

**Abelian Varieties over $\mathbb{Q}$
with Large Endomorphism Algebras
and
Their Simple Components over $\overline{\mathbb{Q}}$**

Elisabeth Eve Pyle

B.S. (Stanford University) 1988

C.Phil. (University of California at Berkeley) 1992

A dissertation submitted in partial satisfaction of the requirements for the degree of

Doctor of Philosophy

in

Mathematics

in the

Graduate Division

of the

University of California at Berkeley

Committee in Charge:

Professor Kenneth A. Ribet, Chair

Professor Andrew P. Ogg

Professor Alan Schoenfeld

1995

Contents

Introduction	1
1 Abelian Varieties over $\mathbb{Q}$ of GL_2-type	4
2 The Brauer Class of $\mathrm{End}(B)$	12
3 The Tensor Product of a Module with an Abelian Variety	21
4 Descent from $\overline{\mathbb{Q}}$ to $\mathbb{Q}$	25
5 Fields of Definition for Building Blocks	35
6 An Example of a $\mathbb{Q}$-Curve	47
7 Further Questions	53
A A Non-Building Block	55
B Useful Facts Concerning Central Simple Algebras	62
Bibliography	64

Introduction

This dissertation expands upon the results of K. Ribet in [Ri 1] and [Ri 2] concerning abelian varieties “of $\mathbf{GL}_2$ -type”. An abelian variety $A/\mathbb{Q}$ is said to be of $\mathbf{GL}_2$ -type if its algebra of $\mathbb{Q}$ -endomorphisms $\mathbb{Q} \otimes \text{End}_{\mathbb{Q}}(A)$ is a number field E of degree equal to the dimension of A .

The study of abelian varieties of $\mathbf{GL}_2$ -type grew out of research surrounding the Taniyama-Shimura Conjecture. Recall that the usual statement of the Taniyama-Shimura Conjecture asserts that every elliptic curve over $\mathbb{Q}$ is a quotient of a modular curve of the form $X_0(M)$. Recent manuscripts circulated by Wiles and Taylor-Wiles prove the Taniyama-Shimura Conjecture for a large class of elliptic curves over $\mathbb{Q}$.

It is well known that an equivalent formulation of the Taniyama-Shimura Conjecture requires only that every elliptic curve over $\mathbb{Q}$ be a quotient of a standard modular curve of the form $X_1(N)$. Furthermore, in [Ma], B. Mazur proved the conjecture’s equivalence to yet another seemingly weaker statement: an elliptic curve over $\mathbb{Q}$ is a quotient over $\mathbb{Q}$ of some $X_1(N)$ if and only if it is a quotient over $\overline{\mathbb{Q}}$ of some $X_1(N)_{/\overline{\mathbb{Q}}}$.

Now every map from $X_1(N)$ to an elliptic curve sending ∞ to O extends uniquely to a map from its Jacobian $J_1(N)$ to the elliptic curve. Hence, this line of inquiry leads naturally to the (closely related) questions: how may we characterize those simple abelian varieties over $\mathbb{Q}$ (respectively, over $\overline{\mathbb{Q}}$) that appear as quotients of $J_1(N)$ (respectively, $J_1(N)_{/\overline{\mathbb{Q}}}$) for some $N \geq 1$? We will loosely use the word “modular” to refer to such abelian varieties.

In [Ri 1], Ribet gives a conjectural answer to one of these questions.

Conjecture. *A simple abelian variety A over $\mathbb{Q}$ is modular if and only if A is of $\mathbf{GL}_2$ -type.*

It is known that every simple quotient of $J_1(N)/\mathbb{Q}$ is of $\mathbf{GL}_2$ -type. Indeed, the primary source of examples of abelian varieties of $\mathbf{GL}_2$ -type is a construction resulting from

extensive work by Shimura on the subject [Sh 2, Sh 4]. Let $f = \sum a_n q^n$ be a normalized cuspidal eigenform of weight two on $\Gamma_1(N)$. Let E be the number field $\mathbb{Q}(\dots, a_n, \dots)$. Then Shimura constructs, as a quotient of $J_1(N)$, an abelian variety A_f over $\mathbb{Q}$ with the following properties: there is an action $E \xrightarrow{\sim} \mathbb{Q} \otimes \text{End}_{\mathbb{Q}}(A_f)$, and the dimension of A_f is equal to $[E:\mathbb{Q}]$. Moreover, every simple quotient of $J_1(N)/\mathbb{Q}$ is isogenous to an A_f constructed in this way.

Thus the conjecture is reduced to: all abelian varieties over $\mathbb{Q}$ of $\mathbf{GL}_2$ -type are isogenous to some A_f . In support of this assertion, Ribet has proved [Ri 1, Thm. 4.4] that if one assumes Serre's conjecture [Se 4, 3.2.4₂] about representations of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, then it follows that all abelian varieties over $\mathbb{Q}$ of $\mathbf{GL}_2$ -type are modular. (See also [Sh 1].)

Now in this dissertation, we look at the complete decomposition over $\overline{\mathbb{Q}}$ of abelian varieties of $\mathbf{GL}_2$ -type. We determine necessary and sufficient conditions for an abelian variety over $\overline{\mathbb{Q}}$ to be a simple component of an abelian variety over $\mathbb{Q}$ of $\mathbf{GL}_2$ -type; such abelian varieties will be called “building blocks”. These results enable us to restate the above conjecture as: a simple abelian variety B over $\overline{\mathbb{Q}}$ is modular if and only if B is a building block.

We would like to emphasize that the work contained herein deals exclusively with the properties of abelian varieties of $\mathbf{GL}_2$ -type, the properties of their component building blocks, and the relationships between these two kinds of abelian varieties, without any recourse to their possible “modular” structure.

In Chapter 1 we define our terminology and review the structure of abelian varieties over $\mathbb{Q}$ of $\mathbf{GL}_2$ -type. Chapter 2 contains a discussion of the Brauer class of the endomorphism algebra of a building block; it culminates in a theorem we will apply in Chapter 4. Chapter 3 is a short preparation of a category-theoretic construction that we will also use in Chapter 4.

Chapter 4 contains the bulk of the technical work; it describes the correspondence between building blocks over $\overline{\mathbb{Q}}$ and abelian varieties over $\mathbb{Q}$ of $\mathbf{GL}_2$ -type. Then Chapter 5 is a collection of further results, mostly connected to fields of definition for these abelian varieties and their endomorphisms. In Chapter 6 we illustrate the theory of Chapters 4 and 5 with explicit examples of a one-dimensional building block and an associated four-dimensional abelian variety of $\mathbf{GL}_2$ -type. Chapter 7 is a brief consideration of some unanswered questions and avenues for future work.

Finally there are two appendices. In the first, we construct a counterexample to

demonstrate the necessity of a certain condition we impose on building blocks. The second is a list of facts we quote from the theory of central simple algebras; we apply these theorems to the endomorphism algebras we encounter.

Notation

Throughout this dissertation we will work in the category of abelian varieties *up to isogeny*. That is the category whose objects are abelian varieties $A, B, \dots$ with morphisms $\mathbb{Q} \otimes \text{Hom}(A, B)$. In other words, we formally invert all isogenies $A \rightarrow B$. In this category, notation is simplified by writing $\text{Hom}(A, B)$ for $\mathbb{Q} \otimes \text{Hom}(A, B)$.

The endomorphism algebra $\text{Hom}(A, A)$ will be denoted $\text{End}(A)$, and the following variants of Hom will also apply to End .

If A and B are abelian varieties defined over a field K , then $\text{Hom}(A, B)$ will refer to *all* morphisms $A_{/\bar{K}} \rightarrow B_{/\bar{K}}$. If we wish to refer to only those morphisms defined over K , we will write $\text{Hom}_K(A, B)$.

In some cases, A and B may be equipped with an action of a ring $\mathcal{R}$; that is, there are fixed maps $\mathcal{R} \rightarrow \text{End}(A)$ and $\mathcal{R} \rightarrow \text{End}(B)$. A morphism $\varphi : A \rightarrow B$ will be said to “respect $\mathcal{R}$ ” (or “respect the actions of $\mathcal{R}$ ”, or “be compatible with $\mathcal{R}$ ”...) if $\varphi \circ r = r \circ \varphi$ for all $r \in \mathcal{R}$. The subgroup of morphisms that respect $\mathcal{R}$ will be denoted $\text{Hom}^{\mathcal{R}}(A, B)$.

We will write $Z(\mathcal{R})$ for the center of a ring $\mathcal{R}$.

The sign “ $\sim$ ” will designate the equivalence relation of isogeny.

The symbol $G_{\mathbb{Q}}$ will denote the absolute Galois group $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ with its usual profinite topology.

Acknowledgments

My warmest thanks go to my dissertation advisor, Ken Ribet, for all his helpful suggestions. Without his patient and continued support, this work would never have been realized.

This work was partially supported by NSF Grant #DMS 93-06898.

Chapter 1

Abelian Varieties over $\mathbb{Q}$ of $\mathbf{GL}_2$ -type

In this first chapter we will recapitulate many of the results from [Ri 1], on which we rely heavily in the remainder of this dissertation. Our approach differs from Ribet's in that it focuses not on ℓ -adic representations, but rather on the structure of endomorphism algebras as semi-simple $\mathbb{Q}$ -algebras. We remind the reader that for an abelian variety A , the notation $\text{End}(A)$ will always refer to the $\mathbb{Q}$ -algebra of endomorphisms of A .

Definition. An abelian variety $A/\mathbb{Q}$ is of $\mathbf{GL}_2$ -type if $\text{End}_{\mathbb{Q}}(A)$, the algebra of endomorphisms of A defined over $\mathbb{Q}$, is a number field of degree equal to the dimension of A .

Note that this definition applies only to abelian varieties defined over $\mathbb{Q}$, although we may not always say so explicitly; i.e., the phrase “ A is of $\mathbf{GL}_2$ -type” will imply that A is defined over $\mathbb{Q}$. Also note that abelian varieties of $\mathbf{GL}_2$ -type are always simple over $\mathbb{Q}$, which is a modification of the terminology in [Ri 1].

Why do we say these abelian varieties are “of $\mathbf{GL}_2$ -type”? If $A/\mathbb{Q}$ is an abelian variety such that $\text{End}_{\mathbb{Q}}(A)$ is a number field E with $[E:\mathbb{Q}] = \dim A$, then it is well known that for any prime ℓ , the Tate module $V_{\ell}(A)$ is free of rank two over $E \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell}$. Thus the action of the absolute Galois group $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = G_{\mathbb{Q}}$ on $V_{\ell}(A)$ defines a representation $G_{\mathbb{Q}} \rightarrow \mathbf{GL}_2(E \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell})$.

Abelian varieties of $\mathbf{GL}_2$ -type with complex multiplication over $\overline{\mathbb{Q}}$ have a particularly simple structure. Indeed, Shimura has proved the following in [Sh 1, Prop. 1.5]:

Proposition 1.1 *Let $A/\mathbb{Q}$ be an abelian variety of $\mathbf{GL}_2$ -type. Suppose $A_{/\overline{\mathbb{Q}}}$ contains a simple abelian subvariety of CM-type. Then $A_{/\overline{\mathbb{Q}}}$ is isogenous to a power of a CM elliptic curve.*

The theory of elliptic curves with complex multiplication is well understood, and requires different techniques from the non-CM case. For these reasons, we will focus on abelian varieties with no complex multiplication. *Henceforth we will consider only abelian varieties of $\mathbf{GL}_2$ -type with no complex multiplication over $\overline{\mathbb{Q}}$.*

We begin our analysis of abelian varieties of $\mathbf{GL}_2$ -type with a review of a familiar lemma that describes the action of a field on an abelian variety. This result is originally due to Albert, and Mumford thoroughly covers the case of a simple abelian variety in [Mu]. Since we will be concerned mostly with non-simple abelian varieties, we include a proof to remind the reader of the details in that situation. In particular, our proof will help us better understand the special case of abelian varieties of $\mathbf{GL}_2$ -type.

We will use the following terminology from the theory of central simple algebras. (See Appendix B for more details.) Let $\mathcal{A}$ be a simple $\mathbb{Q}$ -algebra and let F be the center of $\mathcal{A}$. The *Schur index* of $\mathcal{A}$ is the integer $\sqrt{\dim_F \mathcal{D}}$, where $\mathcal{D}$ is a division algebra (determined up to isomorphism) such that $\mathcal{A} \cong \mathbf{M}_n(\mathcal{D})$ for some $n \geq 1$. A *subfield* of $\mathcal{A}$ is a $\mathbb{Q}$ -subalgebra E of $\mathcal{A}$ such that E is a field. A *maximal subfield* of $\mathcal{A}$ is a subfield that is maximal with respect to inclusion.

Lemma 1.2 *Let A be an abelian variety over $\overline{\mathbb{Q}}$ that has no simple abelian subvariety of CM-type. Let E be a subfield of $\text{End}(A)$. Then $[E:\mathbb{Q}]$ divides $\dim A$.*

Proof. We first consider the case where A is isogenous to a power of a simple abelian variety B . Then for some $n \geq 1$, we may write $A \sim B^n$, $\dim A = n \dim B$, and $\text{End}(A) \cong \mathbf{M}_n(\text{End}(B))$. Now B has no complex multiplication by hypothesis. Therefore $\text{End}(B)$ is a central division algebra over a totally real field F with Schur index $t = 1$ or 2 ; moreover, $t[F:\mathbb{Q}] \mid \dim B$, from [Mu, p. 202]. Thus the endomorphism algebra $\text{End}(A) \cong \mathbf{M}_n(\text{End}(B))$ is seen to be central simple over F with Schur index t . Now E is contained in a maximal subfield of $\text{End}(A)$, and because F is a number field, any such maximal subfield has degree $nt[F:\mathbb{Q}]$, by [Pi, Prop. 13.1]. Thus $[E:\mathbb{Q}] \mid nt[F:\mathbb{Q}]$. From above, however, we have $t[F:\mathbb{Q}] \mid \dim B$. Therefore, $[E:\mathbb{Q}] \mid n \dim B = \dim A$.

In general, of course, A is isogenous to a (finite) product $\prod B_i^{n_i}$, where each B_i is simple, B_i is non-isogenous to B_j if $i \neq j$, and no B_i has complex multiplication. Then

$\text{End}(A)$ is isomorphic to the direct product of the simple algebras $\mathbf{M}_{n_i}(\text{End}(B_i))$. Now because E is a $\mathbb{Q}$ -subalgebra of $\text{End}(A)$, we must have $E \hookrightarrow \mathbf{M}_{n_i}(\text{End}(B_i))$ for each i (via the i th projection map). But then for each i we apply the above argument to find $[E:\mathbb{Q}] \mid n_i \dim B_i$. Hence $[E:\mathbb{Q}] \mid \sum n_i \dim B_i = \dim A$. QED

Thus we see that another way to characterize abelian varieties of $\mathbf{GL}_2$ -type is as those abelian varieties which are simple over $\mathbb{Q}$ but have a “large” or “maximal” number of endomorphisms defined over $\mathbb{Q}$. By applying the lemma in this situation, when $[E:\mathbb{Q}] = \dim A$, we immediately obtain the following description of the endomorphism algebra of an abelian variety of $\mathbf{GL}_2$ -type.

Theorem 1.3 *Let $A/\mathbb{Q}$ be an abelian variety of $\mathbf{GL}_2$ -type with no complex multiplication over $\overline{\mathbb{Q}}$. Let $E = \text{End}_{\mathbb{Q}}(A)$. Then the full endomorphism algebra $\text{End}(A)$ is a central simple algebra over a totally real field $F \subseteq E$; the Schur index of $\text{End}(A)$ is 1 or 2; and $\text{End}(A)$ contains E as a maximal subfield.*

Proof. The equality $[E:\mathbb{Q}] = \dim A$ forces equalities everywhere in the proof of the above lemma. In particular, we see that over $\overline{\mathbb{Q}}$, we must have $A \sim B^n$ for some simple abelian variety $B/\overline{\mathbb{Q}}$ with no complex multiplication; otherwise E would act on proper subvarieties of A , and it is too big to do so. This proves that $\text{End}(A)$ is a central simple algebra over a totally real field F with Schur index $t = 1$ or 2 . Moreover, we have $[E:\mathbb{Q}] = nt[F:\mathbb{Q}] = n \dim B = \dim A$. Thus E must be a maximal subfield of $\text{End}(A)$, which then implies that E contains the center F of $\text{End}(A)$. QED

The Simple Components of $A/\overline{\mathbb{Q}}$

Let A be an abelian variety of $\mathbf{GL}_2$ -type. We now consider the properties of an abelian variety $B/\overline{\mathbb{Q}}$ appearing as a simple component of $A/\overline{\mathbb{Q}}$. Note that the proof of the above theorem provides us with some information about $\text{End}(B)$ as well as $\text{End}(A)$. In fact, we have already proved the following proposition:

Proposition 1.4 *Let B be a simple component over $\overline{\mathbb{Q}}$ of an abelian variety of $\mathbf{GL}_2$ -type. Then the endomorphism algebra $\text{End}(B)$ is a central division algebra over a totally real field F ; the Schur index t of $\text{End}(B)$ is 1 or 2; and $t[F:\mathbb{Q}] = \dim B$.*

Thus B , like A , also has the property that its endomorphism algebra is maximal, if compared with other simple abelian varieties of the same dimension. We remark here that in the case $t = 2$, the condition $t[F : \mathbb{Q}] = \dim B$ means that $\text{End } B$ must be an indefinite quaternion algebra over F . Indeed, the endomorphism algebra of a simple abelian variety is always totally definite or totally indefinite, and the equality $t[F : \mathbb{Q}] = \dim B$ can never hold if $\text{End}(B)$ is a definite quaternion algebra [Sh 3, Prop. 15].

It turns out that B has another interesting property. Namely, it is isogenous to all of its Galois conjugates. More technically, we say that B is a $\mathbb{Q}$ -abelian variety, which is defined as follows.

Definition. An abelian variety $X/\overline{\mathbb{Q}}$ is a $\mathbb{Q}$ -abelian variety if for each $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, there exists an isogeny $\mu_\sigma : {}^\sigma X \rightarrow X$ compatible with the endomorphisms of X ; that is, $\mu_\sigma \circ {}^\sigma \varphi = \varphi \circ \mu_\sigma$ for all $\varphi \in \text{End}(X)$.

It is easy to see that for each $\sigma \in G_{\mathbb{Q}}$, the conjugate ${}^\sigma B$ must be isogenous to B . Indeed, ${}^\sigma B^n \sim {}^\sigma A = A \sim B^n$, because A is defined over $\mathbb{Q}$. Then, by the uniqueness of decomposition of abelian varieties up to isogeny, we must have ${}^\sigma B \sim B$. It takes a little more work to show that there is actually an isogeny which is compatible with $\text{End}(B)$.

Proposition 1.5 *Let B be a simple component over $\overline{\mathbb{Q}}$ of an abelian variety A of $\mathbf{GL}_2$ -type. Then B is a $\mathbb{Q}$ -abelian variety.*

Proof. Fix an isogeny $A/\overline{\mathbb{Q}} \sim B^n$, or equivalently, an isomorphism $\text{End}(A) \cong \mathbf{M}_n(\text{End}(B))$. For each $\sigma \in G_{\mathbb{Q}}$, we form the σ -twist of this isogeny, ${}^\sigma B^n \sim {}^\sigma A$. Let $\varphi \in \text{End}(B)$, and write $\tilde{\varphi}$ for the endomorphism of A which is φ in each place. Then, because, A is defined over $\mathbb{Q}$, there are commutative diagrams

$$\begin{array}{ccc} {}^\sigma B & \xrightarrow{\text{diag.}} & {}^\sigma B^n \sim {}^\sigma A = A \\ {}^\sigma \varphi \downarrow & & \downarrow {}^\sigma \tilde{\varphi} \\ {}^\sigma B & \xrightarrow{\text{diag.}} & {}^\sigma B^n \sim {}^\sigma A = A \end{array} \qquad \begin{array}{ccc} A \sim B^n & \xrightarrow{\pi_j} & B \\ \downarrow \tilde{\varphi} & & \downarrow \varphi \\ A \sim B^n & \xrightarrow{\pi_j} & B \end{array}$$

where π_j is projection onto the j th place of B^n .

Now $\text{End}(A)$ is a central simple algebra, and for each $\sigma \in G_{\mathbb{Q}}$, there is an automorphism of $\text{End}(A)$ given by $\psi \mapsto {}^\sigma \psi$. Hence by the Skolem-Noether Theorem, there exists an invertible $\alpha(\sigma) \in \text{End}(A)$ such that ${}^\sigma \psi = \alpha(\sigma) \circ \psi \circ \alpha(\sigma)^{-1}$ for all $\psi \in \text{End}(A)$. Therefore we may connect the above diagrams with

$$\begin{array}{ccc} A & \xrightarrow{\alpha(\sigma)^{-1}} & A \\ \sigma\tilde{\varphi} \downarrow & & \downarrow \tilde{\varphi} \\ A & \xrightarrow{\alpha(\sigma)^{-1}} & A \end{array}$$

Then the composite map

$$\sigma B \rightarrow \sigma B^n \sim \sigma A = A \xrightarrow{\alpha(\sigma)^{-1}} A \sim B^n \xrightarrow{\pi_j} B$$

is a morphism from σB to B that is compatible with $\text{End}(B)$. For some j this morphism must be non-zero, hence an isogeny because B is simple. Thus, we have found an isogeny $\mu_\sigma : \sigma B \rightarrow B$ such that $\mu_\sigma \circ \sigma\varphi = \varphi \circ \mu_\sigma$ for all $\varphi \in \text{End}(B)$, and so B is a $\mathbb{Q}$ -abelian variety.

QED

We now make a definition based on these properties associated with simple components of abelian varieties of $\mathbf{GL}_2$ -type.

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

- (i) the endomorphism algebra $\text{End}(B)$ is a central division algebra over a totally real field F with Schur index $t = 1$ or 2 , and $t[F:\mathbb{Q}] = \dim B$.
- (ii) B is a $\mathbb{Q}$ -abelian variety.

We will show in Proposition 4.5 that every building block appears as a simple component of some abelian variety over $\mathbb{Q}$ of $\mathbf{GL}_2$ -type.

The Extension E/F

Let A be an abelian variety of $\mathbf{GL}_2$ -type. Let $E = \text{End}_{\mathbb{Q}}(A)$, and let $F = Z(\text{End}(A))$ denote the center of $\text{End}(A)$. We now look more closely at the field extension E/F . In the proof of the above proposition, we saw that for each $\sigma \in G_{\mathbb{Q}}$, the Skolem-Noether Theorem implies that there exists an invertible $\alpha(\sigma) \in \text{End}(A)$ such that $\sigma\varphi = \alpha(\sigma) \circ \varphi \circ \alpha(\sigma)^{-1}$ for all $\varphi \in \text{End}(A)$. Notice that because $E = \text{End}_{\mathbb{Q}}(A)$, the endomorphism $\alpha(\sigma)$ must be contained in the centralizer of E in $\text{End}(A)$. But E is a maximal subfield of $\text{End}(A)$, and hence its own centralizer, as F is a number field [Pi, Prop. 13.1]. Therefore $\alpha(\sigma) \in E$. Furthermore, each $\alpha(\sigma)$ is determined up to (non-zero) elements of the center F of $\text{End}(A)$. We now fix a choice of $\alpha(\sigma) \in E$ for each $\sigma \in G_{\mathbb{Q}}$, choosing

$\alpha(\sigma') = \alpha(\sigma)$ whenever $\sigma'\varphi = \sigma\varphi$ for all $\varphi \in \text{End}(A)$. We may view α as a locally constant function $G_{\mathbb{Q}} \rightarrow E^*$ that is a lift of the evident homomorphism $G_{\mathbb{Q}} \rightarrow E^*/F^*$.

Proposition 1.6 *The field E is generated over F by the $\alpha(\sigma)$.*

Proof. Let $E' = F(\dots, \alpha(\sigma), \dots)$. Then $E' \subseteq E$, since each $\alpha(\sigma) \in E$. Now let φ be an endomorphism of A that lies in the centralizer of E' ; that is, $\varphi \circ \alpha(\sigma) = \alpha(\sigma) \circ \varphi$ for all $\sigma \in G_{\mathbb{Q}}$. But then $\sigma\varphi = \alpha(\sigma) \circ \varphi \circ \alpha(\sigma)^{-1} = \varphi$ for all σ , which means that φ is defined over $\mathbb{Q}$, and thus lies in E . Therefore the centralizer $C(E')$ of E' is also contained in E . Now we use the Double Centralizer Theorem [Pi, Thm. 12.7] to count dimensions, and we find $(\dim_F E')(\dim_F C(E')) = \dim_F \text{End}(A) = (\dim_F E)^2$. Thus we must have $E' = C(E') = E$, and so E is generated over F by the collection $\{\alpha(\sigma)\}$. QED

Now recall that the Rosati involution induced by any polarization of $A/\mathbb{Q}$ is used to define an involution $e \mapsto \bar{e}$ on E which is independent of the polarization. This “complex conjugation” fixes F —indeed, any totally real subfield of E .

Lemma 1.7 *For all $\sigma \in G_{\mathbb{Q}}$, we have $\overline{\alpha(\sigma)} \circ \alpha(\sigma) \in F$.*

Proof. Fix a polarization (over $\mathbb{Q}$) of A and let $\varphi \mapsto \varphi'$ designate the Rosati involution on $\text{End}(A)$ induced by the polarization. Fix $\sigma \in G_{\mathbb{Q}}$. Now for all $\varphi \in \text{End}(A)$ we have $\sigma\varphi = \alpha(\sigma) \circ \varphi \circ \alpha(\sigma)^{-1}$. Taking the Rosati involution of both sides, we find $\sigma\varphi' = \overline{\alpha(\sigma)}^{-1} \circ \varphi' \circ \overline{\alpha(\sigma)}$ for all $\varphi' \in \text{End}(A)$. Replacing φ' with φ , we find $\sigma\varphi = \overline{\alpha(\sigma)}^{-1} \circ \varphi \circ \overline{\alpha(\sigma)}$ for all $\varphi \in \text{End}(A)$. So we see that $\overline{\alpha(\sigma)}^{-1}$ acts via conjugation on $\text{End}(A)$ exactly as $\alpha(\sigma)$ does. Therefore $\overline{\alpha(\sigma)} \circ \alpha(\sigma)$ lies in the center of $\text{End}(A)$, which is F . QED

Proposition 1.8 *The field E is an abelian Galois extension of F .*

Proof. Recall that E is generated over F by the $\alpha(\sigma)$, so it suffices to study the extensions $F(\alpha(\sigma))$. First we write $\alpha(\sigma)^2$ in a more complicated way:

$$\alpha(\sigma)^2 = \left(\alpha(\sigma) / \overline{\alpha(\sigma)} \right) \cdot \left(\overline{\alpha(\sigma)} \alpha(\sigma) \right).$$

We have seen that $\overline{\alpha(\sigma)} \alpha(\sigma)$ lies in F . Now we consider the first factor $\alpha(\sigma) / \overline{\alpha(\sigma)}$.

Note that by construction, the $\alpha(\sigma)$ satisfy $\alpha(\sigma) \circ \alpha(\tau) \circ \alpha(\sigma\tau)^{-1} \in F$ for all $\sigma, \tau \in G_{\mathbb{Q}}$. Therefore

$$\alpha(\sigma) \cdot \alpha(\tau) \cdot \alpha(\sigma\tau)^{-1} = \overline{\alpha(\sigma)} \cdot \overline{\alpha(\tau)} \cdot \overline{\alpha(\sigma\tau)}^{-1},$$

and rearranging terms, we find

$$\left(\alpha(\sigma)/\overline{\alpha(\sigma)}\right) \cdot \left(\alpha(\tau)/\overline{\alpha(\tau)}\right) = \alpha(\sigma\tau)/\overline{\alpha(\sigma\tau)} \quad \text{for all } \sigma, \tau \in G_{\mathbb{Q}}.$$

That is, $\sigma \mapsto \alpha(\sigma)/\overline{\alpha(\sigma)}$ is a continuous character on $G_{\mathbb{Q}}$ with values in E^* . In particular, $\alpha(\sigma)/\overline{\alpha(\sigma)}$ is a root of unity.

Now we have expressed $\alpha(\sigma)^2$ as a product of a root of unity and an element of F . Clearly then, $\alpha(\sigma)$ is contained in an abelian Galois extension of F obtained by adjoining $\sqrt{\overline{\alpha(\sigma)}\alpha(\sigma)}$ and some number of roots of unity. Therefore $F(\alpha(\sigma))$ is an abelian Galois extension, and this is true for any σ . Finally, since E is the compositum of the $F(\alpha(\sigma))$, we see that the field E is also an abelian extension of F . *QED*

Some Cohomology

Let A be an abelian variety of $\mathbf{GL}_2$ -type. Let $E = \text{End}_{\mathbb{Q}}(A)$ and $F = Z(\text{End}(A))$. As in the previous section, let $\alpha : G_{\mathbb{Q}} \rightarrow E^*$ be a locally constant function such that ${}^{\sigma}\varphi = \alpha(\sigma) \circ \varphi \circ \alpha(\sigma)^{-1}$ for all $\varphi \in \text{End}(A)$. Recall that α is well-defined modulo F^* .

We note that $c(\sigma, \tau) \stackrel{\text{def}}{=} \alpha(\sigma)^{-1} \alpha(\tau)^{-1} \alpha(\sigma\tau)$ is a two-cocycle on $G_{\mathbb{Q}}$ with values in F^* (where $G_{\mathbb{Q}}$ acts trivially on F^*). Moreover, a different choice for α leads to a cocycle which is cohomologous to $c(\sigma, \tau)$. Thus the abelian variety A of $\mathbf{GL}_2$ -type supplies us with a well-defined cohomology class $[c] \in H^2(G_{\mathbb{Q}}, F^*)$.

Lemma 1.9 *The class of $c(\sigma, \tau)$ has order dividing two in $H^2(G_{\mathbb{Q}}, F^*)$.*

Proof. Since $c(\sigma, \tau)$ lies in F^* , we have $c(\sigma, \tau) = \overline{c(\sigma, \tau)}$. Hence we may write

$$\begin{aligned} c(\sigma, \tau)^2 &= \overline{c(\sigma, \tau)} c(\sigma, \tau) \\ &= \left(\overline{\alpha(\sigma)} \alpha(\sigma)\right)^{-1} \left(\overline{\alpha(\tau)} \alpha(\tau)\right)^{-1} \left(\overline{\alpha(\sigma\tau)} \alpha(\sigma\tau)\right). \end{aligned}$$

Thus we have expressed $c(\sigma, \tau)^2$ as a coboundary, because we have already shown that $\overline{\alpha(\sigma)} \alpha(\sigma) \in F^*$ for all $\sigma \in G_{\mathbb{Q}}$. *QED*

Now consider the $G_{\mathbb{Q}}$ -module $\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F$, where $\sigma \in G_{\mathbb{Q}}$ acts via $\sigma(r \otimes f) = \sigma(r) \otimes f$. The natural inclusion $F \hookrightarrow \overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F$ induces a map $H^2(G_{\mathbb{Q}}, F^*) \rightarrow H^2(G_{\mathbb{Q}}, (\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^*)$ and this latter group is canonically isomorphic to the Brauer group $\text{Br}(F)$. (The isomorphism will be discussed in detail in Chapter 2.)

The endomorphism algebra $\text{End}(A)$ is a central simple F -algebra, and as such, determines a Brauer class in $\text{Br}(F)$. The class has order dividing two in $\text{Br}(F)$, because the Schur index of $\text{End}(A)$ is 1 or 2 [Pi, Thm. 18.6]. Furthermore, the field E splits $\text{End}(A)$ because E is a maximal subfield of $\text{End}(A)$ [Pi, Cor. 13.3], and E also splits $c(\sigma, \tau)$, by definition of the cocycle c . These observations motivate one to ask whether there is a connection between the class of $\text{End}(A)$ in $\text{Br}(F)$ and the class of c in $H^2(G_{\mathbb{Q}}, (\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^*)$. This question is answered by the following proposition.

Proposition 1.10 *The image of $[c]$ in $H^2(G_{\mathbb{Q}}, (\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^*)$ corresponds (under the natural isomorphism) to the class of $\text{End}(A)$ in $\text{Br}(F)$.*

Proof. [Ri 1, Thm. 5.6].

Alternatively, the results of Chapter 2 and Chapter 4 of this dissertation may be combined to give a different proof of Proposition 1.10.

Chapter 2

The Brauer Class of $\text{End}(B)$

In Chapter 1, we saw how an abelian variety of $\mathbf{GL}_2$ -type decomposes over $\overline{\mathbb{Q}}$ into a product $B \times \dots \times B$ of building blocks B with certain properties. Recall our definitions:

Definition. An abelian variety $B/\overline{\mathbb{Q}}$ is a $\mathbb{Q}$ -*abelian variety* if for each $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, there exists an isogeny $\mu_\sigma : {}^\sigma B \rightarrow B$ compatible with the endomorphisms of B ; that is, $\mu_\sigma \circ {}^\sigma \varphi = \varphi \circ \mu_\sigma$ for all $\varphi \in \text{End}(B)$.

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

- (i) the endomorphism algebra $\text{End}(B)$ is a central division algebra over a totally real field F with Schur index $t = 1$ or 2 , and $t[F:\mathbb{Q}] = \dim B$.
- (ii) B is a $\mathbb{Q}$ -abelian variety.

Our ultimate goal is to show that every building block B appears as a simple quotient of some abelian variety $A/\mathbb{Q}$ of $\mathbf{GL}_2$ -type. Towards that end, in this chapter we will study the class of the endomorphism algebra $\text{End}(B)$ in the Brauer group $\text{Br}(F)$.

Let $G_{\mathbb{Q}}$ be the absolute Galois group $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with its usual profinite topology. A building block $B/\overline{\mathbb{Q}}$ may be constructed from a model over a finite extension K of $\mathbb{Q}$; by abusing notation we will again call such a model B . Then ${}^\sigma B = {}^{\sigma'} B$ if $\sigma, \sigma' \in G_{\mathbb{Q}}$ restrict to the same map on K . Now because B is a $\mathbb{Q}$ -abelian variety, we may fix a collection of isogenies $\{\mu_\sigma : {}^\sigma B \rightarrow B\}_{\sigma \in G_{\mathbb{Q}}}$ respecting $\text{End}(B)$ such that $\mu_\sigma = \mu_{\sigma'}$ whenever ${}^\sigma B = {}^{\sigma'} B$. Define $c(\sigma, \tau) = \mu_\sigma \circ {}^\sigma \mu_\tau \circ \mu_{\sigma\tau}^{-1}$ for each pair $\sigma, \tau \in G_{\mathbb{Q}}$. Then $c(\sigma, \tau)$ is an element of $\text{End}(B)$, as we may see from the diagram $B \xrightarrow{\mu_{\sigma\tau}^{-1}} {}^{\sigma\tau} B \xrightarrow{{}^\sigma \mu_\tau} {}^\sigma B \xrightarrow{\mu_\sigma} B$. Also, $c(\sigma, \tau) \circ \varphi = \varphi \circ c(\sigma, \tau)$ for all $\varphi \in \text{End}(B)$; this follows from the compatibility conditions on the μ_σ . Thus $c(\sigma, \tau)$ lies

in the center of $\text{End}(B)$, and may be thought of as a non-zero element of the field F . Therefore, we may view c as a locally constant two-cocycle on $G_{\mathbb{Q}}$ with values in F^* , and we easily check that a different choice of isogenies $\sigma B \rightarrow B$ changes c by a coboundary. Thus to the abelian variety B we associate a well-defined cohomology class $[c] \in H^2(G_{\mathbb{Q}}, F^*)$, where $G_{\mathbb{Q}}$ acts trivially on F^* .

Next, consider the $G_{\mathbb{Q}}$ -module $\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F$, where the action of $\sigma \in G_{\mathbb{Q}}$ is defined by $\sigma(r \otimes f) = \sigma(r) \otimes f$. The inclusion $F \hookrightarrow \overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F$ induces a map $H^2(G_{\mathbb{Q}}, F^*) \rightarrow H^2(G_{\mathbb{Q}}, (\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^*)$, and this latter group is canonically isomorphic to the Brauer group of F , as we will see.

Theorem 2.1 *The image of $[c]$ in $H^2(G_{\mathbb{Q}}, (\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^*)$ corresponds to the class of $\text{End}(B)$ in the Brauer group $\text{Br}(F)$.*

Theorem 2.1 is reminiscent of Proposition 1.10, which referred to another cohomology class $[c] \in H^2(G_{\mathbb{Q}}, F^*)$ attached to an abelian variety of $\mathbf{GL}_2$ -type. In Chapter 4 we will justify the use of this notation when we show that every building block B appears as a quotient of an abelian variety A over $\mathbb{Q}$ of $\mathbf{GL}_2$ -type in such a way that the definitions of $[c]$ coincide. Since $\text{End}(A)$ and $\text{End}(B)$ determine the same class in $\text{Br}(F)$ whenever $A \sim B \times \dots \times B$, it is evident that Theorem 2.1 is a necessary condition for this assertion to be valid.

The proof of the Theorem 2.1 will be postponed until after we have reviewed the construction of the isomorphism $H^2(G_{\mathbb{Q}}, (\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^*) \xrightarrow{\sim} \text{Br}(F)$.

The Identification of the Brauer Group $\text{Br}(F)$ with $H^2(\text{Gal}(\overline{F}/F), \overline{F}^*)$

Let G be a profinite group, and let X, X_1, X_2, X_3 be discrete (multiplicative) groups equipped with a left action of G . We recall the following definitions and facts from the theory of non-abelian cohomology. (See [Se 2, p. 131–134] for more details.)

- $H^0(G, X) \stackrel{\text{def}}{=} \{x \in X : \sigma(x) = x \text{ for all } \sigma \in G\}$.
- A *one-cocycle* on G with values in X is a continuous map $G \rightarrow X$ sending $\sigma \mapsto x_{\sigma}$ such that $x_{\sigma\tau} = x_{\sigma} \cdot \sigma(x_{\tau})$ for all $\sigma, \tau \in G$.
- The one-cocycles x_{σ} and y_{σ} are *cohomologous* if there exists an $x \in X$ such that $y_{\sigma} = x^{-1} \cdot x_{\sigma} \cdot \sigma(x)$ for all $\sigma \in G$. A one-cocycle is a *coboundary* if it is cohomologous to the trivial cocycle $\sigma \mapsto 1$.

- $H^1(G, X) \stackrel{\text{def}}{=} \{\text{one-cocycles}\} / \{\text{coboundaries}\}$.
- If $1 \rightarrow X_1 \rightarrow X_2 \rightarrow X_3 \rightarrow 1$ is a short exact sequence of non-abelian G -modules then there exists an exact sequence of pointed sets

$$\begin{aligned} 1 \rightarrow H^0(G, X_1) \rightarrow H^0(G, X_2) \rightarrow H^0(G, X_3) \\ \rightarrow H^1(G, X_1) \rightarrow H^1(G, X_2) \rightarrow H^1(G, X_3). \end{aligned}$$

Moreover, if X_1 is contained in the center of X_2 , the sequence may be extended by one more term, with a map to $H^2(G, X_1)$. (Recall that the “kernel” of a morphism of pointed sets is the inverse image of the distinguished element.)

In particular, let $G_F = \text{Gal}(\overline{F}/F)$, where F is a number field. Then

$$1 \rightarrow \overline{F}^* \rightarrow \mathbf{GL}_n(\overline{F}) \rightarrow \mathbf{PGL}_n(\overline{F}) \rightarrow 1$$

is an exact sequence of G_F -modules, and the corresponding cohomology sequence is

$$\cdots \rightarrow H^1(G_F, \mathbf{GL}_n(\overline{F})) \rightarrow H^1(G_F, \mathbf{PGL}_n(\overline{F})) \xrightarrow{\delta_n} H^2(G_F, \overline{F}^*).$$

A generalization of Hilbert’s Theorem 90 states that $H^1(G_F, \mathbf{GL}_n(\overline{F}))$ is trivial [Se 2, Prop. X.3], so in fact the map δ_n is injective.

Now $H^1(G_F, \mathbf{PGL}_n(\overline{F}))$ classifies the *forms* of $\mathbf{M}_n(\overline{F})$. That is, there is a canonical bijection

$$(2.2) \quad H^1(G_F, \mathbf{PGL}_n(\overline{F})) \longrightarrow \text{Br}_n(F),$$

where $\text{Br}_n(F)$ denotes the set of Brauer classes of F -algebras $\mathcal{B}$ such that $\overline{F} \otimes_F \mathcal{B}$ is isomorphic to $\mathbf{M}_n(\overline{F})$ as an $\overline{F}$ -algebra. This correspondence is described explicitly by associating to each one-cocycle $\sigma \mapsto P_\sigma \in \mathbf{PGL}_n(\overline{F})$ the Brauer class of the F -algebra

$$\mathcal{B} \stackrel{\text{def}}{=} \left\{ X \in \mathbf{M}_n(\overline{F}) \mid P_\sigma \cdot \sigma(X) \cdot P_\sigma^{-1} = X \text{ for all } \sigma \in G_F \right\}.$$

Now because $\text{Br}(F)$ is the union (over n) of the $\text{Br}_n(F)$, we may define a map from $\text{Br}(F)$ to $H^2(G_F, \overline{F}^*)$ by using the inverse of (2.2):

$$\begin{array}{ccc} H^2(G_F, \overline{F}^*) & \xleftarrow{\quad \quad \quad} & \text{Br}(F) \\ \uparrow \delta_n & & \uparrow \\ H^1(G_F, \mathbf{PGL}_n(\overline{F})) & \xrightleftharpoons{(2.2)} & \text{Br}_n(F) \end{array}$$

This is the desired isomorphism. (See [Se 2, X.5] for the details.)

REMARK. In the above definition of $\mathcal{B}$ we have written $\sigma(X)$ when $\sigma \in G_F$ and $X \in \mathbf{M}_n(\overline{F})$. Here we are regarding $\mathbf{M}_n(\overline{F})$ as the ring of $\overline{F}$ -endomorphisms of the vector space $\overline{F}^n$, with its standard G_F -module structure. Then $\sigma(X)$ is defined to be the endomorphism $\sigma \circ X \circ \sigma^{-1}$ on $\overline{F}^n$. It is useful to note, however, that we may also describe $\sigma(X)$ as the matrix obtained from $X \in \mathbf{M}_n(\overline{F})$ by applying σ to each entry.

Co-Induced Modules

Let H be a closed subgroup of a profinite group G , and let M be a discrete H -module (possibly non-abelian). The *co-induced* G -module $\text{Coind}_H^G M$ is defined to be the set of continuous functions $\theta : G \rightarrow M$ such that $\theta(\eta x) = \eta(\theta(x))$ for all $x \in G$ and $\eta \in H$. The group structure on $\text{Coind}_H^G M$ is defined by pointwise multiplication, and the action of $\sigma \in G$ is defined by $({}^\sigma \theta)(x) = \theta(x\sigma)$.

In the case $M = \overline{\mathbb{Q}}$, which we consider below, it will be helpful to put a $\overline{\mathbb{Q}}$ -vector space structure on $\text{Coind}_H^G \overline{\mathbb{Q}}$. This is achieved by defining $(r\theta)(x) = x(r) \cdot \theta(x)$ for $r \in \overline{\mathbb{Q}}$, $\theta \in \text{Coind}_H^G \overline{\mathbb{Q}}$, and $x \in G_{\mathbb{Q}}$.

Now we return to the situation $G = G_{\mathbb{Q}}$ to study the $G_{\mathbb{Q}}$ -module $\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F$. Consider the finite set of field embeddings $\{\iota : F \hookrightarrow \overline{\mathbb{Q}}\}$. The group $G_{\mathbb{Q}}$ acts (on the left) on this set in the usual manner; that is to say, if ι is an embedding of F into $\overline{\mathbb{Q}}$ and σ is an element of G , then $\sigma \circ \iota$ is another such embedding. We now fix an embedding ι_0 , let $H = \text{Gal}(\overline{\mathbb{Q}}/\iota_0(F))$, and view $\overline{\mathbb{Q}}$ as an H -module.

Proposition 2.3 *There is a $\overline{\mathbb{Q}}$ -linear isomorphism of $G_{\mathbb{Q}}$ -modules*

$$(2.3) \quad \overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F \xrightarrow{\sim} \text{Coind}_H^G \overline{\mathbb{Q}},$$

in which $1 \otimes f$ is sent to the function $\theta_f : x \mapsto \iota_0(f)$.

Proof. Note that $\theta_f \in \text{Coind}_H^G \overline{\mathbb{Q}}$ because H fixes $\iota_0(F)$ by definition. Also, one may check that ${}^\sigma(r\theta) = \sigma(r){}^\sigma \theta$, and use this formula to verify that (2.3) is a $G_{\mathbb{Q}}$ -module homomorphism.

Now we want to show that this homomorphism is injective. Recall that we may write $\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F \xrightarrow{\sim} \prod_{\iota} \overline{\mathbb{Q}}$ via the map $r \otimes f \mapsto (r \cdot \iota(f))_{\iota}$. We use this isomorphism of $\overline{\mathbb{Q}}$ -algebras to factor (2.3) through the product; the element $(r_{\iota})_{\iota} \in \prod_{\iota} \overline{\mathbb{Q}}$ is then mapped to the function $x \mapsto x(r_{x^{-1}\iota_0})$ in $\text{Coind}_H^G \overline{\mathbb{Q}}$. This correspondence is clearly injective.

Finally we note that a function $\theta \in \text{Coind}_H^G \overline{\mathbb{Q}}$ is determined by its values on any set of right coset representatives of H in $G_{\mathbb{Q}}$. Thus the $\overline{\mathbb{Q}}$ -dimension of $\text{Coind}_H^G \overline{\mathbb{Q}}$ must be

$[G_{\mathbb{Q}} : H] = [F : \mathbb{Q}]$, which is the same as the $\overline{\mathbb{Q}}$ -dimension of $\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F$. But (2.3) is already injective, hence it must actually be an isomorphism. *QED*

Proposition 2.4 *We obtain the following isomorphisms in an analogous manner.*

1. $(\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^* \cong \text{Coind}_H^G \overline{\mathbb{Q}}^*.$
2. $\mathbf{M}_n(\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F) \cong \text{Coind}_H^G \mathbf{M}_n(\overline{\mathbb{Q}}).$
3. $\mathbf{GL}_n(\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F) \cong \text{Coind}_H^G \mathbf{GL}_n(\overline{\mathbb{Q}}).$
4. $\mathbf{PGL}_n(\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F) \cong \text{Coind}_H^G \mathbf{PGL}_n(\overline{\mathbb{Q}}).$

Proof.

1. Follows directly from above because the $G_{\mathbb{Q}}$ -action on $\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F$ respects the multiplicative structure as well as the additive structure.
2. We can see from the definition of “ Coind_H^G ” that $\mathbf{M}_n(\text{Coind}_H^G \overline{\mathbb{Q}}) \cong \text{Coind}_H^G \mathbf{M}_n(\overline{\mathbb{Q}}).$
3. The action of $G_{\mathbb{Q}}$ still respects the multiplicative structure of the matrix algebra.
4. Follows from (1) and (3), and the fact that the functor Coind_H^G commutes with the formation of quotient modules. *QED*

REMARK. By using the isomorphism $\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F \xrightarrow{\sim} \prod_{\iota} \overline{\mathbb{Q}}$ described in the proposition, we may similarly write any of the above $G_{\mathbb{Q}}$ -modules as a product over the set of embeddings $\{\iota\}$. The action of $\sigma \in G_{\mathbb{Q}}$ on such a product sends the ι -place to the $\sigma^{-1}\iota$ -place via σ .

Cohomology of Co-Induced Modules

Let G be a profinite group, H a closed subgroup of G , M a discrete H -module, and $\text{Coind}_H^G M$ the associated co-induced G -module. In the usual case, where M is an abelian group, Shapiro’s Lemma states that the G -cohomology of $\text{Coind}_H^G M$ may be identified with the H -cohomology of M . See for example [Br, Prop. III.6.2]. This fact is also well known for non-abelian modules [Se 1, §5.8b], but for the convenience of the reader we include an explicit proof.

Proposition 2.5 (“Non-Abelian Shapiro’s Lemma”) *There is a natural bijection of pointed sets $H^1(G, \text{Coind}_H^G M) \rightarrow H^1(H, M)$.*

Proof. First note that the projection $\pi : \text{Coind}_H^G M \rightarrow M$ defined by $\theta \mapsto \theta(1)$ is compatible with the inclusion $H \subset G$, in the sense that $\pi({}^n\theta) = \eta(\pi(\theta))$ for $\eta \in H$ and $\theta \in \text{Coind}_H^G M$. Therefore there exists an induced map $H^1(G, \text{Coind}_H^G M) \rightarrow H^1(H, M)$, given by sending the one-cocycle $\sigma \mapsto \theta_\sigma$ to the cocycle $\eta \mapsto \theta_\eta(1)$.

To show that this map is one-to-one, suppose that $\eta \mapsto \theta_\eta(1)$ is a coboundary, i.e., that there is a fixed $m \in M$ such that $\theta_\eta(1) = m^{-1} \cdot \eta(m)$ for all $\eta \in H$. One defines $\psi(x) = m \cdot \theta_x(1)$ for $x \in G$, and checks that $\psi \in \text{Coind}_H^G M$. Then $\theta_\sigma = \psi^{-1} \circ \sigma \psi$ for all $\sigma \in G$, so θ_σ is also a coboundary. Thus we have an injective map $H^1(G, \text{Coind}_H^G M) \rightarrow H^1(H, M)$.

In order to show this map is surjective, let $\eta \mapsto m_\eta$ be a one-cocycle on H with values in M . Fix a set of right coset representatives of H in G , with the representative for H being 1. Now for each $x \in G$, define h_x to be the element of H such that $h_x^{-1}x$ is the chosen coset representative of Hx . Clearly for $\eta \in H$ we have $h_\eta = \eta$, and more generally $h_{\eta x} = \eta h_x$ for all $x \in G$. Define $\theta_\sigma(x) = m_{h_x}^{-1} \cdot m_{h_{x\sigma}}$. One verifies

- $\theta_\sigma \in \text{Coind}_H^G M$,
- $\sigma \mapsto \theta_\sigma$ is a one-cocycle on G , and
- $\theta_\eta(1) = m_\eta$ for $\eta \in H$

to finish the proof of surjectivity. *QED*

The Bijection between $H^1(G_{\mathbb{Q}}, \mathbf{PGL}_n(\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F))$ and $\text{Br}_n(F)$

Again we return to the specific case $G = G_{\mathbb{Q}}$ and $H = \text{Gal}(\overline{\mathbb{Q}}/F)$, where we have identified F with $\iota_0(F) \subset \overline{\mathbb{Q}}$ for some fixed embedding ι_0 . Shapiro's Lemma, together with our proof that $(\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^* \cong \text{Coind}_H^G \overline{\mathbb{Q}}^*$, has already given us an isomorphism of the group $H^2(G_{\mathbb{Q}}, (\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^*)$ with $H^2(H, \overline{\mathbb{Q}}^*) \cong \text{Br}(F)$. We will need a more precise description of the correspondence, however. We have the following commutative diagram for each n :

$$\begin{array}{ccccc}
 H^2(G_{\mathbb{Q}}, (\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^*) & \longrightarrow & H^2(H, \overline{\mathbb{Q}}^*) & \longrightarrow & \text{Br}(F) \\
 \uparrow \delta_n & & \uparrow \delta_n & & \uparrow \\
 H^1(G_{\mathbb{Q}}, \mathbf{PGL}_n(\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)) & \xrightarrow{(2.5)} & H^1(H, \mathbf{PGL}_n(\overline{\mathbb{Q}})) & \xrightarrow{(2.2)} & \text{Br}_n(F)
 \end{array}$$

Here the δ_n are the connecting homomorphisms from the cohomology sequences derived from the two short exact sequences:

$$\begin{aligned}
1 \rightarrow (\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^* &\rightarrow \mathbf{GL}_n(\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F) \rightarrow \mathbf{PGL}_n(\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F) \rightarrow 1 && \text{(co-induced } G_{\mathbb{Q}}\text{-modules)} \\
1 \rightarrow \overline{\mathbb{Q}}^* &\rightarrow \mathbf{GL}_n(\overline{\mathbb{Q}}) \rightarrow \mathbf{PGL}_n(\overline{\mathbb{Q}}) \rightarrow 1 && \text{(H-modules).}
\end{aligned}$$

Note that Proposition 2.5 allows us to identify the two corresponding cohomology sequences. In particular, the map (2.5) is a bijection for which we may find an explicit formula. First write $\mathbf{PGL}_n(\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)$ as the product $\prod_{\iota} \mathbf{PGL}_n(\overline{\mathbb{Q}})$. Let $\sigma \mapsto (P_{\iota, \sigma})_{\iota}$ represent a cohomology class in $H^1(G_{\mathbb{Q}}, \mathbf{PGL}_n(\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F))$. Then the image under (2.5) of this class is the class of $\eta \mapsto P_{\iota_0, \eta}$ in $H^1(H, \mathbf{PGL}_n(\overline{\mathbb{Q}}))$.

Now the image of the class of this latter cocycle under bijection (2.2) is the Brauer class of the algebra

$$\mathcal{B} = \left\{ X \in \mathbf{M}_n(\overline{\mathbb{Q}}) \mid P_{\iota_0, \eta} \cdot \eta(X) \cdot P_{\iota_0, \eta}^{-1} = X \text{ for all } \eta \in H \right\}.$$

But there is an alternate description of this algebra. Consider the parallel construction

$$(2.6) \quad \mathcal{B}' = \left\{ (X_{\iota})_{\iota} \in \mathbf{M}_n(\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F) \mid (P_{\iota, \sigma})_{\iota} \cdot \sigma(X_{\iota})_{\iota} \cdot (P_{\iota, \sigma})_{\iota}^{-1} = (X_{\iota})_{\iota} \text{ for all } \sigma \in G_{\mathbb{Q}} \right\}.$$

It is clear that $\mathcal{B}'$ is also an F -algebra, and that there is an F -algebra homomorphism $\mathcal{B}' \rightarrow \mathcal{B}$ given by $(X_{\iota})_{\iota} \mapsto X_{\iota_0}$. In fact this map is an isomorphism. Indeed, if we fix left coset representatives $\{g_{\iota}\}$ of H in G , then $X \mapsto (g_{\iota}(X))_{\iota}$ is the inverse isomorphism (assuming that $(P_{\iota, \sigma})_{\iota}$ is constructed from $P_{\iota_0, \eta}$ as in Proposition 2.5). The verification, however, is tedious and we leave it to the reader.

Now we see that $\mathcal{B}$ and $\mathcal{B}'$ determine the same class in $\text{Br}_n(F)$. Observe, however, that the construction of $\mathcal{B}'$ avoids the choice of the embedding $\iota_0 : F \hookrightarrow \overline{\mathbb{Q}}$. Therefore, even though bijections (2.5) and (2.2) depend on ι_0 , their composition is independent of this choice, and thus the isomorphism $H^2(G_{\mathbb{Q}}, (\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^*) \cong \text{Br}(F)$ is completely canonical.

The Proof of Theorem 2.1

Let B be a building block, and let $c(\sigma, \tau)$ be the associated two-cocycle on $G_{\mathbb{Q}}$ with values in F^* . Now that we have established the isomorphism $H^2(G_{\mathbb{Q}}, (\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^*) \cong \text{Br}(F)$, we aim to show that the image in $H^2(G_{\mathbb{Q}}, (\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^*)$ of the cohomology class $[c]$ corresponds to the class of $\text{End}(B)$ in $\text{Br}(F)$. Note that the Brauer class of $\text{End}(B)$ lies in $\text{Br}_t(F)$ where $t = 1$ or 2 , since by hypothesis, $\text{End}(B)$ is a central division algebra over F with Schur index $t = 1$ or 2 . Thus from the commutative diagram of the previous section we see it will

suffice to find a one-cocycle with values in $\mathbf{PGL}_t(\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)$ whose class maps to both the image of $[c]$ in $H^2(G_{\mathbb{Q}}, (\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^*)$ and the Brauer class of $\text{End}(B)$ in $\text{Br}_t(F)$.

First, we consider the Lie algebra $\text{Lie } B$. Recall that the space of tangent vectors $\text{Lie } B$ is a $\overline{\mathbb{Q}}$ -vector space canonically attached to the abelian variety B , whose dimension over $\overline{\mathbb{Q}}$ is equal to the dimension of B . (See e.g. [Mu, §11].) Also, $\text{Lie } B$ has the property that $\text{Lie } {}^{\sigma}B \cong {}^{\sigma}(\text{Lie } B) \stackrel{\text{def}}{=} \overline{\mathbb{Q}} \otimes_{\overline{\mathbb{Q}}} \text{Lie } B$, where the map from the base $\overline{\mathbb{Q}}$ to the base extension $\overline{\mathbb{Q}}$ is given by σ . Furthermore, the action of F on B induces an F -vector space structure on $\text{Lie } B$, and it is well known that since F is totally real, $\text{Lie } B$ is free of rank t over $\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F$. (Here is where we use the condition that the dimension of B is exactly $t[F:\mathbb{Q}]$.)

Now each $\mu_{\sigma} : {}^{\sigma}B \rightarrow B$ induces an isomorphism of $\overline{\mathbb{Q}}$ -vector spaces $\lambda_{\sigma} : \text{Lie } {}^{\sigma}B \rightarrow \text{Lie } B$, and the relation $\mu_{\sigma} \circ {}^{\sigma}\mu_{\tau} = c(\sigma, \tau) \mu_{\sigma\tau}$ implies that $\lambda_{\sigma} \circ {}^{\sigma}\lambda_{\tau} = c(\sigma, \tau) \lambda_{\sigma\tau}$ by functoriality. Here ${}^{\sigma}\lambda_{\tau}$ is the map $1 \otimes \lambda_{\tau} : {}^{\sigma}(\text{Lie } {}^{\tau}B) \rightarrow {}^{\sigma}(\text{Lie } B)$. Fix a basis $\{e_i\}_{i=1}^t$ for $\text{Lie } B$ over $\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F$. Then for each $\sigma \in G_{\mathbb{Q}}$, $\{1 \otimes e_i\}_{i=1}^t$ is a basis for the σ -twist ${}^{\sigma}(\text{Lie } B) \cong \text{Lie } {}^{\sigma}B$. We may use this collection of bases to express the maps λ_{σ} as matrices $\Lambda_{\sigma} \in \mathbf{GL}_t(\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)$, and the identity $\lambda_{\sigma} \circ {}^{\sigma}\lambda_{\tau} = c(\sigma, \tau) \lambda_{\sigma\tau}$ translates into $\Lambda_{\sigma} \cdot {}^{\sigma}\Lambda_{\tau} = c(\sigma, \tau) \Lambda_{\sigma\tau}$. At this point one easily verifies that the matrix ${}^{\sigma}\Lambda_{\tau}$ describing the map ${}^{\sigma}\lambda_{\tau}$ is the matrix Λ_{τ} with its entries twisted by σ , i.e., exactly $\sigma(\Lambda_{\tau})$.

We are now provided with a one-cocycle with values in $\mathbf{PGL}_t(\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)$, namely $\sigma \mapsto \Lambda_{\sigma} \bmod (\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^*$.

Proposition 2.7 *The class of $\Lambda_{\sigma} \bmod (\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^*$ in $H^1(G_{\mathbb{Q}}, \mathbf{PGL}_t(\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F))$ is independent of the choice of basis for $\text{Lie } B$.*

Proof. A different choice of basis for $\text{Lie } B$ is described by a change-of-basis matrix $P \in \mathbf{GL}_t(\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)$. The corresponding change of basis on $\text{Lie } {}^{\sigma}B \cong {}^{\sigma}(\text{Lie } B)$ will be given by ${}^{\sigma}P$. Thus the new matrix for the map $\lambda_{\sigma} : \text{Lie } {}^{\sigma}B \rightarrow \text{Lie } B$ will be $P \cdot \Lambda_{\sigma} \cdot {}^{\sigma}P^{-1}$, and the cocycle $\sigma \mapsto P \cdot \Lambda_{\sigma} \cdot {}^{\sigma}P^{-1}$ is cohomologous to $\sigma \mapsto \Lambda_{\sigma}$. QED

It remains to show that the class of the cocycle $\sigma \mapsto \Lambda_{\sigma} \bmod (\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^*$ corresponds to both the image of $[c]$ and the Brauer class of $\text{End}(B)$, as desired.

Proposition 2.8 *The class of $\Lambda_{\sigma} \bmod (\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^*$ in $H^1(G_{\mathbb{Q}}, \mathbf{PGL}_t(\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F))$ maps to the image of $[c]$ in $H^2(G_{\mathbb{Q}}, (\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^*)$.*

Proof. The connecting homomorphism which supplies the inclusion

$$H^1(G_{\mathbb{Q}}, \mathbf{PGL}_t(\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)) \hookrightarrow H^2(G_{\mathbb{Q}}, (\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^*)$$

is defined by the following procedure. First, choose a one-cocycle to represent the given cohomology class. In our case we take $\Lambda_\sigma \bmod (\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^*$. Then lift the chosen cocycle to a map $G_{\mathbb{Q}} \rightarrow \mathbf{GL}_t(\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)$; we choose $\sigma \mapsto \Lambda_\sigma$ for our application. Then $\Lambda_\sigma \cdot \sigma(\Lambda_\tau) \cdot \Lambda_{\sigma\tau}^{-1}$ is a two-cocycle with values in $(\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^*$, and the class of this two-cocycle in $H^2(G_{\mathbb{Q}}, (\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^*)$ is independent of all the choices we made. In our situation, $\Lambda_\sigma \cdot \sigma(\Lambda_\tau) \cdot \Lambda_{\sigma\tau}^{-1} = c(\sigma, \tau)$, which is exactly what we wished to show. *QED*

Proposition 2.9 *The class of $\Lambda_\sigma \bmod (\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^*$ in $H^1(G_{\mathbb{Q}}, \overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)$ corresponds to the class of $\text{End}(B)$ in $\text{Br}_t(F)$.*

Proof. By applying Equation 2.6, we find the Brauer class of F -algebras corresponding to the cocycle $\Lambda_\sigma \bmod (\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^*$ is represented by the algebra

$$\mathcal{B} \stackrel{\text{def}}{=} \left\{ X \in \mathbf{M}_t(\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F) \mid \Lambda_\sigma \cdot \sigma(X) \cdot \Lambda_\sigma^{-1} = X \text{ for all } \sigma \in G_{\mathbb{Q}} \right\}.$$

On the other hand, by the functoriality of “Lie”, there is a ring homomorphism $\text{End}(B) \rightarrow \text{End}(\text{Lie } B)$. In fact this map is an injection, because $\text{End}(B)$ is a division algebra. Then by using our fixed basis of $\text{Lie } B$, we have

$$\text{End}(B) \hookrightarrow \text{End}(\text{Lie } B) \cong \mathbf{M}_t(\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F).$$

We claim that under these maps, the image of $\text{End}(B)$ lands in $\mathcal{B}$. Indeed, for $\varphi \in \text{End}(B)$, let $\Phi \in \mathbf{M}_t(\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)$ be the corresponding matrix. Recall that the original μ_σ satisfied $\varphi \circ \mu_\sigma = \mu_\sigma \circ \sigma\varphi$. Hence by functoriality again, we have $\Phi \cdot \Lambda_\sigma = \Lambda_\sigma \cdot \sigma(\Phi)$ for all σ . Thus $\Lambda_\sigma \cdot \sigma(\Phi) \cdot \Lambda_\sigma^{-1} = \Phi$ for all $\sigma \in G_{\mathbb{Q}}$, which means $\Phi \in \mathcal{B}$.

Finally we see that both $\text{End}(B)$ and $\mathcal{B}$ are t^2 -dimensional over F , so the inclusion must in fact be an isomorphism $\text{End}(B) \xrightarrow{\sim} \mathcal{B}$. *QED*

This proves Theorem 2.1.

Chapter 3

The Tensor Product of a Module with an Abelian Variety

Here we prepare some “abstract nonsense” we will need for our construction of the correspondence between building blocks and abelian varieties of $\mathbf{GL}_2$ -type. The results in this chapter, however, are valid for arbitrary abelian varieties.

Let A be an abelian variety up to isogeny, let $\mathcal{R}$ be a ring with a map $\mathcal{R} \rightarrow \text{End}(A)$, and let M be a finitely generated right $\mathcal{R}$ -module. By abusing notation, we will identify $\mathcal{R}$ with its image in $\text{End}(A)$, and say that A is an abelian variety with an action of $\mathcal{R}$.

Theorem 3.1 *Let $\mathfrak{C}$ be the category of abelian varieties up to isogeny, and let $\mathfrak{A}$ be the category of abelian groups. Let $T : \mathfrak{C} \rightarrow \mathfrak{A}$ be the covariant functor defined by $T(X) = \text{Hom}_{\mathcal{R}}(M, \text{Hom}(A, X))$. Then T is representable.*

Proof. [Mit, Thm. VI.3.1].

We will denote the object representing the functor T as $M \otimes_{\mathcal{R}} A$, and devote this chapter to summarizing some properties of this “tensor product”. First, we may reformulate the above theorem as an assertion of the existence of an abelian variety $M \otimes_{\mathcal{R}} A$ characterized by the following universal property:

(3.2) $M \otimes_{\mathcal{R}} A$ is an abelian variety together with a homomorphism of right $\mathcal{R}$ -modules $\Delta : M \rightarrow \text{Hom}(A, M \otimes_{\mathcal{R}} A)$, which, for an abelian variety X , induces an isomorphism of abelian groups $\text{Hom}(M \otimes_{\mathcal{R}} A, X) \rightarrow \text{Hom}_{\mathcal{R}}(M, \text{Hom}(A, X))$ via $\psi \mapsto (m \mapsto \psi \circ \Delta_m)$.

Next, standard procedures produce the following facts. In the list below, it is understood that each tensor product is equipped with the evident homomorphism Δ , and that the symbol “ $\cong$ ” designates a natural equivalence that respects these homomorphisms.

ELEMENTARY PROPERTIES OF $M \otimes_{\mathcal{R}} A$:

- (i) If A is an abelian variety with an action of $\mathcal{R}$, then $\mathcal{R} \otimes_{\mathcal{R}} A \cong A$.
- (ii) If M is a right $\mathcal{R}$ -module, N is an $\mathcal{R}$ - $\mathcal{S}$ -bimodule, and A is an abelian variety with an action of $\mathcal{S}$, then $M \otimes_{\mathcal{R}} (N \otimes_{\mathcal{S}} A) \cong (M \otimes_{\mathcal{R}} N) \otimes_{\mathcal{S}} A$.
- (iii) If $\{M_i\}$ is a finite collection of right $\mathcal{R}$ -modules, and A is an abelian variety with an action of $\mathcal{R}$, then $(\oplus M_i) \otimes_{\mathcal{R}} A \cong \prod (M_i \otimes_{\mathcal{R}} A)$.
- (iv) If M is a right $\mathcal{R}$ -module and $\{A_i\}$ is a finite collection of abelian varieties, each with a map $\mathcal{R} \rightarrow \text{End}(A_i)$, then $M \otimes_{\mathcal{R}} \prod A_i \cong \prod (M \otimes_{\mathcal{R}} A_i)$.
- (v) $M \otimes_{\mathcal{R}} A$ is functorial in each variable separately. More explicitly, let M_1 and M_2 be right $\mathcal{R}$ -modules and $f \in \text{Hom}_{\mathcal{R}}(M_1, M_2)$. Let A_1 and A_2 be abelian varieties with actions of $\mathcal{R}$ and suppose $\varphi : A_1 \rightarrow A_2$ is a morphism of abelian varieties that respects $\mathcal{R}$; i.e., $r \circ \varphi = \varphi \circ r$ for all $r \in \mathcal{R}$. We write $\varphi \in \text{Hom}^{\mathcal{R}}(A_1, A_2)$. Then $m \mapsto \Delta_{f(m)} \circ \varphi$ is a homomorphism of right $\mathcal{R}$ -modules $M_1 \rightarrow \text{Hom}(A_1, M_2 \otimes_{\mathcal{R}} A_2)$. Hence by (3.2), there exists a unique morphism $f \otimes \varphi \in \text{Hom}(M_1 \otimes_{\mathcal{R}} A_1, M_2 \otimes_{\mathcal{R}} A_2)$ such that $(f \otimes \varphi) \circ \Delta_m = \Delta_{f(m)} \circ \varphi$ for all $m \in M$. Moreover, it is easy to check that if $g : M_2 \rightarrow M_3$ is another $\mathcal{R}$ -module homomorphism and $\psi : A_2 \rightarrow A_3$ another morphism of abelian varieties respecting $\mathcal{R}$, then $(g \otimes \psi) \circ (f \otimes \varphi) = (g \circ f) \otimes (\psi \circ \varphi)$.

If we apply property (v) in the particular case $A_1 = A_2 = A$ and $M_1 = M_2 = M$, we have ring homomorphisms

$$\begin{array}{ccc} \text{End}_{\mathcal{R}} M & \rightarrow & \text{End}(M \otimes_{\mathcal{R}} A) \\ f & \mapsto & f \otimes 1 \end{array} \qquad \begin{array}{ccc} \text{End}^{\mathcal{R}}(A) & \rightarrow & \text{End}(M \otimes_{\mathcal{R}} A) \\ \varphi & \mapsto & 1 \otimes \varphi \end{array}$$

whose images commute. Note that the center $Z(\mathcal{R}) \subseteq \text{End}^{\mathcal{R}}(A)$, and that we may also map $Z(\mathcal{R}) \rightarrow \text{End}_{\mathcal{R}} M$ via $r \mapsto \rho_r =$ right multiplication by r on M . (The condition $r \in Z(\mathcal{R})$ makes ρ_r a homomorphism of right $\mathcal{R}$ -modules.)

Proposition 3.3 *The two maps $Z(\mathcal{R}) \rightarrow \text{End}(M \otimes_{\mathcal{R}} A)$ coincide. Specifically, $1 \otimes r = \rho_r \otimes 1 \in \text{End}(M \otimes_{\mathcal{R}} A)$.*

Proof. By (3.2), it suffices to show that $(\rho_r \otimes 1) \circ \Delta_m = (1 \otimes r) \circ \Delta_m$ for all $m \in M$. But this plainly follows from the definitions: $(\rho_r \otimes 1) \circ \Delta_m = \Delta_{\rho_r(m)} = \Delta_{mr} = \Delta_m \circ r = (1 \otimes r) \circ \Delta_m$.

QED

Thus we obtain a homomorphism of $Z(\mathcal{R})$ -algebras

$$(3.4) \quad \text{End}_{\mathcal{R}} M \otimes_{Z(\mathcal{R})} \text{End}^{\mathcal{R}}(A) \longrightarrow \text{End}^{Z(\mathcal{R})}(M \otimes_{\mathcal{R}} A).$$

Now suppose M is an $\mathcal{S}$ - $\mathcal{R}$ -bimodule. Then we may map $\mathcal{S} \rightarrow \text{End}_{\mathcal{R}} M$ via $s \mapsto \lambda_s = \text{left multiplication by } s \text{ on } M$. By composing this map with $\text{End}_{\mathcal{R}} M \rightarrow \text{End}(M \otimes_{\mathcal{R}} A)$ from above, we find that we have an action of $\mathcal{S}$ on $M \otimes_{\mathcal{R}} A$. Again, we will usually identify $\mathcal{S}$ with its image in $\text{End}(M \otimes_{\mathcal{R}} A)$. We now reconsider the defining property (3.2) of $M \otimes_{\mathcal{R}} A$.

Proposition 3.5 *Let M be an $\mathcal{S}$ - $\mathcal{R}$ -bimodule, and let A be an abelian variety with an action of $\mathcal{R}$. Suppose X is an abelian variety with an action of $\mathcal{S}$. Then Δ induces an isomorphism $\text{Hom}^{\mathcal{S}}(M \otimes_{\mathcal{R}} A, X) \rightarrow \text{Hom}_{\mathcal{S}-\mathcal{R}}(M, \text{Hom}(A, X))$.*

Proof. It is clear that if $\psi : M \otimes_{\mathcal{R}} A \rightarrow X$ respects $\mathcal{S}$, then $m \mapsto \psi \circ \Delta_m$ is a homomorphism of $\mathcal{S}$ - $\mathcal{R}$ -bimodules. On the other hand, suppose $m \mapsto \varphi_m$ is an element of $\text{Hom}_{\mathcal{S}-\mathcal{R}}(M, \text{Hom}(A, X))$. Then there exists a morphism of abelian varieties $\tilde{\varphi} \in \text{Hom}(M \otimes_{\mathcal{R}} A, X)$ such that $\varphi_m = \tilde{\varphi} \circ \Delta_m$ for all $m \in M$. We have to show that $\tilde{\varphi}$ respects $\mathcal{S}$, i.e., that $s \circ \tilde{\varphi} = \tilde{\varphi} \circ s$ for all $s \in \mathcal{S}$. As usual, by (3.2) it suffices to show that $s \circ \tilde{\varphi} \circ \Delta_m = \tilde{\varphi} \circ s \circ \Delta_m$ for all $s \in \mathcal{S}$ and $m \in M$, and this follows directly from the relevant definitions: $s \circ \tilde{\varphi} \circ \Delta_m = s \circ \varphi_m = \varphi_{sm} = \tilde{\varphi} \circ \Delta_{sm} = \tilde{\varphi} \circ s \circ \Delta_m$.

QED

Finally, if $M = \mathcal{S}$ is a ring, then it is an $\mathcal{S}$ - $\mathcal{R}$ -bimodule and the above results hold. Also, we have a ring homomorphism $\mathcal{R} \rightarrow \mathcal{S}$ via $r \mapsto 1 \cdot r$, so an abelian variety X with an action of $\mathcal{S}$ also has an action of $\mathcal{R}$. With the extra structure in this case, we find an isomorphism $\text{Hom}_{\mathcal{S}-\mathcal{R}}(\mathcal{S}, \text{Hom}(A, X)) \xrightarrow{\sim} \text{Hom}^{\mathcal{R}}(A, X)$, by taking the element $s \mapsto \varphi_s$ of $\text{Hom}_{\mathcal{S}-\mathcal{R}}(\mathcal{S}, \text{Hom}(A, X))$ to φ_1 . The reason that $\varphi_1 : A \rightarrow X$ respects $\mathcal{R}$ is because $\mathcal{R}$ commutes with $1 \in \mathcal{S}$. Thus we may now rephrase the defining property of $\mathcal{S} \otimes_{\mathcal{R}} A$ in the category of abelian varieties up to isogeny:

Let A be an abelian variety with an action of $\mathcal{R}$, and let $\mathcal{S}$ be a ring which is also a right $\mathcal{R}$ -module. Then $\mathcal{S} \otimes_{\mathcal{R}} A$ is an abelian variety with an action of $\mathcal{S}$, together with a morphism $\Delta_1 : A \rightarrow \mathcal{S} \otimes_{\mathcal{R}} A$ respecting $\mathcal{R}$, which satisfies the following universal property: given an abelian variety X with an action of $\mathcal{S}$, and a morphism $\varphi : A \rightarrow X$ respecting $\mathcal{R}$, there exists a unique morphism $\tilde{\varphi} : \mathcal{S} \otimes_{\mathcal{R}} A \rightarrow X$ respecting $\mathcal{S}$ such that $\varphi = \tilde{\varphi} \circ \Delta_1$.

Galois Action

Now suppose that A is defined over $\overline{\mathbb{Q}}$; let us consider the effect of twisting by $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = G_{\mathbb{Q}}$ on the tensor product construction. Note that if A is an abelian variety with an action of $\mathcal{R}$, then so is ${}^{\sigma}A$, for each $\sigma \in G_{\mathbb{Q}}$; we may map $\mathcal{R} \rightarrow \text{End}(A) \rightarrow \text{End}({}^{\sigma}A)$ via the usual “twist-by- σ ”.

Lemma 3.6 *Let A, A_1, A_2 be abelian varieties over $\overline{\mathbb{Q}}$ with actions of $\mathcal{R}$, and let M, M_1, M_2 be right $\mathcal{R}$ -modules.*

1. *For each $\sigma \in G_{\mathbb{Q}}$, we have ${}^{\sigma}(M \otimes_{\mathcal{R}} A) \sim M \otimes_{\mathcal{R}} {}^{\sigma}A$.*
2. *Let $f \in \text{Hom}_{\mathcal{R}}(M_1, M_2)$, let $\varphi \in \text{Hom}^{\mathcal{R}}(A_1, A_2)$, and let $f \otimes \varphi$ be the induced map $M_1 \otimes_{\mathcal{R}} A_1 \rightarrow M_2 \otimes_{\mathcal{R}} A_2$ defined by property (v) above. Then for each $\sigma \in G_{\mathbb{Q}}$, we have ${}^{\sigma}(f \otimes \varphi) = f \otimes {}^{\sigma}\varphi$.*

Proof.

1. Fix $\sigma \in G_{\mathbb{Q}}$. We will demonstrate that ${}^{\sigma}(M \otimes_{\mathcal{R}} A)$ satisfies the defining property (3.2) of $M \otimes_{\mathcal{R}} {}^{\sigma}A$. First construct $M \otimes_{\mathcal{R}} A$ and $\Delta : M \rightarrow \text{Hom}(A, M \otimes_{\mathcal{R}} A)$. Then for an abelian variety $X/\overline{\mathbb{Q}}$, the map Δ induces an isomorphism $\text{Hom}(M \otimes_{\mathcal{R}} A, X) \rightarrow \text{Hom}_{\mathcal{R}}(M, \text{Hom}(A, X))$. Now if one defines ${}^{\sigma}\Delta : M \rightarrow \text{Hom}_{\mathcal{R}}({}^{\sigma}A, {}^{\sigma}(M \otimes_{\mathcal{R}} A))$ as $({}^{\sigma}\Delta)_m \stackrel{\text{def}}{=} {}^{\sigma}(\Delta_m)$, then ${}^{\sigma}\Delta$ induces an isomorphism $\text{Hom}({}^{\sigma}(M \otimes_{\mathcal{R}} A), {}^{\sigma}X) \rightarrow \text{Hom}_{\mathcal{R}}(M, \text{Hom}({}^{\sigma}A, {}^{\sigma}X))$. But of course any abelian variety may be written as ${}^{\sigma}X$ for some X , so ${}^{\sigma}(M \otimes_{\mathcal{R}} A)$ and ${}^{\sigma}\Delta$ do satisfy the characteristic property of $M \otimes_{\mathcal{R}} {}^{\sigma}A$.
2. The map $f \otimes \varphi$ is defined to be the unique morphism $M_1 \otimes_{\mathcal{R}} A_1 \rightarrow M_2 \otimes_{\mathcal{R}} A_2$ such that $(f \otimes \varphi) \circ \Delta_m = \Delta_{f(m)} \circ \varphi$ for all $m \in M_1$. Applying σ to both sides, we find ${}^{\sigma}(f \otimes \varphi) \circ {}^{\sigma}\Delta_m = {}^{\sigma}\Delta_{f(m)} \circ {}^{\sigma}\varphi = (f \otimes {}^{\sigma}\varphi) \circ {}^{\sigma}\Delta_m$ for all $m \in M_1$, which implies that ${}^{\sigma}(f \otimes \varphi) = f \otimes {}^{\sigma}\varphi$. *QED*

Chapter 4

Descent from $\overline{\mathbb{Q}}$ to $\mathbb{Q}$

In this chapter we will show how to construct, from a given building block B , an abelian variety $A/\mathbb{Q}$ of $\mathbf{GL}_2$ -type with B as a simple quotient over $\overline{\mathbb{Q}}$. We will then describe a precise correspondence between these two types of abelian varieties. Recall the following definitions.

Definition. An abelian variety $B/\overline{\mathbb{Q}}$ is a $\mathbb{Q}$ -*abelian variety* if for each $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, there exists an isogeny $\mu_\sigma : {}^\sigma B \rightarrow B$ compatible with the endomorphisms of B ; that is, $\mu_\sigma \circ {}^\sigma \varphi = \varphi \circ \mu_\sigma$ for all $\varphi \in \text{End}(B)$.

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

- (i) the endomorphism algebra $\text{End}(B)$ is a central division algebra over a totally real field F with Schur index $t = 1$ or 2 , and $t[F:\mathbb{Q}] = \dim B$.
- (ii) B is a $\mathbb{Q}$ -abelian variety.

Definition. An abelian variety $A/\mathbb{Q}$ is of $\mathbf{GL}_2$ -type if $\text{End}_{\mathbb{Q}}(A)$, the algebra of endomorphisms of A defined over $\mathbb{Q}$, is a number field of degree equal to the dimension of A .

Construction of an Abelian Variety of $\mathbf{GL}_2$ -type

We write $G_{\mathbb{Q}}$ for the absolute Galois group $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with its usual profinite topology. Let B be a building block. Then, by definition, B is a $\mathbb{Q}$ -abelian variety. We have seen in Chapter 2 how to fix for each $\sigma \in G_{\mathbb{Q}}$ a choice of $\mu_\sigma : {}^\sigma B \rightarrow B$ respecting $\text{End}(B)$ such that $c(\sigma, \tau) = \mu_\sigma \circ {}^\sigma \mu_\tau \circ \mu_{\sigma\tau}^{-1}$ is a locally constant two-cocycle on $G_{\mathbb{Q}}$ with values in F^*

(a $G_{\mathbb{Q}}$ -module with trivial action). The class $[c] \in H^2(G_{\mathbb{Q}}, F^*)$ is independent of our choices for μ_{σ} .

Now consider the cohomology group $H^2(G_{\mathbb{Q}}, \overline{F}^*)$, where $G_{\mathbb{Q}}$ acts trivially on $\overline{F}^*$. By a theorem of Tate [Se 3, Thm. 4], this group is trivial. Therefore the image of $[c]$ in $H^2(G_{\mathbb{Q}}, \overline{F}^*)$ is a coboundary; that is, there exists a locally constant function $\beta : G_{\mathbb{Q}} \rightarrow \overline{F}^*$ such that $c(\sigma, \tau) = \beta(\sigma) \cdot \beta(\tau) \cdot \beta(\sigma\tau)^{-1}$ for all $\sigma, \tau \in G_{\mathbb{Q}}$. Fix such a function β . Let E be the field extension of F obtained by adjoining all the values $\beta(\sigma)$. Then E is a finite extension of F (as β is locally constant); set $d = [E:F]$.

Consider the abelian variety $E \otimes_F B$. From Equation 3.4 there is a map

$$(4.1) \quad \text{End}_F E \otimes_F \text{End}(B) \rightarrow \text{End}(E \otimes_F B).$$

We claim this map is an isomorphism of F -algebras. Indeed, fix a basis of E over F . Then we see that $\text{End}_F E$ is isomorphic to the matrix algebra $\mathbf{M}_d(F)$, and so the image of $\text{End}_F E \otimes_F \text{End}(B)$ in $\text{End}(E \otimes_F B)$ is isomorphic to $\mathbf{M}_d(\text{End}(B))$. On the other hand, the same choice of basis for E/F gives us $E \otimes_F B \sim (\bigoplus^d F) \otimes_F B \sim \prod^d B$, so the endomorphism algebra $\text{End}(E \otimes_F B)$ must itself be isomorphic to $\mathbf{M}_d(\text{End}(B))$. From now on we will frequently identify $\text{End}(E \otimes_F B)$ with $\text{End}_F E \otimes_F \text{End}(B)$.

Now we claim that we may descend the abelian variety $E \otimes_F B$ to $\mathbb{Q}$.

For each $\sigma \in G_{\mathbb{Q}}$, define $\nu_{\sigma} \stackrel{\text{def}}{=} \beta(\sigma)^{-1} \otimes \mu_{\sigma} \in \text{Hom}(E \otimes_F {}^{\sigma}B, E \otimes_F B)$, using our fixed $\beta(\sigma)$ and μ_{σ} . Recall that by Lemma 3.6, we have $E \otimes_F {}^{\sigma}B \sim {}^{\sigma}(E \otimes_F B)$; therefore ν_{σ} may be viewed as an isogeny ${}^{\sigma}(E \otimes_F B) \rightarrow E \otimes_F B$.

Proposition 4.2 *There exists an abelian variety A_0 over $\mathbb{Q}$ and an isogeny (over $\overline{\mathbb{Q}}$) $\kappa : E \otimes_F B \rightarrow A_0$ such that $\kappa^{-1} \circ {}^{\sigma}\kappa = \nu_{\sigma}$ for all $\sigma \in G_{\mathbb{Q}}$.*

Proof. First, we see that $\nu_{\sigma} \circ {}^{\sigma}\nu_{\tau} = \nu_{\sigma\tau}$ for all $\sigma, \tau \in G_{\mathbb{Q}}$. Indeed, by using the definitions of $c(\sigma, \tau)$ and $\beta(\sigma)$, and the properties of the tensor product from Chapter 3, we have

$$\begin{aligned} \nu_{\sigma} \circ {}^{\sigma}\nu_{\tau} &= \beta(\sigma)^{-1} \beta(\tau)^{-1} \otimes \mu_{\sigma} \circ {}^{\sigma}\mu_{\tau} \\ &= \beta(\sigma\tau)^{-1} c(\sigma, \tau)^{-1} \otimes c(\sigma, \tau) \mu_{\sigma\tau} \\ &= \beta(\sigma\tau)^{-1} \otimes \mu_{\sigma\tau} \\ &= \nu_{\sigma\tau}. \end{aligned}$$

Therefore, we may apply the method of [Ri 1, Thm. 8.2] to construct A_0 . More explicitly, let K be a finite Galois extension of $\mathbb{Q}$ such that $E \otimes_F B$ is defined over K and

all ν_σ are defined over K . Let X be the abelian variety $\text{Res}_{K/\mathbb{Q}}(E \otimes_F B)$, where “Res” denotes Weil’s “restriction of scalars” functor. (See [We, §1.3].) Then X is defined over $\mathbb{Q}$ and $X_{/K} \cong \prod_g (E \otimes_F B)$, where the product runs over $g \in \text{Gal}(K/\mathbb{Q})$. We now define $\kappa = (\nu_g^{-1})_g : E \otimes_F B \rightarrow X_{/K}$. Lastly, write A_0 for the image of κ (or technically, the image of a suitable multiple of κ).

A direct (if tiresome) computation yields the formula $\kappa^{-1} \circ {}^\sigma \kappa = \nu_\sigma$. QED

Next we ask which endomorphisms of A_0 are defined over $\mathbb{Q}$? Or more generally, how does $\sigma \in G_{\mathbb{Q}}$ act on $\text{End}(A_0)$?

Proposition 4.3 *For each $\sigma \in G_{\mathbb{Q}}$, the automorphism $\varphi \mapsto {}^\sigma \varphi$ of $\text{End}(A_0)$ is equal to conjugation by $\beta(\sigma)^{-1} \in E$. (Here the action of E on A_0 is induced by κ .)*

Proof. The isogeny κ induces an isomorphism $\text{End}(A_0) \xrightarrow{\sim} \text{End}(E \otimes_F B)$ via $\varphi \mapsto \kappa^{-1} \circ \varphi \circ \kappa$. Thus, the automorphism $\varphi \mapsto {}^\sigma \varphi$ on $\text{End}(A_0)$ translates into the automorphism $\kappa^{-1} \circ \varphi \circ \kappa \mapsto \kappa^{-1} \circ {}^\sigma \varphi \circ \kappa$ on $\text{End}(E \otimes_F B)$. Now we may write

$$\begin{aligned} \kappa^{-1} \circ {}^\sigma \varphi \circ \kappa &= \kappa^{-1} \circ (\sigma \kappa \circ \sigma \kappa^{-1}) \circ {}^\sigma \varphi \circ (\sigma \kappa \circ \sigma \kappa^{-1}) \circ \kappa \\ &= \nu_\sigma \circ {}^\sigma (\kappa^{-1} \circ \varphi \circ \kappa) \circ \nu_\sigma^{-1} && \text{because } \kappa^{-1} \circ \sigma \kappa = \nu_\sigma; \\ &= (\beta(\sigma)^{-1} \otimes 1) \circ (1 \otimes \mu_\sigma) \circ {}^\sigma (\kappa^{-1} \circ \varphi \circ \kappa) \circ (1 \otimes \mu_\sigma^{-1}) \circ (\beta(\sigma) \otimes 1) && \text{by def. of } \nu_\sigma; \\ &= (\beta(\sigma)^{-1} \otimes 1) \circ (\kappa^{-1} \circ \varphi \circ \kappa) \circ (\beta(\sigma) \otimes 1). \end{aligned}$$

The last equality follows because for all $\psi \in \text{End}(E \otimes_F B)$, we have $(1 \otimes \mu_\sigma) \circ {}^\sigma \psi = \psi \circ (1 \otimes \mu_\sigma)$. Indeed, write ψ as an element of the tensor product $\text{End}_F E \otimes_F \text{End}(B)$ and use the fact that each μ_σ was originally chosen to be compatible with $\text{End}(B)$.

Finally, translating back to $\text{End}(A_0)$, we see ${}^\sigma \varphi = \beta(\sigma)^{-1} \circ \varphi \circ \beta(\sigma)$. QED

Proposition 4.4 *Under the isomorphism $\text{End}(A_0) \xrightarrow{\sim} \text{End}_F E \otimes_F \text{End}(B)$ induced by the isogeny κ , we have $\text{End}_{\mathbb{Q}}(A_0) \cong E \otimes_F \text{End}(B)$.*

Proof. By applying the above proposition we find that the endomorphisms of A_0 which are fixed by all $\sigma \in G_{\mathbb{Q}}$ are exactly those which commute with all $\beta(\sigma)$. Thus $\text{End}_{\mathbb{Q}}(A_0)$ is an F -subalgebra of $\text{End}(A_0)$; in fact, $\text{End}_{\mathbb{Q}}(A_0)$ is the centralizer $C(E)$ of E in $\text{End}(A_0)$, since E was defined to be the field generated over F by the $\beta(\sigma)$.

Now it is clear that $C(E)$ is contained in $E \otimes_F \text{End}(B)$, so it suffices to show that these subalgebras have the same dimension over F . Recall that we have written

$d = [E:F]$ and $t = 1$ or $2 = \text{Schur index of } \text{End}(B)$. Then $\dim_F E \cdot \dim_F(E \otimes_F \text{End}(B)) = d(dt^2) = \dim_F \text{End}(A_0)$. Therefore, by the Double Centralizer Theorem [Pi, Thm. 12.7], $\dim_F C(E) = \dim_F(E \otimes_F \text{End}(B))$. QED

Proposition 4.5 *There exists an abelian variety $A/\mathbb{Q}$ of $\mathbf{GL}_2$ -type containing B as a simple component.*

Proof. We have seen by Theorem 2.1 that if we send the class of the cocycle $c(\sigma, \tau)$, $[c] \in H^2(G_{\mathbb{Q}}, F^*) \rightarrow H^2(G_{\mathbb{Q}}, (\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^*) \xrightarrow{\sim} \text{Br}(F)$ via the natural maps, then its image in the Brauer group is the class of $\text{End}(B)$. Now consider what happens upon extending to the field E . There is a commutative diagram:

$$\begin{array}{ccccc} H^2(G_{\mathbb{Q}}, F^*) & \longrightarrow & H^2(G_{\mathbb{Q}}, (\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} F)^*) & \cong & \text{Br}(F) \\ \downarrow & & \downarrow & & \downarrow \\ H^2(G_{\mathbb{Q}}, E^*) & \longrightarrow & H^2(G_{\mathbb{Q}}, (\overline{\mathbb{Q}} \otimes_{\mathbb{Q}} E)^*) & \cong & \text{Br}(E) \end{array}$$

On the one hand, $[c] \in H^2(G_{\mathbb{Q}}, F^*)$ maps to the class of $\text{End}(B)$ in $\text{Br}(F)$, which maps to the class of $E \otimes_F \text{End}(B)$ in $\text{Br}(E)$. But on the other hand, c splits when taking values in E ; in fact, this is how E was originally defined. In other words, the image of $[c]$ is trivial in $H^2(G_{\mathbb{Q}}, E^*)$, and hence maps to the trivial class in $\text{Br}(E)$. Therefore $E \otimes_F \text{End}(B)$ must be isomorphic to the matrix algebra $\mathbf{M}_t(E)$, where $t = 1$ or 2 is the Schur index of $\text{End}(B)$.

Fix an isomorphism $E \otimes_F \text{End}(B) \xrightarrow{\sim} \mathbf{M}_t(E)$. Then by the previous proposition, we have $\text{End}_{\mathbb{Q}}(A_0) \xrightarrow{\sim} \mathbf{M}_t(E)$. This isomorphism implies that A_0 must be isogenous over $\mathbb{Q}$ to A^t , where A is an abelian variety over $\mathbb{Q}$ with $\text{End}_{\mathbb{Q}}(A) = E$. (For instance, we may define A to be the image of the endomorphism of A_0 corresponding to the matrix that has a 1 in the upper left corner and zeroes elsewhere.)

Now remember that $E \otimes_F B$ is isogenous to a product of d copies of B , where $d = [E:F]$. It follows that $A^t_{/\overline{\mathbb{Q}}} \sim B^d$, and therefore $A_{/\overline{\mathbb{Q}}} \sim B^{d/t}$. Thus B is a simple component of A . We have already seen that $\text{End}_{\mathbb{Q}}(A) = E$, so to complete the proof we need only calculate the dimension of A in order to show that A is of $\mathbf{GL}_2$ -type. Recall that because B is a building block, we have $\dim B = t[F:\mathbb{Q}]$. Thus the dimension of A is $\frac{d}{t} \dim B = d[F:\mathbb{Q}] = [E:\mathbb{Q}]$, and we see that A is of $\mathbf{GL}_2$ -type, as desired. QED

A More Precise Correspondence

Notice that it was necessary to make several choices in our construction of an abelian variety $A/\mathbb{Q}$ of $\mathbf{GL}_2$ -type from a building block B . We now ask if there is any way to make the correspondence between these two types of abelian varieties more precise. If we start with an $A/\mathbb{Q}$ of $\mathbf{GL}_2$ -type and decompose it into building blocks, what information must we record in order to recover the “same” $A/\mathbb{Q}$ via the above procedure? The main idea is to keep track of the “descent data”—the ν_σ —which provide the isogeny from $B \times \dots \times B$ (defined over $\overline{\mathbb{Q}}$) to A (defined over $\mathbb{Q}$).

First, however, we must say what it means for two abelian varieties of $\mathbf{GL}_2$ -type to be the “same”.

Definition. A $\mathbf{GL}_2$ -type pair is a pair (A, i) where A is an abelian variety over $\mathbb{Q}$ of $\mathbf{GL}_2$ -type and i is an injection $\text{End}_{\mathbb{Q}}(A) \hookrightarrow \overline{\mathbb{Q}}$.

Definition. Two $\mathbf{GL}_2$ -type pairs (A, i) and (A', i') are *equivalent* if there exists an isogeny $a : A \rightarrow A'$ that is defined over $\mathbb{Q}$ and satisfies $i'(a \circ \varphi \circ a^{-1}) = i(\varphi)$ for all $\varphi \in \text{End}_{\mathbb{Q}}(A)$.

We make similar definitions for building blocks.

Definition. A *building block triple* is a triple $(B, j, \{\nu_\sigma\}_{\sigma \in G_{\mathbb{Q}}})$ where

- B is a building block, and we write $\mathcal{B} = \text{End}(B)$;
- j is an injection of the center $Z(\text{End}(B)) \hookrightarrow \overline{\mathbb{Q}}$, and we write F for the image of j ;
- for each $\sigma \in G_{\mathbb{Q}}$, ν_σ is a non-zero element of $\overline{\mathbb{Q}} \otimes_F \text{Hom}^{\mathcal{B}}({}^\sigma B, B)$ such that the family $\{\nu_\sigma\}$ is locally constant and satisfies $\nu_\sigma \circ {}^\sigma \nu_\tau = \nu_{\sigma\tau}$ for all $\sigma, \tau \in G_{\mathbb{Q}}$.

Definition. Two building block triples $(B, j, \{\nu_\sigma\})$ and $(B', j', \{\nu'_\sigma\})$ are *equivalent* if there exists an isogeny $b : B \rightarrow B'$ such that $j'(b \circ \varphi \circ b^{-1}) = j(\varphi)$ for all $\varphi \in Z(\text{End}(B))$, and $\nu'_\sigma = b \circ \nu_\sigma \circ {}^\sigma b^{-1}$ for all $\sigma \in G_{\mathbb{Q}}$.

Suppose we are given a building block triple $(B, j, \{\nu_\sigma\})$. Note that for each σ , $\text{Hom}^{\mathcal{B}}({}^\sigma B, B)$ is a one-dimensional F -vector space; the choice of an isogeny $\mu_\sigma : {}^\sigma B \rightarrow B$ respecting $\mathcal{B}$ then determines $\beta(\sigma) \in \overline{\mathbb{Q}}^*$ such that ν_σ may be written as $\beta(\sigma)^{-1} \otimes \mu_\sigma$. Let $E \subset \overline{\mathbb{Q}}$ be the field that is generated over F by the values $\beta(\sigma)$; then because each $\beta(\sigma)$ is well-defined modulo F^* , we see that E depends only on the ν_σ , and not on our choices for

μ_σ . The field E is a finite extension of F because the collection $\{\nu_\sigma\}$ is locally constant. Now we may view each ν_σ as an element of $\text{Hom}(E \otimes_F {}^\sigma B, E \otimes_F B)$ and construct an abelian variety of $\mathbf{GL}_2$ -type using the procedure described in the previous section.

We claim there is the following relationship between building block triples and $\mathbf{GL}_2$ -type pairs.

Theorem 4.6 *The above construction, which associates a $\mathbf{GL}_2$ -type pair (A, i) to a building block triple $(B, j, \{\nu_\sigma\})$, induces a bijection on equivalence classes.*

We break the proof into several steps.

Step 1 *The correspondence $(B, j, \{\nu_\sigma\}) \rightsquigarrow (A, i)$ is well-defined on equivalence classes.*

Suppose the triple $(B, j, \{\nu_\sigma\})$ is equivalent to $(B', j', \{\nu'_\sigma\})$. Fix an isogeny $b : B \rightarrow B'$ satisfying the stated conditions for equivalence. Our first observation is that the image of j' is equal to the image of j ; we will call their common image F and identify $Z(\mathcal{B})$ and $Z(\mathcal{B}')$ with F . Also, the isogeny b induces an isomorphism $\text{End}(B) \cong \text{End}(B')$, and in particular, we note that $\text{End}(B)$ and $\text{End}(B')$ have the same Schur index $t = 1$ or 2 as central simple F -algebras.

Next, for each $\sigma \in G_{\mathbb{Q}}$, pick $\mu_\sigma \in \text{Hom}({}^\sigma B, B)$ and write $\nu_\sigma = \beta(\sigma)^{-1} \otimes \mu_\sigma$. Then the fact that $\nu'_\sigma = b \circ \nu_\sigma \circ {}^\sigma b^{-1}$ implies that we may write $\nu'_\sigma = \beta(\sigma)^{-1} \otimes (b \circ \mu_\sigma \circ {}^\sigma b^{-1})$. Thus the subfield of $\overline{\mathbb{Q}}$ generated over F by the coefficients of the ν'_σ is the same as the one generated by the coefficients of the ν_σ . Call this field E . Now our construction yields isogenies $\kappa : E \otimes_F B \rightarrow A^t$ and $\kappa' : E \otimes_F B' \rightarrow A'^t$ where A and A' are abelian varieties over $\mathbb{Q}$ of $\mathbf{GL}_2$ -type with $E \xrightarrow{\sim} \text{End}_{\mathbb{Q}}(A)$ and $E \xrightarrow{\sim} \text{End}_{\mathbb{Q}}(A')$. These actions of E on A and A' define the pairs (A, i) and (A', i') , respectively.

Now $a = \kappa' \circ (1 \otimes b) \circ \kappa^{-1}$ is an isogeny $A^t \rightarrow A'^t$. We claim it is an isogeny defined over $\mathbb{Q}$. Indeed, for any $\sigma \in G_{\mathbb{Q}}$ we have:

$$\begin{aligned} \sigma(\kappa' \circ (1 \otimes b) \circ \kappa^{-1}) &= (\kappa' \circ \kappa'^{-1}) \circ {}^\sigma \kappa' \circ (1 \otimes {}^\sigma b) \circ {}^\sigma \kappa^{-1} \circ (\kappa \circ \kappa^{-1}) \\ &= \kappa' \circ \nu'_\sigma \circ (1 \otimes {}^\sigma b) \circ \nu_\sigma^{-1} \circ \kappa^{-1} \\ &= \kappa' \circ (1 \otimes b) \circ \nu_\sigma \circ \nu_\sigma^{-1} \circ \kappa^{-1} \\ &= \kappa' \circ (1 \otimes b) \circ \kappa^{-1}. \end{aligned}$$

Moreover, κ , $1 \otimes b$ and κ' all respect the action of $E \otimes_F \mathcal{B}$. (Here we are using the isomorphism $\mathcal{B}' \cong \mathcal{B}$ induced by b to define the action of $E \otimes_F \mathcal{B}$ on $E \otimes_F B'$ and A'^t .)

Therefore, a respects the action of $E \otimes_F \mathcal{B} \cong \mathbf{M}_t(E)$. But it is easy to see that the natural map $\mathrm{Hom}^E(A, A') \rightarrow \mathrm{Hom}^{\mathbf{M}_t(E)}(A^t, A'^t)$ is an isomorphism, so in fact we may regard a as a morphism $A \rightarrow A'$. Then a is an isogeny defined over $\mathbb{Q}$ that respects E ; that is, a defines an equivalence of pairs (A, i) and (A', i') , as desired.

Step 2 Define the inverse correspondence from pairs (A, i) to triples $(B, j, \{\nu_\sigma\})$.

Let (A, i) be a $\mathbf{GL}_2$ -type pair. Write $\mathcal{A}$ for the full endomorphism algebra $\mathrm{End}(A)$, E for the image of i , and $F = i(Z(\mathcal{A}))$. By our usual abuse of notation, we will use i to identify E and F with the corresponding subalgebras of $\mathcal{A}$. Recall that $\mathcal{A}$ is a central simple algebra over F , by Theorem 1.3. Thus $\mathcal{A}$ has a unique (up to isomorphism) simple right $\mathcal{A}$ -module. Fix such a simple module M .

Let $B = M \otimes_{\mathcal{A}} A$. We claim that B is a building block. By Propositions 1.4 and 1.5, it suffices to show that B is a simple component of A . Now because $\mathcal{A}$ is a simple algebra, for some n we have $\mathcal{A} \cong \bigoplus^n M$ as right $\mathcal{A}$ -modules. Fix such an isomorphism. Then

$$A = \mathcal{A} \otimes_{\mathcal{A}} A \sim (\bigoplus^n M) \otimes_{\mathcal{A}} A \sim \prod^n (M \otimes_{\mathcal{A}} A) \sim \prod^n B.$$

Thus B is a subvariety of A . It remains to show that B is simple.

By [Pi, Cor. 3.5a], $\mathcal{A}$ is isomorphic to $\mathbf{M}_n(\mathcal{B})$, where $\mathcal{B} \stackrel{\mathrm{def}}{=} \mathrm{End}_{\mathcal{A}} M$ is a central division algebra over F . But the above isogeny $A \sim \prod^n B$ implies that $\mathcal{A} \cong \mathbf{M}_n(\mathrm{End}(B))$. Therefore we must have that $\mathrm{End}(B) \cong \mathcal{B}$ is a division algebra, and so B is simple.

We remark that in fact we have an explicit isomorphism $\mathcal{B} \rightarrow \mathrm{End}(B)$, namely the one arising from the general map (3.4):

$$(4.7) \quad \begin{array}{ccc} \mathrm{End}_{\mathcal{A}} M \otimes_F \mathrm{End}^{\mathcal{A}}(A) & \longrightarrow & \mathrm{End}(B) \\ \mathcal{B} \otimes_F F & \xrightarrow{\sim} & \mathrm{End}(B). \end{array}$$

This map induces an isomorphism $F \xrightarrow{\sim} Z(\mathrm{End}(B))$, whose inverse provides us with the definition of j in the building block triple we will associate with B .

For future reference, we write t for the common Schur index of $\mathrm{End}(A)$ and $\mathrm{End}(B)$ (remember $t = 1$ or 2), and note that $[E:F] = nt$, because E is a maximal subfield of $\mathcal{A}$ by Theorem 1.3.

Now we need to define ν_σ for each $\sigma \in G_{\mathbb{Q}}$. We will do so by constructing an isogeny $\kappa : E \otimes_F B \rightarrow A^t$. Because $B = M \otimes_{\mathcal{A}} A$, we will view $E \otimes_F B$ as $(E \otimes_F M) \otimes_{\mathcal{A}} A$.

Note that $E \otimes_F M$ is an $(E \otimes_F \mathcal{B})$ - $\mathcal{A}$ -bimodule. Furthermore, we know that E

splits $\mathcal{B}$ (because E is a maximal subfield of $\mathcal{A}$), so we may fix an isomorphism

$$E \otimes_F \mathcal{B} \xrightarrow{\sim} \mathbf{M}_t(E) \cong \text{End}_{\mathbb{Q}}(A^t).$$

In this way we obtain an action of $E \otimes_F \mathcal{B}$ on A^t , and so, a left action of $E \otimes_F \mathcal{B}$ on $\text{Hom}(A, A^t)$. Now choose an isomorphism of $(E \otimes_F \mathcal{B})$ - $\mathcal{A}$ -bimodules $E \otimes_F M \rightarrow \text{Hom}(A, A^t)$. (They are abstractly isomorphic because they have the same dimension— $n^2 t^3$ —over F [Pi, Cor. 3.3b].) Then by the defining property of the tensor product (3.2), there is a morphism $\kappa : (E \otimes_F M) \otimes_{\mathcal{A}} A \rightarrow A^t$ that respects the actions of $E \otimes_F \mathcal{B}$ (Proposition 3.5).

We claim this morphism is an isogeny. Indeed, the image of κ is a subvariety of A^t with an action of $E \otimes_F \mathcal{B} \cong \mathbf{M}_t(E)$. But the only subvarieties of A^t mapped into themselves by $\mathbf{M}_t(E)$ are the zero subvariety and all of A^t . Now κ cannot be the zero morphism, because the homomorphism of modules used to define κ was non-zero. Therefore the image of κ must be A^t . Now we note that as right $\mathcal{A}$ -modules, $E \otimes_F M \cong \bigoplus^{nt} M \cong \bigoplus^t \mathcal{A}$, so the dimension of $(E \otimes_F M) \otimes_{\mathcal{A}} A$ is equal to the dimension of A^t . Thus κ is an isogeny.

We are now able to define the ν_{σ} . Consider $\kappa^{-1} \circ {}^{\sigma}\kappa : E \otimes_F {}^{\sigma}B \rightarrow E \otimes_F B$, which is an isogeny respecting $E \otimes_F \mathcal{B}$. The fact that

$$\text{Hom}^{E \otimes \mathcal{B}}(E \otimes_F {}^{\sigma}B, E \otimes_F B) \cong E \otimes_F \text{Hom}^{\mathcal{B}}({}^{\sigma}B, B)$$

follows from $\text{End}^{E \otimes \mathcal{B}}(E \otimes_F B) \cong E$ (which we know from the proof of Proposition 4.4). Hence we may write $\nu_{\sigma} = \kappa^{-1} \circ {}^{\sigma}\kappa \in E \otimes_F \text{Hom}^{\mathcal{B}}({}^{\sigma}B, B)$. Plainly, $\nu_{\sigma} \circ {}^{\sigma}\nu_{\tau} = \nu_{\sigma\tau}$ as desired.

Lastly we must check that the ν_{σ} do not depend on the various module isomorphisms chosen above. Suppose we make different choices and construct $\kappa' : E \otimes_F B \rightarrow A^t$ respecting $E \otimes_F \mathcal{B}$. Then $\kappa' \circ \kappa^{-1} : A^t \rightarrow A^t$ is an isogeny respecting $E \otimes_F \mathcal{B} \cong \mathbf{M}_t(E)$. But the only endomorphisms of A^t that respect $\mathbf{M}_t(E)$ lie in E , and are therefore defined over $\mathbb{Q}$. Hence ${}^{\sigma}(\kappa' \circ \kappa^{-1}) = \kappa' \circ \kappa^{-1}$ for all $\sigma \in G_{\mathbb{Q}}$, and we see $\nu'_{\sigma} = \kappa'^{-1} \circ {}^{\sigma}\kappa' = \kappa^{-1} \circ {}^{\sigma}\kappa = \nu_{\sigma}$ is independent of our choices.

Thus to the $\mathbf{GL}_2$ -type pair (A, i) we associate the triple $(B, j, \{\nu_{\sigma}\})$.

Step 3 *The correspondence defined in Step 2 is well-defined on equivalence classes.*

Suppose (A', i') is a pair that is equivalent to (A, i) . Write $\mathcal{A} = \text{End}(A)$ and $\mathcal{A}' = \text{End}(A')$. Let $a : A \rightarrow A'$ be an isogeny which satisfies the stated conditions for the equivalence of pairs. Then a induces an isomorphism $\mathcal{A} \xrightarrow{\sim} \mathcal{A}'$ via $\varphi \mapsto a \circ \varphi \circ a^{-1}$.

First notice that the image of i' is the same as the image of i ; we will call their

common image E . Also $i'(Z(\mathcal{A}')) = i(Z(\mathcal{A}))$, which we will call F . Henceforth we will identify E and F with these subalgebras of the endomorphism algebras.

Now let M be a simple right $\mathcal{A}$ -module, and M' a simple right $\mathcal{A}'$ -module. Form $B = M \otimes_{\mathcal{A}} A$ and $B' = M' \otimes_{\mathcal{A}'} A'$, and the accompanying data j, j', ν_{σ} , and ν'_{σ} as above. Now we use the isomorphism $\mathcal{A} \xrightarrow{\sim} \mathcal{A}'$ to view A' as an abelian variety with an action of $\mathcal{A}$, and M' as an $\mathcal{A}$ -module. Then we may write $B' = M' \otimes_{\mathcal{A}} A'$.

Because $\mathcal{A}$ has a unique simple right module, there must be an isomorphism of $\mathcal{A}$ -modules $f : M \rightarrow M'$. Define $b : B \rightarrow B'$ to be the morphism $f \otimes a : M \otimes_{\mathcal{A}} A \rightarrow M' \otimes_{\mathcal{A}} A'$. Then b is an isogeny because both f and a are invertible, and b respects the action of F , because F commutes with everything in sight.

It remains to show that $\nu'_{\sigma} = b \circ \nu_{\sigma} \circ \sigma b^{-1}$ for each $\sigma \in G_{\mathbb{Q}}$. Remember that ν_{σ} is defined as $\kappa^{-1} \circ \sigma \kappa$ where κ is an isogeny $E \otimes_F B \rightarrow A^t$ respecting $E \otimes_F \mathcal{B}$, and similarly ν'_{σ} is defined in terms of $\kappa' : E \otimes_F B' \rightarrow A'^t$. Now notice that $a^{-1} \circ \kappa' \circ (1 \otimes b) \circ \kappa^{-1}$ is an endomorphism of A^t respecting $E \otimes_F \mathcal{B} \cong \mathbf{M}_t(E)$. But the only such endomorphisms are elements of E , which are endomorphisms defined over $\mathbb{Q}$. Therefore $\kappa' \circ (1 \otimes b) \circ \kappa^{-1}$ is defined over $\mathbb{Q}$, so $\sigma(\kappa' \circ (1 \otimes b) \circ \kappa^{-1}) = \kappa' \circ (1 \otimes b) \circ \kappa^{-1}$ for all $\sigma \in G_{\mathbb{Q}}$, and it follows that $\nu'_{\sigma} = b \circ \nu_{\sigma} \circ \sigma b^{-1}$.

Step 4 *The above correspondences are inverse to each other.*

Suppose we start with a $\mathbf{GL}_2$ -type pair (A, i) , and use it to construct a building block triple $(B, j, \{\nu_{\sigma}\})$. Then from the map (4.7) we have $Z(\text{End}(A)) \xrightarrow{\sim} Z(\text{End}(B))$, so the field F is the same from both viewpoints. Next, we need to show the field $E = \text{image of } i$ is the same as the field E generated over F by the coefficients of the ν_{σ} . Write $\nu_{\sigma} = \beta(\sigma)^{-1} \otimes \mu_{\sigma}$, and remember these ν_{σ} are defined by an isogeny $\kappa : E \otimes_F B \rightarrow A^t$, where $t = 1$ or 2 . Then by Proposition 4.3 we find that for $\varphi \in \text{End}(A^t)$ and $\sigma \in G_{\mathbb{Q}}$, we have $\sigma \varphi = \beta(\sigma)^{-1} \circ \varphi \circ \beta(\sigma)$. Hence the same relationship holds for $\varphi \in \text{End}(A)$. In other words, these $\beta(\sigma)^{-1}$ are the same (up to F^*) as the $\alpha(\sigma)$ appearing in Chapter 1, and we have seen there (Proposition 1.6) that these elements do indeed generate $\text{End}_{\mathbb{Q}}(A)$ over F .

Now clearly when we construct $E \otimes_F B$ and descend it to $\mathbb{Q}$ via the map κ defined by the ν_{σ} , we are just recovering the map $\kappa : E \otimes_F (M \otimes_{\mathcal{A}} A) \rightarrow A^t$ we used to define the ν_{σ} to begin with. Therefore the map from pairs to triples and back to pairs is the identity on equivalence classes.

On the other hand, what happens when we start with a triple $(B, j, \{\nu_{\sigma}\})$ and

construct a pair (A, i) ? From (4.1) we have $Z(\text{End}(B)) \xrightarrow{\sim} Z(\text{End}(A^t)) \cong Z(\text{End}(A))$, and so again we may write F with no confusion. Now we want to show that the building block triple constructed from (A, i) is equivalent to the triple $(B, j, \{\nu_\sigma\})$.

Let M be a simple right $\mathcal{A}$ -module; we may view it as an F - $\mathcal{A}$ -bimodule. Choose an isomorphism of F - $\mathcal{A}$ -bimodules $M \rightarrow \text{Hom}(A, B)$; they are isomorphic because they have the same F -dimension. Then by the defining property of the tensor product (3.2), there is a morphism $M \otimes_{\mathcal{A}} A \rightarrow B$ respecting F . This morphism is an isogeny because it is non-zero by construction and because $M \otimes_{\mathcal{A}} A$ and B are simple abelian varieties. Call the inverse of this map b .

Finally, we have to show that the ν'_σ defined by (A, i) above are equal to $b \circ \nu_\sigma \circ \sigma b^{-1}$ for the original ν_σ associated with B . Let $\kappa : E \otimes_F B \rightarrow A^t$ be defined by the original ν_σ . Then $\kappa' = \kappa \circ (1 \otimes b)^{-1}$ is an isogeny $E \otimes_F (M \otimes_{\mathcal{A}} A) \rightarrow A^t$ respecting $E \otimes_F \text{End}(B)$, where the action of $\text{End}(B)$ on $M \otimes_{\mathcal{A}} A$ is induced by b . We have already seen that any such isogeny is valid for defining the ν'_σ , and so $\nu'_\sigma = \kappa'^{-1} \circ \sigma \kappa' = (1 \otimes b) \circ \kappa^{-1} \circ \sigma \kappa \circ (1 \otimes \sigma b^{-1}) = b \circ \nu_\sigma \circ \sigma b^{-1}$.

This proves Theorem 4.6.

Summary

Let $(B, j, \{\nu_\sigma\})$ be a building block triple; we will write $\nu_\sigma = \beta(\sigma)^{-1} \otimes \mu_\sigma$ with the understanding that the following formulas are independent of the transcriptions chosen. Let (A, i) be a $\mathbf{GL}_2$ -type pair corresponding to $(B, j, \{\nu_\sigma\})$ under Theorem 4.6. The chart below summarizes how to define, from either perspective, the most frequently used constructs associated to this situation.

Construct	$\mathbf{GL}_2$ -type pair (A, i)	Building block triple $(B, j, \{\nu_\sigma\}_{\sigma \in G_{\mathbb{Q}}})$
number field F	$i(Z(\text{End}(A)))$	$j(Z(\text{End}(B)))$
number field E	$i(\text{End}_{\mathbb{Q}}(A))$	extension of F generated by $\{\beta(\sigma) : \sigma \in G_{\mathbb{Q}}\}$
$\alpha : G_{\mathbb{Q}} \rightarrow E^*$ (well-defined mod F^*)	$\sigma \varphi = \alpha(\sigma) \circ \varphi \circ \alpha(\sigma)^{-1}$ for all $\varphi \in \text{End}(A)$	β^{-1}
$[c] \in H^2(G_{\mathbb{Q}}, F^*)$	class of $c(\sigma, \tau) = \alpha(\sigma\tau) \alpha(\sigma)^{-1} \alpha(\tau)^{-1}$	class of $c(\sigma, \tau) = \mu_\sigma \circ \sigma \mu_\tau \circ \mu_{\sigma\tau}^{-1}$

Chapter 5

Fields of Definition for Building Blocks

In this chapter we generalize results of Shimura and Ribet concerning various properties of building blocks, in particular, regarding their fields of definition. Recall that a (finite) compositum of quadratic extensions of a field is said to be a $(2, \dots, 2)$ -extension, and that such an extension is Galois with group $(\mathbb{Z}/2\mathbb{Z})^r$ for some r .

Theorem 5.1 *Let $B/\overline{\mathbb{Q}}$ be a building block. Then B is isogenous over $\overline{\mathbb{Q}}$ to an abelian variety defined over a $(2, \dots, 2)$ -extension of $\mathbb{Q}$.*

Elkies first proved this in the case when B is an elliptic curve [El]. Ribet generalized the result to the case of a building block with $\text{End}(B)$ a totally real field [Ri 2, Thm. 1.2]. In fact, similar arguments apply to the general case, and we follow his approach as we outline the proof below.

Remember that to a building block B we have associated a well-defined cohomology class $[c] \in H^2(G_{\mathbb{Q}}, F^*)$ (where $G_{\mathbb{Q}}$ acts trivially on F^*) by choosing isogenies $\mu_{\sigma} : {}^{\sigma}B \rightarrow B$ which respect $\text{End}(B)$ and defining a two-cocycle $c(\sigma, \tau) = \mu_{\sigma} \circ {}^{\sigma}\mu_{\tau} \circ \mu_{\sigma\tau}^{-1}$. We will see that the class $[c]$ provides certain information about a field of definition for B .

Definition. Let K be a number field. A *building block over K* is an abelian variety B over K such that $B/\overline{\mathbb{Q}}$ is a building block and all endomorphisms of B are defined over K .

Proposition 5.2 *Let K be a number field. Let B be a building block and $[c]$ its associated cohomology class. Then B is isogenous over $\overline{\mathbb{Q}}$ to a building block B_0 over K if and only if $[c]$ lies in the kernel of the restriction map $H^2(G_{\mathbb{Q}}, F^*) \rightarrow H^2(\text{Gal}(\overline{\mathbb{Q}}/K), F^*)$.*

Proof. Suppose B_0 is an abelian variety over K that is isogenous to B . Fix an isogeny $\kappa : B \rightarrow B_0$. Then for each $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/K)$, define $\mu_\sigma = \kappa^{-1} \circ \sigma \kappa : \sigma B \rightarrow B$; these isogenies respect $\text{End}(B)$ because by hypothesis all endomorphisms of B_0 are defined over K . Clearly now $c(\sigma, \tau) = 1$ for all $\sigma, \tau \in \text{Gal}(\overline{\mathbb{Q}}/K)$, and so $[c] = 1 \in H^2(\text{Gal}(\overline{\mathbb{Q}}/K), F^*)$.

Conversely, suppose $[c]$ is trivial in $H^2(\text{Gal}(\overline{\mathbb{Q}}/K), F^*)$. Choose a collection $\{\mu_\sigma\}$ as usual to define the two-cocycle $c(\sigma, \tau)$. Then for $\sigma, \tau \in \text{Gal}(\overline{\mathbb{Q}}/K)$, we may write $c(\sigma, \tau)$ as a coboundary; i.e., $c(\sigma, \tau) = \beta(\sigma) \cdot \beta(\tau) \cdot \beta(\sigma\tau)^{-1}$ where $\beta : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow F^*$ is a locally constant function. Now replace each μ_σ with $\beta(\sigma)^{-1} \circ \mu_\sigma$, which is again an isogeny $\sigma B \rightarrow B$ respecting $\text{End}(B)$. The new family $\{\mu_\sigma\}$ satisfies $\mu_\sigma \circ \sigma \mu_\tau = \mu_{\sigma\tau}$ for all $\sigma, \tau \in \text{Gal}(\overline{\mathbb{Q}}/K)$. Therefore we may apply [Ri 1, Thm. 8.2] to construct B_0/K and an isogeny $\kappa : B \rightarrow B_0/\overline{\mathbb{Q}}$.

Finally, we need to check that all endomorphisms of B_0 are defined over K , but this follows easily from the facts that the μ_σ are compatible with $\text{End}(B)$ and that $\mu_\sigma = \kappa^{-1} \circ \sigma \kappa$ by construction of κ . Indeed, for $\varphi \in \text{End}(B_0)$, we have $\kappa^{-1} \circ \varphi \circ \kappa \in \text{End}(B)$, so $\mu_\sigma \circ \sigma(\kappa^{-1} \circ \varphi \circ \kappa) = (\kappa^{-1} \circ \varphi \circ \kappa) \circ \mu_\sigma$ for all $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/K)$. We may rewrite this as $\kappa^{-1} \circ \sigma \varphi \circ \sigma \kappa = \kappa^{-1} \circ \varphi \circ \sigma \kappa$, and therefore $\sigma \varphi = \varphi$. Since this holds for all $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/K)$, we see that $\varphi \in \text{End}(B_0)$ is defined over K . QED

Note that $[c]$ has order dividing two in $H^2(G_{\mathbb{Q}}, F^*)$. Indeed, we know from Chapter 4 that there exists an abelian variety A of $\mathbf{GL}_2$ -type containing the building block B as a simple component, and that the class of the cocycle $c(\sigma, \tau)$ associated to B is exactly that of the cocycle we associated to A in Chapter 1. We saw there (Lemma 1.9) that the class of this cocycle has order one or two.

Write $H^2(G_{\mathbb{Q}}, F^*)[2]$ for the group of elements of the cohomology group $H^2(G_{\mathbb{Q}}, F^*)$ of order dividing two.

Proposition 5.3 *Let F be a totally real field and define $P = F^*/\{\pm 1\}$. Then $H^2(G_{\mathbb{Q}}, F^*)[2]$ is abstractly isomorphic to $H^2(G_{\mathbb{Q}}, \{\pm 1\}) \times \text{Hom}(G_{\mathbb{Q}}, P/P^2)$.*

Proof. (Ribet) We follow the procedure described in [Ri 2, Thm. 3.3].

Consider the exact sequence of trivial $G_{\mathbb{Q}}$ -modules

$$1 \rightarrow \{\pm 1\} \rightarrow F^* \rightarrow P \rightarrow 1.$$

This sequence is split because P is a free group [Ri 2, Lemma 3.5]. Thus we may write $F^* \cong \{\pm 1\} \times P$. We note that this isomorphism is in general non-canonical (although when $[F:\mathbb{Q}]$ is odd, we may embed $P \hookrightarrow F^*$ as the group of elements of F^* of positive norm). In any case, there is an isomorphism

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

Clearly all elements of $H^2(G_{\mathbb{Q}}, \{\pm 1\})$ are of order dividing two, so $H^2(G_{\mathbb{Q}}, \{\pm 1\})[2] = H^2(G_{\mathbb{Q}}, \{\pm 1\})$.

We now claim that there is an isomorphism $\text{Hom}(G_{\mathbb{Q}}, P/P^2) \xrightarrow{\sim} H^2(G_{\mathbb{Q}}, P)[2]$. Indeed, note that the squaring map $x \mapsto x^2$ is an injective map $P \rightarrow P$, because P is torsion-free. Now look at the exact sequence

$$1 \longrightarrow P \xrightarrow{\text{sq.}} P \longrightarrow P/P^2 \longrightarrow 1.$$

The corresponding long exact cohomology sequence is

$$\cdots \longrightarrow H^1(G_{\mathbb{Q}}, P) \longrightarrow H^1(G_{\mathbb{Q}}, P/P^2) \longrightarrow H^2(G_{\mathbb{Q}}, P) \xrightarrow{\text{sq.}} H^2(G_{\mathbb{Q}}, P).$$

Now $G_{\mathbb{Q}}$ is acting trivially, so we may regard each H^1 as a Hom. Furthermore, P is torsion-free, so $H^1(G_{\mathbb{Q}}, P) = \text{Hom}(G_{\mathbb{Q}}, P) = 1$. Also, the image of $H^1(G_{\mathbb{Q}}, P/P^2)$ in $H^2(G_{\mathbb{Q}}, P)$ is the kernel of the squaring map $H^2(G_{\mathbb{Q}}, P) \rightarrow H^2(G_{\mathbb{Q}}, P)$, which consists exactly of the subgroup of elements of order dividing two. Therefore we may rewrite the cohomology sequence as

$$1 \rightarrow \text{Hom}(G_{\mathbb{Q}}, P/P^2) \twoheadrightarrow H^2(G_{\mathbb{Q}}, P)[2].$$

Hence $\text{Hom}(G_{\mathbb{Q}}, P/P^2)$ is isomorphic to $H^2(G_{\mathbb{Q}}, P)[2]$, proving the proposition. *QED*

We are now ready to prove Theorem 5.1.

Proof. By the previous propositions, it suffices to show that the images of the cohomology class $[c]$ in $H^2(G_{\mathbb{Q}}, \{\pm 1\})$ and $\text{Hom}(G_{\mathbb{Q}}, P/P^2)$ under the isomorphism of Proposition 5.3 are trivialized by restriction to $\text{Gal}(\overline{\mathbb{Q}}/K)$ where K is a $(2, \dots, 2)$ -extension of $\mathbb{Q}$.

Recall that $H^2(G_{\mathbb{Q}}, \{\pm 1\})$ may be identified with $\text{Br}(\mathbb{Q})[2] = \{\text{Brauer classes of quaternion algebras over } \mathbb{Q}\}$. A quaternion algebra over $\mathbb{Q}$ may always be split by a quadratic extension; therefore the image of $[c]$ in $H^2(G_{\mathbb{Q}}, \{\pm 1\})$ is trivial under restriction to some quadratic extension $K_{\pm}$ of $\mathbb{Q}$.

The other “piece” of $[c]$ lies in $\text{Hom}(G_{\mathbb{Q}}, P/P^2)$. Since the image of any continuous homomorphism $G_{\mathbb{Q}} \rightarrow P/P^2$ is a finite elementary 2-group, the kernel of the homomorphism corresponding to the image of $[c]$ is $\text{Gal}(\overline{\mathbb{Q}}/K_P)$, where K_P is a $(2, \dots, 2)$ -extension of $\mathbb{Q}$.

Now let K be the composite of the fields $K_{\pm}$ and K_P . Then K is a $(2, \dots, 2)$ -extension such that $[c]$ is in the kernel of the restriction $H^2(G_{\mathbb{Q}}, F^*) \rightarrow H^2(\text{Gal}(\overline{\mathbb{Q}}/K), F^*)$.

QED

Elkies’s proof of the theorem for elliptic curves shows that the field K_P already trivializes $[c]$ in that case. Ribet’s method demonstrates this interesting fact to be true whenever $[F : \mathbb{Q}]$ is odd [Ri 2, Cor. 4.5]; it is unknown, however, whether it is true in general. In any case, the field K_P is a significant part of the $(2, \dots, 2)$ -extension K , and in order to determine K_P , we will now discuss an explicit description of the image of $[c]$ in $\text{Hom}(G_{\mathbb{Q}}, P/P^2)$.

The “Degree” of μ_{σ}

Let B_1 and B_2 be isogenous building blocks, and fix polarizations $\theta_1 : B_1 \rightarrow \widehat{B}_1$ and $\theta_2 : B_2 \rightarrow \widehat{B}_2$. We will say an isogeny $\mu : B_1 \rightarrow B_2$ is *Rosati compatible* if the isomorphism $\text{End}(B_1) \cong \text{End}(B_2)$ induced by μ is compatible with the Rosati involutions defined by θ_1 and θ_2 . For such an isogeny, we define the “degree” $\delta(\mu) = \mu \circ \theta_1^{-1} \circ \widehat{\mu} \circ \theta_2 \in Z(\text{End}(B_2))$. Note that $\delta(\mu)$ depends on the chosen polarizations θ_1, θ_2 (much as the Rosati involution of an endomorphism algebra depends on a choice of polarization).

The following properties of δ are elementary. If $\varphi : B_2 \rightarrow B_2$, then $\delta(\varphi) = \varphi \circ \varphi'$, where φ' is the Rosati involution of φ with respect to the polarization θ_2 . Also, δ is multiplicative in the following sense: if $\lambda : B_2 \rightarrow B_3$ is another isogeny that is Rosati compatible, then $\delta(\lambda \circ \mu) = (\lambda \circ \delta(\mu) \circ \lambda^{-1}) \circ \delta(\lambda)$ (assuming we use a fixed set of polarizations to calculate the degrees). In particular, if each building block is equipped with an action $F \xrightarrow{\sim} Z(\text{End}(B_i))$, and λ and μ respect F , then we may write $\delta(\lambda \circ \mu) = \delta(\lambda) \cdot \delta(\mu)$ as elements of F .

Proposition 5.4 *Let B_1, B_2 be building blocks with polarizations θ_1, θ_2 , respectively, and let $\mu : B_1 \rightarrow B_2$ be an isogeny that is Rosati compatible. Then the degree $\delta(\mu)$ is a totally positive element of the totally real field F .*

Proof. We will regard the isogeny $\mu : B_1 \rightarrow B_2$ as an element of $\text{End}(B_1 \times B_2)$, and use the properties of the Rosati involution on this endomorphism algebra to prove the proposition.

First define an isomorphism

$$\begin{aligned} \mathbf{M}_2(\text{End}(B_2)) &\longrightarrow \text{End}(B_1 \times B_2) \\ \begin{pmatrix} \varphi_{11} & \varphi_{12} \\ \varphi_{21} & \varphi_{22} \end{pmatrix} &\longmapsto \begin{pmatrix} \mu^{-1} \circ \varphi_{11} \circ \mu & \mu^{-1} \circ \varphi_{12} \\ \varphi_{21} \circ \mu & \varphi_{22} \end{pmatrix}. \end{aligned}$$

Now the polarizations θ_1, θ_2 define a polarization $\theta_1 \times \theta_2$ on $\text{End}(B_1 \times B_2)$ which, in turn, induces a Rosati involution on $\text{End}(B_1 \times B_2)$. Pulling back this involution to $\mathbf{M}_2(\text{End}(B_2))$, we find it is given by the formula

$$\Phi = \begin{pmatrix} \varphi_{11} & \varphi_{12} \\ \varphi_{21} & \varphi_{22} \end{pmatrix} \longmapsto \begin{pmatrix} \varphi'_{11} & \delta(\mu) \circ \varphi'_{21} \\ \varphi'_{12} \circ \delta(\mu)^{-1} & \varphi'_{22} \end{pmatrix} = \Phi'.$$

where $\varphi \mapsto \varphi'$ is the Rosati involution on $\text{End}(B_2)$ coming from θ_2 .

Now the Rosati involution is a positive involution; that is, for a non-zero endomorphism Φ , the trace $\text{Tr}(\Phi\Phi') \in \mathbb{Q}$ is positive [Mu, §21 Thm. 1]. In particular, consider $\Phi \in \text{End}(B_1 \times B_2)$ of the form $\begin{pmatrix} 0 & 0 \\ \varphi & 0 \end{pmatrix}$. Then

$$\Phi' = \begin{pmatrix} 0 & \delta(\mu) \circ \varphi' \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad \Phi\Phi' = \begin{pmatrix} 0 & 0 \\ 0 & \delta(\mu) \circ \varphi \circ \varphi' \end{pmatrix}.$$

Therefore $\text{Tr}(\Phi\Phi') = \text{Tr}(\delta(\mu) \circ \varphi \circ \varphi') > 0$ for all $\varphi \in \text{End}(B_2)$.

We now claim the fact that this inequality holds for all φ implies that $\delta(\mu)$ must be totally positive. Indeed, let I be the finite set of embeddings $\{\iota : F \hookrightarrow \mathbb{R}\}$. Suppose some embedding, call it ι_0 , is such that $\iota_0(\delta(\mu)) < 0$. Now by the Strong Approximation Theorem, we may choose $\varphi \in F$ such that $|\iota_0(\varphi)|^2$ is large, say greater than $\#I/|\iota_0(\delta(\mu))|$, but $|\iota(\varphi)|^2$ is small, say less than $1/\max_{\iota \neq \iota_0} \{|\iota(\delta(\mu))|\}$ for all $\iota \neq \iota_0$.

Now by [Mu, p. 182], $\text{Tr}(\delta(\mu) \circ \varphi \circ \varphi')$ is a positive multiple of $\text{Tr}_{F/\mathbb{Q}}(\delta(\mu) \cdot \varphi^2)$, which we may calculate as

$$\begin{aligned} \text{Tr}_{F/\mathbb{Q}}(\delta(\mu) \cdot \varphi^2) &= \sum_{\iota \in I} \iota(\delta(\mu)) \cdot \iota(\varphi)^2 \\ &= \iota_0(\delta(\mu)) \cdot \iota_0(\varphi)^2 + \sum_{\iota \neq \iota_0} \iota(\delta(\mu)) \cdot \iota(\varphi)^2 \\ &< -\#I + \sum_{\iota \neq \iota_0} 1 \\ &< 0 \end{aligned}$$

because we chose φ carefully.

This contradicts the fact that $\text{Tr}(\delta(\mu) \circ \varphi \circ \varphi')$ is positive for all φ . Therefore $\iota(\delta(\mu))$ must be positive for all embeddings $\{\iota : F \hookrightarrow \mathbb{R}\}$. QED

Next, we look at the relationship between $\delta(\mu)$ and the standard degree $\deg \mu \in \mathbb{Q}$.

Proposition 5.5 *Let $\delta(\mu)$ be the “degree” of an isogeny of building blocks $\mu : B_1 \rightarrow B_2$ defined in terms of polarizations θ_1 and θ_2 with $\deg \theta_1 = \deg \theta_2$. Then $\deg \mu = N_{\mathcal{B}/\mathbb{Q}}(\delta(\mu))$, where $N_{\mathcal{B}/\mathbb{Q}}$ is the canonical reduced norm of $\mathcal{B} = \text{End}(B_2)$ over $\mathbb{Q}$.*

Proof. Write $t = \sqrt{\dim_F \mathcal{B}}$ ($= 1$ or 2) as usual. First, because B_2 is simple, we know $\deg \delta(\mu) = (N_{\mathcal{B}/\mathbb{Q}}(\delta(\mu)))^n$ for some $n \geq 1$ [Mu, p. 182]. But “deg” is a polynomial function of degree $2 \dim B_2$, and $N_{\mathcal{B}/\mathbb{Q}}$ is a polynomial function of degree $t[F:\mathbb{Q}] = \dim B_2$ (since B_2 is a building block). Thus $n = 2$ and $\deg \delta(\mu) = (N_{\mathcal{B}/\mathbb{Q}}(\delta(\mu)))^2$.

On the other hand, $\delta(\mu) = \mu \circ \theta_1^{-1} \circ \hat{\mu} \circ \theta_2$ means that

$$\deg \delta(\mu) = (\deg \mu)(\deg \theta_1)^{-1}(\deg \hat{\mu})(\deg \theta_2) = (\deg \mu)^2,$$

because $\deg \hat{\mu} = \deg \mu$, and $\deg \theta_1 = \deg \theta_2$ by hypothesis.

Therefore, $(\deg \mu)^2 = (N_{\mathcal{B}/\mathbb{Q}}(\delta(\mu)))^2$, so $\deg \mu = \pm N_{\mathcal{B}/\mathbb{Q}}(\delta(\mu)) = \pm (N_{F/\mathbb{Q}}(\delta(\mu)))^t$, as $\delta(\mu)$ lies in F . Now we have seen that $\delta(\mu)$ is totally positive; thus $N_{F/\mathbb{Q}}(\delta(\mu)) > 0$. Of course, $\deg \mu$ is also positive, and so we must have $\deg \mu = + N_{\mathcal{B}/\mathbb{Q}}(\delta(\mu))$. *QED*

Now let B be a building block and fix a collection $\{\mu_\sigma : {}^\sigma B \rightarrow B\}$ respecting $\text{End}(B)$, as usual. Let $\theta : B \rightarrow \hat{B}$ be a polarization of B . Then for each $\sigma \in G_{\mathbb{Q}}$, the isogeny ${}^\sigma \theta : {}^\sigma B \rightarrow {}^\sigma \hat{B}$ is a polarization of ${}^\sigma B$ and we define, as above, the degree $\delta(\mu_\sigma) = \mu_\sigma \circ {}^\sigma \theta^{-1} \circ \hat{\mu}_\sigma \circ \theta$. It is easy to check that the isogenies $\{\mu_\sigma\}$ are Rosati compatible, because each μ_σ was chosen to be compatible with $\text{End}(B)$. Note, however, that by requiring the polarization of ${}^\sigma B$ to be ${}^\sigma \theta$, now $\delta(\mu_\sigma) \in F$ is independent of the chosen polarization θ .

Moreover, the μ_σ are well-defined modulo F^* , and therefore $\delta(\mu_\sigma) \bmod F^{*2}$ depends only on the building block B and not on the choices for μ_σ or the polarization defining δ . Also, $\mu_\sigma \circ {}^\sigma \mu_\tau \circ \mu_{\sigma\tau}^{-1} \in F^*$ implies that $\delta(\mu_\sigma) \cdot \delta(\mu_\tau) \cdot \delta(\mu_{\sigma\tau})^{-1} \in F^{*2}$, and hence $\sigma \mapsto \delta(\mu_\sigma) \bmod F^{*2}$ is a locally constant homomorphism $G_{\mathbb{Q}} \rightarrow F^*/F^{*2}$.

Recall from the previous section the two-cocycle $c(\sigma, \tau) = \mu_\sigma \circ {}^\sigma \mu_\tau \circ \mu_{\sigma\tau}^{-1}$ associated to the building block B . We have seen there is an isomorphism $H^2(G_{\mathbb{Q}}, F^*)[2] \cong H^2(G_{\mathbb{Q}}, \{\pm 1\}) \times \text{Hom}(G_{\mathbb{Q}}, P/P^2)$, where P is defined to be $F^*/\{\pm 1\}$, and we are interested in the image of $[c]$ in $\text{Hom}(G_{\mathbb{Q}}, P/P^2)$.

Proposition 5.6 *The image of $[c]$ in $\text{Hom}(G_{\mathbb{Q}}, P/P^2)$ is exactly the homomorphism $\sigma \mapsto \delta(\mu_\sigma) \bmod \{\pm 1\}F^{*2}$.*

Proof. The projection map $H^2(G_{\mathbb{Q}}, F^*)[2] \rightarrow \text{Hom}(G_{\mathbb{Q}}, P/P^2)$ is broken into two parts: first, the map $H^2(G_{\mathbb{Q}}, F^*)[2] \rightarrow H^2(G_{\mathbb{Q}}, P)[2]$ induced by $F^* \rightarrow F^*/\{\pm 1\} = P$, followed by the inverse of the isomorphism $\text{Hom}(G_{\mathbb{Q}}, P/P^2) \xrightarrow{\sim} H^2(G_{\mathbb{Q}}, P)[2]$ coming from the exact sequence $1 \rightarrow P \xrightarrow{\text{sq.}} P \rightarrow P/P^2 \rightarrow 1$. Thus we have to show that the image of the homomorphism $\sigma \mapsto \delta(\mu_{\sigma}) \bmod \{\pm 1\}F^{*2}$ in $H^2(G_{\mathbb{Q}}, P)[2]$ is the same as the image of $[c]$ in this group.

The isomorphism $\text{Hom}(G_{\mathbb{Q}}, P/P^2) \xrightarrow{\sim} H^2(G_{\mathbb{Q}}, P)[2]$ maps the homomorphism $\sigma \mapsto \delta(\mu_{\sigma}) \bmod \{\pm 1\}F^{*2}$ to a cohomology class as follows: Lift the homomorphism to a map $G_{\mathbb{Q}} \rightarrow P$, e.g., $\sigma \mapsto \delta(\mu_{\sigma}) \bmod \{\pm 1\}$. Then $\delta(\mu_{\sigma}) \cdot \delta(\mu_{\tau}) \cdot \delta(\mu_{\sigma\tau})^{-1} \bmod \{\pm 1\}$ is a square in P , and $\sigma, \tau \mapsto \sqrt{\delta(\mu_{\sigma}) \cdot \delta(\mu_{\tau}) \cdot \delta(\mu_{\sigma\tau})^{-1}} \bmod \{\pm 1\}$ is the two-cocycle that defines the image in $H^2(G_{\mathbb{Q}}, P)[2]$.

On the other hand, $c(\sigma, \tau) = \mu_{\sigma} \circ^{\sigma} \mu_{\tau} \circ \mu_{\sigma\tau}^{-1}$, and taking the degree δ of both sides we find $c(\sigma, \tau)^2 = \delta(\mu_{\sigma}) \cdot \delta(\mu_{\tau}) \cdot \delta(\mu_{\sigma\tau})^{-1}$. Hence $c(\sigma, \tau) = \pm \sqrt{\delta(\mu_{\sigma}) \cdot \delta(\mu_{\tau}) \cdot \delta(\mu_{\sigma\tau})^{-1}}$, and therefore $c(\sigma, \tau) \bmod \{\pm 1\}$ gives the same class in $H^2(G_{\mathbb{Q}}, P)[2]$ that the homomorphism $\sigma \mapsto \delta(\mu_{\sigma}) \bmod \{\pm 1\}F^{*2}$ does. QED

Some Characters

Let B be a building block. As we have seen in Chapter 4, we form a building block triple $(B, j, \{\nu_{\sigma}\})$ by attaching some extra data to B : namely, $j : Z(\text{End}(B)) \hookrightarrow \overline{\mathbb{Q}}$, whose image we call F , and for all $\sigma \in G_{\mathbb{Q}}$, a non-zero $\nu_{\sigma} \in \overline{\mathbb{Q}} \otimes_F \text{Hom}^B({}^{\sigma}B, B)$ such that $\nu_{\sigma} \circ^{\sigma} \nu_{\tau} = \nu_{\sigma\tau}$. Because $\text{Hom}^B({}^{\sigma}B, B)$ is a one-dimensional F -vector space, we can, and do, write $\nu_{\sigma} = \beta(\sigma)^{-1} \otimes \mu_{\sigma}$ for some $\mu_{\sigma} : {}^{\sigma}B \rightarrow B$ respecting $\text{End}(B)$ and some $\beta(\sigma) \in \overline{\mathbb{Q}}^*$. Let E be the field extension of F generated by the $\beta(\sigma)$.

Now let (A, i) be a pair of $\mathbf{GL}_2$ -type corresponding to $(B, j, \{\nu_{\sigma}\})$ under Theorem 4.6. Then i is an isomorphism of $\text{End}_{\mathbb{Q}}(A)$ onto the field E , and $i(Z(\text{End}(A))) = F$. Recall that E is a Galois extension of F . In [Ri 1], Ribet associates a character $\varepsilon : G_{\mathbb{Q}} \rightarrow E^*$ to the abelian variety A . Our goal in this section is to recover ε directly from the triple $(B, j, \{\nu_{\sigma}\})$.

The condition $\nu_{\sigma} \circ^{\sigma} \nu_{\tau} = \nu_{\sigma\tau}$ tells us that

$$\mu_{\sigma} \circ^{\sigma} \mu_{\tau} \circ \mu_{\sigma\tau}^{-1} = c(\sigma, \tau) = \beta(\sigma) \cdot \beta(\tau) \cdot \beta(\sigma\tau)^{-1} \in F^*,$$

and therefore, if δ is the degree map defined in the previous section,

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

Hence we see that $\sigma \mapsto \delta(\mu_\sigma)/\beta(\sigma)^2$ is a continuous character $G_{\mathbb{Q}} \rightarrow E^*$. Note that this character depends only on the triple $(B, j, \{\nu_\sigma\})$ and not on our choices for μ_σ ; we claim that it is in fact equal to the character ε .

In order to define ε and to prove our claim, we need to study the “ λ -adic” representations of $G_{\mathbb{Q}}$ provided by the abelian variety A of $\mathbf{GL}_2$ -type.

Let ℓ be a prime number and let $V_\ell = V_\ell(A)$ be the Tate module associated to A . Because A is of $\mathbf{GL}_2$ -type, $V_\ell(A)$ is free of rank two over $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. Let $\{\lambda\}$ be the set of primes of E lying over ℓ , and for each λ , write E_λ for the completion of E at λ ; then $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong \bigoplus_{\lambda|\ell} E_\lambda$. Now define $V_\lambda = E_\lambda \otimes_{E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell} V_\ell$. We see immediately that each V_λ is a two-dimensional E_λ -vector space, and that $V_\ell \cong \bigoplus_{\lambda|\ell} V_\lambda$. Each V_λ is still also a $G_{\mathbb{Q}}$ -module, since the action of $G_{\mathbb{Q}}$ on V_ℓ commutes with $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$.

Our starting point for studying the V_λ will be the following result of Faltings.

Theorem 5.7 *Let K be a finite Galois extension of $\mathbb{Q}$ such that all endomorphisms of A are defined over K , and let $H = \text{Gal}(\overline{\mathbb{Q}}/K)$. Then*

$$\text{End}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \rightarrow \text{End}_{\mathbb{Q}_\ell[H]} V_\ell$$

is an isomorphism of $\mathbb{Q}_\ell[G_{\mathbb{Q}}]$ -modules.

The $G_{\mathbb{Q}}$ -module structure on V_ℓ induces an action of $G_{\mathbb{Q}}$ on $\text{End}_{\mathbb{Q}_\ell} V_\ell$ via ${}^\sigma f = \sigma \circ f \circ \sigma^{-1}$. Now $\text{End}_{\mathbb{Q}_\ell[H]} V_\ell$ is the submodule of $\text{End}_{\mathbb{Q}_\ell} V_\ell$ fixed by H ; it is still a $G_{\mathbb{Q}}$ -submodule because H is a normal subgroup. This defines the action of $G_{\mathbb{Q}}$ on $\text{End}_{\mathbb{Q}_\ell[H]} V_\ell$ in the theorem. Of course, the action of $G_{\mathbb{Q}}$ on $\text{End}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ comes from the natural action of $G_{\mathbb{Q}}$ on $\text{End}(A)$.

Corollary 5.8 *Let $H \subset G_{\mathbb{Q}}$ be a normal subgroup of finite index with the properties described in the above theorem. Then $\text{End}_{E_\lambda[H]} V_\lambda \cong E_\lambda$ for all $\lambda \mid \ell$.*

Proof. Recall that E is its own centralizer in $\text{End}(A)$. Therefore the centralizer of $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ in $\text{End}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. Applying the isomorphism in the theorem, we find that the centralizer of $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ in $\text{End}_{\mathbb{Q}_\ell[H]} V_\ell$ is again $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. Therefore,

$$\begin{aligned} \text{End}_{(E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)[H]} V_\ell &\cong E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \\ \bigoplus_{\lambda|\ell} \text{End}_{E_\lambda[H]} V_\lambda &\cong \bigoplus_{\lambda|\ell} E_\lambda \\ \text{End}_{E_\lambda[H]} V_\lambda &\cong E_\lambda. \end{aligned}$$

QED

Corollary 5.9 *Let ℓ be a prime that splits completely in E . Then $\text{Hom}_{\mathbb{Q}_\ell[H]}(V_\lambda, V_{\lambda'})$ is non-zero if and only if $\lambda' = \gamma(\lambda)$ for some $\gamma \in \text{Gal}(E/F)$.*

Proof. Regard the isomorphisms

$$\text{End}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong \text{End}_{\mathbb{Q}_\ell[H]} V_\ell \cong \bigoplus_{\lambda, \lambda'} \text{Hom}_{\mathbb{Q}_\ell[H]}(V_\lambda, V_{\lambda'})$$

as isomorphisms of $(F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)$ -modules. Because $F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is the center of $\text{End}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$, every non-zero $f \in \text{Hom}_{\mathbb{Q}_\ell[H]}(V_\lambda, V_{\lambda'})$ must be an $(F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)$ -isomorphism. But it is clear that $V_\lambda \cong V_{\lambda'}$ as $(F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)$ -modules if and only if $E_\lambda \cong E_{\lambda'}$ as F -modules, which is equivalent to the condition $\lambda' = \gamma(\lambda)$ for some $\gamma \in \text{Gal}(E/F)$. In other words, if $\lambda' \neq \gamma(\lambda)$, then $\text{Hom}_{\mathbb{Q}_\ell[H]}(V_\lambda, V_{\lambda'}) = 0$.

Now because ℓ splits completely in E , there are $[E : \mathbb{Q}]$ primes λ lying over ℓ , and we have $E_\lambda \cong \mathbb{Q}_\ell$ for each λ . By the previous corollary, $\text{End}_{\mathbb{Q}_\ell[H]} V_\lambda \cong \mathbb{Q}_\ell$. Therefore, the $\mathbb{Q}_\ell$ -dimension of $\text{Hom}_{\mathbb{Q}_\ell[H]}(V_\lambda, V_{\gamma(\lambda)})$ must be zero or one. Hence the $\mathbb{Q}_\ell$ -dimension of $\bigoplus_{\gamma} \bigoplus_{\lambda} \text{Hom}_{\mathbb{Q}_\ell[H]}(V_\lambda, V_{\gamma(\lambda)})$ is less than or equal to $[E : F][E : \mathbb{Q}]$, with equality holding if and only if each $\text{Hom}_{\mathbb{Q}_\ell[H]}(V_\lambda, V_{\gamma(\lambda)})$ is one-dimensional. On the other hand, the $\mathbb{Q}_\ell$ -dimension of $\text{End}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is $[E : F]^2 \cdot [F : \mathbb{Q}]$, which forces equality above. *QED*

Now consider the action of $G_{\mathbb{Q}}$ on $\text{End}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. Recall that for each $\sigma \in G_{\mathbb{Q}}$ we have defined $\alpha(\sigma) \in E^*$ to be an element of $\text{End}(A)$ such that ${}^\sigma\varphi = \alpha(\sigma) \circ \varphi \circ \alpha(\sigma)^{-1}$. That is to say, $\sigma \in G_{\mathbb{Q}}$ acts on $\text{End}(A)$ via conjugation by $\alpha(\sigma)$, where $\alpha(\sigma) \in E^*$ is well-defined modulo F^* . We fix a choice of $\alpha(\sigma)$ for each σ ; these $\alpha(\sigma)$ satisfy $\alpha(\sigma) \cdot \alpha(\tau) \cdot \alpha(\sigma\tau)^{-1} \in F^*$, as always. Therefore, for each $\gamma \in \text{Gal}(E/F)$, we may define a character $\chi_\gamma : G_{\mathbb{Q}} \rightarrow E^*$ by $\chi_\gamma(\sigma) = \gamma(\alpha(\sigma)) / \alpha(\sigma)$. Note that these characters depend only on the abelian variety A .

NOTATION: Let ℓ be a prime which splits completely in E , and let λ be a prime of E dividing ℓ . Then E_λ will denote $\mathbb{Q}_\ell$ with the map $E \hookrightarrow \mathbb{Q}_\ell$ induced by λ , and the image in $\mathbb{Q}_\ell$ of an element $e \in E$ will be written e_λ .

Lemma 5.10 *Let ℓ be a prime which splits completely in E . Let $\gamma \in \text{Gal}(E/F)$. Then the $\mathbb{Q}_\ell[G_{\mathbb{Q}}]$ -module V_λ is isomorphic to $V_{\gamma(\lambda)} \otimes \chi_{\gamma, \lambda}^{-1}$.*

Proof. We know that V_λ and $V_{\gamma(\lambda)}$ are isomorphic $\mathbb{Q}_\ell[H]$ -modules for some normal subgroup H of $G_{\mathbb{Q}}$ of finite index. Let $f \in \text{Hom}_{\mathbb{Q}_\ell[H]}(V_\lambda, V_{\gamma(\lambda)})$ be an isomorphism. Now $\text{End}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is $G_{\mathbb{Q}}$ -isomorphic to $\text{End}_{\mathbb{Q}_\ell[H]} V_\ell$, and we know σ acts on $\text{End}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ via

conjugation by $\alpha(\sigma)$. Also, $\alpha(\sigma) \in E$ acts on V_λ as $\alpha(\sigma)_\lambda$ for each λ . Thus we may write ${}^\sigma f = \alpha(\sigma)_{\gamma(\lambda)} \cdot f \cdot \alpha(\sigma)_\lambda^{-1}$ in $\text{Hom}_{\mathbb{Q}_\ell[H]}(V_\lambda, V_{\gamma(\lambda)})$. Now because $E_\lambda \cong \mathbb{Q}_\ell$, we have

$${}^\sigma f = \frac{\alpha(\sigma)_{\gamma(\lambda)}}{\alpha(\sigma)_\lambda} \cdot f = \left(\frac{\gamma(\alpha(\sigma))}{\alpha(\sigma)} \right)_\lambda \cdot f = \chi_{\gamma, \lambda}(\sigma) \cdot f.$$

Hence for all $\sigma \in G_\mathbb{Q}$ and $v \in V_\lambda$, we have $\sigma(f(v)) = \chi_{\gamma, \lambda}(\sigma) \cdot f(\sigma(v))$, and we see that f is an isomorphism of $\mathbb{Q}_\ell[G_\mathbb{Q}]$ -modules $V_\lambda \xrightarrow{\sim} V_{\gamma(\lambda)} \otimes \chi_{\gamma, \lambda}^{-1}$. QED

Now what is the character ε ? The action of $G_\mathbb{Q}$ on V_λ defines a representation $\rho_\lambda : G_\mathbb{Q} \rightarrow \text{Aut } V_\lambda$. By [Ri 1, Lemma 3.1] there exists a character of finite order $\varepsilon : G_\mathbb{Q} \rightarrow E^*$ such that for each prime $\lambda \mid \ell$ of E , we have $\det \rho_\lambda = \varepsilon \cdot \chi_\ell$, where $\chi_\ell : G_\mathbb{Q} \rightarrow \mathbb{Q}_\ell^*$ is the ℓ -adic cyclotomic character. As we will soon see, ε is equal to the character $\chi_{\text{conj.}}^{-1}$, where “conj.” $\in \text{Gal}(E/F)$ is the canonical complex conjugation $e \mapsto \bar{e}$ on E .

Lemma 5.11 *Let ℓ be a prime that splits completely in E . Then the $G_\mathbb{Q}$ -module V_λ is isomorphic to $V_{\bar{\lambda}} \otimes \varepsilon_\lambda$.*

Proof. (Ribet) Let $\langle \cdot, \cdot \rangle : V_\ell \times V_\ell \rightarrow \mathbb{Q}_\ell(1)$ be the Weil pairing on $V_\ell(A)$ induced by a fixed polarization of $A/\mathbb{Q}$. Here $\mathbb{Q}_\ell(1)$ denotes the ℓ -adic Tate module $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \varprojlim \mu_{\ell^n}$ of ℓ -power roots of unity in $\bar{\mathbb{Q}}$. Recall that the Weil pairing is non-degenerate and Galois invariant; that is, for $\sigma \in G_\mathbb{Q}$ and $v, w \in V_\ell$ we have ${}^\sigma \langle v, w \rangle = \langle \sigma(v), \sigma(w) \rangle$. Thus we obtain an isomorphism of $G_\mathbb{Q}$ -modules

$$V_\ell \cong \text{Hom}_{\mathbb{Q}_\ell}(V_\ell, \mathbb{Q}_\ell(1)).$$

By writing V_ℓ as the direct sum of the V_λ , we then have

$$(*) \quad \bigoplus_{\lambda \mid \ell} V_\lambda \cong \bigoplus_{\lambda \mid \ell} \text{Hom}_{\mathbb{Q}_\ell}(V_\lambda, \mathbb{Q}_\ell(1)).$$

We claim that under this isomorphism, the $\bar{\lambda}$ -component on the left-hand side corresponds to the λ -component on the right-hand side. Indeed, recall that if $\varphi \mapsto \varphi'$ is the Rosati involution on $\text{End}(A)$ coming from our fixed polarization, then φ and φ' are adjoint with respect to the Weil pairing; in particular, $\langle e v, w \rangle = \langle v, \bar{e} w \rangle$ for $e \in E$ and $v, w \in V_\ell$. Now we may extend the automorphism “conj.” to $E \otimes_\mathbb{Q} \mathbb{Q}_\ell$; it is simply the map which permutes the components of $\bigoplus_{\lambda \mid \ell} E_\lambda$ by taking the λ -component to the $\bar{\lambda}$ -component. The new “conj.” still has the same property with respect to $\langle \cdot, \cdot \rangle$.

Now let $\{\pi_\lambda\}$ be a set of orthogonal idempotents for $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$, so that $V_\lambda = \pi_\lambda V_\ell$. Note that $\overline{\pi_\lambda} = \pi_{\overline{\lambda}}$. By using $\langle \pi_\lambda v, w \rangle = \langle v, \overline{\pi_\lambda} w \rangle$, it is easy to verify that if $v = \pi_\lambda v \in V_\lambda$, then under $(*)$ the corresponding homomorphism f_v is $f_v \circ \pi_{\overline{\lambda}} \in \text{Hom}_{\mathbb{Q}_\ell}(V_{\overline{\lambda}}, \mathbb{Q}_\ell(1))$. This proves the claim, and we have

$$V_{\overline{\lambda}} \cong \text{Hom}_{\mathbb{Q}_\ell}(V_\lambda, \mathbb{Q}_\ell(1)).$$

On the other hand, V_λ is a two-dimensional E_λ -vector space. Therefore the determinant gives a pairing $V_\lambda \times V_\lambda \rightarrow E_\lambda$ which, by definition of ε , defines an isomorphism of $\mathbb{Q}_\ell[G_{\mathbb{Q}}]$ -modules

$$V_\lambda \cong \text{Hom}_{\mathbb{Q}_\ell}(V_\lambda, \mathbb{Q}_\ell(1) \otimes \varepsilon_\lambda) \cong \text{Hom}_{\mathbb{Q}_\ell}(V_\lambda, \mathbb{Q}_\ell(1)) \otimes \varepsilon_\lambda.$$

Combining this with the previous isomorphism, we see $V_\lambda \cong V_{\overline{\lambda}} \otimes \varepsilon_\lambda$.

QED

Theorem 5.12 *Let $(B, j, \{\nu_\sigma\})$ be a building block triple, and let (A, i) be a pair of $\mathbf{GL}_2$ -type corresponding to the triple under Theorem 4.6. Then the character $\sigma \mapsto \delta(\mu_\sigma)/\beta(\sigma)^2$ defined by $(B, j, \{\nu_\sigma\})$ is equal to the character ε defined by (A, i) .*

Proof. Let ℓ be a prime that splits completely in E . Together, the previous two lemmas imply that $\varepsilon_\lambda = \chi_{\text{conj}, \lambda}^{-1}$ for all λ dividing ℓ , and so $\varepsilon = \chi_{\text{conj}}^{-1} : G_{\mathbb{Q}} \rightarrow E^*$. That is, we may write $\varepsilon(\sigma) = \alpha(\sigma)/\overline{\alpha(\sigma)}$ for the usual collection $\{\alpha(\sigma)\}_{\sigma \in G_{\mathbb{Q}}}$ defined by A .

On the other hand, we know that under the correspondence $(B, j, \{\nu_\sigma\}) \rightsquigarrow (A, i)$, we may take $\alpha(\sigma) = \beta(\sigma)^{-1}$. Thus $\varepsilon(\sigma) = \overline{\beta(\sigma)}/\beta(\sigma)$.

Now we compare our two characters by taking their quotient; we find a new character $\sigma \mapsto \varepsilon(\sigma)^{-1} \cdot \delta(\mu_\sigma)/\beta(\sigma)^2 = \delta(\mu_\sigma)/\beta(\sigma)\overline{\beta(\sigma)}$, which takes values in F^* . Therefore $\delta(\mu_\sigma)/\beta(\sigma)\overline{\beta(\sigma)} \in \{\pm 1\}$ for all $\sigma \in G_{\mathbb{Q}}$, because F is a totally real field. But $\delta(\mu_\sigma)$ and $\beta(\sigma)\overline{\beta(\sigma)}$ are both totally positive elements of F^* , so their quotient must be $+1$. Hence we have $\delta(\mu_\sigma) = \beta(\sigma)\overline{\beta(\sigma)}$ for all σ , and $\varepsilon(\sigma) = \delta(\mu_\sigma)/\beta(\sigma)^2$. *QED*

This theorem has some interesting consequences. First, recall our discussion of fields of definition for building blocks. We found that a building block B is always isogenous to a building block B_0 over a $(2, \dots, 2)$ -extension K of $\mathbb{Q}$. Furthermore, that extension may frequently be taken to be the fixed field K_P of the subgroup $\{\sigma : \delta(\mu_\sigma) \in \{\pm 1\}F^{*2}\} \subset G_{\mathbb{Q}}$, and in all cases, a quadratic extension of K_P suffices. Now if A is an abelian variety of $\mathbf{GL}_2$ -type corresponding to B , this information translates into the knowledge of a field K

where A breaks up into its simple components, i.e., $A/K \sim B_0 \times \dots \times B_0$. The theorem lets us compute the field K_P from data associated with A only.

Corollary 5.13 *Let μ_E denote the group of roots of unity in E^* . Then the field K_P is the fixed field of $\{\sigma : \alpha(\sigma) \in \mu_E F^*\} \subset G_{\mathbb{Q}}$.*

Proof. Fix $\sigma \in G_{\mathbb{Q}}$. It suffices to show that $\delta(\mu_\sigma) \in \{\pm 1\}F^{*2}$ if and only if $\alpha(\sigma) \in \mu_E F^*$. Suppose that $\delta(\mu_\sigma) \in \{\pm 1\}F^{*2}$. Then by the theorem, $\alpha(\sigma)^2 = \varepsilon(\sigma)/\delta(\mu_\sigma) \in \mu_E F^{*2}$, which implies that $\alpha(\sigma) \in \mu_E F^*$. Conversely, suppose that $\alpha(\sigma) \in \mu_E F^*$. Then $\delta(\mu_\sigma) = \varepsilon(\sigma)/\alpha(\sigma)^2 \in (\mu_E \cap F^*)F^{*2} = \{\pm 1\}F^{*2}$. QED

Finally, we may formulate a criterion to determine when, given a building block, we may construct from it an abelian variety A of $\mathbf{GL}_2$ -type with $\varepsilon = 1$. This question is motivated by the discussion in the Introduction of a possible “modular” structure on A . Recall that A is “modular” if it appears as a quotient of the Jacobian $J_1(N)$ for some N . In this event, A is isogenous to an abelian variety A_f , where f is a normalized cuspidal eigenform of weight two on $\Gamma_1(N)$. (Conjecturally, all abelian varieties of $\mathbf{GL}_2$ -type may be constructed in this way.) Now when A is modular, the character ε is exactly the character of the modular form f on $\Gamma_0(N)$ [Ri 1, Lemma 4.3]. Thus the case $\varepsilon = 1$ is especially interesting because the morphism $J_1(N) \rightarrow A$ then factors through $J_0(N)$.

The previous theorem tells us that ε depends on our choice of $\nu_\sigma = \beta(\sigma)^{-1} \otimes \mu_\sigma$.

Corollary 5.14 *Let B be a building block, and $[c]$ its associated cohomology class. Then the following are equivalent:*

- (i) *There exists a choice of $\{\nu_\sigma\}$ such that the character ε is trivial.*
- (ii) *The class $[c]$ lies in the kernel of the natural map*

$$H^2(G_{\mathbb{Q}}, F^*) \rightarrow H^2(G_{\mathbb{Q}}, F(\dots, \sqrt{\delta(\mu_\sigma)}, \dots)).$$

Proof. First note that the field extension $F_1 \stackrel{\text{def}}{=} F(\dots, \sqrt{\delta(\mu_\sigma)}, \dots)$ is independent of our choices for μ_σ , because $\delta(\mu_\sigma)$ is well-defined modulo F^{*2} . Furthermore, since all $\delta(\mu)$ are totally positive elements of F^* , we see that the field F_1 is totally real.

Now suppose $\varepsilon = 1$. Then by the theorem, $\beta(\sigma)^2 = \delta(\mu_\sigma)$ for all $\sigma \in G_{\mathbb{Q}}$. Thus $\beta(\sigma) \in F(\sqrt{\delta(\mu_\sigma)})$, and so $c(\sigma, \tau)$ splits in F_1 .

On the other hand, if c splits in F_1 , then we may choose all $\beta(\sigma)$ in this totally real field. Therefore $\overline{\beta(\sigma)} = \beta(\sigma)$ for all σ , and so $\varepsilon = 1$. QED

Chapter 6

An Example of a $\mathbb{Q}$ -Curve

In this chapter we give a concrete example of a building block of dimension one, and we calculate many of the associated functions and characters that were discussed in the previous chapter.

We see from its definition that a building block of dimension one is simply an elliptic curve over $\overline{\mathbb{Q}}$ without complex multiplication that is isogenous to all of its Galois conjugates. The following example of such a $\mathbb{Q}$ -curve was suggested by N. Elkies of Harvard University.

Let B be the elliptic curve over $\mathbb{Q}(\sqrt{-3})$ defined by the equation

$$B : y^2 = x^3 + 2x^2 + bx, \text{ where } b \in \mathbb{Q}(\sqrt{-3}) \text{ is an algebraic integer of trace 1.}$$

Proposition 6.1 *The curve B does not have complex multiplication.*

Proof. Let ω be a primitive cube root of unity in $\mathbb{Q}(\sqrt{-3})$, and let $\mathfrak{p} = (1 - \omega)$ be the unique prime of $\mathbb{Q}(\sqrt{-3})$ lying over 3. We claim that $b \equiv -1 \pmod{\mathfrak{p}}$, because b has trace 1. Indeed, write $b = r + s\omega$ with $r, s \in \mathbb{Z}$. Then $\text{Tr}(b) = 1$ implies that $s = 2r + 1$, and so $b + 1 = (1 - \omega)(1 + r\omega) \in \mathfrak{p}$.

Now the discriminant of B is $64b^2(1 - b) \not\equiv 0 \pmod{\mathfrak{p}}$, so $\mathfrak{p}$ is a prime of good reduction for B . Let $B_{\mathfrak{p}}$ be the reduction of B modulo $\mathfrak{p}$; the equation for $B_{\mathfrak{p}}$ over the field of three elements $\mathbb{F}_3$ is then $y^2 = x^3 + 2x^2 - x$. Recall that $\text{End}(B)$ is a subfield of $\text{End}(B_{\mathfrak{p}})$, and that it is possible to determine $\text{End}(B_{\mathfrak{p}})$ by calculating the characteristic polynomial of the Frobenius endomorphism at $\mathfrak{p}$. We can write down this polynomial after counting the number of $\mathbb{F}_3$ -rational points on $B_{\mathfrak{p}}$. It is easy to see there are only two such points: ∞ and

$(0, 0)$. Therefore the trace of Frobenius is $1 + 3 - 2 = 2$, and the characteristic polynomial is $X^2 - 2X + 3$, by [Si, Chap. V]. Hence $\text{End}(B_p) \cong \mathbb{Q}(\sqrt{-2})$, which is a field with class number one.

Now $\text{End}(B) \hookrightarrow \mathbb{Q}(\sqrt{-2})$, but B cannot have complex multiplication by this field. Indeed, an elliptic curve over $\overline{\mathbb{Q}}$ with complex multiplication by a quadratic imaginary field $\mathcal{K}$ of class number one must have a rational j -invariant [Si, Thm. C.11.2], and the j -invariant of B is $(4 - 3b)^3/b^2(1 - b) \notin \mathbb{Q}$. Thus $\text{End}(B) \cong \mathbb{Q}$. *QED*

Let τ be the non-trivial automorphism of $\mathbb{Q}(\sqrt{-3})$ over $\mathbb{Q}$. Then $\tau(b) = 1 - b$, because b has trace 1, and we may define an isogeny $\mu : {}^\tau B \rightarrow B$ of degree two by

$$\begin{aligned} {}^\tau B : y^2 = x^3 + 2x^2 + (1 - b)x &\xrightarrow{\mu} B : y^2 = x^3 + 2x^2 + bx \\ (x, y) &\longmapsto \left(-\frac{y^2}{2x^2}, \frac{\sqrt{-2}y(1-b-x^2)}{4x^2} \right). \end{aligned}$$

This isogeny may be factored into two steps: first twist ${}^\tau B$ by $\sqrt{-2}$, then use the two-isogeny provided by [Si, Ex. III.4.5]. Similarly, we find a formula for the dual $\hat{\mu} : B \rightarrow {}^\tau B$.

$$\left(-\frac{y^2}{2x^2}, -\frac{\sqrt{-2}y(b-x^2)}{4x^2} \right) \xleftarrow{\hat{\mu}} (x, y)$$

Thus $B/\mathbb{Q}(\sqrt{-3})$ is a $\mathbb{Q}$ -curve, but we note that the isogeny μ is *not* defined over $\mathbb{Q}(\sqrt{-3})$. In fact, we may make the following stronger statement.

Proposition 6.2 *There is no twist of $B/\mathbb{Q}(\sqrt{-3})$ such that the isogeny corresponding to μ is defined over $\mathbb{Q}(\sqrt{-3})$.*

Proof. Any twist of $B/\mathbb{Q}(\sqrt{-3})$ is a twist by $\sqrt{a}$ for some $a \in \mathbb{Q}(\sqrt{-3})$; the resulting curve is $B_a : ay^2 = x^3 + 2x^2 + bx$. Then the isogeny corresponding to μ is

$$\begin{aligned} \tau(B_a) &\longrightarrow B_a \\ (x, y) &\longmapsto \left(-\frac{\tau(a)y^2}{2x^2}, \sqrt{\frac{-2\tau(a)}{a}} \frac{y(1-b-x^2)}{4x^2} \right), \end{aligned}$$

which is not defined over $\mathbb{Q}(\sqrt{-3})$, unless $-2\tau(a)/a$ is a square in $\mathbb{Q}(\sqrt{-3})$. But 2 is a prime in this field, and the valuation at 2 of $-2\tau(a)/a$ must be 1; thus $-2\tau(a)/a$ cannot be a square. *QED*

Now we wish to investigate the two-cocycle $c(g, h) = \mu_g \circ {}^g \mu_h \circ \mu_{gh}^{-1}$. In order to do so, we must extend our base field to $K = \mathbb{Q}(\sqrt{-3}, \sqrt{-2})$. By abusing notation, we now

write τ for the non-trivial element of $\text{Gal}(K/\mathbb{Q})$ fixing $\mathbb{Q}(\sqrt{-2})$, so that τ restricts to our previous τ on $\mathbb{Q}(\sqrt{-3})$. Also, we introduce $\sigma \in \text{Gal}(K/\mathbb{Q})$ as the non-trivial automorphism fixing $\mathbb{Q}(\sqrt{-3})$. Thus we have ${}^\sigma B = B$ and ${}^{\sigma\tau} B = {}^\tau B$, and isogenies $\mu_\sigma = \mu_1 = \text{id} : B \rightarrow B$, and $\mu_{\sigma\tau} = \mu_\tau = \mu : {}^\tau B \rightarrow B$. We remark that by Proposition 5.5, the “degree” $\delta(\mu_g)$ is exactly the usual degree of an isogeny; that is, $\delta(\mu_\sigma) = \delta(\mu_1) = 1$ and $\delta(\mu_{\sigma\tau}) = \delta(\mu_\tau) = 2$.

Note that the following identities are immediate from the formulas for μ and $\hat{\mu}$:

$${}^\sigma \mu = -\mu, \quad {}^\tau \mu = -\hat{\mu}, \quad {}^{\sigma\tau} \mu = \hat{\mu}, \quad \text{and, of course, } \mu\hat{\mu} = 2.$$

We can now calculate the values of $c(g, h)$:

		h			
		1	σ	τ	$\sigma\tau$
g	1	1	1	1	1
	σ	1	1	-1	-1
	τ	1	1	-2	-2
	$\sigma\tau$	1	1	2	2

$c(g, h)$

We would like to split this cocycle as

$$c(g, h) = \frac{\beta(g) \cdot \beta(h)}{\beta(gh)}$$

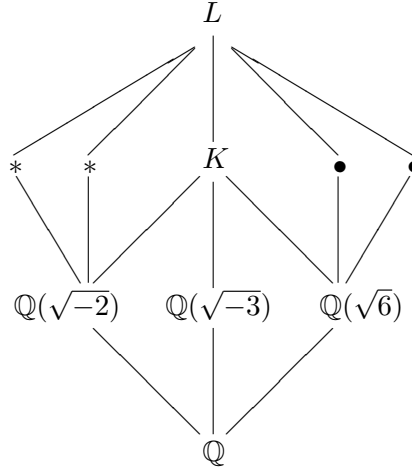
for some (locally constant) function $\beta : G_{\mathbb{Q}} \rightarrow \overline{\mathbb{Q}}^*$. Notice that in order to define such an β , we will again have to extend our base field. There is no such $\beta : G_{\mathbb{Q}} \rightarrow \text{Gal}(K/\mathbb{Q}) \rightarrow \overline{\mathbb{Q}}^*$ because, for example, $\sigma\tau = \tau\sigma$, but $c(\sigma, \tau) \neq c(\tau, \sigma)$. Therefore, we will have to find an extension of K which is non-abelian over $\mathbb{Q}$.

Let L be the splitting field over $\mathbb{Q}$ of the polynomial $X^4 - 4X^2 + 6$. Figure 6.3 diagrams the subfields of L ; in particular, L is a quadratic extension of K .

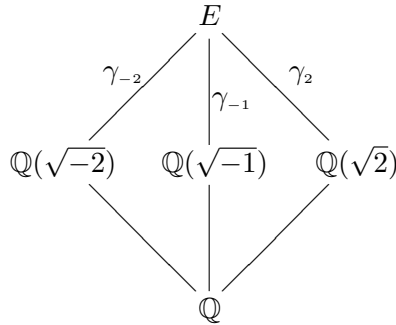
Again we redefine our notation: σ is now an element of $\text{Gal}(L/\mathbb{Q})$ generating the subgroup fixing $\mathbb{Q}(\sqrt{-3})$, and τ is now the (non-trivial) element of $\text{Gal}(L/\mathbb{Q})$ fixing one of the $(*)$ fields, so that σ and τ restrict to our previous σ, τ on K . The Galois group $\text{Gal}(L/\mathbb{Q})$ is of course the dihedral group $D_4 = \langle \sigma, \tau : \sigma^4 = \tau^2 = 1, \tau\sigma = \sigma^3\tau \rangle$.

We are now able to split $c(g, h)$ by defining $\beta(g)$ as follows:

g	1	σ	σ^2	σ^3	τ	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$
$\beta(g)$	1	$\sqrt{-1}$	-1	$-\sqrt{-1}$	$\sqrt{-2}$	$\sqrt{2}$	$-\sqrt{-2}$	$-\sqrt{2}$


 Figure 6.3: The subfields of L

Let E be the field generated by the values of β , i.e., $E = \mathbb{Q}(\sqrt{-1}, \sqrt{-2})$. Then E is a Galois extension of $\mathbb{Q}$, and we write the elements of $\text{Gal}(E/\mathbb{Q})$ as follows.



Now we know from Proposition 4.5 that there is an abelian variety $A/\mathbb{Q}$ of $\mathbf{GL}_2$ -type with $\text{End}_{\mathbb{Q}}(A) \cong E$, such that $A_{/\overline{\mathbb{Q}}}$ is isogenous to $B \times B \times B \times B$. To compute a specific such A , we will use Weil’s “restriction of scalars” functor. We first remind the reader of the salient features of this construction [We, §1.3].

Let $\mathcal{K}/k$ be a finite Galois extension with group G , and let V be an abelian variety over $\mathcal{K}$. The *restriction of scalars* $\text{Res}_{\mathcal{K}/k} V$ from $\mathcal{K}$ to k is an abelian variety W over k , together with a morphism $p : W_{/\mathcal{K}} \rightarrow V$, which represents the functor that takes an abelian variety X over k to the abelian group $\text{Hom}_{\mathcal{K}}(X_{/\mathcal{K}}, V)$. The construction of W shows that

$W_{/K}$ is isomorphic to $\prod_{g \in G} {}^g V$. Thus, applying the universal property with $X = W$, we find

$$\mathrm{End}_k(W) \cong \mathrm{Hom}_K(W_{/K}, V) \cong \mathrm{Hom}_K(\prod_{g \in G} {}^g V, V) \cong \bigoplus_{g \in G} \mathrm{Hom}_K({}^g V, V).$$

Now we return to the specific $\mathbb{Q}$ -curve B , which we view as a curve over the field L . We claim that we may construct A as a quotient of the restriction of scalars $R = \mathrm{Res}_{L/\mathbb{Q}} B$. Indeed, Ribet [Ri 1, Lemma 6.4] has shown that $\mathcal{R} = \mathrm{End}_{\mathbb{Q}}(R)$ is the “twisted group algebra” $\mathbb{Q}[\mathrm{Gal}(L/\mathbb{Q})]^c$, with multiplication defined by $[g][h] = c(g, h)[gh]$ for all $g, h \in \mathrm{Gal}(L/\mathbb{Q})$. The algebra $\mathcal{R}$ maps onto E via $[g] \mapsto \beta(g)$. Moreover, it is easy to see that the kernel of this homomorphism is the ideal $(1 + [\sigma^2])$. Now note that $\frac{1}{2}(1 + [\sigma^2])$ is the central idempotent of the semisimple algebra $\mathcal{R}$ generating this ideal. Therefore, $\frac{1}{2}(1 - [\sigma^2])$ is the complementary central idempotent which projects $\mathcal{R}$ onto E . Thus we may take the abelian variety $A \subset R$ to be the subvariety that is the image of $\frac{1}{2}(1 - [\sigma^2]) \in \mathrm{End}_{\mathbb{Q}}(R)$.

In fact we may describe A more explicitly, by further analysis of the abelian variety R and its endomorphisms over $\mathbb{Q}$. We break down R as $\mathrm{Res}_{K/\mathbb{Q}}(\mathrm{Res}_{L/K} B)$, and first consider $\mathrm{Res}_{L/K} B$, which is an abelian variety over K .

Let B' be the twist of $B_{/K}$ by the quadratic extension L/K . We will continue to write $\mathrm{Gal}(L/K) = \{1, \sigma^2\}$ as a subgroup of $\mathrm{Gal}(L/\mathbb{Q})$.

Lemma 6.4 *The restriction of scalars $\mathrm{Res}_{L/K} B$ is isomorphic over K to $B \times B'$.*

Proof. Recall that by definition, B' is an abelian variety over K which is isomorphic over L (but not over K) to B . Let $\lambda : B \rightarrow B'$ be such an isomorphism over L ; then $\lambda^{-1} \circ \sigma^2 \lambda = -1$. Now define $p : B \times B' \rightarrow B$ by $p = (\frac{1}{2}, \frac{1}{2}\lambda^{-1})$. We will show that the pair $(B \times B', p)$ satisfies the universal property of $\mathrm{Res}_{L/K} B$.

Let X be an abelian variety over K , and $f : X \rightarrow B$ a morphism over L . We must demonstrate the existence of a unique morphism $g : X \rightarrow B \times B'$ over K such that $p \circ g = f$. Note that if g is to be defined over K , we must also have $\sigma^2 p \circ g = \sigma^2 f$. Now using the definition of p , we are able to produce a unique solution to these two equations: $g = (f + \sigma^2 f, \lambda \circ f - \lambda \circ \sigma^2 f)$. Thus $B \times B'$ must be isomorphic to $\mathrm{Res}_{L/K} B$. QED

Now on the one hand, $\mathrm{End}_K(B \times B')$ is plainly equal to $\mathrm{End}_K(B) \times \mathrm{End}_K(B') \cong \mathbb{Q} \times \mathbb{Q}$, while on the other hand, we know $\mathrm{End}_K(\mathrm{Res}_{L/K} B)$ is the group algebra $\mathbb{Q}[\mathrm{Gal}(L/K)]$. Using the isomorphism $(p, \sigma^2 p) : B \times B' \rightarrow B \times \sigma^2 B$ from the above proof, we find that the

induced isomorphism $\text{End}_K(B) \times \text{End}_K(B') \xrightarrow{\sim} \mathbb{Q}[\text{Gal}(L/K)]$ is given by $(1, 0) \mapsto \frac{1}{2}(1 + [\sigma^2])$ and $(0, 1) \mapsto \frac{1}{2}(1 - [\sigma^2])$. In other words, $\frac{1}{2}(1 + [\sigma^2])$ is the projection $\text{Res}_{L/K} B \rightarrow B$, and $\frac{1}{2}(1 - [\sigma^2])$ is the projection $\text{Res}_{L/K} B \rightarrow B'$.

Proposition 6.5 *The abelian variety $A/\mathbb{Q}$ of $\mathbf{GL}_2$ -type is $\text{Res}_{K/\mathbb{Q}} B'$, where B' is the twist of B/K by the quadratic extension L/K .*

Proof. By the universal property of $\text{Res}_{K/\mathbb{Q}}$, there is a map

$$\text{End}_K(\text{Res}_{L/K} B) \rightarrow \text{End}_{\mathbb{Q}}(\text{Res}_{K/\mathbb{Q}}(\text{Res}_{L/K} B)).$$

This is, of course, the natural map $\mathbb{Q}[\text{Gal}(L/K)] \rightarrow \mathbb{Q}[\text{Gal}(L/\mathbb{Q})]^c$. Now as we have seen, $\frac{1}{2}(1 - [\sigma^2])$ is the projection $\text{Res}_{L/K} B \rightarrow B'$; therefore as an endomorphism of $\text{Res}_{L/\mathbb{Q}} B$, this element must project $\text{Res}_{K/\mathbb{Q}}(\text{Res}_{L/K} B)$ onto $\text{Res}_{K/\mathbb{Q}} B'$. But we have defined A to be the image of $\frac{1}{2}(1 - [\sigma^2])$ in $\text{Res}_{L/\mathbb{Q}} B$. Thus $A = \text{Res}_{K/\mathbb{Q}} B'$. *QED*

REMARK. It is important to note that the other factor $\text{Res}_{K/\mathbb{Q}} B$ of R is *not* isogenous over $\mathbb{Q}$ to A . Indeed, an analysis similar to above shows that over $\mathbb{Q}$,

$$\text{Res}_{K/\mathbb{Q}} B \cong \text{Res}_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}} B \times \text{Res}_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}} B_{-2}$$

where B_{-2} is the twist of $B/\mathbb{Q}(\sqrt{-3})$ by $\sqrt{-2}$. Furthermore, recall from our original construction of $\mu : {}^{\tau}B \rightarrow B$ that B is isogenous over $\mathbb{Q}(\sqrt{-3})$ to ${}^{\tau}B_{-2}$. Therefore $\text{Res}_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}} B$ is isogenous over $\mathbb{Q}$ to $\text{Res}_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}} {}^{\tau}B_{-2} = \text{Res}_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}} B_{-2}$. Finally, since we know that ${}^{\tau}B$ is not isogenous to B over $\mathbb{Q}(\sqrt{-3})$, we have $\text{End}_{\mathbb{Q}}(\text{Res}_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}} B) = \mathbb{Q}$. Thus the endomorphism algebra $\text{End}_{\mathbb{Q}}(\text{Res}_{K/\mathbb{Q}} B)$ is isomorphic to $\mathbf{M}_2(\mathbb{Q})$.

Lastly, we calculate some of the functions we have associated to the abelian variety A of $\mathbf{GL}_2$ -type. For example, for each $g \in G_{\mathbb{Q}}$, the automorphism $\varphi \mapsto {}^g\varphi$ on $\text{End}(A)$ is given by conjugation by $\alpha(g) = \beta(g)^{-1}$. We now use these $\alpha(g)$ to calculate the characters $\chi_{\gamma} : G_{\mathbb{Q}} \rightarrow E^*$ defined by $\chi_{\gamma}(g) = \gamma(\alpha(g))/\alpha(g)$ for $\gamma \in \text{Gal}(E/\mathbb{Q})$. Then writing $\sigma, \tau \in \text{Gal}(L/\mathbb{Q})$ as above, we find

$$\begin{array}{lll} \chi_{\gamma_{-2}}(\sigma) & = & -1 \\ \chi_{\gamma_{-2}}(\tau) & = & 1 \end{array} \quad \begin{array}{lll} \chi_{\gamma_{-1}}(\sigma) & = & 1 \\ \chi_{\gamma_{-1}}(\tau) & = & -1 \end{array} \quad \begin{array}{lll} \chi_{\gamma_2}(\sigma) & = & -1 \\ \chi_{\gamma_2}(\tau) & = & -1 \end{array}$$

Also, we remind the reader that the character $\varepsilon : G_{\mathbb{Q}} \rightarrow E^*$ is equal to the inverse of χ_{γ_2} , because γ_2 acts as complex conjugation on E . Thus $\varepsilon(\sigma) = -1$ and $\varepsilon(\tau) = -1$.

Chapter 7

Further Questions

In conclusion, we would like to discuss a few unanswered questions and suggest some avenues of further exploration regarding the topic of abelian varieties of $\mathbf{GL}_2$ -type and their simple components.

The best choice for β ?

One question concerns the construction of abelian varieties of $\mathbf{GL}_2$ -type from building blocks. Given a building block B , we form the two-cocycle $c(\sigma, \tau)$ on $G_{\mathbb{Q}}$ with values in F^* , which we then split as $c(\sigma, \tau) = \beta(\sigma) \cdot \beta(\tau) \cdot \beta(\sigma\tau)^{-1}$, where $\beta : G_{\mathbb{Q}} \rightarrow E^* \subset \overline{F}^*$ is a locally constant function. The question is: what is the “best” choice for β ? And what do we mean by “best”? One possible interpretation is to try to minimize the degree $[E : F]$, which would then minimize the dimension of the abelian variety A of $\mathbf{GL}_2$ -type that we construct from B . Another “best” choice might be to minimize the order of the character ε attached to A . A related question is: what is the connection between abelian varieties of $\mathbf{GL}_2$ -type constructed from the same building block but with different choices of β ?

Generalizing the base field to K ?

We would like to consider the possibility of extending our results from abelian varieties defined over $\mathbb{Q}$ to abelian varieties defined over an arbitrary field K of characteristic zero. The only trouble seems to be in making the “right” definitions; most of the actual work appears to generalize easily. One complication that arises over K but not over $\mathbb{Q}$ is the possibility of quaternionic multiplication over K . It is not hard to show from our results

that if B is a building block over $\mathbb{Q}$, then $\text{End}_{\mathbb{Q}}(B) = \text{End}(B)$ cannot be a quaternion algebra. (There is a more elementary proof of this fact as well, which follows from looking at the action of $\text{End}_{\mathbb{Q}}(B)$ on the Lie algebra $\text{Lie}(B/\mathbb{Q})$.) If K is an arbitrary field, however, then $\text{End}_K(B)$ may be a quaternion algebra.

Now suppose that we try to generalize the definition of building block in the obvious way: a building block is an abelian variety $B/\overline{K}$ such that (i) the endomorphism algebra $\text{End}(B)$ is a central division algebra over a totally real field F with Schur index $t = 1$ or 2 , and $t[F:\mathbb{Q}] = \dim B$; (ii) B is a K -abelian variety; i.e., for each $\sigma \in \text{Gal}(\overline{K}/K)$ there exists an isogeny $\mu_{\sigma} : {}^{\sigma}B \rightarrow B$ that is compatible with $\text{End}(B)$.

Suppose K is a field where a building block and all of its endomorphisms are defined; for instance, consider the case when K is algebraically closed. Then in order to preserve the correspondence between building blocks and abelian varieties of $\mathbf{GL}_2$ -type, it is necessary to broaden our definition of $\mathbf{GL}_2$ -type. We need: an abelian variety A/K is of $\mathbf{GL}_2$ -type if $\text{End}_K(A)$, the algebra of endomorphisms of A defined over K , is a central division algebra over a number field E with Schur index $t = 1$ or 2 , and $t[E:\mathbb{Q}] = \dim A$.

These new definitions certainly demonstrate a symmetry that was lacking in the case $K = \mathbb{Q}$. On the other hand, the terminology “of $\mathbf{GL}_2$ -type” does not make much sense in the case $2[E:\mathbb{Q}] = \dim A$. Therefore we might want to preserve the original definition of $\mathbf{GL}_2$ -type—requiring $\text{End}_K(A) = E$ and $[E:\mathbb{Q}] = \dim A$ —and change the definition of building block accordingly, which would probably require another restriction on the structure of $\text{End}(B)$.

Modularity?

The ultimate goal is to prove that all abelian varieties of $\mathbf{GL}_2$ -type are modular, that is, appear as quotients of Jacobians $J_1(N)$. Modularity would provide us with a lot more information about the structure of our abelian varieties of $\mathbf{GL}_2$ -type and their building blocks. As mentioned in the introduction, Ribet has shown that this result is implied by Serre’s conjecture of [Se 4, (3.2.4)], but an in-depth discussion of this issue is beyond the scope of this paper.

Appendix A

A Non-Building Block

Recall that in our definition of a building block B , we have required that B be a $\mathbb{Q}$ -abelian variety, which we have defined as follows:

Definition. An abelian variety $B/\overline{\mathbb{Q}}$ is a $\mathbb{Q}$ -abelian variety if for each $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, there exists an isogeny $\mu_\sigma : {}^\sigma B \rightarrow B$ compatible with the endomorphisms of B ; that is, $\mu_\sigma \circ {}^\sigma \varphi = \varphi \circ \mu_\sigma$ for all $\varphi \in \text{End}(B)$.

It is natural to ask whether the compatibility conditions on the μ_σ are necessary. Given an abelian variety B over $\overline{\mathbb{Q}}$ that is isogenous to all of its Galois conjugates, is it perhaps always possible to find a collection of isogenies $\{\mu_\sigma\}$ that respect $\text{End}(B)$? We answer this question in the negative.

We will construct a two-dimensional abelian variety A over $\mathbb{Q}$ such that the full endomorphism algebra $\text{End}(A)$ is isomorphic to $\mathbb{Q}(\sqrt{5})$, but not all of the endomorphisms are defined over $\mathbb{Q}$. Thus, if $\sigma \in G_{\mathbb{Q}}$ acts non-trivially on $\text{End}(A)$, there is no isogeny $\mu_\sigma : A = {}^\sigma A \rightarrow A$ such that $\varphi \circ \mu_\sigma = \mu_\sigma \circ {}^\sigma \varphi$ for all $\varphi \in \text{End}(A)$.

The abelian variety A will be the Jacobian of a certain hyperelliptic curve of genus two. A theorem due to Mestre describes how to construct the necessary curve.

Theorem A.1 *Let d be a positive integer. Let E be an elliptic curve over $\overline{\mathbb{Q}}$ equipped with a point S of order $2d+1$ and a point Q such that $2Q$ does not belong to $\langle S \rangle$; let x_E be a function of degree two on E with a double pole at O_E . Define C to be the hyperelliptic curve of genus d described by the equation*

$$y^2 = \prod_{i=0}^{2d} (x - x_E(Q + iS)).$$

Then the Jacobian of C admits an endomorphism whose characteristic polynomial is

$$\prod_{m=1}^d \left(X - 2 \cos \frac{2m\pi}{2d+1} \right).$$

Proof. [Me, Thm. 1].

We remark that we will apply the theorem in the case $d = 2$, when in fact it reduces (via a theorem of Poncelet) to a classical result of Humbert.

NOTE: All the calculations that follow were done on a SparcStation with the GP/PARI Calculator, version 1.37.

Construction of the Curve C

In order for the equation of the curve C to be defined over $\mathbb{Q}$, the set of points $\{Q + iS\}_{i=0}^4$ must be stable under the action of $G_{\mathbb{Q}}$. We thus look for an elliptic curve over $\mathbb{Q}$ with a rational point Q and a subgroup $\langle S \rangle$ of order five that is $G_{\mathbb{Q}}$ -stable. Take E to be the elliptic curve $J_0(11)$, given by the equation

$$E : y^2 + y = x^3 - x^2 - 10x - 20.$$

The point $Q = (16, 60)$ is easily seen to be a rational point on E ; in fact, it has order five, and it generates all the $\mathbb{Q}$ -rational points on E . Now we need to find the rest of the five-torsion subgroup, $E[5]$. According to [Si, III.2.3d], the “duplication formula” for points P on E is

$$x_E(2P) = \frac{x_P^4 + 20x_P^2 + 158x_P + 21}{4x_P^3 - 4x_P^2 - 40x_P - 79} \quad \text{where } x_P = x_E(P).$$

We use this formula to solve for the points P on E satisfying $x_E(4P) = x_E(-P) = x_E(P)$. We find that the x -coordinates of such points are exactly the roots of the following irreducible polynomials:

$$\begin{aligned} & x - 16 \\ & x - 5 \\ (*) \quad & 5x^2 + 5x - 29 \\ & x^4 + x^3 + 11x^2 + 41x + 101 \\ & x^4 + 15x^3 + 120x^2 + 200x + 155 \\ & 3x^4 - 4x^3 - 60x^2 - 237x - 21. \end{aligned}$$

The last polynomial clearly corresponds to the points of order three on E , and we may safely forget about it; the others correspond to $G_{\mathbb{Q}}$ -stable sets of points of order five; e.g., $(x - 16)$ corresponds to $\{\pm Q\}$, and $(x - 5)$ to $\{\pm 2Q\}$.

Let S be a point of E such that $x_E(S)$ is a root of the quadratic polynomial $(*)$; hence $x_E(S) \in \mathbb{Q}(\sqrt{5})$. Note that $x_E(2S)$ must also lie in $\mathbb{Q}(\sqrt{5})$ by the duplication formula, and so $x_E(2S)$ must be the other root of $(*)$. Therefore the points of order five corresponding to $(*)$ are $\{\pm S, \pm 2S\}$, and furthermore, these points must be stable under $G_{\mathbb{Q}}$. In other words, the subgroup $\langle S \rangle$ is $G_{\mathbb{Q}}$ -stable, as desired. (In fact, $\langle S \rangle$ is the Shimura subgroup of $J_0(11)$.)

It is now clear that the monic quartic polynomials above correspond to the sets $\{Q + iS\}_{i=1}^4$ and $\{2Q + iS\}_{i=1}^4$, but we need to determine which is which. There are several ways to do this; we choose brute force, and use a computer.

First we claim that S (and hence $E[5]$, which is generated by Q and S) is defined over $\mathbb{Q}(\zeta)$, where ζ is a primitive fifth root of unity. Indeed, suppose that $\sigma \in G_{\mathbb{Q}}$ fixes $\mathbb{Q}(\zeta)$. Then, because $\langle S \rangle$ is stable under $G_{\mathbb{Q}}$, we may write ${}^{\sigma}S = aS$ for some integer $a \pmod{5}$. Now let e_5 be the Weil pairing $E[5] \times E[5] \rightarrow \mu_5 \subset \mathbb{Q}(\zeta)$. Note that because Q and S generate $E[5]$, $e_5(Q, S) \neq 1$. Now

$$\begin{aligned} e_5(Q, S) &= {}^{\sigma}e_5(Q, S) && \text{because } \sigma \text{ fixes } \mathbb{Q}(\zeta). \\ &= e_5({}^{\sigma}Q, {}^{\sigma}S) && \text{because the Weil pairing is Galois invariant.} \\ &= e_5(Q, aS) && \text{by definition of } a. \\ &= e_5(Q, S)^a. \end{aligned}$$

Thus a must be congruent to 1 $\pmod{5}$; i.e., σ must fix S , so S is defined over $\mathbb{Q}(\zeta)$.

Now we may write down explicit coordinates in $\mathbb{Q}(\zeta)$ for S . Take S to be the point (α, β) , where

$$\begin{aligned} \alpha &= -\frac{11}{5}(\zeta + \zeta^{-1}) - \frac{8}{5}, \\ \beta &= \frac{11}{5}(2\zeta^3 + \zeta^2 + 3\zeta + \frac{14}{11}). \end{aligned}$$

A quick computer calculation supplies us with

$$\prod_{i=0}^4 (x - x_E(Q + iS)) = (x - 16)(x^4 + x^3 + 11x^2 + 41x + 101).$$

We now define C to be the hyperelliptic curve of genus two described by the equation

$$C : y^2 = (x - 16)(x^4 + x^3 + 11x^2 + 41x + 101),$$

and write A for the Jacobian of C . Then A is a two-dimensional abelian variety over $\mathbb{Q}$, and by Theorem A.1, there is an endomorphism of A with characteristic polynomial $X^2 + X - 1$; thus $\text{End}(A) \supseteq \mathbb{Q}(\sqrt{5})$.

The Structure of $\text{End}(A)$

The author would like to thank F. Hazama of Tokyo-Denki University for suggesting the approach used in this section.

Let A be the abelian variety constructed in the previous section. It is well known that if p is a prime of good reduction for A , then the natural map $\text{End}(A) \rightarrow \text{End}(A_p)$ is injective, where A_p is the reduction of A mod p . Indeed, let ℓ be a prime not equal to p ; write $T_\ell(A)$ for the Tate module and $V_\ell(A)$ for $T_\ell(A) \otimes \mathbb{Q}$. Then use the facts that the reduction map is injective on ℓ -power torsion [Si, Prop. VII.3.1], that $\text{End}(A) \hookrightarrow \text{End } V_\ell(A)$ [W-M, Thm. 3], and that $\text{End}(A_p) \cong \text{End } V_\ell(A_p)$, because A_p is defined over a finite field [W-M, Thm. 6]. The result then follows from the commutative diagram:

$$\begin{array}{ccc} \text{End}(A) & \longrightarrow & \text{End}(A_p) \\ \downarrow & & \downarrow \cong \\ \text{End } V_\ell(A) & \hookrightarrow & \text{End } V_\ell(A_p) \end{array}$$

Therefore, in order to study $\text{End}(A)$, we will look at $\text{End}(A_p)$ for various choices of p .

To ease calculation, we search for primes p of good reduction with the properties:

- (i) $\text{End}_{\mathbb{F}_p}(A_p) \cong \mathbb{Q}(\pi_p)$, where π_p is the Frobenius endomorphism.
- (ii) All endomorphisms of A_p are defined over $\mathbb{F}_p$.

We will use [W-M, Thm. 8]:

Theorem A.2 *Let X be a simple abelian variety over the finite field with q elements. Let π_q be the Frobenius endomorphism of X , and let f be the characteristic polynomial of π_q acting on $T_\ell(X)$, where ℓ is a prime not dividing q . Then*

1. $f = g^e$, where g is a monic irreducible polynomial with integer coefficients.
2. $\text{End}_{\mathbb{F}_q}(X)$ is a division algebra whose center is $\mathbb{Q}(\pi_q)$.
3. $\dim_{\mathbb{Q}} \text{End}_{\mathbb{F}_q}(X) = e^2[\mathbb{Q}(\pi_q) : \mathbb{Q}]$, and $2 \dim X = e[\mathbb{Q}(\pi_q) : \mathbb{Q}]$.

Now, in order to prove that a prime p satisfies conditions (i) and (ii), we claim that it is enough to show that the characteristic polynomial of each power of π_p is irreducible of degree four over $\mathbb{Q}$. Indeed, the full endomorphism algebra $\text{End}(A_p)$ is the union $\bigcup_r \text{End}_{\mathbb{F}_{p^r}}(A_p)$, and the Frobenius endomorphism π_{p^r} is simply π_p^r . Therefore, if the characteristic polynomial of π_p^r is irreducible of degree $4 = 2 \dim A_p$ for all r , then by (3) we have $\text{End}_{\mathbb{F}_{p^r}}(A_p) \cong \mathbb{Q}(\pi_p^r)$ for all r . Lastly, we see that $\mathbb{Q}(\pi_p^r) = \mathbb{Q}(\pi_p)$ for all r , because $\mathbb{Q}(\pi_p^r)$ is certainly contained in $\mathbb{Q}(\pi_p)$, and by hypothesis both these fields have degree four over $\mathbb{Q}$.

To calculate the characteristic polynomial of π_p , we recall the Frobenius endomorphism π_{C_p} of the curve C_p , which induces the Frobenius endomorphism π_p on A_p . (We remind the reader that for any variety over $\mathbb{F}_q$ with a projective embedding, the “Frobenius” morphism is simply the map on points $(x_0 : \dots : x_n) \mapsto (x_0^q : \dots : x_n^q)$.) The map π_{C_p} has a characteristic polynomial obtained by considering the action of π_{C_p} on the étale cohomology group $H_{\text{et}}^1(C_p, \mathbb{Z}_\ell)$, where ℓ is prime to p . But by [Mil, Cor. 9.6],

$$H_{\text{et}}^1(C_p, \mathbb{Z}_\ell) \cong H_{\text{et}}^1(A_p, \mathbb{Z}_\ell) \cong T_\ell(A_p)^\vee,$$

where $^\vee$ denotes the $\mathbb{Z}_\ell$ -dual. Hence the characteristic polynomial of π_{C_p} is in fact the same as the characteristic polynomial of π_p acting on $T_\ell(A_p)$, which is what we want. Therefore we will use the curve C_p to calculate this polynomial.

Here we must note that the equation defining C is singular at infinity, so as yet it does not make sense to speak of primes of good reduction for C . However, C has a non-singular model $\tilde{C} \subset \mathbb{P}^4$. The map $\tilde{C} \rightarrow C$ is an isomorphism over all affine points of C , and has a unique point over the singularity of C [Ca, §2]. Furthermore, this “point at infinity” of $\tilde{C}$ is a smooth point mod p for each prime p . Hence to study the reduction of $\tilde{C}$ at p , it suffices to consider the reduction mod p of our affine equation for C .

First, we calculate the discriminant of the fifth degree polynomial appearing in the equation for C ; it is $5^5 \cdot 11^{14}$. Thus the primes of bad reduction for this equation are exactly $p = 5$ or $p = 11$, and these we will avoid. Now we need [M-S, Lemma 3]:

Lemma A.3 *Let C be a curve of genus two over $\mathbb{Q}$ with good reduction at the prime p . Then the characteristic polynomial of the Frobenius element at p is given by*

$$(A.3) \quad X^4 - tX^3 + sX^2 - ptX + p^2,$$

$$\text{where } t = p + 1 - N_1,$$

$$N_1 = \#C_p(\mathbb{F}_p),$$

$$s = \frac{1}{2}(N_1^2 + N_2) + p - N_1 - pN_1,$$

$$N_2 = \#C_p(\mathbb{F}_{p^2}).$$

Abusing notation, we write π_p for a root of (A.3). Recall that we want all powers of π_p to generate a field of degree four over $\mathbb{Q}$. In particular, we must have $t \neq 0$ for this situation to occur (since otherwise π_p^2 is quadratic over $\mathbb{Q}$). A computer search now finds that $p = 19$ gives $N_1 = 16$ and $N_2 = 390$, so (A.3) becomes

$$(A.4) \quad X^4 - 4X^3 + 22X^2 - 76X + 361,$$

which is irreducible over $\mathbb{Q}$. Note that over $\mathbb{Q}(\sqrt{5})$ the polynomial (A.4) factors as

$$(X^2 + 4\varepsilon X + 19)(X^2 - (4 + 4\varepsilon)X + 19) \quad \text{where } \varepsilon = (-1 + \sqrt{5})/2.$$

To fix ideas, let π_{19} be a root of the first factor and let $K = \mathbb{Q}(\pi_{19})$. The field K contains the complex conjugate $\bar{\pi}_{19}$, but is not Galois over $\mathbb{Q}$; it is straightforward to check that the other quadratic polynomial defines a different extension of $\mathbb{Q}(\sqrt{5})$. As a consequence, we see that K has only one non-trivial subfield, namely $\mathbb{Q}(\sqrt{5})$. (Indeed, if K contained another quadratic subfield, it would be biquadratic over $\mathbb{Q}$, and hence Galois.)

We now claim that all powers of π_{19} have degree four over $\mathbb{Q}$. Suppose this were not the case. Then π_{19}^n would lie in $\mathbb{Q}(\sqrt{5})$ for some n , and we would have $\pi_{19}^n = \bar{\pi}_{19}^n$. But then $\pi_{19}/\bar{\pi}_{19}$ would be a root of unity in K , and clearly the only roots of unity in K are ± 1 . But $\bar{\pi}_{19}$ cannot equal $\pm \pi_{19}$, since by definition of π_{19} above, $\pi_{19}\bar{\pi}_{19} = 19$ and $\pi_{19} + \bar{\pi}_{19} = -4\varepsilon$. Therefore π_{19}^n generates $\mathbb{Q}(\pi_{19})$ over $\mathbb{Q}$.

We have now shown that $\text{End}(A_{19}) = \text{End}_{\mathbb{F}_{19}}(A_{19}) \cong \mathbb{Q}(\pi_{19})$.

The next prime we investigate is $p = 59$. In this case $N_1 = 76$ and $N_2 = 3550$, so the characteristic polynomial of Frobenius is

$$(A.5) \quad X^4 + 16X^3 + 162X^2 + 944X + 59^2.$$

The polynomial (A.5) is irreducible over $\mathbb{Q}$ and factors over $\mathbb{Q}(\sqrt{5})$ as

$$(X^2 + (6 - 4\varepsilon)X + 59)(X^2 + (10 - 4\varepsilon)X + 59).$$

We let π_{59} be a root of the first factor and then exactly the same analysis as the case $p = 19$ demonstrates that $\text{End}(A_{59}) = \text{End}_{\mathbb{F}_{59}}(A_{59}) \cong \mathbb{Q}(\pi_{59})$, which is again a non-Galois extension of $\mathbb{Q}$ of degree four whose only non-trivial subfield is $\mathbb{Q}(\sqrt{5})$.

Finally, recall that $\text{End}(A)$ injects into both $\text{End}(A_{19})$ and $\text{End}(A_{59})$, and that $\text{End}(A) \supseteq \mathbb{Q}(\sqrt{5})$. Hence to show $\text{End}(A) \cong \mathbb{Q}(\sqrt{5})$, it suffices to show that $\mathbb{Q}(\pi_{19})$ and

$\mathbb{Q}(\pi_{59})$ are distinct number fields. But this follows immediately from the calculation of their discriminants over $\mathbb{Q}$, which are $5^2 \cdot 149$ and $2^6 \cdot 5^2 \cdot 281$, respectively.

To complete our analysis of the structure of $\text{End}(A)$, it remains to show that not all endomorphisms of A are defined over $\mathbb{Q}$. Now as above, for any prime p of good reduction we have $\text{End}_{\mathbb{Q}}(A) \hookrightarrow \text{End}_{\mathbb{F}_p}(A_p)$. But we are now interested in primes p such that *not* all endomorphisms of A_p are defined over $\mathbb{F}_p$. For instance, we take $p = 3$ and calculate that $N_1 = 4$ and $N_2 = 10$. Therefore the characteristic polynomial of the Frobenius element at 3 is $X^4 + 9$, which is irreducible over $\mathbb{Q}$, and so $\text{End}_{\mathbb{F}_3}(A_3) \cong \mathbb{Q}(\pi_3)$. But $\mathbb{Q}(\pi_3)$ is the field $\mathbb{Q}(\sqrt{-1}, \sqrt{6})$, which clearly does not contain $\mathbb{Q}(\sqrt{5})$ as a subfield. Hence $\text{End}_{\mathbb{Q}}(A)$ cannot be isomorphic to $\mathbb{Q}(\sqrt{5})$, and we must have $\text{End}_{\mathbb{Q}}(A) \cong \mathbb{Q}$.

Now we see that $A/\mathbb{Q}$ is an abelian variety that has all of the properties of a building block, *except* the compatibility conditions on the μ_σ . Of course, a building block over $\mathbb{Q}$ is exactly an abelian variety of $\mathbf{GL}_2$ -type, and we can also see now that A is not of $\mathbf{GL}_2$ -type, since $[\text{End}_{\mathbb{Q}}(A) : \mathbb{Q}] = 1 \neq 2 = \dim A$. This demonstrates the importance of requiring in our definition of building block that all of the isogenies $\mu_\sigma : {}^\sigma B \rightarrow B$ respect $\text{End}(B)$.

Appendix B

Useful Facts Concerning Central Simple Algebras

The endomorphism algebra of an abelian variety is a finite-dimensional semi-simple algebra over $\mathbb{Q}$. In this dissertation, we are concerned mostly with abelian varieties whose endomorphism algebras are in fact simple $\mathbb{Q}$ -algebras. We list here a collection of definitions and facts describing the structure of these algebras.

NOTATION

$Z(\mathcal{A}) = \{x \in \mathcal{A} : xa = ax \ \forall a \in \mathcal{A}\}$ will denote the *center* of an algebra $\mathcal{A}$.

$C_{\mathcal{A}}(\mathcal{B}) = \{x \in \mathcal{A} : xb = bx \ \forall b \in \mathcal{B}\}$ will denote the *centralizer* of a subalgebra $\mathcal{B} \subseteq \mathcal{A}$.

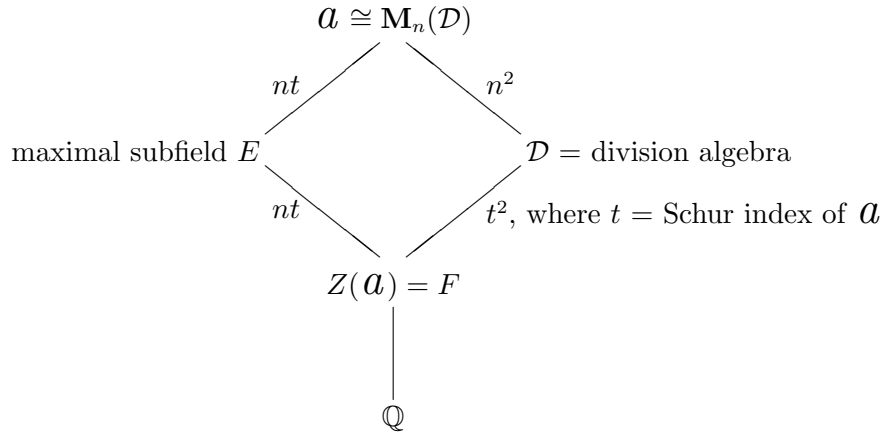
Let $\mathcal{A}$ be a finite-dimensional simple $\mathbb{Q}$ -algebra.

- The center $Z(\mathcal{A})$ is a number field F [Pi, Prop. 12.1]. The algebra $\mathcal{A}$ is then a *central simple algebra* over F .
- $\mathcal{A}$ has a unique (up to isomorphism) simple right module M [Pi, Prop. 3.3b], and as right $\mathcal{A}$ -modules, $\mathcal{A} \cong \bigoplus^n M$ for some $n \geq 1$.
- (Wedderburn Structure Theorem.) As F -algebras, $\mathcal{A} \cong \mathbf{M}_n(\mathcal{D})$, where $\mathcal{D} = \text{End}_{\mathcal{A}} M$ is a central division algebra over F [Pi, Cor. 3.5a].
- The dimension $\dim_F \mathcal{A}$ is a square [Pi, Prop. 13.1].
- The *Schur index* of $\mathcal{A}$ is $\sqrt{\dim_F \mathcal{D}}$.

Note that the Schur index of $\mathcal{A}$ depends only on the class of $\mathcal{A}$ in $\text{Br}(F)$.

- (Hasse-Brauer-Noether Theorem.) The Schur index of $\mathcal{A}$ is equal to the order of the class of $\mathcal{A}$ in the Brauer group $\text{Br}(F)$ [Pi, Thm. 18.6]. (Here it is necessary that F be a number field.)
- (Skolem-Noether Theorem.) Let $\mathcal{B}$ be a simple F -algebra. If $f, g : \mathcal{B} \rightarrow \mathcal{A}$ are homomorphisms, then there is an inner automorphism $\alpha : \mathcal{A} \rightarrow \mathcal{A}$ such that $\alpha \circ f = g$. In particular, any automorphism of $\mathcal{A}$ is inner [Pi, Thm. 12.6].
- (Double Centralizer Theorem.) If $\mathcal{B}$ is a simple subalgebra of $\mathcal{A}$, then [Pi, Thm. 12.7]
 - (i) $C_{\mathcal{A}}(\mathcal{B})$ is simple.
 - (ii) $(\dim_F \mathcal{B})(\dim_F C_{\mathcal{A}}(\mathcal{B})) = \dim_F \mathcal{A}$.
 - (iii) $C_{\mathcal{A}}(C_{\mathcal{A}}(\mathcal{B})) = \mathcal{B}$.
- A *subfield* of $\mathcal{A}$ is a subalgebra E of $\mathcal{A}$ such that E is a field.
A *maximal subfield* of $\mathcal{A}$ is a subfield which is maximal with respect to inclusion.
- The following are equivalent for a subfield $E \subseteq \mathcal{A}$ [Pi, Prop. 13.1].
(Here it is necessary that F be a number field.)
 - (i) E is a maximal subfield of $\mathcal{A}$.
 - (ii) $[E:F] = \sqrt{\dim_F \mathcal{A}}$.
 - (iii) $C_{\mathcal{A}}(E) = E$.
- A maximal subfield $E \subseteq \mathcal{A}$ splits $\mathcal{A}$; i.e., $E \otimes_F \mathcal{A} \cong \mathbf{M}_{nt}(E)$ [Pi, Cor. 13.3].

The following diagram summarizes some of the main points.



Bibliography

- [Br] K. S. BROWN. *Cohomology of Groups*. Graduate Texts in Math. **87**, Springer-Verlag, New York, 1982.
- [Ca] J. W. S. CASSELS. Arithmetic of curves of genus 2. In *Number Theory and Applications*, pp. 27–35, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci. **265**, Kluwer Academic Publishers, Boston, 1989.
- [El] N. ELKIES. Remarks on elliptic K -curves. Preprint, 1993.
- [Ma] B. MAZUR. Number theory as gadfly. *Amer. Math. Monthly* **98** (1991), pp. 593–610.
- [M-S] J. R. MERRIMAN AND N. P. SMART. Curves of genus 2 with good reduction away from 2 with a rational Weierstrass point. *Math. Proc. Cambridge Philos. Soc.* **114** (1993), pp. 203–214.
- [Me] J.-F. MESTRE. Courbes hyperelliptiques à multiplication réelles. *C. R. Acad. Sci. Paris Sér. I Math.* **307** (1988), pp. 721–724.
- [Mil] J. S. MILNE. Jacobian varieties. In G. Cornell and J. H. Silverman (ed.), *Arithmetic Geometry*, pp. 167–212, Springer-Verlag, New York, 1986.
- [Mit] B. MITCHELL. *Theory of Categories*. Pure Appl. Math. **17**, Academic Press, New York, 1965.
- [Mu] D. MUMFORD. *Abelian Varieties*, Second edition. Tata Inst. Fund. Res. Studies in Math. **5**, Oxford University Press, London, 1974.
- [Pi] R. S. PIERCE. *Associative Algebras*. Graduate Texts in Math. **88**, Springer-Verlag, New York, 1982.

- [Ri 1] K. A. RIBET. Abelian varieties over $\mathbb{Q}$ and modular forms. In *1992 Proceedings of KAIST Mathematics Workshop*, pp. 53–79, Korea Advanced Institute of Science and Technology, Taejon, 1992.
- [Ri 2] K. A. RIBET. Fields of definition of abelian varieties with real multiplication. In *Arithmetic Geometry: Conference on Arithmetic Geometry with an Emphasis on Iwasawa Theory, 1993*, pp. 107–118, Contemp. Math. **174**, American Mathematical Society, Providence, 1994.
- [Se 1] J.-P. SERRE. *Cohomologie Galoisienne*, Deuxième édition. Lecture Notes in Math. **5**, Springer-Verlag, Berlin–Göttingen–Heidelberg, 1964.
- [Se 2] J.-P. SERRE. *Corps Locaux*. Actualités Sci. Indust. **1296**, Hermann, Paris, 1968.
- [Se 3] J.-P. SERRE (prepared in collaboration with C. J. BUSHNELL). Modular forms of weight one and Galois representations. In A. Fröhlich (ed.), *Algebraic Number Fields: L-functions and Galois properties*, pp. 193–268, Academic Press, London, 1977.
- [Se 4] J.-P. SERRE. Sur les représentations modulaires de degré 2 de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *Duke Math. J.* **54** (1987), pp. 179–230.
- [Sh 1] G. SHIMURA. Class fields over real quadratic fields and Hecke operators. *Ann. of Math. (2)* **95** (1972), pp. 131–190.
- [Sh 2] G. SHIMURA. *Introduction to the Arithmetic Theory of Automorphic Functions*. Publ. Math. Soc. Japan **11**, Princeton University Press, Princeton, 1971.
- [Sh 3] G. SHIMURA. On analytic families of polarized abelian varieties and automorphic functions. *Ann. of Math. (2)* **78** (1963), pp. 149–192.
- [Sh 4] G. SHIMURA. On the factors of the jacobian variety of a modular function field. *J. Math. Soc. Japan* **25** (1973), pp. 523–544.
- [Si] J. H. SILVERMAN. *The Arithmetic of Elliptic Curves*. Graduate Texts in Math. **106**, Springer-Verlag, New York, 1986.

- [W-M] W. C. WATERHOUSE AND J. S. MILNE. Abelian varieties over finite fields. In *1969 Number Theory Institute*, pp. 53–64, Proc. Sympos. Pure Math. **20**, American Mathematical Society, Providence, 1971.
- [We] A. WEIL. *Adeles and Algebraic Groups*. Progr. Math. **23**, Birkhauser, Boston, 1982.