^{\tilde{s}}B$. Hence, we can multiply the λ_s by elements d in $\mathcal{D}$ in the following way, depending on whether we left or right multiply:

$$d\circ\lambda_s\colon {}^{\widetilde{ts}}B \xrightarrow{{}^{\tilde{t}}\mu_{\tilde{s}}} {}^{\tilde{t}}B \xrightarrow{{}^{\tilde{t}}d} {}^{\tilde{t}}B$$

$$\lambda_s\circ d\colon {}^{\widetilde{ts}}B \xrightarrow{{}^{\widetilde{ts}}d} {}^{\widetilde{ts}}B \xrightarrow{{}^{\tilde{t}}\mu_{\tilde{s}}} {}^{\tilde{t}}B.$$

By the compatibility of the isogenies it is clear that these two maps coincide, and therefore $d\circ\lambda_s = \lambda_s\circ d$. Also the compatibility of the isogenies gives us the formula $\lambda_s\circ\lambda_t = c_{B/K}(s,t)\circ\lambda_{st}$. Hence the multiplication in $\mathrm{End}_k^0(A)$ is given in terms of this basis by formulas (5.6) with cocycle $c_{B/K}$. Therefore this algebra is isomorphic to $\mathcal{D}^{c_{B/K}}[G]$, which is in turn isomorphic to $\mathcal{D}\otimes_E E^{c_{B/K}}[G]$. □

5.5. Restriction of scalars and Ribet-Pyle varieties

In this section we consider abelian k-varieties defined over a Galois extension K/k, and we study under what conditions their restriction of scalars $\mathrm{Res}_{K/k} B$ is k-isogenous to a product of Ribet-Pyle varieties. We begin by characterizing the varieties that appear as simple factors of Ribet-Pyle varieties when decomposed over Galois extensions. The result is, in fact, a generalization of Lemma 5.25.

Proposition 5.33. *Let A be a Ribet-Pyle variety over k, and let K/k be a Galois extension. Then A decomposes up to K-isogeny as $A \sim_K B^n$, where B is an abelian k-variety defined over K and with compatible isogenies between conjugates defined over K. If $\mathcal{D} = \mathrm{End}_K^0(B)$, $E = Z(\mathcal{D})$ and t is the Schur index of $\mathcal{D}$, then $[\mathrm{End}_k^0(A) : E] = tn$.*

Proof. Since $\mathrm{End}_k^0(A) \subseteq \mathrm{End}_K^0(A)$ we have that

$$Z(\mathrm{End}_K^0(A)) \subseteq C(\mathrm{End}_k^0(A)) = \mathrm{End}_k^0(A),$$

which is a field. Hence A is isotypical over K and we have that $A \sim_K B^n$, and from this we see that B is a k-variety. What we have to prove is the existence of compatible isogenies defined over K.

For each $\sigma \in G_k$ there exists an element $\alpha(\sigma)$ belonging to $\mathrm{End}_k^0(A)$ such that ${}^{\sigma}\psi = \alpha(\sigma)\circ\psi\circ\alpha(\sigma)^{-1}$ for all $\psi \in \mathrm{End}_k^0(A)$. This implies that $\alpha(\sigma)$ commutes with all elements of $\mathrm{End}_k^0(A)$, hence $\alpha(\sigma)$ belongs to $\mathrm{End}_k^0(A)$ because the centralizer of a maximal subfield is the field itself. Let φ be an element in $\mathrm{End}_k^0(B)$, and let $\tilde{\varphi}$ the K-endomorphism of $A \sim_K B^n$ obtained

as the diagonal of φ. Denote also by π_i the projection to the i-th component $B^n \to B$. We have the following commutative diagram:

$$\begin{array}{ccccccccccc}
{}^\sigma B & \xrightarrow{\text{diag}} & {}^\sigma B^n & \xrightarrow{\kappa} & {}^\sigma A = A & \xrightarrow{\alpha(\sigma)^{-1}} & A & \xrightarrow{\kappa^{-1}} & B^n & \xrightarrow{\pi_i} & B \\
\downarrow{\scriptstyle {}^\sigma\varphi} & & & & \downarrow{\scriptstyle {}^\sigma\tilde{\varphi}} & & \downarrow{\scriptstyle \tilde{\varphi}} & & & & \downarrow{\scriptstyle \varphi} \\
{}^\sigma B & \xrightarrow{\text{diag}} & {}^\sigma B^n & \xrightarrow{\kappa} & {}^\sigma A = A & \xrightarrow{\alpha(\sigma)^{-1}} & A & \xrightarrow{\kappa^{-1}} & B^n & \xrightarrow{\pi_i} & B.
\end{array}$$

Since the isogeny κ is defined over K, the rows are morphisms ${}^\sigma B \to B$ defined over K. For some i this morphism is non-zero, and so it is an isogeny because B is K-simple. This gives a compatible isogeny ${}^\sigma B \to B$.

Finally, the last statement in the proposition follows from the fact that $\mathrm{End}^0_k(A)$ is a maximal subfield of $\mathrm{End}^0_{\overline{k}}(A)$, hence it is also a maximal subfield of $\mathrm{End}^0_K(A)$. □

Corollary 5.34. *Let B/K be a K-simple variety such that $\mathrm{Res}_{K/k} B$ is k-isogenous to a product of Ribet-Pyle varieties. Then B is a k-variety with a system of compatible isogenies defined over K.*

Proof. Since $\mathrm{Res}_{K/k} B \sim_K \prod_{s\in \mathrm{Gal}(K/k)} {}^s B$, clearly B is a K-simple factor of a Ribet-Pyle variety. □

Let B/K be a K-simple abelian k-variety with a system of compatible isogenies defined over K. Let $G = \mathrm{Gal}(K/k)$, $\mathcal{D} = \mathrm{End}^0_K(B)$, $E = Z(\mathcal{D})$ and t the Schur index of $\mathcal{D}$. We want to characterize under what conditions $\mathrm{Res}_{K/k} B$ is k-isogenous to a product of Ribet-Pyle varieties.

Proposition 5.35. *If $A = \mathrm{Res}_{K/k}(B)$ is k-isogenous to a product of Ribet-Pyle varieties, then*

$$A \sim_k A_1^t \times \cdots \times A_n^t,$$

with the A_i pairwise non-isogenous k-simple Ribet-Pyle varieties. Moreover, the algebra $E^{c_{B/K}}[G]$ is isomorphic to a product of number fields, and each one of them splits $\mathcal{D}$.

Proof. A priori we know that

$$A \sim_k A_1^{s_1} \times \cdots \times A_n^{s_n} \tag{5.8}$$

for some $s_i > 0$ and with the A_i being non-isogenous k-simple Ribet-Pyle varieties. If we put $E_i = \mathrm{End}^0_k(A_i)$ then

$$\mathrm{End}^0_k(A) \simeq \mathrm{M}_{s_1}(E_1) \times \cdots \times \mathrm{M}_{s_n}(E_n). \tag{5.9}$$

On the other hand, from Proposition 5.32 we have that $\mathrm{End}^0_k(A) \simeq \mathcal{D} \otimes_E E^{c_{B/K}}[G]$. The algebra $E^{c_{B/K}}[G]$ is semisimple, so it has a decomposition $E^{c_{B/K}}[G] \simeq \prod_{i=1}^m \mathrm{M}_{r_i}(D_i)$, where each D_i is a simple division algebra of index t_i over its center, which contains E. Therefore, we have that

$$\mathrm{End}^0_k(A) \simeq \mathcal{D} \otimes_E \prod_{i=1}^m \mathrm{M}_{r_i}(D_i) \simeq \prod_{i=1}^m \mathrm{M}_{r_i}(\mathcal{D} \otimes_E D_i). \tag{5.10}$$

Comparing (5.9) and (5.10) we see that necessarily $m = n$ and (rearranging terms if necessary) $\mathcal{D} \otimes_E D_i$ is a matrix algebra over E_i. By looking at the dimensions we know that it has to be in fact isomorphic to $\mathrm{M}_{tt_i}(E_i)$, and this gives that

$$\mathrm{End}_k^0(A) \simeq \prod_{i=1}^{n} \mathrm{M}_{tt_i r_i}(E_i). \tag{5.11}$$

Comparing this expression with (5.9) we see that $s_i \geqslant t$. We claim that, actually, we have the equality $s_i = t$. To prove it, we can use the following isomorphisms

$$\mathrm{End}_k^0(A) \simeq \mathrm{Hom}_K^0(A_K, B) \simeq \mathrm{Hom}_K^0(\prod_{s\in G} {}^sB, B) \simeq \prod_{s\in G} \mathcal{D}.$$

From this we have that

$$\dim_E(\mathrm{End}_k^0(A)) = |G| \dim_E \mathcal{D} = |G|t^2. \tag{5.12}$$

Note that $A_i \sim_K B^{h_i}$ for some h_i. Since A_i is a Ribet-Pyle variety, E_i is a maximal subfield of $\mathrm{End}_K^0(A_i)$ so that $[E_i : E] = h_i t$. If we had $s_i > t$ for some i then we would have that

$$\begin{aligned} \dim_E(\mathrm{End}_k^0(A)) &= s_1^2[E_1 : E] + \cdots + s_n^2[E_n : E] = s_1^2 h_1 t + \cdots + s_n^2 h_n t \\ &> t^2(s_1 h_1 + \cdots + s_n h_n) = t^2|G|, \end{aligned}$$

which would give a contradiction with (5.12), and we conclude that $s_i = t$ for all i.

It only remains to prove the last statement in the proposition. Since A is a product of Ribet-Pyle varieties, by what we have just proved $\mathrm{End}_k^0(A) \simeq \prod_{i=1}^n \mathrm{M}_t(E_i)$. Thus, in (5.11) we must have $r_i = 1$ and $t_i = 1$. Since $t_i = 1$, we see that E_i splits $\mathcal{D}$, and then since $r_i = 1$ we have that $E^{c_{B/K}} \simeq \prod E_i$. □

We have the following converse to the previous proposition, in which we have to impose that all endomorphisms of B are already defined over K.

Proposition 5.36. *Let B be a k-variety completely defined over K. Suppose that $E^{c_{B/K}}[G]$ is commutative and that all of its simple factors split $\mathcal{D}$. Then $A = \mathrm{Res}_{K/k} B$ is k-isogenous to a product of Ribet-Pyle varieties.*

Proof. Let $E^{c_{B/K}}[G] \simeq \prod_{i=1}^m E_i$ be a decomposition into a product of fields. Since each E_i splits $\mathcal{D}$ we have that

$$\mathrm{End}_k^0(A) \simeq \prod_{i=1}^{m} \mathcal{D} \otimes_E E_i \simeq \prod_{i=1}^{m} \mathrm{M}_t(E_i).$$

From this we deduce a decomposition $A \sim_k A_1^t \times \cdots \times A_m^t$, where each A_i is an abelian variety defined over k such that $\mathrm{End}_k^0(A_i) \simeq E_i$. We claim that each A_i is a Ribet-Pyle variety. Indeed, observe that $A_i \sim_K B^{r_i}$, for some non-negative integer r_i. Thus, $A \sim_K B^{tr_1} \times \cdots \times B^{tr_m}$, and we have the

relation $t(r_1 + \cdots + r_m) = |G|$. From the universal property of restriction of scalars we know that

$$[\mathrm{End}^0_k(A) : E] = |G| \cdot [\mathcal{D} : E] = |G| \cdot t^2.$$

On the other hand we have that

$$[\mathrm{End}^0_k(A) : E] = t^2([E_1 : E] + \cdots [E_m : E]).$$

Combining these expressions we find that

$$[E_1 : E] + \cdots [E_m : E] = t(r_1 + \cdots r_m).$$

Since E_i is a subfield of $\mathrm{M}_{r_i}(\mathcal{D})$ we have that $[E_i : E] \leqslant tr_i$. Therefore we find that $[E_i : E] = tr_i$, and E_i is a maximal subfield of $\mathrm{End}^0_K(A_i) = \mathrm{End}^0_{\overline{k}}(A_i)$. $\square$

CHAPTER 6

Modular abelian varieties over number fields

The final two chapters of this thesis have a somewhat different flavor from the preceding ones. In some sense, chapters 2 through 5 were an attempt to extend to arbitrary number fields Ribet's theory of abelian varieties of GL_2-type over $\mathbb{Q}$ and their absolutely simple factors. But in this last part we will only deal with abelian varieties of GL_2-type over $\mathbb{Q}$, also called *modular abelian varieties*, and with their simple factors over number fields. To be more precise, we will look into the properties of their L-series over number fields, being particularly interested in the case where these L-series are equivalent with a product of L-series of classical elliptic modular forms over $\mathbb{Q}$. The varieties satisfying this last property will be called *strongly modular*.

However, it is worth noting that the following chapters are not disconnected from our work up to now. Indeed, at some points it will be crucial to use results from the past chapters, especially from chapters 3 and 5. Whenever possible, we have stated results in their full generality for Ribet-Pyle varieties over k; here we will apply them in the particular case of abelian varieties of GL_2-type over $k = \mathbb{Q}$.

We begin this chapter by introducing in Section 6.1 modular and strongly modular abelian varieties, and by justifying the interest of considering these two different notions of modularity.

6.1. Modular and strongly modular abelian varieties

The Shimura-Taniyama conjecture, also known as the Modularity theorem after being proved by Wiles, Breuil, Conrad, Diamond and Taylor, states that every elliptic curve $E/\mathbb{Q}$ is *modular*. There are several equivalent notions in the literature for what a modular elliptic curve over $\mathbb{Q}$ is, but we are interested in the following two. An elliptic curve $E/\mathbb{Q}$ is said to be *modular* if for some $N \in \mathbb{Z}_{>0}$ there exists a non-constant morphism of algebraic curves $X_0(N) \to E$ defined over $\mathbb{Q}$. Equivalently, $E/\mathbb{Q}$ is *modular* if there exists a classical newform f of weight 2 and level $N \in \mathbb{Z}_{>0}$ such that $L(f;s)$ is equivalent (i.e. equal up to a finite number of Euler factors) to $L(E/\mathbb{Q};s)$. Both of these equivalent notions of modularity are important and have major consequences for the arithmetic of elliptic curves. For instance, the first one has been exploited by Gross, Zagier and Kolyvagin to prove, by means of the theory of Heegner points in $X_0(N)$, the Birch and Swinnerton-Dyer conjecture for elliptic curves of analytic rank less than or

equal to 1. On the other hand, the second notion of modularity is the one that permits the proof of the Hasse conjecture for the L-series $L(E/\mathbb{Q}; s)$.

There is a similar notion of modular abelian variety of arbitrary dimension, which generalizes the previous one-dimensional case. However, now one has to consider modular forms for $\Gamma_1(N)$ instead of $\Gamma_0(N)$. Let $f = \sum a_n q^n$ be a weight two newform for a congruence subgroup $\Gamma_1(N)$, and let $E_f = \mathbb{Q}(\{a_n\})$ be the number field generated by its Fourier coefficients. Shimura attaches to f an abelian variety A_f defined over $\mathbb{Q}$, constructed as a subvariety of the Jacobian $J_1(N)$ of the modular curve $X_1(N)$. The variety A_f has dimension equal to the degree $[E_f : \mathbb{Q}]$ and the algebra $\mathrm{End}^0_{\mathbb{Q}}(A_f)$ of its endomorphisms defined over $\mathbb{Q}$ is isomorphic to the number field E_f. The abelian varieties A_f and, more generally, all abelian varieties $A/\mathbb{Q}$ that are isogenous over $\mathbb{Q}$ to A_f for some f are known as *modular abelian varieties*.

Ribet proved that $J_1(N)$ is isogenous over $\mathbb{Q}$ to a product of abelian varieties of the form A_f, where f is a newform of some level dividing N. Hence, a simple abelian variety $A/\mathbb{Q}$ is modular if and only if there exists a non-constant homomorphism $J_1(N) \to A$ defined over $\mathbb{Q}$ for some N. On the other hand, the L-series $L(A_f/\mathbb{Q}; s)$ is equivalent to the product $\prod_{\sigma:\, E_f \hookrightarrow \mathbb{C}} L({}^{\sigma}f; s)$ of the L-series of the Galois conjugates of the form f [**Sh71**, Section 7.5]. As a consequence of Faltings's isogeny theorem (see Proposition 6.6 below for the details), a simple abelian variety $A/\mathbb{Q}$ is modular if and only if its L-series $L(A/\mathbb{Q}; s)$ is equivalent to a product of L-series of newforms for $\Gamma_1(N)$. Therefore, similar to the one-dimensional case, we can give two equivalent definitions for modular abelian varieties: a simple abelian variety $A/\mathbb{Q}$ is modular if there exists a non-constant homomorphism $J_1(N) \to A$ defined over $\mathbb{Q}$ for some N; equivalently, a simple abelian variety $A/\mathbb{Q}$ is modular if $L(A/\mathbb{Q}; s)$ is equivalent to a product of L-series of newforms for $\Gamma_1(N)$ for some N. As with modular elliptic curves, L-series of modular abelian varieties satisfy the Hasse conjecture, and the theory of Heegner points can be used to produce partial results for modular abelian varieties in the direction of the Birch and Swinnerton-Dyer conjecture.

Because of these nice properties, modular abelian varieties have been intensively studied and exploited in the last decades. In practice, one can easily compute and work with modular forms and the corresponding modular abelian varieties thanks to the powerful tool provided by the theory of modular symbols: see [**Cr97**] for elliptic curves and [**St07**] for arbitrary dimension. The computer systems `Magma` and `Sage` include packages programmed by William Stein and others that are able to perform many explicit computations with those objects.

On the other hand, one would like to characterize the modularity of a given abelian variety $A/\mathbb{Q}$. Obviously, in the one-dimensional case this is achieved by the Shimura-Taniyama conjecture, which asserts that every elliptic curve over $\mathbb{Q}$ is modular. In [**Ri92**] Ribet introduced the concept of a variety of GL_2-type as a variety $A/\mathbb{Q}$ for which $\mathrm{End}^0_{\mathbb{Q}}(A)$ is a number field of

degree equal to the dimension of A. He generalized Shimura-Taniyama by conjecturing that every variety of GL_2-type is modular over $\mathbb{Q}$, and proved that this fact would be a consequence of Serre's conjecture on the modularity of 2-dimensional mod p Galois representations. After the recent proof of Serre's conjecture by Khare and Winterberger [**KW09**], we know that modularity of an abelian variety over $\mathbb{Q}$ is equivalent to the property of being of GL_2-type.

The abelian varieties of GL_2-type are not absolutely simple in general. Indeed, over a number field K, one has a decomposition of the form $A \sim_K B^n$ for some K-simple abelian variety B. Hence, for this B one has a non-constant homomorphism $J_1(N) \to B$ defined over K. It is natural then to make the following definition.

Definition 6.1. A simple abelian variety B/K is *modular over* K if there exists a non-constant homomorphism $J_1(N) \to B$ defined over K for some N.

This generalizes the first of the equivalent definitions we gave of modularity for varieties defined over $\mathbb{Q}$, and one is tempted to use this property for varieties over K in the same way as it was done over $\mathbb{Q}$. But as we have already remarked, in some applications the key property of modularity is the fact that the L-series of the variety is equivalent to a product of L-series of modular forms. In the case of varieties over number fields, this is a more restrictive condition than being a K-simple factor of some $J_1(N)$. This suggests that we make the following definition.

Definition 6.2. An abelian variety B/K defined over a number field K is *strongly modular over* K if its L-series $L(B/K; s)$ is equivalent to a product of L-series of classical newforms for $\Gamma_1(N)$.

The main purpose of this chapter is to give a characterization of modular and strongly modular non-CM abelian varieties over number fields. The description of modular abelian varieties over a number field K can be performed by adapting the techniques that Ribet and Pyle used in their characterization of modular abelian varieties over $\overline{\mathbb{Q}}$. With relation to strongly modular abelian varieties, the case of non-CM elliptic curves was already studied in [**Qu00**]. In fact, this part of the chapter can be seen as a a generalization of some of the results of [**Qu00**] to arbitrary dimension.

The plan for the rest of the chapter is as follows. In Section 6.2, we relate strong modularity with the property that the restriction of scalars of the variety is a product GL_2-type varieties. As a consequence of this, we see that if B/K is strongly modular, then necessarily the extension $K/\mathbb{Q}$ is abelian. In Section 6.3, we characterize modular abelian varieties over Galois number fields. In Section 6.4, we use the results of Sections 5.4 and 5.5 in order to give the main theorem of this chapter characterizing strongly modular abelian varieties. Given a $\overline{\mathbb{Q}}$-simple abelian variety B we

give necessary and sufficient conditions guaranteing the existence of some strongly modular abelian variety in the $\overline{\mathbb{Q}}$-isogeny class of B.

Remark 6.3. As we have already mentioned in Section 5.3, Shimura proved that a variety A_f has a factor with complex multiplication if and only if it is $\overline{\mathbb{Q}}$-isogenous to a power of an elliptic curve with complex multiplication. This is also equivalent to the fact that the newform f admits a twist by a quadratic character whose kernel is the field of complex multiplication of the corresponding elliptic curve. The CM case requires a special treatment, and for the rest of the chapter we will tacitly assume that all abelian varieties considered have no CM-factors up to isogeny; when necessary we will stress this condition by saying "*non-CM abelian variety.*"

6.2. Strong modularity and GL_2-type

The purpose of this section is to show that an abelian variety B/K is strongly modular if and only if the abelian variety $A/\mathbb{Q}$ obtained by restriction of scalars $A = \mathrm{Res}_{K/\mathbb{Q}}(B)$ is isogenous over $\mathbb{Q}$ to a product of abelian varieties of GL_2-type. Due to the fact that this last property is the one that plays a key role in this chapter, many statements become simpler if we enlarge the definition of GL_2-type to include varieties that are not simple over $\mathbb{Q}$.

Definition 6.4. An abelian variety $A/\mathbb{Q}$ is of GL_2*-type* if $\mathrm{End}^0_{\mathbb{Q}}(A)$ contains a commutative semisimple $\mathbb{Q}$-subalgebra of dimension over $\mathbb{Q}$ equal to $\dim A$.

Note that the standard use of "GL_2-type" in the literature (and in the previous chapters of this thesis) corresponds to the varieties that satisfy Definition 6.4 and are simple. The relation between the two concepts is analogous to the relation between arbitrary CM-abelian varieties and the simple ones (cf. [**Mi06**, Pag. 29]), as we now show.

Lemma 6.5. *An abelian variety over $\mathbb{Q}$ is of GL_2-type if and only if all its $\mathbb{Q}$-simple factors are of GL_2-type.*

Proof. For an abelian variety $A/\mathbb{Q}$ let $A \sim_{\mathbb{Q}} A_1^{r_1} \times \cdots \times A_n^{r_n}$ be its decomposition up to $\mathbb{Q}$-isogeny into $\mathbb{Q}$-simple factors. Put $\mathcal{D}_i = \mathrm{End}^0_{\mathbb{Q}}(A_i)$, let F_i be the center of $\mathcal{D}_i$ and let $t_i = [\mathcal{D}_i : F_i]^{1/2}$ be its Schur index. The decomposition of $\mathrm{End}^0_{\mathbb{Q}}(A)$ into simple algebras is

$$\mathrm{End}^0_{\mathbb{Q}}(A) \simeq \mathrm{M}_{r_1}(\mathcal{D}_1) \times \cdots \times \mathrm{M}_{r_n}(\mathcal{D}_n), \tag{6.1}$$

and the reduced degree of $\mathrm{End}^0_{\mathbb{Q}}(A)$ over $\mathbb{Q}$ is $[\mathrm{End}^0_{\mathbb{Q}}(A) : \mathbb{Q}]_{\mathrm{red}} = \sum r_i t_i [F_i : \mathbb{Q}]$.

If every A_i is of GL_2-type then $\mathcal{D}_i = F_i$ has degree $[F_i : \mathbb{Q}] = \dim A_i$. Every field extension E_i/F_i of degree r_i can be embedded in the matrix ring $\mathrm{M}_{r_i}(F_i)$ and the product $\prod E_i$ is a commutative semisimple subalgebra of $\mathrm{End}^0_{\mathbb{Q}}(A)$ of dimension $\sum [E_i : \mathbb{Q}] = \sum r_i [F_i : \mathbb{Q}] = \sum r_i \dim A_i = \dim A$, hence A is of GL_2-type.

For the converse we will make use of the following basic facts about associative algebras: for any semisimple k-algebra $\mathcal{A}$ the maximal commutative semisimple subalgebras $E \subseteq \mathcal{A}$ have dimension $\dim_k E = [\mathcal{A} : k]_{\mathrm{red}}$, and for every faithful $\mathcal{A}$-module M one has $[\mathcal{A} : k]_{\mathrm{red}} \leqslant \dim_k M$ with the equality being only possible if all the simple subalgebras of $\mathcal{A}$ are matrix algebras over fields (cf. [**Mi06**, Propositions 1.3 and 1.2]). The second fact applied to the space of tangent vectors $\mathrm{Lie}(B/\mathbb{Q})$ of an abelian variety $B/\mathbb{Q}$ gives the inequality $[\mathrm{End}^0_{\mathbb{Q}}(B) : \mathbb{Q}]_{\mathrm{red}} \leqslant \dim B = \dim \mathrm{Lie}(B/\mathbb{Q})$.

Assume now that A is of GL_2-type. Let $E \subseteq \mathrm{End}^0_{\mathbb{Q}}(A)$ be a commutative semisimple subalgebra with $[E : \mathbb{Q}] = \dim A$. Then by the previous results

$$\dim A = [E : \mathbb{Q}] \leqslant [\mathrm{End}^0_{\mathbb{Q}}(A) : \mathbb{Q}]_{\mathrm{red}} \leqslant \dim A.$$

Hence each step must be an equality and hence $\mathrm{End}^0_{\mathbb{Q}}(A)$ is a product of matrix algebras over fields, i.e. that $t_i = 1$ for all i.

Now, using the inequalities $[\mathrm{End}^0_{\mathbb{Q}}(A_i) : \mathbb{Q}]_{\mathrm{red}} \leqslant \dim A_i$ for every index, we have

$$\begin{aligned} \dim A &= [\mathrm{End}^0_{\mathbb{Q}}(A) : \mathbb{Q}]_{\mathrm{red}} = \sum r_i [F_i : \mathbb{Q}] \\ &= \sum r_i [\mathrm{End}^0_{\mathbb{Q}}(A_i) : \mathbb{Q}]_{\mathrm{red}} \leqslant \sum r_i \dim A_i = \dim A; \end{aligned}$$

the equality at each summand follows, from which one deduces $[F_i : \mathbb{Q}] = \dim A_i$ for all i and so all simple factors A_i are of GL_2-type. □

Proposition 6.6. *An abelian variety $A/\mathbb{Q}$ is strongly modular over $\mathbb{Q}$ if and only if it is of GL_2-type.*

Proof. If $A/\mathbb{Q}$ is of GL_2-type, by the previous lemma we have that $A \sim_{\mathbb{Q}} A_1^{r_1} \times \cdots \times A_n^{r_n}$, where the A_i's are $\mathbb{Q}$-simple abelian varieties of GL_2-type. By Shimura-Taniyama there exist newforms f_i such that $A_i \sim_{\mathbb{Q}} A_{f_i}$. Then $L(A/\mathbb{Q}, s) \sim \prod L(A_i/\mathbb{Q}, s)^{r_i} \sim \prod L(A_{f_i}/\mathbb{Q}, s)^{r_i}$ and since each $L(A_{f_i}/\mathbb{Q}, s)$ is the product of the L-series of the newforms that are Galois conjugates of f_i, the variety A is strongly modular over $\mathbb{Q}$.

Now we prove the converse. Let $A/\mathbb{Q}$ be a strongly modular abelian variety over $\mathbb{Q}$, and let $f_1, \ldots, f_n$ be newforms such that $L(A/\mathbb{Q}, s) = \prod L(f_i, s)$. Let E_i be the field of Fourier coefficients of f_i, and denote by $E = E_1 E_2 \cdots E_n$ their composition. Let $m = [E : \mathbb{Q}]$ and $m_i = [E : E_i]$, and denote by Σ_E and Σ_{E_i} the corresponding sets of complex embeddings. For every index i, the restriction of all the elements of Σ_E to the field E_i gives m_i copies of every element of Σ_{E_i}.

We will make use of the following notation: if $S = \sum a_n n^{-s}$ is a Dirichlet series with $a_n \in \mathbb{C}$ and σ belongs to $\mathrm{Aut}(\mathbb{C})$, we denote by ${}^{\sigma}S$ the series $\sum {}^{\sigma}a_n n^{-s}$; that is, the series obtained by applying σ to the coefficients a_n. Note that ${}^{\sigma}L(A/\mathbb{Q}; s) = L(A/\mathbb{Q}; s)$ because $L(A/\mathbb{Q}; s)$ has rational

coefficients. One has

$$\begin{aligned} L(A^m/\mathbb{Q};s) &= L(A/\mathbb{Q};s)^m = \prod_{\sigma\in\Sigma_E} {}^{\sigma}L(A/\mathbb{Q};s) = \prod_{\sigma\in\Sigma_E}\prod_{i=1}^{n} {}^{\sigma}L(f_i;s) \\ &= \prod_{i=1}^{n}\prod_{\sigma\in\Sigma_E} L({}^{\sigma}f_i;s) = \prod_{i=1}^{n}\prod_{\sigma\in\Sigma_{E_i}} L({}^{\sigma}f_i;s)^{m_i} \\ &= \prod_{i=1}^{n} L(A_{f_i}/\mathbb{Q};s)^{m_i} = L\left(\left(\prod_{i=1}^{n} A_{f_i}^{m_i}\right)/\mathbb{Q},s\right). \end{aligned}$$

Then by Faltings's isogeny theorem the two varieties A^m and $\prod A_{f_i}^{m_i}$ are isogenous over $\mathbb{Q}$ and by the uniqueness of decomposition up to $\mathbb{Q}$-isogeny into the product of $\mathbb{Q}$-simple varieties it follows that A is isogenous over $\mathbb{Q}$ to a product $\prod A_{f_i}^{e_i}$ for some exponents $e_i \geqslant 0$, and it thus is of GL_2-type. □

For other number fields, strong modularity can be reduced to that of the restriction of scalars.

Proposition 6.7. *An abelian variety B/K over a number field K is strongly modular over K if and only if $\mathrm{Res}_{K/\mathbb{Q}} B$ is of GL_2-type.*

Proof. A theorem of Milne asserts the equality of L-series $L(B/K;s) = L((\mathrm{Res}_{K/\mathbb{Q}} B)/\mathbb{Q};s)$ (see [**Mi72**, Proposition 3]). This implies that B is strongly modular over K if and only if $\mathrm{Res}_{K/\mathbb{Q}} B$ is strongly modular over $\mathbb{Q}$, and by the previous proposition this is the case if and only if $\mathrm{Res}_{K/\mathbb{Q}} B$ is of GL_2-type. □

Combining Lemma 6.6 with the above proposition one immediately obtains the following corollary.

Corollary 6.8. *An abelian variety is strongly modular over a number field K if and only if all its K-simple factors are strongly modular over K.*

Now we aim to show that if B/K is strongly modular over K, then necessarily the extension $K/\mathbb{Q}$ is abelian. We will need the following general property of the varieties obtained by restriction of scalars.

Lemma 6.9. *Let k be a field and k_s a separable closure of k. Let L, M be subfields of k_s of finite degree over k. Let C be an abelian variety over M. If the endomorphisms of the variety $A = \mathrm{Res}_{M/k} C$ are defined over L, then $M \subseteq L$.*

Proof. We will see that $G_L \subseteq G_M$. Suppose this is not the case. Then there exists an automorphism $\sigma \in G_L$ which does not belong to G_M. Let Σ_M denote the set of k-embeddings $\tau\colon M \to k_s$. If we denote by τ_0 the inclusion $\tau_0\colon M \hookrightarrow k_s$, then $\sigma\tau_0 \neq \tau_0$. We will construct an element $\varphi \in \mathrm{End}_{k_s}(A)$ such that ${}^{\sigma}\varphi \neq \varphi$, and this will be a contradiction with the fact that $\mathrm{End}_{k_s}(A) = \mathrm{End}_L(A)$.

Let A_0 be the variety $A_0 = \prod_{\tau\in\Sigma_M} {}^{\tau}C$, and for each $\rho \in G_k$ let $\phi_\rho\colon {}^{\rho}A_0 \to A_0$ be the isomorphism which permutes the coordinates according to the canonical isomorphisms ${}^{\rho}({}^{\tau}C) \simeq {}^{\rho\tau}C$. By the construction of the variety restriction of scalars, there exists a k_s-isomorphism $\lambda\colon A_0 \to A$ such that $\lambda^{-1}\circ{}^{\rho}\lambda = \phi_\rho$ (see Section 1.3).

Let ψ be a diagonal endomorphism of A_0; that is, one of the form $\prod_{\tau\in\Sigma_M}\psi_\tau$, with each ψ_τ an element of $\mathrm{End}_{k_s}({}^{\tau}C)$. Since $\sigma\tau_0 \neq \tau_0$ we can, and do, choose such a ψ with ${}^{\sigma}\psi_{\tau_0} \neq \psi_{\sigma\tau_0}$. Consider now the endomorphism of A given by $\varphi = \lambda\circ\psi\circ\lambda^{-1}$. If ${}^{\sigma}\varphi = \varphi$ then $\lambda^{-1}\circ{}^{\sigma}\lambda\circ{}^{\sigma}\psi = \psi\circ\lambda^{-1}\circ{}^{\sigma}\lambda$, and therefore $\phi_\sigma\circ{}^{\sigma}\psi = \psi\circ\phi_\sigma$. The restriction of $\phi_\sigma\circ{}^{\sigma}\psi$ to ${}^{\sigma\tau_0}C$ is equal to ${}^{\sigma}\psi_{\tau_0}$, whereas the restriction of $\psi\circ\phi_\sigma$ to ${}^{\sigma\tau_0}C$ is equal to $\psi_{\sigma\tau_0}$. But we chose ψ with ${}^{\sigma}\psi_{\tau_0} \neq \psi_{\sigma\tau_0}$, so ${}^{\sigma}\varphi \neq \varphi$ and therefore not all the endomorphisms of A are defined over L. This is a contradiction, thus G_L is indeed contained in G_M as we aimed to see. □

Proposition 6.10. *If an abelian variety B/K is strongly modular over K, then the extension $K/\mathbb{Q}$ is abelian.*

Proof. The variety $\mathrm{Res}_{K/\mathbb{Q}}(B)$ is isogenous over $\mathbb{Q}$ to a product of the form $\prod_f A_f$, for some weight two newforms f. The minimal field of definition of the endomorphisms of A_f is an abelian extension $L_f/\mathbb{Q}$ by [**GL01**, Proposition 2.1]. On the other hand, let A_f and A_g be simple factors over $\mathbb{Q}$ of $\mathrm{Res}_{K/\mathbb{Q}}(B)$. If $\mathrm{Hom}_{\overline{\mathbb{Q}}}(A_f, A_g) \neq 0$, then by [**Ri80**, Theorem 4.7] there exists a Galois character $\chi\colon G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^{\times}$ such that $g = \chi\otimes f$ (identifying χ with a Dirichlet character). If we denote by M the field fixed by the kernel of χ, then $\mathrm{Hom}_M(A_f, A_g) \neq 0$, so there exists a homomorphism between A_f and A_g defined over the abelian extension M. This implies that the endomorphisms between A_f and A_g are defined over the composition ML_fL_g, which is abelian. Thus, all the endomorphisms of $\mathrm{Res}_{K/\mathbb{Q}}(B)$ are defined over a certain abelian extension L. Now Lemma 6.9 implies that $K \subseteq L$, so that K is also abelian over $\mathbb{Q}$ (and in particular Galois). □

6.3. K-building blocks

Since we want to study abelian varieties over a number field K that are quotients up to K-isogeny of varieties of GL_2-type, we slightly adapt the definition of "building block" given by Pyle in [**Py02**, Pag.195], in order to keep track of their decomposition over K and not merely over $\overline{\mathbb{Q}}$.

Definition 6.11. Let $K/\mathbb{Q}$ be a Galois extension. We say that a (non-CM) abelian variety B/K is a *K-building block* if

(1) B is a $\mathbb{Q}$-variety having compatible isogenies $\mu_\sigma\colon {}^{\sigma}B \to B$ defined over K for every $\sigma \in G_{\mathbb{Q}}$.
(2) $\mathrm{End}^0_K(B)$ is a division algebra with center a number field E, having Schur index $t \leqslant 2$ and reduced degree $t[E:\mathbb{Q}] = \dim B$.

We note the following remarks:

- The requirement that $\mathrm{End}_K^0(B)$ is a division algebra implies that K-building blocks are K-simple abelian varieties, but they may factor over larger fields.
- The $\mathbb{Q}$-building blocks are the non-CM $\mathbb{Q}$-simple abelian varieties of GL_2-type.
- The $\overline{\mathbb{Q}}$-building blocks are the building blocks in the sense of Pyle's definition; we will also use this terminology without a prefix field sometimes.
- For $K = \overline{\mathbb{Q}}$, the field $E = Z(\mathrm{End}_K^0(B))$ is necessarily a totally real field, equal to the center of $\mathrm{End}_{\overline{\mathbb{Q}}}^0(B)$. However, for general K the number field $E = Z(\mathrm{End}_K^0(B))$ may be either a totally real or a CM-field, and the center F of $\mathrm{End}_{\overline{\mathbb{Q}}}^0(B)$ is a (necessarily totally real) subfield of E.
- We do not require B to have all its endomorphisms defined over K. This means that a K-building block is not necessarily a $\mathbb{Q}$-variety completely defined over K.

Let B be a K-building block over a Galois number field K, let $G = \mathrm{Gal}(K/\mathbb{Q})$, $E = Z(\mathrm{End}_K^0(B))$, and $F = Z(\mathrm{End}_{\overline{\mathbb{Q}}}^0(B))$. In Section 5.4 we attached B a cohomology class $[c_{B/K}]$, which in this case belongs to $H^2(K/\mathbb{Q}, E^\times)$. Since this cohomology class will play an important role in the characterization of modular and strongly modular varieties, we recall now the definition of the cocycle $c_{B/K}$. Let $\{\mu_\sigma\}_{\sigma\in G_\mathbb{Q}}$ be a compatible set of isogenies defined over K. For each $s \in G$ choose a representative $\tilde{s}$ in $G_\mathbb{Q}$. Then

$$c_{B/K}\colon G \times G \to E^\times, \qquad c_{B/K}(s,t) = \mu_{\tilde{s}} \circ {}^{\tilde{s}}\mu_{\tilde{t}} \circ \mu_{\widetilde{st}}^{-1}. \tag{6.2}$$

When all the endomorphisms of B are defined over K the image of the inflation of $[c_{B/K}]$ to $H^2(G_\mathbb{Q}, F^\times)$ coincides with $[c_B]$. However, since now we are not requiring the field K to be a field of definition of all the endomorphisms of B, we can only guarantee that $c_{B/K}(s,t)$ lies in $E^\times$ but not in $F^\times$ as it happens when the variety is completely defined over K. Nevertheless, the image of $[c_B]$ in $H^2(G_\mathbb{Q}, E^\times)$ is equal to the inflation of $[c_{B/K}]$ to $G_\mathbb{Q}$. The main reason why the cocycle $c_{B/K}$ is relevant to the strong modularity of B is because it appears in the expression for the endomorphisms defined over $\mathbb{Q}$ of the restriction of scalars of B.

Proposition 6.12. *Let B be a K-building block over a Galois number field with $G = \mathrm{Gal}(K/\mathbb{Q})$. Let $\mathcal{D} = \mathrm{End}_K^0(B)$ and $E = Z(\mathcal{D})$. Then,*

$$\mathrm{End}_\mathbb{Q}^0(\mathrm{Res}_{K/\mathbb{Q}}(B)) \simeq \mathcal{D} \otimes_E E^{c_{B/K}}[G]. \tag{6.3}$$

Proof. This is a particular case of Proposition 5.32. □

Proposition 6.13. *A K-simple abelian variety B/K is modular over a Galois number field K if and only if it is a K-building block and $[c_{B/K}]$ has trivial Schur class (i.e. its image in $H^2(K/\mathbb{Q}, \overline{E}^\times)$ is trivial).*

PROOF. Let B/K be a modular variety over K, and let $A/\mathbb{Q}$ be a simple GL_2-type variety with $A \sim_K B^n$. The fact that B is a K-building block follows from Lemma 5.25 and Remark 5.27 in the particular case $k = \mathbb{Q}$. Now let $\mathcal{D} = \mathrm{End}_K^0(B)$, $E = Z(\mathcal{D})$ and $E_0 = \mathrm{End}_{\mathbb{Q}}^0(A)$. By Lemma 5.25, E_0 is a maximal subfield of $\mathrm{End}_K^0(A)$. In particular, since E can be identified with $Z(\mathrm{End}_K^0(A))$ we see that E is contained in E_0. For each $s \in \mathrm{Gal}(K/\mathbb{Q})$ the map

$$\begin{array}{ccc} \mathrm{End}_K^0(A) & \longrightarrow & \mathrm{End}_K^0(A) \\ \varphi & \longmapsto & {}^s\varphi \end{array}$$

is an E-algebra automorphism, hence it is inner. So there exists an element $\alpha(s) \in \mathrm{End}_K^0(A)^\times$ such that ${}^s\varphi = \alpha(s) \circ \varphi \circ \alpha(s)^{-1}$ for all $\varphi \in \mathrm{End}_K^0(A)$. In particular, elements $\varphi \in E_0$ commute with $\alpha(s)$. This means that $\alpha(s)$ belongs to the centralizer of E_0 in $\mathrm{End}_K^0(A)$, and therefore $\alpha(s)$ belongs to E_0. Since $\alpha(s)$ is a compatible isogeny defined over K, we can compute the cocycle $c_{A/K}$ as

$$c(s,t) = \alpha(s) \circ \alpha(t) \circ \alpha(st)^{-1}. \tag{6.4}$$

Since $A \sim_K B^n$ we have that $[c_{B/K}] = [c_{A/K}]$, and (6.4) states that the image of $[c_{A/K}]$ in $H^2(K/\mathbb{Q}, E_0)$ is trivial.

The other implication can be obtained with a slight modification of the ideas in the proof of Theorem 5.3 (or of [**Py02**, Proposition 4.5]), with the algebra of endomorphisms defined over K playing the role that in those proofs was played by the algebra of endomorphisms defined over the algebraic closure. We sketch the key steps of the argument. Let B/K be a K-building block and let $\mathcal{D} = \mathrm{End}_K^0(B)$ and $E = Z(\mathcal{D})$. Starting from a system of compatible isogenies $\{\mu_\sigma \colon {}^\sigma B \to B\}_{\sigma \in G_{\mathbb{Q}}}$ defined over K we construct the cohomology class $[c_{B/K}] \in H^2(K/\mathbb{Q}, E^\times)$ as in (6.2). That is, for each $s \in \mathrm{Gal}(K/\mathbb{Q})$ fix $\tilde{s} \in G_{\mathbb{Q}}$ such that $\tilde{s}_{|K} = s$; define $\mu_s = \mu_{\tilde{s}}$ and then $c_{B/K}(s,t) = \mu_s \circ {}^s\mu_t \circ \mu_{st}^{-1}$. The image of $[c_{B/K}]$ in $H^2(K/\mathbb{Q}, \overline{E}^\times)$ is trivial by hypothesis, so there exist splitting maps β such that $c_{B/K}(s,t) = \beta(s)\beta(t)\beta(st)^{-1}$. The field $E_\beta = E(\{\beta(s)\}_{s \in \mathrm{Gal}(K/\mathbb{Q})})$ acts on B^n as K-endomorphisms, where $n = [E_\beta : E]$, by means of an E-algebra homomorphism $E_\beta \to \mathrm{M}_n(E)$. Hence we can define K-isogenies $\nu_s = \beta(s)^{-1} \circ \hat{\mu}_s$, where $\hat{\mu}_s$ is the diagonal isogeny ${}^sB^n \to B^n$ obtained from μ_s. These isogenies satisfy the condition of Ribet's Theorem 2.4, hence there exists an abelian variety A defined over $\mathbb{Q}$ together with an isogeny $\kappa \colon A \to B^n$ defined over K. As in Corollary 5.12, the algebra $\mathrm{End}_{\mathbb{Q}}^0(A)$ is isomorphic to $\mathcal{D} \otimes_E E_\beta$. Let t be the Schur index of $\mathcal{D}$, and let t_0 be the Schur index of $\mathcal{D} \otimes_E E_\beta$, which is a divisor of t. Since $\mathcal{D} \otimes_E E_\beta$ acts on $\mathrm{Lie}(A/\mathbb{Q})$ we have that $t_0^2[E_\beta : \mathbb{Q}] \mid \dim A$. But $[E_\beta : \mathbb{Q}] = n[E : \mathbb{Q}]$ and $\dim A = n \dim B = nt[E : \mathbb{Q}]$. Thus $t_0^2 \mid t$, and since $t \leqslant 2$ we see that $t_0 = 1$. Thus the variety A decomposes as $A \sim_{\mathbb{Q}} A_0^t$ with $\mathrm{End}_{\mathbb{Q}}^0(A_\beta) \simeq E_\beta$, and one easily checks that A_0 is a variety of GL_2-type. $\square$

Corollary 6.14. *If a K-simple variety is strongly modular over a Galois number field K, then it is a K-building block.*

PROOF. Let B be a K-simple strongly modular abelian variety. By Proposition 6.6, since B is strongly modular over K, $\mathrm{Res}_{K/\mathbb{Q}}(B)$ is of GL_2-type. Since $\mathrm{Res}_{K/\mathbb{Q}}(B) \sim_K \prod_{s\in\mathrm{Gal}(K/\mathbb{Q})} {}^sB$, the variety B is a K-simple factor of the extension of scalars of a $\mathbb{Q}$-simple variety of GL_2-type, and then it is a K-building block by the previous lemma. □

6.4. Strongly modular abelian varieties

Let B be a K-building block over a Galois number field K with $G = \mathrm{Gal}(K/\mathbb{Q})$. Let $\mathcal{D} = \mathrm{End}^0_K(B)$, let $E = Z(\mathcal{D})$, and let t be the Schur index of $\mathcal{D}$. Recall that in the previous section we have associated to B/K a cohomology class $[c_{B/K}] \in H^2(K/\mathbb{Q}, E^\times)$. In this section, we characterize when B is strongly modular over K in terms of that class.

Lemma 6.15. *Let B be a K-building block over a Galois number field K. If $A = \mathrm{Res}_{K/\mathbb{Q}}(B)$ is an abelian variety of GL_2-type, then*

$$A \sim_{\mathbb{Q}} A_1^t \times \cdots \times A_n^t,$$

for some $t \in \mathbb{Z}_{>0}$ and with the A_i pairwise non-isogenous $\mathbb{Q}$-simple abelian varieties of GL_2-type.

PROOF. This is Proposition 5.35 with $k = \mathbb{Q}$. □

Lemma 6.16. *Let B be a K-building block over a Galois number field K with $G = \mathrm{Gal}(K/\mathbb{Q})$. Then B is strongly modular if and only if the algebra $E^{c_{B/K}}[G]$ is commutative.*

PROOF. The proof is similar to those of propositions 5.35 and 5.36. First suppose that $E^{c_{B/K}}[G]$ is commutative. Then it is a product of fields, say $E^{c_{B/K}}[G] = \prod E_i$. Call A the variety $\mathrm{Res}_{K/\mathbb{Q}}(B)$. By Proposition 6.12 we know that

$$\mathrm{End}^0_{\mathbb{Q}}(A) \simeq \mathcal{D} \otimes_E E^{c_{B/K}}[G] \simeq \prod \mathcal{D} \otimes_E E_i,$$

with $\mathcal{D} \otimes_E E_i$ a central simple E_i-algebra with Schur index t_i dividing t. Corresponding to this decomposition of $\mathrm{End}^0_{\mathbb{Q}}(A)$ there is a decomposition of A up to $\mathbb{Q}$-isogeny: $A \sim_{\mathbb{Q}} \prod A_i$, and $\mathrm{End}^0_{\mathbb{Q}}(A_i) \simeq \mathcal{D} \otimes_E E_i$. As $A_K \simeq \prod {}^sB \sim_K B^{|G|}$, each A_i is K-isogenous to B^{n_i} for some n_i. We claim that n_i equals $[E_i : E]$. To prove the claim, first we observe that the natural inclusion $\mathrm{End}^0_{\mathbb{Q}}(A_i) \hookrightarrow \mathrm{End}^0_K(A_i)$ gives an injective morphism $\mathcal{D} \otimes_E E_i \hookrightarrow \mathrm{M}_{n_i}(\mathcal{D})$. Looking at the reduced degrees of these algebras over E we see that $t[E_i : E] \leqslant tn_i$, and then $[E_i : E] \leqslant n_i$. To see the equality, we can use that on the one hand, as $\mathrm{End}^0_{\mathbb{Q}}(A) \simeq \bigoplus_{s\in G} \mathrm{Hom}^0_K({}^sB, B) \simeq \bigoplus_{s\in G} \mathcal{D}$ we have that:

$$[\mathrm{End}^0_{\mathbb{Q}}(A) : E] = |G|t^2 = t^2 \sum n_i.$$

But, on the other hand we have that:

$$[\mathrm{End}^0_{\mathbb{Q}}(A) : E] = [\mathcal{D} \otimes_E \prod E_i \ : E] = t^2 \sum [E_i : E],$$

and this gives that $[E_i : E] = n_i$.

Returning to the proof of the lemma, since $\mathrm{End}^0_{\mathbb{Q}}(A_i) \simeq \mathcal{D} \otimes_E E_i$ is a central simple algebra of index $t_i | t$, there exists a division E_i-algebra $\mathcal{D}_i$ of index t_i acting on the space of tangent vectors of A_i. This space $\mathrm{Lie}(A_i/\mathbb{Q})$ is a $\mathbb{Q}$-vector space of dimension equal to the dimension of A_i, and so we have that $[\mathcal{D}_i : \mathbb{Q}] | \dim A_i$. But $[\mathcal{D}_i : \mathbb{Q}] = t_i^2 [E_i : E][E : \mathbb{Q}]$ and $\dim A_i = n_i \dim B = n_i t [E : \mathbb{Q}] = t[E_i : E][E : \mathbb{Q}]$, because $n_i = [E_i : E]$. This means that

$$t_i^2 [E_i : E][E : \mathbb{Q}] \mid t[E_i : E][E : \mathbb{Q}],$$

so $t_i^2 | t$, which implies that $t_i = 1$. This means that $\mathcal{D} \otimes_E E_i \simeq \mathrm{M}_t(E_i)$, and therefore $A_i \sim_{\mathbb{Q}} (A_i')^t$, for some abelian variety A_i' with $\mathrm{End}^0_{\mathbb{Q}}(A_i') \simeq E_i$. Finally, $A_i' \sim_K B^{n_i/t}$, which gives that

$$[E_i : \mathbb{Q}] = n_i [E : \mathbb{Q}] = \frac{n_i}{t} t [E : \mathbb{Q}] = \frac{n_i}{t} \dim B = \dim A_i',$$

showing that each A_i' is a variety of GL_2-type.

In order to prove the other implication, by the previous lemma we can suppose that $A \sim_{\mathbb{Q}} A_1^t \times \cdots \times A_n^t$, and as a consequence that

$$\mathrm{End}^0_{\mathbb{Q}}(A) \simeq \mathrm{M}_t(E_1) \times \cdots \times \mathrm{M}_t(E_n), \tag{6.5}$$

where the notation is the same as in the first part of the proof. On the other hand,

$$\mathrm{End}^0_{\mathbb{Q}}(A) \simeq \mathcal{D} \otimes_E E^{c_{B/K}}[G] = \mathcal{D} \otimes_E \prod \mathrm{M}_{r_i}(C_i)$$

where the C_i are division algebras. But (6.5) forces $r_i = 1$ and $C_i \simeq E_i$ for all i. □

Now we state our main result giving a characterization of strong modularity.

Theorem 6.17. *Let K be a number field and let B/K be a K-simple abelian variety. Then B is strongly modular over K if and only if $K/\mathbb{Q}$ is abelian, B is a K-building block and $[c_{B/K}]$ lies in $\mathrm{Ext}(K/\mathbb{Q}, E^\times) \subseteq H^2(K/\mathbb{Q}, E^\times)$, the subgroup of classes of symmetric cocycles.*

Proof. By Proposition 6.10, the extension $K/\mathbb{Q}$ is Galois and $G = \mathrm{Gal}(K/\mathbb{Q})$ is abelian. Then, by Corollary 6.14 being a K-building block is a necessary condition, and in that case the previous lemma says that being strongly modular is equivalent to the fact that the algebra $E^{c_{B/K}}[G]$ is commutative. A twisted group algebra $E^c[G]$ is commutative if and only if the group G is abelian and the cocycle c is symmetric, i.e., its class belongs to the subgroup $\mathrm{Ext}(K/\mathbb{Q}, E^\times) \subseteq H^2(K/\mathbb{Q}, E^\times)$ consisting of symmetric cocycle classes. □

Absolutely simple varieties. The previous theorem shows that strong modularity puts very restrictive conditions on varieties. In what follows we will examine the case of $\overline{\mathbb{Q}}$-building blocks and see which varieties in their isogeny class are strongly modular.

For that let B be a $\overline{\mathbb{Q}}$-building block. Let $\mathcal{D} = \mathrm{End}^0_{\overline{\mathbb{Q}}}(B)$. The center $F = Z(\mathcal{D})$ is a totally real number field and $\mathcal{D}$ is either equal to F, in which case $t = 1$ and $[F : \mathbb{Q}] = \dim B$, or it is a totally indefinite quaternion algebra over F, with $t = 2$ and $[F : \mathbb{Q}] = \frac{1}{2}\dim B$. Let $\xi = [c_B] \in H^2(G_{\mathbb{Q}}, F^\times)$ be the cohomology class attached to B.

We fix an embedding $F \hookrightarrow \overline{\mathbb{Q}}$. By Tate's theorem the group $H^2(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^\times)$ is trivial (here $G_{\mathbb{Q}}$ acts trivially in $\overline{\mathbb{Q}}$), so there exist continuous maps $\beta\colon G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^\times$ such that $c_B(\sigma,\tau) = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1}$ for all $\sigma, \tau \in G_{\mathbb{Q}}$; two such maps differ in a Galois character. The map $\overline{\beta}\colon G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^\times/F^\times$ obtained viewing the values of β modulo $F^\times$ is a morphism; let K_β denote the fixed field of its kernel, which is an abelian extension of $\mathbb{Q}$. If d denotes the degree of a compatible isogeny defined in Section 3.3, we can define the map $\varepsilon_\beta(\sigma) = \beta(\sigma)^2/d(\mu_\sigma)$, which is a Galois character $G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^\times$; two such characters differ in the square of a Galois character. Let K_{ε_β} be the fixed field of $\ker \varepsilon_\beta$; the fact that $d(\mu_\sigma)$ is real and totally positive implies that $K_{\varepsilon_\beta} \subseteq K_\beta$. Let $E_\beta = F(\{\beta(\sigma)\}_{\sigma\in G_{\mathbb{Q}}})$ be the number field generated over F by the values of β; from the identity defining $\varepsilon_\beta(\sigma)$ it easily follows that E_β/F is an abelian extension. Even though the splitting maps β depend on the cocycle c_B (or, what is the same, on a system of compatible isogenies between conjugates of B) the morphisms $\overline{\beta}$, the fields K_β and E_β, and the characters ε_β do not depend on that choice. We will call the maps β *splitting maps*, the fields K_β *splitting fields*, and the characters ε_β *splitting characters* for the building block B. The isogeny class of a building block determines a set of morphisms $\overline{\beta} \in \mathrm{Hom}(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^\times/F^\times)$ that is an orbit by the action of the group of Galois characters $\mathrm{Hom}(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^\times)$, and a set of splitting characters $\varepsilon_\beta \in \mathrm{Hom}(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^\times)$ that is an orbit by the action of the subgroup of squares $\mathrm{Hom}(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^\times)^2$.

For every Galois character $\varepsilon\colon G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^\times$ choose square roots of its values and define

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

This is a 2-cocycle of $G_{\mathbb{Q}}$ with values in $\{\pm 1\}$. Its cohomology class $[c_\varepsilon]$ lies in $H^2(G_{\mathbb{Q}}, \{\pm 1\}) \simeq \mathrm{Br}_2(\mathbb{Q})$ and it gives the obstruction to the existence of a square root of ε. If two characters $\varepsilon, \varepsilon'$ differ in the square of a character, then $[c_\varepsilon] = [c_{\varepsilon'}]$. If $\xi = [c_B] \in H^2(G_{\mathbb{Q}}, F^\times)$ is the class attached to a building block B, then $\xi_\pm = [c_\varepsilon]$ with ε any splitting character for B (see [**Qu09**, Theorem 2.6]).

Theorem 6.18. *Let $B/\overline{\mathbb{Q}}$ be a $\overline{\mathbb{Q}}$-building block and let $K/\mathbb{Q}$ be an abelian extension. There exists an abelian variety B_0/K in the $\overline{\mathbb{Q}}$-isogeny class of*

B that is completely defined and strongly modular over K if and only if K contains a splitting field for $[c_B]$.

PROOF. The proof is essentially the same given in [**Qu00**, Proposition 5.2] for the case of $\mathbb{Q}$-curves.

Suppose that K contains the splitting field K_β corresponding to some splitting map β. For every element $s \in G = \mathrm{Gal}(K/\mathbb{Q})$ choose an element $\beta(s)$ as any of the values $\beta(\sigma)$ for $\sigma \in G_\mathbb{Q}$ an automorphism restricting to s, and define $c(s,t) = \beta(s)\beta(t)\beta(st)^{-1}$. Then $[c]$ is an element of $H^2(K/\mathbb{Q}, F^\times)$ whose inflation equals to $[c_B]$. By Proposition 3.18 there exists an abelian variety B_0/K that is $\overline{\mathbb{Q}}$-isogenous to B and completely defined over K with $[c_{B_0/K}] = [c]$. By construction the c is symmetric, hence $[c_{B_0/K}]$ belongs to $\mathrm{Ext}(G, F^\times)$ and by Theorem 6.17 the variety B_0 is strongly modular over K.

Conversely, assume that there is a variety isogenous to B that is strongly modular over K. Let $c_{B_0/K}$ be a cocycle of G attached to this variety. Then by Theorem 6.17 the algebra $F^{c_{B_0/K}}[G]$ is commutative. Hence the $\overline{\mathbb{Q}}$-algebra $\overline{\mathbb{Q}}^{c_{B_0/K}}[G] = \overline{\mathbb{Q}} \otimes_F F^{c_{B_0/K}}[G]$ is also commutative, and by a property of twisted group algebras over algebraically closed fields (cf. [**Ka93**, Chapter 2, Corollary 2.5]) it follows that the image of the class $[c_{B_0/K}]$ into the Schur multiplier group $H^2(K/\mathbb{Q}, \overline{\mathbb{Q}}^\times)$ is trivial. Hence there exists a map $s \mapsto \beta(s) \colon G \to \overline{\mathbb{Q}}^\times$ such that $c_{B_0/K}(s,t) = \beta(s)\beta(t)\beta(st)^{-1}$ and its inflation to the group $G_\mathbb{Q}$ is a splitting map for the variety that factors through the group G, hence $K_\beta \subseteq K$. □

CHAPTER 7

QM-Jacobian surfaces

In this chapter we illustrate some of the previous general results with applications to the study of concrete abelian surfaces with quaternionic multiplication. More precisely, we will consider genus 2 curves C whose Jacobian $B = \mathrm{Jac}(\mathrm{C})$ has as endomorphism algebra a rational quaternion algebra $\mathcal{B}$. In Section 7.1 we will use the theory provided by [**Ro04**] to compute the cohomology classes $[c_B]$, provided that $\mathcal{B}$ is of a specific type called twisting. In Section 7.2 we will particularize this to a family of genus 2 curves defined in [**HM95**], and using some results on its arithmetic that appear in [**BG08**] we will be able to give very explicitly the cocycles needed for the characterization of their strong modularity, and for the computation of $\mathbb{Q}$-endomorphism algebras of their restriction of scalars. After a technical remark about how twisting a curve affects the cohomology classes attached to its Jacobian, to which we have devoted Section 7.3, we will produce in Section 7.4 a series of explicit examples of strongly modular abelian surfaces.

Remark 7.1. So far we have been working in the category of abelian varieties up to isogeny, and for instance all fields of moduli we have considered were fields of moduli up to isogeny. In the present chapter our strategy will be to use what is known about fields of moduli up to isomorphism of abelian surfaces, in order to obtain results in the context that concerns us of abelian surfaces up to isogeny. Consequently, from now on we will be very accurate with the terminology, and for instance for *homomorphism of abelian varieties* we will mean a 'true' homomorphism (and not homomorphism of abelian varieties up to isogeny); accordingly, the notation $\mathrm{Hom}(A, B)$ stands for the $\mathbb{Z}$-module of homomorphisms from A to B. A similar remark holds for the ring of endomorphisms $\mathrm{End}(A)$, and for the word *isomorphism* that is reserved for 'true' isomorphisms.

7.1. Field of moduli of QM-curves

We start this section by recalling some notations and results from [**Ro04**]. For rational numbers a and b we denote by $(a, b)_{\mathbb{Q}}$ the quaternion algebra over $\mathbb{Q}$ generated by $\imath, \jmath$ with $\imath^2 = a$, $\jmath^2 = b$ and $\imath\jmath + \jmath\imath = 0$. Let $\mathcal{B}$ be an indefinite rational quaternion algebra of discriminant $D > 1$, and let $\mathcal{O}$ be a maximal order in $\mathcal{B}$. We will denote by n and tr the corresponding reduced norm and trace.

Definition 7.2. A curve $C/\overline{\mathbb{Q}}$ is said to be a *QM-curve with respect to $\mathcal{O}$* if $\mathcal{O}$ can be embedded in the endomorphism ring of its Jacobian.

Fix an element $\mu \in \mathcal{O}$ such that $\mu^2 + D = 0$, whose existence is guaranteed by Eichler's theory of optimal embeddings, and call the pair $(\mathcal{O}, \mu)$ a *principally polarized order*. A *twist* of $(\mathcal{O}, \mu)$ is an element $\chi \in \mathcal{O} \cap N_{B^\times}(\mathcal{O})$ such that $\chi^2 + \mathrm{n}(\chi) = 0$ and $\chi\mu + \mu\chi = 0$, so that $\mathcal{B} \simeq (-D, -\mathrm{n}(\chi))_{\mathbb{Q}}$. The pair $(\mathcal{O}, \mu)$ is *twisting* if it admits some twist in $\mathcal{O}$, and $\mathcal{B}$ is said to be *twisting* if it contains some twisting polarized maximal order. In fact, $\mathcal{B}$ is twisting if and only if $\mathcal{B} \simeq (-D, m)_{\mathbb{Q}}$ for some m dividing D.

Let $(B, \rho)/\overline{\mathbb{Q}}$ be a polarized abelian variety. Recall that ρ is an isogeny $\rho\colon B \to \hat{B}$. If R is a subring of $\mathrm{End}_{\overline{\mathbb{Q}}}(B)$, the *field of moduli* k_R is defined to be the smallest number field such that for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/k_R)$ there exists an isomorphism $\phi_\sigma\colon {}^\sigma B \to B$ such that the diagram

$$\begin{array}{ccc} {}^\sigma B & \xrightarrow{\phi_\sigma} & B \\ {\scriptstyle {}^\sigma r}\downarrow & & \downarrow{\scriptstyle r} \\ {}^\sigma B & \xrightarrow{\phi_\sigma} & B \end{array}$$

commutes for all $r \in R$, and such that the pullback $\phi_\sigma^*(\rho) = \hat{\phi}_\sigma \circ \rho \circ \phi_\sigma$ is equal to ${}^\sigma\rho$. In other words, k_R is the field of moduli of the object consisting of the polarized abelian variety (B, ρ) together with the subring of endomorphisms $R \subseteq \mathrm{End}_{\overline{\mathbb{Q}}}(B)$.

For any curve C, its Jacobian $\mathrm{Jac}(C)$ is a polarized abelian variety with the canonical polarization induced by C. The *field of moduli of C*, denoted by k_C, is the smallest number field such that ${}^\sigma C$ and C are isomorphic for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/k_C)$. Note that this is the same as the field of moduli $k_{\mathbb{Z}}$ for the subring $\mathbb{Z} \subseteq \mathrm{End}_{\overline{\mathbb{Q}}}(\mathrm{Jac}(C))$. The following result is [**Ro04**, Theorem 4.1].

Theorem 7.3 (Rotger)**.** *Let $C/\overline{\mathbb{Q}}$ be a smooth irreducible curve of genus 2 such that $\mathrm{End}_{\overline{\mathbb{Q}}}(\mathrm{Jac}(C))$ is isomorphic to a maximal order $\mathcal{O}$ in a rational indefinite quaternion algebra of discriminant $D > 1$. Fix an isomorphism $\mathcal{O} \simeq \mathrm{End}_{\overline{\mathbb{Q}}}(\mathrm{Jac}(C))$ and let $\mu \in \mathcal{O}$ such that $\mu^2 + D = 0$. Suppose that under the previous isomorphism the Rosati involution is given by $\varphi' = \mu^{-1}\overline{\varphi}\mu$ for all $\varphi \in \mathcal{O}$, where the bar denotes the canonical involution on the quaternion algebra. Suppose also that the polarized order $(\mathcal{O}, \mu)$ is twisting and let $m \mid D$ such that $\mathcal{B} \simeq (-D, m)_{\mathbb{Q}}$. Then there exist elements ω_m and $\omega_{D/m}$ belonging to $\mathcal{O}$ such that $\mu\omega_m = -\omega_m\mu$ and $\mu\omega_{D/m} = -\omega_{D/m}\mu$, with the property that*

1. *$\omega_m^2 = m$ and $\omega_{D/m}^2 = D/m$,*
2. *$k_{\mathbb{Z}[\omega_m]}$ and $k_{\mathbb{Z}[\omega_{D/m}]}$ are at most quadratic extensions of k_C,*
3. *$k_{\mathcal{O}} = k_{\mathbb{Z}[\omega_m]} \cdot k_{\mathbb{Z}[\omega_{D/m}]}$.*

Let C be a curve as in the previous theorem (in particular we continue with the same notation for the elements μ, ω_m and $\omega_{D/m}$), and let B be

its Jacobian. For each $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/k_C)$ the isomorphism ${}^{\sigma}C \simeq C$ induces an isomorphism of polarized abelian surfaces $\phi_\sigma \colon {}^{\sigma}B \to B$. In particular, ϕ_σ is an isogeny, but it is not guaranteed to be a compatible one. In any case, the following proposition tells us that there exists some compatible isogeny.

Proposition 7.4. *Let $B/\overline{\mathbb{Q}}$ be an abelian variety whose algebra of endomorphisms is a central simple $\mathbb{Q}$-algebra. Let $\sigma \in G_{\mathbb{Q}}$. If ${}^{\sigma}B$ and B are isogenous then there exists a compatible isogeny ${}^{\sigma}B \to B$.*

Proof. Call $\mathcal{D}$ the algebra $\mathrm{End}_{\overline{\mathbb{Q}}}(B) \otimes_{\mathbb{Z}} \mathbb{Q}$, and let $\phi_\sigma \colon {}^{\sigma}B \to B$ be an isogeny. The map $\varphi \mapsto \phi_\sigma \circ {}^{\sigma}\varphi \circ \phi_\sigma^{-1}$ is a $\mathbb{Q}$-algebra automorphism of $\mathcal{D}$ since it fixes the center, which is $\mathbb{Q}$ by hypothesis. Then the Skolem-Noether Theorem implies that it is inner; that is, there exists an element $\psi_\sigma \in \mathcal{D}$ such that $\phi_\sigma \circ {}^{\sigma}\varphi \circ \phi_\sigma^{-1} = \psi_\sigma^{-1} \circ \varphi \circ \psi_\sigma$. The isogeny $\mu_\sigma = \psi_\sigma \circ \phi_\sigma$ is compatible. □

Recall that the degree of a compatible isogeny μ_σ is defined to be $d(\mu_\sigma) = \mu_\sigma \circ {}^{\sigma}\rho \circ \hat{\mu}_\sigma \circ \rho$ (cf. Section 3.3), which in our case can be identified with a rational number since the center of $\mathcal{B}$ is equal to $\mathbb{Q}$. The map

$$\begin{array}{rccc} d\colon & \mathrm{Gal}(\overline{\mathbb{Q}}/k_C) & \to & \mathbb{Q}^\times/\{\pm 1\}\mathbb{Q}^{\times 2} \\ & \sigma & \mapsto & d(\mu_\sigma)\cdot\{\pm 1\}\mathbb{Q}^{\times 2} \end{array}$$

is a homomorphism, and it gives the degree component $\overline{[c_B]}$ of $[c_B]$ under the isomorphism

$$H^2(G_{k_{\mathcal{C}}}, \mathbb{Q}^\times)[2] \simeq H^2(G_{k_{\mathcal{C}}}, \{\pm 1\}) \times \mathrm{Hom}(G_{k_{\mathcal{C}}}, \mathbb{Q}^\times/\{\pm 1\}\mathbb{Q}^{\times 2}) \tag{7.1}$$

of Proposition 3.22. Recall also that in Section 3.3 we introduced the following notation to indicate elements of $\mathrm{Hom}(G_{k_{\mathcal{C}}}, \mathbb{Q}^\times/\{\pm 1\}\mathbb{Q}^{\times 2})$: if $t \in k_C$ and $e \in \mathbb{Q}^\times$ we denote by $(t,e)_P$ the homomorphism that sends an element $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/k_C)$ to $e \cdot \{\pm 1\}\mathbb{Q}^{\times 2}$ if and only if ${}^{\sigma}\sqrt{t} = -\sqrt{t}$.

Proposition 7.5. *Let C be a curve as in Theorem 7.3, and let d be the degree map associated to its Jacobian B. Then $d(\sigma) \equiv 1 \mod \{\pm 1\}\mathbb{Q}^{\times 2}$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/k_{\mathcal{O}})$. If h belongs to $\{m, D/m\}$ and $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/k_{\mathbb{Z}[\omega_h]})$ does not fix $k_{\mathcal{O}}$, then $d(\sigma) \equiv h \mod \{\pm 1\}\mathbb{Q}^{\times 2}$.*

Proof. If $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/k_{\mathcal{O}})$, by the definition of $k_{\mathcal{O}}$ there exists a compatible isomorphism $\phi_\sigma \colon {}^{\sigma}B \to B$ such that $\phi_\sigma^*(\rho) = {}^{\sigma}\rho$, where ρ is the polarization of B given by C. Applying the definition of d we find that

$$d(\phi_\sigma) = \phi_\sigma \circ {}^{\sigma}\rho^{-1} \circ \hat{\phi}_\sigma \circ \rho = \phi_\sigma \circ \phi_\sigma^{-1} \circ \rho^{-1} \circ \hat{\phi}_\sigma^{-1} \circ \hat{\phi}_\sigma \circ \rho = 1.$$

Let σ be an element in $\mathrm{Gal}(\overline{\mathbb{Q}}/k_{\mathbb{Z}[\omega_h]})$ that does not fix $k_{\mathcal{O}}$. By the definition of $k_{\mathbb{Z}[\omega_h]}$ there exists an isomorphism $\phi_\sigma \colon {}^{\sigma}B \to B$ compatible with the endomorphisms in $\mathbb{Z}[\omega_h]$, but not necessarily compatible with all the endomorphisms. However, we know from Proposition 7.4 that we can find $\psi_\sigma \in \mathcal{B}$ such that $\mu_\sigma = \psi_\sigma \circ \phi_\sigma$ is a compatible isogeny. From the proof of Proposition 7.4 we see that ψ_σ is characterized by the property that $\phi_\sigma \circ {}^{\sigma}\varphi \circ \phi_\sigma^{-1} = \psi_\sigma^{-1} \circ \varphi \circ \psi_\sigma$ for all $\varphi \in \mathcal{B}$. But if we take $\varphi \in \mathbb{Z}[\omega_h]$, this particularizes to $\varphi = \psi_\sigma^{-1} \circ \varphi \circ \psi_\sigma$, so ψ_σ commutes with every element in

$\mathbb{Z}[\omega_h]$, which implies that ψ_σ belongs to $\mathbb{Z}[\omega_h] \otimes \mathbb{Q}$. Hence, we have that $\psi_\sigma = a + b\omega_h$ for some $a, b \in \mathbb{Q}$. In fact, $b \neq 0$ because otherwise the isomorphism ψ_σ would be compatible with all the endomorphisms of B, and this is not the case since we are assuming that σ does not fix $k_{\mathcal{O}}$. Using the definition of $d(\mu_\sigma)$ we see that

$$\begin{aligned} d(\mu_\sigma) &= d(\psi_\sigma \circ \phi_\sigma) = \psi_\sigma \circ \phi_\sigma \circ {}^\sigma\rho^{-1} \circ \widehat{\psi_\sigma \circ \phi_\sigma} \circ \rho \\ &= \psi_\sigma \circ \phi_\sigma \circ \phi_\sigma^{-1} \circ \rho^{-1} \circ \hat{\phi}_\sigma^{-1} \circ \hat{\phi}_\sigma \circ \hat{\psi}_\sigma \circ \rho \\ &= \psi_\sigma \circ \rho^{-1} \circ \hat{\psi}_\sigma \circ \rho = \psi_\sigma \circ \psi'_\sigma. \end{aligned}$$

Now we know that the Rosati involution of an element $\varphi \in \mathcal{B}$ is given by $\varphi' = \mu^{-1}\overline{\varphi}\mu$. Hence,

$$\begin{aligned} d(\mu_\sigma) &= \psi_\sigma \circ \psi'_\sigma = (a + b\omega_h)(a + b\omega_h)' = (a + b\omega_h)\mu^{-1}(a - b\omega_h)\mu \\ &= (a + b\omega_h)^2 = a + hb^2 + 2ab\omega_h, \end{aligned}$$

and since $d(\mu_\sigma)$ must lie in $\mathbb{Q}^\times$ and $b \neq 0$, we see that $a = 0$ and $d(\mu_\sigma) \equiv h \pmod{\mathbb{Q}^{\times 2}}$. □

Suppose now that $k_C = \mathbb{Q}$. Then we can give also a description of the sign component $[c_B]_\pm$. The explicit expression for the two components of $[c_B]$ under (7.1) is the following.

Proposition 7.6. *Suppose that $k_C = \mathbb{Q}$, and let $k_{\mathbb{Z}[\omega_h]} = \mathbb{Q}(\sqrt{t_h})$ for $h \in \{m, D/m\}$. The degree and sign components of $[c_B]$ are given by*

$$\overline{[c_B]} = (t_m, D/m)_P \cdot (t_{D/m}, m)_P, \tag{7.2}$$

$$[c_B]_\pm = (t_m, D/m)_{\mathbb{Q}} \cdot (t_{D/m}, m)_{\mathbb{Q}} \cdot (-D, m)_{\mathbb{Q}}. \tag{7.3}$$

Proof. The expression for the degree component follows from Proposition 7.5. First of all, the degree homomorphism d is the inflation of a homomorphism from $\mathrm{Gal}(k_{\mathcal{O}}/\mathbb{Q})$, and we know that $k_{\mathcal{O}} = \mathbb{Q}(\sqrt{t_m}, \sqrt{t_{D/m}})$ (note that we are not assuming this to be a degree 4 extension). Let $\sigma \in \mathrm{Gal}(k_{\mathcal{O}}/k_{\mathbb{Z}[\omega_m]})$ that does not fix $k_{\mathcal{O}}$; then it restricts to a generator of $\mathrm{Gal}(\mathbb{Q}(\sqrt{t_{D/m}})/\mathbb{Q})$, and as we have seen $d(\sigma) \equiv m \mod \{\pm 1\}\mathbb{Q}^{\times 2}$. This gives the part $(t_{D/m}, m)_P$ of the degree homomorphism. In the same way we obtain the part $(t_m, D/m)_P$.

Now, to prove the identity (7.3) we use [**Qu09**, Theorem 2.8], which gives a formula for the Brauer class of the endomorphism algebra of a building block. Specialized to our case, and having computed the degree component, this formula gives

$$(-D, m)_{\mathbb{Q}} = [c_B]_\pm \cdot (t_m, D/m)_{\mathbb{Q}} \cdot (t_{D/m}, m)_{\mathbb{Q}},$$

and from this (7.3) follows since quaternion algebras have order dividing 2 in the Brauer group. □

7.2. A family of QM Jacobian surfaces

Let $\mathcal{B}_6 = (2,3)_{\mathbb{Q}}$ be the rational quaternion algebra of discriminant 6. Let $\imath, \jmath$ be the elements in $\mathcal{B}_6$ such that $\imath^2 = 2$ and $\jmath^2 = 3$, and let $\mu = 2\jmath + \imath\jmath$. The order $\mathcal{O} = \mathbb{Z}[\imath, (1+\jmath)/2]$ is maximal, $(\mathcal{O}, \mu)$ is principally polarized and the elements $\omega_2 = \imath$ and $\omega_3 = \jmath + \imath\jmath$ are twists of $(\mathcal{O}, \mu)$. For ease of notation, we define the subrings $R_2 = \mathbb{Z}[\imath] \simeq \mathbb{Z}[\sqrt{2}]$, $R_3 = \mathbb{Z}[\jmath + \imath\jmath] \simeq \mathbb{Z}[\sqrt{3}]$ and $R_6 = \mathbb{Z}[\mu] \simeq \mathbb{Z}[\sqrt{-6}]$.

The family of surfaces we are going to consider is the following. For every algebraic number $j \in \overline{\mathbb{Q}}$ let C_j be the genus 2 curve with equation

$$
\begin{aligned}
C_j\colon \quad Y^2 = {} & \left(-4 + 3\sqrt{-6j}\right) X^6 - 12(27j+16)X^5 \\
& - 6\,(27j+16)\left(28 + 9\sqrt{-6j}\right) X^4 \\
& + 16(27j+16)^2 X^3 + 12(27j+16)^2\left(28 - 9\sqrt{-6j}\right) X^2 \\
& - 48(27j+16)^3 X + 8(27j+16)^3\left(4 + 3\sqrt{-6j}\right).
\end{aligned} \tag{7.4}
$$

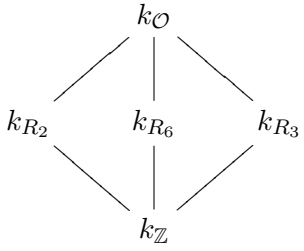
Let $B_j = \mathrm{Jac}(C_j)$ be its Jacobian equipped with the canonical principal polarization induced by C_j. Some properties of these objects proved in [**BG08**] are summarized in the following statement.

Proposition 7.7 (Baba-Granath)**.**

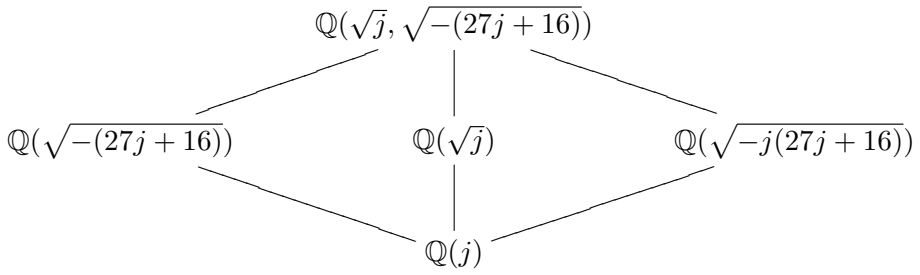
- *The curve C_j has field of moduli $\mathbb{Q}(j)$. For every $\sigma \in G_{\mathbb{Q}(j)}$ such that ${}^{\sigma}\sqrt{-6j} = -\sqrt{-6j}$ the map*

$$(x, y) \mapsto \left(\frac{-2(27j+16)}{x}, \frac{y(-2(27j+16))^{3/2}}{x^3}\right)$$

  is an isomorphism ${}^{\sigma}C_j \to C_j$.
- *The field $\mathbb{Q}(\sqrt{-6j}) \cdot k_{\mathcal{O}}$ is a field of definition of the endomorphisms of B_j.*
- *The curves C_j are QM-curves with respect to $\mathcal{O}$. Moreover, for all $j \in \mathbb{Q}$ except 26 values, $\mathrm{End}^0_{\overline{\mathbb{Q}}}(B_j) \simeq \mathcal{B}_6$. Under this isomorphism the Rosati involution $'$ attached to the canonical polarization of B_j is given by $\varphi' = \mu^{-1}\overline{\varphi}\mu$, where the bar indicates the canonical conjugation of $\mathcal{B}_6$.*
- *The diagram of fields of moduli*



for the canonically polarized jacobian B_j is the following one:



Hence, we see that if j is a rational number and the endomorphism algebra of B_j is isomorphic to $\mathcal{B}_6$, then B_j is a building block completely defined over the field

$$K = \mathbb{Q}(\sqrt{-6j}, \sqrt{j}, \sqrt{-(27j+16)}, \sqrt{-2(27j+16)}).$$

From now on we assume that j is a rational number and that $\mathrm{End}^0_{\overline{\mathbb{Q}}}(B_j) \simeq \mathcal{B}_6$. Now we can use Proposition 7.6 to compute the cohomology class $[c_{B_j}]$.

Proposition 7.8. *The sign and degree components of $[c_{B_j}]$ are given by*

$$\overline{[c_{B_j}]} = (-(27j+16), 3)_P \cdot (-j(27j+16), 2)_P, \tag{7.5}$$

$$[c_{B_j}]_{\pm} = (-(27j+16), 3)_{\mathbb{Q}} \cdot (-j(27j+16), 2)_{\mathbb{Q}} \cdot (2, 3)_{\mathbb{Q}}. \tag{7.6}$$

Proof. It follows immediately from Proposition 7.6, because Proposition 7.7 tells us that for this family of curves $t_2 = -(27j+16)$ and $t_3 = -j(27j+16)$. □

7.3. Cohomology classes of twisted Jacobians

Since we will need quadratic twists later, in this section we include a technical lemma describing the effect of such twists in the cohomology classes of interest. For every abelian variety B/K over a number field K and element $\gamma \in K^\times$ let B_γ denote the $K(\sqrt{\gamma})$-quadratic twist of the variety B over K. In the standard classification of twists by elements of the first Galois cohomology group with values in the automorphism group of the object, this variety corresponds to the morphism of $H^1(G_K, \{\pm 1\})$ whose kernel has $K(\sqrt{\gamma})$ as its fixed field, which is given by the formula $\sigma \mapsto {}^\sigma\sqrt{\gamma}/\sqrt{\gamma}$. Note that here we interpret ± 1 as automorphisms of B. In other words, B_γ is the abelian variety determined up to K-isomorphism by the fact that there exists an isomorphism $\phi\colon B_\gamma \to B$ defined over $K(\sqrt{\gamma})$ such that $\phi \circ {}^\sigma\phi^{-1} = {}^\sigma\sqrt{\gamma}/\sqrt{\gamma}$ for every $\sigma \in G_K$.

For hyperelliptic jacobians the quadratic twists are easily computed: if C is a hyperelliptic curve defined by the equation $Y^2 = F(X)$ then for every $\gamma \in K^\times$ the equation $\gamma Y^2 = F(X)$ defines an hyperelliptic curve that is the $K(\sqrt{\gamma})$-quadratic twist of C over K. The Jacobian $\mathrm{Jac}(\mathrm{B}_\gamma)$ is the $K(\sqrt{\gamma})$-quadratic twist of the abelian variety $\mathrm{Jac}(B)$ over K.

Lemma 7.9. *Let B/K be a $\mathbb{Q}$-variety completely defined over a Galois number field K, and let $\gamma \in K^\times$. The twist B_γ is completely defined over K if and only if the field $K(\sqrt{\gamma})$ is Galois over $\mathbb{Q}$. In this case $[c_{B/K}]$ and $[c_{B_\gamma/K}]$ differ by the cohomology class in $H^2(K/\mathbb{Q}, \{\pm 1\})$ corresponding to the group extension*

$$1 \longrightarrow \mathrm{Gal}(K(\sqrt{\gamma})/K) \longrightarrow \mathrm{Gal}(K(\sqrt{\gamma})/\mathbb{Q}) \longrightarrow \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow 1 \tag{7.7}$$

under the identification $\mathrm{Gal}(K(\sqrt{\gamma})/K) \simeq \{\pm 1\}$.

Proof. Note that the cohomology classes $[c_{B/K}]$ and $[c_{B_\gamma/K}]$ we want to compare take values in groups $F^\times$ consisting of automorphisms of the varieties; the cohomology class attached to the group extension of the statement takes values in the group $\{\pm 1\}$, which must be identified with a subgroup of $F^\times$ by the (canonical) identification of its elements as automorphisms of the variety. In particular, we see that quadratic twisting only affects the sign components of the cohomology classes and leaves the degree components unchanged.

Let $\phi\colon B_\gamma \to B$ be the isomorphism corresponding to the twist. Then ϕ^{-1} is an isomorphism giving B as the $K(\sqrt{\gamma})$-twist of B_γ and for every $\sigma \in G_\mathbb{Q}$ the map ${}^\sigma\phi\colon {}^\sigma(B_\gamma) \to {}^\sigma B$ is an isomorphism giving ${}^\sigma(B_\gamma)$ as the $K(\sqrt{\sigma\gamma})$-twist of ${}^\sigma B$. Every compatible isogeny $\nu_\sigma\colon {}^\sigma B_\gamma \to B_\gamma$ is of the form $\nu_\sigma = \phi^{-1} \circ \mu_\sigma \circ {}^\sigma\phi$ for a compatible isogeny $\mu_\sigma\colon {}^\sigma B \to B$ which by hypothesis is defined over K. For $\tau \in G_K$ one has

$${}^\tau\nu_\sigma = {}^\tau\phi^{-1} \circ {}^\tau\mu_\sigma \circ {}^{\tau\sigma}\phi = {}^\tau\phi^{-1} \circ \phi \circ \nu_\sigma \circ {}^\sigma\phi^{-1} \circ {}^{\tau\sigma}\phi = \frac{\sqrt{\gamma}}{{}^\tau\sqrt{\gamma}} \circ \nu_\sigma \circ \frac{\sqrt{\sigma\gamma}}{{}^\tau\sqrt{\sigma\gamma}}$$

which equals ν_σ if and only if the two other maps, each one equal to ± 1, coincide. But

$$\frac{\sqrt{\gamma}}{{}^\tau\sqrt{\gamma}} = \frac{\sqrt{\sigma\gamma}}{{}^\tau\sqrt{\sigma\gamma}} \quad \Leftrightarrow \quad \frac{\sqrt{\gamma}}{\sqrt{\sigma\gamma}} = \frac{{}^\tau\sqrt{\gamma}}{{}^\tau\sqrt{\sigma\gamma}} \quad \Leftrightarrow \quad \tau \ \text{ fixes } \ \sqrt{\sigma\gamma}/\sqrt{\gamma}.$$

Hence the isogeny ν_σ is defined over K if and only if $\sqrt{\sigma\gamma}/\sqrt{\gamma}$ belongs to K, and this condition is satisfied for every $\sigma \in G_\mathbb{Q}$ exactly when the extension $K(\sqrt{\gamma})/\mathbb{Q}$ is Galois.

Now assume the condition satisfied. For each $s \in \mathrm{Gal}(K/\mathbb{Q})$ fix a a lift $\tilde{s}$ of s in $\mathrm{Gal}(K(\sqrt{\gamma})/\mathbb{Q})$. Then

$$\begin{aligned}
c_{B_\gamma/K}(s,t) &= \nu_{\tilde{s}} \circ {}^{\tilde{s}}\nu_{\tilde{t}} \circ \nu_{\widetilde{st}}^{-1} = \phi^{-1} \circ \mu_{\tilde{s}} \circ {}^{\tilde{s}}\phi \circ {}^{\tilde{s}}\phi^{-1} \circ {}^{\tilde{s}}\mu_{\tilde{t}} \circ {}^{\tilde{s}\tilde{t}}\phi \circ {}^{\widetilde{st}}\phi^{-1} \circ \mu_{\widetilde{st}}^{-1} \circ \phi \\
&= \phi^{-1} \circ \mu_{\tilde{s}} \circ {}^{\tilde{s}}\mu_{\tilde{t}} \circ {}^{\widetilde{st}}\big({}^{\widetilde{st}^{-1}\tilde{s}\tilde{t}}\phi \circ \phi^{-1}\big) \circ \mu_{\widetilde{st}}^{-1} \circ \phi \\
&= \phi^{-1} \circ \mu_{\tilde{s}} \circ {}^{\tilde{s}}\mu_{\tilde{t}} \circ \mu_{\widetilde{st}}^{-1} \circ \phi \circ \big({}^{\widetilde{st}^{-1}\tilde{s}\tilde{t}}\phi \circ \phi^{-1}\big) \\
&= c_{B/K}(s,t) \circ \big({}^{\widetilde{st}^{-1}\tilde{s}\tilde{t}}\phi \circ \phi^{-1}\big) = c_{B/K}(s,t) \cdot \frac{{}^{\widetilde{st}^{-1}\tilde{s}\tilde{t}}\sqrt{\gamma}}{\sqrt{\gamma}},
\end{aligned}$$

and the factor in the right is a cocycle associated to the group extension (7.7). □

7.4. Explicit examples of strongly modular surfaces

Now we use the computations of the previous sections and the results of Chapter 6 to produce some concrete modular Jacobian surfaces. Observe that in order to determine whether an abelian variety B is strongly modular over a number field K or not, one has to check the symmetry of the cohomology class $[c_{B/K}]$. However, for the surfaces B_j we have not computed $[c_{B_j/K}] \in H^2(K/\mathbb{Q}, \mathbb{Q}^\times)$, but only their inflations $[c_{B_j}] \in H^2(G_\mathbb{Q}, \mathbb{Q}^\times)$. For each particular value of j, one can use the knowledge of $[c_{B_j}]$, the structure of $H^2(K/\mathbb{Q}, \{\pm 1\})$ and the computation of some local factors of $L(B_j/K; s)$ to decide the symmetry of $[c_{B/K}]$. As a previous step in this direction, we recall some facts about the group $H^2(K/\mathbb{Q}, \{\pm 1\})$ for polyquadratic number fields K. The reader can consult [**Qu01**, Section 2] for the details, also in a more general situation.

The structure of $H^2(K/\mathbb{Q}, \{\pm 1\})$. Let $K/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^n$. By Kummer theory $K = \mathbb{Q}(\sqrt{S})$, where $S = \{s_1, \cdots, s_n\}$ is a subset of $\mathbb{Q}$. For each $s \in S$, let $\chi_s \colon G \to \{0, 1\}$ be the character given by ${}^\sigma(\sqrt{s}) = (-1)^{\chi_s(\sigma)}\sqrt{s}$. Given $s, t \in S$, let $c_{s,t}$ be the map $\mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(K/\mathbb{Q}) \to \{\pm 1\}$ given by

$$c_{s,t}(\sigma, \tau) = (-1)^{\chi_s(\sigma)\chi_t(\tau)}, \qquad \sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q}).$$

This map $c_{s,t}$ is a 2-cocycle of $\mathrm{Gal}(K/\mathbb{Q})$ with values in $\{\pm 1\}$, and its inflation to $G_\mathbb{Q}$ corresponds to the quaternion algebra $(s, t)_\mathbb{Q}$, under the isomorphism of $H^2(G_\mathbb{Q}, \{\pm 1\})$ with the 2-torsion of the Brauer group of $\mathbb{Q}$.

Let $\varepsilon \colon \mathrm{Gal}(K/\mathbb{Q}) \to \{\pm 1\}$ be a character, and for each $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ fix a square root $\sqrt{\varepsilon(\sigma)}$. Then the map $c_\varepsilon \colon \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(K/\mathbb{Q}) \to \{\pm 1\}$ given by

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

is a two cocycle of $\mathrm{Gal}(K/\mathbb{Q})$ with values in $\{\pm 1\}$. For each $s \in S$, we have the character $\varepsilon_s \colon \mathrm{Gal}(K/\mathbb{Q}) \to \{\pm 1\}$ whose kernel is $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{s}))$. The inflation of c_{ε_s} to $G_\mathbb{Q}$ is the quaternion algebra $(s, -1)_\mathbb{Q}$.

The following proposition gives a basis for $H^2(K/\mathbb{Q}, \{\pm 1\})$ in terms of the cocycles $c_{s,t}$ and c_{ε_s}; it also characterizes the symmetric cocycles.

Proposition 7.10. *The set*

$$\{[c_{\varepsilon_s}]\}_{s \in S} \bigcup \{[c_{s,t}]\}_{s,t \in S,\ s \neq t}$$

is a $\mathbb{Z}/2\mathbb{Z}$-basis of $H^2(K/\mathbb{Q}, \{\pm 1\})$. Moreover, a cohomology class $[c]$ belongs to $\mathrm{Ext}(K/\mathbb{Q}, \mathbb{Q}^\times)$ if and only if its expression in the above basis only involves elements of the form $[c_{\varepsilon_s}]$.

A concrete example: $j = 1/81$. Let us now consider the example corresponding to this value of the parameter; let $C = C_j$ and $B = \mathrm{Jac}(C)$. Note that $\mathrm{End}^0_{\mathbb{Q}}(B) \simeq \mathcal{B}_6$ since $j = 1/81$ is not in the list of CM points listed in [**BG08**]. Then B is a building block completely defined over $K = \mathbb{Q}(\sqrt{-6}, \sqrt{-3})$ and it is strongly modular over K if and only if $[c_{B/K}]$ lies in $\mathrm{Ext}(K/\mathbb{Q}, \mathbb{Q}^\times)$; that is, if and only if it can be represented by a symmetric cocycle. In fact, since the degree component is always symmetric (over an abelian extension) we need to check this property only for the sign component $[c_{B/K}]_\pm \in H^2(K/\mathbb{Q}, \{\pm 1\})$.

For $s = -3, -6$ we denote by ε_s the non-trivial character

$$\varepsilon_s \colon \mathrm{Gal}(\mathbb{Q}(\sqrt{s})/\mathbb{Q}) \to \{\pm 1\}.$$

The group $H^2(K/\mathbb{Q}, \{\pm 1\})$ admits a basis as a $\mathbb{Z}/2\mathbb{Z}$-vector space consisting on the classes the 2-cocycles $c_{\varepsilon_{-6}}$, $c_{\varepsilon_{-3}}$ and $c_{-6,-3}$. Hence, we have that

$$[c_{B/K}]_\pm = [c_{\varepsilon_{-6}}]^u \cdot [c_{\varepsilon_{-3}}]^v \cdot [c_{-6,-3}]^w \tag{7.8}$$

for some $u, v, w \in \{0, 1\}$, and $[c_{B/K}]$ belongs to $\mathrm{Ext}(K/\mathbb{Q}, \{\pm 1\})$ if and only if $w = 0$. We know that $\mathrm{Inf}[c_{B/K}]_\pm = [c_B]_\pm$, which turns out to be trivial in this case by the expression (7.6). Since

$$\mathrm{Inf}[c_{\varepsilon_{-6}}] = (-6, -1)_{\mathbb{Q}},\ \mathrm{Inf}[c_{\varepsilon_{-3}}] = (-3, -1)_{\mathbb{Q}} \text{ and } \mathrm{Inf}[c_{-6,-3}] = (-6, -3)_{\mathbb{Q}},$$

the only possibilities we can have in (7.8) are $u = v = w = 0$ or $u = v = 1$, $w = 0$. In both cases $w = 0$, which implies that $[c_{B/K}]_\pm$ belongs to $\mathrm{Ext}(K/\mathbb{Q}, \{\pm 1\})$ and therefore B is strongly modular over K.

The formula (7.5) particularized to $j = 1/81$ gives that $\overline{[c_B]} = (-3, 6)_P$. Let $\xi_1, \xi_2 \in H^2(K/\mathbb{Q}, \mathbb{Q}^\times)$ be the cohomology classes with degree component $\overline{\xi}_1 = \overline{\xi}_2 = (-3, 6)_P$ and sign component $\xi_{1\pm} = 1$, $\xi_{2\pm} = [c_{\varepsilon_{-6}}] \cdot [c_{\varepsilon_{-3}}]$, and let $A = \mathrm{Res}_{K/\mathbb{Q}} B$. We have seen that either $[c_{B/K}] = \xi_1$ or $[c_{B/K}] = \xi_2$. By direct computation we see that

$$\mathbb{Q}^{\xi_1}[G] \simeq \mathbb{Q}(\sqrt{6}) \times \mathbb{Q}(\sqrt{6})$$

and

$$\mathbb{Q}^{\xi_2}[G] \simeq \mathbb{Q}(\sqrt{6}, \sqrt{-6}),$$

where $G = \mathrm{Gal}(K/\mathbb{Q})$. By Proposition 6.12 we see that if $[c_{B/K}] = \xi_1$ then $A \sim_{\mathbb{Q}} A_g^2 \times A_h^2$ for some newforms g and h with $\mathrm{End}^0_{\mathbb{Q}}(A_g) \simeq \mathrm{End}^0_{\mathbb{Q}}(A_h) \simeq \mathbb{Q}(\sqrt{6})$. On the other hand, if $[c_{B/K}] = \xi_2$ then $A \sim_{\mathbb{Q}} A_f^2$ for some newform f with $\mathrm{End}^0_{\mathbb{Q}}(A_f) \simeq \mathbb{Q}(\sqrt{6}, \sqrt{-6})$.

For a prime $\mathfrak{p}$ of K the local factor $L_{\mathfrak{p}}(B/K; T)$ can be computed by counting points in the reduction of C modulo $\mathfrak{p}$. In fact, to make the computations of the local factors of the L-series, what we have used is a function of `Magma` [**CB09**] that directly gives the zeta function of the reduction of C at $\mathfrak{p}$. If we call $\Psi_{\mathfrak{p}}(C; T)$ the numerator of such zeta

function, then $L_{\mathfrak{p}}(B/K;T) = (T^4\Psi_{\mathfrak{p}}(1/T))^{-1}$. We have then computed $L_p(A/\mathbb{Q};T) = L_p(B/K;T)$ as

$$L_p(B/K;T) = \prod_{\mathfrak{p}\,|\,p} L_{\mathfrak{p}}(B/K;T^{f(\mathfrak{p})}),$$

where $f(\mathfrak{p})$ is the residual degree. The results obtained for the first primes are the following.

p	$L_p(B/K;T)^{-1} = L_p(A/\mathbb{Q};T)^{-1}$
5	$(1-4T^2+5^2T^4)^4$
7	$(1-2T+7T^2)^8$
11	$(1-16T^2+11^2T^4)^4$
13	$(1-25T^2+13^2T^4)^4$
17	$(1-20T^2+17^2T^4)^4$
19	$(1-37T^2+19^2T^4)^4$
23	$(1+40T^2+23^2T^4)^4$
29	$(1-34T^2+29^2T^4)^4$
31	$(1-T+31T^2)^8$
37	$(1-10T^2+37^2T^4)^4$
41	$(1+58T^2+41^2T^4)^4$

We observe that some of these factors are of the form $(1+e_pT^2+p^2T^4)^4$, and if we had $A \sim_{\mathbb{Q}} A_g^2 \times A_h^2$ for some newforms $g = \sum b_n q^n$ and $h = \sum c_n q^n$ this would imply that

$$1 + e_pT^2 + p^2T^4 = (1 - b_pT + pT^2)(1 - {}^{\sigma}b_pT + pT^2),$$

with σ the non-trivial automorphism of $\mathbb{Q}(\sqrt{6})/\mathbb{Q}$, and a similar relation would hold for the coefficients c_p. But this relation implies that $b_p^2 = c_p^2 = 2p - e_p$, which is impossible for the computed values of e_p because then the coefficients b_p and c_p would not lie in $\mathbb{Q}(\sqrt{6})$. Therefore, the actual cohomology class is $[c_{B/K}] = \xi_2$ and $A \sim_{\mathbb{Q}} A_f^2$ for some newform $f = \sum a_n q^n$ with the a_n generating $\mathbb{Q}(\sqrt{6},\sqrt{-6})$. However, Proposition 3.18 tells us that there also exists a variety in the $\overline{\mathbb{Q}}$-isogeny class of B completely defined over K and with cohomology class ξ_1. We will find such a variety as the Jacobian of a quadratic twist of C.

Let $\gamma = 2-\sqrt{2}$. The extension $K(\sqrt{\gamma})/\mathbb{Q}$ is Galois, and an easy computation shows that the cohomology class associated to (7.7) in this particular case is $[c_{\varepsilon_{-6}}] \cdot [c_{\varepsilon_{-3}}]$. Hence, the variety B_γ is completely defined over K and $[c_{B_\gamma/K}] = [c_{B/K}] \cdot [c_{\varepsilon_{-6}}] \cdot [c_{\varepsilon_{-3}}] = \xi_1$. Arguing as before we see that $A_\gamma = \mathrm{Res}_{K/\mathbb{Q}} B_\gamma$ is $\mathbb{Q}$-isogenous to the square of a product of two modular abelian varieties with field of Fourier coefficients equal to $\mathbb{Q}(\sqrt{6})$. In $S_2(\Gamma_0(2^4\cdot 3^5))$ we find a newform with field of Fourier coefficients $\mathbb{Q}(\sqrt{6})$ and Fourier expansion

$$g = q + \sqrt{6}q^5 - 2q^7 + \sqrt{6}q^{11} - q^{13} + 3\sqrt{6}q^{17} + q^{19} - \sqrt{6}q^{23} + \dots$$

Let ε be the quadratic Dirichlet character of conductor 8 with $\varepsilon(3) = \varepsilon(5) = -1$, and let $h = g \otimes \varepsilon$ which is a newform in $S_2(\Gamma_0(2^6 \cdot 3^5))$. In the following table we list some local factors of the L-series corresponding to the varieties B_γ/K, $A_g/\mathbb{Q}$ and $A_h/\mathbb{Q}$.

p	$L_p(B_\gamma/K;T)^{-1}$	$L_p(A_g/\mathbb{Q};T)^{-1}$	$L_p(A_h/\mathbb{Q};T)^{-1}$
5	$(1+4T^2+5^2T^4)^4$	$(1+4T^2+5^2T^4)$	$(1+4T^2+5^2T^4)$
7	$(1+2T+7T^2)^8$	$(1+2T+7T^2)^2$	$(1+2T+7T^2)^2$
11	$(1+16T^2+11^2T^4)^4$	$(1+16T^2+11^2T^4)$	$(1+16T^2+11^2T^4)$
13	$(1-T+13T^2)^4(1+T+13T^2)^4$	$(1+T+13T^2)^2$	$(1-T+13T^2)^2$
17	$(1-20T^2+17^2T^4)^4$	$(1-20T^2+17^2T^4)$	$(1-20T^2+17^2T^4)$
19	$(1-T+19T^2)^4(1+T+19T^2)^4$	$(1-T+19T^2)^2$	$(1+T+19T^2)^2$
23	$(1+40T^2+23^2T^4)^4$	$(1+40T^2+23^2T^4)$	$(1+40T^2+23^2T^4)$
29	$(1+34T^2+29^2T^4)^4$	$(1+34T^2+29^2T^4)$	$(1+34T^2+29^2T^4)$
31	$(1-T+31T^2)^8$	$(1-T+31T^2)^2$	$(1-T+31T^2)^2$
37	$(1-8T+37T^2)^4(1+8T+37T^2)^4$	$(1-8T+37T^2)^2$	$(1+8T+37T^2)^2$
41	$(1+58T^2+41^2T^4)^4$	$(1+58T^2+41^2T^4)$	$(1+58T^2+41^2T^4)$

We have checked the equality of the local factors of the L-series of A_γ and $A_g^2 \times A_h^2$ for all primes $p < 1000$ ($p \neq 2, 3$) and this suggests that $A_\gamma \sim_{\mathbb{Q}} A_g^2 \times A_h^2$.

Comparing the local factors $L_p(B/K;T)$ and $L_p(B_\gamma/K;T)$ we can also find now a modular form f such that $A \sim_{\mathbb{Q}} A_f^2$ as a twist of g. More precisely, let ψ be the Dirichlet character of order 4 and conductor 16 such that $\psi(3) = -\sqrt{-1}$ and $\psi(5) = \sqrt{-1}$. The modular form $f = g \otimes \psi$ is a newform in $S_2(\Gamma_0(2^8 \cdot 3^5), \psi^2)$ and the local factors $L_p(B/K;T)$ and $L_p(A_f;T)^2$ coincide for all primes $p < 1000$ ($p \neq 2, 3$).

A concrete example: $j = -4/27$. We now consider another example, corresponding to the stated value of j. The jacobian B of the curve C_j is also a building block completely defined over $K = \mathbb{Q}(\sqrt{-6}, \sqrt{-3})$ and with $\mathrm{End}^0_{\overline{\mathbb{Q}}}(B) \simeq \mathcal{B}_6$. In this case B is not strongly modular over K. Indeed, a similar analysis of the possibilities for $[c_{B/K}]$ like the one we did in the previous example shows that in this case the only possibilities for $[c_{B/K}]_\pm$ have $w = 1$ in the expression (7.8), so $[c_{B/K}]_\pm$ is not symmetric because its component $[c_{-6,-3}]$ is not trivial. This means that no variety in the $\overline{\mathbb{Q}}$-isogeny class of B is strongly modular over K.

If we let for instance $L = K(\sqrt{-1})$ it is easy to see that there exist symmetric elements of $H^2(L/\mathbb{Q}, \{\pm 1\})$ whose inflation to $G_\mathbb{Q}$ is $[c_B]_\pm$, and then by Proposition 3.18 and Theorem 6.17 there exists a variety $\overline{\mathbb{Q}}$-isogenous to B completely defined and strongly modular over L. Indeed, consider the element $\gamma = \sqrt{6} + \sqrt{18} \in L$. The associated cocycle to the exact sequence (7.7) for this γ is $c_\gamma = c_{\varepsilon_{-1}} \cdot c_{\varepsilon_{-3}} \cdot c_{\varepsilon_{-6}} \cdot c_{-3,-6}$. This implies that $[c_{B_\gamma/L}]_\pm$ is symmetric, because its component $[c_{-3,-6}]$ vanishes. Therefore, B_γ is strongly modular over L. Computing the local factors of $L(B_\gamma/L;T)$ we

obtain

p	$L_p(B_\gamma/L;T)^{-1}$
5	$(1-7T^2+5^2T^4)^8$
11	$(1-5T^2+11^2T^4)^8$
13	$(1-T+13T^2)^8(1+T+13T^2)^8$
17	$(1-22T^2+17^2T^4)^8$
19	$(1-2T^2+19^2T^4)^8$
23	$(1+19T^2+23^2T^4)^8$
29	$(1+17T^2+29^2T^4)^8$
31	$(1-53T^2+31^2T^4)^8$
37	$(1-4T+37T^2)^8(1+4T+37T^2)^8$

Using `Magma` [**CB09**] one can find a modular form $f \in S_2(\Gamma_1(2^4\cdot 3^4),\chi)$, where χ is the quadratic character of conductor 12, whose Fourier expansion begins with

$$\begin{aligned} f &= q-\sqrt{3}\,q^5+3\sqrt{-1}\,q^7-3\sqrt{3}\,q^{11}+q^{13}-2\sqrt{-3}\,q^{17}-6\sqrt{-1}\,q^{19} \\ &+ 3\sqrt{3}\,q^{23}+2\,q^{25}-5\sqrt{-3}\,q^{29}-3\sqrt{-1}\,q^{31}+\cdots, \end{aligned}$$

and a modular form $g \in S_2(\Gamma_1(2^6\cdot 3^4),\chi)$ whose Fourier expansion begins with

$$\begin{aligned} g &= q-\sqrt{3}\,q^5+3\sqrt{-1}\,q^7-3\sqrt{3}\,q^{11}-q^{13}+2\sqrt{-3}\,q^{17}+6\sqrt{-1}\,q^{19} \\ &- 3\sqrt{3}\,q^{23}+2\,q^{25}-5\sqrt{-3}\,q^{29}-3\sqrt{-1}\,q^{31}+\cdots. \end{aligned}$$

These forms f and g satisfy that

$$L_p(B_\gamma/L;T) = L_p(A_f;T)^2\cdot L_p(A_g;T)^2$$

for all primes $p<1000$, $p\neq 2,3$. This suggests that, in fact, one has the following equivalence of L-series

$$L(B_\gamma/L;s) \sim L(A_f;s)^2\cdot L(A_g;s)^2$$

and therefore that

$$\mathrm{Res}_{L/\mathbb{Q}}\, B_\gamma \sim_{\mathbb{Q}} A_f^2\times A_g^2.$$

Thus, in this case we have seen that it is enough to go to a quadratic extension L of K to find a variety in the $\overline{\mathbb{Q}}$-isogeny class of B that is strongly modular over L. However, in the family $\{B_j\}_{j\in\mathbb{Q}}$ we can find varieties where any minimal field L with this property is arbitrarily large. In fact, by Theorem 6.18, it is equivalent to find in this family varieties where the degree of any splitting field is arbitrarily large. We will see this by means of the following lemma.

Lemma 7.11. *Let $r\geqslant 2$ be an integer and let p be a prime such that $p\equiv 1 \pmod{2^r}$ and $p\equiv -1 \pmod 3$. Then the order of any splitting character for $B_{1/p}$ is at least 2^r.*

PROOF. For simplicity we call B the variety $B_{1/p}$, and let $[c_B]$ be its attached cohomology class. By (7.6) the sign component $[c_B]_\pm$ is given as the following product of quaternion algebras:

$$[c_B]_\pm = (-(27+16p)/p, 3)_{\mathbb{Q}} \cdot (-(27+16p), 2)_{\mathbb{Q}} \cdot (2,3)_{\mathbb{Q}}.$$

Applying the formulas for computing the local Hilbert Symbols at p we find that

$$(-(27+16p)/p, 3)_p = -1, \qquad (-(27+16p), 2)_p = 1, \qquad (2,3)_p = 1,$$

and this implies that the local component of $[c_B]_\pm$ at the prime p is -1. But $[c_B]_\pm = [c_\varepsilon]$, where ε is the splitting character associated to any splitting map β for B. We can identify ε with a primitive Dirichlet character of a certain conductor N, and if ε_p denotes the component of ε modulo the largest power of p dividing N, then the local component of $[c_\varepsilon]$ at p is given by $\varepsilon_p(-1)$. The value $\varepsilon_p(-1) = -1$ is taken by the characters of order multiple of $2^{\mathrm{ord}_2(p-1)}$, and it follows that $\mathrm{ord}(\varepsilon) \geqslant \mathrm{ord}(\varepsilon_p) \geqslant 2^{\mathrm{ord}_2(p-1)}$, which is at least 2^r by our choice of p. □

Proposition 7.12. *For any integer r there exists a variety B in the family $\{B_j\}_{j\in\mathbb{Q}}$ such that any splitting field for B has degree at least 2^r.*

PROOF. Take a prime p as in the previous lemma, and take as B the variety $B_{1/p}$. Let β be any splitting map for B, and let ε be its associated splitting character. Then we have that $[K_\beta : \mathbb{Q}] \geqslant [K_\varepsilon : \mathbb{Q}] \geqslant 2^r$. □

From Lemma 7.11 we can derive another interesting consequence.

Proposition 7.13. *Let g be any natural number. There exist varieties B in the family $\{B_j\}_{j\in\mathbb{Q}}$ such that every $\mathbb{Q}$-simple abelian variety A of GL_2-type having B as its simple factor is of dimension $\dim A \geqslant g$.*

PROOF. Let r be an integer such that $\varphi(2^r) = 2^{r-1} \geqslant g$, and take $B = B_{1/p}$ with p a prime as in Lemma 7.11. If A is a simple abelian variety of GL_2-type that has B as its simple factor, the field $E = \mathrm{End}^0_{\mathbb{Q}}(A)$ is isomorphic to E_β for some splitting map β for B. The field E_β contains the values of the splitting character ε associated to β, hence contains the 2^rth cyclotomic extension, of degree $\varphi(2^r)$ over $\mathbb{Q}$, and we have that $\dim A = [E_\beta : \mathbb{Q}] \geqslant \varphi(2^r) \geqslant g$. □

Bibliography

[CF00] T. Chinburg, E. Friedman. *The finite subgroups of maximal arithmetic Kleinian groups.* Ann. Inst. Fourier Grenoble **50** (2000) 1765-1798.

[BG08] S. Baba, H. Granath. *Genus 2 curves with quaternionic multiplication.* Canad. J. Math. **60** (2008), no. 4, 734–757.

[CB09] J. J. Cannon, W. Bosma. (Eds.) *Handbook of Magma Functions*, Edition 2.15-13 (2009).

[Ch87] W. Chi. *Twists of central simple algebras and endomorphism algebras of some abelian varieties.* Math. Ann. **276** (1987), no. 4, 615–632.

[Cr97] J. Cremona. *Algorithms for modular elliptic curves.* Second edition, Cambridge University Press (1997). Available online at:
`www.warwick.ac.uk/~masgaj/book/fulltext/index.html`.

[Da00] H. Darmon. *Rigid local systems, Hilbert modular forms, and Fermat's last theorem.* Duke Math. J. **102** (2000), no. 3, 413–449.

[DJ09] L. Dieulefait, J. Jiménez-Urroz.*Solving Fermat-type equations via modular $\mathbb{Q}$-curves over polyquadratic fields.* J. Reine Angew. Math. **633** (2009), 183–195.

[DD97] P. Dèbes, J.-C. Douai. *Algebraic covers: field of moduli versus field of definition.* Ann. Sci. École Norm. Sup. (4) **30** (1997), no. 3, 303–338.

[DR05] L. V. Dieulefait, V. Rotger. *On abelian surfaces with potential quaternionic multiplication over $\mathbb{Q}$*, Bull. Belg. Math. Soc. 12:4, (2005) 617-624.

[Ell04] J. Ellenberg. *Galois representations attached to $\mathbb{Q}$-curves and the generalized Fermat equation $A^4 + B^2 = C^p$.* Amer. J. Math. **126** (2004), no. 4, 763–787.

[ES01] J. Ellenberg, C. Skinner. *On the modularity of $\mathbb{Q}$-curves.* Duke Math. J. **109** (2001), no. 1, 97–122.

[El02] N. Elkies. *On elliptic K-curves.* Modular curves and abelian varieties, Progress in Math., vol. 224 (2002), pp. 81–91.

[Fa86] G. Faltings. *Finiteness theorems for abelian varieties over number fields*; in: Arithmetic geometry, G. Cornell and J. H. Silverman (eds.), Springer, 1986, 9–27.

[GL98] J. González, J.-C. Lario. *Rational and elliptic parametrizations of $\mathbb{Q}$-curves.* J. Number Theory **72** (1998), no. 1, pp. 13–31.

[GL01] J. González, J.-C. Lario. *$\mathbb{Q}$-curves and the Manin ideal.* Amer. J. Math. **123** (2001), no. 3, pp. 475–503.

[GL] J. González, J.-C. Lario. *Modular elliptic directions with complex multiplication (with an application to Gross's elliptic curves).* Comment. Math. Helv. (To appear.)

[GM09] X. Guitart, S. Molina. *Parametrization of abelian K-surfaces with quaternionic multiplication.* C. R. Acad. Sci. Paris, Ser. I **347** (2009), 1325–1330.

[HM95] K.-I. Hashimoto, N. Murabayashi. *Shimura curves as intersections of Humbert surfaces and defining equations of QM-curves of genus two.* Tôhoku Math. J. **47** (1995), no. 2, pp. 272–295.

[HS00] M. Hindry, J. H. Silverman. *Diophantine geometry. An introduction.* Graduate Texts in Mathematics, **201**. Springer-Verlag, New York, 2000.

[Ka93] G. Karpilovski. *Group representations, vol. 2.* North-Holland Mathematics Studies, 177. North-Holland Publishing Co., Amsterdam, 1993.

[KW09] C. Khare, J-P. Wintenberger, *Serre's modularity conjecture. I.* Invent. Math. **178** (2009), no. 3, 485–504.

[Mi72] J. S. Milne. *On the arithmetic of abelian varieties.* Invent. Math. **17** (1972), 177–190.

[Mi86] J. S. Milne. *Abelian varieties.* Arithmetic geometry (Storrs, Conn., 1984), 103–150, Springer, New York, 1986.

[Mi06] J. S. Milne. *Complex Multiplication (v0.00).* Available at `www.jmilne.org/math`.

[Mi08] J. S. Milne. *Class Field Theory (v4.00).* Available at `www.jmilne.org/math`.

[MoGe] B. Moonen, G. van der Geer. *Abelian varieties* (preliminary version). Available at `http://staff.science.uva.nl/~bmoonen/boek/BookAV.html`

[Mu70] D. Mumford. *Abelian varieties.* Tata Institute of Fundamental Research Studies in Mathematics, No. 5 Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London 1970 viii+242 pp.

[Pi82] R. S. Pierce. *Associative Algebras.* Graduate Texts in Mathematics, 88. Studies in the History of Modern Science, 9. Springer-Verlag, New York-Berlin, 1982.

[Py02] E. Pyle. *Abelian varieties over $\mathbb{Q}$ with large endomorphism algebras and their simple components over $\overline{\mathbb{Q}}$.* Modular curves and abelian varieties, Progress in Math., vol. 224 (2002), pp. 189–239.

[Qu00] J. Quer. *$\mathbb{Q}$-curves and abelian varieties of GL_2-type.* Proc. London Math. Soc. **81** (2000) no. 2, pp. 285–317.

[Qu01] J. Quer. *Embedding problems over abelian groups and an application to elliptic curves.* J. Algebra **237** (2001), no. 1, pp. 186–202.

[Qu09] J. Quer. *Fields of definition of building blocks.* Math. Comp. **78** (2009), pp. 537–554.

[Ri80] K. A. Ribet. *Twists of modular forms and endomorphisms of abelian varieties.* Math. Ann. **253** (1980), no. 1, 43–62.

[Ri92] K. A. Ribet. *Abelian varieties over $\mathbb{Q}$ and modular forms.* Algebra and topology 1992 (Taejŏn), 53–79, Korea Adv. Inst. Sci. Tech., Taejŏn, 1992. Reprinted on *Modular curves and abelian varieties*, 241–261, Progr. Math. 224, Birkhäuser, Basel, 2004.

[Ri94] K. A. 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.

[Ro04] V. Rotger. *The field of moduli of quaternionic multiplication on abelian varieties.* Int. J. Math. Math. Sci. 2004, no. 49-52, 2795–2808.

[Se77] 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.

[Se79] J.-P. Serre. *Local Fields.* Graduate Texts in Mathematics, **67**. Springer-Verlag, New York-Berlin, 1979.

[Sh71] G. Shimura. *Introduction to the arithmetic theory of automorphic functions.* Publ. Math. Soc. Japan, vol. 11, Princeton University Press (1971).

[Sh72] G. Shimura. *Class fields over real quadratic fields and Hecke operators.* Ann. of Math. (2) **95** (1972), 130–190.

[St07] W. Stein. *Modular forms: A computational approach, with an appendix by Paul Gunnells.* AMS Graduate Studies in Mathematics, vol. 79. (2007).

[We56] A. Weil. *The field of definition of a variety.* Amer. J. Math. **78** (1956), 509524.

[We82] A. Weil. *Adeles and algebraic groups.* With appendices by M. Demazure and Takashi Ono. Progress in Mathematics, **23**. Birkhuser, Boston, Mass., 1982. iii+126 pp.