UNIVERSITAT DE BARCELONA

Abelian Varieties of GL_n-type and Galois Representations

by

Enric Florit Zacarías

PhD Dissertation

Advisors: Luis Victor Dieulefait and Francesc Fité Naya

Tutor: Xavier Guitart Morales

Doctoral Program of Mathematics and Computer Science

Barcelona, September 2025

Als meus pares, Toni i Loli,
i a l'Ana

Abstract

This thesis is concerned with the arithmetic properties of abelian varieties in relation to their endomorphism algebras. We study the reductions of an abelian variety defined over a number field, as well as the system of Galois representations attached to it. We also give some results on modularity of abelian varieties with respect to Siegel modular forms.

Chapter 1 gives some background definitions and results on central simple algebras and abelian varieties. The proper content begins with Chapter 2, in which we study embeddings of simple algebras. An emphasis is made in characterising the existence of an embedding between two simple algebras. We specialize a criterion of Chia-Fu Yu for algebras over global and local fields, which plays an important role in Chapters 3, 5 and 7.

Chapter 3 studies the properties of abelian varieties defined over finite fields under the assumption that their endomorphism algebra is noncommutative. We focus on classifying abelian fourfolds with quaternionic multiplication. We show that an abelian variety over a number field with noncommutative endomorphism algebra splits modulo all but finitely many primes. This generalizes the analogue result for fake elliptic curves, and strengthens a conjecture of Murty and Patankar. We also give an example of an abelian fourfold with exactly two good, geometrically simple reductions.

Chapter 4 begins the description of the systems of Galois representations associated to abelian varieties with some noninteger endomorphism. We describe the irreducible constituents of the Tate module in terms of the endomorphism algebra, and we show how the representations take values in a twisted form of the algebraic group GL_n. We also show the nature of the Weil pairing on these irreducible consituents, which depends on the Albert type of the endomorphisms. Chapter 5 is based on joint work with F. Fité and X. Guitart. It defines the notion of an abelian variety genuinely of GL_n-type, to generalize Ribet's abelian varieties of GL_2-type without potential complex multiplication. These are the varieties whose system of Galois representations stays absolutely irreducible when taking a base change to a finite field extension. We give a theory of building blocks. Under a technical hypothesis, we define inner twists and the Nebentype character of an abelian variety. We give a characterization of abelian varieties with symplectic or orthogonal Galois representation, which we call genuinely of GSp_n or GO_n-type. This enlarges the class of abelian varieties with such representations previously given by Banaszak, Gajda and Krasoń. Finally, we prove that an abelian variety genuinely of GL_4-type is Siegel modular if and only if it is genuinely of GSp_4-type.

In Chapter 6 we construct a family of building blocks of GL_4-type. These are given as Jacobians of genus 2 curves with a Richelot isogeny to their Galois conjugate. Under certain conditions, we obtain by Weil restriction examples of

abelian fourfolds genuinely of GSp_4-type. The family includes examples of Galois representations with image in GSp_4 and nontrivial Nebentype.

Chapter 7 is based on joint work with A. Pacetti. It deals with the Galois representations associated with abelian k-varieties. One of the key points is that we do not assume that all endomorphisms are defined over the base field. This allows to treat abelian varieties potentially of GL_n-type. A recipe is given to attach a representation of the absolute Galois group of k to such an abelian variety. In addition, some results are given to characterize when these preserve a pairing induced by the Weil pairing, building on the ideas of Chapter 4. As an application, we show that abelian surfaces over $\mathbb{Q}$ with potential quaternionic multiplication are Siegel modular.

Keywords: abelian varieties, central simple algebras, Honda–Tate theory, Galois representations, quaternionic multiplication, modularity.

Acknowledgements

First of all, I wish to thank Francesc Fité and Xavier Guitart. Their guidance and support during the past four years have made this thesis possible. I especially thank Francesc for his dedication and attention to detail, and Xevi for posing many of the questions answered in this work –and some more that I am still trying to answer. I also thank them for the mathematical discussions. But above all, I thank them both for their never-ending patience. I also thank Luis Dieulefait for his support and advice, and for his interest in this project.

Next, I want to express my gratitude to Ariel Pacetti and the Universidade de Aveiro for their hospitality during the fall of 2023. I am very glad for the many discussions we have held since. I am particularly indebted to Ariel for providing the approach to see the Nebentypes in the family of fourfolds, which ultimately made it possible to pass from GL_4 to GSp_n and GO_n.

I thank all my peers in the doctoral program at the Facultat de Matemàtiques i Informàtica for their companionship and good spirit. I especially wish to mention the students that are part of the (extended) Seminari de Teoria de Nombres de Barcelona: Ignasi Sánchez, Javier Guillán, Eloi Torrents, Francesc Pedret, Josu Pérez, Filip Gawron, José Castro, Matilde Costa, Antti Haavikko, and Oriol Navarro. All of you have helped me way more than you can imagine.

Vull agrair també l'ajuda i l'encoratjament dels meus amics i família. Gràcies a l'Oriol per tots els ànims que m'ha donat. Agraeixo de tot cor el suport dels meus pares, Toni i Loli, que sempre m'han animat a seguir en aquest camí.

Finalment, tanco aquestes línies donant gràcies a l'Ana, de qui he rebut –durant la tesi i sempre– el seu suport incondicional. Mai no hauria arribat tan lluny sense tu.

This work has received the following financial support:

- Ministerio de Universidades – Formación del Profesorado Universitario FPU20/05059.
- Ministerio de Ciencia e Innovación: PID2022-137605NB-I00, PID2019-107297GB-I00.
- Agència de Gestió d'Ajuts Universitaris i de Recerca: 2021 SGR 0146.
- Ajuts per a la realització d'estades formatives a Espanya i l'estranger finançades per la Fundació Montcelimar, convocatòria 2023.

Contents

Notations

We denote the ring of n-by-n matrices over a ring R by $\mathrm{M}_n(R)$. The identity matrix is denoted by Id. Matrix transposition is denoted by $^\top$. If X is a central simple algebra over a number field Z, we let $\mathrm{Ram}(X)$ be the set of places of Z at which X ramifies. Given a place v of Z, the local Hasse invariant of X at v is denoted by $\mathrm{inv}_v[X]$.

Given a group G and a character χ with values in a field F, we denote by $F(\chi)$ the representation afforded by χ. If V is another representation of G, we write $V(\chi)$ or $V \otimes \chi$ for the representation $V \otimes F(\chi)$. The notation $\mathrm{End}_{F[G]}(V)$, or simply $\mathrm{End}_G(V)$, denotes the endomorphisms of V as an F-vector space which commute with the action of G.

We fix once and for all an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$. Given a number field k embedded in $\bar{\mathbb{Q}}$, we let G_k be its absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/k)$. Occasionally, we will also write $\bar{k}$ instead of $\bar{\mathbb{Q}}$. For a prime v of k, $\mathrm{Frob}_v \in G_k$ denotes an arithmetic Frobenius element over v. Assuming a fixed embedding $\bar{k} \hookrightarrow \bar{k}_v$, the inertia subgroup at v is denoted by I_v. For a rational prime ℓ, we denote the ℓ-adic cyclotomic character by χ_ℓ. In particular, if $F/\mathbb{Q}_\ell$ is an extension, $F(\chi_\ell)$ is the $F[G_k]$-module affording the cyclotomic character.

If X is a scheme over a field k and K/k is an extension, we denote by X_K the extension of scalars $X \times_{\mathrm{Spec}\, k} \mathrm{Spec}\, K$. For an abelian variety A defined over a field k, $\mathrm{End}(A)$ denotes the ring of endomorphisms of A that are defined over k, and we let $\mathrm{End}^0(A) := \mathrm{End}(A) \otimes \mathbb{Q}$ be the endomorphism algebra of A. Hence, if K/k is an extension, we write $\mathrm{End}(A_K)$ and $\mathrm{End}^0(A_K)$ to denote the ring and algebra of endomorphisms that are defined over K. If k is a number field and A is an abelian variety over k, we denote by S_A the finite set of primes of bad reduction for A, and by Σ_A the set of primes of good reduction.

Introduction

This thesis concerns the arithmetic properties of abelian varieties in relation to their endomorphism algebras. Specifically, given some abelian variety A over a number field k, we study its reductions modulo good primes, as well as the shape of the representations given by the action of Galois on the Tate module of A. We consider these aspects especially in the presence of noncommutative endomorphisms. We also explore connections to modularity.

Several of the main results and expectations on the arithmetic of abelian varieties require some restriction on the endomorphism algebra. To name some, we find the theory of complex multiplication, Serre's open image theorem (and the closely related Mumford–Tate conjecture), and the modularity theorems for elliptic curves and abelian varieties of GL_2-type. This sort of result usually employs one of the following hypotheses:

(1) $\mathrm{End}(A) \otimes \mathbb{Q}$ is a CM field of degree $2 \dim A$.
(2) $\mathrm{End}(A) \otimes \mathbb{Q}$ is a field of degree $\dim A$.
(3) $\mathrm{End}(A_{\bar{k}}) = \mathbb{Z}$.
(4) $\mathrm{End}(A) = \mathrm{End}(A_{\bar{k}})$.

Here and in the rest of the thesis, $\mathrm{End}(A)$ denotes the ring of endomorphisms of A that are defined over its base field, and we let $\mathrm{End}^0(A) := \mathrm{End}(A) \otimes \mathbb{Q}$ be the endomorphism algebra of A. An abelian variety satisfying (1) is usually said to have complex multiplication, while (2) corresponds to abelian varieties of GL_2-type. All of these conditions are imposed to control the image of the Galois representation given by the (rational) ℓ-adic Tate module of A. For each rational prime ℓ, this module is defined as the projective limit

$$V_\ell(A) := \varprojlim_n A[\ell^n] \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

The absolute Galois group $G_k = \mathrm{Gal}(\bar{k}/k)$ acts on $V_\ell(A)$, and we have $V_\ell(A) \simeq \mathbb{Q}_\ell^{2 \dim A}$ as $\mathbb{Q}_\ell$-vector spaces. Moreover, after fixing a polarization for A, we have the G_k-equivariant, alternating, nondegenerate Weil pairing

$$\psi_\ell : V_\ell(A) \times V_\ell(A) \to \mathbb{Q}_\ell(\chi_\ell).$$

Therefore we obtain a continuous representation $\rho_{A,\ell} : G_k \to \mathrm{GSp}_{2 \dim A}(\mathbb{Q}_\ell)$. A famous theorem of Faltings gives further information on the image of this representation: for every finite extension K/k, we have

$$\mathrm{End}^0(A_K) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \simeq \mathrm{End}_{G_K}(V_\ell(A)). \tag{0.1}$$

After this isomorphism, we see that conditions (3) and (4) above are imposed to ensure that the image of the representation $\rho_{A,\ell}$ does not change substantially upon restriction to a finite index subgroup of G_k. When the endomorphism ring $\mathrm{End}(A)$

is strictly larger than $\mathbb{Z}$, by (0.1) the representation $\rho_{A,\ell}$ cannot be absolutely irreducible, and the module $V_\ell(A)$ must be decomposed into irreducible pieces.

We introduce the following terminology to systematize the possible restrictions on the endomorphism algebra $\mathrm{End}^0(A)$.

Definition 0.0.1.

(1) *We say an abelian variety A over a field k is* of GL_n-type *if there exists a number field E with $[E:\mathbb{Q}] = 2\dim A/n$ and an embedding of $\mathbb{Q}$-algebras $E \to \mathrm{End}^0(A)$.*[1]

(2) *We say A is* genuinely of GL_n-type *if A is simple, of GL_n-type, and $A_{\bar{k}}$ has no isogeny factor of GL_m-type with $m < n$.*

For example, suppose that A has complex multiplication, i.e. $E = \mathrm{End}^0(A)$ is a CM field of degree $2\dim A$. Then $V_\ell(A)$ is a free $E \otimes \mathbb{Q}_\ell$-module of rank 1. By considering all primes $\mathfrak{L}$ of E over ℓ, we have the decomposition $E \otimes \mathbb{Q}_\ell \simeq \prod_{\mathfrak{L}|\ell} E_{\mathfrak{L}}$, and consequently a decomposition of $E \otimes \mathbb{Q}_\ell[G_k]$-modules

$$V_\ell(A) = \bigoplus_{\mathfrak{L}|\ell} V_{\mathfrak{L}}(A),$$

with each $V_{\mathfrak{L}}(A)$ an $E_{\mathfrak{L}}$-vector space of dimension 1. Considering the Galois action we obtain a representation $\rho_{A,\mathfrak{L}} : G_k \to E_{\mathfrak{L}}^\times$ for each $\mathfrak{L}$. Since $E_{\mathfrak{L}}^\times = \mathrm{GL}_1(E_{\mathfrak{L}})$, it makes sense that A is called of GL_1-type.

If we move on to GL_2-type, we have a similar pattern. Suppose there is a number field E of degree $[E:\mathbb{Q}] = \dim A$ embedding into $\mathrm{End}^0(A)$, so that A is of GL_2-type. Then for every prime $\mathfrak{L}$ of E over ℓ there is a Galois representation $\rho_{A,\mathfrak{L}} : G_k \to \mathrm{GL}_2(E_{\mathfrak{L}})$, which corresponds to a 2-dimensional piece $V_{\mathfrak{L}}(A)$ of $V_\ell(A)$. From the perspective of representation theory, these are some of the first nonabelian representations of G_k one encounters.

Abelian varieties of GL_2-type over $\mathbb{Q}$ originally appeared as quotients of the Jacobians $J_0(N)$ and $J_1(N)$ of modular curves. This is sometimes known as the Eichler–Shimura relation (see [**DS05**, Chapter 8] for an exposition). In [**Rib04**, §4], Ribet showed that every abelian variety of GL_2-type over $\mathbb{Q}$ appears in this way up to isogeny, using Serre's modularity conjecture. After the proof of this conjecture by Khare and Wintenberger [**KW09a, KW09b**], we have the following parametrisation.

Theorem 0.0.2 (Eichler–Shimura, Ribet, Khare–Wintenberger)**.** *Let N be a positive integer. There is a bijection between the following sets:*

(1) *Isogeny classes of simple abelian varieties $A/\mathbb{Q}$, of GL_2-type and conductor N.*

(2) *Normalized classical modular eigen newforms $f \in S_2^{new}(\Gamma_1(N))$, up to Galois conjugation.*

The bijection is such that, if a modular eigenform f corresponds to the variety A_f, and we let $E_f = \mathrm{End}^0(A_f) = \mathbb{Q}(\{a_p(f)\}_{p\nmid N})$, then

$$L(A_f, s) = \prod_{\sigma : E_f \to \mathbb{C}} L({}^\sigma f, s).$$

[1] For us, an embedding of (associative, unital) algebras is an injective ring homomorphism sending $1 \mapsto 1$.

We remark that there is an important difference between Theorem 0.0.2 and the modularity theorem for elliptic curves (cf. [**Wil95, TW95, BCDT01**]). Every elliptic curve corresponds to some eigenform f which is modular for the group $\Gamma_0(N)$. If we restrict to abelian varieties A_f such that $f \in S_2(\Gamma_0(N))$, then necessarily $E_f = \mathrm{End}^0(A_f)$ is a totally real number field. To allow for coefficients that are not totally real, we need to allow f to have nontrivial Nebentype, thus requiring f to have level $\Gamma_1(N)$ (see [**DS05**] for more details).

The Nebentype is also present in the Tate modules attached to A, as was shown in [**Rib04**]. We have the following result, describing the endomorphism algebra over $\mathbb{Q}$ and $\bar{\mathbb{Q}}$, as well as the representations $\rho_{A,\mathfrak{L}}$.

Theorem 0.0.3 (Ribet)**.** *Let $A/\mathbb{Q}$ be a simple abelian variety genuinely of GL_2-type. Let E be a subfield of $\mathrm{End}^0(A)$ with $[E:\mathbb{Q}] = \dim A$. Then:*

1. *A is geometrically isotypical: there exists some simple abelian variety $B/\bar{\mathbb{Q}}$ of GL_2-type and not of GL_1-type, such that $A_{\bar{\mathbb{Q}}} \sim B^r$ for some r.*
2. *$E = \mathrm{End}^0(A)$, and $\mathrm{End}^0(B)$ is either a totally real field, or an indefinite quaternion algebra over a totally real field.*
3. *For every rational prime ℓ and every prime $\mathfrak{L}$ of E above ℓ, there is a continuous absolutely irreducible representation*

$$\rho_{A,\mathfrak{L}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(E_{\mathfrak{L}}),$$

such that $\rho_{A,\ell} \simeq \bigoplus_{\mathfrak{L}|\ell} \mathrm{Res}_{E_{\mathfrak{L}}/\mathbb{Q}_\ell} \rho_{A,\mathfrak{L}}$. The representations $\{\rho_{A,\mathfrak{L}}\}_{\mathfrak{L}}$ form a strictly compatible system of E-rational representations. Moreover, there exists an odd character $\varepsilon : G_{\mathbb{Q}} \to \bar{\mathbb{Q}}^\times$ of finite order, independent of $\mathfrak{L}$, such that $\det \rho_{A,\mathfrak{L}} = \varepsilon\chi_\ell$. Here χ_ℓ denotes the cyclotomic character.

4. *Let F be the center of $\mathrm{End}^0(B)$. If we let N be the conductor of A, then for every prime $\mathfrak{L} \mid \ell$ of E,*

$$E = \mathbb{Q}(\{\mathrm{Tr}(\rho_{A,\mathfrak{L}}(\mathrm{Frob}_p))\}_{p\nmid \ell N}), \qquad \text{and}$$
$$F = \mathbb{Q}\left(\left\{\frac{\mathrm{Tr}(\rho_{A,\mathfrak{L}}(\mathrm{Frob}_p))^2}{\varepsilon(\mathrm{Frob}_p)}\right\}_{p\nmid \ell N}\right)$$

Going back to the modularity theorem, let $f \in S_2(N)$ be a classical eigenform and let $A_f/\mathbb{Q}$ be the corresponding abelian variety. If A_f is genuinely of GL_2-type, then by Theorem 0.0.3 we know that $A_{f,\bar{\mathbb{Q}}} \sim B^r$ for some simple abelian variety $B/\bar{\mathbb{Q}}$ of GL_2-type, and $\mathrm{End}^0(B)$ is either a totally real field or a totally indefinite quaternion algebra over a totally real field. The variety B is called the *building block* associated to A [**Pyl04**].

If our base field k is larger than $\mathbb{Q}$, a GL_2-type abelian variety A can have a noncommutative endomorphism algebra. Given an abelian surface A/k of GL_2-type, we say A has quaternionic multiplication (QM for short) if $\mathrm{End}^0(A)$ is an indefinite quaternion algebra.[2] In this case we know that the factors in the Euler product of the L-function $L(A,s)$ are all squares. This is a consequence of Honda–Tate theory, but in fact we can say more.

We let Σ_A be the set of primes of k of good reduction for A, and denote by A_v the reduction of A modulo a prime $v \in \Sigma_A$.

[2]If A is genuinely of GL_2-type, then it cannot have QM by a definite quaternion algebra.

Theorem 0.0.4 (Morita, Yoshida, Ohta)**.** *Let A be a simple abelian surface over a number field k. Suppose that $D = \mathrm{End}^0(A)$ is a noncommutative division algebra. Let $\mathrm{Ram}(D)$ be the set of rational primes ℓ such that $D \otimes \mathbb{Q}_\ell$ is a division algebra.*

(1) Let $v \in \Sigma_A$ be a prime with residue characteristic p, and suppose D splits at p. Then A_v is isogenous to the square of an elliptic curve. In particular, A splits modulo all but finitely many primes.

(2) For every prime $\ell \notin \mathrm{Ram}(D)$, there exists an absolutely irreducible continuous representation $\sigma_{A,\ell} : G_k \to \mathrm{GL}_2(\mathbb{Q}_\ell)$ such that

$$\rho_{A,\ell} \simeq \sigma_{A,\ell} \oplus \sigma_{A,\ell}.$$

(3) If $\ell \in \mathrm{Ram}(D)$, then there is a representation

$$\sigma_{A,\ell} : G_k \to (D \otimes \mathbb{Q}_\ell)^\times$$

which is compatible with the representations at split primes in the following sense. Let ℓ' be a prime at which D splits. For almost all primes v of G_k, the reduced trace and norm of $\sigma_{A,\ell}(\mathrm{Frob}_v)$ coincide with the trace and determinant of $\sigma_{A,\ell'}(\mathrm{Frob}_v)$, respectively.

Because of Theorem 0.0.4, abelian surfaces with QM are sometimes called fake elliptic curves. The $\mathbb{Q}_\ell$ coefficients in the representation $\sigma_{A,\ell}$ for non-ramified ℓ might seem surprising: in the definition of the submodules $V_{\mathfrak{L}}(A)$ above, we had chosen a maximal subfield $E \subset D$, which in this case would be quadratic. But choosing such a subfield is arbitrary (there are infinitely many of them inside of D), and it is more natural to use the idempotents in the algebra $D \otimes \mathbb{Q}_\ell \simeq \mathrm{M}_2(\mathbb{Q}_\ell)$ to decompose $V_\ell(A)$ into 2-dimensional submodules.

Going beyond GL_2-types, the first variety we find not treated by these considerations is an abelian surface A defined over $\mathbb{Q}$ and such that $\mathrm{End}^0(A) = \mathbb{Q}$, and more generally abelian varieties of GL_4-type. The surface A is of GL_4-type, and it has a system of Galois representations

$$\rho_{A,\ell} : G_{\mathbb{Q}} \to \mathrm{GSp}_4(\mathbb{Q}_\ell). \tag{0.2}$$

The Langlands philosophy says that $\rho_{A,\ell}$ (or at least the associated L-function $L(A,s)$) should come from an automorphic object, just as we had in Theorem 0.0.2. Brumer and Kramer [**BK14**] proposed a precise modularity conjecture involving Siegel modular forms of genus 2 and paramodular level. We briefly recall their definition, which parallels that of classical modular forms, and refer the reader to [**PY15**] and [**JLRS23**, Part II] for further details. The Siegel upper half-space of genus 2 is defined to be the set of complex symmetric 2-by-2 matrices with positive definite imaginary part,

$$\mathcal{H}_2 := \{Z \in \mathrm{M}_2(\mathbb{C}) \mid Z^\top = Z,\, \mathrm{Im}(Z) > 0\}.$$

This is a 3-dimensional complex manifold. Let $\mathrm{Sp}_4(\mathbb{R})$ be the symplectic group of 4-by-4 real matrices preserving a fixed alternating form. This group acts on $\mathcal{H}_2$ by matrix Möbius transformations

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \cdot Z \mapsto (AZ + B)(CZ + D)^{-1}.$$

For every positive integer N, our substitute for the classical $\Gamma_0(N)$ is the paramodular group

$$K(N) = \begin{pmatrix} * & N* & * & * \\ * & * & * & */N \\ * & N* & * & * \\ N* & N* & N* & * \end{pmatrix} \cap \mathrm{Sp}_4(\mathbb{Q}),$$

where each $* \in \mathbb{Z}$. A Siegel modular form of weight 2 and paramodular level N is an holomorphic map $f : \mathcal{H}_2 \to \mathbb{C}$ satisfying $f(M \cdot Z) = \det(CZ + D)^{-2} f(Z)$ for all $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in K(N)$. We denote the vector space of such forms by $S_2(K(N))$. There is a theory of Hecke operators on this space, leading to the notion of eigenforms. The Paramodular Conjecture of Brumer and Kramer can be stated as follows.

Conjecture 0.0.5 (Paramodularity, first version)**.** *For every abelian surface A defined over $\mathbb{Q}$ with $\mathrm{End}^0(A) = \mathbb{Q}$ and conductor N, there exists a Siegel paramodular eigenform $f \in S_2(K(N))$ such that*

$$L(A, s) = L(f, s).$$

We say an abelian surface A satisfying Conjecture 0.0.5 is paramodular. The converse direction of this conjecture is known to be false. The first reason why is that there is a lift from Jacobi forms into Siegel paramodular forms $\mathrm{Grit} : J^{cusp}_{2,N} \to S_2(K(N))$, known as the Gritsenko lift, and L-functions of forms which are Gritsenko lifts cannot correspond to abelian varieties (cf. the introduction of [**BK14**]). But even if we disregard these lifts, there is yet another class of abelian varieties with representations in the same shape as (0.2). Much in the same way that QM abelian surfaces have 2-dimensional representations (cf. Theorem 0.0.4), we obtain 4-dimensional representations from QM fourfolds. The precise statement comes from [**Chi90**].

Theorem 0.0.6 (Chi)**.** *Let A/k be a simple abelian fourfold such that $D = \mathrm{End}^0(A)$ is an indefinite quaternion algebra with center $\mathbb{Q}$. Then for every prime $\ell \notin \mathrm{Ram}(D)$ there exists a continuous, absolutely irreducible representation*

$$\sigma_{A,\ell} : G_k \to \mathrm{GSp}_4(\mathbb{Q}_\ell)$$

with $\mathrm{sim} \circ \sigma_{A,\ell} = \chi_\ell$ such that $\rho_{A,\ell} \simeq \sigma_{A,\ell} \oplus \sigma_{A,\ell}$.

The fact that the image of $\sigma_{A,\ell}$ lands in a symplectic group (and not just in $\mathrm{GL}_4(\mathbb{Q}_\ell)$) is nontrivial: one needs to find a decomposition of $\mathbb{Q}_\ell[G_k]$-modules $V_\ell(A) \simeq X \oplus Y$, in such a way that the Weil pairing ψ_ℓ on $V_\ell(A)$ restricts to nondegenerate pairings on X and Y. This theorem of Chi holds more generally for any dimension of A, under the assumption that $D = \mathrm{End}^0(A)$ is a totally indefinite quaternion algebra over a totally real field. Banaszak, Gajda, Krasoń and Kaim-Garnek have generalized the pairing construction to allow $\mathrm{End}^0(A)$ to have any Albert type [**BGK06, BGK10, BKG21**].

Calegari et al. [**BCGP21**] were the first to observe that QM abelian fourfolds may well exist over $\mathbb{Q}$, and so Conjecture 0.0.5 should be adapted accordingly. The updated Paramodularity conjecture for Siegel paramodular forms with rational eigenvalues is as follows (cf. [**BK19**, Conjecture]).

Conjecture 0.0.7 (Paramodularity conjecture, updated version)**.** *Let N be a positive integer. Let $\mathcal{A}_N$ be the set of isogeny classes of abelian surfaces defined over $\mathbb{Q}$ with $\mathrm{End}^0(A) = \mathbb{Q}$ and conductor N. Let $\mathcal{B}_N$ be the set of isogeny classes of simple abelian fourfolds over $\mathbb{Q}$ with $\mathrm{End}^0(A)$ an indefinite quaternion algebra with center $\mathbb{Q}$ and conductor N^2. Let $\mathcal{P}_N$ be the set of eigenforms $f \in S_2(K(N))$ with rational Hecke eigenvalues, modulo scalars, which are not Gritsenko lifts. There is a bijection $\mathcal{P}_N \leftrightarrow \mathcal{A}_N \cup \mathcal{B}_N$ such that, if $f \in \mathcal{P}_N$ and A_f is the corresponding abelian variety,*

$$L(A_f, s) = \begin{cases} L(f,s), & \text{if } A_f \in \mathcal{A}_N, \\ L(f,s)^2, & \text{if } A_f \in \mathcal{B}_N. \end{cases}$$

The biggest hurdle towards establishing this conjecture is that there cannot be an Eichler–Shimura construction realizing the abelian variety A_f corresponding to some paramodular form f. In particular, we do not know how to predict whether $A_f \in \mathcal{A}_N$ or $A_f \in \mathcal{B}_N$ in terms of f.

By means of techniques for comparison of Galois representations and modularity lifting theorems, many cases of Conjecture 0.0.5 are now known. In [**BCGP21**], it was shown that infinitely many abelian surfaces are paramodular. Some abelian surfaces of small conductor have been shown to be paramodular (cf. [**BPP$^+$19, BK20**]). Some explicit paramodular surfaces were also found in [**CCG20**]. The recent preprint [**BCGP25**] shows paramodularity of many abelian surfaces, by imposing local conditions at 2 and 3.

In [**BK14**, Conjecture 1.4], Brumer and Kramer already give a more general conjecture for an abelian variety A of GL_4-type such that $\mathrm{End}^0(A)$ is a totally real field of degree $\dim A/2$. This conjecture is probably incomplete, as it does not include varieties with QM by a totally indefinite quaternion algebra. On the other hand, these conjectures do not cover every possible abelian variety of GL_4-type over $\mathbb{Q}$. We will aim to classify these in order to make the picture clearer.

0.1. Main results

A substantial portion of this thesis aims to generalize Theorems 0.0.3, 0.0.4 and 0.0.6 for abelian varieties genuinely of GL_n-type with arbitrary n.

0.1.1. Embeddings of simple algebras. Given a simple abelian variety A defined over a number field k, the endomorphism algebra $\mathrm{End}^0(A)$ is a division algebra. To study it, we can relate it to several other algebras, given by base changes of A. On the one hand, we may consider a field extension K/k, so that we obtain an embedding $\mathrm{End}^0(A) \to \mathrm{End}^0(A_K)$. On the other, we may take a prime v of good reduction for A, and consider the injection into the endomorphisms of the reduction, $\mathrm{End}^0(A) \to \mathrm{End}^0(A_v)$. A third base change operation (which we will not consider) would be taking specializations of an abelian scheme $\mathcal{X} \to S$ over some base scheme S.

Since we see embeddings of semisimple algebras so often, it makes sense to study them in general first. Let Q be a perfect field. Suppose that Y is a simple Q-algebra and that X is a simple Q-subalgebra of Y. Let Z_X and Z_Y be the respective centers of X and Y. If $Z_Y \subseteq Z_X$, then the Double Centralizer theorem [**Pie82**, Theorem 12.7] relates the dimensions of X, Y, and the centralizer of X in Y. It also gives a certain relation between the Brauer classes of these three algebras, in

particular, the centralizer has the same Brauer class as $X \otimes Y^{op}$, where Y^{op} is the opposite algebra of Y.

In [**Yu12**], Chia-Fu Yu gives a general criterion to characterize when a simple algebra X embeds into another simple algebra Y. The criterion uses invariants of X, Y and $X \otimes Y^{op}$, and as such it can be seen as both a generalization and a converse of the Double Centralizer theorem, especially when we do not have the inclusion $Z_Y \subseteq Z_X$.

Since we will only encounter algebras over number fields, we will prove a criterion (equivalent to Yu's) that gives us a stronger relation between X and Y. Essentially, it says that X embeds into Y if and only if a dimension condition holds, and X and Y have similar Brauer classes.

Theorem 0.1.1 (Adapted from Theorem 2.3.2)**.** *Let Q be a global or a local field, let Z_X and Z_Y be finite extensions of Q, and let X,Y be simple Q-algebras with respective centers Z_X and Z_Y. Let $Y \simeq \mathrm{M}_r(Y')$, with Y' a division algebra. Consider the product of fields*

$$Z_X \otimes_Q Z_Y \simeq F_1 \times \cdots \times F_s.$$

There exists an embedding of Q-algebras $\iota : X \to Y$ if and only if there exist non-negative integers $r_1, \ldots, r_s$ with

(1) $\sum_{i=1}^{s} r_i = r$, and

(2) If $r_i > 0$, then the quantity $d_i = \frac{r_i \sqrt{\dim_{Z_Y} Y}}{[F_i : Z_Y]\sqrt{\dim_{Z_X} X}}$ is an integer, and we have

$$d_i[X \otimes_{Z_X} F_i] = d_i[Y \otimes_{Z_Y} F_i].$$

Many results throughout the thesis use the theorem above in some form.

0.1.2. Split and simple reductions. As stated in Theorem 0.0.4, an abelian surface with quaternionic multiplication splits modulo all but finitely many primes. Based on this phenomenon, Murty and Patankar proposed the following conjecture [**MP08**].

Conjecture 0.1.2 (Murty–Patankar, as stated in [**Zyw14**])**.** *Let A be an abelian variety over a number field k. Let $\mathcal{V}$ be the set of primes of good, simple reduction for A. Then, after possibly replacing k by a finite extension, the density of $\mathcal{V}$ exists and is equal to 1 if and only if $\mathrm{End}^0(A_{\bar{k}})$ is commutative.*

This conjecture has been shown to be true in many cases [**Ach09, Ach12**], and holds for all abelian varieties satisfying the Mumford–Tate conjecture [**Zyw14**]. The result is in fact easy to show in the case where $\mathrm{End}^0(A)$ is noncommutative, using a result of Waterhouse [**Wat69**, Theorem 6.1]. We prove a strengthening of this fact.

Theorem 3.5.2. *Let A/k be a simple abelian variety such that $D = \mathrm{End}^0(A)$ is noncommutative. If A_v is simple for some v over a rational prime p, then D ramifies at some prime over p. In particular, A splits modulo all but finitely many primes.*

This result prompts two follow-up questions. First, what are the possible good reductions of an abelian variety with noncommutative endomorphism algebra? And second, does there exist an abelian variety A over some number field k, such that A_v is (geometrically) simple modulo some good prime v?

For abelian surfaces with QM, the first question has been answered in [**Jor86**, §2] and [**Yu13b**]. We give some results for arbitrary dimension, and classify all QM abelian fourfolds over finite fields. Regarding the second question, we display an abelian fourfold having exactly two primes of good, geometrically simple reduction.

0.1.3. Galois representations. Given a simple abelian variety A/k of GL_n-type, we wish to precisely describe the system of representations $\rho_{A,\mathfrak{L}} : G_k \to \mathrm{GL}_n(E_{\mathfrak{L}})$. At least when the field k is totally real and $n = 2$, the answer is essentially a combination of Theorems 0.0.3 and 0.0.4 (the extension to k totally real follows from adapting the arguments in Pyle's thesis, cf. [**Pyl04**]). However, the subject is not so easy when we let $n > 2$, as the group GL_n is quite large, and $\rho_{A,\mathfrak{L}}$ will usually have some self-duality property coming from the Weil pairing. In this sense, the notion of GL_n-*type* is too coarse, though we maintain it for convenience.

As we had in the GL_2-type case for quaternionic multiplication, choosing a maximal field $E \subseteq \mathrm{End}^0(A)$ is somewhat arbitrary. To avoid this choice, we work with representations with noncommutative coefficients. Given a positive integer m and a simple algebra D, recall that the algebraic group $\mathbf{GL}_m(D)$ represents the functor $\mathrm{Alg} \to \mathrm{Grp}$ given by $A \mapsto (\mathrm{M}_m(D \otimes A))^\times$. We have the following result.

Theorem 0.1.3 (Theorem 4.2.7, Proposition 5.1.3, Proposition 5.4.3)**.** *Let A be a simple abelian variety defined over a number field k. Let $D = \mathrm{End}^0(A)$, H the center of D, t_A the Schur index of D, and $n := \frac{2\dim A}{t_A[H:\mathbb{Q}]}$. Let S_A be the set of primes of k of bad reduction for A, and let $\mathrm{Ram}(D)$ be the set of primes of H at which D ramifies.*

1. *The number n is the smallest integer such that A is of GL_n-type. The Schur index t_A divides n.*
2. *The variety A has an associated strictly compatible system $\{\rho_{A,\lambda}\}_{\lambda \subset H}$ of H-rational λ-adic representations with values in $\mathbf{GL}_{n/t_A}(D^{op})$, with exceptional set S_A.*
3. *Fix any prime λ of H. The center H is generated over $\mathbb{Q}$ by the traces of $\rho_{A,\lambda}(\mathrm{Frob}_v)$, for v outside of S_A and coprime with λ.*
4. *For every $\lambda \notin \mathrm{Ram}(D)$, the representation $\rho_{A,\lambda}$ takes values in $\mathrm{GL}_n(H_\lambda)$ and is absolutely irreducible.*
5. *If ℓ is a rational prime such that $\lambda \notin \mathrm{Ram}(D)$ for every $\lambda \mid \ell$, then we have a decomposition*

$$\rho_{A,\ell} \simeq \bigoplus_{\lambda|\ell} \mathrm{Res}_{H_\lambda/\mathbb{Q}_\ell} \rho_{A,\lambda}^{\oplus t_A}.$$

In addition, if we fix $E \subseteq D$ a maximal subfield such that E/H is Galois, a prime λ of H, and a prime $\mathfrak{L}$ of E over λ, then we have $\rho_{A,\mathfrak{L}} \simeq \rho_{A,\lambda} \otimes_{H_\lambda} E_{\mathfrak{L}}$.

Given a simple abelian variety A of GL_n-type and a prime $\lambda \notin \mathrm{Ram}(\mathrm{End}^0(A))$ of the center H, we let $W_\lambda(A)$ be the absolutely irreducible $H_\lambda[G_k]$-module realizing the representation $\rho_{A,\lambda}$.

Next, we give the precise self-duality condition and Nebentype of the system above under two natural hypotheses. First, we assume that A is *genuinely of* GL_n-*type*. This implies in particular that $A_{\bar{k}} \sim B^r$, with $B/\bar{k}$ a simple abelian variety of GL_n-type (we call B the building block associated to A).

If one follows the arguments leading to Theorem 0.0.3, it becomes apparent that they essentially follow from the fact that the center F of the endomorphism algebra of the building block is totally real (a property implied by $k = \mathbb{Q}$ and $n = 2$). Hence we make the following definition.

Definition 0.1.4. *Let A be genuinely of GL_n-type with associated building block B. We say A is* geometrically of the first kind *if the center F of $\mathrm{End}^0(B)$ is a totally real field.*

It can be shown that, if A is genuinely of GL_n-type and geometrically of the first kind, then n is necessarily even. Abelian varieties geometrically of the first kind are characterized by the following property.

Theorem 0.1.5 (Proposition 5.5.12, Theorem 5.6.4, Theorem 5.7.4)**.** *Let A/k be an abelian variety genuinely of GL_n-type and let B be its associated building block. Let H be the center of $D = \mathrm{End}^0(A)$, and let F be the center of $\mathrm{End}^0(B)$. The following are equivalent:*

(1) A is geometrically of the first kind.
(2) There exists a finite order character $\varepsilon : G_k \to \bar{\mathbb{Q}}^\times$, called the Nebentype of *A, and a set T of primes of H of density one, with the following property. For every $\lambda \in T$ there exists a nondegenerate H_λ-bilinear, G_k-equivariant pairing*

$$\psi_\lambda : W_\lambda(A) \times W_\lambda(A) \to H_\lambda(\varepsilon\chi_\ell).$$

Suppose that these hold. Then:

(i) The set T is the complement of $\mathrm{Ram}(D)$. Moreover, for each $\lambda \in T$, the pairing ψ_λ on $W_\lambda(A)$ is unique up to scalars.
(ii) The pairings ψ_λ are alternating if $\mathrm{End}^0(B)$ has Albert type I or II, and symmetric if $\mathrm{End}^0(B)$ has Albert type III.
(iii) Fix a prime λ of H. The center F of $\mathrm{End}^0(B)$ is generated over $\mathbb{Q}$ by the elements $\mathrm{Tr}(\rho_{A,\lambda}(\mathrm{Frob}_v))^2/\varepsilon(\mathrm{Frob}_v)$, for v outside of a finite set.

Corollary 0.1.6 (Corollary 5.7.6)**.** *Suppose that A is genuinely of GL_n-type and geometrically of the first kind. Let B be the building block associated to A. Then the following holds:*

(i) If B has Albert type I or II, then for all but finitely many λ the representation $\rho_{A,\lambda}$ takes values in $\mathrm{GSp}_n(H_\lambda)$.
(ii) If B has Albert type III, then for all but finitely many λ the representation $\rho_{A,\lambda}$ takes values in $\mathrm{GO}_n(H_\lambda)$.

We say an abelian variety A is *genuinely of GSp_n-type* if it falls in Case (i) of Corollary 0.1.6, and *genuinely of GO_n-type* if it falls in Case (ii). We provide families of examples of abelian fourfolds genuinely of GSp_4-type, both with trivial and nontrivial Nebentype. These results are based on joint work with Francesc Fité and Xavier Guitart [**FFG24**].

Beyond varieties genuinely of GL_n-type, we also consider abelian varieties of GL_r-type such that A_L is isotypical over some extension L/k, but possibly of GL_n-type over L, $n < r$.

Theorem 0.1.7 (Adapted from Theorem 7.2.1)**.** *Let A/k be a simple abelian variety, and let L/k be a finite Galois extension such that A_L is isotypical. Let H' be the center of $\mathrm{End}^0(A_L)$. Let H'_0 be the fixed subfield of H' with respect to the*

action of $\mathrm{Gal}(L/k)$ *on* H' *(cf. Proposition 7.1.3). Suppose* A_L *is of* GL_n*-type and let* $m = n \cdot [H' : H'_0]$*. For every prime* λ *of* H' *not in* $\mathrm{Ram}(\mathrm{End}^0(A_L))$*, there exist:*

(1) A finite order character $\xi : G_L \to (\bar{H}'_\lambda)^\times$*, and*
(2) An absolutely irreducible representation $R_{A,\lambda} : G_k \to \mathrm{GL}_m(\bar{H}'_\lambda)$*,*

such that $R_{A,\lambda}|G_L$ *admits* $\rho_{A_L,\lambda} \otimes \xi$ *as an irreducible constituent.*

The result above holds more generally for weak abelian k-varieties. If L/k is a Galois extension, we say an abelian variety A/L is a weak k-variety if A is isogenous to ${}^sA$ for all $s \in \mathrm{Gal}(L/k)$. In some cases, we also give some results that ensure that the representation $R_{A,\lambda}$ preserves a nondegenerate pairing. These results are part of joint work with Ariel Pacetti [**FP24**].

0.1.4. Siegel-modular abelian varieties. In [**BK14**, Conjecture 1.4], Brumer and Kramer proposed a generalization of Conjecture 0.0.7 for nonlift Siegel paramodular forms with coefficients in a field of degree > 1. One would like to further extend the conjecture to all abelian varieties genuinely of GSp_4-type, including those with nontrivial Nebentypes.

There is a difference with the classical picture: for a positive integer N, the quotient $\Gamma_0(N)/\Gamma_1(N)$ is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^\times$, and so we can have characters of $\Gamma_0(N)$ of many orders. The paramodular group $K(N)$, however, does not enjoy this property. Its abelianization is always a subgroup of $(\mathbb{Z}/12\mathbb{Z})^2$ [**DM02**], and so we are limited in the characters that are possible.

Let π be a cuspidal automorphic representation of $\mathrm{GSp}_4(\mathbb{A}_\mathbb{Q})$ of weight $(2,2)$, and let E be its coefficient field. As explained in [**Wei22**, Theorem 3.3], if π is not CAP or endoscopic then there exists a compatible system of Galois representations $\{\rho_{A,\ell} : G_\mathbb{Q} \to \mathrm{GSp}_4(\bar{E}_\lambda)\}_\lambda$. We say an abelian variety $A/\mathbb{Q}$ is *Siegel-modular* if its associated system of Galois representations is isomorphic (up to extension of scalars) to the system attached to π. This allows us to consider a representation π with arbitrary central character, corresponding to a Dirichlet character acting as the Nebentype.

We will not focus here on finding the substitute level for the paramodular group, instead, we look at the problem of describing the endomorphisms of A in terms of the corresponding automorphic representation π.

Theorem 5.8.1. *Let* π *be a cuspidal automorphic representation of* $\mathrm{GSp}_4(\mathbb{A}_\mathbb{Q})$ *of weight* $(2,2)$ *which is not CAP or endoscopic. Suppose that* $A/\mathbb{Q}$ *is an abelian variety genuinely of* GL_4*-type that is Siegel-modular and corresponds to* π*. Let* B *be the building block associated to* A*. Then:*

(1) A is geometrically of the first kind, and $\mathrm{End}^0(B)$ *is either a totally real field or a totally indefinite quaternion algebra over a totally real field.*
(2) The Nebentypes of π *and* A *coincide, and the centers of* $\mathrm{End}^0(A)$ *and* $\mathrm{End}^0(B)$ *are determined by the Hecke eigenvalues of* π*, as given in Theorems 0.1.3 and 0.1.5.*

In particular, Theorem 5.8.1 discards the possibility that a Siegel-modular abelian fourfold $A/\mathbb{Q}$ has $\mathrm{End}^0(A)$ a definite quaternion algebra, as suggested in [**BCGP21**, §10.4.1].

Using Theorem 0.1.7, we show the modularity of abelian surfaces over $\mathbb{Q}$ with potential quaternionic multiplication. This result is also part of [**FP24**]. Recall

that an order $\mathcal{O}$ of a quaternion algebra D is said to be *hereditary* if every left ideal $I \subset \mathcal{O}$ is projective as a left $\mathcal{O}$-module.

Theorem 0.1.8 (Theorem 7.5.3 and Corollary 7.5.5)**.** *Let $A/\mathbb{Q}$ be an abelian surface such that $\mathrm{End}^0(A) = \mathbb{Q}$ and $\mathrm{End}^0(A_{\bar{\mathbb{Q}}})$ is either $\mathrm{M}_2(\mathbb{Q})$, or a division indefinite quaternion algebra with center $\mathbb{Q}$. Then A is Siegel-modular.*

If in addition $\mathrm{End}(A_{\bar{\mathbb{Q}}})$ is a hereditary quaternion order and A admits a principal polarization, then A is paramodular.

0.2. Chapter organization

The thesis is organized in seven chapters. In Chapter 1 we give an overview of the background for developing the results. We give the basic definitions and results about central simple algebras and Galois cohomology. We also review some definitions on abelian varieties, and we give the Albert classification.

We study embeddings of simple algebras in Chapter 2. This chapter gives a version of Yu's criterion, which plays an important role in Chapters 3, 5 and 7.

Chapter 3 studies the properties of abelian varieties defined over finite fields under the assumption that their endomorphism algebra is noncommutative. The chapter focuses on classifying which abelian fourfolds have a fixed quaternion algebra embedded in their endomorphism algebra. The main result of [**Flo25**] is given (cf. Theorem 3.5.2), and we also explore the primes of good, simple reduction for surfaces and fourfolds with QM.

Chapter 4 begins the description of the ℓ-adic systems of Galois representations associated to abelian varieties with endomorphism ring larger than $\mathbb{Z}$. We give a unified and systematic presentation of the Galois representations with coefficients in the (opposite) endomorphism algebra, together with the Weil pairings on the consitutents of the Tate module. Most of these properties were scattered across different sources (including [**Oht74, Rib76, Del82, Chi91, BGK06, BGK10, BKG21**]).

Chapter 5 is based on joint work with F. Fité and X. Guitart [**FFG24**]. It treats the notion of abelian varieties genuinely of GL_n-type. The property makes the representations of $\mathrm{Gal}(\bar{k}/k)$ from Chapter 4 not only absolutely irreducible, but also absolutely irreducible when restricted to $\mathrm{Gal}(\bar{k}/L)$ for any finite extension L of k. After describing the dimension conditions on the endomorphism algebra of A, we define the notion of building block, taking after the classical GL_2-type theory of Ribet [**Rib76, Rib04**] and Pyle [**Pyl04**]. Assuming A is geometrically of the first kind, we define the inner twists associated with A, and in particular the *Nebentype* of A. Building on Chapter 4, a characterization of abelian varieties with a symplectic or orthogonal Galois representation is given. This enlarges the class of abelian varieties with symplectic or orthogonal Galois representations given in [**BGK06**] and [**BGK10**]. The Nebentype character then coincides with the similitude character of the symplectic or orthogonal Galois representation associated to A. Finally, the chapter characterizes which abelian varieties genuinely of GL_4-type can be Siegel-modular.

Chapter 6 gives the construction of a family of GL_4-type building blocks, which also appeared in [**FFG24**]. For a given quadratic number field k satisfying a certain condition, these are genus 2 curves C/k such that their Jacobians are k-isogenous to their Galois conjugates. By Weil restriction, one obtains $\mathbb{Q}$-simple abelian fourfolds with endomorphism algebra $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{-2})$. The generic fiber of the family of

Jacobians has trivial endomorphism ring. This is the first known instance of a family of GL_4-type $\mathbb{Q}$-surfaces. In the case of multiplication by $\sqrt{-2}$, this gives a family of Galois representations with image in GSp_4 and nontrivial Nebentype.

Chapter 7 is based on joint work with A. Pacetti [**FP24**]. It deals with the Galois representations associated with abelian k-varieties A defined over a number field L with L/k being a Galois extension. One of the key points is not assuming that A has all its endomorphisms defined over the base field L. This allows to treat abelian varieties *potentially of* GL_n*-type*, as opposed to those genuinely of GL_n-type. A recipe is given to attach a representation of minimal dimension R_A of $\mathrm{Gal}(\bar{k}/k)$ to A. Moreover, some results are given to characterize when R_A will preserve a pairing coming from the Weil pairing of A, again derived from the information of Chapter 4. The Siegel-modularity of abelian surfaces $A/\mathbb{Q}$ with potential QM is shown as an application.

CHAPTER 1

Background

In this chapter we introduce some basic definitions and results that will be used throughout the text. In Section 1.1 we review the main results on simple algebras, in particular over global and local fields. We continue in Section 1.2 with Galois cohomology, in particular, we give the cohomological interpretation of the Brauer group. We give the basic definitions on abelian varieties in Section 1.3. In Section 1.4 we state the Albert classification for division algebras with positive involution.

1.1. Central simple algebras

In this section we define simple algebras, and we give three of the fundamental results about them: Wedderburn's theorem, the Skolem–Noether theorem, and the Double Centralizer theorem. We introduce the Brauer group, and we state the main exact sequence relating the Brauer group of a global field with the local Brauer groups. For a short introduction to simple algebras, we refer the reader to [**Mil20**, Chapter IV]. For more thorough treatments, see [**Pie82**] and [**Rei03**].

Throughout the section we let F be a perfect field, and we fix once and for all an algebraic closure $\bar{F}$ of F.

Let X be an associative ring with unit. The subring $Z = \{z \mid zx = xz, \text{ for all } x \in X\}$ is called the *center* of X. We say X is an *F-algebra* if $F \subseteq Z$ and X is finite-dimensional as an F-vector space. We say X is *F-central* if $Z = F$. The left and right ideals of X satisfy the usual definitions. We say an ideal I of X is two-sided if it is a left and a right ideal at the same time. We say X is *simple* if it has no nontrivial two-sided ideals. We say X is a *central simple F-algebra* if X is F-central and simple. When the center is clear from the context, we just say X is a central simple algebra.

Examples of central simple F-algebras are F itself (since a field has no nontrivial ideals) and the matrix ring $\mathrm{M}_n(F)$, for every $n \geq 1$.

Lemma 1.1.1. *The following are equivalent.*

(1) F is the center of X, and X has no nontrivial two-sided ideals.
(2) $X \otimes_F \bar{F} \simeq \mathrm{M}_n(\bar{F})$ for some positive integer n.

We say an algebra X is *semisimple* if it is isomorphic to a product of simple algebras.[1]

We say an algebra X is a division algebra if every nonzero element has a multiplicative inverse. A division algebra is simple; the proof is the same used to show that a field has no nontrivial ideals. The following result states that a simple algebra is isomorphic to a ring of matrices with coefficients in a division algebra.

[1]The usual definition of a semisimple algebra says that every X-module is semisimple, but the two definitions are equivalent.

Theorem 1.1.2 (Wedderburn)**.** *Let X be a simple algebra. There exists some $n \geq 1$ and a division algebra D such that $X \simeq \mathrm{M}_n(D)$.*

In particular, the dimension over F of a central simple F-algebra X is a square, say $n^2 = \dim_F X$. We say n is the *degree* of X. We say X is a *quaternion algebra* if X is an algebra of degree 2.

Given a central simple F-algebra X, its group of F-linear ring automorphisms is denoted by $\mathrm{Aut}_F(X)$. For example, it is well-known that $\mathrm{Aut}_F(\mathrm{M}_n(F)) \simeq \mathrm{PGL}_n(F)$, the n-by-n matrices in F modulo scalars. This is equivalent to saying that every F-automorphism of $\mathrm{M}_n(F)$ is *inner*. More generally, we have the following result (cf. [**Pie82**, §12.6]).

Theorem 1.1.3 (Skolem–Noether)**.** *Let $\psi : X \to X$ be an F-linear automorphism of X. Then there exists some $a \in X^\times$ such that for all $x \in X$, $\psi(x) = axa^{-1}$.*

We now introduce the Brauer group and some properties of Brauer classes (cf. [**Pie82**, 12.5]). Given an algebra X, recall that its *opposite algebra* X^{op} has the same underlying set and addition as X, but the multiplication is reversed: for $x, y \in X^{op}$, we define $x * y := yx$.

We say two central simple algebras X and Y are *Brauer equivalent* if there are integers m and n with $\mathrm{M}_m(X) \simeq \mathrm{M}_n(Y)$. This defines an equivalence relation on the set of all central simple F-algebras. We denote by $[X]$ the *Brauer class* of X. The set of all such classes is denoted by $\mathrm{Br}(F)$. Given central simple F-algebras X and Y, $X \otimes_F Y$ is again simple. In addition, we have the following properties:

(1) For every $n \geq 1$, $X \otimes_F \mathrm{M}_n(F) \simeq \mathrm{M}_n(X)$.
(2) The tensor product (with respect to F) is associative and commutative.
(3) If X is a central simple algebra of degree n, then $X \otimes_F X^{op} \simeq \mathrm{M}_{n^2}(F)$.

Observe that these properties allow us to define a sum operation on $\mathrm{Br}(F)$. Given $[X], [Y] \in \mathrm{Br}(F)$, we define $[X] + [Y] := [X \otimes_F Y]$, and $-[X] := [X^{op}]$. The neutral element is $[F]$, and $\mathrm{Br}(F)$ is thus an abelian group called the *Brauer group*. By the properties of the tensor product, the Brauer group is functorial with respect to field extensions. Given an extension L/F, the map $\mathrm{Br}(F) \to \mathrm{Br}(L)$ given by $[X] \mapsto [X \otimes_F L]$ is a group homomorphism.

We now give another fundamental result on simple algebras. Given a subalgebra X of an algebra Y, we define the *centralizer of X in Y* as

$$C_Y(X) := \{y \in Y \mid yx = xy \text{ for all } x \in X\}.$$

Namely, $C_Y(X)$ is the subalgebra of all elements of Y commuting with X. In particular, the center of X is included in $C_Y(X)$.

Theorem 1.1.4 (Double Centralizer theorem)**.** *Let X and Y be central simple algebras over the fields Z_X and Z_Y, respectively. Suppose that X is a Z_Y-subalgebra of Y (in particular, $Z_Y \subseteq Z_X$). Let $C_Y(X)$ be the centralizer of X in Y.*

(1) $C_Y(X)$ is a central simple algebra over Z_X.
(2) $\dim_{Z_Y} X \cdot \dim_{Z_Y} C_Y(X) = \dim_{Z_Y} Y$.
(3) $C_Y(C_Y(X)) = X$.
(4) $[X \otimes_{Z_X} C_Y(X)] = [Y \otimes_{Z_Y} Z_X]$ in $\mathrm{Br}(Z_X)$.

Proof. Statements (1), (2) and (3) are standard, see e.g. [**Pie82**, Theorem 12.7]. Along the proof of this result, it is shown that the algebras $Y \otimes_{Z_Y} X^{op}$

and $C_Y(X)$ are Brauer equivalent. From the isomorphism $Y \otimes_{Z_Y} X^{op} \simeq (Y \otimes_{Z_Y} Z_X) \otimes_{Z_X} X^{op}$, we obtain the equality

$$[Y \otimes_{Z_Y} Z_X] - [X] = [C_Y(X)]$$

in $\mathrm{Br}(Z_X)$, and statement (4) follows from this. □

We are mainly interested in central simple algebras with center a number field. We now describe the Brauer groups of such fields. To begin, we let F be a local field. If $F = \mathbb{C}$, then F is algebraically closed, and therefore all central simple F-algebras have trivial Brauer class. Hence $\mathrm{Br}(\mathbb{C}) = 0$. For $F = \mathbb{R}$, Frobenius showed that the only nontrivial Brauer class is given by the Hamilton quaternions $\mathcal{H}$ (cf. [**Pie82**, Corollary 13.1c]), and so $\mathrm{Br}(\mathbb{R}) \simeq \frac{1}{2}\mathbb{Z}/\mathbb{Z}$. We will think of these Brauer groups as subgroups of $\mathbb{Q}/\mathbb{Z}$.

If F is a nonarchimedean local field, then there is a canonical isomorphism $\mathrm{inv}_F : \mathrm{Br}(F) \to \mathbb{Q}/\mathbb{Z}$, called the Hasse invariant (cf. [**Pie82**, §17.10]). Note that $[X]$ is the trivial class if and only if $\mathrm{inv}_F[X] = 0$. If L/F is a finite extension, the invariants of X and $X \otimes_F L$ are related by the formula $\mathrm{inv}_L[X \otimes_F L] \equiv [L : F] \cdot \mathrm{inv}_F[X] \pmod{\mathbb{Z}}$.

Let now K be a global field and v a place of K. If we denote by K_v the completion of K along v, we then have a group homomorphism $\mathrm{Br}(K) \to \mathrm{Br}(K_v)$, $[X] \mapsto [X \otimes_K K_v]$. We define the local Hasse invariant at v by $\mathrm{inv}_v[X] := \mathrm{inv}_{K_v}[X \otimes K_v]$. The following result says the local-global principle for the triviality of Brauer classes holds.

Theorem 1.1.5 (Albert–Brauer–Hasse–Noether)**.** *Let K be a global field and let X be a central simple K-algebra. Then $[X] = [K]$ if and only if $[X \otimes_K K_v] = [K_v]$ for every place v of K. Equivalently, two central simple K-algebras X and Y are Brauer equivalent if and only if $\mathrm{inv}_v[X] = \mathrm{inv}_v[Y]$ for every place v of K.*

Theorem 1.1.5 above says that the group homomorphism $\mathrm{Br}(K) \to \bigoplus_v \mathrm{Br}(K_v)$ is injective. The image is given by the elements in $\bigoplus_v \mathrm{Br}(K_v)$ whose Hasse invariants sum to zero.

Theorem 1.1.6. *Let K be a global field. The following sequence is exact:*

$$0 \to \mathrm{Br}(K) \to \bigoplus_v \mathrm{Br}(K_v) \overset{\sum_v \mathrm{inv}_{K_v}}{\to} \mathbb{Q}/\mathbb{Z} \to 0.$$

A proof of this result is given in [**Pie82**, Chapter 18]. Sometimes, one refers informally to this exact sequence as the *parity condition*. For example, if X is a division quaternion algebra over a global field K, then $\mathrm{inv}_v[X] = 0$ or $1/2$ for every place v, and the exactness implies there must be an even number of places v with $\mathrm{inv}_v[X] = 1/2$. Similar conditions can be derived for division algebras of higher degree.

Given a central simple algebra X over a global field K, we say X *ramifies* at a place v if $\mathrm{inv}_v[X] \neq 0$. We denote by $\mathrm{Ram}(X)$ the (finite) set of places v of K at which X ramifies.

1.1.1. Indices and exponents of Brauer classes. For a central simple F-algebra X, we let X' be a central division F-algebra such that $X \simeq \mathrm{M}_c(X')$. We say $c = c_X$ is the *capacity* of X. The *Schur index* of X, denoted by t_X, is defined

to be the degree of the division algebra X'. In particular, the Schur indices of X and X' coincide. We have the equality

$$\dim_F X = (c_X t_X)^2 .$$

Given a central simple F-algebra X, we say a field $E \supseteq F$ is a *splitting field for* X if $[X \otimes_F E] = [E]$. We also say that E *splits* X. The algebraic closure $\bar{F}$ of F always splits X, but we can find smaller splitting fields. We say a field $E \subseteq X$ is a *maximal subfield* if for every $x \in X \setminus E$, the subalgebra of X generated by E and x is no longer a field. Any maximal subfield E of X contains the center F, and we have $\dim_F X = [E : F]^2$. In addition, E is a splitting field for X.[2] These facts amount to saying that, if X is a division F-algebra and t_X is its Schur index, then there exists a maximal subfield $E \subseteq X$ such that $[E : F] = t_X$, and $X \otimes_F E \simeq \mathrm{M}_{t_X}(E)$.

Using Theorem 1.1.5 in combination with the Grunwald–Wang theorem (cf. [**Pie82**, §18.6]), one can show that every central simple algebra X over a number field F has a maximal subfield E such that E/F is a cyclic extension.

We now consider another invariant of X. We say the order $\mathrm{ord}_F[X]$ of the class of X in $\mathrm{Br}(F)$ is the *exponent* of X. It is closely related to the Schur index by the following proposition (cf. [**Pie82**, Proposition 14.4b]).

Proposition 1.1.7.

(i) The exponent $\mathrm{ord}_Z[X]$ *divides the Schur index* t_X*.*
(ii) Every prime divisor of t_X *divides* $\mathrm{ord}_Z[X]$*.*

In several occasions, we will assume the following hypothesis.

Hypothesis 1.1.8. *We say X satisfies the* ***exponent-index*** *(or* ***EI****) condition if* $t_X = \mathrm{ord}_Z[X]$.

The **EI** condition is satisfied in any of the following cases:

(1) t_X is squarefree.
(2) Z is a local field (cf. [**Rei03**, Theorem 31.4]).
(3) Z is a global field (cf. [**Rei03**, Theorem 32.19]).

The reader can find a valuable historical overview of (2) and (3) in [**Roq05**] and the references therein. We now state some properties of exponents of Brauer classes.

Proposition 1.1.9. *Let L/Z_Y be a finite extension of fields, and let Y be a central simple Z_Y-algebra.*

(1) If L splits Y, then $\mathrm{ord}_K[Y]$ *divides* $[L : Z_Y]$*.*
(2) Y contains a subfield L that splits it, and $\mathrm{ord}_{Z_Y}[Y] = [L : Z_Y]$*.*
(3) $\mathrm{ord}_{Z_Y}[Y]$ *divides* $[L : Z_Y] \cdot \mathrm{ord}_L[Y \otimes_{Z_Y} L]$*.*
(4) Suppose that Y is a division algebra and L is a Z_Y-subalgebra of Y. Then

$$\mathrm{ord}_L[Y \otimes_{Z_Y} L] = \frac{\mathrm{ord}_{Z_Y}[Y]}{[L : Z_Y]}.$$

Proof. The first three properties are proven in Section 13.4 of [**Pie82**]. Let us show (4). By (3) we have

$$\mathrm{ord}_{Z_Y}[Y] \mid [L : Z_Y] \cdot \mathrm{ord}_L[Y \otimes_{Z_Y} L].$$

[2] All of these statements are proven in [**Pie82**, Chapter 13]. However, Pierce calls these fields *strictly maximal*.

To see the *reverse divisibility*, we let $M \subset Y$ be a maximal field containing L. Then M splits Y, and in particular it splits $Y \otimes_{Z_Y} L$. Therefore by (1) we obtain

$$\mathrm{ord}_L[Y \otimes_{Z_Y} L] \mid [M : L]$$

and we are done since $[M : L] = \frac{[M:Z_Y]}{[L:Z_Y]} = \frac{\mathrm{ord}_{Z_Y}[Y]}{[L:Z_Y]}$. □

We now give a consequence of the Double Centralizer theorem (cf. Theorem 1.1.4), due to Jiangwei Xue, for algebras satisfying the exponent-index condition.

Proposition 1.1.10. *Let Y be a central division Z_Y-algebra and X a Z_Y-subalgebra of Y. Let $C = C_Y(X)$ be the centralizer of X in Y. Suppose that X, Y and C satisfy the **EI** condition. Then*

$$\mathrm{ord}_{Z_X}[X] \cdot \mathrm{ord}_{Z_X}[C] = \mathrm{ord}_{Z_X}[Y \otimes_{Z_Y} Z_X]$$

and $\gcd(\mathrm{ord}_{Z_X}[X], \mathrm{ord}_{Z_X}[C]) = 1$. *Moreover, if we let $d = \mathrm{ord}_{Z_X}[C]$, then we have an equality of nontrivial classes*

$$d[X] = d[Y \otimes_{Z_Y} Z_X] \text{ in } \mathrm{Br}(Z_X).$$

Proof. Theorem 1.1.4 applied to X gives

$$\dim_{Z_Y} X \cdot \dim_{Z_Y} C = \dim_{Z_Y} Y.$$

Since all algebras involved are division algebras, this equality can be expanded to

$$(\mathrm{ord}_{Z_X}[X])^2 \cdot (\mathrm{ord}_{Z_X}[C])^2 \cdot [Z_X : Z_Y]^2 = (\mathrm{ord}_{Z_Y}[Y])^2.$$

Therefore, applying Proposition 1.1.9(4) we obtain

$$\mathrm{ord}_{Z_X}[X] \cdot \mathrm{ord}_{Z_X}[C] = \mathrm{ord}_{Z_X}[Y \otimes_{Z_Y} Z_X].$$

Moreover, the Double Centralizer theorem also gives the equality

$$[X] + [C] = [Y \otimes_{Z_Y} Z_X]. \tag{1.1}$$

The following elementary lemma then implies that $d = \mathrm{ord}_{Z_X}[C]$ is coprime to $\mathrm{ord}_{Z_X}[X]$.

Lemma 1.1.11. *Let $(G, +)$ be a torsion abelian group and let $a, b \in G$. Then*

$$\mathrm{ord}(a + b) = \mathrm{ord}(a) \cdot \mathrm{ord}(b) \iff \gcd(\mathrm{ord}(a), \mathrm{ord}(b)) = 1.$$

Multiplying (1.1) by d yields the desired equality of nontrivial Brauer classes. □

1.2. Galois cohomology

In this section we introduce just enough Galois cohomology to give a different interpretation of the Brauer group. In particular, we give the two constructions of central simple algebras from 1- and 2-cocycles, and we show that these give opposite algebras. For these constructions, we need to consider the action of the Galois group on GL_n and PGL_n, and so we introduce the nonabelian cohomology sets H^0, H^1 and H^2.

Let G be a profinite group. A G-module is a discrete group A, not necessarily abelian, endowed with a left G-action. We say A is a G-module. We define the following terms.

- $H^0(G, A) := A^G$, the subgroup of elements of A pointwise fixed by G.

- A 1-cocycle is a continuous map $G \to A$ satisfying $a_{st} = a_s \cdot s(a_t)$. We say $a_s \in Z^1(G, A)$.
- Two 1-cocycles a_s, b_s are cohomologous if there exists some $a \in A$ such that $b_s = a^{-1} \cdot a_s \cdot s(a)$ for all $s \in G$.
- $a_s = 1$ is the *unit cocycle*.
- $H^1(G, A) := Z^1(G, A)/\sim$, where $\sim$ is the relation of being cohomologous. This is a pointed set with distinguished element the unit cocycle.

Suppose now A is abelian. In this case, $H^1(G, A)$ is also a group, with product of 1-cocycles defined by $(ab)_s := a_s \cdot b_s$. A 2-cocycle with values in A is a continuous map $c : G \times G \to A$ satisfying

$$g(c_{h,j}) \cdot c_{g,hj} = c_{g,h} \cdot c_{gh,j} \tag{1.2}$$

for all $g, h, j \in G$. We denote the set of 2-cocycles by $Z^2(G, A)$. This is an abelian group under multiplication of cocycles. Given any map $f : G \to A$, there is an associated 2-cocycle $c_{g,h} = f_g \cdot g(f_h) \cdot f_{gh}^{-1}$, called a 2-coboundary. The group generated by 2-coboundaries is denoted by $B^2(G, A)$. We finally define the second cohomology group of G with coefficients in A to be

$$H^2(G, A) := Z^2(G, A)/B^2(G, A).$$

Let A, B, C be G-modules, and consider a short exact sequence

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0.$$

Assume that $A \subseteq Z(B)$. Then, there is an exact sequence of pointed sets

$$\begin{aligned} 0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \\ \to H^1(G, A) \to H^1(G, B) \to H^1(G, C) \xrightarrow{\delta} H^2(G, A). \end{aligned}$$

The relevant map for us is δ, and is given as follows. Let $g \mapsto c_g$ be a 1-cocycle in $H^1(G, C)$. By definition we have $c_{gh} = c_g \cdot {}^g c_h$ for $g, h \in G$. For each $g \in G$, let $b_g \in B$ be such that $p(b_g) = c_g$. Then $p(b_{gh}) = p(b_g \cdot {}^g b_h)$, and so $b_g \cdot {}^g b_h \cdot b_{gh}^{-1} \in A$. We then define

$$(g, h) \mapsto \alpha_{g,h} := b_g \cdot {}^g b_h \cdot b_{gh}^{-1},$$

and let $\delta(c) = \alpha$. One checks that $\alpha \in H^2(G, A)$, this is where the assumption $A \subseteq Z(B)$ is needed. For the missing details, see [**Ser79**, Appendix to Chapter VII].

Let L/F be a Galois extension of fields. It is well-known that $G = \mathrm{Gal}(L/F)$ is a profinite group. Let A be a G-module. For $r \in \{0, 1, 2\}$, we have an description of the rth cohomology group of G as a direct limit,

$$H^r(G, M) \simeq \varinjlim_{F \subseteq E \subseteq L} H^r(\mathrm{Gal}(E/F), A^{\mathrm{Gal}(L/E)}),$$

where E ranges through all the intermediate fields such that E/F is finite and Galois, and $M^{\mathrm{Gal}(L/E)}$ denotes the elements of A fixed by the open subgroup $\mathrm{Gal}(L/E)$ of G. A common G-module once considers is $A = L^\times$, and so we let $H^r(L/F) := H^r(\mathrm{Gal}(L/F), L^\times)$.

We now give the cohomological interpretation of Brauer groups. Let F be a field, and let E/F be a finite Galois extension. We consider the set of Brauer classes

$$\mathrm{Br}(E/F) = \{[X] \in \mathrm{Br}(F) \mid E \text{ splits } X\}.$$

It is straightforward to check that $\mathrm{Br}(E/F)$ is a group, and that $\mathrm{Br}(F) = \varinjlim_{E/F} \mathrm{Br}(E/F)$. Fix a separable algebraic closure $\bar{F}$ of F.

Theorem 1.2.1. *For every finite Galois extension E/F, we have an isomorphism $\mathrm{Br}(E/F) \simeq H^2(E/F)$. Given a further extension E'/E with E'/F Galois, the corresponding isomorphisms are compatible with the injections $\mathrm{Br}(E/F) \to \mathrm{Br}(E'/F)$ and $H^2(E/F) \to H^2(E'/F)$. As a consequence, $\mathrm{Br}(F) \simeq H^2(\bar{F}/F)$.*

For a full proof of this theorem, we refer the reader to [**Ser79**, Chapter X] or [**Mil20**, § IV.3]. Here, we only give the morphism $H^2(E/F) \to \mathrm{Br}(E/F)$ from 2-cocycles with values in $E^\times$ to central simple F-algebras split by E. Since $\mathrm{Br}(E/F)$ is abelian, there are in fact two isomorphisms one can give inverse to each other. One is given by crossed-product algebras, and the other is its opposite.

We first see the construction of crossed-product algebras. Let F be a field, and let E/F be a finite Galois extension of degree n. Let $G = \mathrm{Gal}(E/F)$. Consider n symbols $\{u_s\}_{s\in G}$ and, for each pair $s, t \in G$, fix a constant $f_{s,t} \in E^\times$. Then we can define a multiplication on the vector space $X := \bigoplus Eu_s$ by $u_s \cdot x = s(x) \cdot u_s$ for every $x \in E$, and $u_s \cdot u_t = f_{s,t}u_{s,t}$. The product in X is then associative if and only if the relation (1.2) is satisfied for all $s, t, u \in \mathrm{Gal}(E/F)$. We also denote X by $E^f[G]$ and we call it the *crossed-product algebra given by f*.

The following result is [**Rei03**, Theorem 29.6].

Theorem 1.2.2. *For each 2-cocycle $f_{s,t}$, the crossed-product algebra $X = E^f[G]$ is a central simple F-algebra. The field E is its own centralizer in X, and it is a maximal subfield of X. If $g_{s,t}$ is another 2-cocyle, then $E^f[G]$ is F-isomorphic to $E^g[G]$ if and only if f and g are cohomologous.*

We now review the second construction of an algebra from a cocycle, which will be the opposite to the above. Let again E/F be a finite Galois extension of degree n and let $G = \mathrm{Gal}(E/F)$. Consider the exact sequence of G-modules

$$1 \to E^\times \to \mathrm{GL}_n(E) \xrightarrow{p} \mathrm{PGL}_n(E) \to 1.$$

We obtain an exact sequence of pointed sets in cohomology

$$H^1(G, \mathrm{GL}_n(E)) \xrightarrow{p} H^1(G, \mathrm{PGL}_n(E)) \xrightarrow{\delta} H^2(E/F).$$

By [**Ser79**, Chapter X, Proposition 3] we have $H^1(G, \mathrm{GL}_n(E)) = 0$, and so δ is "injective" in the sense that $\delta(c) = 0$ if and only if $c \in H^1(G, \mathrm{PGL}_n(E))$ is cohomologous to the trivial cocycle. Now consider a 1-cocycle $c_g = A_g \pmod{E}^\times$ in $\mathrm{PGL}_n(E)$ (so that $A_g \in \mathrm{GL}_n(E)$ for each $g \in G$). Recall that we have

$$\delta(c)_{g,h} = A_g \cdot {}^gA_h \cdot A_{gh}^{-1}.$$

We define the following F-vector space:

$$\mathcal{A}_c := \{X \in \mathrm{M}_n(E) \mid {}^gX = A_g^{-1} \cdot X \cdot A_g \text{ for each } g \in G\}.$$

The following result is well-known (see [**Chi87**, §1] for a proof).

Proposition 1.2.3. *$\mathcal{A}_c$ is a central simple F-algebra of dimension n^2 and satisfies $\mathcal{A}_c \otimes_F E \simeq \mathrm{M}_n(E)$. If c and d represent the same class in $H^1(G, \mathrm{PGL}_n(E))$, then $\mathcal{A}_c \simeq \mathcal{A}_d$.*

Proposition 1.2.4. *We have an isomorphism $\mathcal{A}_c \simeq E^{\delta(c)}[G]^{op}$ of F-algebras.*

PROOF. Fix a basis $\{e_g\}_{g\in G}$ of $V = H^n$. We will see it as an E-basis for $V \otimes E$. For each $g \in G$, let B_g be a matrix in $\mathrm{GL}_n(E)$ such that $B_g e_h = c_{g,h} e_{gh}$. By [**Ser79**, § X.5, Lemma 1] the map $g \mapsto B_g \mod E^\times$ is a 1-cocycle cohomologous to $g \mapsto A_g \mod E^\times$. Hence we may assume that

$$\mathcal{A}_c = \{X \in \mathrm{M}_n(E) \mid {}^g X = B_g^{-1} \cdot X \cdot B_g \text{ for each } g \in G\}.$$

For each $g \in G$ and $x \in E$, we consider matrices U_g and V_x in $\mathrm{GL}_n(E)$ satisfying

$$U_g \cdot e_h = c_{h,g} e_{hg} \quad \text{and} \quad V_x \cdot e_h = h(x) e_h$$

for all $h \in G$. We first check that $U_g \in \mathcal{A}_c$, which is equivalent to the equality $U_g B_h = B_h h(U_g)$. Indeed, for all $g, h, i \in G$ we have

$$\begin{aligned} U_g B_h e_i &= U_g c_{h,i} e_{hi} = c_{h,i} c_{hi,g} e_{hig} = h(c_{i,g}) c_{h,ig} e_{hig} \\ &= h(c_{i,g}) B_h e_{ig} = B_h \cdot h(c_{i,g} e_{ig}) \\ &= B_h h(U_g h^{-1}(e_i)) = B_h h(U_g) e_i. \end{aligned}$$

Now we check that $V_x \in \mathcal{A}_c$. For all $g, h \in G$, we have

$$\begin{aligned} B_g g(V_x) e_h &= B_g g(V_x g^{-1}(e_h)) = B_g g(V_x e_h) \\ &= B_g g h(x) e_h = g h(x) c_{g,h} e_{gh} = V_x B_g e_h. \end{aligned}$$

Now we need to check that the matrices V_x and U_g satisfy the relations of $E^{\delta(c)}[G]^{op}$, namely $U_h U_g = U_{gh} V_{c_{g,h}}$ and $V_x U_g = U_g V_{g(x)}$. For the first, we let $i \in G$ and compute

$$\begin{aligned} U_h U_g e_i &= U_h c_{i,g} e_{ig} = c_{i,g} c_{ig,h} e_{igh} = c_{i,g} c_{ig,h} c_{i,gh}^{-1} U_{gh} e_i \\ &= i(c_{g,h}) U_{gh} e_i = U_{gh} V_{c_{g,h}} e_i. \end{aligned}$$

The second is checked in the same way:

$$V_x U_g e_i = V_x c_{i,g} e_{ig} = i g(x) c_{i,g} e_{ig} = U_g i g(x) e_i = U_g V_{g(x)} e_i.$$

Hence the map $V_x \mapsto x$, $U_g \mapsto [g]$ gives an isomorphism of algebras $A_c \simeq E^{\delta(c)}[G]^{op}$. □

1.3. Abelian varieties

In this section we review the basic concepts about our main objects of study. Our main references for the topic are [**Mum08**] and [**Mil08**]. Let K be a field and fix an algebraic closure $\bar{K}$ of K.

An *abelian variety* A is a complete algebraic variety over K with a point $0 \in A(K)$ and morphisms of algebraic varieties $m : A \times A \to A$, $i : A \to A$ such that $A(\bar{K})$ is a group with binary operation m, inverse i, and identity element 0. More succinctly, an abelian variety over K is a complete group variety with its operations and identity element defined over K. Using the hypothesis that A is complete, one shows that $A(\bar{K})$ is an abelian group. For every extension L/K, the set of points $A(L)$ is also an (abelian) group.

Example 1.3.1. *Two common examples to keep in mind are elliptic curves and Jacobians. An elliptic curve is a (smooth, geometrically irreducible, projective) genus 1 curve with a point over K. Elliptic curves are the abelian varieties of dimension 1. Given a curve C/K of genus ≥ 1, its* Jacobian $\mathrm{Jac}(C)$ *is an abelian variety over K with the following property. For every extension L/K such that $C(L) \neq \emptyset$, there is an isomorphism of groups $\mathrm{Jac}(C)(L) \simeq \mathrm{Pic}^0(C)^{G_L}$.*

Let A and B be abelian varieties over K. A *morphism of abelian varieties* $\phi : A \to B$ is a morphism of algebraic varieties taking the identity 0_A to the identity 0_B (unless otherwise specified, we suppose that ϕ is itself defined over K). It can be shown that ϕ induces a group homomorphism $A(L) \to B(L)$ for every extension L/K. We say ϕ is an *isogeny* if (1) the induced map $A(\bar{K}) \to B(\bar{K})$ is surjective, (2) $\dim A = \dim B$, and (3) the kernel[3] of ϕ is a finite subgroup of $A(\bar{K})$. Note that any two of these properties implies the third. In that case, we write $A \sim B$ and say that A and B are *isogenous*. If L/K is an extension, we say A and B are L-isogenous if there is an isogeny $A_L \to B_L$ defined over L. The *degree* $\deg \phi$ of an isogeny ϕ is the order of its kernel.[4]

We denote by $\mathrm{Hom}(A, B)$ the abelian group of all morphisms $A \to B$ *that are defined over* K. If $A = B$, we let $\mathrm{End}(A) := \mathrm{Hom}(A, A)$, this is the *endomorphism ring of* A. Given an extension L/K, we have an injective ring homomorphism $\mathrm{End}(A) \to \mathrm{End}(A_L)$. The absolute Galois group G_K acts on $\mathrm{End}(A_{\bar{K}})$, we have $\mathrm{End}(A_L) = \mathrm{End}(A_{\bar{K}})^{\mathrm{Gal}(\bar{K}/L)}$.

Let n be a nonzero integer. By repeated use of the morphisms m and i, one sees that the multiplication-by-n map $[n] : A \to A$ is an endomorphism of A. In fact, more is true: the kernel of $[n]$ is always finite, and if $\mathrm{char}\, K \nmid n$, its kernel is isomorphic (as an abstract group) to $(\mathbb{Z}/n\mathbb{Z})^{2 \dim A}$. Therefore, $[n]$ is an isogeny. Once shows that $[n] \neq [n']$ for $n \neq n'$. Hence there is an injective ring homomorphism $\mathbb{Z} \to \mathrm{End}(A)$, and $\mathrm{End}(A)$ is a ring of characteristic zero. It can be shown that $\mathrm{End}(A)$ is finitely generated as a $\mathbb{Z}$-module.

For every abelian variety A, there is a *dual abelian variety* $A^\vee$, which has the property that $A^\vee(\bar{K}) \simeq \mathrm{Pic}^0(A_{\bar{K}})$ as groups. Every ample invertible sheaf $\mathcal{L}$ on A defines an isogeny $\phi_{\mathcal{L}} : A \to A^\vee$, which we call a *polarization*. If $\deg \phi_{\mathcal{L}} = 1$, we say $\phi_{\mathcal{L}}$ is a *principal polarization*. A fundamental result says that every abelian variety A admits a polarization, and in particular every abelian variety is projective.

Let $\phi : A \to B$ be an isogeny, and let $n = \deg \phi$. There is a *dual isogeny* $\phi^\vee : B^\vee \to A^\vee$ such that $\phi^\vee \circ \phi = [n]_A$. If ψ_A is a polarization of A, and $\phi : A \to A$ is an isogeny, then there exists an isogeny $\phi^\dagger : A \to A$ such that $[\deg \psi_A] \circ \phi^\dagger = \psi_A^\vee \circ \phi^\vee \circ \psi_A$. We call $\phi^\dagger$ the *Rosati dual* of ϕ. The Rosati dual is independent of the choice of polarization.

We say A is *simple* if it contains no abelian subvariety other than 0 and A itself. If A and B are simple, then any nonzero morphism $A \to B$ must be an isogeny.

We let $\mathrm{End}^0(A) := \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ be the *endomorphism algebra* of A. This is a semisimple $\mathbb{Q}$-algebra. If A and B are isogenous, then $\mathrm{End}^0(A) \simeq \mathrm{End}^0(B)$. Note that if $\phi \in \mathrm{End}(A)$ is an isogeny, then its image in $\mathrm{End}^0(A)$ is invertible, and every invertible element in $\mathrm{End}^0(A)$ is a rational multiple of an isogeny. Thus, $\mathrm{End}^0(A)$ is a division algebra if and only if A is simple. More generally, we have the following result.

Theorem 1.3.2. *Let A be an abelian variety. There exist simple abelian varieties $A_1, \ldots, A_r$ and positive integers $n_1, \ldots, n_r$ such that $\mathrm{Hom}(A_i, A_j) = 0$ for $i \neq j$, and*

$$A \sim A_1^{n_1} \times \cdots \times A_r^{n_r}.$$

[3]This is a scheme-theoretic kernel. For the sake of exposition, we may assume that K is a field of zero characteristic.

[4]This is again the order of the kernel as a finite group scheme.

Moreover, $\mathrm{End}^0(A) \simeq \mathrm{End}^0(\prod_{i=1}^r A_i^{n_i}) \simeq \prod_{i=1}^r \mathrm{M}_{n_i}(\mathrm{End}^0(A_i))$.

We say A is *split* if it is isogenous to a product of nonzero abelian varieties $B \times B'$, equivalently, if $r \cdot n_1 > 1$ in Theorem 1.3.2. We say A is *isotypical* if A is isogenous to the power B^n of a simple abelian variety B, equivalently, if $r = 1$ in Theorem 1.3.2 (n_1 may be larger than 1). We say A is geometrically simple (resp. split, isotypical) if $A_{\bar{K}}$ is simple (resp. split, isotypical).

1.4. The Albert classification

Let X be a central simple algebra. An *involution* $(\cdot)' : X \to X$ is an isomorphism of additive groups such that $x'' = x$, and with the property that for all $x, y \in X$, $(xy)' = y' \cdot x'$. We say an involution is *of the first kind* if it restricts to the identity on the center F on X, and *of the second kind* otherwise. An involution of the second kind restricts to an order-2 automorphism of F.

Let $\bar{F}$ be an algebraic closure of F. Given an element x of X, we define its (reduced) trace $\mathrm{Tr}_{X/F}(x)$ to be the trace of the image of x under the composition $X \to X \otimes_F \bar{F} \xrightarrow{\sim} \mathrm{M}_n(\bar{F})$, where n is the degree of X.

Suppose now X is a division algebra with center a number field F. Given $a \in X$, we let $\mathrm{Tr}_{X/\mathbb{Q}}(a) := \mathrm{Tr}_{F/\mathbb{Q}}(\mathrm{Tr}_{X/F}(a))$. We say an involution $(\cdot)' : X \to X$ is *positive* if $\mathrm{Tr}_{X/\mathbb{Q}}(xx') > 0$ for every nonzero x in X. Albert classified the division algebras with positive involution into four types.

Theorem 1.4.1. *Let F be a number field and let D be a central division algebra over F. Suppose D has a positive involution $'$, let F_0 be the subfield of F of elements fixed by $'$. Then $(D,')$ falls in one of the following cases.*

- *Type I.* $D = F = F_0$ *is a totally real field and $'$ is the identity.*
- *Type II.* $F = F_0$ *is a totally real field and D is a totally indefinite quaternion algebra.*
- *Type III.* $F = F_0$ *is a totally real field and D is a totally definite quaternion algebra. Moreover, the involution $'$ is the standard involution $x' = \mathrm{Tr}_{D/F}(x) - x$.*
- *Type IV. F is a CM field, F_0 is its maximal totally real subfield. Let σ be the nontrivial automorphism of F which is trivial on F_0. Then D is a central division algebra over F with the properties*
  - *(a)* $\mathrm{inv}_v[D \otimes_F F_v] = 0$ *for every place v of F fixed by σ,*
  - *(b)* $\mathrm{inv}_v[D \otimes_F F_v] + \mathrm{inv}_{\sigma v}[D \otimes_F F_{\sigma v}] = 0$ *for any finite place v of F.*

We observe that types I, II and III correspond to involutions of the first kind, while type IV corresponds to an involution of the second kind.

Let A be a simple abelian variety. Then the endomorphism algebra $\mathrm{End}^0(A)$ is a division $\mathbb{Q}$-algebra. Fix a polarisation and let $(\cdot)^\dagger : \mathrm{End}^0(A) \to \mathrm{End}^0(A)$ be the map giving the Rosati dual. One shows that this a positive involution. Therefore, Theorem 1.4.1 applies to $\mathrm{End}^0(A)$, and the endomorphism algebra falls in one of the four Albert types.

Let t_A be the Schur index of $\mathrm{End}^0(A)$. Let F be the center of $\mathrm{End}^0(A)$ and let F_0 be the subfield of F fixed by Rosati. We let $e = [F : \mathbb{Q}]$ and $e_0 = [F_0 : \mathbb{Q}]$. We also let S be the subset of $\mathrm{End}^0(A)$ on which the Rosati involution is trivial,

$$S = \{\phi \in \mathrm{End}^0(A) \mid \phi^\dagger = \phi\},$$

Type	e	t_A	η	Restriction in char 0	Restriction in char $p > 0$
I	e_0	1	1	$e \mid g$	$e \mid g$
II	e_0	2	$\frac{3}{4}$	$2e \mid g$	$2e \mid g$
III	e_0	2	$\frac{1}{4}$	$2e \mid g$	$e \mid g$
IV	$2e_0$	t_A	$\frac{1}{2}$	$e_0 t_A^2 \mid g$	$e_0 t_A \mid g$

TABLE 1.1. Summary of the Albert types for the endomorphism algebra $\mathrm{End}^0(A)$ of a simple abelian variety A.

and let $\eta = \frac{\dim_{\mathbb{Q}} S}{\dim_{\mathbb{Q}} \mathrm{End}^0(A)}$. In Table 1.1, we list the conditions on e, e_0, t_A, and η according to the Albert type of the algebra $\mathrm{End}^0(A)$ (cf. [**Mum08**, pg. 202] for some remarks on these conditions).

CHAPTER 2

Embeddings of simple algebras

Let Q be a perfect field. Throughout this whole chapter, we let X and Y be simple finite-dimensional Q-algebras. We denote their respective centers by Z_X and Z_Y. Recall that an *embedding of Q-algebras* $\iota\colon X \to Y$ is an injective ring homomorphism which is Q-linear. In particular, we have $\iota(1) = 1$ and $\iota(qx) = q\iota(x)$ for all $q \in Q$ and all $x \in X$. Sometimes we also say ι is an *embedding* when it is an embedding of algebras over the prime field, without any implication for the linearity with respect to a larger field.

The main goal of the chapter is to characterize the existence of an embedding of Q-algebras $X \to Y$. We begin in Section 2.1 by reviewing a theorem of Chia-Fu Yu which gives a general numerical criterion based on invariants of the algebras X and Y. We then study the class of *primitive embeddings* in Section 2.2. This allows us to give a criterion equivalent to Yu's theorem in Section 2.3, which only requires comparing the Brauer classes of X and Y. We end by giving some applications in particular cases in Section 2.4.

2.1. A numerical criterion for embeddings

Given a simple algebra Y, by Wedderburn's structure theorem (cf. Theorem 1.1.2) there exists a division algebra Y' and a positive integer c such that $Y = \mathrm{M}_c(Y')$. Recall that $c = c(Y)$ is the *capacity* of Y. We denote by t_Y the Schur index of Y, so that $\dim_{Z_Y} Y' = t_Y^2$. Recall also that

$$\dim_{Z_Y} Y = t_Y^2 c_Y^2. \tag{2.1}$$

Let Y be a division algebra and let E/Z_Y be a finite extension with $[E : Z_Y] = t_Y$. It is well-known that E is contained in Y if and only if E splits Y (cf. [**Pie82**, §13.4 Lemma]). In [**Yu12**, Theorem 1.2], Chia-Fu Yu has given the following generalization of this fact, which characterizes all possible subalgebras of Y.

Theorem 2.1.1. *Let X and Y be two finite-dimensional simple algebras over a field Q with centers Z_X and Z_Y, respectively. Let $Y \simeq \mathrm{M}_r(Y')$, with Y' a division algebra.*

(1) Suppose that Z_X and Z_Y are Q-linearly disjoint, so that $L = Z_X \otimes_Q Z_Y$ is a field. Then, there is an embedding of Q-algebras $X \to Y$ if and only if

$$\dim_Q X \mid r \cdot c,$$

where c is the capacity of the L-central simple algebra

$$Y' \otimes_Q X^{op} \simeq (Y' \otimes_{Z_Y} L) \otimes_L (L \otimes_{Z_X} X^{op}).$$

(2) *More generally, consider the product of fields* $Z_X \otimes_Q Z_Y = F_1 \times \cdots \times F_s$, *so that we have*

$$Y' \otimes_Q X^{op} \simeq \prod_{i=1}^{s} M_{c_i}(\Delta_i),$$

where Δ_i *is a central division algebra over* F_i. *Then, there is a* Q*-algebra embedding of* X *into* Y *if and only if there are non-negative integers* $r_1, \ldots, r_s$ *such that* $\sum r_i = r$, *and for each* $i = 1, \ldots, s$,

$$\frac{c_i \dim_Q \Delta_i}{\dim_Q Y'} \;\Big|\; r_i.$$

PROOF. We give a proof of (1) following [**Yu13b**, Proposition 2.2]. Let V be a right Y'-module such that $Y = \mathrm{End}_{Y'}(V)$. There is an embedding of Q-algebras $X \to Y$ if and only if V is an (X, Y')-bimodule, that is, if and only if V is a right $(Y' \otimes_Q X^{op})$-module. Let

$$Y' \otimes_Q X^{op} \simeq \mathrm{M}_c(\Delta)$$

with Δ a division $Z_X \otimes_Q Z_Y$-algebra. Then V is a right $Y' \otimes_Q X^{op}$-module if and only if $c \dim_Q \Delta$ divides $\dim_Q V$. Let us rewrite this quantities: on the one hand, we have

$$\dim_Q Y' \otimes_Q X^{op} = \dim_Q Y' \cdot \dim_Q X = c^2 \dim_Q \Delta,$$

and hence $c \dim_Q \Delta = \dim_Q Y' \cdot \dim_Q X/c$. On the other hand, we have $\dim_Q V = r \dim_Q Y'$. It follows that $c \dim_Q \Delta \mid \dim_Q V$ if and only if $\dim_Q X \mid c \cdot r$, as claimed.

Part (2) is a particular case of [**Yu12**, Theorem 1.2], which requires us to look at the maximal semisimple quotient of $Y' \otimes_H X^{op}$. To apply it we note that, since Q is a perfect field, all our (finite-dimensional, simple) algebras are separable [**Pie82**, §10.7, Corollary b]. Hence $Y' \otimes_Q X^{op}$ is again separable [**Rei03**, Corollary 7.19] and so it is semisimple with the stated form, thus we obtain our statement. See Remark 2.3.3 below for a different proof. □

In this chapter we will give more conceptual criteria equivalent to Theorem 2.1.1(2) to determine the subalgebras of a central simple algebra Y. We do this in Theorem 2.3.2.

Remark 2.1.2. *Yu's theorem contains the classical characterization of maximal subfields of* Y. *Indeed, let* $\dim_{Z_Y} Y = t_Y^2 c_Y^2$ *and let* $E \supseteq Z_Y$ *be a field with* $[E : Z_X] = t_Y c_Y$. *Then* $E \subseteq Y$ *if and only if*

$$[E : Z_X] \mid c(Y \otimes_{Z_Y} E).$$

Since $c(Y \otimes_{Z_Y} E) \leq \sqrt{\dim_{Z_Y} Y}$, *this is the case if and only if* $Y \otimes_{Z_Y} E = \mathrm{M}_{t_Y c_Y}(E)$, *that is, if and only if* E *splits* Y.

Remark 2.1.3. *In the same notation of the Theorem, we observe that when* $L = Z_X \otimes_Q Z_Y$ *is a field, we have the equality*

$$r \cdot c(Y' \otimes_Q X^{op}) = c(M_r(Y') \otimes_Q X^{op}) = c(Y \otimes_Q X^{op}).$$

This means that we do not need to separate the division part of Y *in order to compute the involved invariants.*

2.2. Primitive embeddings

Let $\iota : X \to Y$ be an embedding of Q-algebras. Denote by $\mathcal{Z}$ the subalgebra of Y generated by $\iota(Z_X)$ and Z_Y. There is a surjective homomorphism defined by

$$Z_X \otimes_Q Z_Y \to \mathcal{Z} \tag{2.2}$$

$$x \otimes y \mapsto \iota(x) \cdot y. \tag{2.3}$$

If we suppose that Z_X and Z_Y are Q-linearly disjoint, then $\mathcal{Z}$ is a field. This will be a particularly useful property, and we make the following definition.

Definition 2.2.1. *We say an embedding $X \to Y$ is* primitive *if the subalgebra $\mathcal{Z}$ of Y is a field.*

Example 2.2.2. *If Y is a division algebra and X is a Q-subalgebra of Y, then the embedding $X \to Y$ is primitive. Indeed, the algebra $\mathcal{Z} = Z_X Z_Y$ is a field, since Z_Y is the center of Y and so it commutes with Z_X.*

Remark 2.2.3. *Let $\alpha \in \mathrm{Aut}_{Z_Y}(Y)$ be an automorphism of Y and let $\iota : X \to Y$ be an embedding. Then ι is primitive if and only if $\alpha \circ \iota$ is primitive.*

Lemma 2.2.4. *An embedding $\iota : X \to Y$ of Q-algebras is primitive if and only if there exist an extension F/Z_X with $F \supseteq Z_Y$ and an embedding $\tilde{\iota} : X \otimes_{Z_X} F \to Y$ of Z_Y-algebras such that*

(1) $\tilde{\iota}|_X = \iota$, and
(2) $\tilde{\iota}$ restricts to an isomorphism between F and $\mathcal{Z}$.

Proof. If such a $\tilde{\iota}$ exists, its properties ensure that ι is primitive. Conversely, suppose ι is a primitive embedding. Let $f(x) \in Q[x]$ be an irreducible polynomial such that $Z_Y \simeq Q[x]/(f(x))$. This polynomial factors as $f_1(x) \cdots f_s(x)$ in $Z_X[x]$. Letting $F_j := Z_X[x]/(f_j(x))$, we obtain the isomorphism

$$\begin{aligned} Z_X \otimes_Q Z_Y &\simeq Z_X \otimes_Q Q[x]/(f(x)) \simeq Z_X[x]/(f(x)) \\ &\simeq Z_X[x]/(f_1(x)) \times \cdots \times Z_X[x]/(f_s(x)) = F_1 \times \cdots \times F_s. \end{aligned}$$

Let $Z_Y = Q(\alpha)$ for some α with $f(\alpha) = 0$, and $F_j = Z_X(\gamma_j)$ for some γ_j with $f_j(\gamma_j) = 0$ for each j. The field Z_Y embeds into each F_j via

$$\begin{aligned} \varphi_j : Z_Y &\to F_j \\ \sum a_i \alpha^i &\mapsto \sum a_i \gamma_j^i. \end{aligned}$$

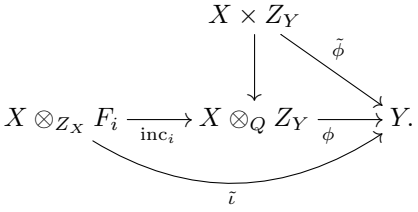
This gives each F_j a Z_Y-algebra structure, and makes explicit the isomorphism $Z_X \otimes_Q Z_Y \simeq F_1 \times \cdots \times F_s$ (of Z_Y-algebras) as

$$\begin{aligned} Z_X \otimes_Q Z_Y &\to F_1 \times \cdots \times F_s \\ a \otimes k &\mapsto (a\varphi_1(k), \ldots, a\varphi_s(k)). \end{aligned}$$

The above discussion yields a direct product decomposition $X \otimes_Q Z_Y \simeq \prod_j X \otimes_{Z_X} F_j$, this isomorphism is of Z_Y-algebras. We denote by inc_i the canonical monomorphism (of Z_Y-modules) $X \otimes_{Z_X} F_i \to \prod_j X \otimes_{Z_X} F_j \simeq X \otimes_Q Z_Y$. Note that inc_i sends $1 \mapsto e_i = (0, \ldots, 1, \ldots, 0)$ (the vector with a 1 in the ith place), and so it is *not* a morphism of Z_Y-algebras. However, inc_i *is* multiplicative, as

$$\mathrm{inc}_i(ab) = (0, \ldots, ab, \ldots, 0) = (0, \ldots, a, \ldots, 0)(0, \ldots, b, \ldots, 0).$$

Let $\tilde{\phi} : X \times Z_Y \to Y$ denote multiplication inside Y, $(x, y) \mapsto \iota(x)y$. The map $\tilde{\phi}$ is Q-bilinear, so it factors through a unique Q-linear map $\phi : X \otimes_Q Z_Y \to Y$. In fact, ϕ is Z_Y-linear, this is seen directly from the definition of $\tilde{\phi}$. In addition, ϕ is not the zero map. Therefore, there is some $i \in \{1, \ldots, s\}$ for which $\phi \circ \mathrm{inc}_i$ is not the zero map. We let $\tilde{\iota} := \phi \circ \mathrm{inc}_i$. Our situation is as follows:



A priori, $\tilde{\iota}$ is only a morphism of Z_Y-modules. We want to see that it is multiplicative and sends $1 \mapsto 1$. For the multiplicativity, take $a, a' \in Z_X$ and $k, k' \in Z_Y$. Because Z_Y is the center of Y, it commutes with $\iota(X)$ and we have

$$\phi(\alpha\alpha' \otimes kk') = \iota(\alpha\alpha')kk' = \iota(\alpha)k\iota(\alpha')k' = \phi(\alpha \otimes k)\phi(\alpha' \otimes k').$$

Hence ϕ and $\tilde{\iota} = \phi \circ \mathrm{inc}_i$ are multiplicative; ϕ is also a ring homomorphism since it sends $1 \mapsto 1$.

The kernel of $\tilde{\iota}$ is a two-sided ideal of $X \otimes_{Z_X} F_i$. Since this is a simple algebra, we deduce that $\tilde{\iota}$ is injective. Hence it restricts to an injection $F_i \to \mathcal{Z} = \iota(Z_X)Z_Y$. Therefore $\tilde{\iota}(1) = 1$, and so $\tilde{\iota}$ is an embedding of Z_Y-algebras. It is clear that it agrees with ι on X, since for $d \in X$,

$$\tilde{\iota}(d) = \phi(\mathrm{inc}_i(d)) = \phi(d \cdot \mathrm{inc}_i(1)) = \phi(d) \cdot \phi(\mathrm{inc}_i(1)) = \iota(d).$$

To see (2), we note that $\iota(Z_X) \subseteq \tilde{\iota}(F_i)$. We also have $Z_Y \subseteq \tilde{\iota}(F_i)$, since $\tilde{\iota}$ is Z_Y-linear. Finally, $\tilde{\iota}(F_i) \subseteq \iota(Z_X)Z_Y$, because $\iota(Z_X)Z_Y$ is the image of the center $Z_X \otimes_Q Z_Y$ of $X \otimes_Q Z_Y$ through ϕ. Therefore $\tilde{\iota}(F_i) = \iota(Z_X)Z_Y = \mathcal{Z}$. □

Example 2.2.5. *The isomorphism $Z_X \otimes_Q Z_Y \simeq F_1 \times \cdots \times F_s$ and the action of Z_Y on each F_j become clearer with the following example. Let $Z_X = \mathbb{Q}(\sqrt[4]{2})$ and $Z_Y = \mathbb{Q}(i\sqrt[4]{2})$ (as subfields of $\mathbb{C}$), and let $Q = \mathbb{Q}$. Then $Z_Y = \mathbb{Q}[x]/(x^4 - 2)$, and the identity*

$$x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2}) = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x^2 + \sqrt{2})$$

in $Z_X[x]$ gives

$$\begin{aligned}\mathbb{Q}(\sqrt[4]{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(i\sqrt[4]{2}) &= \mathbb{Q}(\sqrt[4]{2})[x]/(x^4 - 2) \\ &\simeq \mathbb{Q}(\sqrt[4]{2})[x]/(x - \sqrt[4]{2}) \times \mathbb{Q}(\sqrt[4]{2})[x]/(x + \sqrt[4]{2}) \times \mathbb{Q}(\sqrt[4]{2})[x]/(x^2 + \sqrt{2}) \\ &\simeq \mathbb{Q}(\sqrt[4]{2}) \times \mathbb{Q}(\sqrt[4]{2}) \times \mathbb{Q}(\sqrt[4]{2}, i).\end{aligned}$$

The two actions of $Z_Y = \mathbb{Q}(i\sqrt[4]{2})$ on $F_1 = F_2 = \mathbb{Q}(\sqrt[4]{2})$ correspond to the two isomorphisms that send $i\sqrt[4]{2} \mapsto \sqrt[4]{2}$ and $i\sqrt[4]{2} \mapsto -\sqrt[4]{2}$. Meanwhile, the action of Z_Y on $F_3 = \mathbb{Q}(\sqrt[4]{2}, i)$ is given by the obvious inclusion, given the chosen generators.

Suppose now that we have positive integers $r_1, \ldots, r_k$ and primitive embeddings

$$\iota_i : X \to \mathrm{M}_{r_i}(Y),\ i = 1, \ldots, k.$$

By setting $r = \sum_i r_i$, we can define a block-diagonal embedding

$$\iota = \prod \iota_i : X \to \prod_i \mathrm{M}_{r_i}(Y) \subseteq \mathrm{M}_r(Y),$$

which is not necessarily primitive. We now show that all embeddings are essentially of this form.

Proposition 2.2.6. *Let $\iota : X \to \mathrm{M}_r(Y)$ be any embedding of Q-algebras. Then there exist integers $r_1, \dots, r_k$ with $\sum_i r_i = r$ and primitive embeddings $\iota_i : X \to \mathrm{M}_{r_i}(Y)$ such that the block-diagonal embedding*

$$\prod \iota_i : X \to \prod_i \mathrm{M}_{r_i}(Y) \subseteq \mathrm{M}_r(Y)$$

is conjugate to ι.

Proof. As above, let $\mathcal{Z}$ be the subalgebra of $\mathrm{M}_r(Y)$ generated by $\iota(Z_X)$ and Z_Y. As in the proof of Lemma 2.2.4, let $F_1, \dots, F_s$ be fields such that

$$Z_X \otimes_Q Z_Y \simeq F_1 \times \cdots \times F_s.$$

We claim that there exists a subset $I \subseteq \{1, \dots, s\}$ with

$$\mathcal{Z} \simeq \prod_{i \in I} F_i. \tag{2.4}$$

Indeed, this is the case since we have a surjective ring homomorphism $Z_X \otimes_Q Z_Y \to \mathcal{Z}$ (cf. (2.2)), and its kernel is an ideal of the product ring $\prod_{i=1}^s F_i$. Hence this kernel is of the form $\prod_{j \notin I} F_j \times \prod_{i \in I} \{0_{F_i}\}$. By the same construction as in Lemma 2.2.4, we have a Z_Y-algebra homomorphism

$$\tilde{\iota} : \prod_{i \in I} X \otimes_{Z_X} F_i \to \mathrm{M}_r(Y)$$

such that its precomposition with the diagonal embedding $X \to \prod_{i \in I} X \otimes F_i$ is equal to the original ι.

For each $i \in I$, let $e_i \in \mathcal{Z}$ be the (nonzero) idempotent corresponding to F_i through (2.4). We have $\sum_{i \in I} e_i = 1$. By Lemma 2.2.7 below, each e_i is conjugate to a diagonal matrix whose only nonzero entries equal 1. Since all the idempotents commute, we may diagonalise them simultaneously by an element of $\mathrm{GL}_r(Y)$ to find that the image of $\tilde{\iota}$ lands in a block-diagonal subalgebra $\mathrm{M}_{r_1}(Y) \times \cdots \times \mathrm{M}_{r_k}(Y) \subseteq \mathrm{M}_r(Y)$. In particular, $\tilde{\iota}$ is injective, and its restriction to each $X \otimes_{Z_X} F_i$, $i \in I$, gives an embedding

$$\tilde{\iota}_i : X \otimes_{Z_X} F_i \to \mathrm{M}_{r_i}(Y)$$

which is Z_Y-linear. Again as in Lemma 2.2.4 we have that $\tilde{\iota}_i|_{F_i}$ is an isomorphism of F_i with the compositum of Z_X and Z_Y in $\mathrm{M}_{r_i}(Y)$. Hence the restriction $\tilde{\iota}_i|_X$ is a primitive embedding. Finally, the product embedding $\prod \tilde{\iota}_i|_X$ is conjugate to the original ι. □

Lemma 2.2.7. *Let Z_Y be a field, Y a division algebra with center Z_Y, and $r \geq 1$ an integer. An idempotent $e \in \mathrm{M}_r(Y)$ is conjugate by a matrix in $\mathrm{GL}_r(Y)$ to a diagonal matrix whose only nonzero entries equal 1.*

PROOF. The minimal polynomial of an idempotent $e \in \mathrm{M}_r(Y)$ is $x(x-1)$, so in particular e is a separable element. By [**Yu13a**, Lemma 2], the (reduced) characteristic polynomial of e equals $x^a(x-1)^b$ for some a, b with $a + b = rt_Y$. We can write $\mathrm{M}_r(Y) = \mathrm{End}_Y(V)$ for some Z_Y-vector space V, and by the theory of canonical forms for $\mathrm{M}_r(Y)$ (cf. [**Yu13a**, §3 and §5]) we can decompose V as a $(Z_Y[e], Y)$-bimodule as

$$V \simeq V_0^a \oplus V_1^b.$$

Here we are choosing V_i so that it is a Y-module of dimension 1 on which e acts as $i = 0$ or 1. Letting $f \in \mathrm{M}_r(Z_Y) \subseteq \mathrm{M}_r(Y)$ be a diagonal matrix with a entries equal to 1 and b entries equal to 0, we obtain the same decomposition of V as a $(Z_Y[f], Y)$-bimodule. This implies e, f are conjugate by some element in $\mathrm{GL}_r(Y)$. □

Example 2.2.8. *The following is an example of a non-primitive embedding. Let* $Y = \mathrm{M}_2(\mathbb{Q}(\sqrt{5}))$ *and let* $Z_X = X = \mathbb{Q}(\sqrt{5})$*. We have the embedding of* $\mathbb{Q}$*-algebras*

$$\iota : \mathbb{Q}(\sqrt{5}) \to \mathrm{M}_2(\mathbb{Q}(\sqrt{5}))$$
$$\sqrt{5} \mapsto \begin{pmatrix} 0 & 5 \\ 1 & 0. \end{pmatrix}$$

It is straightforward to see that the compositum of $\iota(\mathbb{Q}(\sqrt{5}))$ *and the center* $\mathbb{Q}(\sqrt{5})$ *is the product of fields* $\mathbb{Q}(\sqrt{5}) \times \mathbb{Q}(\sqrt{5})$*, which is conjugate to the diagonal matrices. By conjugating* ι *we obtain*

$$\mathbb{Q}(\sqrt{5}) \to \mathbb{Q}(\sqrt{5}) \times \mathbb{Q}(\sqrt{5}) \subset \mathrm{M}_2(\sqrt{5})$$
$$\sqrt{5} \mapsto (\sqrt{5}, -\sqrt{5}).$$

This is the product of two primitive embeddings from Proposition 2.2.6.

In particular, this example shows that the composition of primitive embeddings is not necessarily a primitive embedding. Indeed, ι *is the compositum of two primitive embeddings* $\mathbb{Q}(\sqrt{5}) \to \mathrm{M}_2(\mathbb{Q})$ *and* $\mathrm{M}_2(\mathbb{Q}) \to \mathrm{M}_2(\mathbb{Q}(\sqrt{5}))$*.*

As a corollary of Proposition 2.2.6, we obtain the following result.

Corollary 2.2.9. *Let* X *and* Y *be simple* Q*-algebras with centers* Z_X *and* Z_Y *satisfying* $\dim_{Z_X} X = \dim_{Z_Y} Y$*. Given an embedding of* Q*-algebras* $\iota : X \to Y$*, we have* $\iota(Z_X) \subseteq Z_Y$ *and* $Y \simeq X \otimes_{Z_X} Z_Y$*. In particular, any embedding between algebras of the same degree is primitive.*

PROOF. Write $Y = \mathrm{M}_r(Y')$ with Y' a division algebra, we have $\dim_{Z_Y} Y = r^2 \dim_{Z_Y} Y'$. By Proposition 2.2.6, there is some $r' \leq r$ and a finite extension F/Z_X such that there is an embedding $\iota' : X \otimes_{Z_X} F \to \mathrm{M}_{r'}(Y')$. Therefore we have

$$\dim_{Z_Y} \mathrm{M}_{r'}(Y') = (r')^2 \dim_{Z_Y} Y' \geq \dim_{Z_Y} X \otimes_{Z_X} F \geq \dim_{Z_X} X = r^2 \dim_{Z_Y} Y'.$$

Therefore $r' \geq r$, and $r = r'$. It follows that $Y \simeq X \otimes_{Z_X} F$, so $F = Z_Y$, and therefore $Z_X \subseteq Z_Y$. □

Remark 2.2.10. *Corollary 2.2.9 appears as Lemma 7.4.2 in* [**CMSV19**]*. Our proof is different from theirs in that we do not use the Albert–Brauer–Hasse–Noether theorem or the Chebotaryov density theorem, and in particular applies to fields that are not number fields.*

2.3. A criterion on Brauer classes

Recall from Section 1.1 that an algebra X is said to satisfy the exponent-index (**EI**) condition if $t_X = \left(\sqrt{\dim_{Z_X} X}\right)/c_X = \mathrm{ord}_{Z_X}[X]$, where t_X (resp. c_X, $\mathrm{ord}_{Z_X}[X]$) is the Schur index (resp. capacity, exponent) of X. In this section, we assume that all algebras satisfy the **EI** condition. In later chapters, we will always have Z_X and Z_Y number fields, so this condition will be automatically satisfied.

We consider the problem of deciding when there exists an embedding of X into Y in a particularly simple situation.

Proposition 2.3.1. *Let X and Y be simple algebras such that Z_X is a Z_Y-subalgebra of Y. Then, X is a Z_Y-subalgebra of Y if and only if the quantity*

$$d = \frac{t_Y c_Y}{t_X c_X [Z_X : Z_Y]}$$

is an integer and the equality $d[X] = d[Y \otimes_{Z_Y} Z_X]$ holds in $\mathrm{Br}(Z_X)$.

Proof. By Theorem 2.1.1(1), X is a Z_Y-subalgebra of Y if and only if $\dim_{Z_Y} X = t_X^2 c_X^2 [Z_X : Z_Y]$ divides the capacity c of the algebra $(Y \otimes_{Z_Y} Z_X) \otimes_{Z_X} X^{op}$. The dimension of this algebra is

$$\dim_{Z_X}((Y \otimes_{Z_Y} Z_X) \otimes_{Z_X} X^{op}) = (\dim_{Z_Y} Y) \cdot (\dim_{Z_X} X) = (t_Y c_Y t_X c_X)^2.$$

Let t be the Schur index of the algebra $(Y \otimes_{Z_Y} Z_X) \otimes_{Z_X} X^{op}$. Then by (2.1), we have

$$c = c((Y \otimes_{Z_Y} Z_X) \otimes_{Z_X} X^{op}) = \frac{t_Y c_Y t_X c_X}{t}.$$

Hence $\dim_{Z_Y} X \mid c$ if and only if

$$d := \frac{t_Y c_Y}{t_X c_X [Z_X : Z_Y]}$$

is an integer and $t \mid d$. Since we assume the **EI** condition, $t = \mathrm{ord}_{Z_X}[(Y \otimes_{Z_Y} Z_X) \otimes_{Z_X} X^{op}]$ is the exponent of $(Y \otimes_{Z_Y} Z_X) \otimes_{Z_X} X^{op}$, and so X is a Z_Y-algebra of Y if and only if $d \in \mathbb{Z}$ and $d[(Y \otimes_{Z_Y} Z_X) \otimes_{Z_X} X^{op}] = [Z_X]$, if and only if

$$d[Y \otimes_{Z_Y} Z_X] = d[X].$$

The statement follows. □

As a direct corollary, we obtain the following equivalent formulation of Theorem 2.1.1.

Theorem 2.3.2. *Let X and Y be simple Q-algebras with respective centers Z_X and Z_Y. Let $Y \simeq \mathrm{M}_r(Y')$, with Y' a division algebra. Consider the product of fields*

$$Z_X \otimes_Q Z_Y \simeq F_1 \times \cdots \times F_s.$$

There exists an embedding of Q-algebras $\iota : X \to Y$ if and only if there exist non-negative integers $r_1, \ldots, r_s$ with

(1) $\sum_{i=1}^{s} r_i = r$, and
(2) If $r_i > 0$, then the quantity $d_i = \frac{r_i t_Y}{[F_i : Z_Y] t_X c_X}$ is an integer, and we have

$$d_i[X \otimes_{Z_X} F_i] = d_i[Y \otimes_{Z_Y} F_i].$$

Moreover, ι is a primitive embedding if and only if $r_{i_0} = r$ for some i_0.

PROOF. By Proposition 2.2.6, having an embedding $\iota : X \to \mathrm{M}_r(Y')$ is equivalent to having nonnegative integers $r_1, \dots, r_s$ with $\sum_i r_i = r$ and primitive embeddings $\iota_i : X \to \mathrm{M}_{r_i}(Y')$ whenever $r_i > 0$. By Lemma 2.2.4, each ι_i extends to some embedding $\tilde{\iota}_i : X \otimes_{Z_X} F_i \to \mathrm{M}_{r_i}(Y')$, and then condition (2) comes directly from Proposition 2.3.1. □

Remark 2.3.3. *We can now prove Theorem 2.1.1 using Theorem 2.3.2. Write $Y \simeq \mathrm{M}_r(Y')$. In the notation of Theorem 2.1.1, let*

$$\mathrm{M}_{c_i}(\Delta_i) \simeq (Y' \otimes_{Z_Y} F_i) \otimes_{F_i} (X \otimes_{Z_X} F_i)^{op}$$

for each $i = 1, \dots, s$. Let $t_{\Delta_i} = \mathrm{ord}_{F_i}[\Delta_i]$. Then, our criterion says that having an embedding $X \to Y$ is equivalent to having

$$t_{\Delta_i}[Y' \otimes_{Z_Y} F_i] = t_{\Delta_i}[X \otimes_{Z_X} F_i]$$

and $t_{\Delta_i}[F_i : Z_Y]c_X t_X \mid r_i t_Y$. By direct manipulation, this divisibility relation is equivalent to

$$\frac{t_{\Delta_i}[F_i : Q]t_Y c_X t_X}{\dim_Q Y'} \mid r_i,$$

since $\dim_Q Y' = t_Y^2[Z_Y : Q]$. But now we have $c_i^2 \dim_{F_i} \Delta_i = t_Y^2 c_X^2 t_X^2$ and $\dim_{F_i} \Delta_i = t_{\Delta_i}^2$, and so the above is equivalent to

$$\frac{c_i t_{\Delta_i}^2[F_i : Q]}{\dim_Q Y'} = \frac{c_i \dim_Q \Delta_i}{\dim_Q Y'} \mid r_i.$$

This is the condition from Theorem 2.1.1.

2.4. Applications

As in the previous section, we assume that all algebras satisfy the **EI** condition. We give three consequences of Propositions 2.2.6 and 2.3.1.

2.4.1. Existence of a primitive embedding. Let X and Y be Q-algebras with respective centers Z_X and Z_Y, and let $\varphi : X \to Y$ be an embedding. We want to give conditions to ensure the existence of a (possibly different) primitive embedding of X into Y.

To be able to give general conditions, let us give the setup for the next lemma. Write $Y = \mathrm{M}_r(Y')$ with Y' a division algebra. Let $F_1, \dots, F_s$ be fields such that $Z_X \otimes_Q Z_Y \simeq F_1 \times \cdots \times F_s$, and let $\{r_i\}_{i=1}^s$ be nonnegative integers giving the decomposition of φ into primitive embeddings $\varphi_i : X \to \mathrm{M}_{r_i}(Y')$ (cf. Proposition 2.2.6). Let $I = \{i \mid r_i > 0\} \subseteq \{1, \dots, s\}$, this is the set of indices i such that the field F_i *intervenes in the decomposition of φ.*

Lemma 2.4.1. *Suppose that for some $i_0 \in \{1, \dots, s\}$ there is a field homomorphism $F_{i_0} \to F_i$ for every $i \in I$. Then, there exists a primitive embedding $\psi : X \to Y$.*

PROOF. Theorem 2.3.2 asserts that:

(i) For each $i \in I$, $[F_i : Z_Y]t_X c_X \mid r_i t_Y$, and
(ii) If we let $d_i = \frac{r_i t_Y}{[F_i : Z_Y]t_X c_X}$, then $d_i[X \otimes_{Z_X} F_i] = d_i[Y \otimes_{Z_Y} F_i]$.

If we let $C_i := (X \otimes_{Z_X} F_i) \otimes_{F_i} (Y \otimes_{Z_Y} F_i)^{op}$, then (ii) amounts to $\mathrm{ord}_{F_i}[C_i] \mid d_i$. We have the equality

$$[F_i : F_{i_0}]d_i = \frac{r_i t_Y}{[F_{i_0} : Z_Y]t_X c_X},$$

from which we know that $[F_{i_0} : Z_Y]t_X c_X \mid \sum_i r_i t_Y = rt_Y$. From the relation $[C_i] = [C_{i_0} \otimes_{F_{i_0}} F_i]$ and Proposition 1.1.9, we have

$$\operatorname{ord}[C_{i_0}] \mid \operatorname{ord}[C_{i_0} \otimes_{F_{i_0}} F_i] \cdot [F_i : F_{i_0}] \mid d_i \cdot [F_i : F_{i_0}],$$

and hence $d_i \cdot [F_i : F_{i_0}] \cdot [C_{i_0}]$ is the trivial class in $\mathrm{Br}(F_{i_0})$. It follows that

$$\left(\sum_i d_i \cdot [F_i : F_{i_0}] \right) \cdot [C_{i_0}] = \frac{rt_Y}{[F_{i_0} : Z_Y]t_X c_X} \cdot [C_{i_0}] = [F_{i_0}].$$

Therefore, letting $d = \frac{rt_Y}{[F_{i_0}:Z_Y]t_X c_X}$ we have

$$d[X \otimes_{Z_X} F_{i_0}] = d[Y \otimes_{Z_Y} F_{i_0}],$$

and by Theorem 2.3.2, there exists an embedding $\psi : X \to Y$ which is primitive. □

Theorem 2.4.2. *Let X and Y be Q-algebras with respective centers Z_X and Z_Y. Suppose that either Z_X/Q or Z_Y/Q is a Galois extension. If there is an embedding of Q-algebras $\varphi : X \to Y$, then there exists a (possibly different) primitive embedding of Q-algebras $\psi : X \to Y$.*

Proof. Let $F_1, \ldots, F_s$ be fields such that $Z_X \otimes_Q Z_Y \simeq F_1 \times \cdots \times F_s$. The condition that Z_X/Q or Z_Y/Q is Galois implies that there are isomorphisms $F_i \simeq F_j$ for all i and j. Hence a primitive embedding $\psi : X \to Y$ exists by Lemma 2.4.1. □

As a second consequence of Lemma 2.4.1, we can guarantee the existence of primitive embeddings whenever one of the centers is relatively small.

Theorem 2.4.3. *Suppose that there exists an embedding $\varphi : X \to Y$ and either Z_X/Q or Z_Y/Q is an extension of degree at most 4. Then, there exists a primitive embedding $\psi : X \to Y$.*

Proof. Let $\delta = [Z_X : Q]$. Since the argument is symmetric, we shall assume that $\delta \leq 4$. If $\delta = 1$ the embedding φ is primitive, and if $\delta = 2$ then a primitive ψ exists by Theorem 2.4.2.

Write $Z_X \otimes_Q Z_Y \simeq F_1 \times \cdots \times F_s$ as usual, and let r_i be the integers associated to each F_i and φ as in the beginning of the section. Note that

$$[Z_X : Q] = \delta = \sum_{i=1}^{s} [F_i : Z_Y]. \tag{2.5}$$

We suppose that $r_i < r = c_Y$ for all i, otherwise φ is already primitive.

Suppose $\delta = 3$. By (2.5) there must exist some $i_0 \in \{1, 2, 3\}$ such that $[F_{i_0} : Z_Y] = 1$, that is, such that $F_{i_0} \simeq Z_Y$. Since for every i, F_i is an extension of Z_Y, there is a homomorphism $F_{i_0} \to F_i$. Lemma 2.4.1 implies that a primitive $\psi : X \to Y$ exists.

Finally, suppose $\delta = 4$. By the same argument as above, we conclude the existence of a primitive embedding $\psi : X \to Y$ assuming that $[F_{i_0} : Z_Y] = 1$ for some i_0. Hence, it only remains to show that ψ exists assuming $s = 2$ and $[F_1 : Z_Y] = [F_2 : Z_Y] = 2$. There is an irreducible polynomial $f \in Q[x]$, of degree 4, such that $Z_X \simeq Q[x]/(f)$. Our situation amounts to saying that $f = g_1 g_2$ in $Z_Y[x]$, where g_1, g_2 are degree-2 irreducible polynomials, and $F_i \simeq Z_Y[x]/(g_i)$. If g_1 splits in F_2, then clearly $F_1 \simeq F_2$. Otherwise, the field $K = Z_Y[x]/(g_1, g_2)$ is a biquadratic Galois extension of Z_Y, which is a splitting field for f. Hence K contains the Galois closure L of Z_X/Q. Now we let α_i, β_i be the two roots of g_i. In

our situation, the group $\mathrm{Gal}(L/Q)$ is a transitive subgroup of S_4 containing $C_2 \times C_2$, and so there is a Q-automorphism σ of L sending $\alpha_1 \leftrightarrow \alpha_2$ and $\beta_1 \leftrightarrow \beta_2$. Therefore σ induces an isomorphism $F_1 \simeq F_2$.

In any case, the isomorphism $F_1 \simeq F_2$ gives us a primitive embedding $\psi : X \to Y$ by Lemma 2.4.1. □

We now show a smallest example of algebras X, Y such that an embedding $X \to Y$ exists, but it cannot be a primitive embedding.

Example 2.4.4. *Let L/Q be a Galois extension with Galois group S_5. Choose a subgroup H of S_5 isomorphic to S_4, and let $F = L^H$, this is a degree-5 extension of Q which is not Galois. Choose a subgroup H' of S_5 isomorphic to $D_{2\cdot 6}$; it can be shown that H' is a maximal subgroup. Let $K = L^{H'}$ be the fixed field, we have $[K : Q] = 10$, and K has no proper subfields other than Q. In particular, there is no homomorphism $F \to K$.*

We observe that F and K are not linearly disjoint: indeed, a compositum of F and K is a subfield of L, but $[F : Q][K : Q] = 50$ does not divide $[L : Q] = 120$. Hence there is an integer $s \geq 2$ and fields $F_1, \ldots, F_s$ such that

$$F \otimes_Q K \simeq F_1 \times \cdots \times F_s.$$

For each i, we necessarily have $[F_i : K] > 1$, since otherwise F would admit an injection to K. From the relation $\sum_i [F_i : K] = [F : Q] = 5$ it follows that $s = 2$, $[F_1 : K] = 2$, and $[F_2 : K] = 3$.

Now by Theorem 2.3.2 there exists an embedding $F \to \mathrm{M}_5(K)$, by letting $r_1 = 2$ and $r_2 = 3$. But there cannot exist such an embedding which is also primitive, since neither $[F_1 : K]$ nor $[F_2 : K]$ divides 5.

2.4.2. Algebras with a shared maximal subfield. The second application concerns algebras which share a maximal subfield.

Theorem 2.4.5. *Let X and Y be simple Q-algebras. Let $E \supseteq Q$ be a field which is a maximal subfield of both X and Y. Then X is a Q-subalgebra of Y if and only if $Z_Y \subseteq Z_X$ and $[X] = [Y \otimes_{Z_Y} Z_X]$ in $\mathrm{Br}(Z_X)$.*

Proof. If E is a maximal subfield of Y, then $Z_Y \subseteq E$. Hence Z_Y is a subfield of X. Suppose that X is a Q-subalgebra of Y. Then $Z_Y \subseteq Z_X$, since Z_Y commutes with all the elements of X. Now we have $[E : Z_Y] = t_Y c_Y$ and $[E : Z_X] = t_X c_X$, from which we obtain $\frac{t_Y c_Y}{t_X c_X [Z_X : Z_Y]} = 1$. By Proposition 2.3.1 we obtain $[X] = [Y \otimes_{Z_Y} Z_X]$.

Conversely, the conditions $Z_Y \subseteq Z_X$ and the Brauer class equation imply that X is a Q-subalgebra of Y (and even a Z_Y-subalgebra) by Proposition 2.3.1. □

2.4.3. Embeddings of division algebras. Our third application concerns embeddings of division algebras.

Theorem 2.4.6. *Suppose X and Y are division Q-algebras. Suppose Z_X is a Q-subalgebra of Y and let $\mathcal{Z} = Z_X Z_Y$ be the subalgebra of Y generated by the fields Z_X and Z_Y. Then, X is a Q-subalgebra of Y if and only if $d = \frac{t_Y}{[\mathcal{Z} : Z_Y] t_X}$ is an integer and there is a equality*

$$d[X \otimes_{Z_X} \mathcal{Z}] = d[Y \otimes_{Z_Y} \mathcal{Z}]$$

in $\mathrm{Br}(\mathcal{Z})$. The Brauer classes in this equality are nontrivial if $t_X > 1$. Moreover, $\frac{t_Y}{[\mathcal{Z} : Z_Y] t_X}$ is coprime with t_X.

PROOF. By Example 2.2.2, $\mathcal{Z}$ is a field. Hence by Lemma 2.2.4, X is a Q-subalgebra of Y if and only if $X \otimes_{Z_X} \mathcal{Z}$ is a Z_Y-subalgebra of Y. The necessary and sufficient equality of Brauer classes is given by Proposition 2.3.1 for

$$d = \frac{t_Y}{[\mathcal{Z} : Z_Y]t_X}.$$

The equality of Brauer classes is necessarily nontrivial when $t_X > 1$. Indeed, by Proposition 1.1.9(4) we have $\mathrm{ord}_{\mathcal{Z}}[Y \otimes_{Z_Y} \mathcal{Z}] = \frac{t_Y}{[\mathcal{Z}:Z_Y]}$. Hence $d[Y \otimes_{Z_Y} \mathcal{Z}]$ is never the trivial class, since $d < t_Y/[\mathcal{Z} : Z_Y]$.

If X is a subalgebra of Y, then so is $X \otimes_{Z_X} \mathcal{Z}$. Hence $t_{X\otimes\mathcal{Z}} = t_X$. By Proposition 1.1.10, $\frac{t_Y}{[\mathcal{Z}:Z_Y]t_X}$ is the Schur index of the centralizer of X in Y, which in particular is coprime to t_X. □

CHAPTER 3

Local conditions for endomorphism algebras

Let A be an abelian variety defined over a number field k, let v be a prime of good reduction for A, and denote by A_v the reduction of A modulo v. In this chapter we explore some consequences of Theorem 2.3.2 applied to the embedding of $\mathbb{Q}$-algebras $\mathrm{End}^0(A) \to \mathrm{End}^0(A_v)$ given by reduction modulo v. We focus on the particular case that $\mathrm{End}^0(A)$ is noncommutative. The structure of $\mathrm{End}^0(A_v)$ is well-known from Honda–Tate theory, and we aim to relate the invariants at places over p_v for both endomorphism algebras.

We begin in Section 3.1 by recalling some facts about $\mathrm{End}^0(B)$ for an abelian variety B defined over a finite field $\mathbb{F}_q$. After proving some generalities about $\mathrm{End}^0(B)$ assuming it contains a noncommutative algebra in Section 3.2, we study the problem of determining whether a quaternion algebra D admits an embedding $D \to \mathrm{End}^0(B)$ in Section 3.3. We give a complete answer to this problem when B is an abelian fourfold in Section 3.4.

In Section 3.5 we give an application to the global case. We show that if $\mathrm{End}^0(A)$ is noncommutative, then A_v is split modulo all but finitely many primes v of k. We also study the possible places of simple reduction in Section 3.5.1. The local conditions give the possible isotypical reductions of a fourfold with quaternionic multiplication. We give an example of a QM abelian fourfold with two primes of geometrically simple reduction.

3.1. Preliminaries

Let p be a prime and let $\mathbb{F}_q$ be the finite field with $q = p^d$ elements. Let B be an abelian variety of dimension g defined over $\mathbb{F}_q$. The Frobenius automorphism $x \mapsto x^q$ of $\bar{\mathbb{F}}_q/\mathbb{F}_q$ induces an endomorphism of B which we denote by π_B, or by π when there is no confusion. Let $L_B(T)$ be the characteristic polynomial of π_B. By [**Tat66**, Proposition 2], for any $\ell \neq p$ there is an isomorphism

$$\mathrm{End}(B) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \simeq \mathrm{End}_{G_{\mathbb{F}_q}}(V_\ell(B)),$$

where $V_\ell(V)$ is the ℓ-adic Tate module of B. The fact that $\dim_{\mathbb{Q}_\ell} V_\ell(B) = 2g$ implies $\deg L_B(T) = 2g$. We factor L_B as a product of powers of irreducible polynomials over $\mathbb{Q}$,

$$L_B(T) = \prod P(T)^{a(P)},$$

and define the invariant $r(L_B) = \sum_P a(P)^2 \deg P$. Tate shows [**Tat66**, Theorem 1] that

$$\mathrm{rank}_{\mathbb{Z}} \mathrm{End}(B) = r(L_B).$$

The properties of $\mathrm{End}^0(B) = \mathrm{End}(B) \otimes \mathbb{Q}$ in relation to π_B are explained in [**Tat66**, Theorem 2], which we state here for convenience.

Theorem 3.1.1 (Tate)**.**

(a) The algebra $\mathbb{Q}[\pi]$ is the center of the semisimple algebra $\mathrm{End}^0(B)$.
(b) We have $2g \le \dim_{\mathbb{Q}} \mathrm{End}^0(B) = r(L_B) \le (2g)^2$.
(c) The following statements are equivalent:
  (c1) $\dim_{\mathbb{Q}} \mathrm{End}^0(B) = 2g$.
  (c2) $L_B(T)$ has no multiple root.
  (c3) $\mathrm{End}^0(B) = \mathbb{Q}[\pi]$.
  (c4) $\mathrm{End}^0(B)$ is commutative.
(d) The following statements are equivalent:
  (d1) $\dim_{\mathbb{Q}} \mathrm{End}^0(B) = (2g)^2$.
  (d2) $L_B(T)$ is a power of a linear polynomial.
  (d3) $\mathbb{Q}[\pi] = \mathbb{Q}$.
  (d4) $\mathrm{End}^0(B) \simeq \mathrm{M}_g(D_p)$, where D_p is the quaternion algebra over $\mathbb{Q}$ ramified at p and infinity.
  (d5) $B \sim E^g$, where E is a supersingular elliptic curve whose endomorphisms are all defined over $\mathbb{F}_q$.
(e) B is $\mathbb{F}_q$-isogenous to a power of a $\mathbb{F}_q$-simple abelian variety if and only if $L_B(T)$ is a power of a $\mathbb{Q}$-irreducible polynomial $P(T)$. When this is the case, $\mathbb{Q}(\pi)$ is a field, and $\mathrm{End}^0(B)$ is a central simple algebra over $\mathbb{Q}(\pi)$ which splits at all finite primes v of $\mathbb{Q}(\pi)$ not dividing p, and has invariant $\frac{1}{2}$ at every real prime of $\mathbb{Q}(\pi)$. At primes $\mathfrak{p} \mid p$, the invariant is

$$\mathrm{inv}_{\mathfrak{p}}[\mathrm{End}^0(B)] \equiv \frac{\mathrm{ord}_{\mathfrak{p}}(\pi) \cdot [\mathbb{Q}(\pi)_{\mathfrak{p}} : \mathbb{Q}_p]}{\mathrm{ord}_{\mathfrak{p}}(q)} \pmod{\mathbb{Z}}.$$

Suppose now that $L_B(T) = P(T)^m$ with $P(T)$ irreducible in $\mathbb{Q}[T]$, which corresponds to B being $\mathbb{F}_q$-isogenous to the rth power of a simple abelian variety for some $r \mid m$ (we also say B is *isotypical*). Then, $\mathbb{Q}(\pi)$ is the field $\mathbb{Q}[T]/(P(T))$, and we have $\dim_{\mathbb{Q}} \mathrm{End}^0(B) = m^2 \deg P$. Hence we have

$$\dim_{\mathbb{Q}(\pi)} \mathrm{End}^0(B) = m^2 = \left(\frac{2g}{\deg P(T)}\right)^2 = \left(\frac{2g}{[\mathbb{Q}(\pi) : \mathbb{Q}]}\right)^2. \tag{3.1}$$

In particular, the maximal subfields M in $\mathrm{End}^0(B)$ satisfy $[M : \mathbb{Q}(\pi)] = 2g/[\mathbb{Q}(\pi) : \mathbb{Q}]$, equivalently, $[M : \mathbb{Q}] = 2g$.

Recall that an elliptic curve $E/\mathbb{F}_q$ is called supersingular if the group scheme $E[p]$ has no $\bar{\mathbb{F}}_q$-points other than 0. More generally, we say an abelian variety $B/\mathbb{F}_q$ is supersingular if it is $\bar{\mathbb{F}}_q$-isogenous to a product of supersingular elliptic curves.

Proposition 3.1.2. *For an abelian variety B defined over $\mathbb{F}_q$, the following are equivalent:*

(1) B is supersingular.
(2) There is a root of unity ζ such that $\pi = \zeta\sqrt{q}$.
(3) The ideals (π^2) and (q) coincide.
(4) The ideals (π) and $(\bar{\pi})$ coincide.

Proof. These characterizations are well-known. The proof follows from considering the Frobenius endomorphism of a supersingular elliptic curve, plus the facts that $\pi\bar{\pi} = q$ and $|\pi|_{\mathbb{C}} = \sqrt{q}$. For further reference, see e.g. [**Gon98**] and [**Yu13b**, Theorem 2.9]. □

By Albert's classification (cf. Theorem 1.4.1), $\mathbb{Q}(\pi)$ is either a totally real or a CM number field.

Lemma 3.1.3. *If $\mathbb{Q}(\pi)$ is a totally real field, then it equals $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{p})$ whenever q is an even or an odd power of p, respectively. If moreover B is simple, then:*

- *$\mathbb{Q}(\pi) = \mathbb{Q}$ if and only if B is a supersingular elliptic curve.*
- *$\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{p})$ if and only if B is a supersingular abelian surface. In that case, $\mathrm{End}^0(B)$ is the quaternion algebra over $\mathbb{Q}(\sqrt{p})$ ramified exactly at the two infinite places.*

Proof. By the Weil conjectures, we have $|\pi| = \sqrt{q}$ for every archimedean absolute value $|\cdot|$ of $\mathbb{Q}(\pi)$. Hence if $\mathbb{Q}(\pi)$ is totally real we have $\pi^2 = q$, so B is supersingular. Hence $\mathbb{Q}(\pi)$ equals $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{p})$ when q is an even or odd power of p.

By Theorem 3.1.1 we know that $\mathbb{Q}(\pi) = \mathbb{Q}$ if and only if B is a supersingular elliptic curve. Hence if B is a simple abelian surface with $\mathbb{Q}(\pi)$ totally real, this must equal $\mathbb{Q}(\sqrt{p})$. Conversely, suppose that $\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{p})$. By Theorem 3.1.1 we know that $\mathrm{End}^0(B)$ ramifies at the infinite places, and possibly at some place over p. In particular we have

$$\mathrm{inv}_{\infty_i}[\mathrm{End}^0(B)] = \frac{1}{2} \bmod \mathbb{Z},\ i = 1, 2$$

for both embeddings $\infty_1, \infty_2 : \mathbb{Q}(\sqrt{p}) \to \mathbb{R}$. Since p ramifies in $\mathbb{Q}(\sqrt{p})$, and the local invariants of the algebra $\mathrm{End}^0(B)$ sum to an integer, we must have

$$\mathrm{inv}_p[\mathrm{End}^0(B)] = 0 \bmod \mathbb{Z}.$$

It follows that $\mathrm{End}^0(B)$ is a quaternion algebra over $\mathbb{Q}(\sqrt{p})$, and hence its maximal fields have degree $2 \dim B = 4$ over $\mathbb{Q}$. Hence B must be a surface. In addition, the Frobenius endomorphism of $B_{\mathbb{F}_{q^2}}$ is $\pi^2 = q$, which gives the center $\mathbb{Q}$. Hence $B_{\mathbb{F}_{q^2}}$ is isogenous to the square of a supersingular elliptic curve. □

As a direct consequence of the previous lemma, we obtain the following fact.

Corollary 3.1.4. *Suppose that $B/\mathbb{F}_q$ is simple and $\dim B \geq 3$. Then $\mathbb{Q}(\pi)$ is a CM field.*

We will occasionally be interested in the p-rank of B, which is defined as

$$f(B) := \dim_{\mathbb{F}_p} \mathrm{Hom}(\mu_p, B[p]),$$

where μ_p is the group scheme of pth roots of unity. Recall (e.g. from [**Mum08**, §15]) that $f(B)$ satisfies $0 \leq f(B) \leq g$ and $|B[p^n](\bar{\mathbb{F}}_q)| = p^{n \cdot f(B)}$. The number $f(B)$ is an isogeny invariant and is invariant under base change. When $f(B) = g$, we say B is *ordinary*. Supersingular varieties have p-rank zero, but the converse is only true for $\dim B \leq 2$.

3.2. Noncommutative endomorphisms over finite fields

Let B be an abelian variety $\mathbb{F}_q$. In this section, we state some general facts about the endomorphism algebra $\mathrm{End}^0(B)$ assuming it is noncommutative.

We have seen that in Lemma 3.1.3 that B is a (power of a) simple surface with quaternionic multiplication when $\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{p})$. For completeness, we list all possibilities of noncommutative algebras of simple abelian surfaces.

Proposition 3.2.1. *Let B be a simple abelian surface over a finite field $\mathbb{F}_q$ of characteristic p. Let $Y = \mathrm{End}^0(B)$ and let $\mathbb{Q}(\pi)$ be the center of Y. If Y is noncommutative, then B is supersingular, and one of the following is true:*

(1) $\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{p})$, Y is the unique quaternion algebra over $\mathbb{Q}(\pi)$ ramified at both infinite places, and d is odd.
(2) $\mathbb{Q}(\pi)$ is a quadratic imaginary field where p splits, Y is the quaternion algebra over $\mathbb{Q}(\pi)$ ramified at both places over p, d is even, and
   a. $p \equiv 1 \pmod 4$, $\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{-1})$, and π is a root of $T^2 + p^d$,
   b. $p \equiv 1 \pmod 3$, $\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{-3})$, and π is a root of $T^2 \pm p^{d/2}T + p^d$.

Proof. See the Remark in [**Oor88**, p. 487]. □

The following result due to Waterhouse (cf. [**Wat69**, Theorem 6.1]) explains the relation between the degree of $\mathbb{F}_q/\mathbb{F}_p$ and the Schur index of $\mathrm{End}^0(B)$.

Proposition 3.2.2 (after Waterhouse)**.** *Let B be a simple abelian variety defined over $\mathbb{F}_q$. If $\mathbb{Q}(\pi)$ is a CM field and t_B denotes the Schur index of $\mathrm{End}^0(B)$, then t_B divides $d = [\mathbb{F}_q : \mathbb{F}_p]$.*

In the particular case where $d = 1$ and B is defined over $\mathbb{F}_p$, we deduce that $\mathrm{End}^0(B) = \mathbb{Q}(\pi)$.

Proof. By Theorem 3.1.1, $\mathrm{End}^0(B)$ can only ramify at primes of $\mathbb{Q}(\pi)$ over p. Let $\mathfrak{p} \mid p$, we let $[\mathbb{Q}(\pi)_\mathfrak{p} : \mathbb{Q}_p] = e_\mathfrak{p} f_\mathfrak{p}$ so that $e_\mathfrak{p}$ is the ramification degree of $\mathfrak{p}$ over p. We have the formula

$$\mathrm{inv}_\mathfrak{p}[\mathrm{End}^0(B)] \equiv \frac{\mathrm{ord}_\mathfrak{p}(\pi) \cdot e_\mathfrak{p} f_\mathfrak{p}}{\mathrm{ord}_\mathfrak{p}(p^d)} = \frac{\mathrm{ord}_\mathfrak{p}(\pi) \cdot e_\mathfrak{p} f_\mathfrak{p}}{d e_\mathfrak{p}} = \frac{\mathrm{ord}_\mathfrak{p}(\pi) \cdot f_\mathfrak{p}}{d} \pmod{\mathbb{Z}}.$$

Since $\mathrm{ord}_{\mathbb{Q}(\pi)}[\mathrm{End}^0(B)]$ divides $\mathrm{ord}_{\mathbb{Q}(\pi)_\mathfrak{p}}[\mathrm{End}^0(B)]$, and the latter divides d, the statement follows. □

We start our investigation of subalgebras of $\mathrm{End}^0(B)$. We first show some relations between the Schur index and the dimension of B.

Proposition 3.2.3. *Let $q = p^d$, $B = \prod_i B_i^{r_i}$ be an abelian variety over $\mathbb{F}_q$ with each B_i simple and $B_i \not\sim B_j$ for $i \neq j$. Let Z be a number field and let X be a central simple Z-algebra. Suppose there exists an embedding of $\mathbb{Q}$-algebras $\varphi : X \to \mathrm{End}^0(B)$. Let t_X denote the Schur index of X and let π_i be the Frobenius endomorphism of B_i. We have the following properties.*

(a) The characteristic polynomial of the Frobenius endomorphism of B is of the form $P(T)^{t_X}$ with $P(T) \in \mathbb{Z}[T]$.
(b) The relation $t_X[Z : \mathbb{Q}] \mid 2 \dim B$ holds.
(c) If Z is totally real and all the fields $\mathbb{Q}(\pi_i)$ are CM, then $t_X[Z : \mathbb{Q}] \mid \dim B$.

Proof. Since $\mathrm{End}^0(B) \simeq \prod_i \mathrm{M}_{r_i}(\mathrm{End}^0(B_i))$, the embedding φ is a product of embeddings $\varphi_i : X \to \mathrm{M}_{r_i}(\mathrm{End}^0(B_i))$. By Proposition 2.2.6, there exist primitive embeddings

$$\psi_{ij} : X \to \mathrm{M}_{s_{ij}}(\mathrm{End}^0(B_i))$$

such that $\sum_j s_{ij} = r_i$ and $\varphi_i = \prod_j \psi_{ij}$. Let π_i be the Frobenius endomorphism of B_i and let t_i be the Schur index of $\mathrm{End}^0(B_i)$. Let F_{ij} be fields such that $Z \otimes_\mathbb{Q} \mathbb{Q}(\pi_i) \simeq F_{i1} \times \cdots \times F_{ik}$. Then by Proposition 2.3.2 we know that $t_X[F_{ij} : \mathbb{Q}(\pi_i)]$ divides $s_{ij} t_i$, and hence t_X divides $r_i t_i$. By Tate's theorem, it follows that the

characteristic polynomial of Frobenius of $B_i^{r_i}$ is a t_Xth power in $\mathbb{Z}[T]$, and (a) follows. For (b), we multiply the divisibility relation by $[\mathbb{Q}(\pi_i):\mathbb{Q}]$ to obtain

$$t_X[F_{ij}:Z][Z:\mathbb{Q}] \mid r_i t_i[\mathbb{Q}(\pi_i):\mathbb{Q}] = 2r_i \dim B_i.$$

Hence $t_X[Z:\mathbb{Q}] \mid \sum_i 2r_i \dim B_i = 2\dim B$. For (c), we note that since Z is totally real and $\mathbb{Q}(\pi_i)$ is CM, we necessarily have $[F_{ij}:Z]$ even. Hence we obtain $2t_X[Z:\mathbb{Q}] \mid 2\dim B$, which yields the result. □

3.3. Quaternionic multiplication over finite fields

For this section we fix a prime p, a finite field $\mathbb{F}_q$ with $q = p^d$, and an isotypical abelian variety $B = (B')^r$ defined over $\mathbb{F}_q$ and of dimension $g = \dim B$. We let $Y' = \mathrm{End}^0(B')$ and $Y = \mathrm{M}_r(Y') = \mathrm{End}^0(B)$. We also let t_B be the Schur index of $[Y] = [Y']$ in $\mathrm{Br}(\mathbb{Q}(\pi))$. Consider the following variation on Oort's problem [**Oor88**] (cf. [**Yu13b**], where the case $\dim B = 2$ is treated).

Problem 3.3.1. *Let F be a totally real number field and D a division quaternion algebra with center F. Give necessary and sufficient conditions in order to have an embedding $D \to Y$.*

We separate Problem 3.3.1 in two: first, the center F should be a subalgebra of Y; second, an embedding $F \to Y$ should extend to an embedding $D \to Y$. The first is solved easily by the numerical conditions described in the previous chapter. By specializing Theorem 2.3.2, we have the following criterion.

Let X and Y be simple algebras with respective centers Z_X and Z_Y. Recall from Definition 2.2.1 that an embedding $\phi : X \to Y$ is said to be primitive if the subalgebra of Y generated by $\phi(Z_X)$ and Z_Y is a field.

Proposition 3.3.2. *Consider the decomposition $F \otimes_{\mathbb{Q}} \mathbb{Q}(\pi) \simeq F_1 \times \cdots \times F_s$. Then, there exists an embedding of $\mathbb{Q}$-algebras $\iota : F \to Y = \mathrm{M}_r(Y')$ if and only if there exist nonnegative integers $r_1, \ldots, r_s$ such that*

(1) $\sum_i^s r_i = r$, and
(2) For each i such that $r_i > 0$, $[F_i : \mathbb{Q}(\pi)]$ divides $r_i t_B$, and the class of $[Y \otimes_{\mathbb{Q}(\pi)} F_i]$ in $\mathrm{Br}(\mathbb{Q}(\pi))$ has order dividing $r_i t_B / [F_i : \mathbb{Q}(\pi)]$.

The embedding ι is primitive if and only if $r = r_{i_0} > 0$ for some index i_0. □

For the rest of the section we will assume that F is a $\mathbb{Q}$-subalgebra of Y. In addition to the assumption that F is totally real, we know that the center $\mathbb{Q}(\pi)$ of Y is either a totally real or a CM field. Moreover, we have certain divisibility relations.

Lemma 3.3.3. *Suppose that there is an embedding $D \to Y$ and $\mathbb{Q}(\pi)$ is a CM field. Then $[\mathbb{Q}(\pi):\mathbb{Q}] \mid g$ and $[F:\mathbb{Q}] \mid \frac{g}{2}$.*

Proof. The first relation is Proposition 3.2.3(a), and the second is Proposition 3.2.3(c). □

The rest of the section is organised as follows. We begin by solving Problem 3.3.1 whenever $\mathbb{Q}(\pi)$ is a totally real field. Then, we solve it for the two maximal cases in Lemma 3.3.3 assuming $\mathbb{Q}(\pi)$ is a CM field. Namely, we first treat the case $[\mathbb{Q}(\pi):\mathbb{Q}] = g$, and then the case where $[F:\mathbb{Q}] = g/2$. We will give the complete solution for the case $g = 4$ in Section 3.4. In the specific case of fourfolds, we are in some instances able to compute the p-rank of B, as well as some information about $\mathbb{Q}(\pi)$ and Y.

3.3.1. $\mathbb{Q}(\pi)$ totally real. We denote by D_p the unique quaternion algebra over $\mathbb{Q}$ ramified at p and infinity. We denote by D_∞ the unique quaternion algebra over $\mathbb{Q}(\sqrt{p})$ ramified at both infinite places. Throughout this section, $E/\mathbb{F}_q$ denotes a suitable supersingular elliptic curve with $\mathrm{End}^0(E) = D_p$, and S denotes a supersingular surface with $\mathrm{End}^0(S) = D_\infty$.

Recall from Lemma 3.1.3 that, if $\mathbb{Q}(\pi)$ is totally real, then we either have $\mathbb{Q}(\pi) = \mathbb{Q}$ or $\mathbb{Q}(\sqrt{p})$. The first case then corresponds to $B \sim E^g$, and $Y = \mathrm{M}_g(D_p)$. The second case corresponds to $B \sim S^{g/2}$, with $Y = \mathrm{M}_{g/2}(D_\infty)$.

Fix embeddings $F \to \bar{\mathbb{Q}}$ and $\mathbb{Q}(\pi) \to \bar{\mathbb{Q}}$. We let $F(\pi)$ be the compositum of F and $\mathbb{Q}(\pi)$ in this common algebraic closure. The algebras D_p and D_∞ are ramified at the real places of $\mathbb{Q}(\pi)$. Since $F(\pi)$ is totally real, the real places of $\mathbb{Q}(\pi)$ do not ramify in $F(\pi)$, and so $D_p \otimes_{\mathbb{Q}(\pi)} F(\pi)$ and $D_\infty \otimes_{\mathbb{Q}(\pi)} F(\pi)$ remain ramified at infinity. In particular, they are both quaternion division algebras over $F(\pi)$.

Recall that D is said to be definite at a place $F \hookrightarrow \mathbb{R}$ if $D \otimes_F \mathbb{R}$ is isomorphic to the Hamilton quaternions, otherwise we say D splits at that place. We say D is totally definite if it is definite for every place $F \hookrightarrow \mathbb{R}$.

Proposition 3.3.4. *Suppose that D splits at some infinite place of F. Then, there exists an embedding $D \to Y$ if and only if one of the following happens:*

(1) $B \sim E^g$, $Y = \mathrm{M}_g(D_p)$, and $2[F:\mathbb{Q}] \mid g$.
(2) $B \sim S^{g/2}$, $Y = \mathrm{M}_{g/2}(D_\infty)$, and either:
  (a) $\sqrt{p} \in F$, and $2[F:\mathbb{Q}] \mid g$; or
  (b) $\sqrt{p} \notin F$, and $4[F:\mathbb{Q}] \mid g$.

Suppose instead that D is totally definite. Then, there exists an embedding $D \to Y$ if and only if one of the following happens:

(3) $B \sim E^g$, $Y = \mathrm{M}_g(D_p)$, and either $2[F:\mathbb{Q}] \mid g$, or $[F:\mathbb{Q}] \mid g$ and
$$[D] = [D_p \otimes_{\mathbb{Q}} F] \text{ in } \mathrm{Br}(F).$$
(4) $B \sim S^{g/2}$, $Y = \mathrm{M}_{g/2}(D_\infty)$, and either:
  (a) $\sqrt{p} \in F$, and either $2[F:\mathbb{Q}] \mid g$, or $[F:\mathbb{Q}] \mid g$ and $[D] = [D_\infty \otimes_{\mathbb{Q}(\sqrt{p})} F]$ in $\mathrm{Br}(F)$ (i.e., $\mathrm{Ram}(D)$ equals the set of infinite places of F);
  (b) $\sqrt{p} \notin F$, and either $4[F:\mathbb{Q}] \mid g$, or $2[F:\mathbb{Q}] \mid g$ and
$$[D \otimes_F F(\sqrt{p})] = [D_\infty \otimes_{\mathbb{Q}(\sqrt{p})} F(\sqrt{p})] \text{ in } \mathrm{Br}(F(\sqrt{p})).$$

Proof. Consider the intersection $F \cap \mathbb{Q}(\pi)$ inside of Y. Since $\mathbb{Q}(\pi)/F \cap \mathbb{Q}(\pi)$ is an extension of degree at most 2, by Theorem 2.4.2 there must exist an embedding $\iota : F \to Y$ which is primitive. We will consider the necessary and sufficient conditions for ι to extend to an embedding $D \to Y$. For convenience, we let $Q = \iota(F) \cap \mathbb{Q}(\pi)$.

Let c_B, t_B be the capacity and Schur index of Y. Then we have
$$c_B t_B = \begin{cases} 2g, & \text{if } \mathbb{Q}(\pi) = \mathbb{Q}, \\ g, & \text{if } \mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{p}). \end{cases}$$
Since $\iota : F \to Y$ is a primitive embedding, by Proposition 2.3.2 we have an embedding $\tilde{\iota} : D \to Y$ extending ι if and only if $2[F(\pi):\mathbb{Q}(\pi)]$ divides $c_B t_B$, and
$$d[D \otimes_F F(\pi)] = d[Y \otimes_{\mathbb{Q}(\pi)} F(\pi)] \tag{3.2}$$
with $d = \frac{c_B t_B}{2[F(\pi):\mathbb{Q}(\pi)]}$. Now we reason by cases (a summary can be found in Table 3.3.1). If D splits at some infinite place, then (3.2) can only hold if d is even.

This yields the condition $4[F(\pi):\mathbb{Q}(\pi)] \mid c_B t_B$. Now $[F(\pi):\mathbb{Q}(\pi)] = [F:\mathbb{Q}]$ if $Q = \iota(F) \cap \mathbb{Q}(\pi) = \mathbb{Q}$, and $[F(\pi):\mathbb{Q}(\pi)] = [F:\mathbb{Q}]/2$ otherwise. Cases (1) and (2) follow.

If we suppose that D is totally definite, then (3.2) holds if d is even (recovering the condition $4[F(\pi):\mathbb{Q}(\pi)] \mid c_B t_B$ once again) or if d is odd, $2[F(\pi):\mathbb{Q}(\pi)] \mid c_B t_B$, and the equation

$$[D \otimes_F F(\pi)] = [Y \otimes_{\mathbb{Q}(\pi)} F(\pi)] \tag{3.3}$$

holds. The previous reasoning yields cases (3) and (4). □

D is totally definite?	r	$\iota(F) \cap \mathbb{Q}(\pi)$	$\mathbb{Q}(\pi)$	Conditions
no	g	$\mathbb{Q}$	$\mathbb{Q}$	$2[F:\mathbb{Q}] \mid g$
no	$g/2$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{p})$	$4[F:\mathbb{Q}] \mid g$
no	$g/2$	$\mathbb{Q}(\sqrt{p})$	$\mathbb{Q}(\sqrt{p})$	$2[F:\mathbb{Q}] \mid g$
yes	g	$\mathbb{Q}$	$\mathbb{Q}$	$2[F:\mathbb{Q}] \mid g$, or (3.3) and $[F:\mathbb{Q}] \mid g$
yes	$g/2$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{p})$	$4[F:\mathbb{Q}] \mid g$, or (3.3) and $2[F:\mathbb{Q}] \mid g$
yes	$g/2$	$\mathbb{Q}(\sqrt{p})$	$\mathbb{Q}(\sqrt{p})$	$2[F:\mathbb{Q}] \mid g$, or (3.3) and $[F:\mathbb{Q}] \mid g$

TABLE 3.1. Cases considered during the proof of Proposition 3.3.4. The integer r is such that $B \sim (B')^r$ with B' simple.

Remark 3.3.5. *The proof of Proposition 3.3.4 gives an embedding of D into Y which is always primitive. We observe that this is due to the fact that $\mathbb{Q}(\pi)/\mathbb{Q}$ is an extension of degree 1 or 2, from which one produces a primitive embedding $\iota : F \to Y$. If one starts with a different, nonprimitive embedding $\iota' : F \to Y$, it is also possible to characterize whether it extends to a nonprimitive embedding $D \to Y$.*

Remark 3.3.6. *When D splits at all infinite places of F, we say that D is totally indefinite. Then Table 1.1 says that a simple abelian variety B over $\mathbb{F}_q$ can have $\mathrm{End}^0(B) \simeq D$ with D totally indefinite only if $2[F:\mathbb{Q}] \mid g$. The similar condition $[F:\mathbb{Q}] \mid g$ appears when D is totally definite.*

The proposition above generalizes these conditions to the case of B not simple having an embedding $D \to \mathrm{End}^0(B)$.

3.3.2. $\mathbb{Q}(\pi)$ a CM field of degree g. In the remaining we consider what happens when $\mathbb{Q}(\pi)$ is a CM field. We write $\mathbb{Q}(\pi)^+$ for its maximal totally real subfield. Recall that $B \sim (B')^r$ with B' a simple abelian variety, so that $Y' = \mathrm{End}^0(B')$ is a division algebra and $Y = \mathrm{End}^0(B) = \mathrm{M}_r(Y')$. We first consider the special case where $[\mathbb{Q}(\pi):\mathbb{Q}] = g$. Fix an embedding $\iota : F \to Y$.

By Theorem 3.1.1, Y' is a division algebra that splits at all finite primes $\ell \neq p$ and ramifies at the real primes. But since $\mathbb{Q}(\pi)$ has no real primes, if Y' is not commutative then it must at least ramify at two primes of $\mathbb{Q}(\pi)$ over p. As a result of these considerations, we obtain the following two propositions.

Proposition 3.3.7. *The embedding $\iota : F \to Y$ extends to D if and only if $\iota(F) \subset \mathbb{Q}(\pi)$ and $Y \simeq D \otimes_F \mathbb{Q}(\pi)$. In that case, let $\mathfrak{l} \in \mathrm{Ram}(D)$ be over some prime $\ell \neq p$, and let $\mathfrak{L}_1, \ldots, \mathfrak{L}_s$ be the primes of $\mathbb{Q}(\pi)$ over $\mathfrak{l}$. Then $[\mathbb{Q}(\pi)_{\mathfrak{L}_i} : F_{\mathfrak{l}}]$ is even for all $i = 1, \ldots, s$.*

Proof. By Theorem 3.1.1, $[\mathbb{Q}(\pi) : \mathbb{Q}] = g$ implies that Y is a quaternion algebra over $\mathbb{Q}(\pi)$. The first statement then follows from Corollary 2.2.9. For the second, let $\mathfrak{l}$ and $\mathfrak{L}_1, \ldots, \mathfrak{L}_s$ be as above. We have $\mathrm{inv}_{\mathfrak{l}} D = \frac{1}{2}$ and $\mathrm{inv}_{\mathfrak{L}_i}(Y) = 0$. By the formula

$$\mathrm{inv}_{\mathfrak{L}_i}(Y) \equiv [\mathbb{Q}(\pi)_{\mathfrak{L}_i} : F_{\mathfrak{l}}] \cdot \mathrm{inv}_{\mathfrak{l}}(D) \pmod{\mathbb{Z}},$$

we clearly need $[\mathbb{Q}(\pi)_{\mathfrak{L}_i} : F_{\mathfrak{l}}]$ to be even. □

Proposition 3.3.8. *Suppose that there is an embedding $\iota : D \to Y$. The following are equivalent:*

1. *B is simple.*
2. *$\mathbb{Q}(\pi)$ does not split D.*
3. *There is a prime $\mathfrak{p} \in \mathrm{Ram}(D)$ dividing p and a prime $\mathfrak{P}$ in $\mathbb{Q}(\pi)$ over $\mathfrak{p}$ with $\mathfrak{P}, \bar{\mathfrak{P}} \in \mathrm{Ram}(D \otimes_F \mathbb{Q}(\pi))$ and $[\mathbb{Q}(\pi)_{\mathfrak{P}} : F_{\mathfrak{p}}]$, $[\mathbb{Q}(\pi)_{\bar{\mathfrak{P}}} : F_{\mathfrak{p}}]$ odd.*

Proof. By Proposition 3.3.7 we have $Y = D \otimes_F \mathbb{Q}(\pi)$. The variety B is simple if and only if Y is a division algebra, which happens if and only if $\mathbb{Q}(\pi)$ does not split D.

Suppose $D \otimes_F \mathbb{Q}(\pi)$ is a division algebra. Let $\bar{\cdot}$ denote complex conjugation. Then there are two primes $\mathfrak{P}, \bar{\mathfrak{P}}$ in $\mathbb{Q}(\pi)$ over p with

$$\mathrm{inv}_{\mathfrak{P}}(D \otimes_F \mathbb{Q}(\pi)) = \mathrm{inv}_{\bar{\mathfrak{P}}}(D \otimes_F \mathbb{Q}(\pi)) = \frac{1}{2}.$$

Let $\mathfrak{p} = \mathfrak{P} \cap F = \bar{\mathfrak{P}} \cap F$. Then by the formula

$$\mathrm{inv}_{\mathfrak{P}}(D \otimes_F \mathbb{Q}(\pi)) \equiv [\mathbb{Q}(\pi)_{\mathfrak{P}} : F_{\mathfrak{p}}] \cdot \mathrm{inv}_{\mathfrak{p}}(D) \pmod{\mathbb{Z}}$$

and the fact that D is a division quaternion algebra, we obtain $\mathfrak{p} \in \mathrm{Ram}(D)$ and $[\mathbb{Q}(\pi)_{\mathfrak{P}} : F_{\mathfrak{p}}] = [\mathbb{Q}(\pi)_{\bar{\mathfrak{P}}} : F_{\mathfrak{p}}]$ is odd.

Conversely, suppose that we have $\mathfrak{p}, \mathfrak{P}_1, \mathfrak{P}_2$ as in (3). Then

$$\mathrm{inv}_{\mathfrak{P}_i}(D \otimes_F \mathbb{Q}(\pi)) = [\mathbb{Q}(\pi)_{\mathfrak{P}_i} : F_{\mathfrak{p}}] \cdot \mathrm{inv}_{\mathfrak{p}}(D) = \frac{1}{2} \pmod{\mathbb{Z}},$$

so $D \otimes_F \mathbb{Q}(\pi)$ is a division algebra, and $\mathbb{Q}(\pi)$ does not split D. □

We now give a special case in which B splits geometrically.

Proposition 3.3.9. *Suppose that the following conditions are satisfied:*

1. *$[\mathbb{Q}(\pi) : \mathbb{Q}] = g$,*
2. *p splits completely in $\mathbb{Q}(\pi)$,*
3. *ι extends to D, and*
4. *D ramifies at every prime of F over p.*

Then B is supersingular.

Proof. By Proposition 3.3.8, having p split completely in $\mathbb{Q}(\pi)$ implies $\mathrm{End}^0(B) \simeq D \otimes_F \mathbb{Q}(\pi)$ ramifies at each prime $\mathfrak{P} \mid p$. In fact we know more: we have $[\mathbb{Q}(\pi)_{\mathfrak{P}} : \mathbb{Q}_p] = 1$, and by Theorem 3.1.1 then

$$\mathrm{inv}_{\mathfrak{P}}(Y) = \frac{\mathrm{ord}_{\mathfrak{P}}(\pi)}{d} \equiv \frac{1}{2} \pmod{\mathbb{Z}}.$$

But $\pi\bar{\pi} = q = p^d$, so $\mathrm{ord}_{\mathfrak{P}}(\pi) \leq d$. These observations imply $\mathrm{ord}_{\mathfrak{P}}(\pi) = d/2$ for all $\mathfrak{P} \mid p$. Hence $(\pi^2) = (p^d)$, and the result follows by Proposition 3.1.2. □

3.3.3. $[F : \mathbb{Q}] = g/2$, $\mathbb{Q}(\pi)$ **CM.** We now treat the case in which $\mathbb{Q}(\pi)$ is a CM field and $[F : \mathbb{Q}] = g/2$. As before, we let $Y = \mathrm{End}^0(B)$ and we fix an embedding $\iota : F \to Y$.

Lemma 3.3.10. *Suppose that $\iota : F \to Y$ extends to D. Then, the following properties hold.*

(1) The embedding ι is primitive.
(2) The compositum $F(\pi)$ of $\iota(F)$ and $\mathbb{Q}(\pi)$ in Y is a field of degree g.
(3) ι extends to an embedding $D \otimes_F F(\pi) \to Y$.
(4) The intersection $\iota(F) \cap \mathbb{Q}(\pi)$ is the maximal totally real field $\mathbb{Q}(\pi)^+$.

Proof. Suppose we have an embedding $\iota : D \to Y = \mathrm{M}_r(Y')$. Let $F_1, \ldots, F_s$ be fields with

$$F \otimes_{\mathbb{Q}} \mathbb{Q}(\pi) \simeq F_1 \times \cdots \times F_s.$$

By Theorem 2.3.2 there exist non-negative integers $r_1, \ldots, r_s$ with $\sum_i r_i = r$ and such that $2[F_i : \mathbb{Q}(\pi)] \mid r_i t_Y$ for all i, where t_Y is the Schur index of Y (we do not need the Brauer class equation yet). Multiplying by the degree of $\mathbb{Q}(\pi)$, we obtain the divisibility relation

$$2[F_i : \mathbb{Q}] \mid r_i t_Y [\mathbb{Q}(\pi) : \mathbb{Q}].$$

Now we note that $[F_i : \mathbb{Q}] \geq 2[F : \mathbb{Q}] = g$, since F is totally real and $\mathbb{Q}(\pi)$ is totally imaginary. Hence the left-hand side is at least $2g$ for every i. On the other hand, we have $r_i t_Y [\mathbb{Q}(\pi) : \mathbb{Q}] \leq r t_Y [\mathbb{Q}(\pi) : \mathbb{Q}] = 2g$. Hence there is a single i_0 with $r_{i_0} > 0$, which must be $r = r_{i_0}$. It follows that ι is primitive, and the compositum $F_{i_0} = F(\pi)$ of $\iota(F)$ and $\mathbb{Q}(\pi)$ has degree g. This gives (1) and (2). Since ι is primitive, Lemma 2.2.4 gives (3).

Now we have $[F(\pi) : \mathbb{Q}] = g$, and $F(\pi)$ is a CM field, since it is a quadratic totally imaginary field with maximal totally real field F. Hence, $\iota(F)$ contains the maximal totally real subfield $\mathbb{Q}(\pi)^+$ of $\mathbb{Q}(\pi)$. This proves (4). □

Remark 3.3.11. *A slightly stronger statement holds. Let $B = \prod B_i^{r_i}$ is a product of isotypical components with $\mathrm{Hom}(B_i, B_j) = 0$ for $i \neq j$, such that the center $\mathbb{Q}(\pi_i)$ of $\mathrm{End}^0(B_i^{r_i})$ is a CM field. Consider the same hypotheses on F and D and assume we have an embedding $D \to \mathrm{End}^0(B)$. We can then apply Lemma 3.3.10 to each isotypical component, and deduce that $D \to \mathrm{End}^0(B_i^{r_i})$ must be a primitive embedding. But the algebra $D \otimes_F F(\pi)$ contains maximal fields of degree $2 \dim B$, and therefore we must have $r_i \dim B_i = \dim B$. It follows that B was already isotypical.*

We are ready to state the main result of this section.

Theorem 3.3.12. *Suppose F is a totally real field with $[F : \mathbb{Q}] = g/2$ and $\mathbb{Q}(\pi)$ is a CM field. Then, $\iota : F \to Y$ extends to $D \to Y$ if and only if $\mathbb{Q}(\pi)^+ \subseteq \iota(F)$ and the equality*

$$[D \otimes_F F(\pi)] = [Y \otimes_{\mathbb{Q}(\pi)} F(\pi)]$$

holds in $\mathrm{Br}(F(\pi))$.

PROOF. We have shown in Lemma 3.3.10 above that in order to have an embedding $\iota : D \to Y$ it is necessary that ι is a primitive embedding and $\mathbb{Q}(\pi)^+ \subset \iota(F)$. Hence the existence of $D \to Y$ is equivalent to having an embedding $D \otimes_F F(\pi) \to Y$. By Proposition 2.3.1 we know that this is the case if and only if

$$d[D \otimes_F F(\pi)] = d[Y \otimes_{\mathbb{Q}(\pi)} F(\pi)]$$

in $\mathrm{Br}(F(\pi))$, where $d = \frac{rt_Y}{2[F(\pi):\mathbb{Q}(\pi)]} = \frac{rt_Y[\mathbb{Q}(\pi):\mathbb{Q}]}{2[F(\pi):\mathbb{Q}]} = 1$. This proves the statement. □

Remark 3.3.13. *This result appears in* [**AT23**, Theorem 1.3]*. In their case, F is not assumed to be totally real, which means Lemma 3.3.10 does not need to apply, and in particular B is not automatically isotypical. Instead, two isotypical components of dimension $g/2$ can occur. Moreover, if F is not totally real then the embedding $\iota : D \to Y$ is not necessarily primitive, but it can be shown that there exists an embedding if and only if a primitive embedding exists (cf. Theorem 2.4.2).*

3.4. Endomorphism algebras of fourfolds with QM

The results of Section 3.3 are enough to solve Problem 3.3.1 for fourfolds completely. Namely, we give here a classification of the endomorphism algebras that an abelian fourfold B over $\mathbb{F}_q$ with quaternionic multiplication can have. We let F be a totally real field and D a division quaternion algebra over F. We assume that F is a $\mathbb{Q}$-subalgebra of $\mathrm{End}^0(B)$, and ask ourselves whether there exists an embedding $\iota : D \to \mathrm{End}^0(B)$. We assume $B \sim (B')^r$ is isotypical, with B' simple over $\mathbb{F}_q$. The non-isotypical case has already been treated, since it can be reduced to the case of surfaces, see [**Yu13b**].

The case where $\mathbb{Q}(\pi)$ was totally real was studied in Proposition 3.3.4. Hence we restrict to $\mathbb{Q}(\pi)$ being a CM field. By Lemma 3.3.3, if there exists an embedding $D \to \mathrm{End}^0(B)$ then we have the following possibilities for F and $\mathbb{Q}(\pi)$:

i. $F = \mathbb{Q}$, and $\mathbb{Q}(\pi)$ is quadratic imaginary.
ii. $F = \mathbb{Q}$, and $\mathbb{Q}(\pi)$ is a quartic CM field.
iii. $\mathbb{Q}(\pi)$ is a quartic CM field and $F \simeq \mathbb{Q}(\pi)^+$ is its real quadratic field (cf. Lemma 3.3.10).
iv. F is a real quadratic field and $\mathbb{Q}(\pi)$ is an imaginary quadratic field.

Since $[\mathbb{Q}(\pi) : \mathbb{Q}] \leq 4$, it follows from Theorem 2.4.3 that if there is an embedding $D \to \mathrm{End}^0(B)$, then there must also exist a (possibly different) primitive embedding (cf. Definition 2.2.1). In fact, since the algebra $\mathrm{End}^0(B)$ is not too large, we can say more.

Lemma 3.4.1. *If there exists an embedding $\iota : D \to \mathrm{End}^0(B)$, then it must be primitive.*

PROOF. We reason by the cases listed above. If $F = \mathbb{Q}$ then the embedding ι is obviously primitive. If F is real quadratic and $\mathbb{Q}(\pi)$ is imaginary quadratic then they are linearly disjoint and again ι is primitive. Finally, if F is real quadratic and $\mathbb{Q}(\pi)$ is quartic CM, and ι extends to $D \to \mathrm{End}^0(B)$, then we are in the situation of Lemma 3.3.10, so that $\iota(F) \simeq \mathbb{Q}(\pi)^+ \subset \mathbb{Q}(\pi)$ and again ι is primitive. □

From now on we assume that there exists a fixed primitive embedding $\iota : F \to \mathrm{End}^0(B)$. Our goal is to characterize whether ι extends to an embedding of D into $\mathrm{End}^0(B)$.

Example 3.4.2. *Suppose $F = \mathbb{Q}$ and $B \sim E^4$ with E an elliptic curve. Then, there is always an embedding $D \to \mathrm{End}^0(B)$. In fact, $D \subset \mathrm{M}_4(\mathbb{Q})$, as can be checked either by means of Theorem 2.1.1; or by taking a maximal quadratic field M of D and realising D as a subalgebra of $\mathrm{M}_2(M) \subset \mathrm{M}_4(\mathbb{Q})$; or by considering the action of D on itself.*

Proposition 3.4.3 (Case i.)**.** *Suppose $F = \mathbb{Q}$ and $\mathbb{Q}(\pi)$ is quadratic imaginary. There exists an embedding $\iota : D \to \mathrm{End}^0(B)$ if and only if one of the following holds:*

(1) $B \sim E^4$, with E an elliptic curve.
(2) $B \sim S^2$, where S is a supersingular $\mathbb{F}_q$-simple abelian surface with $\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$, and $\mathrm{End}^0(S)$ the unique quaternion algebra over $\mathbb{Q}(\pi)$ ramified at the places above p, and $[\mathbb{F}_q : \mathbb{F}_p]$ is even.

Proof. Let $B \sim B'^r$ with B' simple. If $r = 1$ then $\mathrm{End}^0(B)$ has Schur index 4. Since $F \subset \mathbb{Q}(\pi)$, and $\frac{t_B}{t_D} = 2$ is not coprime with $t_D = 2$, Theorem 2.4.6 implies D is not a subalgebra of $\mathrm{End}^0(B)$. Hence it is necessary that $r = 2$ or 4; if $r = 4$ then B' is an elliptic curve, and ι extends to D by Example 3.4.2.

If $r = 2$ then B' is a $\mathbb{F}_q$-simple surface. Proposition 3.2.1 tells us the possible endomorphism algebras of B'. In particular, $\mathrm{End}^0(B')$ is a quaternion algebra. Now by Theorem 2.3.2, D embeds into $\mathrm{M}_2(\mathrm{End}^0(B'))$ if and only if

$$2[D \otimes_{\mathbb{Q}} \mathbb{Q}(\pi)] = 2[\mathrm{End}^0(B')] = [\mathbb{Q}(\pi)].$$

Since $2[D] = [\mathbb{Q}]$, this condition is always satisfied, and the case $r = 2$ is always possible. □

Proposition 3.4.4 (Cases ii. and iii.)**.** *Suppose $\mathbb{Q}(\pi)$ is quartic CM. Then ι extends to $D \to \mathrm{End}^0(B)$ if and only if*

$$\iota(F) \subset \mathbb{Q}(\pi) \text{ and } \mathrm{End}^0(B) \simeq D \otimes_F \mathbb{Q}(\pi).$$

In that case, B is simple if and only if D ramifies at a prime over p and $\mathbb{Q}(\pi)$ does not split D. Otherwise, $B \sim S^2$ for a simple surface S with $\mathrm{End}^0(S) = \mathbb{Q}(\pi)$.

Proof. This follows from Propositions 3.3.7 and 3.3.8. □

Proposition 3.4.5 (Case iv.)**.** *Suppose F is real quadratic and $\mathbb{Q}(\pi)$ is imaginary quadratic. Then ι extends to $D \to \mathrm{End}^0(B)$ if and only if one of the following happens:*

(1) $B \sim E^4$, with E an elliptic curve with $\mathrm{End}^0(E) = \mathbb{Q}(\pi)$, and $F(\pi)$ splits D. If in addition D ramifies at a prime over p, then E is supersingular.
(2) $B \sim S^2$, with S a supersingular $\mathbb{F}_q$-simple abelian surface with $\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$, $\mathrm{End}^0(S)$ the unique quaternion algebra over $\mathbb{Q}(\pi)$ ramified at the places above p, $[\mathbb{F}_q : \mathbb{F}_p]$ is even, and

$$[D \otimes_F F(\pi)] = [\mathrm{End}^0(S) \otimes_{\mathbb{Q}(\pi)} F(\pi)] \text{ in } \mathrm{Br}(F(\pi)).$$

(3) B is geometrically simple, has p-rank 0, and $\mathrm{End}^0(B)$ is a degree-4 division algebra over $\mathbb{Q}(\pi)$, such that

$$[D \otimes_F F(\pi)] = [\mathrm{End}^0(B) \otimes_{\mathbb{Q}(\pi)} F(\pi)] \text{ in } \mathrm{Br}(F(\pi)).$$

In particular, $[\mathbb{F}_q : \mathbb{F}_p]$ is a multiple of 4 and B is not supersingular. The prime p does not split in F, and D ramifies at p.

PROOF. Since $\mathbb{Q}(\pi)$ is quadratic, we have $\mathbb{Q}(\pi)^+ = \mathbb{Q}$. Theorem 3.3.12 says that D embeds into $\mathrm{End}^0(B)$ if and only if

$$[D \otimes_F F(\pi)] = [\mathrm{End}^0(B) \otimes_{\mathbb{Q}(\pi)} F(\pi)]$$

in $\mathrm{Br}(F(\pi))$. Let $B \sim (B')^r$ with B' simple. If $r = 4$, then $B \sim E^4$ with E an elliptic curve, so that $[\mathrm{End}^0(B)] = [\mathbb{Q}(\pi)]$, which yields the condition that $F(\pi)$ splits D. If D ramifies at a prime over p, then it must be the case that p is not split in $\mathbb{Q}(\pi)$. If we let $\mathfrak{p} \mid p$ in $\mathbb{Q}(\pi)$, then $\bar{\mathfrak{p}} = \mathfrak{p}$ and so $\pi = \bar{\pi}$. Proposition 3.1.2 implies E is supersingular.

If $r = 2$, then $B \sim S^2$ is the square of a simple surface. Proposition 3.2.1 gives the only possibilities for $\mathrm{End}^0(S)$.

Suppose $r = 1$ so that B is simple. Since $\mathrm{End}^0(B)$ contains a maximal field M of degree 4 over $\mathbb{Q}(\pi)$, it is indeed a division algebra of Schur index 4 (cf. Section 3.1). By [**Gon98**, 3.2], the degree of $\mathrm{End}^0(B)$ divides the p-rank $f(B)$ of B, so $f(B) = 0$ or 4. But if $f(B) = 4$ then $\mathrm{End}^0(B)$ would be a field [**Gon98**, 3.6], which is a contradiction. Hence B has p-rank 0. If B is not geometrically simple, then over $\bar{\mathbb{F}}_p$ it is isogenous to a power of a curve or a surface having p-rank 0, and hence it is supersingular. Hence $B_{\bar{\mathbb{F}}_q} \sim E^4$, with E a supersingular elliptic curve with endomorphism algebra D_p. But this is not possible, because Proposition 2.3.1 imposes the condition $[\mathrm{End}^0(B)] = [D_p \otimes_{\mathbb{Q}} \mathbb{Q}(\pi)]$, which does not hold.

Therefore B is geometrically simple, and in it is particular not supersingular. It remains to show that p is nonsplit in F and that D ramifies at p. Because $\mathrm{End}^0(B)$ is a division algebra, p has to split in $\mathbb{Q}(\pi)$, say as $\mathfrak{p}\bar{\mathfrak{p}}$, and (possibly after exchanging $\mathfrak{p}, \bar{\mathfrak{p}}$) we have

$$\mathrm{inv}_{\mathfrak{p}}(\mathrm{End}^0(B)) = \frac{1}{4}, \quad \mathrm{inv}_{\bar{\mathfrak{p}}}(\mathrm{End}^0(B)) = \frac{3}{4}.$$

Let $\mathfrak{P}$ be a place of $F(\pi)$ over $\mathfrak{p}$, and let $\mathfrak{q} = \mathfrak{P} \cap F$. Then, by the equality of classes in $\mathrm{Br}(F(\pi))$ we have

$$\begin{aligned}[F(\pi)_{\mathfrak{P}} : F_{\mathfrak{q}}] \cdot \mathrm{inv}_{\mathfrak{q}}(D) \equiv \mathrm{inv}_{\mathfrak{P}}(D \otimes_F F(\pi)) &\equiv \mathrm{inv}_{\mathfrak{P}}(\mathrm{End}^0(B) \otimes_{\mathbb{Q}(\pi)} F(\pi)) \\ &\equiv [F(\pi)_{\mathfrak{P}} : \mathbb{Q}(\pi)_{\mathfrak{p}}] \cdot \mathrm{inv}_{\mathfrak{p}}(\mathrm{End}^0(B)) \pmod{\mathbb{Z}}.\end{aligned}$$

Modulo integers, we can only have $\mathrm{inv}_{\mathfrak{P}}(D \otimes_F F(\pi)) = 0$ or $1/2$. But since $\mathrm{inv}_{\mathfrak{p}}(\mathrm{End}^0(B)) = 1/4$, for $\mathrm{inv}_{\mathfrak{P}}(\mathrm{End}^0(B) \otimes_{\mathbb{Q}(\pi)} F(\pi))$ to equal 0 we would need $[F(\pi)_{\mathfrak{P}} : \mathbb{Q}(\pi)_{\mathfrak{p}}] = 4$, which is impossible since $[F(\pi) : \mathbb{Q}(\pi)] = 2$. Hence

$$\mathrm{inv}_{\mathfrak{P}}(\mathrm{End}^0(B) \otimes_{\mathbb{Q}(\pi)} F(\pi)) = 1/2,$$

and therefore $[F(\pi)_{\mathfrak{P}} : \mathbb{Q}(\pi)_{\mathfrak{p}}] = 2$. Hence $[F(\pi)_{\mathfrak{P}} : \mathbb{Q}_p] = 2$. This implies that p is nonsplit in F, otherwise, p would split completely in $F(\pi)$. Finally, $\mathrm{inv}_{\mathfrak{P}}(D \otimes_F F(\pi)) = 1/2$ requires D to be ramified at p. □

Example 3.4.6. *Let us give examples of the geometrically simple fourfolds appearing in case (3) in Proposition 3.4.5 over several $\mathbb{F}_q$.*

- *Over $\mathbb{F}_{2^4}$, we can take B to have characteristic polynomial of Frobenius $(T^2 - 6T + 16)^4$.*
- *Over $\mathbb{F}_{3^4}$, we take the polynomial $(T^2 - 15T + 81)^4$.*
- *Over $\mathbb{F}_{5^4}$, we take the polynomial $(T^2 - 45T + 625)^4$.*
- *Over $\mathbb{F}_{7^4}$, we take the polynomial $(T^2 - 91T + 2401)^4$.*

Other examples can be computed by searching through quadratic Weil polynomials with independent term $q = p^4$.

Finally, we summarize the situation when $F = \mathbb{Q}$.

Theorem 3.4.7. *Let D be a quaternion algebra over $\mathbb{Q}$, and let B be an isotypic abelian fourfold over a finite field $\mathbb{F}_q$ of characteristic p with $\mathbb{Q}(\pi)$ a CM field. There exists an embedding $\iota : D \to \mathrm{End}^0(B)$ if and only if one of the following happens:*

(1) B is isogenous to E^4, where E is an elliptic curve.
(2) B is isogenous to the square of a simple surface S, with either
  a. $\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$, $\mathrm{End}^0(S)$ is a quaternion algebra, $D \otimes_{\mathbb{Q}} \mathbb{Q}(\pi) \simeq \mathrm{End}^0(S)$, and $[\mathbb{F}_q : \mathbb{F}_p]$ is even.
  b. $\mathrm{End}^0(S) = \mathbb{Q}(\pi)$ a quartic CM field that splits D. If in addition D ramifies at p, then S is ordinary or supersingular.
(3) B is a supersingular simple fourfold, $\mathbb{Q}(\pi)$ is a quartic CM field, $\mathrm{End}^0(B) \simeq D \otimes_{\mathbb{Q}} \mathbb{Q}(\pi)$, and D ramifies at p.

Proof. Case (1) is Example 3.4.2. Case (2a) comes from Proposition 3.4.3. Finally, cases (2b) and (3) are the two possibilities from Proposition 3.4.4.

Suppose that we are in case (2b) and D ramifies at p. Suppose that the p-rank $f(S)$ is not 0, we want to discard the possibility that $f(S) = 1$. Since $f(S) \geq 1$, $S_{\bar{\mathbb{F}}_q}$ is either simple or the square of an elliptic curve: if it was the product of nonisogenous elliptic curves, then at least one of them would be ordinary with quadratic endomorphism ring, where the quartic field $\mathbb{Q}(\pi)$ cannot embed. Hence it remains to see that if S is geometrically simple, then $f(S) = 2$. In that case we have $\mathrm{End}^0(S_{\bar{\mathbb{F}}_q}) = \mathbb{Q}(\pi)$. By Proposition 3.3.8 every prime $\mathfrak{p} \mid p$ of $\mathbb{Q}(\pi)$ satisfies that the degree $[\mathbb{Q}(\pi)_{\mathfrak{p}} : \mathbb{Q}_p]$ is even. The proof of [**Gon98**, Theorem 3.7] shows that $f(S) = 2$.

In case (3), it remains to show that B is supersingular. Suppose then that B is a simple fourfold, $\mathbb{Q}(\pi)$ is a quartic CM field, $\mathrm{End}^0(B) = D \otimes_{\mathbb{Q}} \mathbb{Q}(\pi)$, and D ramifies at p. If the prime p splits completely in $\mathbb{Q}(\pi)$, then B is supersingular by Proposition 3.3.9.

Suppose p does not split completely in $\mathbb{Q}(\pi)$. Since we are assuming B is simple, $\mathrm{End}^0(B)$ is a division quaternion algebra, and by Theorem 1.1.6 it must ramify at exactly two primes $\mathfrak{p}_1, \bar{\mathfrak{p}}_1$ of $\mathbb{Q}(\pi)$ over p, which satisfy $[\mathbb{Q}(\pi)_{\mathfrak{p}_1} : \mathbb{Q}_p] = [\mathbb{Q}(\pi)_{\bar{\mathfrak{p}}_1} : \mathbb{Q}_p] = 1$ by Proposition 3.3.8. Moreover, (p) decomposes as $\mathfrak{p}_1\bar{\mathfrak{p}}_1\mathfrak{p}_2^e$ in the ring of integers of $\mathbb{Q}(\pi)$, with $e = 1$ or 2 and the prime $\mathfrak{p}_2$ satisfying $[\mathbb{Q}(\pi)_{\mathfrak{p}_2} : \mathbb{Q}_p] = 2$ and $\bar{\mathfrak{p}}_2 = \mathfrak{p}_2$. We have $\mathrm{ord}_{\mathfrak{p}_1}(\pi) \leq \mathrm{ord}_{\mathfrak{p}_1}(\pi\bar{\pi}) = \mathrm{ord}_{\mathfrak{p}_1}(p^d) = d$ and also $\mathrm{ord}_{\bar{\mathfrak{p}}_1}(\pi) \leq d$, where $q = p^d$. On the other hand, by Theorem 3.1.1 we have

$$\frac{\mathrm{ord}_{\mathfrak{p}_1}(\pi) \cdot [\mathbb{Q}(\pi)_{\mathfrak{p}_1} : \mathbb{Q}_p]}{\mathrm{ord}_{\mathfrak{p}_1}(p^d)} = \frac{\mathrm{ord}_{\mathfrak{p}_1}(\pi)}{d} \equiv \frac{1}{2} \pmod{\mathbb{Z}}$$

and the same relation for $\mathrm{ord}_{\bar{\mathfrak{p}}_1}(\pi)$. We thus obtain $\mathrm{ord}_{\mathfrak{p}_1}(\pi) = \mathrm{ord}_{\bar{\mathfrak{p}}_1}(\pi) = d/2$. On the other hand, we have $\mathrm{ord}_{\mathfrak{p}_2}(\pi) = \mathrm{ord}_{\bar{\mathfrak{p}}_2}(\bar{\pi}) = \mathrm{ord}_{\mathfrak{p}_2}(\bar{\pi})$, so necessarily $\mathrm{ord}_{\mathfrak{p}_2}(\pi) = \mathrm{ord}_{\mathfrak{p}_2}(p)d/2 = ed/2$. Hence $(\pi^2) = (\pi\bar{\pi}) = (p^d)$, so there exists a root of unity ζ with $\pi = \zeta\sqrt{p^d}$, and B is supersingular. □

Corollary 3.4.8. *In case (3) of Theorem 3.4.7, $\mathbb{Q}(\pi)$ is the cyclotomic field $\mathbb{Q}(\zeta_n)$ for $n = 5, 8$ or 12, and we have $p \equiv 1 \pmod{n}$.*

PROOF. With our hypothesis, B is supersingular and $q = p^d$ with d even. Because B is supersingular, we know that $\pi = \zeta_n\sqrt{q}$ for some n, and so $\mathbb{Q}(\pi) = \mathbb{Q}(\zeta_n)$. The possibilities for n come from the condition $\varphi(n) = 4$. By Proposition 3.3.8, there must exist some prime $\mathfrak{p} \mid p$ with $[\mathbb{Q}(\pi)_\mathfrak{p} : \mathbb{Q}_p] = 1$, which implies at once that p splits completely in $\mathbb{Q}(\zeta_n)$. This gives the congruence condition. □

Example 3.4.9. *By searching through degree-4 Weil polynomials (cf.* [**MNH02**]*), we can give examples of case (3) of Theorem 3.4.7. Let D be the quaternion algebra over $\mathbb{Q}$ ramified at 2 and 11. Over $\mathbb{F}_{11^2}$, consider the abelian fourfold B whose characteristic polynomial of Frobenius is*

$$(T^4 - 11T^3 + 121T^2 - 1331T + 14641)^2.$$

One checks that $\mathbb{Q}(\pi) = \mathbb{Q}(\zeta_5)$, in which 2 is inert and 11 splits completely. Moreover, $\mathrm{ord}_\mathfrak{p}(\pi) = 1$ for every $\mathfrak{p} \mid 11$. It follows from Theorem 3.1.1 that $\mathrm{End}^0(B)$ is a quaternion algebra over $\mathbb{Q}(\zeta_5)$ ramified at every prime over 11, and that $\mathrm{End}^0(B) \simeq D \otimes_\mathbb{Q} \mathbb{Q}(\zeta_5)$.

An example with $\mathbb{Q}(\pi) = \mathbb{Q}(\zeta_8)$ arises by taking $B/\mathbb{F}_{17^2}$ with polynomial $(T^4 + 83521)^2$. To obtain $\mathbb{Q}(\pi) = \mathbb{Q}(\zeta_{12})$, we may take $B/\mathbb{F}_{13^2}$ with polynomial $(T^4 - 169T^2 + 28561)^2$.

3.5. A theorem on split reductions

We end the chapter by considering reductions of abelian varieties. We let k be a number field, A an abelian variety over k, and Σ_A the set of primes of k of good reduction for A. For $v \in \Sigma_A$, we denote by A_v the reduction of A modulo v. We also denote by $\mathbb{F}_v$ the residue field of v and by p_v its characteristic.

We begin by recalling a classical result about surfaces, which goes back to Morita [**Mor70**, §4] and Yoshida [**Yos73**, Lemma 6].

Proposition 3.5.1. *Suppose A is a simple abelian surface with quaternionic multiplication. Let $v \in \Sigma_A$. If A_v is simple, then $\mathrm{End}^0(A)$ ramifies at p_v.*

PROOF. The fact that A is simple and has quaternionic multiplication implies by [**Shi63**, Proposition 15] that $\mathrm{End}^0(A)$ is an indefinite quaternion algebra with center $\mathbb{Q}$. The reduction modulo v gives an embedding of $\mathbb{Q}$-algebras

$$\mathrm{End}^0(A) \to \mathrm{End}^0(A_v),$$

making $\mathrm{End}^0(A_v)$ noncommutative. We are assuming A_v simple, and so $\mathrm{End}^0(A_v)$ is a division algebra. Its center is the field $\mathbb{Q}(\pi)$ generated by Frobenius. By Theorem 3.1.1, $\mathbb{Q}(\pi)$ strictly contains $\mathbb{Q}$. It follows by Table 1.1 that $[\mathbb{Q}(\pi) : \mathbb{Q}] = 2$ and $\mathrm{End}^0(A_v)$ is a quaternion algebra. By Corollary 2.2.9 we have

$$\mathrm{End}^0(A_v) \simeq \mathrm{End}^0(A) \otimes_\mathbb{Q} \mathbb{Q}(\pi). \tag{3.4}$$

Again by Theorem 3.1.1, if $\mathbb{Q}(\pi)$ is real quadratic then $\mathrm{End}^0(A_v)$ needs to be totally definite. But this cannot be since $\mathrm{End}^0(A)$ is indefinite. Hence $\mathbb{Q}(\pi)$ is an imaginary quadratic field in which p_v splits, and $\mathrm{End}^0(A_v)$ ramifies exactly at the primes over p_v. It follows from (3.4) that $\mathrm{End}^0(A)$ ramifies at p_v. □

The following is the main result of this section, which is part of [**Flo25**].

Theorem 3.5.2. *Suppose A is simple and $\mathrm{End}^0(A)$ is noncommutative. Let $v \in \Sigma_A$. If A_v is simple, then $\mathrm{End}^0(A)$ ramifies at some prime above p_v. In particular, A splits modulo all but finitely many primes.*

Proof. The reduction modulo v produces an embedding

$$\iota : \mathrm{End}^0(A) \to \mathrm{End}^0(A_v).$$

Since we are assuming A_v simple, $\mathrm{End}^0(A_v)$ is a division algebra. By Example 2.2.2, ι is a primitive embedding. Let $Z(\pi)$ be the subfield of $\mathrm{End}^0(A_v)$ given by composing the centers Z and $\mathbb{Q}(\pi)$ of $\mathrm{End}^0(A)$ and $\mathrm{End}^0(A_v)$, respectively. Then by Theorem 2.4.6 there is some positive integer t and an equality of nontrivial classes

$$t[\mathrm{End}^0(A) \otimes_Z Z(\pi)] = t[\mathrm{End}^0(A_v) \otimes_{\mathbb{Q}(\pi)} Z(\pi)] \tag{3.5}$$

in $\mathrm{Br}(Z(\pi))$. By Proposition 3.5.1, we may assume $\dim A \geq 3$. Hence we know by Corollary 3.1.4 that $\mathbb{Q}(\pi)$ is a CM field, and so by Theorem 3.1.1 $\mathrm{End}^0(A_v)$ ramifies at some prime of $\mathbb{Q}(\pi)$ over p_v. The nontriviality of (3.5) implies that $\mathrm{End}^0(A)$ ramifies at some prime of Z over p_v. □

3.5.1. Primes of simple reduction. We keep the notation above. Given a simple abelian variety A with noncommutative endomorphism algebra, the conclusion of Theorem 3.5.2 is that we have a finite set $S \subset \Sigma_A$ described in terms of $\mathrm{End}^0(A)$ such that A_v is simple for every $v \in S$. We now focus on saying something more about the primes in S. In particular, we want to show whether S is ever a nonempty set.

It has been claimed that A_v is never simple if $\mathrm{End}^0(A)$ is an indefinite quaternion algebra (cf. the introduction of [**Ach12**], but also some older proofs of Proposition 3.5.1). Among other considerations, we give here two examples of abelian varieties with quaternionic multiplication having at least one prime of simple reduction.

We begin by making a remark on the field $\mathbb{F}_v$. By Proposition 3.2.2, we need the residual degree $f_v = [\mathbb{F}_v : \mathbb{F}_{p_v}]$ of v to be strictly greater than 1. More concretely, we have the following.

Proposition 3.5.3. *Let A be an abelian variety over a number field k. Let $v \in \Sigma_A$ be such that A_v is simple. Then t_A divides f_v.*

Proof. Let t_v be the Schur index of $\mathrm{End}^0(A_v)$. As a consequence of Proposition 3.2.2, we have $t_v \mid f_v$. Now we note that the embedding $\mathrm{End}^0(A) \to \mathrm{End}^0(A_v)$ is primitive, and so t_A divides t_v by Proposition 2.3.1. The result follows. □

In the case of abelian surfaces, we have the following situation.

Proposition 3.5.4. *Let A be a simple abelian surface with $D = \mathrm{End}^0(A)$ a quaternion algebra over $\mathbb{Q}$. Let $v \in \Sigma_A$ and suppose A_v is simple.*

(a) A_v is geometrically isogenous to the square of a supersingular elliptic curve.
(b) We have $p_v \notin \{2, 3\}$ and $p_v \not\equiv 11 \pmod{12}$.
(c) If k is quadratic field, then p_v is prime in k.
(d) If $k = \mathbb{Q}(\sqrt{-1})$, then $p_v \equiv 7 \pmod{12}$.
(e) If $k = \mathbb{Q}(\sqrt{-3})$, then $p_v \equiv 5 \pmod{12}$.

PROOF. We have the isomorphism

$$\mathrm{End}^0(A) \otimes_{\mathbb{Q}} \mathbb{Q}(\pi) \simeq \mathrm{End}^0(A_v),$$

so that $\mathrm{End}^0(A)$ ramifies at p_v and $\mathrm{End}^0(A_v)$ is a division quaternion algebra. By Proposition 3.2.1 we know that A is supersingular, and we either have $p_v \equiv 1 \pmod 4$ (whenever $\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{-1})$) or $p_v \equiv 1 \pmod 3$ (if $\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{-3})$). Hence A_v is not geometrically simple. To prove (a) we show that, if $A_{v,\bar{\mathbb{F}}_v} \sim E \times E'$, then E and E' are isogenous. This is because otherwise we would have an embedding $D \to \mathrm{End}^0(E) \simeq D_{p_v}$, but this would contradict the fact that D is indefinite, while D_{p_v} is definite. Alternatively, the curves E and E' are supersingular, so they are isogenous over $\bar{\mathbb{F}}_v$. The congruence conditions give (b).

In addition, v needs to have even residual degree by Proposition 3.5.3, and so we obtain (c). In the particular case where $k = \mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$, we obtain (d) and (e) as the combination of (b) and (c). □

Looking at the discriminants smaller than 100, we obtain the following.

Corollary 3.5.5. *Let A/k be a simple abelian surface with QM by the quaternion algebra D with discriminant 6, 22, 33, 46, 69 or 94. Then, the reduction A_v is isogenous to the square of an elliptic curve for every $v \in \Sigma_A$.*

The following example is an instance of an abelian surface with quaternionic multiplication having a prime of simple reduction.

Example 3.5.6. *Let ε be the quadratic character of $G_{\mathbb{Q}}$ given by the extension $\mathbb{Q}(\sqrt{79})/\mathbb{Q}$, and let f be an eigenform in the unique Galois orbit of $S_2^{new}(\Gamma_0(316), \varepsilon)$ (*[**LMF25**, Newform orbit 316.2.d.a]*). Then $\mathbb{Q}(\{a_p(f)\})$ has degree 4 over $\mathbb{Q}$, and the abelian fourfold A_f decomposes over $k = \mathbb{Q}(\sqrt{-1}, \sqrt{79})$ as the square of a geometrically simple abelian surface A_0/k with QM by the quaternion algebra D of discriminant 14 (cf.* [**Que12**, §5.1]*).*

Let v be one of the two primes of k over 7, so that $\mathbb{F}_v = \mathbb{F}_{7^2}$. Then, the characteristic polynomial of the Frobenius $\pi_{A_{0,v}}$ of $A_{0,v}$ is $(T^2 + 7T + 49)^2$. One easily computes using Theorem 3.1.1 that $A_{0,v}$ is simple, $\mathrm{End}^0(A_{0,v})$ is the quaternion algebra over $\mathbb{Q}(\pi_{A_{0,v}}) = \mathbb{Q}(\sqrt{-3})$ ramified at the two primes over 7, and $A_{0,v}$ is supersingular in accordance with Proposition 3.2.1.

Hence not every abelian surface with quaternionic multiplication splits modulo all its primes of good reduction.

If we let A/k be a fourfold, we find that A splits (geometrically) modulo all primes $v \in \Sigma_A$ if $\mathrm{End}^0(A)$ is a division quaternion algebra with center $\mathbb{Q}$. On the other hand, we will also show an example of a fourfold A such that $\mathrm{End}^0(A)$ is a quaternion algebra over a real quadratic field F, and such that A_v is geometrically simple for certain primes $v \in \Sigma_A$.

Theorem 3.5.7. *Let A/k be a simple abelian fourfold such that $\mathrm{End}^0(A)$ has a quaternion subalgebra D over $\mathbb{Q}$. Let $v \in \Sigma_A$ be over a rational prime p at which D ramifies. Then, one of the following possibilities occurs.*

(1) A_v is $\mathbb{F}_v$-isogenous to E^4, where E is an ordinary elliptic curve.
(2) A_v is $\mathbb{F}_v$-isogenous to S^2, where S is an ordinary abelian surface.
(3) A_v is supersingular.

In particular, A_v is split or supersingular (and hence geometrically split) for every $v \in \Sigma_A$.

PROOF. Let $v \in \Sigma_A$, let p_v be the residual characteristic of $\mathbb{F}_v$, and let π be the Frobenius endomorphism of A_v. We assume that D ramifies at p_v.

Suppose that A_v is not simple. Then A_v is isogenous to a product of simple varieties. Each simple isogeny factor (say A') is of dimension 1 or 2. Indeed, if $\dim A' = 3$ and A' is simple, then $\mathbb{Q}(\pi_{A'})$ is a CM field and $D \subseteq \mathrm{End}^0(A')$, and then by Proposition 3.2.3 we have $2 = \mathrm{ord}_{\mathbb{Q}}[D] \mid \dim A' = 3$, a contradiction. If $A_v \sim A_1 \times A_2$ with $\mathrm{Hom}(A_1, A_2) = 0$, then we have an embedding $D \to \mathrm{End}^0(A_i)$ for $i = 1, 2$. We have already seen that $\dim A_i \leq 2$, and therefore A_i is supersingular (if A_i is an elliptic curve this is well-known; if it is a surface, we use [**Yu13b**, Lemma 2.8]). It follows that A_v is supersingular.

If A_v is nonsimple isotypical or simple, the result follows from the various possibilities in Theorem 3.4.7.

□

We now display an example of an abelian fourfold with noncommutative endomorphism algebra which is geometrically simple modulo at least one prime.

Example 3.5.8. *Let ε be the quadratic character of $G_{\mathbb{Q}}$ associated to the field $\mathbb{Q}(\sqrt{29})$, and consider the space $S_2^{new}(\Gamma_0(156), \varepsilon)$. In this space, there is a unique Galois orbit of eigenforms without CM (*[**LMF25**, Newform orbit 156.2.h.b]*). Let f be one such eigenform. Then we have $[\mathbb{Q}(\{a_p(f)\}) : \mathbb{Q}] = 16$, so that the abelian variety $A_f/\mathbb{Q}$ given by Eichler–Shimura has dimension 16.*

Let $k = \mathbb{Q}(\sqrt{-3}, \sqrt{-1}, \sqrt{13})$. By [**Que12**, §5.2]*, there exists a geometrically simple abelian fourfold A_0/k such that $A_{f,k} \sim A_0^4$. Let $F = \mathbb{Q}(\sqrt{17})$, $\mathfrak{p}_2, \mathfrak{p}_2'$ the primes of F over 2, and $\mathfrak{p}_{17}$ the prime of F over 17. Then $\mathrm{End}^0(A_0)$ is the quaternion algebra over F ramified at $\mathfrak{p}_2$ and $\mathfrak{p}_{17}$. Since A_f has good reduction at 17, so does A_0. The characteristic polynomial of the Frobenius π_A of $A_{f,17}$ is*

$$(T^8 - 17T^6 + 136T^4 - 4913T^2 + 83521)^4.$$

The two primes of k over 17 have residue field isomorphic to $\mathbb{F}_{17^2}$. Let $v \mid 17$, then $\pi_{A_{0,v}} = \pi_{A_v}^2$ has characteristic polynomial

$$(T^4 - 17T^3 + 136T^2 - 4913T + 83521)^2.$$

We observe that the slopes of the Newton polygon attached to $A_{0,v}$ are $\frac{1}{4}$ and $\frac{3}{4}$, and hence $A_{0,v}$ is geometrically simple (these slopes would not occur if $A_{0,v}$ had an isogeny factor of dimension ≤ 2). Alternatively, we may apply the criterion in [**FFG24**, Lemma 9.1] *to see $A_{0,v}$ is geometrically simple, and in fact the center of $\mathrm{End}^0(A_{0,\bar{\mathbb{F}}_v})$ is $\mathbb{Q}(\pi_{A_{0,v}})$.*

Now we see from Proposition 3.4.4 that $\mathrm{End}^0(A_{0,\bar{\mathbb{F}}_{17}}) = \mathrm{End}^0(A_{0,v}) \simeq \mathrm{End}^0(A) \otimes_F \mathbb{Q}(\pi_{A_{0,v}})$ is the quaternion algebra over $\mathbb{Q}(\pi_{A_{0,v}})$ ramified at the two primes over 17. Therefore A_0/k is an example of an abelian variety that splits modulo all but finitely many primes of k, but has exactly two geometrically simple good reductions.

More generally, we pose the following problem.

Problem 3.5.9. *Let A be an abelian variety over a number field k, such that*

(1) A is geometrically simple,

(2) $\mathrm{End}^0(A)$ is a noncommutative algebra, and

(3) For some $v \in \Sigma_A$, A_v is geometrically simple.

Give necessary conditions to be satisfied by v and $\mathrm{End}^0(A)$.

We end with the following complimentary result, which in fact does not pose any additional restrictions for A_v to be simple. However, it does give information on $[\mathbb{F}_v : \mathbb{F}_{p_v}]$ whenever A_v is not simple.

Proposition 3.5.10. *Let A be an abelian variety over a number field k. Suppose that* $\mathrm{End}^0(A)$ *is a quaternion algebra with center F. Let K be the Galois closure of $k/\mathbb{Q}$. Let FK be the compositum of F and K in a common algebraic closure. If* $\frac{\dim A}{[FK:K]} \equiv 2 \pmod 4$, *then FK splits* $\mathrm{End}^0(A)$.

Proof. Let $D = \mathrm{End}^0(A)$ and $g = \dim A$. Consider the embedding of $\mathbb{Q}$-algebras

$$\varphi : D \to \mathrm{End}(\mathrm{Lie}(A_K)) \simeq \mathrm{M}_g(K),$$

where $\mathrm{Lie}(A_K)$ is the tangent space of A_K at the identity element. Since $K/\mathbb{Q}$ is Galois, by Theorem 2.4.2 we may pick a (possibly different) primitive embedding $\psi : D \to \mathrm{M}_g(K)$. Hence by Proposition 2.3.1 we have that $2[FK : K]$ divides g and, letting $d = g/2[FK : K]$, we have $d[D \otimes_F FK] = d[FK]$. But d is odd, so this equality of Brauer classes becomes $[D \otimes_F FK] = [FK]$. Hence FK splits D as claimed. □

Remark 3.5.11. *Let D be an indefinite quaternion algebra with center $\mathbb{Q}$. It is expected* [**BCGP21**, §10.3] *that there exists a simple abelian fourfold A over $\mathbb{Q}$ with* $\mathrm{End}^0(A) = D$. *The statement (and proof) of Proposition 3.5.10 clearly do not apply in this situation, and no information about D can be extracted from the base field.*

CHAPTER 4

Tate modules and pairings

In this chapter, we study the Tate modules of an abelian variety A defined over a number field k. We describe the absolutely irreducible G_k-submodules arising from the action of the endomorphism algebra of A. We also explain how these pieces inherit the Weil pairing, and how the Albert type of A conditions the nature of the pairing. The chapter is meant to serve as a survey of results that will be used throughout the next few chapters.

In Section 4.1 we introduce the necessary definitions on compatible systems of representations with values in the algebraic group of a simple algebra. In Section 4.2 we describe the strictly compatible system associated to A; the main result is Theorem 4.2.7. In Section 4.3 we restrict the Weil pairing to our system of representations.

4.1. Compatible systems of representations

In this section we explain the notion of a compatible system of Galois representations with values in the algebraic group of a simple algebra, following [**Ser98**, Chapter I, §2.4]. The definitions we introduce generalize the usual notion of compatible system of Galois representations (with values in GL_n). We will show that the rationality and compatibility of the system can be expressed in terms of *reduced characteristic polynomials*.

Let F be a number field and let $\mathcal{G}$ be a linear algebraic group over F. Let $R_{\mathcal{G}}$ be the coordinate ring of $\mathcal{G}$. An element $f \in R_{\mathcal{G}}$ is called *central* if $f(\alpha\beta) = f(\beta\alpha)$ for all $\alpha, \beta \in \mathcal{G}(A)$ and every commutative F-algebra A. If $\alpha \in \mathcal{G}(A)$, we say the conjugacy class of α in $\mathcal{G}$ is *F-rational* if $f(\alpha) \in F$ for every central $f \in R_{\mathcal{G}}$.

Example 4.1.1. *Let $\mathcal{G} = \mathrm{GL}_{n/F} = \operatorname{Spec} F[\{x_{ij}\}_{1\leq i,j\leq n}, \det^{-1}]$. For $M \in \mathcal{G}(F)$, let $c_i(M)$ be the ith coefficient of the characteristic polynomial of M, $0 \leq i \leq n-1$. In particular, $c_0 = \det$ and $c_{n-1} = -\operatorname{Tr}$. Then $c_i \in R_{\mathrm{GL}_n}$ is a central element, and moreover every central element is of the form $P(c_0, \ldots, c_{n-1})$ for some polynomial $P \in F[x_0, \ldots, x_{n-1}]$.*

Note that for every prime λ of F, the group $\mathcal{G}(F_\lambda)$ has a natural topological group structure.

Definition 4.1.2. *Let k be a number field and let λ be a prime of F. A* λ-adic representation with values in $\mathcal{G}$ *is a continuous homomorphism $\rho_\lambda : G_k \to \mathcal{G}(F_\lambda)$. In addition:*

- *We say ρ_λ is* unramified *at a prime v of k if $\rho_\lambda(I_w) = \{1\}$ for any valuation w of $\bar{k}$ extending v.*
- *We say ρ_λ is* F-rational *if there is a finite set S of primes of k such that ρ_λ is unramified outside S, and such that $\rho_\lambda(\mathrm{Frob}_v)$ is F-rational for every $v \notin S$.*

Definition 4.1.3. *Let λ, λ' be two primes of F and let $\rho_\lambda, \rho_{\lambda'}$ be F-rational representations of G_k with values in $\mathcal{G}$. Then $\rho_\lambda, \rho_{\lambda'}$ are* compatible *if they are unramified outside of a finite set S, and $f(\rho_\lambda(\mathrm{Frob}_v)) = f(\rho_{\lambda'}(\mathrm{Frob}_v))$ for all $v \notin S$ and every central element $f \in R_{\mathcal{G}}$.*

We now give the main definition in this section. For a prime λ of F (resp. v of k), we let p_λ (resp. p_v) be its residual characteristic. Let $S_\lambda := \{v \text{ prime of } k \mid p_v = p_\lambda\}$.

Definition 4.1.4. *For each prime λ of F, let ρ_λ be an F-rational λ-adic representation with values in $\mathcal{G}$. The collection $\{\rho_\lambda\}_\lambda$ is called an* F-rational compatible system *if ρ_λ and $\rho_{\lambda'}$ are compatible for all λ, λ'. The system is called* strictly compatible *if there exists a finite set S of primes of k such that*

(1) For every $v \notin S \cup S_\lambda$, ρ_λ is unramified at v, and $\rho_\lambda(\mathrm{Frob}_v)$ is F-rational.
(2) For every $v \notin S \cup S_\lambda \cup S_{\lambda'}$ and every central element $f \in R_{\mathcal{G}}$, we have

$$f(\rho_\lambda(\mathrm{Frob}_v)) = f(\rho_{\lambda'}(\mathrm{Frob}_v)).$$

The smallest possible set S is called the exceptional set *of the system. When the group $\mathcal{G}$ is $\mathrm{GL}_{n/F}$ for some n, we will also call $\{\rho_\lambda\}_\lambda$ a* (strictly) compatible system*, without specifying the group in which the representations take their values.*

Recall that any central simple F-algebra D defines a group scheme $\mathbf{GL}_1(D)$, whose functor of points is

$$\begin{aligned} \mathrm{Alg}_F &\to \mathrm{Grp} \\ A &\mapsto (D \otimes_F A)^\times. \end{aligned}$$

In particular, we have $\mathbf{GL}_1(\mathrm{M}_n(F)) \simeq \mathbf{GL}_{n/F}$. Moreover, for every extension L/F we have $\mathbf{GL}_1(D)_L = \mathbf{GL}_1(D \otimes_F L)$ (see [**KMRT98**, Chapter IV, 20.2] for details).

We want to consider systems of λ-adic representations with values in $\mathbf{GL}_1(D)$ for some central simple algebra D. Hence we need to study the notions of F-rationality and compatibility, which are stated in terms of the central elements of $R_{\mathbf{GL}_1(D)}$. We will see that central elements are expressed in terms of reduced characteristic polynomials.

Definition 4.1.5. *Let D be a central simple F-algebra, L any field containing F, and $m \geq 1$ an integer. Given an F-algebra homomorphism $\phi : D \to \mathrm{M}_m(L)$, the ϕ-characteristic polynomial of an element $\alpha \in D$ is*

$$\mathrm{CharPol}_\phi(x, \alpha) := \det(x\mathrm{Id} - \phi(\alpha)) \in L[x],$$

the characteristic polynomial of the image of α through ϕ. This definition is independent of the choice of homomorphism of D into $\mathrm{M}_m(L)$ by the Skolem–Noether theorem (cf. Theorem 1.1.3).

Given a central simple F-algebra D of dimension n^2, any element $\alpha \in D$ defines by left multiplication an F-linear map $\alpha_l \in \mathrm{Hom}_F(D, D)$. After fixing a basis, this left-regular representation gives a homomorphism of F-algebras $\phi_l : D \to \mathrm{M}_{n^2}(F)$. The *characteristic polynomial* of α is defined to be $\mathrm{CharPol}_{\phi_l}(x, \alpha)$. This polynomial clearly has degree n^2.

Let E be any field containing F that splits D. Then, the isomorphism $D \otimes_F E \simeq \mathrm{M}_n(E)$ gives an embedding of F-algebras $\phi_E : D \to \mathrm{M}_n(E)$. We define the *reduced characteristic polynomial* of α to be

$$\mathrm{RedCharPol}(x, \alpha) := \mathrm{CharPol}_{\phi_E}(x, \alpha).$$

This is a polynomial of degree n. The notation reflects the fact that $\mathrm{RedCharPol}(x,\alpha)$ is independent of the choice of E, as stated in the following result.

Proposition 4.1.6. *If E, E' are two splitting fields for D, then* $\mathrm{CharPol}_{\phi_E}(x,\alpha) = \mathrm{CharPol}_{\phi_{E'}}(x,\alpha)$. *Moreover,* $\mathrm{RedCharPol}(x,\alpha) \in F[x]$.

Proof. See [**Rei03**, §9a] and [**Pie82**, §16.1]. □

The adjective *reduced* conveys the idea that every ϕ-characteristic polynomial comes from $\mathrm{RedCharPol}(x,\alpha)$. This is made precise by the following result.

Proposition 4.1.7. *Let $\phi : D \to \mathrm{M}_m(L)$ be any F-algebra homomorphism. Then $m = nk$ for some integer k, and* $\mathrm{CharPol}_\phi(x,\alpha) = \mathrm{RedCharPol}(x,\alpha)^k$. *In particular, if $\phi_l : D \to \mathrm{M}_{n^2}(F)$ is the left-regular representation of D, then*

$$\mathrm{CharPol}_{\phi_l}(x,\alpha) = \mathrm{RedCharPol}(x,\alpha)^n.$$

Proof. The divisibility $n \mid m$ comes e.g. from Proposition 2.3.1. For the rest, see [**Pie82**, §16.1, Lemma 1]. □

We now want to see the coefficients of $\mathrm{RedCharPol}(x,\alpha)$ as elements of the ring $R_{\mathbf{GL}_1(D)}$.

Proposition 4.1.8. *Let $u_1, \dots, u_{n^2}$ be an F-basis of D and let $\alpha = \sum_{i=1}^{n^2} a_i u_i$ be an element of D, $a_i \in F$. Denote by $\mathbf{a}$ the vector $(a_1, a_2, \dots, a_{n^2})$. Then, there are polynomials $\tau_0, \dots, \tau_{n-1} \in F[\xi_1, \dots, \xi_{n^2}]$ such that*

$$\mathrm{RedCharPol}(x,\alpha) = x^n + \tau_{n-1}(\mathbf{a})x^{n-1} + \cdots + \tau_0(\mathbf{a}).$$

In particular, each τ_i is a central element of $R_{\mathbf{GL}_1(D)}$.

Proof. The existence of the polynomials τ_i is shown in [**Jac96**, §1.6]. To see that each τ_i is a central element, it is enough to see them in $R_{\mathbf{GL}_1(D)} \otimes_F E \simeq R_{\mathrm{GL}_n,E}$ for a splitting field E, where they are the coefficients of the characteristic polynomial. □

Lemma 4.1.9. *Let D be a central simple F-algebra and consider the linear algebraic group $\mathcal{G} = \mathbf{GL}_1(D)$. Let L/F be an extension. Then, the coefficients of* $\mathrm{RedCharPol}(x,\alpha)$ *of an element $\alpha \in \mathcal{G}(L)$ determine the values of $f(\alpha)$ for any central element $f \in R_{\mathcal{G}}$.*

Proof. Note that it is enough to show the statement for elements $\alpha \in \mathcal{G}(F)$. Let $f \in R_{\mathcal{G}}$ be central. For any splitting field E of D, we have

$$\mathbf{GL}_1(D)_E = \mathbf{GL}_1(D \otimes_F E) \simeq \mathrm{GL}_{n/E},$$

and hence we have an isomorphism $R_{\mathcal{G}} \otimes_F E \simeq R_{\mathrm{GL}_n/E}$ of E-algebras. Now we compose the inclusion $R_{\mathcal{G}} \to R_{\mathcal{G}} \otimes_F E$ with this isomorphism. Since $f \otimes 1$ is still a central element in $R_{\mathcal{G}} \otimes_F E$, we can express f as a polynomial in $E[x_0, \dots, x_{n-1}]$ of the coefficients of the reduced characteristic polynomial. □

Corollary 4.1.10. *Let $\mathcal{G} = \mathbf{GL}_1(D)$ and let L/F be an extension. Then, an element $\alpha \in \mathcal{G}(L)$ is F-rational if and only if its reduced characteristic polynomial lies in $F[x]$.*

PROOF. This is a consequence of Proposition 4.1.8 and Lemma 4.1.9. Indeed, if $f \in R_{\mathcal{G}}$ is a central element, then it can be expressed as a polynomial $P(\tau_0, \dots, \tau_{n-1})$ with coefficients in a splitting field E of D. At the same time, we have $\tau_0, \dots, \tau_{n-1} \in R_{\mathcal{G}}$. But f takes values in F for all elements in $\mathcal{G}(F)$, and so $P(x_0, \dots, x_{n-1})$ has coefficients in F (cf. [**Jac96**, §3.1, pg. 98]).

□

4.2. The Tate module

We begin by briefly recalling some definitions on equivariant pairings. Let E be a field and let $\bar{E}$ be an algebraic closure of E. Let V be a finite-dimensional E-vector space. Let $\psi : V \times V \to E$ be a map which is E-linear in the first entry and additive in the second.

(i) We say ψ is an *alternating* pairing, if $\psi(v, w) = -\psi(w, v)$ for all $v, w \in V$.
(ii) We say ψ is a *symmetric* pairing, if $\psi(v, w) = \psi(w, v)$ for all $v, w \in V$.
(iii) Suppose that E has an automorphism $\sigma : E \to E$ of order 2. Then we say ψ is a *σ-hermitian* (or simply, hermitian) pairing if $\psi(v, w) = \sigma(\psi(w, v))$ for all $v, w \in V$.

In particular, an alternating or symmetric pairing is E-bilinear, while a hermitian pairing is E-antilinear in the second entry. If unspecified, a pairing ψ on V is an alternating, symmetric or hermitian pairing.

Fix a non-degenerate pairing $\psi : V \times V \to E$. Let G be a group and consider a representation $\rho : G \to \mathrm{GL}(V) \simeq \mathrm{GL}_n(E)$, where $n = \dim_E V$. Recall that a subspace $W \subseteq V$ is said to be *G-invariant* if $\rho(G)w \subseteq W$ for all $w \in W$. We say ρ is *irreducible* if the only nontrivial G-invariant subspace of V is V itself, and *absolutely irreducible* if $V \otimes_E \bar{E}$ is irreducible. Recall that a pairing $\psi : G \to E^\times$ is *G-equivariant* with *similitude character* χ if $\psi(gv, gw) = \chi(g)\psi(v, w)$ for all $g \in G$ and $v, w \in V$. When the character is clear from the context, we just say ψ is G-equivariant.

For the rest of the chapter, we let k be a number field and A be a simple abelian variety over k of dimension g. We let S_A be the set of primes of k of bad reduction for A. We fix once and for all a polarization on A (i.e. an ample divisor $\mathcal{L}$, which induces an isogeny $\phi_{\mathcal{L}} : A \to A^\vee$). For every $f \in \mathrm{End}^0(A)$, we denote its Rosati involution by $f^\dagger$.

For every prime number ℓ and positive integer n, the ℓ^n-torsion $A[\ell^n]$ of A is isomorphic as (an abstract group) to $(\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$. Multiplication by ℓ gives a surjective map $A[\ell^{n+1}] \to A[\ell^n]$. One forms the ℓ-adic Tate module by taking the projective limit,

$$T_\ell A := \varprojlim_n A[\ell^n],$$

which is abstractly isomorphic to the group $\mathbb{Z}_\ell^{2g}$. The absolute Galois group G_k acts on each of the $A[\ell^n]$ and commutes with multiplication by ℓ. Hence we have a continuous homomorphism

$$\rho_{A,\ell} : G_k \to \mathrm{Aut}(T_\ell A) \simeq \mathrm{GL}_{2g}(\mathbb{Z}_\ell).$$

When we work with A up to isogeny, we study the rational ℓ-adic Tate module, defined as $V_\ell(A) := T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. The image of the representation $\rho_{A,\ell}$ then lands in $\mathrm{GL}_{2g}(\mathbb{Q}_\ell)$. In general, the image is constrained by the Weil pairing (cf. [**Mum08**, §20]). Recall that $\chi_\ell : G_k \to \mathbb{Q}_\ell^\times$ denotes the ℓ-adic cyclotomic character.

Proposition 4.2.1. *There exists a nondegenerate, $\mathbb{Q}_\ell$-bilinear, G_k-equivariant alternating pairing $\psi_\ell : V_\ell(A) \times V_\ell(A) \to \mathbb{Q}_\ell(\chi_\ell)$. For every $f \in \mathrm{End}^0(A)$ and all $v, w \in V_\ell(A)$, we have $\psi_\ell(fv, w) = \psi_\ell(v, f^\dagger w)$.*

In the rest of the chapter, ψ_ℓ will always denote the Weil pairing on $V_\ell(A)$. We now state the important result of Faltings (cf. [**Fal83**, Satz 4]).

Theorem 4.2.2 (Faltings)**.** *For every extension K/k, $V_\ell(A)$ is a semisimple $\mathbb{Q}_\ell[G_K]$-module, and we have $\mathrm{End}^0(A_K) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \simeq \mathrm{End}_{G_K}(V_\ell(A))$.*

Let H be the center of $\mathrm{End}^0(A)$. The $\mathbb{Q}_\ell$-vector space $V_\ell(A)$ has an action of H, and hence is a free $H \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-module. Consider the decomposition as a product of fields

$$H \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \simeq \prod_{\lambda|\ell} H_\lambda,$$

where λ ranges over the primes of H dividing ℓ. Let e_λ be the idempotent corresponding to 1 in H_λ. Then we can define a subspace of $V_\ell(A)$, $V_\lambda(A) := e_\lambda \cdot V_\ell(A)$. If $\sigma_\lambda : H \otimes \mathbb{Q}_\ell \to H_\lambda$ corresponds to the projection onto the λ-adic factor, we can also think of $V_\lambda(A)$ as the tensor product $V_\ell(A) \otimes_{H \otimes \mathbb{Q}_\ell} H_\lambda$ with respect to σ_λ. If $\mathrm{Res}_{H_\lambda/\mathbb{Q}_\ell} V_\lambda(A)$ denotes $V_\lambda(A)$ seen as a $\mathbb{Q}_\ell[G_k]$-module, we have an isomorphism of $\mathbb{Q}_\ell[G_k]$-modules

$$V_\ell(A) \simeq \bigoplus_{\lambda|\ell} \mathrm{Res}_{H_\lambda/\mathbb{Q}_\ell} V_\lambda(A).$$

Proposition 4.2.3. *The subspace $V_\lambda(A)$ has dimension $\dim_{H_\lambda} V_\lambda(A) = \frac{2g}{[H:\mathbb{Q}]}$, and*

$$\mathrm{End}_{H_\lambda[G_k]}(V_\lambda(A)) \simeq \mathrm{End}^0(A) \otimes_H H_\lambda.$$

In particular, if $\mathrm{End}^0(A) = H$ is commutative, then each $V_\lambda(A)$ is an absolutely irreducible $H_\lambda[G_k]$-module.

Proof. The dimension statement is [**Rib76**, Theorem 2.1.1]. The second statement is a consequence of Theorem 4.2.2. Indeed, we have

$$\mathrm{End}_{H \otimes \mathbb{Q}_\ell[G_k]}(V_\ell(A)) \simeq \mathrm{End}^0(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \simeq \bigoplus_{\lambda|\ell} \mathrm{End}^0(A) \otimes_H H_\lambda,$$

and now we observe that $\mathrm{End}_{H_\lambda[G_k]}(V_\lambda(A))$ contains $\mathrm{End}^0(A) \otimes_H H_\lambda$ (and cannot be larger). □

The following is [**Rib76**, Theorem 2.1.2].

Proposition 4.2.4. *The action of G_k on each $V_\lambda(A)$ yields a strictly compatible system of H-rational representations with exceptional set S_A.*

To make notation lighter, from now on we let $D = \mathrm{End}^0(A)$. We have already seen that the $V_\lambda(A)$ are absolutely irreducible when D is commutative. More generally, we let t_A be the Schur index of D. Let λ be a prime of H not in $\mathrm{Ram}(D)$, so that

$$D \otimes_H H_\lambda \simeq \mathrm{M}_{t_A}(H_\lambda).$$

Since the action of D and G_k on $V_\lambda(A)$ commute, there must exist an $H_\lambda[G_k]$-submodule $W_\lambda(A)$ of $V_\lambda(A)$ such that $V_\lambda(A) \simeq W_\lambda(A)^{\oplus t_A}$. We let $\rho_{A,\lambda} : G_k \to \mathrm{GL}(W_\lambda(A))$ be the representation given by the action of G_k.

Proposition 4.2.5. *The following properties hold.*

(a) *The $H_\lambda[G_k]$-module $W_\lambda(A)$ is absolutely irreducible.*
(b) *If $\lambda' \notin \mathrm{Ram}(D)$, then $\rho_{A,\lambda}$ and $\rho_{A,\lambda'}$ are compatible.*
(c) *For every prime $v \notin S_A \cup S_\lambda$, $\rho_{A,\lambda}(\mathrm{Frob}_v)$ is H-rational.*

PROOF. (a) By Proposition 4.2.3 we have $\mathrm{End}_{H_\lambda[G_k]}(V_\lambda(A)) = \mathrm{M}_t(H_\lambda)$. The isomorphism $V_\lambda(A) \simeq W_\lambda(A)^{\oplus t_A}$ implies $\mathrm{End}_{H_\lambda[G_k]}(W_\lambda(A)) = H_\lambda$. It follows that $W_\lambda(A)$ is absolutely irreducible.

(b) For $v \notin S_A \cup S_\lambda \cup S_{\lambda'}$, let $f_\lambda(T)$ and $f_{\lambda'}(T)$ be the respective characteristic polynomials of $\rho_{A,\lambda}(\mathrm{Frob}_v)$. Since $V_\lambda(A) \simeq W_\lambda(A)^{\oplus t_A}$ and $V_{\lambda'}(A) \simeq W_{\lambda'}(A)^{\oplus t_A}$, and the representations $V_\lambda(A)$ and $V_{\lambda'}(A)$ are compatible, we obtain $f_\lambda(T)^{t_A} = f_{\lambda'}(T)^{t_A}$. Hence $f_\lambda(T) = f_{\lambda'}(T)$.

(c) Let $f(T)$ be the characteristic polynomial of $\rho_{A,\lambda}(\mathrm{Frob}_v)$. Since $V_\lambda(A) \simeq W_\lambda(A)^{\oplus t_A}$, by Proposition 4.2.4 we have $f(T)^{t_A} \in H[T]$. Therefore $f(T) \in \bar{H}[T]$. For every $\sigma \in G_H$, we have ${}^\sigma(f(T)^{t_A}) = f(T)^{t_A}$, so σ sends each root of $f(T)^{t_A}$ to a root of $f(T)^{t_A}$. It follows that σ sends each root of $f(T)$ to a root of $f(T)$, and so $f(T) \in H[T]$ as desired. □

Remark 4.2.6. *Let ℓ be a rational prime and let $\lambda \mid \ell$. Let $f(T)$ be the characteristic polynomial of $\rho_{A,\lambda}(\mathrm{Frob}_v)$. The isomorphism of $\mathbb{Q}_\ell[G_k]$-modules*

$$V_\ell(A) \simeq \bigoplus_{\lambda|\ell} \mathrm{Res}_{H_\lambda/\mathbb{Q}_\ell} W_\lambda(A)^{\oplus t_A}$$

implies that the characteristic polynomial $P(T)$ of Frob_v acting on $V_\ell(A)$ equals

$$\mathrm{Nm}_{H[T]/\mathbb{Q}[T]}(f(T))^{t_A} = \prod_{\sigma: H \to \bar{\mathbb{Q}}} \sigma(f(T))^{\oplus t_A}.$$

On the other hand, $P(T)$ equals the characteristic polynomial of the Frobenius endomorphism π_v of the reduction A_v. By e.g. Proposition 3.2.3, there exists a polynomial $g \in \mathbb{Z}[T]$ with $P(T) = g(T)^{t_A}$. In follows that

$$g(T) = \mathrm{Nm}_{H[T]/\mathbb{Q}[T]}(f(T)).$$

We are close to having a compatible system from the modules $W_\lambda(A)$. It remains to build compatible representations at the ramified primes. For a positive integer r we let $\mathbf{GL}_r(D^{op})$ the group scheme $\mathbf{GL}_1(\mathrm{M}_r(D^{op}))$. We now show the following result.

Theorem 4.2.7. *Let A be a simple abelian variety defined over a number field k. Let $D = \mathrm{End}^0(A)$, H the center of D, t_A the Schur index of D, and $n := \frac{2g}{t_A[H:\mathbb{Q}]}$.*

(1) The variety A has an associated strictly compatible system $\{\rho_{A,\lambda}\}_\lambda$ of H-rational λ-adic representations with values in $\mathbf{GL}_{n/t_A}(D^{op})$.
(2) For every $\lambda \notin \mathrm{Ram}(D)$, the representation $\rho_{A,\lambda}$ takes values in $\mathrm{GL}_n(H_\lambda)$ and is absolutely irreducible.
(3) The exceptional set of the compatible system is S_A.

PROOF. Let $\lambda \in \mathrm{Ram}(D)$ be such that $D_\lambda := D \otimes_H H_\lambda$ is a division algebra (this always holds if t_A is prime). By Theorem 4.2.2 we have $\mathrm{End}_{H_\lambda[G_k]}(V_\lambda(A)) = D_\lambda$. By the assumption that D_λ is division, $V_\lambda(A)$ is a *free* left D_λ-module of rank

$$\mathrm{rank}_{D_\lambda} V_\lambda(A) = \frac{\dim_{H_\lambda} V_\lambda(A)}{\dim_{H_\lambda} D_\lambda} = \frac{2g}{t_A^2[H:\mathbb{Q}]}.$$

We define $n := \frac{2g}{t_A[H:\mathbb{Q}]}$ and identify $V_\lambda(A) \simeq D_\lambda^{n/t_A}$ as a left D_λ-module. We recall a well-known property.

Lemma 4.2.8. *Let X be a central simple algebra, and consider X as a left X-module. Then $\mathrm{End}_X(X) \simeq X^{op}$. For $m \geq 1$, we have $\mathrm{End}_X(X^m) \simeq \mathrm{M}_m(X^{op})$.*

Proof. For $a \in X$, the map $\varphi_a : x \mapsto xa$ is X-linear, and hence $\varphi_a \in \mathrm{End}_X(X)$. If $\varphi \in \mathrm{End}_X(X)$, then $\varphi = \varphi_a$ for $a = \varphi(1)$. The isomorphism of algebras comes from the equality $\varphi_a(\varphi_b(1)) = \varphi_a(b) = ba = \varphi_{ba}(1)$. The general case of X^m is identical, by considering the action of some $\varphi \in \mathrm{End}_X(X^m)$ on a basis. □

In view of the lemma, the action of G_k on $V_\lambda(A)$ gives a subgroup of

$$\mathrm{Aut}_{D_\lambda}(D_\lambda^{n/t_A}) \simeq \mathrm{GL}_{n/t_A}(D_\lambda^{op}).$$

This yields a representation $\rho_{A,\lambda} : G_k \to \mathrm{GL}_{n/t_A}(D_\lambda^{op})$. Note that reduced characteristic polynomials of elements in $\mathrm{GL}_{n/t_A}(D_\lambda^{op})$ have degree n. It remains to show that the representation $\rho_{A,\lambda}$ is H-rational and compatible with $\rho_{A,\lambda'}$ for any other $\lambda' \notin \mathrm{Ram}(D)$.

Consider the homomorphism $\varphi : \mathrm{GL}_{n/t_A}(D_\lambda^{op}) \to \mathrm{GL}_{nt_A}(H_\lambda)$, which corresponds to the restriction of scalars $\mathrm{Aut}_{D_\lambda}(D_\lambda^{n/t_A}) \subset \mathrm{Aut}_{H_\lambda}(D_\lambda^{n/t_A})$. Then by Proposition 4.1.7, the φ-characteristic polynomial of any $\alpha \in \mathrm{GL}_{n/t_A}(D_\lambda^{op})$ acting on D_λ^{n/t_A} equals $(\mathrm{RedCharPol}(\alpha, T))^{t_A}$.

Now recall from Proposition 4.2.4 that the vector spaces $\mathrm{Res}_{D_\lambda/H_\lambda}(V_\lambda(A))$ and $V_{\lambda'}(A)$ are part of the same strictly compatible system of representations. Moreover, we have $V_{\lambda'}(A) \simeq W_{\lambda'}(A)^{\oplus t_A}$. It follows that

$$(\mathrm{RedCharPol}(\rho_{A,\lambda}(\mathrm{Frob}_v), T))^{t_A} = (\mathrm{CharPol}(\rho_{A,\lambda'}(\mathrm{Frob}_v), T))^{t_A}.$$

Since both $\mathrm{RedCharPol}(\rho_{A,\lambda}(\mathrm{Frob}_v), T)$ and $\mathrm{CharPol}(\rho_{A,\lambda'}(\mathrm{Frob}_v), T)$ are monic polynomials, we obtain the result by Lemma 4.1.9 and Corollary 4.1.10.

For $t_A = 1$ or prime, the argument just given proves the result. For composite t_A, one may perform a similar argument by seeing $V_\lambda(A)$ as a free D'_λ-module, where D'_λ is a central division H_λ-algebra such that $D_\lambda \simeq \mathrm{M}_r(D'_\lambda)$. We give an alternative full proof using descent in Section 5.4. □

Remark 4.2.9. *The theorem above appears in* [**Oht74**] *in the case where A is a simple abelian surface with indefinite quaternionic multiplication.*

4.3. Weil pairings with values in H_λ

In this section we let A be a simple abelian variety over a number field k. As in the previous section we fix a polarization for A and denote by $(\cdot)^\dagger$ the Rosati involution. We let H be the center of $\mathrm{End}^0(A)$ and let λ be a prime of H. In the same way as $V_\ell(A)$ has a nondegenerate G_k-equivariant pairing (cf. Proposition 4.2.1), we want to endow each $H_\lambda[G_k]$-module $W_\lambda(A)$ with such a pairing. We will explain the pairing constructions introduced by Chi in [**Chi90**], and expanded by Banaszak, Gajda and Krasoń in [**BGK06, BGK10**]. Unlike in these works, we do not require that A has all of its endomorphisms defined over k.[1]

[1]In fact, the cited references do not need all endomorphisms to be defined over k to construct the pairings either, but they do require them in order to show some cases of the Mumford–Tate conjecture.

We begin by recalling a classical result introduced by Deligne.

Lemma 4.3.1. *Let Q be a field and E an étale Q-algebra. Let V, W be free E-modules of finite rank. Suppose that $\psi : V \times W \to Q$ is a Q-bilinear pairing such that $\psi(ev, w) = \psi(v, ew)$ for all $v \in V$, $w \in W$, $e \in E$. Then there exists a unique E-bilinear pairing $\phi : V \times W \to E$ such that*

$$\psi(v, w) = \mathrm{Tr}_{E/Q}\, \phi(v, w).$$

Moreover, ϕ is nondegenerate if and only if ψ is nondegenerate.

Proof. We follow [**Del82**, Sublemma 4.7]. We first note that the trace $\mathrm{Tr}_{E/Q}$ defines an isomorphism

$$\mathrm{Hom}_E(V \otimes_E W, E) \xrightarrow{\sim} \mathrm{Hom}_Q(V \otimes_E W, Q) \tag{4.1}$$

of Q-vector spaces by mapping $f \mapsto \mathrm{Tr}_{E/Q} \circ f$. Indeed, the nondegeneracy of the trace implies the map is injective. Let r, s be the E-rank of V and W, respectively. Now the Q-dimension of $\mathrm{Hom}_E(V \otimes_E W, E)$ is $rs \dim_Q E$, which is the same as the Q-dimension of $\mathrm{Hom}_Q(V \otimes_E W, Q)$. Therefore the map is an isomorphism.

Now we see the Q-bilinear form ψ as a Q-bilinear map $V \otimes_E W \to Q$. From (4.1) we obtain a $\phi \in \mathrm{Hom}_E(V \otimes_E W, E)$ with $\mathrm{Tr}_{E/Q}\, \phi = \psi$, which is necessarily unique.

It is clear that if ϕ is degenerate then so is ψ. If ϕ is nondegenerate, then for all $v \in V$, $w \in W$ with $\phi(v, w) \neq 0$ there exists some $\alpha \in E$ such that $\mathrm{Tr}_{E/Q}(\alpha\phi(v, w)) \neq 0$, and so $\psi(v, \alpha w) \neq 0$. Hence ψ is nondegenerate. □

We now apply Lemma 4.3.1 to give a pairing on $V_\lambda(A)$.

Proposition 4.3.2. *Suppose that H is totally real. Then there exists a unique nondegenerate H_λ-bilinear alternating pairing $\phi_\lambda : V_\lambda(A) \times V_\lambda(A) \to H_\lambda(\chi_\ell)$, with the following properties:*

(1) For every endomorphism $f \in \mathrm{End}^0(A) \otimes_H H_\lambda$ and all $v, w \in V_\lambda(A)$,

$$\phi_\lambda(fv, w) = \phi_\lambda(v, f^\dagger w).$$

(2) ϕ_λ is G_k-equivariant.

Proof. As stated in Proposition 4.2.1, $V_\ell(A)$ is endowed with a nondegenerate $\mathbb{Q}_\ell$-bilinear pairing ψ_ℓ. Since H is totally real, the Rosati involution acts trivially on it, and so $\psi_\ell(ev, w) = \psi_\ell(v, ew)$ for every $e \in H$ and all $v, w \in V_\ell(A)$. Hence we can apply Lemma 4.3.1 to find that there is an $(H \otimes \mathbb{Q}_\ell)$-bilinear nondegenerate pairing $\Phi_\ell : V_\ell(A) \times V_\ell(A) \to H \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$.

This pairing is the unique one with the property that $\mathrm{Tr}_{H \otimes_{\mathbb{Q}} \mathbb{Q}_\ell / \mathbb{Q}_\ell}(\Phi_\ell) = \psi_\ell$, and all properties of Φ_ℓ are checked using this uniqueness. We check first that it is alternating: for all $v, w \in V_\ell(A)$, note that

$$\mathrm{Tr}(\Phi_\ell(v, w)) = \psi_\ell(v, w) = -\psi_\ell(w, v) = -\mathrm{Tr}(\Phi_\ell(w, v)).$$

Property (1) is similar, since for all $f \in \mathrm{End}^0(A)$,

$$\mathrm{Tr}(\Phi_\ell(fv, w)) = \psi_\ell(fv, w) = \psi_\ell(v, f^\dagger w) = \mathrm{Tr}(\Phi_\ell(v, f^\dagger w)).$$

For (2), let $s \in G_k$, and then

$$\mathrm{Tr}(\Phi_\ell({}^s v, {}^s w)) = \psi_\ell({}^s v, {}^s w) = \mathrm{Tr}(\chi_\ell(s)\Phi_\ell(v, w)).$$

Now let $\sigma_\lambda : H \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \to H_\lambda$ be the projection, and define $\phi_\lambda := \sigma_\lambda \circ \Phi_\ell|_{V_\lambda(A) \times V_\lambda(A)}$. All the properties are maintained, and it only remains to check that ψ_λ is nondegenerate. But this is a consequence of the $H \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-linearity of Φ_ℓ. Indeed, suppose that ψ_λ were degenerate and fix some $e_\lambda v \in V_\lambda(A)$. Then for all $\lambda' \neq \lambda$ we have $e_\lambda e_{\lambda'} = 0$, and so for all $e_{\lambda'} w \in V_{\lambda'}(A)$ we have

$$\Phi_\ell(e_\lambda v, e_{\lambda'} w) = e_\lambda e_{\lambda'} \Phi_\ell(v, w) = 0.$$

But this is implies that Φ_ℓ is a degenerate pairing, which is a contradiction. Therefore we have seen that $V_\lambda(A)$ and $V_{\lambda'}(A)$ are orthogonal with respect to Φ_ℓ, and so ϕ_λ is nondegenerate. □

We next proceed according to the Albert type of A. When A has Albert type I, we have seen in Proposition 4.2.3 that $V_\lambda(A)$ is absolutely irreducible, and we obtain pairings on the compatible system $\{\rho_{A,\lambda}\}_\lambda$ as claimed. However, if A has Albert type II or III then $V_\lambda(A)$ is no longer irreducible, and we will need to show that there is a restriction of ϕ_λ which is nondegenerate on an irreducible submodule $W_\lambda(A)$. We will also mention the situation for Albert type IV, which is not covered by Proposition 4.3.2.

4.3.1. Albert type I. Let A be a simple abelian variety over k such that $H = \mathrm{End}^0(A)$ is a totally real field. This corresponds to A having Albert type I (cf. Section 1.4). To keep notational consistency, we let $W_\lambda(A) := V_\lambda(A)$ and denote the pairing on $W_\lambda(A)$ from Proposition 4.3.2 by ψ_λ. We have the following result, which is found in [**BGK06**, Section 5].

Theorem 4.3.3. *For every prime λ of H, the $H_\lambda[G_k]$-module $W_\lambda(A)$ satisfies:*

1. $\dim_{H_\lambda} W_\lambda(A) = \frac{2 \dim A}{[H:\mathbb{Q}]}$.
2. *$W_\lambda(A)$ is absolutely irreducible.*
3. *There exists a nondegenerate, H_λ-bilinear, alternating, G_k-equivariant pairing*
$$\psi_\lambda : W_\lambda(A) \times W_\lambda(A) \to H_\lambda(\chi_\ell).$$

Proof. The first two points come from Proposition 4.2.3; in particular, $W_\lambda(A)$ is absolutely irreducible since $\mathrm{End}_{H_\lambda[G_k]}(W_\lambda(A)) = H_\lambda$. The pairing ψ_λ comes from Proposition 4.3.2. □

4.3.2. Albert types II and III. We now let A be a simple abelian variety over k such that $D = \mathrm{End}^0(A)$ is a division quaternion algebra with center a totally real field H. This corresponds to A having Albert type II (when D is totally indefinite) or III (D totally definite).

Let λ be a prime of H not in $\mathrm{Ram}(D)$. We have seen that $V_\lambda(A) \simeq W_\lambda(A)^{\oplus 2}$. Following [**Chi90**] and [**BGK06, BGK10**], we will find a suitable isomorphic copy of $W_\lambda(A)$ such that $V_\lambda(A)$ inherits the nondegenerate pairing from Proposition 4.3.2.

Since $\lambda \notin \mathrm{Ram}(D)$, we have $D \otimes_H H_\lambda \simeq \mathrm{M}_2(H_\lambda)$. We take as generators for this algebra the matrices

$$t = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \; u = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

which satisfy the relations $u^2 = t^2 = 1$ and $tu = -ut$. As explained in Section 1.1, the irreducible $\mathrm{M}_2(H_\lambda)$-modules are isomorphic to H_λ^2. However, there are several ways to decompose $V_\lambda(A)$ as a sum of two submodules. We perform such a decomposition in two ways. Let $e = \frac{1}{2}(1+t)$, and

$$X := eV_\lambda(A),\ Y := (1-e)V_\lambda(A).$$

Then we have $V_\lambda(A) \simeq X \oplus Y$ (as $H_\lambda[G_k]$-modules). Moreover, the subspaces X and Y are isomorphic via multiplication by u. Hence $\dim_{H_\lambda} X = \dim_{H_\lambda} Y = \frac{1}{2}\dim_{H_\lambda} V_\lambda(A) = \frac{\dim A}{[H:\mathbb{Q}]}$.

Similarly, let $f = \frac{1}{2}(1+u)$, and

$$\tilde{X} := fV_\lambda(A),\ \tilde{Y} := (1-f)V_\lambda(A).$$

The same assertions as above hold for $\tilde{X}$ and $\tilde{Y}$: $V_\lambda(A) \simeq \tilde{X} \oplus \tilde{Y}$ as $H_\lambda[G_k]$-modules, $\tilde{X} \simeq \tilde{Y}$, and $\dim_{H_\lambda} \tilde{X} = \dim_{H_\lambda} \tilde{Y} = \frac{1}{2}\dim_{H_\lambda} V_\lambda(A)$.

Proposition 4.3.4. *The $H_\lambda[G_k]$-modules $X, Y, \tilde{X}$ and $\tilde{Y}$ are absolutely irreducible.*

Proof. By Theorem 4.2.2, we have $\mathrm{End}_{H_\lambda[G_k]}(V_\lambda(A)) \simeq D \otimes_H H_\lambda \simeq \mathrm{M}_2(H_\lambda)$. Since $V_\lambda(A)$ can be written as the direct sum of two copies of X, we have $\mathrm{End}_{H_\lambda[G_k]}(X) \simeq H_\lambda$. We conclude that X is absolutely irreducible. The same reasoning applies to $Y, \tilde{X}$ and $\tilde{Y}$. □

Since the modules X and Y are irreducible as $H_\lambda[G_k]$-modules, the following property holds: either they are both (maximal) isotropic with respect to the pairing

$$\phi_\lambda : V_\lambda(A) \times V_\lambda(A) \to H_\lambda(\chi_\ell)$$

introduced in Proposition 4.3.2, or ϕ_λ is a nondegenerate on both X and Y. The second case is moreover equivalent to X and Y being orthogonal, since ϕ_λ is alternating. The same reasoning holds for $\tilde{X}$ and $\tilde{Y}$.

4.3.2.1. *Type II.* We specialize to the case where D is totally indefinite. The following proof is a simplification of [**Chi90**, Lemma 3.3].

Lemma 4.3.5. *The modules X and Y are isotropic if and only if the modules $\tilde{X}$ and $\tilde{Y}$ are orthogonal.*

Proof. Suppose X and Y are maximal isotropic. Then for all $v, w \in V_\lambda(A)$ we have

$$\psi_\lambda(ev, ew) = \psi_\lambda(v, e^\dagger ew) = 0,$$
$$\psi_\lambda((1-e)v, (1-e)w) = \psi_\lambda(v, (1-e)^\dagger(1-e)w) = 0.$$

Since ψ_λ is nondegenerate, it follows that $e^\dagger e = 0$ and $(1-e)^\dagger(1-e) = 0$, and hence $e^\dagger = 1 - e$. By the Lemma 4.3.6 below, there exists a symmetric matrix $B \in \mathrm{M}_2(H_\lambda)$ such that the Rosati involution takes the form $A^\dagger = BA^\top B^{-1}$ for all A. By equating $e^\dagger = BeB^{-1} = 1 - e$ we obtain

$$B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

This gives $u^\dagger = BuB^{-1} = u$ and $t^\dagger = BtB^{-1} = -t$.

Now we have $ux = x$ for all $x \in \tilde{X}$, and $uy = -y$ for all $y \in \tilde{Y}$. Therefore we have

$$\psi_\lambda(x, y) = \psi_\lambda(ux, y) = \psi_\lambda(x, uy) = \psi_\lambda(x, -y),$$

which implies $\psi(x,y)=0$. Hence $\tilde{X}$ and $\tilde{Y}$ are orthogonal.

The argument is symmetric if we assume that $\tilde{X}$ and $\tilde{Y}$ are maximal isotropic: in that case, we obtain the equality $f^\dagger = 1-f$, which in turn implies that the Rosati involution takes the form $A^\dagger = BA^\top B^{-1}$ with $B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Hence $u^\dagger = -u$, $t^\dagger = t$. We conclude that X and Y are orthogonal, since $tx = x$ for all $x \in X$ and $ty = -y$ for all $y \in Y$. □

Lemma 4.3.6. *Let A be a simple abelian variety such that $D = \mathrm{End}^0(A)$ has Albert type II. Let H be the center of X, and let λ be a prime of H where D splits. Then, the Rosati involution on D_λ is given by $X^\dagger = BX^\top B^{-1}$ for all $X \in D_\lambda$, where $B \in D_\lambda \simeq \mathrm{M}_2(H_\lambda)$ is a symmetric matrix.*

Proof. Since † and $^\top$ are both involutions fixing every element of the center H of D_λ, by Skolem–Noether (cf. Theorem 1.1.3) there exists some $B \in D_\lambda$ (up to multiplication by scalars in $H_\lambda^\times$) such that $X^\dagger = BX^\top X^{-1}$ for all $X \in D_\lambda$. Hence we have

$$X = X^{\dagger\dagger} = B(B^{-1})^\top X B^\top B^{-1}$$

for all $X \in D_\lambda$, and therefore $B = \varepsilon B^\top$ for some $\varepsilon \in H$. On the other hand, $B = B^{\top\top} = \varepsilon^2 B$, from which we know that $\varepsilon \in \{+1,-1\}$. Hence B is either symmetric or antisymmetric.

Suppose B is antisymmetric. Then we can multiply B by a constant so that it takes the form $B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Hence the Rosati involution takes the form

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^\dagger = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}.$$

This would imply that $\dim_{H_\lambda}\{X \in D \otimes_H H_\lambda \mid X^\dagger = X\} = 2$. But this is in contradiction with Table 1.1, since D is of Albert type II, and we know the dimension of the elements fixed by Rosati is 3. Therefore B is a symmetric matrix. □

Putting everything together, we obtain the following result.

Theorem 4.3.7. *Let A/k be a simple abelian variety such that $D = \mathrm{End}^0(A)$ has Albert type II. Let H be the center of D. For every prime λ where D splits, there exists an absolutely irreducible $H_\lambda[G_k]$-submodule $W_\lambda(A)$ of $V_\lambda(A)$ such that*

(1) $\dim_{H_\lambda} W_\lambda(A) = \frac{\dim A}{[H:\mathbb{Q}]}$.
(2) $V_\lambda(A) \simeq W_\lambda(A) \oplus W_\lambda(A)$.
(3) There exists a nondegenerate, H_λ-bilinear, alternating, G_k-equivariant pairing

$$\psi_\lambda : W_\lambda(A) \times W_\lambda(A) \to H_\lambda(\chi_\ell).$$

Proof. We choose $W_\lambda(A)$ to be the submodule X or $\tilde{X}$ of $V_\lambda(A)$, according to whether $\tilde{X}$ or X is isotropic for $\phi_\lambda : V_\lambda(A) \times V_\lambda(A) \to H_\lambda(\chi_\ell)$. The isomorphisms $X \simeq Y$ and $\tilde{X} \simeq \tilde{Y}$ give the decomposition of $V_\lambda(A)$ and the dimension of $W_\lambda(A)$. Finally, we let $\psi_\lambda := \phi_\lambda|_{W_\lambda(A)\times W_\lambda(A)}$. □

Remark 4.3.8. *Let ψ be a nondegenerate alternating form on an n-dimensional F-vector space V. Recall that the symplectic similitude group of ψ is*

$$\mathrm{GSp}_n(F) = \{g \in \mathrm{GL}(V) \mid \psi(gv,gw) = \chi(g)\psi(v,w), \ \text{all } v,w \in V\}$$

where $\chi(g) \in F^\times$ is the similitude of g.

Given a prime $\lambda \notin \mathrm{Ram}(D)$, the representation $\rho_{A,\lambda} : G_k \to \mathrm{GL}_n(H_\lambda)$ given by the action of G_k on $W_\lambda(A)$ has image in $\mathrm{GSp}_n(H_\lambda)$, where $n = \dim_{H_\lambda} W_\lambda$. For a prime $\lambda \in \mathrm{Ram}(D)$, we have a representation $\rho_{A,\lambda} : G_k \to \mathrm{GL}_{n/2}(D_\lambda)$, which holds a similar restriction. Indeed, let $\mathcal{E} \subset D_\lambda$ be a maximal subfield. Then the representation $\rho_{A,\lambda} \otimes_{H_\lambda} \mathcal{E}$ takes values in $\mathrm{GL}_n(\mathcal{E})$, and by the compatibility of the system of representations we in fact find that the image lies in $\mathrm{GSp}_n(\mathcal{E})$.

4.3.2.2. *Type III.* We now specialize to the case in which $D = \mathrm{End}^0(A)$ is totally definite. As above we let λ be a prime of H such that D splits, and again we take the generators

$$t = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \, u = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

for $D \otimes_H H_\lambda \simeq \mathrm{M}_2(H_\lambda)$. We let $e = \frac{1}{2}(1+t)$ and $f = \frac{1}{2}(1+u)$, and then define the following subspaces of $V_\lambda(A)$:

$$X := eV_\lambda(A), \, Y := (1-e)V_\lambda(A);$$
$$\tilde{X} := fV_\lambda(A), \, \tilde{Y} := (1-f)V_\lambda(A).$$

We again have isomorphisms of $H_\lambda[G_k]$-modules $X \simeq Y$, $\tilde{X} \simeq \tilde{Y}$, and $V_\lambda(A) \simeq X \oplus Y \simeq \tilde{X} \oplus \tilde{Y}$. However, we encounter the following problem.

Lemma 4.3.9. *The subspaces X, Y, $\tilde{X}$ and $\tilde{Y}$ are all isotropic with respect to the pairing ϕ_λ.*

Proof. By Theorem 1.4.1, the Rosati involution † on D, and hence on $D \otimes_H H_\lambda$, is the standard involution. Hence for all $x \in \mathrm{M}_2(H_\lambda)$ we have

$$x^\dagger = \mathrm{Tr}\, x - x.$$

By direct computation we obtain $e^\dagger = 1 - e$ and $f^\dagger = 1 - f$. In particular, we obtain $e^\dagger e = 0$. Hence for all $v, w \in V_\lambda(A)$, we have

$$\phi_\lambda(ev, ew) = \phi_\lambda(v, e^\dagger ew) = 0.$$

This shows that X is isotropic. The similar equalities $(1-e)^\dagger(1-e) = 0$ and $f^\dagger f = (1-f)^\dagger(1-f) = 0$ show that $Y, \tilde{X}$ and $\tilde{Y}$ are isotropic too. □

To define a pairing on the subspaces of $V_\lambda(A)$, we let $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and define

$$\psi_\lambda(v, w) := \phi_\lambda(Jv, w)$$

for all $v, w \in V_\lambda(A)$. This is an H_λ-bilinear, nondegenerate, G_k-equivariant pairing. We have the following properties.

Lemma 4.3.10. *The pairing ψ_λ is symmetric, and for all $B \in \mathrm{M}_2(H_\lambda)$ and $v, w \in V_\lambda(A)$ we have*

$$\psi_\lambda(Bv, w) = \psi_\lambda(v, B^\top w).$$

Moreover, X (resp. $\tilde{X}$) is orthogonal to Y (resp. $\tilde{Y}$) with respect to ψ_λ.

Proof. We first note that $J^\dagger = -J = J^\top = J^{-1}$. With this and the property that $\phi_\lambda(Bv, w) = \phi_\lambda(v, B^\dagger w)$ we have

$$\begin{aligned} \psi_\lambda(v, w) = \phi_\lambda(Jv, w) = -\phi_\lambda(J^\dagger w, v) = \phi_\lambda(Jw, v) \\ = \psi_\lambda(w, v). \end{aligned}$$

Hence ψ_λ is symmetric. For the second property, we have already noted that $B^\dagger = J^{-1}B^\top J = J^\dagger B^\top J$ for every $B \in \mathrm{M}_2(H_\lambda)$. Therefore $B^\dagger J^\dagger = J^\dagger B^\top$, and

$$\begin{aligned}\psi_\lambda(Bv, w) &= \phi_\lambda(JBv, w) = \phi_\lambda(v, B^\dagger J^\dagger w)\\ &= \phi_\lambda(v, J^\dagger B^\top w) = \phi_\lambda(Jv, B^\top w) = \psi_\lambda(v, B^\top w).\end{aligned}$$

To see that X and Y are orthogonal, note that $e^\top = e = e^2$, and so for all $v, w \in V_\lambda(A)$ we have

$$\psi_\lambda(ev, (1-e)w) = \psi_\lambda(v, e(1-e)w) = 0.$$

Similarly, we have $f^\top = f = f^2$, and hence $\tilde{X} = fV_\lambda(A)$ and $\tilde{Y} = (1-f)V_\lambda(A)$ are also orthogonal. □

Theorem 4.3.11. *Let A/k be a simple abelian variety such that $D = \mathrm{End}^0(A)$ has Albert type III. Let H be the center of D. For every prime λ where D splits, there exists an absolutely irreducible $H_\lambda[G_k]$-submodule $W_\lambda(A)$ of $V_\lambda(A)$ such that*

(1) $\dim_{H_\lambda} W_\lambda(A) = \frac{\dim A}{[H:\mathbb{Q}]}$.
(2) $V_\lambda(A) \simeq W_\lambda(A) \oplus W_\lambda(A)$.
(3) There exists a nondegenerate, H_λ-bilinear, symmetric, G_k-equivariant pairing

$$\psi_\lambda : W_\lambda(A) \times W_\lambda(A) \to H_\lambda(\chi_\ell).$$

Proof. Everything is proven by Lemma 4.3.10: we only need to choose $W_\lambda(A)$ to be X (in fact, we may also choose $Y, \tilde{X}$, or $\tilde{Y}$), and then consider the restriction of the pairing ψ_λ on $V_\lambda(A)$ to $W_\lambda(A)$. □

Remark 4.3.12. *Let ψ be a nondegenerate symmetric form on an n-dimensional F-vector space V. Recall that the orthogonal similitude group of ψ is*

$$\mathrm{GO}_n(F) = \{g \in \mathrm{GL}(V) \mid \psi(gv, gw) = \chi(g)\psi(v, w), \text{ all } v, w \in V\}$$

where $\chi(g) \in F^\times$ is the similitude of g.

The content of Remark 4.3.8 holds as well in Albert type III with the appropriate change. For $\lambda \notin \mathrm{Ram}(D)$ the representations $\rho_{A,\lambda} : G_k \to \mathrm{GL}_n(H_\lambda)$ take values in $\mathrm{GO}_n(H_\lambda)$. Meanwhile, if $\lambda \in \mathrm{Ram}(D)$ and $\mathcal{E} \subset D_\lambda$ is a maximal subfield, then the representation $\rho_{A,\lambda} \otimes_{H_\lambda} \mathcal{E}$ takes values in $\mathrm{GO}_n(\mathcal{E})$.

4.3.3. Albert Type IV. We conclude the chapter with a brief mention of the remaining Albert type. Suppose that H is a CM field, so that $D = \mathrm{End}^0(A)$ is an algebra with Albert type IV. Let λ be a prime of H. In the same spirit as for the first three Albert types, we wish to endow $V_\lambda(A)$ with some nondegenerate pairing that helps us study the action of Galois.

Denote by H^+ be the maximal totally real field in H and let $\bar{\cdot} : H \to H$ denote complex conjugation. This induces an involution on the étale $\mathbb{Q}_\ell$-algebra $H_\ell := H \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$, namely $\bar{\cdot} \otimes \mathrm{id} : H \otimes \mathbb{Q}_\ell \to H \otimes \mathbb{Q}_\ell$. Recall that a pairing ψ on a free H_ℓ-module V is hermitian if it is H_ℓ-linear in the first component, and for all $v, w \in V$ we have $\psi(v, w) = \overline{\psi(w, v)}$. We have the following lemma from [**Chi91**].

Lemma 4.3.13. *Let $j \in H^\times$ be such that $\bar{j} = -j$. There exists a unique nondegenerate, G_k-equivariant, hermitian pairing*

$$\Phi_\ell : V_\ell(A) \times V_\ell(A) \to H_\ell(\chi_\ell)$$

such that $\mathrm{Tr}_{H_\ell/\mathbb{Q}_\ell}(j\Phi_\ell) = \psi_\ell$.

PROOF (SKETCH). This is shown in a similar fashion to Proposition 4.3.2 for H totally real. The key difference is that the Rosati involution restricted to H acts as complex conjugation, so that $\psi_\ell(fv, w) = \psi_\ell(v, \bar{f}w)$ for all $v, w \in V_\ell(A)$ and all $f \in H$. In other words, ψ_ℓ is an $H \otimes \mathbb{Q}_\ell$-bilinear pairing $V_\ell(A) \times U_\ell(A) \to \mathbb{Q}_\ell(\chi_\ell)$, where $U_\ell(A) := V_\ell(A) \otimes_{H \otimes \mathbb{Q}_\ell} H \otimes \mathbb{Q}_\ell$ by taking the tensor via the involution $\bar{\cdot} \otimes \mathrm{id}$. Lemma 4.3.1 yields a unique biadditive pairing

$$\tilde{\Phi}_\ell : V_\ell(A) \times V_\ell(A) \to H_\ell$$

with $\mathrm{Tr}_{H_\ell/\mathbb{Q}_\ell}(\tilde{\Phi}_\ell) = \psi_\ell$ which is H_ℓ-linear in the first variable and H_ℓ-antilinear in the second variable. One then defines $\Phi_\ell := j^{-1}\tilde{\Phi}_\ell$ and checks the remaining properties for Φ_ℓ. See [**Chi91**, Lemma 2.2] and [**BKG21**, §3] for further details. □

Notice that the action of complex conjugation on $H_\ell \simeq \prod_{\lambda|\ell} H_\lambda$ exchanges the factors H_λ and $H_{\bar{\lambda}}$. This poses an issue when trying to restrict the pairing Φ_ℓ to each factor $V_\lambda(A)$ of $V_\ell(A)$. We can circumvent this by restricting to certain primes.

Proposition 4.3.14. *Suppose* $\mathrm{End}^0(A) = H$ *is commutative. Let* λ *be a prime of* H, λ_0 *the prime of* H^+ *below it, and suppose that* λ_0 *is inert in* H *(so that* $[H_\lambda : H^+_{\lambda_0}] = 2$*). Then* Φ_ℓ *restricts to a nondegenerate,* G_k*-equivariant,* H_λ*-hermitian pairing*

$$\phi_\lambda : V_\lambda(A) \times V_\lambda(A) \to H_\lambda(\chi_\ell).$$

More care has to be taken when D has Schur index $t_A > 1$. As explained in Section 4.2, we still have a decomposition $V_\lambda(A) \simeq W_\lambda(A)^{\oplus t_A}$. However, the results on the existence of a pairing are less developed. We summarize the situation in the following result and refer to [**BKG21**] for the remaining details.

Theorem 4.3.15 (Banaszak, Kaim-Garnek)**.** *There is a positive density set* $\mathcal{L}$ *of primes of* H *such that, if* $\lambda \in \mathcal{L}$*, there exists a nondegenerate, bilinear,* H_λ*-hermitian,* G_k*-equivariant pairing*

$$\phi_\lambda : W_\lambda(A) \times W_\lambda(A) \to H_\lambda(\chi_\ell).$$

CHAPTER 5

Abelian varieties genuinely of GL_n-type

Throughout this chapter, we let k be a number field and A an abelian variety defined over k. We say that A is *of* GL_n*-type* for some positive integer n if there is a number field E with an embedding $E \to \mathrm{End}^0(A)$ and such that $[E : \mathbb{Q}] = \frac{2\dim A}{n}$. We say that A is *genuinely of* GL_n*-type* if A is simple, of GL_n-type, and $A_{\bar{k}}$ has no isogeny factor of GL_m-type for $m < n$. In this chapter, we study the Galois representations introduced in the previous chapter for A, mainly under the assumption that A is genuinely of GL_n-type.

We start in Section 5.1 by studying the possible endomorphism algebras for an abelian variety A of GL_n-type. We then introduce in Section 5.2 the hypothesis that A is genuinely of GL_n-type, and study its decomposition over $\bar{k}$. This yields the notion of the building block associated to A. Section 5.3 is somewhat technical and deals with Galois descent on the field of coefficients of representations. We use the results in Section 5.4, where we finish proving Theorem 4.2.7 for arbitrary Schur indices of $\mathrm{End}^0(A)$.

The next few sections focus on abelian varieties geometrically of the first kind. We introduce the inner twists of A in Section 5.5, and in particular we define the Nebentype character. In Section 5.6 we give a characterization of the property of being geometrically of the first kind. In Section 5.7 we show that the representations attached to these varieties take values in a symplectic or orthogonal group. We end the chapter in Section 5.8 with a description of the abelian varieties genuinely of GL_4-type that correspond to automorphic representations of $\mathrm{GSp}_4(\mathbb{A}_\mathbb{Q})$.

A substantial portion of this chapter is joint work with Francesc Fité and Xavier Guitart, and has been written up in [**FFG24**].

5.1. Endomorphism algebra and isogeny decomposition

Let k be a number field and A an abelian variety defined over k. Let E be a number field and let $E \to \mathrm{End}^0(A)$ be an embedding. After fixing some embedding $k \to \mathbb{C}$, the $\mathbb{Q}$-vector space $V = H^1(A(\mathbb{C})^{top}, \mathbb{Q})$ has dimension $2\dim A$, and by functoriality we obtain an embedding $E \to \mathrm{End}_\mathbb{Q}(V) \simeq \mathrm{M}_{2\dim A}(\mathbb{Q})$. Hence $[E : \mathbb{Q}]$ divides $2\dim A$.

Definition 5.1.1. *Let* $n := \frac{2\dim A}{[E:\mathbb{Q}]}$. *We say* A *is* of GL_n-type.

For example, if $n = 1$ then E is necessarily a CM field (cf. Table 1.1), and we also say A has complex multiplication by E. Abelian varieties of GL_2-type defined over $\mathbb{Q}$ have been studied in relation to the Shimura–Taniyama conjecture, see [**Rib76, Rib04**]. Any abelian surface is of GL_4-type by taking $E = \mathbb{Q}$.

As explained in Section 4.2, to every abelian variety A of GL_n-type we can attach a compatible system of Galois representations with values in a form of GL_n, coming from the irreducible subrepresentations of the Tate module.

In this section, we study the endomorphism algebra (and thus the isogeny decomposition) of an abelian variety A/k of GL_n-type. We begin by quoting the following result (cf. [**Rib04**, Theorem 2.1] and [**Shi72**, Proposition 1.5]).

Proposition 5.1.2. *Let A/k be an abelian variety of GL_2-type. Then one of the following is true.*

(i) A is k-isogenous to a product of abelian varieties of GL_1-type.
(ii) A is k-isogenous to the power $(A')^r$ of a simple abelian variety A'/k, which is of GL_2-type and not of GL_1-type. The algebra $\mathrm{End}^0(A')$ is either a number field of degree $\dim A'$, or a division quaternion algebra over a number field of degree $\dim A'/2$.

Before generalizing the result above, we observe the following straightforward fact: if A is of GL_n-type and E is a field in $\mathrm{End}^0(A)$ such that $n = 2\dim A/[E:\mathbb{Q}]$, then A^r is of GL_n-type for all $r \geq 1$. Indeed, $\mathrm{End}^0(A^r) = \mathrm{M}_r(\mathrm{End}^0(A))$ contains fields of degree $r[E:\mathbb{Q}]$, and $n = \frac{2r\dim A}{r[E:\mathbb{Q}]}$.

Proposition 5.1.3. *Let A/k be an abelian variety of GL_n-type. Then one of the following is true.*

(i) A is k-isogenous to a product $A_1 \times \cdots \times A_s$, $s \geq 1$, where each A_i is of GL_{n_i}-type for some $n_i < n$.
(ii) A is k-isogenous to $(A')^r$, where A' is a simple abelian variety defined over k which is of GL_n-type and not of GL_m-type for any $m < n$. Moreover, $\mathrm{End}^0(A')$ is a division algebra of Schur index $t_{A'}$ over a number field H with $[H:\mathbb{Q}] = \frac{2\dim A'}{nt_{A'}}$, and $t_{A'} \mid n$.

Proof. Write $A \sim A_1 \times \cdots \times A_s$, with each A_i an isotypical variety such that $\mathrm{Hom}(A_i, A_j) = 0$ for all $i \neq j$. Fix a field E with an embedding $E \to \mathrm{End}^0(A)$, so that $n = 2\dim A/[E:\mathbb{Q}]$. Then we have for each i an embedding $E \to \mathrm{End}^0(A_i)$. Hence there exist integers $n_1 \ldots, n_s$ such that $n_i = \frac{2\dim A_i}{[E:\mathbb{Q}]}$. If $s \geq 2$, we obtain

$$n_i = \frac{2\dim A_i}{[E:\mathbb{Q}]} < \frac{2\dim A}{[E:\mathbb{Q}]} = n.$$

This shows most of (i): the only remaining case is when $s = 1$, and $\mathrm{End}^0(A)$ contains a number field of degree strictly larger than $[E:\mathbb{Q}]$, which again yields $n_1 < n$.

Suppose now that $s = 1$ and $A \sim (A')^r$ with A' not of GL_m-type for $m < n$. Our task is to show A is not of GL_m-type for any $m < n$, and to describe $\mathrm{End}^0(A')$. Let D be the centralizer of E in $\mathrm{End}^0(A)$. We claim that D is a division algebra. This is equivalent to saying that every $\lambda \in \mathrm{End}(A)$ that commutes with E is an isogeny. Indeed, if that was not the case then the image of λ would be an abelian subvariety B of A with $\dim B < \dim A$. In particular, B would be isotypical. Since λ and E commute, there would exist an embedding $E \to \mathrm{End}^0(B)$, and hence an integer $d = \frac{2\dim B}{[E:\mathbb{Q}]}$ such that B is of GL_d-type. By induction on d (and using Proposition 5.1.2), it follows that B is isogenous to a power of an abelian variety of GL_d-type. Hence A' is of GL_d-type. But

$$d = \frac{2\dim B}{[E:\mathbb{Q}]} < \frac{2\dim A}{[E:\mathbb{Q}]} = n,$$

which contradicts the assumption that A' is not of GL_d-type. Hence D is a division algebra.

Now E must be a maximal subfield of D, since otherwise A would be of GL_m-type for some $m < n$. The Double Centralizer theorem (cf. Theorem 1.1.4) implies that $D = E$ and E is maximal in $\mathrm{End}^0(A)$. Now if we let

- $Q = \mathrm{End}^0(A')$,
- H the center of Q, and
- $t_{A'} = \mathrm{ord}_H[Q]$ the Schur index of Q,

then $\mathrm{End}^0(A) = \mathrm{M}_r(Q)$, and $[E : H] = rt_{A'}$. Hence

$$[H : \mathbb{Q}] = \frac{[E : \mathbb{Q}]}{[E : H]} = \frac{2r \dim A'}{nrt_{A'}} = \frac{2 \dim A'}{nt_{A'}}.$$

We now have that $H^1((A')^{top}_{\mathbb{C}}, \mathbb{Q})$ is a free left Q-module, and $\dim_{\mathbb{Q}} Q = t^2_{A'}[H : \mathbb{Q}]$ divides $2 \dim A' = nt_{A'}[H : \mathbb{Q}]$. It follows that $t_{A'} \mid n$. Finally we see that A' is of GL_n-type, since Q contains a (maximal) number field of degree $t_{A'}[H : \mathbb{Q}] = \frac{2 \dim A'}{n}$. □

Remark 5.1.4. *It A falls in Case (ii) of Proposition 5.1.3, then then we have seen that the field E is maximal in* $\mathrm{End}^0(A)$. *In particular, E contains the center H of* $\mathrm{End}^0(A)$. *Let $t_A = \mathrm{ord}_H[\mathrm{End}^0(A)]$ be the Schur index of* $\mathrm{End}^0(A)$. *If A is simple, then we have*

$$2 \dim A = n[E : \mathbb{Q}] = nt_A[H : \mathbb{Q}].$$

Example 5.1.5. *Let A/k be an abelian variety of* GL_4*-type which lands in Case (i) of Proposition 5.1.3. Then A is k-isogenous to the product of either:*

(a) four abelian varieties of GL_1*-type, all of the same dimension* $\dim A/4$*;*
(b) two abelian varieties of GL_1*-type of dimension* $\dim A/4$*, and an abelian variety of* GL_2*-type and dimension* $\dim A/2$*;*
(c) two abelian varieties of GL_2*-type, each of dimension* $\dim A/2$*;*
(d) an abelian variety of GL_1*-type and dimension* $\dim A/4$ *times one of* GL_3*-type and dimension* $3 \dim A/4$.

The stated isogeny factors may be isogenous (so that we have a power of a GL_1 *or* GL_2*-type abelian variety). Each possible isogeny factor can in turn be isotypical.*

Example 5.1.6. *Let A be an abelian variety over k and of* GL_4*-type which satisfies Case (ii) of Proposition 5.1.3. Then $A \sim (A')^r$, where A' is of* GL_4*-type, and* $\mathrm{End}^0(A')$ *is either:*

(a) a totally real field of degree $\dim A'/2$*;*
(b) a quaternion algebra over a totally real field of degree $\dim A'/4$*;*
(c) a CM field of degree $\dim A'/2$*;*
(d) a quaternion algebra over a CM field of degree $\dim A'/4$*;*
(e) a division algebra of Schur index 4 over a CM field of degree $\dim A'/8$.

Proposition 5.1.7. *Let A be an abelian variety over k of* GL_n*-type. Suppose that k is a number field and $[k : \mathbb{Q}]$ is coprime with $2[E : \mathbb{Q}]$. If A falls in Case (ii) of Proposition 5.1.3, then $2t_A$ divides n. In particular, n is even.*

Proof. Let $A \sim (A')^r$ with A' simple. Let $V = \mathrm{Lie}(A')$ be the tangent space at the origin of A', this is a k-vector space of k-dimension $\dim A'$. Hence we have $\dim_{\mathbb{Q}} V = [k : \mathbb{Q}] \dim A'$. By functoriality it is also a free left $\mathrm{End}^0(A')$-module,

and so $\dim_{\mathbb{Q}} \mathrm{End}^0(A') = t_{A'}^2[H:\mathbb{Q}]$ divides $[k:\mathbb{Q}]\dim A' = [k:\mathbb{Q}]\frac{nt_{A'}[H:\mathbb{Q}]}{2}$. It follows that $2t_{A'}$ divides $[k:\mathbb{Q}]n$. Since $[k:\mathbb{Q}]$ is coprime with $2[E:\mathbb{Q}]$, it is also coprime with $2t_{A'}$, and hence $2t_{A'}$ divides n. The statement follows since $t_A = \mathrm{ord}_H[\mathrm{End}^0(A)] = \mathrm{ord}_H[\mathrm{End}^0(A')] = t_{A'}$. □

Definition 5.1.8. *Let A/k be an abelian variety of GL_n-type. We say A is genuinely of GL_n-type if $A_{\bar{k}}$ has no simple isogeny factor of GL_m-type for $m < n$. Equivalently, we ask that $A_{\bar{k}}$ is of GL_n-type and satisfies Case (ii) of Proposition 5.1.3.*

Proposition 5.1.9. *A simple abelian variety A is genuinely of GL_n-type for some n if and only if it $\mathrm{End}^0(A_{\bar{k}})$ is simple, and there exists a maximal subfield of $\mathrm{End}^0(A)$ which is also maximal in $\mathrm{End}^0(A_{\bar{k}})$.*

Proof. Suppose that A is genuinely of GL_n-type. Then by Case (ii) of Proposition 5.1.3 applied to $A_{\bar{k}}$ we obtain that $A_{\bar{k}}$ is isotypical, and so $\mathrm{End}^0(A_{\bar{k}})$ is simple. The proof of the same result (cf. Remark 5.1.4) shows that there is a maximal subfield E of $\mathrm{End}^0(A)$ which is also maximal in $\mathrm{End}^0(A_{\bar{k}})$.

We now show the converse. Since we assume that $\mathrm{End}^0(A_{\bar{k}})$ is simple, there exists a simple abelian variety B over $\bar{k}$ such that $A_{\bar{k}} \sim B^r$. Let E be a maximal subfield of $\mathrm{End}^0(A)$ which is also maximal in $\mathrm{End}^0(A_{\bar{k}}) \simeq \mathrm{M}_r(\mathrm{End}^0(B))$. If we let F be the center of $\mathrm{End}^0(B)$ and $t_B = \mathrm{ord}_F[\mathrm{End}^0(B)]$ the Schur index of $\mathrm{End}^0(B)$, then we have the equality

$$[E:\mathbb{Q}] = rt_B[F:\mathbb{Q}] = \frac{2\dim A}{n}.$$

On the other hand, a maximal subfield E' of $\mathrm{End}^0(B)$ has degree $[E':\mathbb{Q}] = t_B[F:\mathbb{Q}] = \frac{2\dim B}{m}$, where m is the minimal integer such that B is of GL_m-type. We end the proof by noting that

$$nrt_B[F:\mathbb{Q}] = 2\dim A = 2r\dim B = mrt_B[F:\mathbb{Q}],$$

from which we obtain $m = n$. Hence $A_{\bar{k}}$ has a single isotypical factor of GL_n-type, with n minimal. Therefore A is genuinely of GL_n-type. □

5.2. GL_n-type building blocks

Let k be a number field and let L/k be a Galois extension. Let B/L be an abelian variety. We say B is a *strong k-variety relative to L* [1] if for every $s \in \mathrm{Gal}(L/k)$ there is an L-isogeny $\mu_s : {}^sB \to B$ and, for every $s \in \mathrm{Gal}(L/k)$ and every $\varphi \in \mathrm{End}(B)$ we have the equality

$$\varphi \circ \mu_s = \mu_s \circ {}^s\varphi.$$

In the literature, one usually says *B is a k-variety* if $B_{\bar{k}}$ is a strong k-variety relative to $\bar{k}$.

Definition 5.2.1. *Let n be a positive integer. We say a variety $B/\bar{k}$ is a k-building block of GL_n-type if the following conditions are satisfied:*

(1) B is a strong k-variety relative to $\bar{k}$, and
(2) $\mathrm{End}^0(B)$ is a division algebra with center F and Schur index t_B such that

$$nt_B[F:\mathbb{Q}] = 2\dim B.$$

[1] We will discuss the notion of a weak k-variety in Chapter 7

Lemma 5.2.2. *Let A/k be a simple abelian variety genuinely of GL_n-type, so that $A_{\bar{k}} \sim B^r$ for a k-building block B. Let H and F denote the respective centers of $\mathrm{End}^0(A)$ and $\mathrm{End}^0(B)$. Then $F \subseteq H$.*

Proof. From Proposition 5.1.9, the simple algebras $\mathrm{End}^0(A)$ and $\mathrm{End}^0(A_{\bar{k}}) \simeq \mathrm{M}_r(\mathrm{End}^0(B))$ have a common maximal subfield, say E. Hence $F \subseteq E \subseteq \mathrm{End}^0(A)$. Since F commutes with all of $\mathrm{End}^0(A)$, we obtain $F \subseteq H$. □

Proposition 5.2.3. *Let A/k be genuinely of GL_n-type. Then, the isotypical factor B of $A_{\bar{k}}$ is a GL_n-type k-building block.*

Proof. By Lemma 5.2.2, for every $s \in G_k$ the map

$$\begin{aligned} \mathrm{End}^0(A_{\bar{k}}) &\to \mathrm{End}^0(A_{\bar{k}}) \\ \varphi &\mapsto {}^s\varphi \end{aligned}$$

is an F-algebra homomorphism. By the Skolem–Noether theorem (cf. Theorem 1.1.3) there exists some $\alpha(s) \in \mathrm{End}^0(A_{\bar{k}})^\times$ such that ${}^s\varphi = \alpha(s)\varphi\alpha(s)^{-1}$. Since A is defined over k, we have ${}^sA_{\bar{k}} = A_{\bar{k}}$, and so $\alpha(s)$ is an isogeny ${}^sA_{\bar{k}} \to A_{\bar{k}}$. Hence $A_{\bar{k}}$ is an abelian k-variety. By [**Gui10**, Proposition 3.2], B is also an abelian k-variety. □

From now on, if A/k is an abelian variety genuinely of GL_n-type and $A_{\bar{k}} \sim B^r$ with B simple, we say B is the *building block associated to* A.

Proposition 5.2.4. *Let $B/\bar{k}$ be a GL_n-type k-building block for some n. There exists an abelian variety A defined over k which is genuinely of GL_n-type and whose associated building block is B.*

Proof. By [**Gui12**, Theorem 2.5], there exists an abelian variety A defined over k such that $A_{\bar{k}} \sim B^r$ for some r, and such that $E = \mathrm{End}^0(A)$ is a field which is maximal in $\mathrm{End}^0(A_{\bar{k}})$. As B is of GL_n-type, we need to show that A is of GL_n-type as well. Let F and t_B be the center and Schur index of $\mathrm{End}^0(B)$, respectively. Then we have $[E : \mathbb{Q}] = rt_B[F : \mathbb{Q}]$, and so

$$\frac{2\dim A}{[E:\mathbb{Q}]} = \frac{2r\dim B}{rt_B[F:\mathbb{Q}]} = \frac{2\dim B}{t_B[F:\mathbb{Q}]} = n.$$

We have indeed shown that A is of GL_n-type. □

Proposition 5.2.5. *Let A be an abelian variety genuinely of GL_n-type and let B be its associated building block. Let H and F be the respective centers of $\mathrm{End}^0(A)$ and $\mathrm{End}^0(B)$. Then, the equality of Brauer classes*

$$[\mathrm{End}^0(A)] = [\mathrm{End}^0(B) \otimes_F H]$$

holds in $\mathrm{Br}(H)$. In particular, $\mathrm{ord}_H[\mathrm{End}^0(A)]$ divides $\mathrm{ord}_F[\mathrm{End}^0(B)]$.

Proof. By Proposition 5.1.9, the algebras $\mathrm{End}^0(A)$ and $\mathrm{End}^0(A_{\bar{k}}) \simeq \mathrm{M}_r(\mathrm{End}^0(B))$ share a maximal field, say E. The equality of Brauer classes is then given by Theorem 2.4.5 and the fact that $[\mathrm{End}^0(A_{\bar{k}})] = [\mathrm{End}^0(B)]$. The divisibility between Schur indices follows from the fact that

$$\mathrm{Br}(F) \to \mathrm{Br}(H),\ [X] \mapsto [X \otimes_F H]$$

is a group homomorphism. □

Recall from Section 1.4 that an algebra X with positive involution is *of the first kind* if the involution restricts to the identity on the center Z of X, otherwise we say X of the second kind. According to Theorem 1.4.1, X being of the first kind is equivalent to Z being totally real, and to X having Albert type I, II or III.

Definition 5.2.6. *Let A/k be an abelian variety genuinely of GL_n-type with associated building block $B/\bar{k}$. We say A is* of the first kind *(resp.* second kind*) if the endomorphism algebra $\mathrm{End}^0(A)$ is of the first kind (resp. second kind).*

We say A is geometrically of the first kind *(resp.* geometrically of the second kind*) if the building block B is of the first kind (resp. second kind).*

Remark 5.2.7. *If k has a real embedding and A/k is genuinely of GL_2-type then* [**Shi63**, Theorem 5] *implies that A is geometrically of the first kind (see* [**Gui12**, Proposition 3.4] *for a proof). The properties of the Galois representation associated to such an A when $k = \mathbb{Q}$ were explained in* [**Rib04**]*. In the subsequent sections we will show that the representation associated to an abelian variety geometrically of the first kind (and genuinely of GL_n-type, any n) has many of these properties.*

Remark 5.2.8. *If A is geometrically of the first kind, then n is even. This can be checked on the building block B. Indeed, if $\mathrm{End}^0(B) = F$ has Albert type I, then by Table 1.1 we have $[F : \mathbb{Q}] \mid \dim B$, and so $n = 2 \dim B/[F : \mathbb{Q}]$ is even. If $\mathrm{End}^0(B)$ has Albert type II or III, then from Proposition 5.1.3 we know $\mathrm{ord}_F[\mathrm{End}^0(B)] = 2$ divides n.*

Proposition 5.2.9. *Let A be an abelian variety genuinely of GL_n-type and let B be its associated building block. If A is of the first kind, then B is also of the first kind. More precisely,*

(i) If A has Albert type I, then B has Albert type I or II.
(ii) If A has Albert type II, then B has Albert type II.
(iii) If A has Albert type III, then B has Albert type III.

Proof. If we let H and F be the respective centers of $\mathrm{End}^0(A)$ and $\mathrm{End}^0(B)$, then we have seen that $F \subseteq H$, and

$$[\mathrm{End}^0(A)] = [\mathrm{End}^0(B) \otimes_F H].$$

If A is of the first kind, then H is totally real, and therefore F is totally real. Hence B is also of the first kind. Assuming H totally real, the Brauer class equation tells us that the real places of $\mathrm{End}^0(A)$ are ramified if and only if the real places of $\mathrm{End}^0(B)$ are ramified. In addition, if t_A and t_B are the respective Schur indices of these algebras, we have $t_A \mid t_B$.

If A has Albert type II or III then this says $t_A = 2 = t_B$, and the Albert type of B has to coincide with that of A. If A has Albert type I, then $\mathrm{End}^0(A)$ is split at the real places, and so must be $\mathrm{End}^0(B)$. Hence B has Albert type I or II. □

Corollary 5.2.10. *Let A be an abelian variety genuinely of GL_n-type and geometrically of the first kind. Then $\mathrm{End}^0(A)$ is a field or a quaternion algebra. In addition, if B is the building block associated to A, and $\mathrm{End}^0(A)$ is a quaternion algebra, then $\mathrm{End}^0(B)$ is a quaternion algebra.*

5.3. Descent of trace fields

In this section, we let $\mathbb{E}/\mathbb{H}$ be a finite Galois extension with Galois group $\Delta = \mathrm{Gal}(\mathbb{E}/\mathbb{H})$. Let G be a group, and consider a representation

$$\rho : G \to \mathrm{Aut}_{\mathbb{E}}(\mathbb{E}^n) \simeq \mathrm{GL}_n(\mathbb{E})$$

on $V = \mathbb{E}^n$. We assume that ρ is absolutely irreducible and that the characteristic polynomial of every $\rho(s)$ for every $s \in G$ lies in $\mathbb{H}[T]$. If $\mathrm{char}\,\mathbb{H} = 0$, it is enough to suppose that $\mathrm{Tr}\,\rho(s) \in \mathbb{H}$ for each $s \in G$. We want to study when the representation ρ is realizable over $\mathbb{H}$. More precisely, we ask whether there exists an $\mathbb{H}[G]$-module W such that $W \otimes_{\mathbb{H}} \mathbb{E} \simeq V$ as $\mathbb{E}[G]$-modules. This is equivalent to having $\rho(G) \subseteq \mathrm{GL}_n(\mathbb{H})$ up to conjugation. The cohomological approach we will take goes back to [**Sch04**] (see also [**Nek12**, Appendix B]).

For $g \in \Delta$, consider the representation ${}^gV$ whose underlying vector space is V, and the action of $s \in G$ is given by conjugating every entry of $\rho(s)$ by g. Denote by ${}^g\rho$ the corresponding group homomorphism $G \to \mathrm{GL}_n(\mathbb{E})$. Since V and ${}^gV$ are irreducible and $\mathrm{Tr}(\rho) = \mathrm{Tr}({}^g\rho) \in \mathbb{H}$, these two representations are isomorphic (cf. [**Bou22**, §21.1, Proposition 1]) and there exist homomorphisms $\{A_g \in \mathrm{Hom}_{\mathbb{E}}({}^gV, V)\}_{g\in\Delta}$ (unique up to scalars in $\mathbb{E}$) such that the diagram commutes for every $g \in \Delta$:

$$\begin{array}{ccc} {}^gV & \xrightarrow{A_g} & V \\ {\scriptstyle {}^g\rho}\downarrow & & \downarrow{\scriptstyle \rho} \\ {}^gV & \xrightarrow[A_g]{} & V. \end{array}$$

We identify each A_g with a matrix in $\mathrm{GL}_n(\mathbb{E})$ such that $\rho(s) = A_g\,{}^g\rho(s)A_g^{-1}$ for every $s \in G$.

Lemma 5.3.1. *The map $\Delta \to \mathrm{PGL}_n(\mathbb{E})$, $g \mapsto A_g \pmod{\mathbb{E}^\times}$ is a 1-cocycle.*

Proof. From the equality

$$A_{gh}\,{}^{gh}\rho(s)A_{gh}^{-1} = \rho(s) = (A_g\,{}^gA_h)\,{}^{gh}\rho(s)(A_g\,{}^gA_h\,{}^{gh})^{-1}$$

and the fact that ρ is irreducible, we deduce that there must exist some $e \in \mathbb{E}^\times$ such that $A_{gh} = eA_g\,{}^gA_h$. Hence $g \mapsto A_g \pmod{\mathbb{E}^\times}$ is a 1-cocycle. □

Recall the exact sequence of Δ-modules

$$1 \to \mathbb{E}^\times \to \mathrm{GL}_n(\mathbb{E}) \to \mathrm{PGL}_n(\mathbb{E}) \to 1.$$

From Section 1.2, there is a connecting homomorphism δ of pointed sets and an exact sequence of pointed sets

$$H^1(\Delta, \mathrm{GL}_n(\mathbb{E})) \to H^1(\Delta, \mathrm{PGL}_n(\mathbb{E})) \xrightarrow{\delta} H^2(\Delta, \mathbb{E}^\times).$$

We recall that δ is injective, since $H^1(\Delta, \mathrm{GL}_n(\mathbb{E}))$ vanishes. We let $c_V(g,h)$ be the image through δ of the cocycle $g \mapsto A_g \pmod{\mathbb{E}^\times}$. This 2-cocycle is given explicitly as

$$c_V(g,h) = A_g \cdot {}^gA_h \cdot A_{gh}^{-1}.$$

In particular, $c_V(g,h) \in \mathbb{E}^\times$ for all $g, h \in \Delta$.

Lemma 5.3.2. *Consider the algebra*

$$\mathcal{A} = \{X \in \mathrm{M}_n(\mathbb{E}) \mid X = A_g \cdot {}^g X \cdot A_g^{-1} \text{ for all } g \in \Delta\},$$

attached to the 1-cocycle $g \mapsto A_g \pmod{\mathbb{E}^\times}$ *(cf. Section 1.2). The group homomorphism* $\rho : G \to \mathrm{GL}_n(\mathbb{E})$ *has image contained in* $\mathcal{A}^\times$.

Proof. This is obvious from the definition of the matrices A_g. □

Proposition 5.3.3. *The representation* ρ *is realizable over* $\mathbb{H}$ *if and only if the 1-cocyle* $A_g \pmod{\mathbb{E}^\times}$ *is trivial (equivalently, if the 2-cocyle* c_V *is trivial).*

Proof. If ρ is realizable over $\mathbb{H}$, then we can take the matrix A_g to be the identity for each $g \in \Delta$, and the cocycle is trivial. Conversely, suppose that $A_g \pmod{\mathbb{E}^\times}$ is the trivial cocycle. Then by Lemmas 5.3.2 and 1.2.3 the image of ρ is conjugate to a subgroup of $\mathrm{GL}_n(\mathbb{H})$, and so it acts on the $\mathbb{H}$-vector space $W = \mathbb{H}^n$. It is immediate that $W \otimes_{\mathbb{H}} \mathbb{E} \simeq V$ as $\mathbb{E}[G]$-modules. □

Recall that from the 2-cocycle c_V we can define the crossed product algebra $\mathbb{E}^{c_V}[\Delta] = \bigoplus_{g\in\Delta}[g]\cdot\mathbb{E}$. The product operation in $\mathbb{E}^{c_V}[\Delta]$ is defined by the relations

$$[g]\cdot[h] = c_V(g,h)[gh] \text{ and } [g]\cdot a = {}^g a \cdot [g],$$

for all $g, h \in \Delta$ and $a \in \mathbb{E}$.

For the coming proof, we will need the property that extension of scalars is left adjoint to the restriction of scalars. More concretely, let R and S be commutative rings, $f : R \to S$ a ring homomorphism, M an R-module and N an S-module. Then there is an isomorphism of groups

$$\mathrm{Hom}_S(M \otimes_R S, N) \simeq \mathrm{Hom}_R(M, \mathrm{Res}_{S/R} N)$$

which sends $\phi \in \mathrm{Hom}_S(M \otimes_R S, N)$ to the R-homomorphism $m \mapsto \phi(m \otimes f(1))$. For more details, we refer the reader to [**Bou98**, Chapter II, §5].

Lemma 5.3.4. *There is an* $\mathbb{H}$*-algebra isomorphism* $\mathrm{End}_{\mathbb{H}[G]}(\mathrm{Res}_{\mathbb{E}/\mathbb{H}} V) \simeq \mathbb{E}^{c_V}[\Delta]$. *In particular, if* $n = [\mathbb{E} : \mathbb{H}]$ *then* $\mathrm{End}_{\mathbb{H}[G]}(\mathrm{Res}_{\mathbb{E}/\mathbb{H}} V) \simeq \mathcal{A}^{op}$.

Proof. We have a chain of isomorphisms

$$\begin{aligned}\mathrm{End}_{\mathbb{H}[G]}(\mathrm{Res}_{\mathbb{E}/\mathbb{H}} V) &= \mathrm{Hom}_{\mathbb{H}[G]}(\mathrm{Res}_{\mathbb{E}/\mathbb{H}} V, \mathrm{Res}_{\mathbb{E}/\mathbb{H}} V)\\ &\simeq \mathrm{Hom}_{\mathbb{E}[G]}(\mathrm{Res}_{\mathbb{E}/\mathbb{H}} V \otimes_{\mathbb{H}} \mathbb{E}, V)\\ &\simeq \bigoplus_{g\in\Delta} \mathrm{Hom}_{\mathbb{E}[G]}({}^g V, V).\end{aligned}$$

Since V is irreducible as an $\mathbb{E}[G]$-module, the $\mathbb{E}$-vector space $\mathrm{Hom}_{\mathbb{E}[G]}({}^g V, V)$ is generated by a single map, say λ_g, which sends ${}^g v \mapsto A_g {}^g v$ for each $v \in V$. Hence $\mathrm{End}_{\mathbb{H}[G]}(\mathrm{Res}_{\mathbb{E}/\mathbb{H}} V)$ is isomorphic to $\mathbb{E}^{c_V}[\Delta]$ as an $\mathbb{E}$-vector space, and we need to check the relations for the crossed-product algebra.

For $g \in \Delta$ we have

$$\begin{aligned}\lambda_g : \mathrm{Res}\, V &\to \mathrm{Res}\, V\\ v \mapsto \lambda_g(v \otimes 1) &= \lambda_g({}^t v)_{t\in\Delta}) = A_g \cdot {}^g v.\end{aligned}$$

Hence, given $g, h \in \Delta$ and $v \in V$ we obtain

$$\lambda_g \circ \lambda_h(v) = \lambda_g(A_h \cdot {}^h v) = A_g \cdot {}^g A_h \cdot {}^{gh} v = c_V(g,h) \cdot A_{gh} \cdot {}^{gh} v = c_V(g,h)\lambda_{gh}(v),$$

by the definition of the 2-cocycle c_V. On the other hand, given $a \in \mathbb{E}$ and $g \in \Delta$ we have

$$\lambda_g(av) = A_g \cdot {}^g(av) = {}^g a A_g {}^g v = {}^g a \cdot \lambda_g(v).$$

Therefore $\mathrm{End}_{\mathbb{H}[G]}(\mathrm{Res}_{\mathbb{E}/\mathbb{H}} V) \simeq \mathbb{E}^{c_V}[\Delta]$ as $\mathbb{H}$-algebras. The second assertion is a consequence of Proposition 1.2.4. □

5.4. λ-adic representations

In this section, we let k be a number field and A be a simple abelian variety defined over k. Let S_A be the set of primes of bad reduction for A. Let H and t_A be the center and Schur index of $\mathrm{End}^0(A)$, respectively. By Proposition 5.1.3, A is of GL_n-type for $n = 2\dim A/t_A[H:\mathbb{Q}]$. In the previous chapter we have proved the following result for $t_A = 1$ or a prime.

Theorem 4.2.7. *The abelian variety A has an associated strictly compatible system $\{\rho_{A,\lambda}\}_\lambda$ of H-rational λ-adic representations with values in $\mathbf{GL}_{n/t_A}(D^{op})$, where $D = \mathrm{End}^0(A)$. For every $\lambda \notin \mathrm{Ram}(D)$, ρ_λ takes values in $\mathrm{GL}_n(H_\lambda)$ and is absolutely irreducible. The exceptional set of the compatible system is S_A.*

Our goal is to prove this result for arbitrary t_A. We let E be a maximal subfield of $\mathrm{End}^0(A)$. We ask that E/H is a Galois extension; such an E always exists by the theorem of Albert–Brauer–Hasse–Noether (cf. Theorem 1.1.5). It might be possible to remove this hypothesis, but we impose it since it makes our arguments easier.

Let ℓ be a rational prime. As in Section 4.2, we denote by $V_\ell(A)$ the ℓ-adic Tate module of A. The field E acts on $V_\ell(A)$, making it a free $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-module of rank n. We have the direct product decomposition $E \otimes \mathbb{Q}_\ell \simeq \prod_{\mathfrak{L}|\ell} E_{\mathfrak{L}}$, where $\mathfrak{L}$ ranges over the primes of E dividing ℓ, and for each $\mathfrak{L}$ we define the $\mathfrak{L}$-adic Tate module as

$$V_{\mathfrak{L}}(A) := V_\ell(A) \otimes_{E \otimes \mathbb{Q}_\ell} E_{\mathfrak{L}}.$$

Let $\rho_{A,\mathfrak{L}} : G_k \to \mathrm{Aut}_{E_{\mathfrak{L}}}(V_{\mathfrak{L}}(A)) \simeq \mathrm{GL}_n(E_{\mathfrak{L}})$ be the corresponding Galois representation. Theorem 2.1.2 in [**Rib76**] asserts that $\{\rho_{A,\mathfrak{L}}\}_{\mathfrak{L}}$ forms a strictly compatible system of E-rational representations of G_k. There is an isomorphism of $\mathbb{Q}_\ell[G_k]$-modules

$$V_\ell(A) \simeq \bigoplus_{\mathfrak{L}|\ell} \mathrm{Res}_{E_{\mathfrak{L}}/\mathbb{Q}_\ell}(V_{\mathfrak{L}}(A)). \tag{5.1}$$

Lemma 5.4.1. *We have $\mathrm{End}_{E_{\mathfrak{L}}[G_k]}(V_{\mathfrak{L}}(A)) = E_{\mathfrak{L}}$. If in addition A is genuinely of GL_n-type, then for every finite extension L/k we have $\mathrm{End}_{E_{\mathfrak{L}}[G_L]}(V_{\mathfrak{L}}(A)) = E_{\mathfrak{L}}$. In particular, $V_{\mathfrak{L}}(A)$ is an absolutely irreducible $E_{\mathfrak{L}}[G_k]$-module.*

Proof. This is a consequence of Theorem 4.2.2, which gives us the isomorphism $\mathrm{End}^0(A_L) \otimes \mathbb{Q}_\ell \simeq \mathrm{End}_{G_L}(V_\ell(A))$. Since we are assuming that A is genuinely of GL_n-type, the field E is maximal in $\mathrm{End}^0(A_L)$, and hence

$$\mathrm{End}_{E \otimes \mathbb{Q}_\ell[G_L]}(V_\ell(A)) = E \otimes \mathbb{Q}_\ell \simeq \bigoplus_{\mathfrak{L}|\ell} E_{\mathfrak{L}}.$$

On the other hand, $\mathrm{End}_{E_{\mathfrak{L}'}[G_L]}(V_{\mathfrak{L}}(A))$ contains $E_{\mathfrak{L}'}$ for every $\mathfrak{L}' \mid \ell$. This implies $\mathrm{End}_{E_{\mathfrak{L}'}[G_L]}(V_{\mathfrak{L}'}(A)) = E_{\mathfrak{L}'}$. □

Fix a prime $\lambda \mid \ell$ of H and a prime $\mathfrak{L}$ of E over λ. We now want to show that the representation $\rho_{A,\mathfrak{L}}$ has traces in H_λ. To do so we use the $H_\lambda[G_k]$-module $V_\lambda(A)$ from Section 4.2, defined as $V_\lambda(A) = V_\ell(A) \otimes_{H\otimes\mathbb{Q}_\ell} H_\lambda$. This satisfies the isomorphism of $H_\lambda[G_k]$-modules

$$V_\lambda(A) \simeq \bigoplus_{\mathfrak{L}'|\lambda} \mathrm{Res}_{E_{\mathfrak{L}'}/H_\lambda} V_{\mathfrak{L}'}(A). \tag{5.2}$$

For every other $\mathfrak{L}' \mid \lambda$, fix an isomorphism $E_{\mathfrak{L}} \simeq E_{\mathfrak{L}'}$, this allows us to see $V_{\mathfrak{L}'}(A)$ as an $E_{\mathfrak{L}}$-vector space (this is where we use the hypothesis that E/H is Galois).

Proposition 5.4.2. *For every prime $\mathfrak{L}'$ of E and every $v \notin S_A$ not dividing ℓ, $\mathrm{Tr}(\mathrm{Frob}_v \mid V_{\mathfrak{L}}(A)) \in H$. Moreover, we have an isomorphism of $E_{\mathfrak{L}}[G_k]$-modules ${}^gV_{\mathfrak{L}'}(A) \simeq V_{\mathfrak{L}''}(A)$ for all $g \in \mathrm{Gal}(E_{\mathfrak{L}}/H_\lambda)$ and all $\mathfrak{L}'$ and $\mathfrak{L}''$ dividing the same prime λ of H.*

Proof. By Theorem 4.2.2, we have the isomorphism $\mathrm{End}^0(A)\otimes_H H_\lambda \simeq \mathrm{End}_{H_\lambda[G_k]}(V_\lambda(A))$, this is a central division H_λ-algebra of H_λ-dimension $t_A^2 = [E : H]^2$. From (5.2) we have

$$\begin{aligned}
\mathrm{End}_{H_\lambda[G_k]}(V_\lambda(A)) &\simeq \mathrm{End}_{H_\lambda[G_k]}\Big(\bigoplus_{\mathfrak{L}'|\ell} \mathrm{Res}_{E_{\mathfrak{L}}/H_\lambda} V_{\mathfrak{L}'}(A)\Big) \\
&\simeq \bigoplus_{\mathfrak{L}',\mathfrak{L}''|\lambda} \mathrm{Hom}_{H_\lambda[G_k]}(\mathrm{Res}_{E_{\mathfrak{L}}/H_\lambda} V_{\mathfrak{L}'}(A), \mathrm{Res}_{E_{\mathfrak{L}}/H_\lambda} V_{\mathfrak{L}''}(A)) \\
&\simeq \bigoplus_{\mathfrak{L}',\mathfrak{L}''|\lambda} \mathrm{Hom}_{E_{\mathfrak{L}}[G_k]}(\mathrm{Res}_{E_{\mathfrak{L}}/H_\lambda} V_{\mathfrak{L}'}(A) \otimes_{H_\lambda} E_{\mathfrak{L}}, V_{\mathfrak{L}''}(A)) \\
&\simeq \bigoplus_{\mathfrak{L}',\mathfrak{L}''|\lambda} \bigoplus_{g\in\mathrm{Gal}(E_{\mathfrak{L}}/H_\lambda)} \mathrm{Hom}_{E_{\mathfrak{L}}[G_k]}({}^gV_{\mathfrak{L}'}(A), V_{\mathfrak{L}''}(A)).
\end{aligned}$$

Now by Lemma 5.4.1 each $E_{\mathfrak{L}}[G_k]$-module is absolutely irreducible, and hence $\dim_{E_{\mathfrak{L}}} \mathrm{Hom}_{E_{\mathfrak{L}}[G_k]}({}^gV_{\mathfrak{L}'}(A), V_{\mathfrak{L}''}(A)) \leq 1$ with equality if and only if ${}^gV_{\mathfrak{L}'}(A) \simeq V_{\mathfrak{L}''}(A)$ as $E_{\mathfrak{L}}[G_k]$-modules. Hence the H_λ-dimension of $\mathrm{End}_{H_\lambda[G_k]}(V_\lambda(A))$ is at most $\left(\frac{[E:H]}{[E_{\mathfrak{L}}:H_\lambda]}\right)^2 [E_{\mathfrak{L}} : H_\lambda]^2 = [E : H]^2$, with equality if and only if ${}^gV_{\mathfrak{L}'}(A) \simeq V_{\mathfrak{L}''}(A)$ for every $g \in \mathrm{Gal}(E_{\mathfrak{L}}/H_\lambda)$ and all $\mathfrak{L}', \mathfrak{L}'' \mid \lambda$. This is indeed the case, since this dimension coincides with that of $\mathrm{End}^0(A) \otimes_H H_\lambda$.

In particular, we have found that ${}^gV_{\mathfrak{L}}(A) \simeq V_{\mathfrak{L}}(A)$ for all $g \in \mathrm{Gal}(E_{\mathfrak{L}}/H_\lambda)$. Therefore $\mathrm{Tr}(\mathrm{Frob}_v \mid V_{\mathfrak{L}}(A)) \in H_\lambda$ for every prime λ of H. Since this trace also belongs to E, we conclude that $\mathrm{Tr}(\mathrm{Frob}_v \mid V_{\mathfrak{L}}(A)) \in H$. □

Recall from Section 4.2 that, when $\lambda \notin \mathrm{Ram}(\mathrm{End}^0(A))$, the $H_\lambda[G_k]$-module $V_\lambda(A)$ has an absolutely irreducible submodule $W_\lambda(A)$, such that $V_\lambda(A) \simeq W_\lambda(A)^{\oplus t_A}$.

Proposition 5.4.3. *The $E_{\mathfrak{L}}[G_k]$-module $V_{\mathfrak{L}}(A)$ is realizable over H_λ if and only if $\lambda \notin \mathrm{Ram}(\mathrm{End}^0(A))$. More precisely,*

1. *If $\lambda \notin \mathrm{Ram}(\mathrm{End}^0(A))$, then*
$$V_{\mathfrak{L}}(A) \simeq W_\lambda(A) \otimes_{H_\lambda} E_{\mathfrak{L}}$$
as $E_{\mathfrak{L}}[G_L]$-modules.
2. *If there exists an $H_\lambda[G_k]$-module W such that $V_{\mathfrak{L}}(A) \simeq W \otimes_{H_\lambda} E_{\mathfrak{L}}$ as $E_{\mathfrak{L}}[G_k]$-modules, then $\lambda \notin \mathrm{Ram}(\mathrm{End}^0(A))$.*

PROOF. For the first statement, we have that for every $v \notin S_A$ and not dividing λ,

$$\begin{aligned} t_A \operatorname{Tr}_{H_\lambda}(\mathrm{Frob}_v \mid W_\lambda(A)) &= \operatorname{Tr}_{H_\lambda}(\mathrm{Frob}_v \mid V_\lambda(A)) \\ &= \sum_{\mathfrak{L}'\mid\lambda} \operatorname{Tr}_{H_\lambda}(\mathrm{Frob}_v \mid \operatorname{Res}_{E_\mathfrak{L}/H_\lambda} V_{\mathfrak{L}'}(A)) \quad (5.2) \\ &= \sum_{\mathfrak{L}'\mid\lambda} [E_\mathfrak{L} : H_\lambda] \operatorname{Tr}_{E_\mathfrak{L}}(\mathrm{Frob}_v \mid V_\mathfrak{L}(A)) \quad \text{(Proposition 5.4.2)} \\ &= [E : H] \operatorname{Tr}_{E_\mathfrak{L}}(\mathrm{Frob}_v \mid V_\mathfrak{L}(A)) \\ &= t_A \operatorname{Tr}_{E_\mathfrak{L}}(\mathrm{Frob}_v \mid V_\mathfrak{L}(A)) \quad (E \text{ is maximal}). \end{aligned}$$

Hence the traces of Frobenius coincide for $W_\lambda(A)$ and $V_\mathfrak{L}(A)$, and we obtain the stated isomorphism from the Chebotaryov density theorem.

For the second part, suppose that there is an $H_\lambda[G_k]$-module W such that $V_\Lambda(A) \simeq W \otimes_{H_\lambda} E_\mathfrak{L}$. Then by (5.2) and Proposition 5.4.2 we obtain

$$V_\lambda(A) \simeq W^{\oplus t_A}.$$

Then from Proposition 4.2.3 we have

$$\mathrm{End}^0(A) \otimes_H H_\lambda \simeq \mathrm{End}_{H_\lambda[G_k]}(V_\lambda(A)) \simeq \mathrm{End}_{H_\lambda[G_k]}(W^{\oplus t_A}) \simeq \mathrm{M}_{t_A}(H_\lambda),$$

which implies $\lambda \notin \mathrm{Ram}(\mathrm{End}^0(A))$. □

We have determined the primes $\mathfrak{L}$ of E such that $V_\mathfrak{L}(A)$ can be descended to H. We will now finish the proof of Theorem 4.2.7.

PROOF OF THEOREM 4.2.7. Given a prime λ of H, pick a prime $\mathfrak{L} \mid \lambda$ of E. Since $[E_\mathfrak{L} : H_\lambda] \mid t_A \mid n$, we can fix a Galois extension $\mathbb{E}/H_\lambda$ of degree n containing $E_\mathfrak{L}$. Let

$$\rho_\lambda : G_k \to \mathrm{GL}_n(\mathbb{E})$$

be the representation given by the action of G_k on $V := V_\mathfrak{L}(A) \otimes_{E_\mathfrak{L}} \mathbb{E}$. We will show that the homomorphism ρ_λ takes values in $\mathrm{GL}_{n/t_A}((D \otimes_H H_\lambda)^{op})$.

We know by Lemmas 5.3.2 and 5.3.4 that the image of ρ_λ lands in the units of $\mathrm{End}_{H_\lambda[G_k]}(\mathrm{Res}_{\mathbb{E}/H_\lambda} V)^{op}$. Let s be the number of primes of E over λ, we observe that $[\mathbb{E} : E_\mathfrak{L}] = \frac{n}{[E_\mathfrak{L}:H_\lambda]} = \frac{ns}{[E:H]} = \frac{ns}{t_A}$. By Proposition 5.4.2 and Faltings' isomorphism we obtain

$$\begin{aligned} D \otimes_H H_\lambda \simeq \mathrm{End}_{H_\lambda[G_k]}(V_\lambda(A)) &\simeq \mathrm{End}_{H_\lambda[G_k]}(\bigoplus_{\mathfrak{L}'\mid\lambda} \mathrm{Res}_{E_\mathfrak{L}/H_\lambda} V_{\mathfrak{L}'}(A)) \\ &\simeq \mathrm{End}_{H_\lambda[G_k]}(V_\mathfrak{L}(A)^{\oplus s}) \\ &\simeq \mathrm{M}_s(\mathrm{End}_{H_\lambda[G_k]}(\mathrm{Res}_{E_\mathfrak{L}/H_\lambda} V_\mathfrak{L}(A))). \end{aligned}$$

From the isomorphism $\mathrm{Res}_{\mathbb{E}/E_\mathfrak{L}} V \simeq V_\mathfrak{L}(A)^{\oplus[\mathbb{E}:E_\mathfrak{L}]}$, we have

$$\begin{aligned} \mathrm{End}_{H_\lambda[G_k]}(\mathrm{Res}_{\mathbb{E}/H_\lambda} V)^{op} &\simeq \mathrm{M}_{[\mathbb{E}:E_\mathfrak{L}]}(\mathrm{End}_{H_\lambda[G_k]}(\mathrm{Res}_{E_\mathfrak{L}/H_\lambda} V_\mathfrak{L}(A)))^{op} \\ &= \mathrm{M}_{ns/t_A}(\mathrm{End}_{H_\lambda[G_k]}(\mathrm{Res}_{E_\mathfrak{L}/H_\lambda} V_\mathfrak{L}(A)))^{op} \\ &\simeq \mathrm{M}_{n/t_A}(D \otimes_H H_\lambda)^{op}. \end{aligned}$$

Thus we obtain the result. □

5.5. Inner twists and the Nebentype

In this section we let A be an abelian variety defined over k genuinely of GL_n-type, and let B be its associated building block. There exists a minimal extension K/k over which A has all its endomorphisms defined. We let H and F be the centers of $\mathrm{End}^0(A)$ and $\mathrm{End}^0(B)$, respectively. For each $s \in \mathrm{Gal}(K/k)$, there is an F-algebra homomorphism

$$\begin{aligned} \Psi_s : \mathrm{End}^0(A_K) &\to \mathrm{End}^0(A_K) \\ \varphi &\mapsto {}^s\varphi \end{aligned}$$

As in the proof of Proposition 5.2.3, there exists some $\alpha(s) \in \mathrm{End}^0(A_K)^\times$ such that ${}^s\varphi = \alpha(s)\varphi\alpha(s)^{-1}$. We fix a choice of $\alpha(s)$ for every $s \in \mathrm{Gal}(K/k)$.

We first observe that the $\alpha(s)$ generate H over F.

Lemma 5.5.1. *We have $F(\{\alpha(s)\}_{s\in\mathrm{Gal}(K/k)}) = H$.*

Proof. Let $D = \mathrm{End}^0(A)$, $X = \mathrm{End}^0(A_K)$ and $H' = F(\{\alpha(s)\}_{s\in\mathrm{Gal}(K/k)})$. For every $\varphi \in X$ we have $\varphi = {}^s\varphi$ if and only if $\varphi \in D$, and ${}^s\varphi = \alpha(s)\varphi\alpha(s)^{-1}$. Hence ${}^s\alpha(s) = \alpha(s)$ for every s, and $H' \subseteq H$. Moreover, we find $D = C_X(H')$, the centralizer of H' in X. On the other hand, we have $H \subseteq C_X(D)$, so $H \subseteq C_X(C_X(H'))$. We now apply the Double Centralizer theorem (cf. Theorem 1.1.4), which yields $H \subseteq C_X(C_X(H')) = H'$. □

We now define certain maps (which will be seen to be characters) that will be used later to study the Tate modules of A.

Definition 5.5.2. *For every $\gamma \in \mathrm{Aut}(H/F)$, we define the* inner twist associated to γ *as the map*

$$\begin{aligned} \chi_\gamma : \mathrm{Gal}(K/k) &\to H^\times \\ s &\mapsto {}^\gamma\alpha(s)/\alpha(s). \end{aligned}$$

Lemma 5.5.3. *For all $\gamma, \delta \in \mathrm{Aut}(H/F)$ we have the cocycle identity $\chi_{\gamma\delta} = \chi_\gamma \cdot {}^\gamma\chi_\delta$. Each map χ_γ is a character.*

Proof. The first assertion is a simple check. For the second, we define

$$\xi(s,t) = \alpha(s)\alpha(t)\alpha(st)^{-1}.$$

By the definition of $\alpha : \mathrm{Gal}(K/k) \to H^\times$ we see that $\xi(s,t)$ commutes with all $\mathrm{End}^0(A_K)$ and so $\xi(s,t) \in F^\times$. Hence we also have

$$\xi(s,t) = {}^\gamma\alpha(s)\,{}^\gamma\alpha(t)\,{}^\gamma\alpha(st)^{-1}.$$

Dividing both equalities it follows that $\chi_\gamma(st) = \chi_\gamma(s)\chi_\gamma(t)$. □

Suppose from now on that A is geometrically of the first kind, so that F is totally real. The field H is either totally real or a CM field. We can thus consider the complex conjugation $\gamma = c \in \mathrm{Aut}(H/F)$, and we say $\varepsilon := \chi_c^{-1}$ is the *Nebentype* of A. Note that ε is nontrivial if and only if H is a CM field. We will often consider each inner twist χ_γ as a (finite order) character of G_k.

Remark 5.5.4. *Since A is geometrically of the first kind, we have that n is even. A treatment of inner and outer twists for odd n can be found in* [**Sha25**].

For the next result, we fix a polarization of A, and denote by $'$ the Rosati involution on $\mathrm{End}^0(A)$. Recall that this involution restricts to c on the center H of $\mathrm{End}^0(A)$.

Proposition 5.5.5. *If A is geometrically of the first kind, then the extension H/F is abelian.*

Proof. Since it makes notation clearer, we will use $\bar{\cdot}$ to denote complex conjugation. Note first that we can write

$$\alpha(s)^2 = \alpha(s) \cdot \overline{\alpha(s)} \cdot \varepsilon(s) \tag{5.3}$$

for every $s \in \mathrm{Gal}(K/k)$. Let us show that $\alpha(s) \cdot \overline{\alpha(s)} \in F$ by checking that it commutes with every element $\varphi \in \mathrm{End}^0(A_K)$. Indeed, we have

$${}^s\varphi = \alpha(s)\varphi\alpha(s)^{-1}, \quad ({}^s\varphi)' = \overline{\alpha(s)^{-1}}\varphi'\overline{\alpha(s)}.$$

Now we note that ${}^s\varphi' = ({}^s\varphi)'$, since the polarization of A is defined over k. Hence we obtain $\alpha(s)^{-1}\overline{\alpha(s)^{-1}}\varphi'\overline{\alpha(s)}\alpha(s) = \varphi'$ for all $\varphi \in \mathrm{End}^0(A_K)$, and so $\alpha(s)\overline{\alpha(s)} \in F$ for all s.

We finish observing that, by (5.3), H is contained in the extension of F generated by the square roots of $\alpha(s)\overline{\alpha(s)}$ and by ζ_{2m}, where m is the order of ε. □

Let $D = \mathrm{End}^0(A)$. In the remaining of the section we will show how the inner twists just defined interact with the system of representations $\rho_{A,\lambda} : G_k \to \mathrm{GL}_{n/t_A}(D_\lambda^{op})$ from Theorem 4.2.7, under the assumption that A is geometrically of the first kind. For a prime λ of H we let $V_\lambda(A) = V_\ell(A) \otimes_{H\otimes\mathbb{Q}_\ell} H_\lambda$ as usual, and for $\lambda \notin \mathrm{Ram}(D)$, we let $W_\lambda(A)$ be the absolutely irreducible $H_\lambda[G_k]$-module realising $\rho_{A,\lambda}$.

By Proposition 5.5.5 we have that H/F is a Galois extension. Given some $\lambda \mid \ell$, we fix an isomorphism $H_\lambda \simeq H_{\lambda'}$ for every other $\lambda' \mid \ell$. If $V_{\lambda'}(A)$ and $W_{\lambda'}(A)$ are the $H_{\lambda'}[G_k]$-modules associated to A, this isomorphism allows us to consider them as vector spaces over H_λ. For each prime $\mathfrak{l} \mid \ell$ of F, we let $V_\mathfrak{l}(A) := V_\ell(A) \otimes_{F\otimes\mathbb{Q}_\ell} F_\mathfrak{l}$. Similarly as in (5.2), we have an isomorphism

$$V_\mathfrak{l}(A) \simeq \bigoplus_{\lambda\mid\mathfrak{l}} \mathrm{Res}_{H_\lambda/F_\mathfrak{l}} V_\lambda(A)$$

of $F_\mathfrak{l}[G_k]$-modules. Let S_A be the primes of k of bad reduction for A, and $S_{A,K}$ the primes of K lying above the primes in S_A.

Proposition 5.5.6. *Let $\mathfrak{l}$ be some prime of F and a prime $\lambda \mid \mathfrak{l}$ of H. For all primes $\lambda', \lambda'' \mid \mathfrak{l}$ of H and every $g \in \mathrm{Gal}(H_\lambda/F_\mathfrak{l})$, we have an isomorphism*

$${}^gV_{\lambda'}(A) \simeq V_{\lambda''}(A)$$

of $H_\lambda[G_K]$-modules. In particular, for every prime $w \notin S_{A,K}$ the trace $\mathrm{Tr}(\mathrm{Frob}_w \mid V_\lambda(A))$ belongs to F. If in addition λ', λ'' are not in $\mathrm{Ram}(\mathrm{End}^0(A))$, then we have an isomorphism ${}^gW_{\lambda'}(A) \simeq W_{\lambda''}(A)$ of $H_\lambda[G_K]$-modules.

Proof. The proof is identical to that of Proposition 5.4.2, we provide it for completeness. By the isomorphism $V_\lambda(A) \simeq W_\lambda(A)^{\oplus t_A}$ (whenever $\lambda \notin \mathrm{Ram}(\mathrm{End}^0(A))$), it is enough to have the stated isomorphisms for the modules $V_\lambda(A)$. By applying Theorem 4.2.2 we have the isomorphism

$$\mathrm{End}^0(A_K) \otimes_F F_\mathfrak{l} \simeq \mathrm{End}_{F_\mathfrak{l}[G_K]}(V_\mathfrak{l}(A)). \tag{5.4}$$

Let E be a maximal subfield of $\mathrm{End}^0(A)$ with E/H Galois. The left-hand side of (5.4) is an algebra of $F_\mathfrak{l}$-dimension $[E:F]^2$, as E is maximal in $\mathrm{End}^0(A_K)$. We now let $G = \mathrm{Gal}(H_\lambda/F_\mathfrak{l})$ and rewrite the right-hand side as follows:

$$\begin{aligned}\mathrm{End}_{F_\mathfrak{l}[G_K]}(V_\mathfrak{l}(A)) &\simeq \bigoplus_{\lambda',\lambda''\mid\mathfrak{l}} \mathrm{Hom}_{F_\mathfrak{l}[G_K]}(\mathrm{Res}_{H_\lambda/F_\mathfrak{l}} V_{\lambda'}(A), \mathrm{Res}_{H_\lambda/F_\mathfrak{l}} V_{\lambda''}(A)) \\ &\simeq \bigoplus_{\lambda',\lambda''\mid\mathfrak{l}} \bigoplus_{g\in G} \mathrm{Hom}_{H_\lambda[G_K]}({}^gV_{\lambda'}(A), V_{\lambda''}(A)).\end{aligned}$$

Now $\dim_{F_\mathfrak{l}} \mathrm{Hom}_{H_\lambda[G_K]}({}^gV_{\lambda'}(A), V_{\lambda''}(A)) \le t_A^2[H_\lambda : F_\mathfrak{l}]$, and hence the $F_\mathfrak{l}$-dimension of $\mathrm{End}_{F_\mathfrak{l}[G_K]}(V_\mathfrak{l}(A))$ is at most $t_A^2[H:F]^2 = [E:F]^2$, with equality if and only if ${}^gV_{\lambda'}(A) \simeq V_{\lambda''}(A)$ for all $\lambda', \lambda'' \mid \mathfrak{l}$ and $g \in \mathrm{Gal}(H_\lambda/F_\mathfrak{l})$. This is indeed the case, and we have the desired isomorphisms.

In particular we now have ${}^g\,\mathrm{Tr}(\mathrm{Frob}_w \mid V_\lambda(A)) = \mathrm{Tr}(\mathrm{Frob}_w \mid V_\lambda(A))$ for every $w \notin S_{A,K}$ and $g \in \mathrm{Gal}(H_\lambda/F_\mathfrak{l})$, and so the trace of Frob_w belongs to $F_\mathfrak{l} \cap H$. As this holds for any prime $\mathfrak{l}$ of F, we obtain $\mathrm{Tr}(\mathrm{Frob}_w \mid V_\lambda(A)) \in F$. □

Remark 5.5.7. *The proof we have just given still holds if A is geometrically of the second kind, as long as the extension of CM fields H/F is Galois.*

Given $\lambda, \lambda' \notin \mathrm{Ram}(D)$, we now know that $W_\lambda(A)$ and $W_{\lambda'}(A)$ are isomorphic as $H_\lambda[G_K]$-modules. We wish to describe their relation as G_k-modules. We begin by observing the following fact.

Lemma 5.5.8. *Let A be geometrically of the first kind and $\lambda, \lambda' \notin \mathrm{Ram}(D)$. There exists at most one finite image character $\chi : G_k \to H_\lambda^\times$ such that $W_\lambda(A) \simeq \chi \otimes W_{\lambda'}(A)$. In particular, if χ satisfies $W_\lambda(A) \simeq \chi \otimes W_\lambda(A)$, then χ is trivial.*

Proof. Let $\chi, \xi : G_k \to H_\lambda^\times$ be two finite characters such that

$$W_\lambda(A) \simeq \chi \otimes W_{\lambda'}(A) \simeq \xi \otimes W_{\lambda'}(A).$$

Let L/k be a finite Galois extension such that G_L is contained in the kernel of χ and ξ. By irreducibility of $W_\lambda(A)$ and $W_{\lambda'}(A)$ as $H_\lambda[G_L]$-modules, we have that

$$\mathrm{Hom}_{G_L}(W_\lambda(A), W_{\lambda'}(A))$$

has H_λ-dimension 1. But this is a representation of $\mathrm{Gal}(L/k)$, and hence it must equal both χ and ξ, so $\chi = \xi$. □

We now show how the character in the previous lemma is precisely an inner twist. As in Section 5.3, for every $\gamma \in \mathrm{Gal}(H/F)$ we let ${}^\gamma W_\lambda(A)$ be the $H_\lambda[G_k]$-module $W_\lambda(A)$ with the action of G_k given by conjugating every entry in the image of $\rho_{A,\lambda}$ by γ.

Proposition 5.5.9. *Let A be geometrically of the first kind, let $\lambda \notin \mathrm{Ram}(D)$ be a prime of H, and let $\gamma \in \mathrm{Gal}(H/F)$. We have the isomorphism of $H_\lambda[G_k]$-modules*

$$W_\lambda(A) \simeq \chi_\gamma^{-1} \otimes {}^\gamma W_\lambda(A),$$

where $\chi_\gamma(s) = {}^\gamma\alpha(s)/\alpha(s)$ is the inner twist associated to γ. In particular, we have

$$W_\lambda(A) \simeq \varepsilon \otimes {}^c W_\lambda(A),$$

where c denotes complex conjugation and $\varepsilon = \chi_c^{-1}$ is the Nebentype of A.

PROOF. To show the statement is equivalent to showing it for $V_\lambda(A)$ and ${}^\gamma V_\lambda(A)$. By Proposition 5.5.6 we have $V_\lambda(A) \simeq {}^\gamma V_\lambda(A)$ as $H_\lambda[G_K]$-modules. Hence to show

$$V_\lambda(A) \simeq \chi_\gamma^{-1} \otimes {}^\gamma V_\lambda(A)$$

is equivalent to showing that $\mathrm{Gal}(K/k)$ acts via χ_γ^{-1} on

$$({}^\gamma V_\lambda(A)^\vee \otimes V_\lambda(A))^{G_K} \simeq \mathrm{Hom}_{H_\lambda[G_K]}({}^\gamma V_\lambda(A), V_\lambda(A)),$$

where $^\vee$ denotes the contragredient representation. Let $\mathfrak{l}$ be the prime of F below λ and $\gamma(\lambda)$. We have seen that

$$\mathrm{End}^0(A_K) \otimes_F F_\mathfrak{l} \simeq \bigoplus_{\lambda', \lambda'' \mid \mathfrak{l}} \bigoplus_{h \in \mathrm{Gal}(H_\lambda / F_\mathfrak{l})} \mathrm{Hom}_{H_\lambda[G_K]}({}^h V_{\lambda'}(A), V_{\lambda''}(A)),$$

and any $s \in \mathrm{Gal}(K/k)$ acts on $\mathrm{End}^0(A_K)$ by conjugation by $\alpha(s)$. In particular, if $\lambda' = \sigma(\lambda)$ and $\lambda'' = \tau(\lambda)$, then $\alpha(s)$ acts on $\mathrm{Hom}_{H_\lambda[G_K]}({}^h V_{\lambda'}(A), V_{\lambda''}(A))$ as ${}^\tau\alpha(s)/{}^{\sigma h}\alpha(s)$. Hence $\mathrm{Gal}(K/k)$ acts on $\mathrm{Hom}_{H_\lambda[G_K]}({}^\gamma V_\lambda(A), V_\lambda(A))$ as $\alpha(s)/{}^\gamma\alpha(s) = \chi_\gamma(s)^{-1}$, as expected. □

Remark 5.5.10. *Let $\mathfrak{l}$ be a prime of F splitting completely in H and let λ be a prime of H over $\mathfrak{l}$. For every $\gamma \in \mathrm{Gal}(H/F)$, γ acts on $W_\lambda(A)$ by conjugating the entries of $G_k \to \mathrm{Aut}(W_\lambda(A)) \simeq \mathrm{GL}_n(H_\lambda)$ by γ (cf. Section 5.3). If $\sigma_\lambda : H \otimes_\mathbb{Q} \mathbb{Q}_\ell \to H_\lambda$ and $\sigma_{\gamma(\lambda)} : H \otimes_\mathbb{Q} \mathbb{Q}_\ell \to H_{\gamma(\lambda)}$ denote the projections onto the respective factors, we have $\sigma_{\gamma(\lambda)} = \gamma \circ \sigma_\lambda$. Recall that $V_\lambda(A) = V_\ell(A) \otimes_{H \otimes \mathbb{Q}_\ell} H_\lambda \simeq W_\lambda(A)^{\oplus t_A}$, with the tensor product being taken with respect to σ_λ, and similarly for $\gamma(\lambda)$. Hence we obtain ${}^\gamma W_\lambda(A) \simeq W_{\gamma(\lambda)}(A)$ as $H_\lambda[G_k]$-modules (i.e. as $F_\mathfrak{l}[G_k]$-modules, since $H_\lambda \simeq F_\mathfrak{l}$). Therefore, the isomorphism in the proposition above becomes*

$$W_\lambda(A) \simeq \chi_\gamma^{-1} \otimes W_{\gamma(\lambda)}(A).$$

This corresponds to Lemmas 5.10 and 5.11 in [**Pyl04**].

In general, if $\mathfrak{l}$ is any prime of F, $\lambda \mid \mathfrak{l}$ and $\gamma \in \mathrm{Gal}(H/F)$, then ${}^\gamma W_\lambda(A) \simeq {}^g W_{\gamma(\lambda)}(A)$ for some $g \in \mathrm{Gal}(H_\lambda/F_\mathfrak{l})$. Note that this is an artifact of having to choose an isomorphism $H_\lambda \simeq H_{\gamma(\lambda)}$ to be able to compare the modules in the first place.

Corollary 5.5.11. *Suppose A is geometrically of the first kind. The subextension of K/k cut out by all the inner twists is K/k itself. In particular, $\mathrm{Gal}(K/k)$ is abelian.*

PROOF. Let $\mathfrak{l}$ be a prime of F that splits completely in H and such that every $\lambda \mid \mathfrak{l}$ is not in $\mathrm{Ram}(D)$. By the proof of Proposition 5.5.6, K/k is the smallest extension such that $W_\lambda(A) \simeq W_{\lambda'}(A)$ for all $\lambda, \lambda' \mid \mathfrak{l}$. By Proposition 5.5.9, K/k is the extension cut out by the inner twists. □

We have seen the relation between the $H_\lambda[G_k]$-modules $W_\lambda(A)$ and the inner twists of A. We now use the properties seen so far to endow $W_\lambda(A)$ with a pairing, which in particular will allow us to compute the determinant of the representation.

Proposition 5.5.12. *Suppose A is geometrically of the first kind. For each $\lambda \notin \mathrm{Ram}(D)$, there exists an H_λ-bilinear, G_k-equivariant, nondegenerate pairing*

$$\psi_\lambda : W_\lambda(A) \times W_\lambda(A) \to H_\lambda(\varepsilon\chi_\ell).$$

This pairing is unique up to multiplication by elements in $H_\lambda^\times$.

PROOF. We first note that we have isomorphisms

$$\begin{aligned}\mathrm{Hom}_{H_\lambda[G_k]}(W_\lambda(A)\otimes W_\lambda(A),\varepsilon\chi_\ell) &\simeq ((W_\lambda(A)\otimes W_\lambda(A))^\vee\otimes\varepsilon\chi_\ell)^{G_k}\\ &\simeq (W_\lambda(A)^\vee\otimes(W_\lambda(A)^\vee\otimes\varepsilon\chi_\ell))^{G_k}\\ &\simeq \mathrm{Hom}_{H_\lambda[G_k]}(W_\lambda(A),W_\lambda(A)^\vee\otimes\varepsilon\chi_\ell),\end{aligned}$$

where all tensor products are with respect to H_λ to account for H_λ-linearity. Hence, the existence of a pairing is equivalent to having an isomorphism $W_\lambda(A)\simeq W_\lambda(A)^\vee\otimes\varepsilon\chi_\ell$ of $H_\lambda[G_k]$-modules. Its uniqueness will be a consequence of the irreducibility of $W_\lambda(A)$. By Proposition 5.5.9, we have the isomorphism

$$W_\lambda(A)\simeq {}^cW_\lambda(A)\otimes\varepsilon.$$

Let $v\notin S_A$ and let α be an eigenvalue of Frob_v acting on $W_\lambda(A)$. By the Weil conjectures, we have $\bar{\alpha}=\mathrm{Nm}(v)/\alpha$. It follows from this fact and the Chebotaryov density theorem that

$${}^cW_\lambda(A)\simeq W_\lambda(A)^\vee\otimes\chi_\ell.$$

Combining the displayed isomorphisms we obtain $W_\lambda(A)\simeq W_\lambda(A)^\vee\otimes\varepsilon\chi_\ell$, as desired. □

Remark 5.5.13. *If A is of the first kind over k, then the module $W_\lambda(A)$ already has a nondegenerate G_k-equivariant pairing $\tilde{\psi}_\lambda$ by Theorems 4.3.3, 4.3.7 and 4.3.11. Hence the pairing just constructed must agree with $\tilde{\psi}_\lambda$ up to scalars.*

Corollary 5.5.14. *Suppose A is genuinely of GL_n-type and geometrically of the first kind. For every prime $\lambda\notin\mathrm{Ram}(D)$, the determinant of the representation $W_\lambda(A)$ equals $\varepsilon^{n/2}\chi_\ell^{n/2}$.*

PROOF. The previous proposition gives an isomorphism $W_\lambda(A)\simeq W_\lambda(A)^\vee\otimes\varepsilon\chi_\ell$. Hence, if $s\in G_k$ then the eigenvalues of s acting on $W_\lambda(A)$ come in pairs α,α' such that $\alpha\alpha'=\varepsilon(s)\chi_\ell(s)$. The product of all the eigenvalues of s is thus equal to $\varepsilon(s)^{n/2}\chi_\ell(s)^{n/2}$. □

5.6. A converse theorem

Let A be an abelian variety defined over k genuinely of GL_n-type and let B be its building block. We have seen in Proposition 5.5.12 that the Tate modules of A have a non-degenerate, bilinear, Galois-equivariant pairing if A is geometrically of the first kind. In this section we prove the converse statement: if some Tate modules of A have such a pairing, then A is geometrically of the first kind.

The main idea in our statement takes inspiration from [**Rib04**, Theorem 5.3], where Ribet treats the case of an abelian variety $A/\mathbb{Q}$ which is genuinely of GL_2-type. We shall see along our reasoning that Ribet was using the determinant pairing (cf. [**Rib04**, Lemma 3.1]) to show A is geometrically of the first kind.

Let H be the center of $D=\mathrm{End}^0(A)$, F the center of $\mathrm{End}^0(B)$, and E a maximal subfield of $\mathrm{End}^0(A)$. Let S_A be the set of primes of k of bad reduction for A.

We begin by characterizing the center of the endomorphism algebra of A as we take an extension of k.

Proposition 5.6.1. *Let L/k be a finite extension and let $S_{A,L}$ be the set of primes of L above S_A. The following fields coincide:*

(1) *The center* M_1 *of* $\mathrm{End}^0(A_L)$.
(2) *The field* M_2 *generated over* $\mathbb{Q}$ *by the traces* $\mathrm{Tr}(\mathrm{Frob}_v \mid W_\lambda(A))$*, where* λ *is a fixed prime of* H *and* v *varies over the primes of* L *not in* $S_{A,L}$ *and coprime with* λ.

If in addition we fix a rational prime ℓ *that splits completely in* H*, then* M_1 *and* M_2 *are also equal to:*

(3) *The smallest subfield* M_3 *of* H *satisfying the following property: two primes* λ, λ' *of* H *lie over the same prime* $\mathfrak{l} \mid \ell$ *of* M_3 *if and only if* $W_\lambda(A) \simeq W_{\lambda'}(A)$ *as* $\mathbb{Q}_\ell[G_L]$*-modules.*

Proof. Since the center M_1 of $\mathrm{End}^0(A_L)$ does not vary with ℓ, and the $W_\lambda(A)$ form a compatible system, it is enough to prove the equality of all three fields assuming that ℓ splits completely in H. Note then that $H_\lambda = \mathbb{Q}_\ell$ for every $\lambda \mid \ell$. By letting ℓ be a rational prime that splits completely in H, the primes over ℓ are in one-to-one correspondence with the embeddings $H \to \mathbb{Q}_\ell$. If $\lambda \mid \ell$, we denote by b_λ the image of $b \in H$ through the corresponding embedding.

For each prime v of L not in $S_{A,L}$, we let $a_v \in H$ be the corresponding trace of Frobenius. With these, we have

$$\mathrm{Tr}(\mathrm{Frob}_v \mid W_\lambda(A)) = a_{v,\lambda} \quad \mathrm{Tr}(\mathrm{Frob}_v \mid W_{\lambda'}(A)) = a_{v,\lambda'}$$

for all $\lambda, \lambda' \mid \ell$. We now have $W_\lambda(A) \simeq W_{\lambda'}(A)$ as $\mathbb{Q}_\ell[G_L]$-modules if and only if $a_{v,\lambda} = a_{v,\lambda'}$ for all but finitely many v, and this is the case if and only if the embeddings given by λ and λ' coincide on $M_2 = \mathbb{Q}(\{a_v\}_{v \notin S_{A,L}})$. Moreover, the embeddings given by λ, λ' coincide on M_2 if and only if they lie over the same prime $\mathfrak{l} \mid \ell$ of M_2. Hence $M_2 = M_3$.

Now we know that $W_\lambda(A)$ is an absolutely irreducible $\mathbb{Q}_\ell[G_L]$-module, and that $\mathrm{End}_{\mathbb{Q}_\ell[G_L]}(W_\lambda(A)) = H_\lambda = \mathbb{Q}_\ell$. We observe that

$$V_\ell(A) = \bigoplus_{\lambda \mid \ell} \mathrm{Res}_{H_\lambda/\mathbb{Q}_\ell} W_\lambda(A)^{\oplus t_A} = \bigoplus_{\lambda \mid \ell} W_\lambda(A)^{\oplus t_A}.$$

Using the characterizing property of M_3, we see the endomorphisms of this representation are

$$\mathrm{End}_{\mathbb{Q}_\ell[G_L]}(V_\ell(A)) = \sum_{\lambda, \lambda' \mid \ell} \mathrm{Hom}_{\mathbb{Q}_\ell[G_L]}(W_\lambda(A)^{\oplus t_A}, W_{\lambda'}(A)^{\oplus t_A}) = \bigoplus_{\mathfrak{l}_3' \mid \ell} \mathrm{M}_{t_A[H:M_3]}(\mathbb{Q}_\ell),$$

where $\mathfrak{l}_3'$ ranges over the primes of M_3 above ℓ. On the other hand, Faltings' isomorphism tells us that $\mathrm{End}_{\mathbb{Q}_\ell[G_L]}(V_\ell(A)) = \mathrm{End}^0(A_L) \otimes \mathbb{Q}_\ell$. The latter is an algebra with center

$$M_1 \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \simeq \prod_{\mathfrak{l}_1' \mid \ell} M_{1,\mathfrak{l}_1'} = \prod_{\mathfrak{l}_1' \mid \ell} \mathbb{Q}_\ell,$$

where $\mathfrak{l}_1'$ ranges over the primes of M_1 above ℓ. This shows $M_1 \otimes \mathbb{Q}_\ell = M_3 \otimes \mathbb{Q}_\ell$. This is an equality inside $H \otimes \mathbb{Q}_\ell$, so M_1 satisfies the same property as M_3, and hence $M_1 = M_3$. □

Recall that K/k is the minimal extension such that $\mathrm{End}(A_K) = \mathrm{End}(A_{\bar{k}})$.

Corollary 5.6.2. *Let* ℓ *be a rational prime that splits completely in* H *and let* $\lambda, \lambda' \mid \ell$ *be primes of* H*. Then* λ *and* λ' *lie over the same prime of* F *if and only if there exists a finite order character* $\chi : G_k \to H^\times$ *such that* $W_\lambda(A) \simeq W_{\lambda'}(A) \otimes \chi$.

PROOF. This is a direct application of Proposition 5.6.1, by taking $L = K$ and considering that $F = M_1$ is the center of $\mathrm{End}^0(A_K)$. □

Proposition 5.6.3. *Let $\xi : G_k \to \bar{\mathbb{Q}}^\times$ be a finite order character. Suppose that there is a set T of primes of H of density one with the following property. For every $\lambda \in T$, there exists a nondegenerate, H_λ-bilinear, G_k-equivariant pairing*

$$W_\lambda(A) \times W_\lambda(A) \to H_\lambda(\xi\chi_\ell),$$

Then $F = \mathbb{Q}\left(\left\{\frac{\mathrm{Tr}(\mathrm{Frob}_v|W_\lambda(A))^2}{\xi(\mathrm{Frob}_v)}\right\}_{v\notin S_A}\right)$.

PROOF. Choose a rational prime ℓ splitting completely in H, in such a way that every prime $\lambda \mid \ell$ of H is in the set T. Fix some prime $\mathfrak{l} \mid \ell$ of F and two primes $\lambda, \lambda' \mid \mathfrak{l}$ of H. In particular, $W_\lambda(A)$ and $W_{\lambda'}(A)$ have each a pairing as stated. Then by Corollary 5.6.2 there exists a character χ of G_k with

$$W_\lambda(A) \simeq W_{\lambda'}(A) \otimes \chi.$$

Therefore, for every prime v of k not in S_A and coprime with ℓ we have

$$a_{v,\lambda} = a_{v,\lambda'} \cdot \chi(\mathrm{Frob}_v).$$

By taking similitudes with respect to the G_k-equivariant pairings, and then dividing by the cyclotomic character, we have

$$\xi(\mathrm{Frob}_v)_\lambda = (\chi(\mathrm{Frob}_v)^2\xi(\mathrm{Frob}_v))_{\lambda'}.$$

We thus obtain

$$\frac{a_{v,\lambda}^2}{\xi(\mathrm{Frob}_v)_\lambda} = \frac{a_{v,\lambda'}^2}{\xi(\mathrm{Frob}_v)_{\lambda'}}, \tag{5.5}$$

and hence $\frac{a_v^2}{\xi(\mathrm{Frob}_v)} \in F$. By varying ℓ, we obtain the inclusion $\mathbb{Q}(\{\frac{a_v^2}{\xi(\mathrm{Frob}_v)}\}_{v\notin S_A}) \subseteq F$.

To see the reverse inclusion, suppose that the equality (5.5) holds for every pair λ and λ' over the fixed prime ℓ, and for all $v \notin S_A$ and not dividing ℓ. Our goal is to see that λ and λ' lie over the same prime of F. By the Chebotaryov density theorem, the functions $\frac{\mathrm{Tr}^2}{\mathrm{sim}}$ of G_k agree for $W_\lambda(A)$ and $W_{\lambda'}(A)$. By taking an extension L of k containing K and such that $G_L \subseteq \ker\xi$, we see that $\mathrm{Tr}(g \mid W_\lambda(A)) = \pm\,\mathrm{Tr}(g \mid W_{\lambda'}(A))$ for all $g \in G_L$. Hence $W_\lambda(A)$ and $W_{\lambda'}(A)$ become $G_{L'}$-isomorphic once we take a further finite extension L'/L. It follows by Proposition 5.6.1 that λ and λ' lie over the same prime of F, and hence $F \subseteq \mathbb{Q}(\{\frac{a_v^2}{\xi(\mathrm{Frob}_v)}\}_{v\notin S_A})$. □

In summary, we have obtained the following result.

Theorem 5.6.4. *Let A be genuinely of GL_n-type. The following are equivalent.*

1. *A is geometrically of the first kind.*
2. *There exists a finite order character $\xi : G_k \to \bar{\mathbb{Q}}^\times$ and a set T of primes of H of density one, such that for every $\lambda \in T$ there exists a nondegenerate H_λ-bilinear, G_k-equivariant pairing*

$$W_\lambda(A) \times W_\lambda(A) \to H_\lambda(\xi\chi_\ell).$$

In that case, $\xi = \varepsilon$, and $F = \mathbb{Q}(\{\frac{a_v^2}{\xi(\mathrm{Frob}_v)}\}_{v\notin S_A})$.

PROOF. That (1) implies (2) is Proposition 5.5.12. Conversely, if we assume (2) then by Proposition 5.6.3 we have the equality

$$F = \mathbb{Q}\left(\left\{\frac{\mathrm{Tr}(\mathrm{Frob}_v \mid W_\lambda(A))^2}{\xi(\mathrm{Frob}_v)}\right\}_{v\notin S_A}\right).$$

Let $\lambda \in T$ and let c denote complex conjugation. By the Weil conjectures, we have ${}^cW_\lambda(A) \simeq W_\lambda(A)^\vee \otimes \chi_\ell$. The pairing on $W_\lambda(A)$ is equivalent to an isomorphism $W_\lambda(A) \simeq W_\lambda(A)^\vee \otimes \xi\chi_\ell$. Combining both isomorphisms we obtain

$${}^cW_\lambda(A) \simeq W_\lambda(A)^\vee \otimes \chi_\ell \simeq W_\lambda(A) \otimes \xi^{-1}.$$

Hence, if we let $a_v = \mathrm{Tr}(\mathrm{Frob}_v \mid W_\lambda(A))$, then $c(a_v) = a_v/\xi(\mathrm{Frob}_v)$. It follows that

$$c\left(\frac{a_v^2}{\xi(\mathrm{Frob}_v)}\right) = \frac{c(a_v)^2}{\xi(\mathrm{Frob}_v)^{-1}} = \frac{a_v^2}{\xi(\mathrm{Frob}_x)},$$

and F is totally real. This is the definition of A being geometrically of the first kind, and we obtain (1). A posteriori, $\xi = \varepsilon$, due to the uniqueness in Proposition 5.5.12. □

5.7. Symplectic and orthogonal representations

In this section, we let A/k be an abelian variety genuinely of GL_n-type and geometrically of the first kind. We let K/k be the minimal extension such that $\mathrm{End}(A_K) = \mathrm{End}(A_{\bar{k}})$, we have $A_K \sim B^r$, where B is the building block associated to A. As before, we let H be the center of $D = \mathrm{End}^0(A)$ and F be the center of $\mathrm{End}^0(B)$.

Lemma 5.7.1. *Let λ be a prime of H lying over a prime $\mathfrak{l} \notin \mathrm{Ram}(\mathrm{End}^0(B))$ of F. Then $\lambda \notin \mathrm{Ram}(\mathrm{End}^0(A))$.*

PROOF. This is a consequence of the Brauer class equation

$$[\mathrm{End}^0(A)] = [\mathrm{End}^0(B) \otimes_F H]$$

from Proposition 5.2.5. Indeed, if $\mathrm{End}^0(B) \otimes_F F_\mathfrak{l}$ is a matrix algebra, then so is $(\mathrm{End}^0(B) \otimes_F F_\mathfrak{l}) \otimes_{F_\mathfrak{l}} H_\lambda$, and we are done since the latter is isomorphic to $(\mathrm{End}^0(B) \otimes_F H) \otimes_H H_\lambda$. □

Fix a prime $\mathfrak{l} \notin \mathrm{Ram}(\mathrm{End}^0(B))$ and let λ be a prime of H over $\mathfrak{l}$. In Section 5.4, we studied the G_k-modules $V_\lambda(A) = V_\ell(A) \otimes_{H\otimes\mathbb{Q}_\ell} H_\lambda$ and $V_\mathfrak{l}(A) = V_\ell(A) \otimes_{F\otimes\mathbb{Q}_\ell} F_\mathfrak{l}$, which are related via the isomorphism

$$V_\mathfrak{l}(A) = \bigoplus_{\lambda'\mid\mathfrak{l}} \mathrm{Res}_{H_{\lambda'}/F_\mathfrak{l}} V_\lambda(A). \tag{5.6}$$

of $F_\mathfrak{l}[G_k]$-modules. Recall that there is an absolutely irreducible $H_\lambda[G_k]$-module $W_\lambda(A)$ such that $V_\lambda(A) \simeq W_\lambda(A)^{\oplus t_A}$. By Proposition 5.5.12, there exists an H_λ-bilinear, non-degenerate, G_k-equivariant pairing

$$\psi_\lambda : W_\lambda(A) \times W_\lambda(A) \to H_\lambda(\varepsilon\chi_\ell),$$

where ε is the Nebentype character of A. If H is a totally real field, then ε is trivial, and moreover ψ_λ is either alternating (if $\mathrm{End}^0(A)$ has Albert type I or II) or symmetric (if $\mathrm{End}^0(A)$ has Albert type III). This is a consequence of Theorems 4.3.3, 4.3.7 and 4.3.11, together with the uniqueness of ψ_λ up to scalars.

We now want to show the alternating or symmetric nature under the assumption that H is not totally real using the building block B. Since $A_K \sim B^r$, we have $V_\ell(A) \simeq V_\ell(B)^{\oplus r}$ as $\mathbb{Q}_\ell[G_K]$-modules. We let $V_\mathfrak{l}(B) = V_\ell(B) \otimes_{F\otimes\mathbb{Q}_\ell} F_\mathfrak{l}$, we then have the isomorphism of $F_\mathfrak{l}[G_K]$-modules

$$V_\mathfrak{l}(A) \simeq V_\mathfrak{l}(B)^{\oplus r}. \tag{5.7}$$

Since B is of the first kind and $\mathfrak{l} \notin \mathrm{Ram}(\mathrm{End}^0(B))$, we know (again from the results of Chapter 4) that there exists an absolutely irreducible $F_\mathfrak{l}[G_K]$-module $W_\mathfrak{l}(B)$ such that $V_\mathfrak{l}(B) \simeq W_\mathfrak{l}(B)^{\oplus t_B}$. Moreover, this module comes with an $F_\mathfrak{l}$-bilinear, non-degenerate, G_K-equivariant pairing

$$\psi_\mathfrak{l} : W_\mathfrak{l}(B) \times W_\mathfrak{l}(B) \to F_\mathfrak{l}(\chi_\ell\,|_{G_K}),$$

which is alternating if B has Albert type I or II, and symmetric if B has Albert type III.

Proposition 5.7.2. *For every $\mathfrak{l} \notin \mathrm{Ram}(\mathrm{End}^0(B))$ and every λ of H over $\mathfrak{l}$, there is an isomorphism $W_\lambda(A) \simeq W_\mathfrak{l}(B) \otimes_{F_\mathfrak{l}} H_\lambda$ of $H_\lambda[G_K]$-modules.*

Proof. Since we are assuming A to be geometrically of the first kind, H/F is a Galois extension by Proposition 5.5.5. Hence we may fix an isomorphism $H_{\lambda'} \simeq H_\lambda$ for each $\lambda' \mid F_\mathfrak{l}$, and see $W_{\lambda'}(A)$ as an $H_\lambda[G_K]$-module. We have isomorphisms of $F_\mathfrak{l}[G_K]$-modules

$$\begin{aligned} V_\mathfrak{l}(A) &\simeq V_\mathfrak{l}(B) \simeq W_\mathfrak{l}(B)^{\oplus r t_B} \\ V_\mathfrak{l}(A) &\simeq \bigoplus_{\lambda'|\mathfrak{l}} \mathrm{Res}_{H_\lambda|F_\mathfrak{l}} V_{\lambda'}(A) \simeq \bigoplus_{\lambda'|\mathfrak{l}} \mathrm{Res}_{H_\lambda|F_\mathfrak{l}} W_{\lambda'}(A)^{\oplus t_A}. \end{aligned}$$

Let $S_{A,K}$ be the set of primes of K above the primes of S_A. For every prime w of K, $w \notin S_{A,K}$, we have

$$\begin{aligned} r t_B \,\mathrm{Tr}_{F_\mathfrak{l}}(\mathrm{Frob}_w \mid W_\mathfrak{l}(B)) &= \mathrm{Tr}_{F_\mathfrak{l}}(\mathrm{Frob}_w \mid V_\mathfrak{l}(A)) \\ &= t_A \sum_{\lambda'|\mathfrak{l}} \mathrm{Tr}_{F_\mathfrak{l}}(\mathrm{Frob}_w \mid \mathrm{Res}_{H_\lambda|F_\mathfrak{l}}(W_{\lambda'}(A))). \end{aligned}$$

Now by Proposition 5.5.6 we know that $\mathrm{Tr}_{H_\lambda}(\mathrm{Frob}_w \mid W_{\lambda'}(A)) \in F$ and that $W_{\lambda'}(A) \simeq W_\lambda(A)$. Hence the above is equal to

$$t_A[H_\lambda : F_\mathfrak{l}] \sum_{\lambda'|\mathfrak{l}} \mathrm{Tr}_{H_\lambda}(\mathrm{Frob}_w \mid W_{\lambda'}(A)) = t_A[H : F] \,\mathrm{Tr}_{H_\lambda}(\mathrm{Frob}_w \mid W_\lambda(A)).$$

Now we have $r t_B = [E : F] = t_A[H : F]$. Hence the proof concludes from the equalities $\mathrm{Tr}_{F_\mathfrak{l}}(\mathrm{Frob}_w \mid W_\mathfrak{l}(B)) = \mathrm{Tr}_{H_\lambda}(\mathrm{Frob}_w \mid W_\lambda(A))$ and the Chebotaryov density theorem. □

Remark 5.7.3. *Just as in Remark 5.5.7, the proposition above works exactly the same whenever F is a CM field, as long as we assume H/F is a Galois extension.*

Theorem 5.7.4. *Let $\mathfrak{l} \notin \mathrm{Ram}(\mathrm{End}^0(B))$ and λ a prime of H over $\mathfrak{l}$. The H_λ-bilinear, G_k-equivariant, nondegenerate pairing*

$$\psi_\lambda : W_\lambda(A) \times W_\lambda(A) \to H_\lambda(\varepsilon\chi_\ell)$$

from Proposition 5.5.12 is alternating if B has Albert type I or II, and symmetric if B has Albert type III.

PROOF. By Proposition 5.7.2, we can define a pairing on $W_\lambda(A)$,

$$\tilde{\psi}_\lambda : W_\lambda(A) \times W_\lambda(A) \to H_\lambda(\chi_\ell|_{G_K}), \quad \tilde{\psi}_\lambda(v \otimes a, w \otimes b) := ab \cdot \psi_{\mathfrak{l}}(v, w)$$

for $v, w \in W_{\mathfrak{l}}(B)$ and $a, b \in H_\lambda$. The pairing $\tilde{\psi}_\lambda$ inherits the properties of $\psi_{\mathfrak{l}}$: it is H_λ-bilinear, nondegenerate, G_K-equivariant, alternating if B has Albert type I or II, and symmetric if B has Albert type III. Now we see that the G_k-equivariant pairing

$$\psi_\lambda : W_\lambda(A) \times W_\lambda(A) \to H_\lambda(\varepsilon\chi_\ell)$$

must coincide, up to some scalar in $H_\lambda^\times$, with $\tilde{\psi}_\lambda$ when seen as a G_K-equivariant pairing: this is a consequence of the irreducibility of $W_\lambda(A)$ as an $H_\lambda[G_K]$-module. Hence ψ_λ is necessarily alternating or symmetric according to the nature of $\psi_{\mathfrak{l}}$. □

Remark 5.7.5. *Theorem 5.7.4 gives an alternative proof of the following fact: there is no abelian variety A/k which is genuinely of GL_2-type and whose building block B has Albert type III (cf.* [**Shi63**, Theorem 5(a)]*). Indeed, the H_λ-bilinear, G_K-equivariant, nondegenerate symmetric pairing*

$$\psi_\lambda : W_\lambda(A) \times W_\lambda(A) \to H_\lambda(\varepsilon\chi_\ell)$$

must coincide with the determinant pairing on $W_\lambda(A)$ up to a scalar in $H_\lambda^\times$. However, the latter is an alternating pairing, which would imply ψ_λ is degenerate, which is a contradiction. Hence B cannot have Albert type III.

We summarize the results we have obtained.

Corollary 5.7.6. *Let A be a simple abelian variety over a number field k which is genuinely of GL_n-type and geometrically of the first kind. Let H be the center of $D = \mathrm{End}^0(A)$ and let $t_A \in \{1, 2\}$ be the Schur index of D. Attached to A there is a strictly compatible system $\{\rho_{A,\lambda}\}_\lambda$ of H-rational representations with values in $\mathbf{GL}_{n/t_A}(D^{op})$.*

Let B be the building block associated to A. For every $\lambda \notin \mathrm{Ram}(D)$, the representation ρ_λ is absolutely irreducible, and moreover:

(1) If B has Albert type I or II, then ρ_λ takes values in $\mathrm{GSp}_n(H_\lambda)$.
(2) If B has Albert type III, then ρ_λ takes values in $\mathrm{GO}_n(H_\lambda)$.

In both cases, the similitude factor of ρ_λ equals $\varepsilon\chi_\ell$.

Definition 5.7.7. *Let A/k be an abelian variety genuinely of GL_n-type and let $B/\bar{k}$ be its associated building block. We say A is genuinely of GSp_n-type if B has Albert type I or II. We say A is genuinely of GO_n-type if B has Albert type III.*

We close the section by giving some examples.

Example 5.7.8.

(1) Any abelian variety A/k with $\mathrm{End}(A_{\bar{k}}) = \mathbb{Z}$ is genuinely of $\mathrm{GSp}_{2\dim A}$-type. As the center $H = \mathbb{Q}$, the Nebentype of A is trivial.

(2) Given any even g, Mestre [**Mes09**] *has constructed families of genus g curves C/k such that (generically) $\mathrm{Jac}(C)$ is geometrically simple and has*

$$\mathrm{End}^0(\mathrm{Jac}(C)_{\bar{\mathbb{Q}}}) = \mathbb{Q}(\sqrt{2}).$$

In our language, this is a family of varieties genuinely of GSp_g-type. Note that the Nebentype is always trivial, since $\mathbb{Q}(\sqrt{2})$ is totally real. For an example, we may take the curve

$$C : y^2 = (x-3)(3x-1)(x^2-5)(x^2+11)(x^2+7)(x^2-4)_{/k},$$

where $k = \mathbb{Q}(\sqrt{5})$. By using the algorithm in [**CMSV19**]*, one checks that*

$$\mathrm{End}^0(\mathrm{Jac}(C)) = \mathrm{End}^0(\mathrm{Jac}(C)_{\bar{k}}) = \mathbb{Q}(\sqrt{2}).$$

(3) *In Chapter 6, we will give families of abelian fourfolds genuinely of GSp_4-type. By taking appropriate specializations, we will obtain fourfolds whose Nebentype is a nontrivial quadratic character.*

(4) *In* [**CFLV23**]*, Cantoral-Farfán, Lombardo and Voight give curves $C/\mathbb{Q}$ of every even genus $g \geq 4$, such that its jacobian $A = \mathrm{Jac}(C)$ has $\mathrm{End}^0(A) = \mathbb{Q}(\sqrt{-1})$, and $\mathrm{End}^0(A_{\bar{\mathbb{Q}}})$ is the quaternion algebra ramified at 2 and ∞. It follows that A is genuinely of GO_g-type and has nontrivial Nebentype. For a concrete example, we may take the jacobian of the genus-4 curve*

$$C : y^2 = x(x^4 - 1)(x^4 + x^2 + 1).$$

5.8. Siegel-modular abelian varieties

Let π be a cuspidal automorphic representation of $\mathrm{GSp}_4(\mathbb{A}_{\mathbb{Q}})$ of weight $(2,2)$ which is not CAP or endoscopic. Let ε_π be the Dirichlet character corresponding to the central character of π, and let H_π be the coefficient field of π. By [**Wei22**, Theorem 3.3], for each prime λ of H_π there is a continuous, semisimple Galois representation

$$\rho_{\pi,\lambda} : G_{\mathbb{Q}} \to \mathrm{GSp}_4(\bar{H}_{\pi,\lambda})$$

with similitude $\varepsilon_\pi \chi_\ell$. Moreover, the representations $\{\rho_{\pi,\lambda}\}$ form a strictly compatible system (with exceptional set equal to the set of primes at which π ramifies). We let $W_\lambda(\pi)$ be the $\bar{H}_{\pi,\lambda}$-vector space on which $G_{\mathbb{Q}}$ acts through $\rho_{\pi,\lambda}$. We fix a prime λ of H dividing a rational prime ℓ, and we define the number field

$$F_\pi = \mathbb{Q}\left(\left\{\frac{\mathrm{Tr}(\rho_{\pi,\lambda}(\mathrm{Frob}_p))^2}{\varepsilon_\pi(p)}\right\}_{p \nmid \ell N}\right).$$

Theorem 5.8.1. *Let $A/\mathbb{Q}$ be an abelian variety genuinely of GL_4-type and let $B/\bar{\mathbb{Q}}$ be its associated building block. Let H_A be the center of $\mathrm{End}^0(A)$ and let F_A be the center of $\mathrm{End}^0(A_{\bar{\mathbb{Q}}})$. Let ℓ be a rational prime. Fix embeddings $H_\pi \to \bar{\mathbb{Q}}_\ell$ and $H_A \to \bar{\mathbb{Q}}_\ell$ and let λ, λ' be the corresponding primes of H_π and H_A over ℓ, respectively. Suppose that $\lambda' \notin \mathrm{Ram}(\mathrm{End}^0(A))$ and that there is an isomorphism of $\bar{\mathbb{Q}}_\ell[G_{\mathbb{Q}}]$-modules*

$$W_\lambda(\pi) \simeq W_{\lambda'}(A) \otimes_{H_{\lambda'}} \bar{\mathbb{Q}}_\ell.$$

Then A is geometrically of the first kind and B has Albert type I *or* II*. Moreover, we have $H_A = H_\pi$, $F_A = F_\pi$, and if ε_A denotes the Nebentype of A, then $\varepsilon_A = \varepsilon_\pi$.*

Proof. The fields H_π and H_A are generated by the traces of Frobenius elements Frob_v for v acting on $W_\lambda(\pi)$ and $W_\lambda(A)$ outside of a finite set, respectively. It follows that $H_A = H_\pi$, and we may assume $\lambda = \lambda'$. The fact that $\rho_{\pi,\lambda}$ takes values in $\mathrm{GSp}_4(\bar{H}_{\pi,\lambda})$ means there is a $G_{\mathbb{Q}}$-equivariant, nondegenerate, $\bar{H}_{\pi,\lambda}$-bilinear alternating pairing

$$\Psi_\lambda : W_\lambda(\pi) \times W_\lambda(\pi) \to \bar{H}_{\pi,\lambda}(\varepsilon_\pi \chi_\ell).$$

Since the image of $\rho_{\pi,\lambda} \simeq \rho_{A,\lambda}$ also lands in $\mathrm{GL}_4(H_{\pi,\lambda})$, and Ψ_λ is given by linear conditions and has similitude $\varepsilon_\pi \chi_\ell$, it follows that there exists a pairing on $W_\lambda(A)$ with similitude $\varepsilon_\pi \chi_\ell$. Namely, we have a pairing

$$\psi_\lambda : W_\lambda(A) \times W_\lambda(A) \to H_{A,\lambda}(\varepsilon_\pi \chi_\ell)$$

which is equivariant, nondegenerate and alternating. We now observe that for every other rational prime $\tilde{\ell}$ and $\tilde{\lambda} \mid \tilde{\ell}$ of H_A not in $\mathrm{Ram}(\mathrm{End}^0(A))$, we have

$$W_{\tilde{\lambda}}(\pi) \simeq W_{\tilde{\lambda}}(A) \otimes \bar{H}_{A,\tilde{\lambda}},$$

because the representations in both sides are part of their respective compatible systems. In particular, $W_\lambda(A)$ carries an alternating pairing for all but finitely many λ. By Theorem 5.6.4, A is geometrically of the first kind and $\varepsilon_\pi = \varepsilon_A$, and we also obtain $F_A = F_\pi$. Finally, assume for a contradiction the building block B has Albert type III. Then by Theorem 5.7.4 we would have a nondegenerate symmetric pairing ψ'_λ on $W_\lambda(A)$ with similitude character $\varepsilon_A \chi_\ell$. By the uniqueness of the pairing ψ'_λ up to scalars from Proposition 5.5.12, we have $\psi_\lambda = \kappa \psi'_\lambda$ for some nonzero κ, and so ψ_λ is both alternating and symmetric. But then this is a degenerate pairing, which is a contradiction. Hence B has Albert type I or II. □

Remark 5.8.2. *In* [**KKW22**, § 2.1]*, the field F_π has been identified as the field generated by the traces of $\rho_{\pi,\lambda}$ after restricting to the field cut out by inner twists. By Corollary 5.5.11, Proposition 5.6.1 and Proposition 5.6.3, this corresponds to our characterization of the center F_A of* $\mathrm{End}^0(A_{\bar{\mathbb{Q}}})$.

In the particular case where A is a fourfold and $\mathrm{End}^0(A) = D$ is a quaternion algebra, the result we just proved confirms the expectation in [**BCGP21**, §10.4.1] that D should be indefinite. More precisely, we have the following result.

Proposition 5.8.3. *Let π be an automorphic representation of* $\mathrm{GSp}_4(\mathbb{A}_\mathbb{Q})$ *of weight* $(2,2)$ *which is not CAP or endoscopic, and suppose that $H_\pi = \mathbb{Q}$ (in particular, the character ε_π is trivial). If $A/\mathbb{Q}$ is a simple abelian variety genuinely of* GL_4*-type such that $\rho_{\pi,\ell} \simeq \rho_{A,\ell}$ for some prime ℓ, then either*

1. *A is an abelian surface with* $\mathrm{End}^0(A_{\bar{\mathbb{Q}}}) = \mathbb{Q}$*, or*
2. *A is an abelian fourfold, and* $\mathrm{End}^0(A)$ *is a division indefinite quaternion algebra with center* $\mathbb{Q}$.

In both cases, $\mathrm{End}^0(A) = \mathrm{End}^0(A_{\bar{\mathbb{Q}}})$ *and A is geometrically simple.*

Proof. By Theorem 5.8.1, the variety A is geometrically of the first kind and $H_A = \mathbb{Q}$, and its associated building block has Albert type I or II. By Proposition 5.2.9, we obtain that $\mathrm{End}^0(A)$ is an algebra with either Albert type I or II. The first case yields $\mathrm{End}^0(A) = \mathbb{Q}$, and since A is genuinely of GL_4-type, necessarily $\dim A = 2$ and A is geometrically simple with $\mathrm{End}^0(A_{\bar{\mathbb{Q}}}) = \mathbb{Q}$.

The second case implies $D = \mathrm{End}^0(A)$ is an indefinite quaternion algebra over $\mathbb{Q}$, and letting E be a maximal subfield of endomorphisms we obtain $\dim A = \frac{n[E:\mathbb{Q}]}{2} = \frac{4\cdot 2}{2} = 4$. That A is geometrically simple also follows: otherwise, $A_{\bar{\mathbb{Q}}}$ would be isogenous to the square of a simple surface with trivial endomorphism ring, and we would have an embedding $D \to \mathrm{M}_2(\mathbb{Q})$. But this would contradict the fact that D was a division algebra, therefore, $A_{\bar{\mathbb{Q}}}$ is simple. □

Remark 5.8.4. *The existence of an abelian variety $A/\mathbb{Q}$ associated to a representation π as in the previous result has been shown (assuming several open conjectures) in* [**BCGP21**, Lemma 10.3.2].

CHAPTER 6

Families of abelian fourfolds of GSp_4-type

Let k be a number field. In this chapter we construct a family of abelian surfaces which are k-building blocks of GL_4-type (cf. Definition 5.2.1). Assuming a certain norm condition on k, we will obtain abelian fourfolds A/k whose associated building block is a given member B of our family. We also show that $\mathrm{End}^0(A)$ is either $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{-2})$. This yields examples of abelian fourfolds genuinely of GSp_4-type, and in particular we will encounter nontrivial Nebentypes.

The construction uses Richelot isogenies of genus 2 curves. We review them in Section 6.1, as well as some ideas from effective elimination theory. We then compute the family of building blocks in Section 6.2. We show how to descend the building blocks to a quadratic extension of k in Section 6.3, this also gives us the abelian fourfolds genuinely of GSp_4-type and their endomorphisms. We conclude in Section 6.4 with some particular examples.

Throughout the chapter, if $C : y^2 = f(x)$ is a hyperelliptic curve over a field K and $d \in K^\times$, we let $C_d : dy^2 = f(x)$ be the quadratic twist of C by d. If d is a nonsquare, the curve C_d is the twist of C corresponding to the extension $K(\sqrt{d})/K$. We will use a similar notation for abelian varieties, letting $\mathrm{Jac}(C)_d$ be the the twist of $\mathrm{Jac}(C)$ by $K(\sqrt{d})/K$. In this way, we can identify the twist $\mathrm{Jac}(C)_d$ with $\mathrm{Jac}(C_d)$.

6.1. Preliminaries

We begin by recalling the notion of a building block from Definition 5.2.1. Let k be a number field, and let $B/\bar{k}$ be an abelian variety. We say B is a k-building block of GL_n-type if the following conditions hold:

(1) For every $s \in G_k$, there exists an isogeny $\mu_s : {}^sB \to B$, such that for all $\varphi \in \mathrm{End}^0(B)$, $\varphi \circ \mu_s = \mu_s \circ {}^s\varphi$.
(2) $\mathrm{End}^0(B)$ is a division algebra with center F and Schur index t_B such that $nt_B[F : \mathbb{Q}] = 2 \dim B$.

If we let K/k be a finite Galois extension such that B is defined over K and $\mathrm{End}^0(B_K) = \mathrm{End}^0(B_{\bar{k}})$, then we may replace the group G_k in (1) by $\mathrm{Gal}(K/k)$, and condition (2) amounts to saying that B is geometrically simple, of GL_n-type, and not of GL_m-type for $m < n$.

We wish to produce an abelian surface B/K which is a k-building block of GL_4-type. Since a simple abelian surface genuinely of GL_4-type has trivial endomorphism ring, asking for condition (1) in the definition above is equivalent to asking for a set of isogenies $\{\mu_s : {}^sB \to B\}_{s \in \mathrm{Gal}(K/k)}$, possibly defined over $\bar{k}$. We also make the simplification that K/k is quadratic. Our problem is the following.

Problem 6.1.1. *Let K/k be a quadratic extension of number fields and let s be the nontrivial element of $\mathrm{Gal}(K/k)$. Compute an abelian surface B/K with $\mathrm{End}(B_{\bar{K}}) = \mathbb{Z}$ such that there is an isogeny $\mu_s : {}^sB \to B$.*

We will in fact look for a genus 2 curve C/K such that $B = \mathrm{Jac}(C)$ satisfies the conditions in the problem. The $(2,2)$-isogenies on B (called Richelot isogenies) can be easily computed in terms of C, and we will impose equations so that the codomain surface is the jacobian of ${}^sC$. We shall solve these equations by using the results of elimination theory.

6.1.1. Richelot isogenies. We follow [**BD11**], which in turn follows [**Smi05**, Chapter 8]. The interested reader may also consult [**CF96**, Chapter 9]. In this section, we let K be a field of characteristic different from 2 and C be a genus two curve defined over K. Such a curve can always be given as

$$C : Y^2 = f(X) = \prod_{i=1}^{6}(X - e_i)$$

where $e_i \in \bar{K}$ for each $i = 1, \ldots, 6$. The Weierstrass points of C are $T_i = (e_i, 0)$ for $i = 1, \ldots, 6$. Then it can be shown that

$$\mathrm{Pic}^0(C_{\bar{K}})[2] = \{[T_i - T_j]\}_{i,j\in\{1,\ldots,6\}}.$$

In particular, given a reordering $\{i_1, \ldots, i_6\}$ of the set $\{1, \ldots, 6\}$, one can show that

$$[T_{i_1} - T_{i_2}] + [T_{i_3} - T_{i_4}] = [T_{i_5} - T_{i_6}].$$

This makes $\{0, [T_{i_1} - T_{i_2}], [T_{i_3} - T_{i_4}], [T_{i_5} - T_{i_6}]\}$ a subgroup of $\mathrm{Pic}^0(C_{\bar{K}})[2]$. Upon considering the mod 2 Weil pairing $\bar{\psi}_2 : \mathrm{Jac}(C)[2] \times \mathrm{Jac}(C)[2] \to \{\pm 1\}$, it turns out that all maximal isotropic subgroups of $\mathrm{Pic}^0(C_{\bar{K}})[2]$ are precisely of this form. Such a subgroup of $\mathrm{Pic}^0(C_{\bar{K}})[2]$ is then represented by a quadratic splitting

$$f(X) = F_1(X)F_2(X)F_3(X),$$

where F_1, F_2, F_3 are quadratic polynomials

$$\begin{aligned} F_1(X) &= a_2X^2 + a_1X + a_0, \\ F_2(X) &= b_2X^2 + b_1X + b_0, \\ F_3(X) &= c_2X^2 + c_1X + c_0 \end{aligned}$$

with coefficients in $\bar{K}$ (in practice, we will assume the coefficients lie in K). The quadratic splitting is said to be non-singular if the determinant

$$\delta := \det \begin{pmatrix} a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 \\ c_0 & c_1 & c_2 \end{pmatrix}$$

is non-zero. In that case, we let

$$\tilde{G}_i(X) := F_j'(X)F_k(X) - F_j(X)F_k'(X),$$

and $G_i = \delta^{-1}\tilde{G}_i$, where the tuple (i, j, k) is one of $(1, 2, 3), (2, 3, 1), (3, 1, 2)$. Then for $d \in K^\times$, we define the curve

$$\tilde{C}_d : dV^2 = G_1(U)G_2(U)G_3(U). \tag{6.1}$$

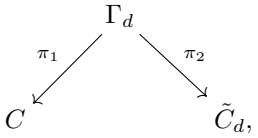
In particular, the curve $\tilde{C}_d$ is a quadratic twist of $\tilde{C} := \tilde{C}_1$. There is a correspondence $\Gamma_d \subset (C \times \tilde{C}_d)_{\bar{K}}$,

$$\Gamma_d : \begin{cases} F_1(X)G_1(U) + F_2(X)G_2(U) = 0 \\ \sqrt{d}YV = F_1(X)G_1(U)(X-U). \end{cases} \tag{6.2}$$

This correspondence induces two isogenies

$$\varphi : \mathrm{Pic}^0(C_{\bar{K}}) \to \mathrm{Pic}^0(\tilde{C}_{d,\bar{K}}), \quad \hat{\varphi} : \mathrm{Pic}^0(\tilde{C}_{d,\bar{K}}) \to \mathrm{Pic}^0(C_{\bar{K}}),$$

dual of each other, of degree $(2,2)$ (meaning that $\ker\varphi, \ker\hat{\varphi} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$). The isogenies come from considering the diagram



where π_1 and π_2 are the restrictions to Γ_d of the projections from $C \times \tilde{C}_d$, so that $\varphi = \pi_{2,*} \circ \pi_1^*$ and $\hat{\varphi} = \pi_{1,*} \circ \pi_2^*$. Observe that these are maps between $\mathrm{Pic}(C)$ and $\mathrm{Pic}(\tilde{C}_d)$, so we can compute them for divisors of arbitrary degree.

We now describe φ and $\hat{\varphi}$ explicitly on affine divisors $\sum n_i(a_i, b_i)$, it is enough to find the image of the class of $(a,b) \in C(\bar{K})$ and extend by linearity. We let α_1, α_2 be the two roots of the quadratic equation

$$F_1(a)G_1(U) + F_2(a)G_2(U) = 0.$$

Suppose $b \neq 0$. Then, for $i = 1, 2$ we let $\beta_i = \frac{F_1(a)G_1(\alpha_i)(a-\alpha_i)}{b\sqrt{d}}$, so that

$$\varphi([(a,b)]) = [(\alpha_1, \beta_1) + (\alpha_2, \beta_2)].$$

Note that either $\alpha_1, \alpha_2 \in K$, or they live in a quadratic extension of K and are Galois conjugates. This means that the image of $[(a,b)]$ is a divisor defined over K. However, we remark that Γ_d itself might only be defined over the quadratic extension $K(\sqrt{d})$ of K. In particular, φ is defined over K if and only if $d \in (K^\times)^2$.

The correspondence (6.2) is symmetric in (X,Y) and (U,V), so that $\hat{\varphi}$ is obtained with the same procedure. Indeed, let $(u,v) \in \tilde{C}_d(\bar{K})$ be an affine point with $v \neq 0$, and let μ_1, μ_2 be the two roots of the quadratic equation

$$F_1(X)G_1(u) + F_2(X)G_2(u) = 0.$$

Then, for $i = 1, 2$ we let $\nu_i = \frac{F_1(\mu_i)G_1(u)(\mu_i - u)}{v\sqrt{d}}$, so that

$$\hat{\varphi}([(u,v)]) = [(\mu_1, \nu_1) + (\mu_2, \nu_2)].$$

As for φ, the isogeny $\hat{\varphi}$ is defined over K if and only if $d \in (K^\times)^2$.

6.1.2. Elimination theory. We briefly summarize some tools that we need from [**CLO15**, Chapter 3]. To find parametrizations of genus 2 curves equipped with a Richelot isogeny, we will need to solve fairly large systems of equations. Elimination theory can help us do that, by reducing to a lower-dimensional variety that is hopefully simpler.

Let k be a field. Given an ideal $I = (f_1, \ldots, f_s) \subset k[x_1, \ldots, x_n]$, the jth elimination ideal I_j is the ideal of $k[x_{j+1}, \ldots, x_n]$ given by

$$I_j = I \cap k[x_{j+1}, \ldots, x_n].$$

This ideal is easily computed with the aid of Gröbner bases (cf. [**CLO15**, Theorem 2]). The vanishing locus $V(I)$ of the ideal I is an affine variety in $\mathbb{A}^n(\bar{k})$, while the vanishing locus of $V(I_j)$ of the jth elimination ideal is an affine variety in $\mathbb{A}^{n-j}(\bar{k})$. We have a projection map

$$\pi_j : \mathbb{A}^n \to \mathbb{A}^{n-j}$$

which maps $V(I)$ inside $V(I_j)$. This step is called "elimination", since the equations defining $V(I_j)$ have fewer variables. A point $x \in V(I_j)$ is called a *partial solution*. If we work over $\bar{k}$, we have the following theorem.

Theorem 6.1.2 (Closure theorem)**.** *Let $V = V(I) \subset \mathbb{A}^n(\bar{k})$ and let I_j be the jth* elimination ideal *of I. Then:*

(1) $V(I_j)$ is the smallest affine variety containing $\pi_j(I)$, that is, $\overline{\pi_j(I)} = V(I_j)$.
(2) When $V \neq \emptyset$, there is an affine variety $W \subsetneq V(I_j)$ such that $V(I_j) \setminus W \subseteq \pi_j(V)$.

Provided we can find points in $V(I_j)$, we want to recover points in $V(I_{j-1})$. For that, we observe that we have a filtration

$$V(I) \to V(I_1) \to V(I_2) \to \cdots \to V(I_n),$$

so that we can treat the problem as if we had eliminated one variable at a time.

Theorem 6.1.3 (Extension theorem)**.** *Let $I = (f_1, \ldots, f_s) \subset \bar{k}[x_1, \ldots, x_n]$ and let I_1 be the first elimination ideal of I. For each $1 \leq i \leq s$, write f_i in the form*

$$f_i = c_i(x_2, \ldots, x_n)x_1^{N_i} + \text{terms of lower degree in } x_1,$$

where $N_i \geq 0$ and $c_i \in \bar{k}[x_2, \ldots, x_n]$ is nonzero. Suppose that we have a partial solution $(a_2, \ldots, a_n) \in V(I_1)$. If $(a_2, \ldots, a_n) \notin V(c_1, \ldots, c_s)$, then there exists $a_1 \in \bar{k}$ such that $(a_1, a_2, \ldots, a_n) \in V(I)$.

If we wish to parametrize points in $V(I)(k)$, we will have to be careful enough to choose points in the smaller variety $V(I_j)$ such that their successive extensions happen in k. In our particular example, this will be possible thanks to the linear form of the extension equations.

6.2. k-varieties over $\bar{k}$

In this section we give a family of genus 2 curves whose Jacobians solve Problem 6.1.1. Our treatment is mostly computational, we give the family in Theorem 6.2.1.

We work over a base field k. Let $\Delta \in k^\times$ be a nonsquare and let $K = k(\sqrt{\Delta})$. Let also $\mathrm{Gal}(K/k) = \langle\sigma\rangle$. Let a_{ij}, b_{ij}, c_{ij} be variables with $0 \leq i \leq 2$ and $j = 1, 2$, and set

$$a_i = a_{i0} + a_{i1}\sqrt{\Delta}, \qquad b_i = b_{i0} + b_{i1}\sqrt{\Delta}, \qquad c_i = c_{i0} + c_{i1}\sqrt{\Delta},$$

for $i = 0, 1, 2$. With similar notation as in Section 6.1.1, we consider polynomials $F_i \in K[X, a_{ij}, b_{ij}, c_{ij}]$,

$$\begin{aligned} F_1(X) &= a_2X^2 + a_1X + a_0, \\ F_2(X) &= b_2X^2 + b_1X + b_0, \\ F_3(X) &= c_2X^2 + c_1X + c_0. \end{aligned}$$

We let

$$\delta := \det \begin{pmatrix} a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 \\ c_0 & c_1 & c_2 \end{pmatrix},$$

and $\tilde{G}_i := F_j' F_k - F_j F_k'$ for $(i,j,k) = (1,2,3), (2,3,1), (3,1,2)$. We also introduce a variable d (cf. (6.1)), which we will adjust to solve our equations. We have seen that there is a Richelot correspondence between the curves $C : Y^2 = F_1(X)F_2(X)F_3(X)$ and $\tilde{C}_d : d\delta^3 V^2 = \tilde{G}_1(U)\tilde{G}_2(U)\tilde{G}_3(U)$, which are defined over $K[d, a_{ij}, b_{ij}, c_{ij}]$.

With notation as above, a first possibility would be to ask for the equality ${}^\sigma C = \tilde{C}_d$, that is, asking for the equation ${}^\sigma(d\delta^3 F_1F_2F_3) = \tilde{G}_1\tilde{G}_2\tilde{G}_3$ to be satisfied. The problem is that the polynomial δ^3 is too complicated, and it would be hard to solve the system. Instead, we will ask for the equality ${}^\sigma C = \tilde{C}_{d/\delta^3}$, via the equation

$${}^\sigma(dF_1F_2F_3) = \tilde{G}_1\tilde{G}_2\tilde{G}_3$$

By equating the coefficients of powers of X in terms of the basis 1, $\sqrt{\Delta}$ of K/k, this produces a set of twelve equations in the nineteen variables $\{d, a_{ij}, b_{ij}, c_{ij}\}$, corresponding to an affine variety $W \subset \mathbb{A}^{19}_k$. Each point on $W(k)$ will give a genus 2 curve C/K with ${}^\sigma C = \tilde{C}_{d/\delta^3}$ and a $(2,2)$-isogeny $\mathrm{Jac}(C) \to \mathrm{Jac}(\tilde{C}_{d/\delta^3}) = \mathrm{Jac}({}^\sigma C)$. We observe that the isogeny will be defined over the field $K(\sqrt{d}, \sqrt{\delta})$, which is a priori a biquadratic extension of K. However, the variety W is still difficult to parametrize. A reasonable restriction is to impose the equations

$$ {}^\sigma(dF_1) = \tilde{G}_1, \qquad {}^\sigma F_2 = \tilde{G}_2, \qquad {}^\sigma F_3 = \tilde{G}_3. \tag{6.3}$$

which correspond to a subvariety $V \subset W$. The vanishing ideal for V has the following generating polynomials:

$$\begin{aligned}
&-\Delta c_{01}b_{11} + \Delta c_{11}b_{01} + c_{10}b_{00} + da_{00} - c_{00}b_{10}, && c_{00}b_{11} - c_{11}b_{00} - c_{10}b_{01} + da_{01} + c_{01}b_{10},\\
&\Delta c_{01}a_{11} - \Delta c_{11}a_{01} + c_{00}a_{10} - c_{10}a_{00} + b_{00}, && -c_{01}a_{10} - c_{00}a_{11} + c_{11}a_{00} + c_{10}a_{01} + b_{01},\\
&-\Delta b_{01}a_{11} + \Delta b_{11}a_{01} - b_{00}a_{10} + a_{00}b_{10} + c_{00}, && b_{01}a_{10} + b_{00}a_{11} - b_{11}a_{00} - a_{01}b_{10} + c_{01},\\
&2\Delta c_{21}b_{01} - 2\Delta c_{01}b_{21} + 2c_{20}b_{00} + da_{10} - 2c_{00}b_{20}, && -2c_{21}b_{00} - 2c_{20}b_{01} + da_{11} + 2c_{01}b_{20} + 2c_{00}b_{21},\\
&2\Delta c_{01}a_{21} - 2\Delta c_{21}a_{01} + 2c_{00}a_{20} - 2c_{20}a_{00} + b_{10}, && -2c_{01}a_{20} - 2c_{00}a_{21} + 2c_{21}a_{00} + 2c_{20}a_{01} + b_{11},\\
&-2\Delta b_{01}a_{21} + 2\Delta a_{01}b_{21} - 2b_{00}a_{20} + 2a_{00}b_{20} + c_{10}, && 2b_{01}a_{20} + 2b_{00}a_{21} - 2a_{01}b_{20} - 2a_{00}b_{21} + c_{11},\\
&\Delta c_{21}b_{11} - \Delta c_{11}b_{21} + da_{20} - c_{10}b_{20} + c_{20}b_{10}, && -c_{20}b_{11} + da_{21} + c_{11}b_{20} + c_{10}b_{21} - c_{21}b_{10},\\
&\Delta c_{11}a_{21} - \Delta c_{21}a_{11} + c_{10}a_{20} - c_{20}a_{10} + b_{20}, && -c_{11}a_{20} - c_{10}a_{21} + c_{21}a_{10} + c_{20}a_{11} + b_{21},\\
&-\Delta b_{11}a_{21} + \Delta a_{11}b_{21} + a_{10}b_{20} - a_{20}b_{10} + c_{20}, && b_{11}a_{20} - a_{11}b_{20} - a_{10}b_{21} + a_{21}b_{10} + c_{21}.
\end{aligned}$$

We wish to find (at least some of) the points in $V(k)$. The first step towards that is considering the elimination ideal

$$I_a = I(V) \cap k[d, a_{20}, a_{21}, a_{10}, a_{11}, a_{00}, a_{01}].$$

By using Sage [**The23**], we find that I_a has a decomposition as the product of ideals

$$I_a = (a_{20}, a_{21}, a_{10}, a_{11}, a_{00}, a_{01})(a_{10}^2 - \Delta a_{11}^2 + 4\Delta a_{21}a_{01} - 4a_{20}a_{00} + 1).$$

In other words, $V(I_a)$ has two irreducible components, one of them corresponding to the polynomial F_1 being zero. This case does not interest us, in fact, we can replace V by an open set such that no points correspond to a product of polynomials with either F_1, F_2 or F_3 vanishing identically. Let I_a' be the ideal generated by $a_{10}^2 - \Delta a_{11}^2 + 4\Delta a_{21}a_{01} - 4a_{20}a_{00} + 1$.

The interesting component is a quadric hypersurface, which is very easy to parametrize. Moreover, if we define two more elimination ideals

$$I_b = I(V) \cap k[d, b_{20}, b_{21}, b_{10}, b_{11}, b_{00}, b_{01}],$$
$$I_b = I(V) \cap k[d, c_{20}, c_{21}, c_{10}, c_{11}, c_{00}, c_{01}]$$

and discard the convenient points, we have the very similar generators

$$I'_b = (b_{10}^2 - \Delta b_{11}^2 + 4\Delta b_{21}b_{01} - 4b_{20}b_{00} + d),$$
$$I'_c = (c_{10}^2 - \Delta c_{11}^2 + 4\Delta c_{21}c_{01} - 4c_{20}c_{00} + d).$$

We denote by $V' \subset V$ the affine subvariety at which the polynomials F_i are not identically zero.

In the following, we will make F_2 a degree-1 polynomial, an we will extend the partial solutions from the varieties $V(I'_a)$ and $V(I'_b) \cap \{b_{20} = b_{21} = 0\}$ (cf. Theorem 6.1.3). Note that we have projections

$$\begin{array}{ccc} & V' & \\ \swarrow & & \searrow \\ V(I'_a) & & V(I'_b). \end{array}$$

Since the polynomial defining I'_b evaluated at $b_{20} = b_{21} = 0$ is

$$b_{10}^2 - \Delta b_{11}^2 + d,$$

setting the parameter $d = \Delta$ gives the trivial root $(b_{10}, b_{11}) = (0, 1)$. We fix values in k for $a_{20}, a_{21}, a_{10}, a_{11}, a_{01}$. Using the quadratic generator of I'_a and imposing $a_{20} \neq 0$ we have

$$a_{00} = \frac{a_{10}^2 - \Delta a_{11}^2 + 4\Delta a_{21}a_{01} + 1}{4a_{20}}.$$

Substituting these fixed values of $b_{20}, b_{21}, b_{10}, b_{11}$ and of a_{ij} in the generators of I that do not involve b_{00} or b_{01}, we have the following (linear) system of equations on the variables c_{ij}:

$$\begin{cases} c_{20} & = \Delta a_{21} \\ c_{21} & = -a_{20} \\ -2a_{00}c_{20} - 2\Delta a_{01}c_{21} + 2a_{20}c_{00} + 2\Delta a_{21}c_{01} & = 0 \\ -a_{10}c_{20} - \Delta a_{11}c_{21} + a_{20}c_{10} + \Delta a_{21}c_{11} & = 0 \\ 2a_{01}c_{20} + 2a_{00}c_{21} - 2a_{21}c_{00} - 2a_{20}c_{01} & = -1 \\ a_{11}c_{20} + a_{10}c_{21} - a_{21}c_{10} - a_{20}c_{11} & = 0 \end{cases} \tag{6.4}$$

We immediately find that $c_{20} = \Delta a_{21}$ and $c_{21} = -a_{20}$. Solving the rest of the system yields the values

$$c_{10} = -\Delta a_{11}, \qquad c_{11} = -a_{10}, \qquad c_{00} = -\Delta a_{01}, \qquad c_{01} = \frac{1}{2} - a_{00}.$$

We now let M be the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ -2a_{00} & -2\Delta a_{01} & 0 & 0 & 2a_{20} & 2\Delta a_{21} \\ -a_{10} & -\Delta a_{11} & a_{20} & \Delta a_{21} & 0 & 0 \\ 2a_{01} & 2a_{00} & 0 & 0 & -2a_{21} & -2a_{20} \\ a_{11} & a_{10} & -a_{21} & -a_{20} & 0 & 0 \end{pmatrix}$$

corresponding to the homogeneous system of (6.4). We find that $\det M = -4\,\mathrm{Nm}_{K/k}(a_{20}+\sqrt{\Delta}a_{21})^2$, so the given solution to the system is unique if and only if $a_2 = a_{20} + \sqrt{\Delta}a_{21} \neq 0$, if and only if the polynomial $F_1(X)$ has degree 2. Since we have chosen $F_2(X)$ to have degree 1, and the product $F_1F_2F_3$ needs to have degree 5 or 6, the condition $a_2 \neq 0$ was already necessary. It remains to compute b_{00} and b_{01}. Among the equations defining V' we have

$$b_{00} = c_{10}a_{00} - c_{00}a_{10} + \Delta(c_{11}a_{01} - c_{01}a_{11}),$$
$$b_{01} = c_{01}a_{10} + c_{00}a_{11} - c_{11}a_{00} - c_{10}a_{01}.$$

These values are compatible with the previously found ones in the sense of Theorem 6.1.3, yielding a point of $V'(k)$.

To obtain an explicit parametrization, we choose values $r, s, t \in k$ and let $a_{20} = 1, a_{21} = 0, a_{10} = r, a_{11} = s, a_{01} = t$. We have proved the first half of our main result.

Theorem 6.2.1. *Let k be a number field and let $K = k(\sqrt{\Delta})$ be a quadratic extension. Let σ be the nontrivial element of $\mathrm{Gal}(K/k)$. Given $r, s, t \in k$, let $w = (r^2 - \Delta s^2 + 1)/4$, and define three polynomials*

$$F_1(X) = X^2 + (r + s\sqrt{\Delta})X + (w + t\sqrt{\Delta})$$
$$F_2(X) = \sqrt{\Delta}X + \left(-\frac{s\Delta}{2} + \frac{r}{2}\sqrt{\Delta}\right)$$
$$F_3(X) = -\sqrt{\Delta}X^2 - (s\Delta + r\sqrt{\Delta})X + \left(-\Delta t + \left(\frac{1}{2} - w\right)\sqrt{\Delta}\right).$$

Let $C_{r,s,t}$ be the curve $Y^2 = F_1(X)F_2(X)F_3(X)$, provided it is smooth. Then the jacobian of $C_{r,s,t}$ is $(2,2)$-isogenous over $K(\sqrt{-2}) = k(\sqrt{\Delta}, \sqrt{-2})$ to the jacobian of ${}^\sigma C_{r,s,t}$. In particular, $\mathrm{Jac}(C_{r,s,t})$ is a genus-2 k-surface with respect to $\bar{k}$.

Proof. It remains to see that $\mathrm{Jac}(C)$ is $(2,2)$-isogenous to $\mathrm{Jac}({}^\sigma C)$ over $K(\sqrt{-2})$. We already know that there is an equality ${}^\sigma C = \tilde{C}_{\Delta/\delta^3}$, and we have an isogeny $\mathrm{Jac}(C) \to \mathrm{Jac}(\tilde{C}_{\Delta/\delta^3})$, which is defined over $K(\sqrt{\delta})$. By direct computation, we have

$$\delta = \begin{vmatrix} w + t\sqrt{\Delta} & r + s\sqrt{\Delta} & 1 \\ 0 & \sqrt{\Delta} & \frac{1}{2}(-s\Delta + r\sqrt{\Delta}) \\ -\sqrt{\Delta} & (-s\Delta - r\sqrt{\Delta}) & -\Delta t + \left(\frac{1}{2} - w\right)\sqrt{\Delta} \end{vmatrix} = -\frac{\Delta}{2},$$

so that $K(\sqrt{\delta}) = K(\sqrt{-2})$. □

Remark 6.2.2. *The discriminant of $C = C_{r,s,t}$ is a nonzero polynomial in r, s, t and w (which is seen by evaluating e.g. at $(r, s, t) = (1, -1, 2)$), so the curve is generically smooth.*

In addition, the family contains infinitely many non-isomorphic curves. To see this, we restrict to the one-parameter family $C_{0,1,t}$, and compute its absolute Igusa invariants as given by Sage's `absolute_igusa_invariants_kohel`. *We find that the first of these invariants is a quotient of polynomials $p(t)/q(t)$ with $\deg p = 10$ and $\deg q = 6$.*

6.3. Twisting and fourfolds over k

We begin by fixing the notation for this section. Let k be a number field, $\Delta \in k^\times$ a nonsquare, and $K = k(\sqrt{\Delta})$. Let $r, s, t \in k$ and let $C_{r,s,t}/K$ be the corresponding genus 2 curve from Theorem 6.2.1 (we assume that it is smooth). Let σ be the nontrivial automorphism of K/k.

By our construction, we know that there is a Richelot isogeny $\mathrm{Jac}(C) \to \mathrm{Jac}({}^\sigma C)$, which is defined over $K(\sqrt{-2})$. In this section we show how to twist the curve C so that the corresponding isogeny is defined over K. With this twist, the Weil restriction to k will give an abelian fourfold genuinely of GSp_4-type with building block $\mathrm{Jac}(C)$ (cf. Proposition 5.2.4).

Theorem 6.3.1. *Let $C = C_{r,s,t}$ be as above. Suppose that there is an element $\alpha \in K^\times$ such that $-2\,\mathrm{Nm}_{K/k}(\alpha)$ is a square in K. Then the jacobian of the twisted curve C_α is $(2,2)$-isogenous over K to the jacobian of ${}^\sigma C_\alpha$.*

Proof. We follow closely the proof of [**Has97**, Proposition 4.2], where a similar situation is solved for families of elliptic $\mathbb{Q}$-curves.

Recall that the equation defining the curve C has the form $y^2 = F_1(X)F_2(X)F_3(X)$, which is a quadratic splitting in the language of Section 6.1.1. We let $f(x) := F_1(X)F_2(X)F_3(X)$. For each $d \in K^\times$ there is a $(2,2)$-isogeny $\mathrm{Jac}(C) \to \mathrm{Jac}(\tilde{C}_d)$ over $K(\sqrt{d})$, where $\tilde{C}_d : dv^2 = G_1(u)G_2(u)G_3(u)$ and G_1, G_2, G_3 are obtained from F_1, F_2, F_3. By the construction leading to Theorem 6.2.1, together with its proof, we have ${}^\sigma C = \tilde{C}_{-2\cdot\frac{4}{\Delta^2}}$, and there is an isogeny

$$\varphi : \mathrm{Jac}(C) \to \mathrm{Jac}(\tilde{C}_{-2\cdot\frac{4}{\Delta^2}}) = \mathrm{Jac}({}^\sigma C) \tag{6.5}$$

which is defined over $K(\sqrt{-2})$.

Let $[a,b]$ be the divisor corresponding to a point (a,b) on $C(\bar{K})$ with $b \neq 0$. As explained in Section 6.1.1 φ is given on affine divisors by

$$\varphi([a,b]) = \sum_{i=1,2} [\left(\xi_i, \frac{\Delta}{2\sqrt{-2}} \frac{F_1(a)G_1(\xi_i)(a-\xi_i)}{b}\right)]$$

with ξ_1, ξ_2 the roots of the quadratic equation $F_1(a)G_1(X) + F_2(a)G_2(X) = 0$.

Let $\alpha \in K^\times$ be such that $-2\mathrm{Nm}_{K/k}(\alpha)$ is a square in K. Let C_α be the twist $\alpha y^2 = f(x)$ of C, and let $\tau : C_\alpha \to C$ be the $K(\sqrt{\alpha})$-isomorphism $(x,y) \mapsto (x, y/\sqrt{\alpha})$. We also denote by τ the isomorphism of jacobians $\mathrm{Jac}(C_\alpha) \to \mathrm{Jac}(C)$.

Let $\tilde{\sigma}$ be an automorphism in $\mathrm{Gal}(K(\sqrt{-2}, \sqrt{\alpha})/k)$ such that $\tilde{\sigma}|K(\sqrt{-2}) = \sigma$. The composition $\psi := {}^{\tilde{\sigma}}\tau^{-1} \circ \varphi \circ \tau$ is then a $(2,2)$-isogeny $\mathrm{Jac}(C_\alpha) \to \mathrm{Jac}({}^\sigma C_\alpha)$. Let $[a,b]$ be the divisor corresponding to an affine point (a,b) on $C_\alpha(\bar{K})$. Letting ξ_1, ξ_2 be the roots of $F_1(a)G_1(X) + F_2(a)G_2(X) = 0$, ψ is given by

$$\psi([a,b]) = \sum_{i=1,2} [\left(\alpha_i, \frac{\Delta \cdot \tilde{\sigma}(\sqrt{\alpha})\sqrt{\alpha}}{2\sqrt{-2}} \frac{F_1(a)G_1(\alpha_i)(a-\alpha_i)}{b}\right)]$$

We have $(\tilde{\sigma}(\sqrt{\alpha})\sqrt{\alpha})^2 = \mathrm{Nm}_{K/k}(\alpha)$, and so

$$\frac{\tilde{\sigma}(\sqrt{\alpha})\sqrt{\alpha}}{\sqrt{-2}} = \frac{\mathrm{Nm}_{K/k}(\alpha)}{\sqrt{-2\,\mathrm{Nm}_{K/k}(\alpha)}}.$$

By hypothesis $-2\,\mathrm{Nm}_{k/\mathbb{Q}}(\alpha)$ is a square in K, so indeed the isogeny $\psi : \mathrm{Jac}(C_\alpha) \to \mathrm{Jac}({}^\sigma C_\alpha)$ is defined over K. □

From this point on we suppose that there exists some $\alpha \in K$ is such that $-2\mathrm{Nm}_{K/k}(\alpha)$ is a square in K. We let $C = C_{r,s,t}$ and we consider the abelian surface $A = \mathrm{Jac}(C_\alpha)$. We assume that $\mathrm{End}^0(A_{\bar{K}}) = \mathbb{Q}$. We want to compute the endomorphism algebra of the Weil restriction $\mathrm{Res}_{K/k}(A)$.

We know by construction that there is an isogeny $\mu_\sigma : {}^\sigma A \to A$ (this is the dual to the isogeny ${}^{\tilde{\sigma}}\tau^{-1} \circ \varphi \circ \tau$, in the notation of the proof of Theorem 6.3.1). We also let μ_{id} be the identity isogeny $A \to A$. For each $s \in G_k$, let $\mu_s = \mu_\sigma$ if $s|K = \sigma$, and $\mu_s = \mu_{\mathrm{id}} = \mathrm{id}$ otherwise. We define the following map:

$$\begin{aligned} c : G_k \times G_k &\to \mathbb{Q}^\times \\ (s,t) &\mapsto c(s,t) = \mu_s \circ {}^s\mu_t \circ \mu_{st}^{-1}. \end{aligned}$$

As is classically known, c is a 2-cocycle of G_k with values in $\mathbb{Q}^\times$ (see e.g. Chapter 3 of [**Gui10**]).[1] We now compute this 2-cocycle. We first observe that if $s, t \in G_K$ then $c(s,t) = 1$, and similarly if $s|K = \sigma$ and $t \in G_K$ then $c(s,t) = c(t,s) = 1$.

Proposition 6.3.2. *Let α and c be as above. For every automorphism $s \in G_k$ restricting to σ on K,*

$$c(s,s) = \begin{cases} +2, & \text{if } \mathrm{Nm}_{K/k}(\alpha) \in -2\Delta(k^\times)^2, \\ -2, & \text{if } \mathrm{Nm}_{K/k}(\alpha) \in -2(k^\times)^2. \end{cases}$$

Proof. The result will follow by comparing $\hat{\mu}_\sigma$ and ${}^\sigma\mu_\sigma$. Indeed, we have

$$c(s,s) = \mu_\sigma \circ {}^\sigma\mu_\sigma \circ \mu_{\sigma^2}^{-1},$$

and since $\mu_{\sigma^2} = 1$ and A is assumed to have trivial endomorphisms, by taking degrees we will have $\mu_\sigma \circ {}^\sigma\mu_\sigma = [\pm 2] = \mu_\sigma \circ \hat{\mu}_\sigma$.

If we write $C' = (C_{r,s,t})_\alpha$, then $A = \mathrm{Jac}(C')$ is $(2,2)$-isogenous to the Jacobian of ${}^\sigma C' = \tilde{C}_{-2\,\mathrm{Nm}(\alpha)}$. Recall that the Richelot correspondence $\Gamma \subset C' \times {}^\sigma C'$ gives the form of μ_σ and its dual isogeny. The correspondence is sent via σ to ${}^\sigma\Gamma \subset {}^\sigma(C' \times {}^\sigma C') = {}^\sigma C' \times C'$, and has the explicit form

$${}^\sigma\Gamma : \begin{cases} {}^\sigma F_1(X)\,{}^\sigma G_1(U) + {}^\sigma F_2(X)\,{}^\sigma G_2(U) = 0 \\ \sigma(\sqrt{-2\,\mathrm{Nm}(\alpha)})YV = {}^\sigma F_1(X)\,{}^\sigma G_1(U)(X-U) \\ -\sigma(\sqrt{-2\,\mathrm{Nm}(\alpha)})YV = {}^\sigma F_2(X)\,{}^\sigma G_2(U)(X-U). \end{cases}$$

In what follows, we need to keep in mind that the affine points in ${}^\sigma(C' \times {}^\sigma C') = {}^\sigma C' \times C'$ have coordinates $((U,V),(X,Y))$, and we see them on $C' \times {}^\sigma C'$ through the isomorphism $((U,V),(X,Y)) \mapsto ((X,Y),(U,V))$. Recall the explicit formula for $\hat{\mu}_\sigma$: if $(u,v) \in {}^\sigma C'(\bar{K})$, the points $\{(\mu_1,\nu_1),(\mu_2,\nu_2)\} = V(\Gamma \cap (U-u, V-v))$ give the image $\hat{\mu}_\sigma(u,v) = (\mu_1,\nu_1) + (\mu_2,\nu_2)$. In particular, μ_1 and μ_2 are the roots of

$$F_1(X)G_1(u) + F_2(X)G_2(u) = 0.$$

[1] We will study this map in some generality in Chapter 7.

On the other hand, the image through ${}^\sigma\mu_\sigma$ of $u, v \in {}^\sigma C'$ is given by the points $\{(\alpha_1, \beta_1), (\alpha_2, \beta_2)\} = V({}^\sigma\Gamma \cap (X-u, Y-v))$, so that ${}^\sigma\mu_\sigma(u, v) = (\alpha_1, \beta_1)+(\alpha_2, \beta_2)$. This means that α_1 and α_2 are the roots of

$$ {}^\sigma F_1(u){}^\sigma G_1(U) + {}^\sigma F_2(u){}^\sigma G_2(U) = 0.$$

By the hypothesis defining the variety V we have

$$ {}^\sigma(F_1(X)G_1(U) + F_2(X)G_2(U)) = F_1(U)G_1(X) + F_2(U)G_2(X),$$

so $\{\alpha_1, \alpha_2\} = \{\mu_1, \mu_2\}$. Hence to decide on the sign of ${}^\sigma\mu_\sigma = \pm\hat{\mu}_\sigma$ we only need to compare the signs of $\{\beta_1, \beta_2\}$ and $\{\nu_1, \nu_2\}$. For $i = 1, 2$ we have

$$ \nu_i = \frac{F_1(\mu_i)G_1(u)(\mu_i - u)}{\sqrt{-2\,\mathrm{Nm}(\alpha)}v}, \qquad \beta_i = \frac{{}^\sigma F_1(u){}^\sigma G_1(\alpha_i)(u - \alpha_i)}{\sigma(\sqrt{-2\,\mathrm{Nm}(\alpha)})v}.$$

Since ${}^\sigma F_1(X){}^\sigma G_1(U) = F_1(U)G_1(X)$, we have $\beta_i = -\frac{F_1(\alpha_i)G_1(u)(\alpha_i - u)}{\sigma(\sqrt{-2\,\mathrm{Nm}(\alpha)})v}$ and so ${}^\sigma\mu_\sigma = \hat{\mu}_\sigma$ whenever $\sigma(\sqrt{-2\,\mathrm{Nm}(\alpha)}) = -\sqrt{-2\,\mathrm{Nm}(\alpha)}$. Likewise, we obtain ${}^\sigma\mu_\sigma = -\hat{\mu}_\sigma$ whenever $\sigma(\sqrt{-2\,\mathrm{Nm}(\alpha)}) = \sqrt{-2\,\mathrm{Nm}(\alpha)}$.

Now α has been chosen so that $-2\,\mathrm{Nm}(\alpha)$ is a square in $K^\times$. Any element in K is of the form $a + b\sqrt{\Delta}$, with $a, b \in k$, and $(a + b\sqrt{\Delta})^2 = a^2 + 2ab\sqrt{\Delta} + b^2\Delta$. Since $-2\,\mathrm{Nm}_{K/k}(\alpha)$ is in k, its square root can only be of the form $a \in k$ (with $b = 0$) or $b\sqrt{\Delta} \in k$ (with $a = 0$). The two cases in the statement follow. □

Proposition 6.3.3. *Let K/k be a quadratic extension, $C_{r,s,t}/K$ a genus 2 curve in the family of Theorem 6.2.1, and let $A = \mathrm{Jac}(C_{r,s,t})$. Suppose that $\mathrm{End}(A_{\bar{K}}) = \mathbb{Z}$. Let $\alpha \in K^\times$ be such that $-2\mathrm{Nm}_{K/k}(\alpha)$ is a square in $K^\times$. Let $A_\alpha = \mathrm{Jac}((C_{r,s,t})_\alpha)$. Then*

$$ \mathrm{End}^0(\mathrm{Res}_{K/k}(A_\alpha)) \simeq \begin{cases} \mathbb{Q}(\sqrt{+2}), & \text{if } \mathrm{Nm}_{K/k}(\alpha) \in -2\Delta(k^\times)^2, \\ \mathbb{Q}(\sqrt{-2}), & \text{if } \mathrm{Nm}_{K/k}(\alpha) \in -2(k^\times)^2. \end{cases}$$

Proof. From [**Gui10**, Proposition 5.32] we have that $\mathrm{End}^0(\mathrm{Res}_{K/k}(A_\alpha))$ is isomorphic to the twisted group algebra $\mathbb{Q}^c[\mathrm{Gal}(K/k)] = \mathbb{Q} \cdot [1] \oplus \mathbb{Q} \cdot [\sigma]$, whose product satisfies the rules

$$ [1]^2 = [1], \quad [1] \cdot [\sigma] = [\sigma] \cdot [1] = [\sigma], \quad [\sigma]^2 = c(\sigma, \sigma)[1].$$

The result follows from Proposition 6.3.2. □

6.4. Examples

We now showcase some examples of the fourfolds constructed in the previous section when $k = \mathbb{Q}$. Let $r, s, t \in \mathbb{Q}$ be such that the curve $C = C_{r,s,t}$ given in Theorem 6.2.1 is smooth and let $A = \mathrm{Jac}(C)$. As in the previous section, given $\alpha \in K^\times$ we let $A_\alpha = \mathrm{Jac}(C_\alpha)$ be the corresponding twist. We begin with the following observation.

Lemma 6.4.1. *Let $\Delta \in \mathbb{Q}_{<0}$ and let $K = \mathbb{Q}(\sqrt{\Delta})$. Suppose there exists some $\alpha \in K^\times$ such that $-2\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)$ is a square in K. If $\mathrm{End}(A_{\bar{K}}) = \mathbb{Z}$, then*

$$ \mathrm{End}^0(\mathrm{Res}_{K/\mathbb{Q}}(A_\alpha)) = \mathbb{Q}(\sqrt{2}).$$

PROOF. Let α be such that $-2\mathrm{Nm}(\alpha) \in K^{\times,2}$. As computed in the proof of Proposition 6.3.2, $\mathrm{Nm}(\alpha)$ necessarily lies in $-2\Delta(\mathbb{Q}^\times)^2$ or $-2(\mathbb{Q}^\times)^2$. Since the norm on a quadratic imaginary field is positive, we necessarily have $\mathrm{Nm}(\alpha) \in -2\Delta(\mathbb{Q}^\times)^2$. The endomorphism algebra of the Weil restriction of A_α comes from Proposition 6.3.3. □

Example 6.4.2. *For $\Delta \in \{-4, -7, -8\}$, the field $K = \mathbb{Q}(\sqrt{\Delta})$ contains elements of norm -2Δ. For an explicit example, let $\Delta = -7$ and $\mathrm{Gal}(\mathbb{Q}(\sqrt{-7})/\mathbb{Q}) = \langle\sigma\rangle$, let $(r, s, t) = (-1, 3, -3)$, and consider the genus-2 curve*

$$\begin{aligned} C = C_{-1,3,-3} : Y^2 &= F_1(X)F_2(X)F_3(X), \\ F_1(X) &= X^2 + (3\sqrt{-7} - 1)X - 3\sqrt{-7} + \frac{65}{4}, \\ F_2(X) &= \sqrt{-7}X - \frac{X}{2} + \frac{21}{2}, \\ F_3(X) &= -\sqrt{-7}X^2 + (\sqrt{-7} + 21)X - \frac{63\sqrt{-7}}{4} - 21, \end{aligned}$$

defined over $\mathbb{Q}(\sqrt{-7})$. We compute (for instance, using the criterion in [**FFG24**, §9]*, or the algorithm of* [**CMSV19**]*) that* $\mathrm{End}(\mathrm{Jac}(C)_{\bar{K}}) = \mathbb{Z}$.

The polynomials $\tilde{G}_1(X), \tilde{G}_2(X), \tilde{G}_3(X)$ are

$$\begin{aligned} \tilde{G}_1(X) &= -7X^2 + (21\sqrt{-7} + 7)X - 21\sqrt{-7} - \frac{455}{4} = -7 \cdot {}^\sigma F_1(X), \\ \tilde{G}_2(X) &= -\sqrt{-7}X + \frac{1}{2}Z + \frac{21}{2} = {}^\sigma F_2(X), \\ \tilde{G}_3(X) &= \sqrt{-7}X^2 + (-\sqrt{-7} + 21)X + \frac{63}{4}\sqrt{-7} - 21 = {}^\sigma F_3(X). \end{aligned}$$

The relations indicate that ${}^\sigma C = \tilde{C}_{-2\cdot\frac{4}{7}}$, with $\tilde{C}_{-2\cdot\frac{4}{7}} : -7y^2 = \tilde{G}_1(X)\tilde{G}_2(X)\tilde{G}_3(X)$. Moreover $\mathrm{Jac}(C)$ is $(2,2)$-isogenous over $K(\sqrt{-2})$ to $\mathrm{Jac}(\tilde{C}_{-2\cdot\frac{4}{7}})$. If we twist C by $\alpha = \frac{7-\sqrt{-7}}{2}$ (which has norm 14) we obtain an isogeny

$$\mathrm{Jac}(C_\alpha) \to \mathrm{Jac}(C_\alpha),$$

and letting $X = \mathrm{Res}_{K/\mathbb{Q}}(\mathrm{Jac}(C_\alpha))$, we must have $\mathrm{End}^0(X) = \mathbb{Q}(\sqrt{2})$. Hence X is an abelian variety genuinely of GSp_4-type *(cf. Definition 5.7.7), and it has an associated system of Galois representations*

$$\left\{\rho_{X,\lambda} : G_\mathbb{Q} \to \mathrm{GSp}_4(\mathbb{Q}(\sqrt{2})_\lambda)\right\}_{\lambda \subset \mathcal{O}_{\mathbb{Q}(\sqrt{2})}}.$$

The Nebentype of X is trivial since $H = \mathbb{Q}(\sqrt{2})$ is a totally real field, and hence if λ divides the rational prime ℓ we have $\mathrm{sim} \circ \rho_{X,\lambda} = \chi_\ell$, the ℓ-adic cyclotomic character.

We end by presenting an example over a real quadratic field.

Example 6.4.3. *We work over $K = \mathbb{Q}(\sqrt{17})$. Again using the family of Theorem 6.2.1, we let $(r, s, t) = (1, -3, 1)$, and consider the corresponding genus 2 curve*

$$C = C_{1,-3,1} : Y^2 = F_1(X)F_2(X)F_3(X).$$

Letting $A = \mathrm{Jac}(C)$, we check (by the same techniques as in the previous example) that $\mathrm{End}(A_{\bar{K}}) = \mathbb{Z}$. By twisting, we will again be able to find a fourfold over $\mathbb{Q}$ which is genuinely of GSp_4-type. The remarkable fact is that in K we have the following elements:

- $\alpha = \frac{17-5\sqrt{17}}{2}$, *with* $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) = -2 \cdot 17$.
- $\beta = -\frac{3+\sqrt{17}}{2}$, *with* $\mathrm{Nm}_{K/\mathbb{Q}}(\beta) = -2$.

In particular, if we let $X(\alpha) = \mathrm{Res}_{K/\mathbb{Q}}(A_\alpha)$ and $X(\beta) = \mathrm{Res}_{K/\mathbb{Q}}(A_\beta)$, we find that $\mathrm{End}^0(X(\alpha)) = \mathbb{Q}(\sqrt{2})$, while $\mathrm{End}^0(X(\beta)) = \mathbb{Q}(\sqrt{-2})$. Both of these abelian fourfolds are genuinely of GSp_4. In the first case, there is a Galois representation $\rho_{X(\alpha),\lambda} : G_\mathbb{Q} \to \mathrm{GSp}_4(\mathbb{Q}(\sqrt{2})_\lambda)$ for each prime λ over a rational prime ℓ, and $\mathrm{sim} \circ \rho_{X(\alpha),\lambda} = \chi_\ell$. In the second case, the representations $\rho_{X(\beta),\lambda}$ take values in $\mathrm{GSp}_4(\mathbb{Q}(\sqrt{-2}))$, and $\mathrm{sim} \circ \rho_{X(\beta),\lambda} = \eta_{K/\mathbb{Q}}\chi_\ell$, where $\eta_{K/\mathbb{Q}} : G_\mathbb{Q} \to \{\pm 1\}$ is the character that cuts the extension $K/\mathbb{Q}$.

We can see the character explicitly in the characteristic polynomials of Frobenius for the system of representations associated to $X(\beta)$. For instance, we have $\eta_{K/\mathbb{Q}}(\mathrm{Frob}_{31}) = -1$, so that there is a single prime $\mathfrak{p}$ of $\mathbb{Q}(\sqrt{-2})$ over 31. Let λ be a prime of $\mathbb{Q}(\sqrt{-2})$ coprime with 31. We compute that

$$L_\mathfrak{p}(T) = \det(\rho_{X(\beta),\lambda}(\mathrm{Frob}_\mathfrak{p}) - 1) = T^4 - 2\sqrt{-2}T^3 - 26T^2 + 62\sqrt{-2}T + 961.$$

By numerically approximating the roots of this polynomial, we find that it has roots $\pi_1 \approx -5.04 - 2.38i$, $\pi_2 \approx -4.08 + 3.79i$, and $\frac{-31}{\pi_1}$, $\frac{-31}{\pi_2}$. The negative sign is giving us the Nebentype (cf. the proof of Proposition 5.5.12).

On the other hand, the prime 43 splits in K, so that $\eta_{K/\mathbb{Q}}(\mathrm{Frob}_{43}) = 1$. For any of the two primes $\mathfrak{p} \mid 43$ in $\mathbb{Q}(\sqrt{-2})$, we have

$$L_\mathfrak{p}(T) = T^4 - 8T^3 + 62T^2 - 344T + 1849.$$

This polynomial has approximate roots $\pi_1 \approx -1.16 - 6.45i$, $\pi_2 \approx 5.16 - 4.04i$, and $\frac{43}{\pi_1}$, $\frac{43}{\pi_2}$.

CHAPTER 7

Galois representations from abelian k-varieties

In this chapter we generalize some of the results in Chapter 5 for abelian k-varieties. Most of the results have been written up in joint work with Ariel Pacetti (see [**FP24**]).

Let L/k be a Galois extension of number fields. We say an abelian variety A is a weak k-variety if it is isogenous to all of its $\mathrm{Gal}(L/k)$-Galois conjugates. This definition relaxes the classical notion of a k-variety, which we rename here to *strong k-variety*. We give the definitions and implications for the Galois representations attached to k-varieties in Section 7.1.

By a process of extension and induction, in Section 7.2 we construct representations of G_k from the compatible system of Chapter 4. In Section 7.3 we discuss some results on extension and induction of equivariant pairings for general group representations, which we apply in Section 7.4 to our Galois representations. Finally, Section 7.5 contains the following application: if $A/\mathbb{Q}$ is an abelian surface with potential quaternionic multiplication, then A is Siegel-modular. In many cases, we also show that A is paramodular.

7.1. Abelian k-varieties

Throughout this section, k is a number field and L/k is a finite Galois extension. Let A/L be an isotypical abelian variety. We say A is a *weak k-variety* if for every $s \in \mathrm{Gal}(L/k)$ there is an L-isogeny

$$\mu_s : {}^sA \to A.$$

We say A is a *strong k-variety* if, in addition, for every $s \in \mathrm{Gal}(L/k)$ and every $\varphi \in \mathrm{End}(A)$ we have the equality

$$\varphi \circ \mu_s = \mu_s \circ {}^s\varphi. \tag{7.1}$$

Since $s \in G_k$ acts on $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes \mathbb{Q}$ as ${}^s(\varphi \otimes x) := {}^s\varphi \otimes x$ for $\varphi \in \mathrm{End}(A)$, $x \in \mathbb{Q}$, we can also state (7.1) in terms of $\mathrm{End}^0(A)$. It is clear that there must exist some intermediate field $k \subseteq K \subseteq L$ such that A is a strong K-variety. The extension L/K is Galois. Our goal is to show the following result.

Proposition 7.1.1. *There exists a smallest field K with $k \subseteq K \subseteq L$ such that A is a strong K-variety. Moreover, K/k is Galois.*

Let H be the center of the simple algebra $D = \mathrm{End}^0(A)$. Suppose that we have fixed a system of isogenies $\{\mu_s : {}^sA \to A\}_{s \in \mathrm{Gal}(L/k)}$, which we inflate to a system of isogenies $\{\mu_s\}_{s \in G_k}$.

Lemma 7.1.2. *Consider the map $c : G_k \times G_k \to D^\times$ given by $c(s,t) := \mu_s \circ {}^s\mu_t \circ \mu_{st}^{-1}$. If A is a strong k-variety, then $c \in Z^2(G_k, H^\times)$, with the trivial action of G_k on $H^\times$.*

PROOF. The proof is a standard verification. We carry it out since the result is usually stated for strong k-varieties for which $\mathrm{End}(A) = \mathrm{End}(A_{\bar{k}})$ (which is not required in our definition).

Suppose that for all $\varphi \in D = \mathrm{End}^0(A)$ and all $s \in G_k$ we have ${\mu_s}^s\varphi = \varphi\mu_s$. Then for all $\varphi \in D$ we have

$$\begin{aligned} c(s,t)\varphi = \left({\mu_s}^s\mu_t\mu_{st}^{-1}\right)^{st}\varphi &= {\mu_s}^s{\mu_t}^{st}\varphi\mu_{st}^{-1} \\ &= {\mu_s}^s\varphi^s\mu_t\mu_{st}^{-1} = \varphi{\mu_s}^s\mu_t\mu_{st}^{-1} = \varphi c(s,t). \end{aligned}$$

Hence $c(s,t)$ belongs to the center H of D. Since it is defined as a composition of isogenies, we obtain $c(s,t) \in H^\times$.

The map $c : G_k \times G_k \to H^\times$ is a 2-cocycle with the trivial action of G_k on $H^\times$ if and only if for all $s,t,u \in G_k$ the equality

$$c(t,u)\cdot c(s,tu) = c(s,t)\cdot c(st,u)$$

holds. The left-hand side is the composition of isogenies $c(t,u){\mu_s}^s\mu_{tu}\mu_{stu}^{-1}$, while the right-hand side equals ${\mu_s}^s\mu_t\mu_{st}^{-1}{\mu_{st}}^{st}\mu_u\mu_{stu}^{-1}$. Hence we have equality if and only if

$$c(t,u){\mu_s}^s\mu_{tu} = {\mu_s}^s({\mu_t}^t\mu_u),$$

if and only if $c(t,u){\mu_s}^sc(t,u)^{-1} = \mu_s$. This equality holds because $c(t,u)$ belongs to H, and so $c(t,u)\mu_s = {\mu_s}^sc(t,u)$. □

For every $\varphi \in H$ and $s \in \mathrm{Gal}(L/k)$, we define an endomorphism of A by

$$s\cdot\varphi := \mu_s \circ {}^s\varphi \circ \mu_s^{-1}. \tag{7.2}$$

The following result is the content of [**Gui10**, §2.1]. We give a proof for completeness.

Proposition 7.1.3. *We have the following properties.*

1. *The endomorphism $s\cdot\varphi$ lies in H.*
2. *The value of $s\cdot\varphi$ is independent of the choice of the isogeny μ_s.*
3. *The map*

$$\mathrm{Gal}(L/k)\times H \to H, \quad (s,\varphi)\mapsto s\cdot\varphi$$

defines an action of $\mathrm{Gal}(L/k)$ on H.

PROOF. To show (1), let $\alpha \in \mathrm{End}^0(A)$ and let $\beta := \mu_s^{-1}\alpha\mu_s \in \mathrm{End}^0({}^sA)$. Then we have ${}^s({}^{s^{-1}}\beta)$, and

$$\begin{aligned} {\mu_s}^s\varphi\mu_s^{-1}\alpha = {\mu_s}^s\varphi\beta\mu_s^{-1} &= {\mu_s}^s(\varphi({}^{s^{-1}}\beta))\mu_s^{-1} \\ &= {\mu_s}^s({}^{s^{-1}}\beta\varphi)\mu_s^{-1} = \alpha{\mu_s}^s\varphi\mu_s^{-1}. \end{aligned}$$

Hence $s\cdot\varphi = {\mu_s}^s\varphi\mu_s^{-1} \in H$. For (2), suppose $\nu_s : {}^sA \to A$ is a different isogeny. Then

$$\mu_s{}^s\varphi\mu_s^{-1} = \mu_s(\mu_s^{-1}\nu_s)^s\varphi(\mu_s^{-1}\nu_s)^{-1}\mu_s^{-1}.$$

Now we conclude by the fact that ${}^s\varphi$ lies in the center of $\mathrm{End}^0({}^sA)$, and $\mu_s^{-1}\nu_s \in \mathrm{End}^0({}^sA)$.

Finally, we show (3). As in Lemma 7.1.2, for all $s,t \in \mathrm{Gal}(L/k)$ we let $c(s,t) := \mu_s \circ {}^s\mu_t \circ \mu_{st}^{-1}$. We remark that we are not asking that A is a strong k-variety, so

c is not necessarily a 2-cocycle, but it does take values in D. Let $s, t \in \mathrm{Gal}(L/k)$ and $\varphi \in H$. Then we have

$$\begin{aligned} s \cdot (t \cdot \varphi) &= \mu_s \circ {}^s(\mu_t \circ {}^t\varphi \circ \mu_t^{-1}) \circ \mu_s^{-1} = (\mu_s \circ {}^s\mu_t) \circ {}^{st}\varphi \circ (\mu_s \circ {}^s\mu_t)^{-1} \\ &= c(s,t) \circ \mu_{st} \circ {}^{st}\varphi \circ \mu_{st}^{-1} \circ c(s,t)^{-1} = \mu_{st} \circ {}^{st}\varphi \circ \mu_{st}^{-1} = (st) \cdot \varphi. \end{aligned}$$

In the second-to-last equality, we have used that $\mu_{st} \circ {}^{st}\varphi \circ \mu_{st}^{-1}$ lies in H, and so it commutes with $c(s,t) = D$. Hence we have shown that $s \cdot (t \cdot \varphi) = (st) \cdot \varphi$, and we have an action of $\mathrm{Gal}(L/k)$ on H. □

Definition 7.1.4. *We define G_0 to be the subgroup of $\mathrm{Gal}(L/k)$ acting trivially on H through (7.2). We define H_0 to be the subfield of H fixed by the action of $\mathrm{Gal}(L/k)$.*

Lemma 7.1.5. *The extension H/H_0 is Galois, the group G_0 is a normal subgroup of $\mathrm{Gal}(L/k)$, and we have an isomorphism*

$$\mathrm{Gal}(L/k)/G_0 \simeq \mathrm{Gal}(H/H_0).$$

Moreover, we have an inclusion-reversing bijection between the subgroups of $\mathrm{Gal}(L/k)$ containing G_0, and the subextensions of H/H_0.

Proof. Consider the group homomorphism $\psi : \mathrm{Gal}(L/k) \to \mathrm{Aut}(H)$ given by the action defined in (7.2). From this, we see that the extension H/H_0 is Galois since H_0 is the fixed subfield of H by the image of ψ, and the subgroup G_0 of $\mathrm{Gal}(L/k)$ is normal since it is the kernel of ψ. The remaining remarks are given by the first isomorphism theorem for groups and the Galois correspondence. □

Before proving Proposition 7.1.1, we need one more (well-known) lemma.

Lemma 7.1.6. *Let $K \subseteq L$ be a subfield. Then A is a strong K-variety if and only if $\varphi \circ \mu_s = \mu_s \circ {}^s\varphi$ for all $\varphi \in H$ and $s \in \mathrm{Gal}(L/K)$.*

Proof. If A is a strong K-variety, then the equation holds by definition for all $\varphi \in D$, and in particular for all $\varphi \in H$. Conversely, suppose that for all $s \in \mathrm{Gal}(L/K)$ and all $\varphi \in H$ we have $\varphi \circ \mu_s = \mu_s \circ {}^s\varphi$. For each $s \in \mathrm{Gal}(L/K)$, we define a $\mathbb{Q}$-algebra automorphism

$$\Psi_s : D \to D, \quad \varphi \mapsto \mu_s \circ {}^s\varphi \circ \mu_s^{-1}.$$

The hypothesis implies that Ψ_s is an H-algebra automorphism. Therefore, by Skolem–Noether (Theorem 1.1.3) there exists some $\alpha_s \in D^\times$ such that

$$\mu_s \circ {}^s\varphi \circ \mu_s^{-1} = \alpha_s^{-1} \varphi \alpha_s$$

for all $\varphi \in D$. It follows that A is a strong K-variety with respect to the system of isogenies $\{\alpha_s \mu_s\}_{s \in \mathrm{Gal}(L/K)}$. □

Proof of Proposition 7.1.1. We want to show that there is a smallest subfield K of L/k such that A is a strong K-variety, and that K/k is a Galois extension.

Let G_0 be as in Definition 7.1.4 and let $K = L^{G_0}$. Since G_0 is normal, the extension K/k is Galois. We have to check that, if $k \subseteq K' \subseteq L$ and A is a strong K'-variety, then $K \subseteq K'$. Let $s \in \mathrm{Gal}(L/K')$. Since A is a strong K'-variety, by Lemma 7.1.6 we have $s \cdot \varphi = \varphi$ for all $\varphi \in H$, and so $s \in G_0$. It follows that $K \subseteq K'$. □

Remark 7.1.7. *The field K given by Proposition 7.1.1 is sensitive to the field L over which A is defined. As an example, consider an elliptic curve $E/\mathbb{Q}$ with $\mathrm{End}^0(E_{\bar{\mathbb{Q}}}) = \mathbb{Q}(\sqrt{-1})$ (and $\mathrm{End}^0(E) = \mathbb{Q}$). If we let $k = L = \mathbb{Q}$, then we obviously have $K = \mathbb{Q}$. Hence E is both a weak and a strong $\mathbb{Q}$-variety.*

Let now $L' = \mathbb{Q}(\sqrt{-1})$, and let K' be the smallest intermediate subfield of $L'/\mathbb{Q}$ such that $E_{L'}$ is a strong K'-variety. Since $\mathrm{End}^0(E_L) = \mathrm{End}^0(E_{\bar{\mathbb{Q}}}) = \mathbb{Q}(\sqrt{-1})$, which is commutative, we have $K' = L'$, otherwise E would have all its endomorphisms defined over $\mathbb{Q}$. Hence $E_{\mathbb{Q}(\sqrt{-1})}$ is a strong $\mathbb{Q}(\sqrt{-1})$-variety, and it cannot be a strong $\mathbb{Q}$-variety.

7.2. Representations of G_k

Let L/k be a Galois extension of number fields. Let A/L be a simple weak k-variety. Let $D = \mathrm{End}^0(A)$, H the center of D, t_A the Schur index of D, and let $n = 2\dim A/t_A[H:\mathbb{Q}]$ so that A is of GL_n-type. In this section we prove the following result.

Theorem 7.2.1. *Let λ be a prime of H not in $\mathrm{Ram}(D)$ and let $\rho_{A,\lambda} : G_L \to \mathrm{GL}_n(H_\lambda)$ be the representation attached to A by Theorem 4.2.7. Let H_0 be the subfield of H fixed by the action of $\mathrm{Gal}(L/k)$ (cf. Proposition 7.1.3) and let $m = n[H:H_0]$. There exist:*

(1) A finite order character $\xi : G_L \to \bar{H}_\lambda^\times$, and
(2) An absolutely irreducible representation $R_{A,\lambda} : G_k \to \mathrm{GL}_m(\bar{H}_\lambda)$,

such that $R_{A,\lambda}|G_L$ admits $\rho_{A,\lambda} \otimes \xi$ as an irreducible constituent. If moreover A is genuinely of GL_n-type and geometrically of the first kind, then there is a strictly compatible system of representations $\{R'_{A,\lambda} : G_k \to \mathrm{GL}_m(\bar{H}_\lambda)\}_\lambda$ such that $R_{A,\lambda} = R'_{A,\lambda}$ for all but finitely many λ.

Let K be the smallest intermediate subfield in L/k such that A is a strong K-variety (cf. Proposition 7.1.1). For every $s \in \mathrm{Gal}(L/K)$, fix an isogeny $\mu_s : {}^sA \to A$ such that is a strong K-variety with respect to the set $\{\mu_s\}_{s\in\mathrm{Gal}(L/K)}$. By inflation we have an isogeny μ_s for every $s \in G_K$. Let $\{\rho_{A,\lambda}\}_\lambda$ be the H-rational strictly compatible system of representations with values in $\mathbf{GL}_{n/t_A}(D^{op})$ from Theorem 4.2.7.

For every prime $\lambda \notin \mathrm{Ram}(D)$, the representation $\rho_{A,\lambda}$ takes values in $\mathrm{GL}_n(H_\lambda)$ and is realized by an $H_\lambda[G_L]$-module $W_\lambda(A)$. Note that for every $s \in G_K$ and $t \in G_L$, ${}^s\rho_{A,\lambda}(t) := \rho_{A,\lambda}(sts^{-1})$ is the representation corresponding to $W_\lambda({}^sA)$. Using that A is a strong K-variety, we will find an isomorphism

$$ {}^s\rho_{A,\lambda} \simeq \rho_{A,\lambda}. $$

Then we will be able to extend the representation $\rho_{A,\lambda}$ to G_K up to a twist.

Let $B, B'/L$ be any two abelian varieties. Recall that Faltings' theorem gives an isomorphism $\mathrm{Hom}(B,B') \otimes \mathbb{Q}_\ell \to \mathrm{Hom}_{G_L}(V_\ell(B), V_\ell(B'))$. If $\varphi : B \to B'$ is a morphism, we denote by φ_ℓ the induced morphism of representations $V_\ell(B) \to V_\ell(B')$. For every $s \in G_K$ we let $\mu_{s,\ell} : V_\ell({}^sA) \to V_\ell(A)$ be the isomorphism of $\mathbb{Q}_\ell[G_L]$-modules induced by the isogeny $\mu_s : {}^sA \to A$.

Lemma 7.2.2. *Let ℓ be a rational prime.*

(1) For every prime $\lambda \mid \ell$ of H not in $\mathrm{Ram}(D)$ there exists an isomorphism of $H_\lambda[G_L]$-modules $\mu_{s,\lambda} : W_\lambda({}^sA) \to W_\lambda(A)$.

(2) If $\lambda \notin \mathrm{Ram}(\mathrm{End}^0(A))$ for every $\lambda \mid \ell$, then the isomorphism $\mu_{s,\ell} : V_\ell({}^sA) \to V_\ell(A)$ decomposes as $\mu_{s,\ell} = \bigoplus_{\lambda|\ell} \mu_{s,\lambda}^{\oplus t_A}$.

PROOF. Since $V_\lambda(A) = W_\lambda(A)^{\oplus t_A}$, it is enough to show the lemma for $V_\lambda(A)$. Hence we will prove that there exists some $\varphi_{s,\lambda} : V_\lambda({}^sA) \to V_\lambda(A)$ satisfying the commutative diagram in the statement, and then take $\mu_{s,\lambda}$ so that $\varphi_{s,\lambda} = \mu_{s,\lambda}^{\oplus t_A}$.

Let e_λ be the idempotent corresponding to the λ-adic factor in $H \otimes \mathbb{Q}_\ell = \prod_{\lambda|\ell} H_\lambda$. Note that there exist endomorphisms $\alpha_i \in \mathrm{End}(A)$ and constants $q_i \in \mathbb{Q}_\ell$ for $i = 1, \dots, k$ such that $e_\lambda = \sum_{i=1}^k \alpha_i \otimes q_i$. Now we define $\varphi_{s,\lambda} := \mu_{s,\ell} \circ {}^s e_\lambda$. We first show that $\varphi_{s,\lambda}$ has image in $V_\lambda(A)$. Indeed, we have ${}^s e_\lambda = \sum_i {}^s\alpha_i \otimes q_i$, and so

$$\varphi_{s,\lambda} = \mu_{s,\ell} \circ {}^s e_\lambda = \sum_i \mu_{s,\ell} \circ {}^s\alpha_i \otimes q_i = \sum_i \alpha_i \circ \mu_{s,\ell} \otimes q_i = e_\lambda \circ \mu_{s,\ell}.$$

Now (1) is a consequence of the equality $\rho_{A,\ell} \circ \mu_{s,\ell} = \mu_{s,\ell} \circ {}^s\rho_{A,\ell}$. For (2), note that if ${}^s v \in V_\ell({}^sA)$, then ${}^s v = \sum_\lambda {}^s e_\lambda {}^s v$, and so

$$\mu_{s,\ell}({}^s v) = \mu_{s,\ell}(\sum_\lambda {}^s e_\lambda {}^s v) = \sum_\lambda \mu_{s,\lambda}({}^s v).$$

□

Theorem 7.2.3. *Let L/K be a Galois extension and let A/L be a strong K-variety. There exists a finite order character $\xi : G_L \to \bar{H}^\times$ and a representation $\tilde{\rho}_{A,\lambda} : G_K \to \mathrm{GL}_n(\bar{H}_\lambda)$, such that $\tilde{\rho}_{A,\lambda}\,|_{G_L} = \rho_{A,\lambda} \otimes \xi$. Moreover, ξ is independent of λ, and the representation $\tilde{\rho}_{A,\lambda}$ is unique up to twisting by finite characters of G_K.*

PROOF. By Lemma 7.2.2 there exists an isomorphism of representations $\mu_{s,\lambda} : W_\lambda({}^sA) \to W_\lambda(A)$, so that ${}^s\rho_{A,\lambda} \simeq \rho_{A,\lambda}$ for every $s \in G_K$. Hence for every $s \in G_K$ there exists a matrix $B_s \in \mathrm{GL}_n(H_\lambda)$ such that

$$ {}^s\rho_{A,\lambda}(t) = B_s \cdot \rho_{A,\lambda}(t) \cdot B_s^{-1} \tag{7.3}$$

for all $s \in G_K$ and $t \in G_L$. By Schur's lemma, and because $\rho_{A,\lambda}$ is irreducible, each B_s is unique up to scalars. In particular, we choose $B_t = \rho_{A,\lambda}(t)$ for all $t \in G_L$. Now let $\mathbb{P}\rho_{A,\lambda} : G_L \to \mathrm{PGL}_n(H_\lambda)$ be the projective representation obtained by composing $\rho_{A,\lambda}$ with the projection $\pi : \mathrm{GL}_n(H_\lambda) \to \mathrm{PGL}_n(H_\lambda)$. We can then extend $\mathbb{P}\rho_{A,\lambda}$ to a map $\widetilde{\mathbb{P}\rho_{A,\lambda}} : G_K \to \mathrm{PGL}_n(H_\lambda)$ by setting $\widetilde{\mathbb{P}\rho_{A,\lambda}}(s) = B_s$ for every $s \in G_K$. Since the B_s are unique up to scalars, this is a well-defined map. Define $c_\lambda(s,t) := B_s \cdot B_t \cdot B_{st}^{-1}$. By the irreducibility of $\rho_{A,\lambda}$ and (7.3) we have that $c_\lambda(s,t) \in H_\lambda^\times$. It follows that $\widetilde{\mathbb{P}\rho_{A,\lambda}}$ is a homomorphism.

It is a straightforward computation to check that c_λ is a 2-cocyle in $H^2(G_K, H_\lambda^\times)$, where we consider the trivial action of G_K on $H_\lambda^\times$. The λ-adic 2-cocycle c_λ comes in fact from the global 2-cocycle $c(s,t) \in H^2(G_K, H^\times)$ introduced in Lemma 7.1.2. Indeed, the construction of the isomorphisms $\mu_{s,\lambda}$, and thus of c_λ, implies that c_λ is the image of c through the composition of the maps

$$H \to H \otimes \mathbb{Q}_\ell \overset{\text{Faltings}}{\to} \mathrm{End}_{H\otimes\mathbb{Q}_\ell[G_K]}(V_\ell(A)) \overset{\sigma_\lambda}{\to} \mathrm{End}_{H_\lambda[G_K]}(V_\lambda(A)),$$

where as usual $\sigma_\lambda : H \otimes \mathbb{Q}_\ell \to H_\lambda$ denotes the projection. Now a result of Tate (see [**Ser77**, § 6.5]) says that $H^2(G_K, \bar{H}^\times)$ is trivial. This means that there exists a locally constant function $\beta : G_K \to \bar{H}^\times$, which equals 1 on $G_{L'}$ for some finite extension L' of L, such that $c_\lambda(s,t) = \beta(s)\beta(t)\beta(st)^{-1}$. Note that β is independent

of λ, since it is a splitting of the global cocycle c. Hence we may lift $\widetilde{\mathbb{P}\rho_{A,\lambda}}$ to a representation $\tilde{\rho}_{A,\lambda} : G_K \to \mathrm{GL}_n(\bar{H}_\lambda)$ by letting $\tilde{\rho}_{A,\lambda}(s) = B_s\beta(s)^{-1}$ for all $s \in G_K$.

Since β is trivial when restricted to $G_{L'}$, we find that $\tilde{\rho}_{A,\lambda}|G_{L'} = \rho_{A,\lambda}|G_{L'}$. Hence there exists a finite order character $\xi_\lambda : G_L \to \bar{H}^\times$ such that $\tilde{\rho}_{A,\lambda}|G_L = \rho_{A,\lambda} \otimes \xi_\lambda$. But this automatically implies that $\beta|G_L = \xi_\lambda^{-1}$, and since β is independent of λ, so is $\xi = \xi_\lambda$. Finally, the uniqueness of $\tilde{\rho}_{A,\lambda}$ up to finite twists of G_K comes from Schur's lemma and the fact that the representation $\rho_{A,\lambda}$ is absolutely irreducible (cf. Theorem 4.2.7). □

Remark 7.2.4. *If L/K is a cyclic extension, then the representation $\rho_{A,\lambda}$ extends to a representation of G_K without twisting. Indeed, let s be an element in G_K generating $\mathrm{Gal}(L/K)$, and let $d = [L : K]$ so that $s^d \in G_L$. As in the proof above, there exists some $B_s \in \mathrm{GL}_n(H_\lambda)$ such that for all $t \in G_L$,*

$$\rho_{A,\lambda}(sts^{-1}) = B_s\rho_{A,\lambda}(t)B_s^{-1}.$$

On the other hand, we must have $\rho_{A,\lambda}(s^d) = \kappa B_s^d$ for some $\kappa \in H_\lambda$. Hence we may define $\tilde{\rho}_{A,\lambda}(s)$ to be $\sqrt[d]{\kappa}B_s$ (up to some dth root of unity). This definition yields an extension to G_K.

On the other hand, the twist is usually needed. An example provided by Alex Bartel is the following. If we let Q_8 be the quaternion group, then its center is $C = \{\pm 1\}$, and we may look at the nontrivial character $\rho : C \to \mathbb{C}^\times$. This character satisfies ${}^s\rho = \rho$ for all $s \in Q_8$, but it cannot extend to the full group, precisely because C is the center.

Example 7.2.5. *Let $\Delta \in \mathbb{Q}$ be squarefree and let $L = \mathbb{Q}(\sqrt{\Delta})$. In Theorem 6.2.1 we have constructed abelian surfaces A/L such that $A_{\bar{L}}$ is a $\mathbb{Q}$-surface (given that $\mathrm{End}(A_{\bar{L}}) = \mathbb{Z}$). In that construction an isogeny $A_{\bar{L}} \sim {}^sA_{\bar{L}}$ is not necessarily defined over L, but only over $L(\sqrt{-2})$. Even when no twist of A is a $\mathbb{Q}$-variety over L, it is always possible to twist the representation $\rho_{A,\ell} : G_L \to \mathrm{GSp}_4(\mathbb{Q}_\ell)$ by a character so that it extends to $G_\mathbb{Q}$, since $\rho_{A_{L(\sqrt{-2})},\ell} = \rho_{A,\ell}|G_{L(\sqrt{-2})}$ extends up to twist by Theorem 7.2.3.*

Using the fact that A is genuinely of GL_4-type, the extension has the following geometric interpretation. We know that $A_{L(\sqrt{-2})}$ is a $\mathbb{Q}$-abelian variety, and so $A_{\bar{\mathbb{Q}}}$ is a GL_4-type building block (cf. Definition 5.2.1). Hence by Proposition 5.2.4 there exists an abelian variety A_0 defined over $\mathbb{Q}$, which is genuinely of GL_4-type, and such that A is its associated building block. This implies that $A_{0,\bar{\mathbb{Q}}} \sim A_{\bar{\mathbb{Q}}}^r$ for some r. Let $M/\mathbb{Q}$ be a Galois extension with $L(\sqrt{-2}) \subset M$ over which this isogeny is defined. Let H be the center of $\mathrm{End}^0(A_{0/\mathbb{Q}})$. For each prime $\lambda \notin \mathrm{Ram}(\mathrm{End}^0(A))$, A has an associated representation $\rho_{A_0,\lambda} : G_\mathbb{Q} \to \mathrm{GSp}_4(H_\lambda)$. Let ℓ be the rational prime below λ. By Proposition 5.7.2, up to extension of scalars we have $\rho_{A_0,\lambda}|G_M \simeq \rho_{A_L,\ell} = \rho_{A,\ell}|G_M$. Hence there exists a character $\xi : G_L \to \bar{\mathbb{Q}}^\times$ factoring through $\mathrm{Gal}(M/L)$ such that $\rho_{A,\ell} \otimes \xi$ extends to $\rho_{A_0,\lambda}$. Observe that in the situation of Theorem 6.3.1 (in which $A \sim {}^sA$ over L) the abelian variety A_0 is just the fourfold given by the Weil restriction $\mathrm{Res}_{L/\mathbb{Q}}(A)$.

The same situation in the case of elliptic $\mathbb{Q}$-curves is found in [**PVT22**] *and* [**PVT23**]*, where the character ξ is computed explicitly in some cases.*

The example above generalizes in a straightforward manner assuming the hypotheses introduced in Chapter 5. In fact, since we produced an abelian variety

defined over K, the individual representations from Theorem 7.2.3 form a compatible system.

Theorem 7.2.6. *Let L/K be a Galois extension and let A/L be an abelian variety. Suppose that A is genuinely of GL_n-type and geometrically of the first kind. Suppose in addition that A is a strong K-variety.*

Then there exists an abelian variety genuinely of GL_n-type A_0/K such that if we let $D_0 = \mathrm{End}^0(A_{0,K})$, then the compatible system $\{\rho_{A_0,\lambda_0} : G_K \to \mathbf{GL}_{n/t_{A_0}}(D_0^{op})\}_{\lambda_0}$ extends $\{\rho_{A,\lambda}\}_\lambda$ up to twist in the sense of Theorem 7.2.3 for all but finitely many primes.

Proof. Let B be the building block associated to A and let F be the center of $\mathrm{End}^0(B)$. Let L'/K be a Galois extension containing L such that the building block B is defined over L' and $A_{L'} \sim B^r$ over L'. Let $\mathfrak{l}$ be a prime of F not in $\mathrm{Ram}(\mathrm{End}^0(B))$ and let λ be a prime of H over $\mathfrak{l}$. Let $\rho_{B,\mathfrak{l}} : G_{L'} \to \mathrm{GL}_n(F_\mathfrak{l})$ be the $\mathfrak{l}$-adic representation associated to B, and let $W_\lambda(A)$ and $W_\mathfrak{l}(B)$ be the respective $H_\lambda[G_L]$ and $F_\mathfrak{l}[G_{L'}]$-modules.

Since $F \subseteq H$ (cf. Lemma 5.2.2), the fact that A is a strong K-variety implies B is also a strong K-variety by Lemma 7.1.6. Hence by Proposition 5.2.4 there exists an abelian variety A_0/K which is genuinely of GL_n-type and whose associated building block is B. By enlarging L', we may assume that B is defined over L' and that we have an L'-isogeny $A_{0,L'} \sim B^r$. We let H_0 be the center of $D_0 = \mathrm{End}^0(A_0)$ and λ_0 be a prime of H_0 over $\mathfrak{l}$. Then we have an $H_{0,\lambda_0}[G_K]$-module $W_{\lambda_0}(A_0)$, and a corresponding representation $\rho_{A_0,\lambda_0} : G_K \to \mathrm{GL}_n(\bar{H}_{0,\lambda_0})$. We claim that the set $\{\rho_{A_0,\lambda_0}\}_{\lambda_0}$ is the compatible system we want, after performing the necessary book-keeping to have one representation for every prime λ of H.

Let us show that ρ_{A_0,λ_0} satisfies the extension property we need with respect to $\rho_{A,\lambda}$. By Propositions 5.5.6 and 5.7.2, we have an isomorphism of $H_\lambda[G_{L'}]$-modules

$$W_\lambda(A) \simeq W_\mathfrak{l}(B) \otimes_{F_\mathfrak{l}} H_\lambda,$$

and a corresponding isomorphism of $H_{0,\lambda_0}[G_{L'}]$-modules

$$W_{\lambda_0}(A_0) \simeq W_\mathfrak{l}(B) \otimes_{F_\mathfrak{l}} H_{0,\lambda_0}.$$

Hence up to extension of scalars we have $\rho_{A,\lambda}|G_{L'} \simeq \rho_{A_0,\lambda_0}|G_{L'}$. On the other hand, there exists a finite order character $\xi : G_L \to \bar{\mathbb{Q}}^\times$ and a representation $\tilde{\rho}_{A,\lambda} : G_K \to \mathrm{GL}_n(\bar{H}_\lambda)$, such that $\tilde{\rho}_{A,\lambda}|G_L \simeq \rho_{A,\lambda} \otimes \xi$. By irreducibility of $\rho_{A,\lambda}|G_{L'}$, it follows that (up to extension of scalars) the representations $\tilde{\rho}_{A,\lambda}$ and ρ_{A_0,λ_0} must be twists of each other. Hence there exists a finite order character $\chi : G_K \to \bar{\mathbb{Q}}^\times$ such that $\rho_{A_0,\lambda_0}|G_L \simeq \rho_{A,\lambda} \otimes \chi$. This proves the claim.

□

Remark 7.2.7. *The theorem above may be extended to abelian K-varieties genuinely of GL_n-type and geometrically of the second kind, as long as one can construct the variety A_0/K in such a way that the center of $\mathrm{End}^0(A_0)$ is Galois over the center of the algebra of the building block B (cf. Remarks 5.5.7 and 5.7.3).*

More generally, we expect the representations of Theorem 7.2.3 to form a compatible system without the assumption that A is genuinely of GL_n-type. This should follow by considering the endomorphisms of the restriction of scalars to K of $A_{L'}^r$ for some finite extension L'/L and a suitable r.

We now wish to extend the representation $\tilde{\rho}_{A,\lambda}$ from Theorem 7.2.3 further, so that we obtain a representation of G_k (remember that $L \supseteq K \supseteq k$, and A is a weak k-variety). We define

$$R_{A,\lambda} := \mathrm{Ind}_{G_K}^{G_k} \tilde{\rho}_{A,\lambda}.$$

If $\tilde{W}_\lambda$ denotes the $\bar{H}_\lambda$-vector space on which G_K acts through $\tilde{\rho}_{A,\lambda}$, then the vector space associated to the representation $R_{A,\lambda}$ is

$$U_\lambda = \bigoplus_{s \in \mathrm{Gal}(K/k)} s\tilde{W}_\lambda.$$

Recall from the previous section that $\mathrm{Gal}(L/k)$ acts on the center H of $\mathrm{End}^0(A)$. Let H_0 be the subfield of H fixed by this action.

Lemma 7.2.8.

(1) The representation $R_{A,\lambda}$ has dimension $\frac{2g}{t_A[H_0:\mathbb{Q}]} = n[H : H_0]$.

(2) Assume that ${}^s\tilde{\rho}_{A,\lambda}$ is not isomorphic to $\rho_{A,\lambda}$ for any $s \in \mathrm{Gal}(K/k)$. Then the representation $R_{A,\lambda}$ is absolutely irreducible.

Proof. For (1), we have

$$\dim_{\bar{H}_\lambda} U_\lambda = \dim_{H_\lambda} W_\lambda(A)[K : k] = n[K : k] = \frac{2g}{t_A[H : \mathbb{Q}]}[H : H_0] = \frac{2g}{t_A[H_0 : \mathbb{Q}]},$$

where we are using the correspondence in Lemma 7.1.5 to deduce $[K : k] = [H : H_0]$. The absolute irreducibility of $R_{A,\lambda}$ is a consequence of Mackey's irreducibility criterion [**Bou22**, §21, exercise 8]. □

We conclude the proof of the main result of the section.

Proof of Theorem 7.2.1. We briefly recall the notation: L/k is a Galois extension, A/L a simple weak k-variety, and K/k the smallest subextension such that A is a strong K-variety. The field H is the center of $D = \mathrm{End}^0(A)$ and t_A the Schur index of D. The variety A is of GL_n-type with $n = \frac{2\dim A}{t_A[H:\mathbb{Q}]}$. For a given prime $\lambda \notin \mathrm{Ram}(D)$ of H, we construct a representation $R_{A,\lambda}$ of G_k in two steps:

(1) *Extension.* Let $\rho_{A,\lambda} : G_L \to \mathrm{GL}_n(H_\lambda)$. By Theorem 7.2.3 there exists a finite character $\xi : G_L \to \bar{H}_\lambda^\times$ and a representation $\tilde{\rho}_{A,\lambda} : G_K \to \mathrm{GL}_n(\bar{H}_\lambda)$ such that $\tilde{\rho}_{A,\lambda}|G_L \simeq \rho_{A,\lambda} \otimes \xi$. We let H_0 be the subfield of H fixed by the action of $\mathrm{Gal}(L/k)$.

(2) *Induction.* By taking a G_K-twist of $\tilde{\rho}_{A,\lambda}$, it is always possible to ensure that ${}^s\tilde{\rho}_{A,\lambda} \not\simeq \tilde{\rho}_{A,\lambda}$ for all $s \in G_k$. Hence by Lemma 7.2.8, the induction $R_{A,\lambda} := \mathrm{Ind}_{G_K}^{G_k} \tilde{\rho}_{A,\lambda}$ is absolutely irreducible, and has dimension $n[H : H_0]$.

Finally, suppose A is genuinely of GL_n-type and geometrically of the first kind. By Theorem 7.2.6 in the extension step we have a compatible system of representations $\{\tilde{\rho}_{A_0,\lambda_0} : G_K \to \mathbf{GL}_{n/t_{A_0}}(D_0^{op})\}_{\lambda_0}$. Here A_0/K is a certain abelian variety defined over K and $D_0 = \mathrm{End}^0(A_0)$, and the representation $\tilde{\rho}_{A_0,\lambda_0}$ extends $\rho_{A,\lambda}$ for all but finitely many primes (some book-keeping is required to match primes λ and λ_0). By letting H_0 be the center of D_0 and extending scalars to $\bar{H}_{0,\lambda_0}$, we obtain a system of representations with values in GL_n. Once again we may take a twist and induce to an absolutely irreducible representation. □

7.2.1. Dimension and base change. We continue with the notation in the section. Namely, L/k is a Galois extension, A/L a weak k-variety, and K is the smallest intermediate subfield such that K/k is Galois and A is a strong K-variety.

Let H be the center of $\mathrm{End}^0(A)$. For all but finitely many primes λ of A, Theorem 7.2.1 gives a representation $R_{A,\lambda}^{(L)} : G_k \to \mathrm{GL}_m(\bar{H}_\lambda)$ coming from the Tate module of A, where m is some known dimension. Let L'/k be another Galois extension such that $L \subseteq L'$. We now discuss the relation between $R_{A,\lambda}^{(L)}$ and the representation of G_k associated to $A_{L'}$ by the same result. This relation is not necessarily obvious, since by Remark 7.1.7 the subfield K' of L'/k analogous to K may be different for $A_{L'}$.

We assume that $A_{L'}$ is isotypical, so that $A_{L'} \sim B^r$ for some L'-simple variety B. We denote by H' the center of $\mathrm{End}^0(A_{L'}) = \mathrm{M}_r(\mathrm{End}^0(B))$. For a prime λ' of H', let $R_{B,\lambda}^{(L')} : G_k \to \mathrm{GL}_{m'}(\bar{H}'_{\lambda'})$ be the representation of G_k associated to B by Theorem 7.2.1. Note that B (and so A) is of $\mathrm{GL}_{n'}$-type for some $n' \leq n$, in accordance with Proposition 5.1.3. We let $R_{A,\lambda'}^{(L')} := R_{B,\lambda'}^{(L')}$.

We begin by comparing the dimensions m and m' of $R_{A,\lambda}^{(L)}$ and $R_{A,\lambda'}^{(L')}$, respectively. Recall that the group $\mathrm{Gal}(L'/k)$ acts on H', this leaves a fixed subfield $H'_0 \subseteq H'$ (cf. Proposition 7.1.3). The same group also acts on H (since $\mathrm{Gal}(L/k)$ acts on H, and any $s \in \mathrm{Gal}(L'/k)$ which fixes L also fixes H), and so we have a fixed subfield $H_0 \subseteq H$. For the next lemma, we let t_A and t_B be the respective Schur indices of $\mathrm{End}^0(A)$ and $\mathrm{End}^0(B)$, and recall that $\mathrm{End}^0(A_{L'}) \simeq \mathrm{M}_r(\mathrm{End}^0(B))$.

Lemma 7.2.9. *The field H'_0 is a subfield of H_0. Moreover, the degree $[H_0 : H'_0]$ divides the integer $\frac{rt_B}{t_A}$.*

Proof. For the inclusion of H'_0 into H_0, we have

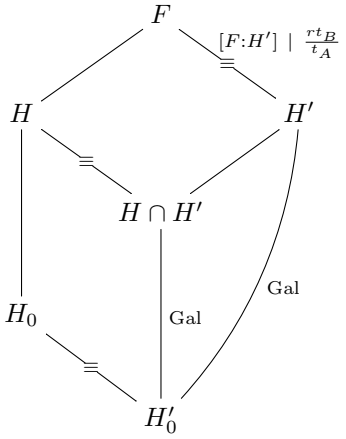
$$H'_0 = {H'}^{\mathrm{Gal}(L'/K)} = ({H'}^{\mathrm{Gal}(L'/L)})^{\mathrm{Gal}(L/K)} = (H' \cap H)^{\mathrm{Gal}(L/K)} \subseteq H^{\mathrm{Gal}(L/K)} = H_0.$$

We know from Lemma 7.1.5 that the extension H'/H'_0 is Galois. Now the base change of A to $A_{L'}$ gives us an embedding of H'_0-algebras $\mathrm{End}^0(A) \to \mathrm{M}_r(\mathrm{End}^0(B))$. By Theorem 2.4.2, there exists a possibly different primitive embedding of H'_0-algebras $\psi : \mathrm{End}^0(A) \to \mathrm{M}_r(\mathrm{End}^0(B))$. Recall that ψ being primitive means that the subalgebra of $\mathrm{M}_r(\mathrm{End}^0(B))$ generated by $\psi(H)$ and H' is a field. Denote by F this compositum of $\psi(H)$ and H'. Then Theorem 2.3.2 gives us the divisibility relation

$$t_A[F : H'] \mid rt_B.$$

Hence rt_B/t_A is an integer, and it is a multiple of $[F : H']$. The result will follow from the fact that $[F : H'] = [H_0 : H'_0]$, as we now show. Since H'/H'_0 is Galois, so is the extension $H'/H \cap H'$, and so we have the equality $[H : H \cap H'] = [F : H']$. On the other hand, we have $H'_0 = (H \cap H')^{\mathrm{Gal}(L/K)}$, so $(H \cap H')/H'_0$ is also a Galois

extension. Hence $[H_0 : H_0'] = [H : H \cap H'] = [F : H']$, as claimed.



□

As a consequence of the above result, we can compare the dimensions of $R_{A,\lambda}^{(L)}$ and $R_{A,\lambda'}^{(L')}$.

Corollary 7.2.10. *The dimension of $R_{A,\lambda'}^{(L')}$ divides the dimension of $R_{A,\lambda}^{(L)}$. Moreover, the dimensions are equal if and only if $[H_0 : H_0'] = rt_B/t_A$, and in particular if A remains of GL_n-type upon base change to L'.*

Proof. We have

$$\dim R_{A,\lambda}^{(L)} = \frac{2g}{t_A[H_0 : \mathbb{Q}]} = \frac{2g}{rt_B[H_0 : \mathbb{Q}]} \cdot \frac{rt_B}{t_A} = \frac{2g}{rt_B[H_0' : \mathbb{Q}]} \cdot \frac{1}{[H_0 : H_0']} \cdot \frac{rt_B}{t_A}.$$

By Lemma 7.2.9, $[H_0 : H_0']$ divides rt_B/t_A. On the other hand we have $\dim B = \dim A/r = g/r$, and by Lemma 7.2.8 we have $\dim R_{B,\lambda'}^{(L')} = \frac{2g}{rt_B[H_0' : \mathbb{Q}]}$. The statement holds since we have defined $R_{A,\lambda'}^{(L')}$ to be $R_{B,\lambda'}^{(L')}$. Finally, if A and B are of GL_n-type (and not of GL_m-type for $m < n$), then $t_A = rt_B$, so that $rt_B/t_A = 1$ and $[H_0 : H_0'] = rt_B/t_A$. Hence the dimensions are equal if $A_{L'}$ remains of GL_n-type. □

We end the section by showing that the representations $R_{A,\lambda}^{(L)}$ and $R_{A,\lambda'}^{(L')}$ are isomorphic up to twist when A is genuinely of GL_n-type and geometrically of the first kind. In Section 7.5 below, we will determine the precise relation between the representations $R_{A,\lambda}^{(L)}$ and $R_{A,\lambda'}^{(L')}$ when A is not genuinely of GL_n-type in a very particular case.

Proposition 7.2.11. *With the notation above, suppose that A is genuinely of GL_n-type. Then $H' \subseteq H$ and $m = m'$. If in addition A is geometrically of the first kind, then given a prime λ of H dividing a prime λ' of H', the representations $R_{A,\lambda}^{(L)}$ and $R_{A,\lambda'}^{(L')}$ are isomorphic up to a twist.*

Proof. The inclusion $H' \subseteq H$ is proven as in the beginning of Section 5.5. Since A is genuinely of GL_n-type, it is of GL_n-type both over L and L', and so if we let $A_{L'} \sim B^r$ with B simple and t_A, t_B the Schur indices of $\mathrm{End}^0(A)$ and

$\mathrm{End}^0(B)$, we have $rt_B = t_A$ (cf. the proof of Proposition 5.1.9). The equality of dimensions $m = m'$ then follows from Corollary 7.2.10. Finally, the isomorphism of the representations up to twist follows from Theorem 7.2.6 and the fact that A and B that they are both constructed from the same building block The inclusion $H' \subseteq H$ is proven as in the beginning of Section 5.5. Since A is genuinely of GL_n-type, it is of GL_n-type both over L and L', and so if we let $A_{L'} \sim B^r$ with B simple and t_A, t_B the Schur indices of $\mathrm{End}^0(A)$ and $\mathrm{End}^0(B)$, we have $rt_B = t_A$ (cf. the proof of Proposition 5.1.9). The equality of dimensions $m = m'$ then follows from Corollary 7.2.10. Finally, the isomorphism of the representations up to twist follows from Theorem 7.2.6 and the fact that A and B have the same associated building block. □

7.3. Pairings and representations

In this section we consider some results on equivariant pairings for arbitrary group representations. We will later apply these to the representations $R_{A,\lambda}$ constructed in the previous section. We begin with a variation on a classical result.

Lemma 7.3.1 (Schur's lemma)**.** *Let $\rho : G \to \mathrm{GL}_n(E)$ be an irreducible representation. Let $\chi : G \to E^\times$ be a character and let $^\dagger : \mathrm{GL}_n(E) \to \mathrm{GL}_n(E)$ be any map. Suppose that there exist two matrices $M, M' \in \mathrm{GL}_n(E)$ such that*

$$\begin{cases} M\rho(g) &= \chi(g)\rho(g)^\dagger M, \\ M'\rho(g) &= \chi(g)\rho(g)^\dagger M' \end{cases}$$

for every $g \in G$. Then, there exists some $\lambda \in E^\times$ such that $M = \lambda M'$.

Proof. Consider the characteristic polynomial $p(x) = \det(M - xM')$. This polynomial is nonzero, and in fact has leading coefficient $(-1)^n \det M'$ and degree-0 coefficient $\det M$. Let $\lambda \in \bar{E}^\times$ be a root of $p(x)$ and consider a nonzero vector $v \in \ker(M - \lambda M')$. For every $g \in G$ we then have

$$(M - \lambda M')\rho(g)v = \chi(g)\rho(g)^\dagger(M - \lambda M')v = 0.$$

Therefore $\ker(M - \lambda M')$ is a nonzero G-invariant subspace of V. Since G is irreducible, we obtain the equality $M = \lambda M'$. In turn, this implies that $\lambda \in E^\times$, and the lemma follows. □

Remark 7.3.2. *The usual* Schur's lemma *is a particular case of Lemma 7.3.1, once we let χ be the trivial character, $X^\dagger = X$ and $M' = \mathrm{Id}$.*

We apply the previous result to show that there is essentially a unique G-equivariant pairing on V of a given kind and with a given similitude character.

Corollary 7.3.3. *Let $\rho : G \to \mathrm{GL}(V)$ be an irreducible representation. Let $\chi : G \to E^\times$ be a character, and let ψ and ϕ be two pairings on V of the same kind (i.e. both alternating, symmetric or hermitian). If both ψ and ϕ are G-equivariant with similitude character χ, then there exists a constant $\lambda \in E^\times$ with $\psi = \lambda\phi$.*

Proof. We set $\rho(g)^\dagger = \rho(g)^\top$ if ψ, ϕ are alternating or bilinear, and $\rho(g)^\dagger = \overline{\rho(g)}^\top$ if they are hermitian. Moreover, we set M, M' to be the respective matrices giving the pairings on a basis of V. Then we get the result as a consequence of Lemma 7.3.1. □

A second important application is the following extension result.

Corollary 7.3.4. *Let $\rho : G \to \mathrm{GL}(V)$ be a representation and let H be a normal irreducible subgroup of G. Let $\chi : H \to E^\times$ be a character and suppose that $\psi : V \times V \to E^\times$ is a non-degenerate H-equivariant pairing with similitude character χ. The following are equivalent.*

1. *The pairing ψ is G-equivariant for some similitude character $\tilde{\chi} : G \to E^\times$.*
2. *There exists a character $\chi' : G \to E^\times$ extending χ.*
3. *For all $s \in G$, the character χ satisfies ${}^s\chi = \chi$.*

Proof. The implications (1) $\implies$ (2) $\implies$ (3) are immediate. To see (3) $\implies$ (1), suppose that ${}^s\chi = \chi$ for all $s \in H$. After fixing a basis of V, we replace the group G by its image through ρ in $\mathrm{GL}_n(E)$. Let $M \in \mathrm{GL}_n(E)$ be a matrix representing the pairing ψ. Then for every $h \in H$ we have

$$h^\dagger M h = \chi(h) M$$

with either $h^\dagger = h^\top$ or $h^\dagger = \bar{h}^\top$. Moreover, for every $g \in G$ and $h \in H$ we have

$$(ghg^{-1})^\dagger M (ghg^{-1}) = \chi(ghg^{-1})M = {}^g\chi(h)M = \chi(h)M.$$

By manipulation, we obtain $h^\dagger (g^\dagger M g) h = \chi(h) g^\dagger M g$. By Lemma 7.3.1 applied to M and $M' = g^\dagger M g$, there exists some $\tilde{\chi} = \tilde{\chi}(g) \in E^\times$ such that $g^\dagger M g = \tilde{\chi}(g) M$. This defines a map $\tilde{\chi} : G \to E^\times$ which coincides with χ on H, and it is directly checked to be a character. Therefore ψ is G-equivariant with similitude character $\tilde{\chi}$. □

The remaining step in the section is to characterize when we can endow an induced representation with a pairing.

Proposition 7.3.5. *Let G be a group, let H be a normal subgroup of G of finite index, and let $\rho : H \to \mathrm{GL}(V)$ be an irreducible representation. Consider the induced representation $\mathrm{Ind}_H^G \rho$, given by the action of G on the vector space*

$$U = \bigoplus_{[g] \in G/H} gV.$$

Suppose $\psi : V \times V \to E^\times$ is a nondegenerate H-equivariant pairing with similitude character χ. The following are equivalent.

1. *There is a nondegenerate G-equivariant pairing $\Psi : U \times U \to E^\times$ whose restriction to V is ψ.*
2. *The character χ extends to a character of G.*

Proof. Let $\Psi : U \times U \to E$ be a G-equivariant pairing with similitude character $\chi' : G \to E^\times$ and suppose that $\Psi | V \times V = \psi$. Then $\chi' | H = \chi$, and χ' is an extension of χ to G.

Conversely, let $\tilde{\chi} : G \to E^\times$ be an extension of the character χ. Let $h_1, \ldots, h_r$ be coset representatives for the quotient G/H. We define the following diagonal pairing on U:

$$\Psi(h_i u, h_j v) := \begin{cases} 0, & \text{if } i \neq j, \\ \tilde{\chi}(h_i)\psi(u,v), & \text{if } i = j. \end{cases}$$

It is clear by the definition that Ψ is nondegenerate and that it restricts to ψ on V. □

Remark 7.3.6. *Observe that we have not proved Proposition 7.3.5 above with Corollary 7.3.3, and in fact the pairing Ψ is not unique. Indeed, this is because the induced representation U is not irreducible as a representation of H. Moreover, there are as many pairings Ψ on U extending ψ as characters of G extending the similitude of ψ.*

7.4. Pairings and k-varieties

In this section we let L/k be a Galois extension and let A/L be a simple weak k-variety. Let K be the smallest subfield of L/k such that A is a strong K-variety. Let H be the center of $D = \mathrm{End}^0(A)$, and let t_A be the Schur index of D. Let $n = 2\dim A/t_A[H:\mathbb{Q}]$, so that A is of GL_n-type.

We let $\{\rho_{A,\lambda}\}_\lambda$ be the compatible system of Galois representations of G_L attached to A by Theorem 4.2.7. For each λ of H, we let $\tilde{\rho}_{A,\lambda}$ be a representation of G_K given by Theorem 7.2.3. Let $\xi : G_L \to \bar{\mathbb{Q}}^\times$ be the finite character such that $\tilde{\rho}_{A,\lambda}|G_L \simeq \rho_{A,\lambda} \otimes \xi$. Let $R_{A,\lambda}$ be the induced representation of G_k given by Theorem 7.2.1.

Proposition 7.4.1. *Suppose that A is genuinely of GL_n-type and geometrically of the first kind. Let $\varepsilon_A : G_L \to H^\times$ be the Nebentype character attached to A. Let $\lambda \notin \mathrm{Ram}(D)$ be a prime of H.*

1. *The representation $\tilde{\rho}_{A,\lambda}$ preserves a nondegenerate, G_K-equivariant, $\bar{H}_\lambda$-bilinear pairing ψ_λ with similitude character $\varepsilon_0\chi_\ell$, where $\varepsilon_0 : G_K \to \bar{\mathbb{Q}}^\times$ is a finite character such that $\varepsilon_0|G_L = \varepsilon_A\xi^2$.*
2. *The representation $R_{A,\lambda}$ preserves a pairing Ψ_λ induced from ψ_λ if and only if ε_0 extends to a character of G_k.*

In addition, if B is the building block associated to A, then the pairings are alternating if B has Albert type I or II, and symmetric if B has Albert type III.

Proof. The hypotheses that A is genuinely of GL_n-type and geometrically of the first kind allow us to apply Theorem 7.2.6 so that $\tilde{\rho}_{A,\lambda}$ is the λ_0-adic representation coming from some A_0/K which is genuinely of GL_n-type and shares the associated building block with A. Hence the character ε_0 is the Nebentype of A_0, as explained in Section 5.5. Now the representation $\rho_{A,\lambda}$ preserves a pairing ψ_λ with similitude character ε_A, and so the similitude of $\rho_{A,\lambda} \otimes \xi \simeq \rho_{A_0,\lambda_0}$ is $\varepsilon_A\xi^2$. Hence $\varepsilon_0|G_L = \varepsilon_A\xi^2$.

The statement in (2) comes directly from Proposition 7.3.5, since $\varepsilon_0\chi_\ell$ extends to a character of G_k if and only if ε_0 extends. Finally, the alternating or symmetric nature of the pairing ψ_λ (and Ψ_λ, when it exists) is determined by Theorem 5.7.4 and the irreducibility of $\rho_{A,\lambda}$. □

More generally, we know that since A is of GL_n-type, there is a set $\mathcal{L}$ of primes of H such that for all $\lambda \in \mathcal{L}$, there exists a nondegenerate, G_L-equivariant pairing $\psi_\lambda : W_\lambda(A) \times W_\lambda(A) \to H_\lambda(\chi_\ell)$. Moreover:

(a) If A has Albert type I or II, then $\mathcal{L}$ comprises all primes of H not in $\mathrm{Ram}(D)$, and ψ_λ is alternating (cf. Theorems 4.3.3 and 4.3.7).
(b) If A has Albert type III, then $\mathcal{L}$ comprises all primes of H not in $\mathrm{Ram}(D)$, and ψ_λ is symmetric (cf. Theorem 4.3.11).
(c) If A has Albert type IV, then $\mathcal{L}$ is disjoint from $\mathrm{Ram}(D)$, has positive density, and ψ_λ is hermitian (cf. Section 4.3.3).

With this notation, the most general resulting after Corollary 7.3.4 and Proposition 7.3.5 is the following.

Proposition 7.4.2. *Let $\lambda \in \mathcal{L}$.*

(1) The representation $\tilde{\rho}_{A,\lambda}$ preserves a pairing $\tilde{\psi}_\lambda$ (of the same kind as ψ_λ) if and only if ξ^2 extends to a character of G_K.
(2) Suppose that $\tilde{\rho}_{A,\lambda}$ preserves a pairing $\tilde{\psi}_\lambda$ as above with similitude character $\varepsilon : G_K \to \mathbb{Q}^\times$. Then $R_{A,\lambda}$ admits a nondegenerate, G_k-equivariant pairing Ψ_λ extending ψ_λ if and only if ε admits a further extension to G_k.

7.5. Modularity of surfaces with potential quaternionic multiplication

In this section we let $A/\mathbb{Q}$ be an abelian surface satisfying the following:

- $\mathrm{End}(A) = \mathbb{Z}$, and
- $D = \mathrm{End}^0(A_{\bar{\mathbb{Q}}})$ is either $\mathrm{M}_2(\mathbb{Q})$ or a division indefinite quaternion algebra with center $\mathbb{Q}$.

We will prove that A is Siegel-modular in Theorem 7.5.3. Under certain hypotheses, we will also show that A is paramodular in Corollary 7.5.5.

We let $L/\mathbb{Q}$ be the smallest extension such that $\mathrm{End}^0(A_L) = \mathrm{End}^0(A_{\bar{\mathbb{Q}}})$. By [**DR04**, Proposition 2.1], $L/\mathbb{Q}$ has Galois group C_n or $D_{2\cdot n}$ for $n = 2, 3, 4$, or 6.

Lemma 7.5.1. *A_L is a strong $\mathbb{Q}$-variety.*

Proof. The variety A is defined over $\mathbb{Q}$, and therefore A_L is isogenous (via the identity) to all its Galois conjugates. This makes A_L is a weak $\mathbb{Q}$-variety. Since $\mathrm{End}^0(A_L) = \mathrm{End}^0(A_{\bar{\mathbb{Q}}})$, the center of $\mathrm{End}^0(A_L)$ is $\mathbb{Q}$, and so the identity ${\mu_s}^s\varphi = \varphi\mu_s$ with $\mu_s = \mathrm{id}$ is satisfied for all $\varphi \in \mathbb{Q}$ and all $s \in G_\mathbb{Q}$. It follows from Lemma 7.1.6 that A_L is a strong $\mathbb{Q}$-variety. □

After the lemma above, we fix an isogeny $\mu_s : {}^sA \to A$ for every $s \in \mathrm{Gal}(L/\mathbb{Q})$ in such a way that A is a strong $\mathbb{Q}$-variety with respect to μ_s.

Lemma 7.5.2. *For every subfield $K \subseteq L$ with L/K cyclic, the endomorphism algebra $\mathrm{End}^0(A_K)$ contains a quadratic field. In particular, the hypothesis that $\mathrm{End}(A) = \mathbb{Z}$ implies that $L/\mathbb{Q}$ is a dihedral Galois extension. Moreover, for each such K, A_K is genuinely of GL_2-type.*

Proof. Let L/K be cyclic and let s be a generator of $\mathrm{Gal}(L/K)$. If $L = K$ then $D = \mathrm{End}^0(A_L)$ contains a quadratic subfield and there is nothing to prove. Otherwise we consider the $\mathbb{Q}$-algebra automorphism

$$\Psi_s : D \to D, \quad \varphi \mapsto {}^s\varphi.$$

By the Skolem–Noether theorem (cf. Theorem 1.1.3), there exists some $\alpha(s) \in D^\times$ such that ${}^s\varphi = \Psi_s(\varphi) = \alpha(s)\varphi\alpha(s)^{-1}$ for all $\varphi \in D$. Then $\alpha(s) \in \mathrm{End}^0(A_K)$: indeed, ${}^s\alpha(s) = \alpha(s)$. We claim that $\alpha(s) \notin \mathbb{Q}$, otherwise, for all $\varphi \in D$ we would have ${}^s\varphi = \varphi \in \mathrm{End}^0(A)$, contradicting the well-known fact that abelian surfaces over $\mathbb{Q}$ cannot have quaternionic multiplication (see for instance Proposition 5.1.7).

Hence $\mathbb{Q}(\alpha(s))$ is a (maximal) quadratic subfield of D, and is contained in $\mathrm{End}^0(A_K)$. It follows that $L/\mathbb{Q}$ cannot be cyclic, for otherwise $\mathrm{End}^0(A)$ would contain a quadratic field. That A is genuinely of GL_2-type also follows. □

Recall from Section 5.8 that an abelian variety $B/\mathbb{Q}$ is said to be Siegel-modular if there is a cuspidal automorphic representation π of $\mathrm{GSp}_4(\mathbb{A}_\mathbb{Q})$ such that $L(A,s) = L(\pi,s)$.

Theorem 7.5.3. *The abelian surface A is Siegel-modular.*

PROOF. Since A_L is a strong $\mathbb{Q}$-variety genuinely of GL_2-type and geometrically of the first kind, by Theorem 7.2.6 there exists an abelian variety A_0 defined over $\mathbb{Q}$ which is genuinely of GL_2-type whose associated building block is $A_{\bar{\mathbb{Q}}}$, and whose compatible system of representations extends that of A_L. By [**Rib04**, Theorem 4.4] and Serre's modularity conjecture [**KW09a, KW09b**], A_0 is modular.

The modularity of A follows from base change and automorphic induction, as we now explain. Let $K/\mathbb{Q}$ be a quadratic subextension of $L/\mathbb{Q}$ and let $E = \mathrm{End}^0(A_K)$ be the corresponding quadratic field of endomorphisms. Let $E_0 = \mathrm{End}^0(A_0)$ (which is a number field of degree $\dim A_0$, by e.g. Proposition 5.1.7), let ℓ be a rational prime splitting in E and at which $D = \mathrm{End}^0(A_L)$ splits, and let λ_0 be a prime of E_0 over ℓ. For some character $\xi : G_L \to \bar{\mathbb{Q}}^\times$ (as constructed in Theorem 7.2.3), we have

$$\rho_{A_0,\lambda_0}|G_L \simeq \rho_{A_L,\ell} \otimes \xi.$$

Now the representation $\rho_{A_0,\lambda_0}|G_L$ is modular by [**Lan80**], since $L/\mathbb{Q}$ is a solvable extension. Undoing the twist by ξ we obtain that $\rho_{A_L,\ell}$ is modular for some cuspidal automorphic representation π_L of $\mathrm{GL}_2(\mathbb{A}_L)$. Let λ, λ' be the primes of E over ℓ. Again by cyclic base change, the representation $\rho_{A_K,\lambda} : G_K \to \mathrm{GL}_2(E_\lambda)$ (which extends $\rho_{A_L,\ell}$) corresponds to some automorphic representation π_K of $\mathrm{GL}_2(\mathbb{A}_K)$.

Now we have an isomorphism of representations ${}^s\rho_{A_K,\lambda} \simeq \rho_{A_K,\lambda'}$ for a generator s of $\mathrm{Gal}(K/\mathbb{Q})$, since A_K is a weak $\mathbb{Q}$-variety (and it is not strong). Hence the representation $\rho_{A,\ell} : G_\mathbb{Q} \to \mathrm{GSp}_4(\mathbb{Q}_\ell)$ equals the induction $\mathrm{Ind}_K^\mathbb{Q} \rho_{A_K,\lambda}$. By automorphic induction (e.g. as in [**Hen12**, Théorème 3]) there exists an automorphic representation $\pi_\mathbb{Q}$ of $\mathrm{GL}_4(\mathbb{A}_\mathbb{Q})$ corresponding to $\rho_{A,\ell}$. It remains to show that $\pi_\mathbb{Q}$ is the transfer of an automorphic representation Π of $\mathrm{GSp}_4(\mathbb{A}_\mathbb{Q})$. This follows from the fact that $\rho_{A,\ell}$ preserves the usual Weil pairing, and so it is of *symplectic type* in the terminology of [**BCGP21**, §2.9]. The result follows from [**BCGP21**, Theorem 2.9.3]. □

Lemma 7.5.4. *Suppose $\mathrm{Gal}(L/\mathbb{Q}) \simeq D_4 \simeq C_2 \times C_2$. Then there are two quadratic subfields K, K' of L such that the endomorphism algebras $\mathrm{End}^0(A_K)$ and $\mathrm{End}^0(A_{K'})$ are real quadratic fields.*

PROOF. There are three different quadratic subfields in L. Let K_1, K_2 be two such fields. If $E_i = \mathrm{End}^0(A_{K_i})$ were an imaginary quadratic field for $i = 1$ and 2, this would contradict the fact that D is an indefinite quaternion algebra. Indeed, in the notation of Lemma 7.5.2, $E_i = \mathbb{Q}(\alpha(s_i))$, where $\mathrm{Gal}(L/K_i) = \langle s_i \rangle$, and $\alpha(s_1), \alpha(s_2)$ generate D as a $\mathbb{Q}$-algebra. But E_i being quadratic imaginary would imply D is generated by noncommuting elements a_1, a_2 with $a_i^2 < 0$, and then $D \otimes \mathbb{R}$ would be isomorphic to the Hamilton quaternions. Hence for some $i \in \{1,2\}$, E_i must be a real quadratic field. □

Recall from [**Voi21**, Chapter 21] that an order $\mathcal{O}$ in a quaternion algebra is said to be hereditary if every left ideal $I \subset \mathcal{O}$ is projective as a left $\mathcal{O}$-module.

Corollary 7.5.5. *If $\mathrm{Gal}(L/\mathbb{Q}) \simeq C_2 \times C_2$, then A is paramodular. In particular, this is the case if A is principally polarizable and $\mathrm{End}(A_{\bar{\mathbb{Q}}})$ is a hereditary order.*

PROOF. Suppose $\mathrm{Gal}(L/\mathbb{Q}) \simeq C_2 \times C_2$. In virtue of Lemma 7.5.4, we may fix a quadratic subfield K of L such that $E = \mathrm{End}^0(A_K)$ is a real quadratic field. Let λ be a prime of E and consider the representation $\rho_{A_K,\lambda} : G_K \to \mathrm{GL}_2(E_\lambda)$. Since E is real quadratic and A_K is genuinely of GL_2-type, there is a finite order character ε of G_K such that $\det \rho_{A,\lambda} = \varepsilon\chi_\ell$ (cf. Corollary 5.5.14). The character ε is actually trivial, since it is defined in terms of complex conjugation acting on E, which is a totally real field (cf. Definition 5.5.2).

Now we use a modification of the proof of Theorem 7.5.3. Recall that there exists a cuspidal automorphic representation π_K of $\mathrm{GL}_2(\mathbb{A}_K)$ corresponding to $\rho_{A_K,\lambda}$. Suppose K is real quadratic. Since $\det \rho_{A_K,\lambda} = \chi_\ell$, we may apply [**JLR12**, Main Theorem] to show that the induction of π_K to $\mathbb{Q}$ is paramodular. If K is imaginary quadratic, the analogue result is [**BDPc15**, Theorem 4.1], and again A is paramodular.

By [**DR04**, Theorem 3.4], if A admits a principal polarization and $\mathrm{End}(A_L)$ is a hereditary order then $\mathrm{Gal}(L/\mathbb{Q}) \simeq C_2 \times C_2$. Hence the result applies in this situation. □

Remark 7.5.6. *The proof we have just given does not generalize when* $\mathrm{Gal}(L/\mathbb{Q})$ *is not isomorphic to* $C_2 \times C_2$ *because the representation* $\rho_{A_K,\lambda}$ *always has determinant* $\varepsilon\chi_\ell$ *with* ε *a nontrivial character of* $\mathrm{Gal}(L/K)$*. In fact, more is true: if we let* K *be the (only) quadratic subfield of* L*, then* $\mathrm{End}^0(A_K)$ *is always imaginary quadratic (cf.* [**FKRS12**, Table 7]*). The construction of the Nebentype of* A_K *then implies* ε *is nontrivial. The theorems we use to show paramodularity don't apply in this case.*

But the situation is even worse: in many cases (such as $\mathrm{Gal}(L/\mathbb{Q}) \simeq D_{2\cdot 3}$*) the character* ε *does not extend to a character of the full Galois group of* L*, and then by Proposition 7.4.1 (applied to the weak* $\mathbb{Q}$*-variety* A_K*) the induction of* $\rho_{A_K,\lambda}$ *cannot preserve a pairing coming from the determinant form. The problem is then that we do not control the level of the induction on the automorphic side.*

Example 7.5.7. *The following abelian surface satisfies Corollary 7.5.5. We let* C *be the genus 2 curve*

$$y^2 = \left(x^2 + \frac{7}{2}\right)\left(\frac{83}{30}x^4 + 13x^3 - \frac{1519}{30}x^2 + 49x - \frac{1813}{120}\right)$$

and let $A = \mathrm{Jac}(C)$ *be its jacobian. As computed in* [**DR05**, Theorem 2.1]*, we have:*

- $\mathrm{End}(A) = \mathbb{Z}$*,*
- $\mathrm{End}^0(A_{\mathbb{Q}(\sqrt{-14})}) = \mathbb{Q}(\sqrt{2})$*,*
- $\mathrm{End}^0(A_{\mathbb{Q}(\sqrt{21})}) = \mathbb{Q}(\sqrt{3})$*,*
- $\mathrm{End}^0(A_{\mathbb{Q}(\sqrt{-6})}) = \mathbb{Q}(\sqrt{-6})$*, and*
- $\mathrm{End}^0(A_{\mathbb{Q}(\sqrt{-6},\sqrt{-14})})$ *is a maximal order in the quaternion algebra of discriminant 6.*

Hence in Corollary 7.5.5 we may take $K = \mathbb{Q}(\sqrt{-14})$ *or* $K = \mathbb{Q}(\sqrt{21})$ *to obtain a representation of* G_K *with trivial Nebentype, and then its induction to* $G_\mathbb{Q}$ *must coincide with* $\rho_{A,\ell}$*. The induced pairing coincides with the Weil pairing. It follows that* A *is paramodular.*

We remark that $\rho_{A,\ell}$ *preserves a second pairing* φ_ℓ*, given by extending the nontrivial character of* $\mathrm{Gal}(\mathbb{Q}(\sqrt{-6},\sqrt{-14})/\mathbb{Q}(\sqrt{-6}))$ *to* $G_\mathbb{Q}$ *and then applying Proposition 7.3.5. This does not contradict the uniqueness of pairings, since the Weil*

pairing and φ_ℓ have different Nebentypes. This phenomenon correlates with the fact that $\rho_{A,\ell}$ has many traces equal to zero: otherwise, we would be able to show that φ_ℓ must, in fact, have similitude character equal to χ_ℓ.

Bibliography

[Ach09] Jeffrey D. Achter. Split reductions of simple abelian varieties. *Math. Res. Lett.*, 16(2):199–213, 2009. 9

[Ach12] Jeffrey D. Achter. Explicit bounds for split reductions of simple abelian varieties. *Journal de théorie des nombres de Bordeaux*, 24(1):41–55, 2012. 9, 53

[AT23] Keisuke Arai and Yuuki Takai. An equivalent condition for abelian varieties over finite fields to have QM. *arXiv preprint arXiv:2311.11051*, 2023. 48

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939, 2001. 5

[BCGP21] George Boxer, Frank Calegari, Toby Gee, and Vincent Pilloni. Abelian surfaces over totally real fields are potentially modular. *Publ. Math. Inst. Hautes Études Sci.*, 134:153–501, 2021. 7, 8, 12, 56, 93, 121

[BCGP25] George Boxer, Frank Calegari, Toby Gee, and Vincent Pilloni. Modularity theorems for abelian surfaces. *arXiv preprint arXiv:2502.20645*, 2025. 8

[BD11] Nils Bruin and Kevin Doerksen. The arithmetic of genus two curves with $(4, 4)$-split Jacobians. *Canad. J. Math.*, 63(5):992–1024, 2011. 96

[BDPc15] Tobias Berger, Lassina Dembélé, Ariel Pacetti, and Mehmet Haluk Şengün. Theta lifts of Bianchi modular forms and applications to paramodularity. *J. Lond. Math. Soc. (2)*, 92(2):353–370, 2015. 122

[BGK06] G. Banaszak, W. Gajda, and P. Krasoń. On the image of l-adic Galois representations for abelian varieties of type I and II. *Doc. Math.*, pages 35–75, 2006. 7, 13, 63, 65

[BGK10] Grzegorz Banaszak, Wojciech Gajda, and Piotr Krasoń. On the image of Galois l-adic representations for abelian varieties of type III. *Tohoku Math. J. (2)*, 62(2):163–189, 2010. 7, 13, 63, 65

[BK14] Armand Brumer and Kenneth Kramer. Paramodular abelian varieties of odd conductor. *Trans. Amer. Math. Soc.*, 366(5):2463–2516, 2014. 6, 7, 8, 12

[BK19] Armand Brumer and Kenneth Kramer. Corrigendum to "Paramodular abelian varieties of odd conductor". *Transactions of the American Mathematical Society*, 372(3):2251–2254, 2019. 7

[BK20] Tobias Berger and Krzysztof Klosin. Deformations of Saito-Kurokawa type and the paramodular conjecture. *Amer. J. Math.*, 142(6):1821–1875, 2020. With and appendix by Chris Poor, Jerry Shurman, and David S. Yuen. 8

[BKG21] Grzegorz Banaszak and Aleksandra Kaim-Garnek. The Tate module of a simple abelian variety of type IV. *New York J. Math.*, 27:1240–1257, 2021. 7, 13, 70

[Bou98] Nicolas Bourbaki. *Algebra I. Chapters 1–3*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998. Translated from the French, Reprint of the 1989 English translation [MR0979982 (90d:00002)]. 78

[Bou22] N. Bourbaki. *Elements of Mathematics. Algebra. Chapter 8*. Springer, Cham, 2022. English translation of [3027127], Translated by Reinie Erné. 77, 114

[BPP+19] Armand Brumer, Ariel Pacetti, Cris Poor, Gonzalo Tornaría, John Voight, and David S. Yuen. On the paramodularity of typical abelian surfaces. *Algebra Number Theory*, 13(5):1145–1195, 2019. 8

[CCG20] Frank Calegari, Shiva Chidambaram, and Alexandru Ghitza. Some modular abelian surfaces. *Math. Comp.*, 89(321):387–394, 2020. 8

[CF96] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus* 2, volume 230 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1996. 96

[CFLV23] Victoria Cantoral-Farfán, Davide Lombardo, and John Voight. Monodromy groups of Jacobians with definite quaternionic multiplication. *arXiv preprint arXiv:2303.00804*, 2023. 92

[Chi87] Wên Chên Chi. Twists of central simple algebras and endomorphism algebras of some abelian varieties. *Math. Ann.*, 276(4):615–632, 1987. 21

[Chi90] Wên Chên Chi. On the l-adic representations attached to some absolutely simple abelian varieties of type II. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 37(2):467–484, 1990. 7, 63, 65, 66

[Chi91] Wên Chên Chi. On the l-adic representations attached to simple abelian varieties of type IV. *Bull. Austral. Math. Soc.*, 44(1):71–78, 1991. 13, 69, 70

[CLO15] David A. Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, Cham, fourth edition, 2015. An introduction to computational algebraic geometry and commutative algebra. 97, 98

[CMSV19] Edgar Costa, Nicolas Mascot, Jeroen Sijsling, and John Voight. Rigorous computation of the endomorphism ring of a Jacobian. *Math. Comp.*, 88(317):1303–1339, 2019. 32, 92, 105

[Del82] P. Deligne. *Hodge Cycles on Abelian Varieties*, pages 9–100. Springer Berlin Heidelberg, Berlin, Heidelberg, 1982. 13, 64

[DM02] Tobias Dern and Axel Marschner. Characters of paramodular groups and some extensions. *Comm. Algebra*, 30(9):4589–4604, 2002. 12

[DR04] Luis V. Dieulefait and Victor Rotger. The arithmetic of QM-abelian surfaces through their Galois representations. *J. Algebra*, 281(1):124–143, 2004. 120, 122

[DR05] Luis V. Dieulefait and Victor Rotger. On abelian surfaces with potential quaternionic multiplication. *Bull. Belg. Math. Soc. Simon Stevin*, 12(4):617–624, 2005. 122

[DS05] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005. 4, 5

[Fal83] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983. 61

[FFG24] Francesc Fité, Enric Florit, and Xavier Guitart. Abelian varieties genuinely of GL_n-type. *arXiv preprint arXiv:2412.21183*, 2024. 11, 13, 55, 71, 105

[FKRS12] Francesc Fité, Kiran S. Kedlaya, Víctor Rotger, and Andrew V. Sutherland. Sato-Tate distributions and Galois endomorphism modules in genus 2. *Compos. Math.*, 148(5):1390–1442, 2012. 122

[Flo25] Enric Florit. Abelian varieties that split modulo all but finitely many primes. *Proc. Amer. Math. Soc.*, 153(4):1491–1499, 2025. 13, 52

[FP24] Enric Florit and Ariel Pacetti. K-varieties and Galois representations. *arXiv preprint arXiv:2412.03184*, 2024. 12, 14, 107

[Gon98] Josep González. On the p-rank of an abelian variety and its endomorphism algebra. *Publ. Mat.*, 42(1):119–130, 1998. 40, 50, 51

[Gui10] Xavier Guitart. *Arithmetic properties of Abelian varieties under Galois conjugation*. PhD thesis, Universitat Politècnica de Catalunya (UPC), 2010. 75, 103, 104, 108

[Gui12] Xavier Guitart. Abelian varieties with many endomorphisms and their absolutely simple factors. *Rev. Mat. Iberoam.*, 28(2):591–601, 2012. 75, 76

[Has97] Yuji Hasegawa. $\mathbf{Q}$-curves over quadratic fields. *Manuscripta Math.*, 94(3):347–364, 1997. 102

[Hen12] Guy Henniart. Induction automorphe globale pour les corps de nombres. *Bull. Soc. Math. France*, 140(1):1–17, 2012. 121

[Jac96] Nathan Jacobson. *Finite-dimensional division algebras over fields*. Springer-Verlag, Berlin, 1996. 59, 60

[JLR12] Jennifer Johnson-Leung and Brooks Roberts. Siegel modular forms of degree two attached to Hilbert modular forms. *J. Number Theory*, 132(4):543–564, 2012. 122

[JLRS23] Jennifer Johnson-Leung, Brooks Roberts, and Ralf Schmidt. *Stable Klingen vectors and paramodular newforms*, volume 2342 of *Lecture Notes in Mathematics*. Springer, Cham, [2023] ©2023. 6

[Jor86] Bruce W. Jordan. Points on Shimura curves rational over number fields. *J. Reine Angew. Math.*, 371:92–114, 1986. 10

[KKW22] Arvind Kumar, Moni Kumari, and Ariel Weiss. On the Lang–Trotter conjecture for Siegel modular forms. *arXiv preprint arXiv:2201.09278*, 2022. 93

[KMRT98] Max-Albert Knus, Alexander Merkurjev, Markus Rost, and Jean-Pierre Tignol. *The book of involutions*, volume 44 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 1998. With a preface in French by J. Tits. 58

[KW09a] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture. I. *Invent. Math.*, 178(3):485–504, 2009. 4, 121

[KW09b] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture. II. *Invent. Math.*, 178(3):505–586, 2009. 4, 121

[Lan80] Robert P. Langlands. *Base change for* GL(2), volume No. 96 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ; University of Tokyo Press, Tokyo, 1980. 121

[LMF25] The LMFDB Collaboration. The L-functions and modular forms database. `https://www.lmfdb.org`, 2025. [Online; accessed 13 February 2025]. 54, 55

[Mes09] Jean-François Mestre. Couples de jacobiennes isogènes de courbes hyperelliptiques de genre arbitraire. *arXiv preprint arXiv:0902.3470*, 2009. 91

[Mil08] J.S. Milne. Abelian varieties, course notes, version 2.00, 2008. Available from the author's webpage at `https://www.jmilne.org/math/CourseNotes/AV.pdf`. 22

[Mil20] J.S. Milne. Class field theory, course notes, version 4.03, 2020. Available from the author's webpage at `https://www.jmilne.org/math/CourseNotes/CFT.pdf`. 15, 21

[MNH02] Daniel Maisner, Enric Nart, and Everett W Howe. Abelian surfaces over finite fields as Jacobians. *Experimental mathematics*, 11(3):321–337, 2002. 52

[Mor70] Yasuo Morita. Ihara's conjectures and moduli space of abelian varieties, master's thesis, 1970. 52

[MP08] V. Kumar Murty and Vijay M. Patankar. Splitting of abelian varieties. *Int. Math. Res. Not. IMRN*, (12):Art. ID rnn033, 27, 2008. 9

[Mum08] David Mumford. *Abelian varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics*. Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition. 22, 25, 41, 60

[Nek12] Jan Nekovář. Level raising and anticyclotomic Selmer groups for Hilbert modular forms of weight two. *Canad. J. Math.*, 64(3):588–668, 2012. 77

[Oht74] Masami Ohta. On l-adic representations of Galois groups obtained from certain two-dimensional abelian varieties. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 21:299–308, 1974. 13, 63

[Oor88] Frans Oort. Endomorphism algebras of abelian varieties. In Hijikata et al., editors, *Algebraic Geometry and Commutative Algebra*, pages 469–502. Academic Press, 1988. 42, 43

[Pie82] Richard S. Pierce. *Associative algebras*, volume 9 of *Studies in the History of Modern Science*. Springer-Verlag, New York-Berlin, 1982. 8, 15, 16, 17, 18, 27, 28, 59

[PVT22] Ariel Pacetti and Lucas Villagra Torcomian. $\mathbb{Q}$-Curves, Hecke characters and some Diophantine equations. *Math. Comp.*, 91(338):2817–2865, 2022. 112

[PVT23] Ariel Pacetti and Lucas Villagra Torcomian. $\mathbb{Q}$-curves, Hecke characters and some Diophantine equations II. *Publ. Mat.*, 67(2):569–599, 2023. 112

[PY15] Cris Poor and David S. Yuen. Paramodular cusp forms. *Math. Comp.*, 84(293):1401–1438, 2015. 6

[Pyl04] Elisabeth E. Pyle. Abelian varieties over $\mathbb{Q}$ with large endomorphism algebras and their simple components over $\overline{\mathbb{Q}}$. In *Modular curves and abelian varieties*, volume 224 of *Progr. Math.*, pages 189–239. Birkhäuser, Basel, 2004. 5, 10, 13, 85

[Que12] Jordi Quer. Package description and tables for the paper "Fields of definition of building blocks". *arXiv preprint arXiv:1202.3061*, 2012. 54, 55

[Rei03] I. Reiner. *Maximal orders*, volume 28 of *London Mathematical Society Monographs. New Series*. The Clarendon Press, Oxford University Press, Oxford, 2003. Corrected reprint of the 1975 original, With a foreword by M. J. Taylor. 15, 18, 21, 28, 59

[Rib76] Kenneth A. Ribet. Galois action on division points of Abelian varieties with real multiplications. *Amer. J. Math.*, 98(3):751–804, 1976. 13, 61, 71, 79

[Rib04] Kenneth A. Ribet. Abelian varieties over **Q** and modular forms. In *Modular curves and abelian varieties*, volume 224 of *Progr. Math.*, pages 241–261. Birkhäuser, Basel, 2004. 4, 5, 13, 71, 72, 76, 86, 121

[Roq05] Peter Roquette. *The Brauer-Hasse-Noether theorem in historical perspective*, volume 15 of *Schriften der Mathematisch-Naturwissenschaftlichen Klasse der Heidelberger Akademie der Wissenschaften [Publications of the Mathematics and Natural Sciences Section of Heidelberg Academy of Sciences]*. Springer-Verlag, Berlin, 2005. 18

[Sch04] I. Schur. Über die Darstellung der endlichen Gruppen durch gebrochen lineare Substitutionen. *J. Reine Angew. Math.*, 127:20–50, 1904. 77

[Ser77] J.-P. Serre. Modular forms of weight one and Galois representations. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 193–268. Academic Press, London-New York, 1977. 111

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg. 20, 21, 22

[Ser98] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*, volume 7 of *Research Notes in Mathematics*. A K Peters, Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original. 57

[Sha25] Alireza Shavali. On the image of automorphic Galois representations. *arXiv preprint arXiv:2502.10799*, 2025. 82

[Shi63] Goro Shimura. On analytic families of polarized abelian varieties and automorphic functions. *Ann. of Math. (2)*, 78:149–192, 1963. 52, 76, 91

[Shi72] Goro Shimura. Class fields over real quadratic fields and Hecke operators. *Ann. of Math. (2)*, 95:130–190, 1972. 72

[Smi05] Benjamin Smith. *Explicit endomorphisms and correspondences*. PhD thesis, University of Sydney, 2005. 96

[Tat66] John Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones mathematicae*, 2(2):134–144, 1966. 39

[The23] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.1)*, 2023. `https://www.sagemath.org`. 99

[TW95] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995. 5

[Voi21] John Voight. *Quaternion Algebras*. Graduate Texts in Mathematics. Springer International Publishing, 2021. 121

[Wat69] William C. Waterhouse. Abelian varieties over finite fields. *Annales scientifiques de l'École Normale Supérieure*, Ser. 4, 2(4):521–560, 1969. 9, 42

[Wei22] Ariel Weiss. On the images of Galois representations attached to low weight Siegel modular forms. *Journal of the London Mathematical Society*, 106(1):358–387, 2022. 12, 92

[Wil95] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995. 5

[Yos73] Hiroyuki Yoshida. On an analogue of the Sato conjecture. *Invent. Math.*, 19:261–277, 1973. 52

[Yu12] Chia-Fu Yu. Embeddings of fields into simple algebras: generalizations and applications. *J. Algebra*, 368:1–20, 2012. 9, 27, 28

[Yu13a] Chia-Fu Yu. Characteristic polynomials of central simple algebras. *Taiwanese J. Math.*, 17(1):351–359, 2013. 32

[Yu13b] Chia-Fu Yu. Endomorphism algebras of qm abelian surfaces. *Journal of Pure and Applied Algebra*, 217(5):907–914, 2013. 10, 28, 40, 43, 48, 55

[Zyw14] David Zywina. The splitting of reductions of an abelian variety. *Int. Math. Res. Not. IMRN*, (18):5042–5083, 2014. 9

Resum en català

En aquesta tesi es consideren les propietats aritmètiques de les varietats abelianes en relació amb les seves àlgebres d'endomorfismes. Més precisament, estudiem les reduccions bones d'una varietat abeliana definida sobre un cos de nombres, així com les representacions de Galois associades. També donem alguns resultats de modularitat de varietats abelianes respecte de formes modulars de Siegel.

El Capítol 1 dona algunes definicions i resultats preliminars sobre àlgebres simples i varietats abelianes. El treball pròpiament dit comença amb el Capítol 2, on estudiem les immersions[1] d'àlgebres simples. Hem fet un èmfasi especial en caracteritzar l'existència d'una immersió entre dues àlgebres simples. Donem una especialització d'un criteri de Chia-Fu Yu per a àlgebres sobre cossos globals i locals, que pren un paper important en els Capítols 3, 5 i 7.

El Capítol 3 estudia les propietats de les varietats abelianes definides sobre cossos finits sota la hipòtesi que l'àlgebra d'endomorfismes és no commutativa. Ens centrem en classificar les 4-varietats abelianes amb multiplicació quaterniònica. Demostrem el següent resultat: una varietat abeliana sobre un cos de nombres amb endomorfismes no commutatius és no simple mòdul tot primer fora d'un conjunt finit. Aquest enunciat generalitza el resultat anàleg per a les anomenades "corbes el·líptiques falses", i fa més precisa una de les direccions de la Conjectura de Murty i Patankar. D'altra banda, també donem un exemple d'una 4-varietat abeliana amb exactament dues reduccions geomètricament simples.

Al Capítol 4, comencem la descripció de les representacions de Galois associades a varietats abelianes amb algun endomorfisme no enter. Descrivim les components irreductibles del mòdul de Tate en termes de l'àlgebra d'endomorfismes, i provem que les representacions de Galois prenen valors en una forma del grup algebraic GL_n. També explicitem la natura de l'emparellament de Weil en aquestes components irreductibles, que depèn del tipus d'Albert de l'àlgebra d'endomorfismes. El Capítol 5 es basa en un treball conjunt amb F. Fité i X. Guitart. Hi definim la noció de varietat abeliana genuïnament de tipus GL_n, tot generalitzant les varietats abelianes de tipus GL_2 i sense multiplicació complexa potencial considerades per Ribet. El sistema de representacions associat a aquestes varietats té la propietat de ser absolutament irreductible al fer un canvi de base a una extensió finita. Donem una teoria de *building blocks* per a aquestes varietats. Sota certa hipòtesi tècnica, definim també els *inner twists* i el caràcter d'una varietat abeliana, anomenat Nebentipus. Caracteritzem les varietats amb representació de Galois simplèctica o ortogonal, que anomenem genuïnament de tipus GSp_n o GO_n, respectivament. D'aquesta manera, ampliem la classe de varietats abelianes amb tals representacions donada

[1] En anglès, embeddings.

anteriorment per Banaszak, Gajda i Krasoń. Finalment, demostrem que una varietat abeliana genuïnament de tipus GL_4 és modular de Siegel si i només si aquesta és genuïnament de tipus GSp_4.

Al Capítol 6 construïm una família de *building blocks* de tipus GL_4. Aquests venen donats per les Jacobianes de certes corbes de gènere 2 amb una isogènia de Richelot a les seves conjugades de Galois. Sota certes condicions, la restricció de Weil ens dona exemples de 4-varietats abelianes genuïnament de tipus GSp_4. La família inclou exemples de representacions de Galois amb imatge a GSp_4 i Nebentipus no trivial.

El Capítol 7 està basat en un treball conjunt amb A. Pacetti. S'hi tracten les representacions de Galois associades a k-varietats abelianes. Un dels punts principals és que no assumim que tots els endomorfismes de la varietat estan definits sobre el cos base. Això permet tractar varietats abelianes potencialment de tipus GL_n. Donem un procediment per a construir una representació del grup absolut de Galois de k associada a una k-varietat abeliana. A més, donem alguns resultats sobre l'aparellament de Weil induït a aquestes representacions. Com a aplicació, demostrem que les superfícies abelianes sobre $\mathbb{Q}$ amb multiplicació quaterniònica potencial són modulars de Siegel.

Paraules clau: varietats abelianes, àlgebres centrals simples, teoria d'Honda–Tate, representacions de Galois, multiplicació quaterniònica, modularitat.