Explicit surjectivity of Galois representations for abelian surfaces and GL_2-varieties

Davide Lombardo [*]

Département de Mathématiques d'Orsay

ABSTRACT

Let A be an absolutely simple abelian variety without (potential) complex multiplication, defined over the number field K. Suppose that either $\dim A = 2$ or A is of GL_2-type: we give an explicit bound $\ell_0(A, K)$ such that, for every prime $\ell > \ell_0(A, K)$, the image of $\mathrm{Gal}\left(\overline{K}/K\right)$ in $\mathrm{Aut}(T_\ell(A))$ is as large as it is allowed to be by endomorphisms and polarizations.

Keywords. Abelian varieties over number fields; abelian surfaces; GL_2-varieties; Galois representations; isogeny theorem; Mumford-Tate conjecture.

1 Introduction

The purpose of this work is the study of Galois representations attached to abelian varieties over number fields, with a particular focus on the case of abelian surfaces. Throughout the paper, the letters K and A will respectively denote a number field and an abelian variety defined over K, and the letter ℓ will be reserved for prime numbers. Along with abelian surfaces, we also consider abelian varieties of GL_2-type, which we define as follows:

Definition 1.1 *(cf. [Rib76]) An abelian variety A/K is said to be of GL_2-type if its endomorphism algebra $\mathrm{End}_{\overline{K}}(A) \otimes \mathbb{Q}$ is a totally real number field E such that $[E : \mathbb{Q}] = \dim A$.*

The representations we examine are those given by the natural action of $\mathrm{Gal}\left(\overline{K}/K\right)$ on the various Tate modules of A (denoted by $T_\ell(A)$), and the problem we study is that of describing the image G_{ℓ^∞} of $\mathrm{Gal}\left(\overline{K}/K\right)$ in $\mathrm{Aut}\left(T_\ell(A)\right)$. In a sense to be made precise shortly, we aim to show that this image is as large as it is permitted by some 'obvious' constraints, as soon as ℓ exceeds a certain bound $\ell_0(A, K)$ that we explicitly compute in terms of arithmetical invariants of K and of the semistable Faltings height of A (which we denote $h(A)$, and for which we use Faltings' original normalization: see [GR14b, §2.3]).

For the abelian varieties we consider – surfaces and GL_2-type – this fact, in its qualitative form, has been known since the work of Serre [Ser86] and Ribet [Rib76]: the novelty of the result we present here lies in its being completely explicit. Indeed, to the best of the author's knowledge, before the present work the only paper dealing with the problem of effective surjectivity results for abelian surfaces was [Kaw03], that only covered the case $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$ (and was not completely explicit). Unfortunately, the argument of [Kaw03] seems to contain a gap, for in his case analysis the author does not include the subgroup of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ arising from the unique 4-dimensional symplectic representation of SL_2 (case (2) in theorem 3.3): this is essentially the hardest case, and dealing with it requires nontrivial results of Raynaud on the structure of the action of inertia.

Before stating our main result let us elaborate a little on the 'obvious' conditions that are imposed on G_{ℓ^∞}. The choice of any K-polarization on A equips the Tate modules $T_\ell(A)$ with

---

[*]davide.lombardo@math.u-psud.fr

a bilinear form, the Weil pairing $\langle \cdot, \cdot \rangle$, compatible with the Galois action: this forces G_{ℓ^∞} to be contained in the group of similitudes with respect to the bilinear form $\langle \cdot, \cdot \rangle$. Furthermore, the action of $\mathrm{Gal}\left(\overline{K}/K\right)$ commutes with the natural action of $\mathrm{End}_K(A)$ on $T_\ell(A)$, so G_{ℓ^∞} is also contained in the centralizer of $\mathrm{End}_K(A)$ inside $\mathrm{Aut}(T_\ell(A))$.

This second condition leads naturally to classifying abelian surfaces according to the structure of $\mathrm{End}_{\overline{K}}(A)$. A study of those rings that appear as endomorphism rings of abelian surfaces (a particular case of the so-called Albert classification, cf. for example [Mum70, p. 203]) leads to the conclusion that only five cases can arise:

1. Type I, trivial endomorphisms: A is absolutely simple and $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$;

2. Type I, real multiplication: A is absolutely simple and $\mathrm{End}_{\overline{K}}(A)$ is an order in a real quadratic field (so A is in particular a GL_2-variety);

3. Type II, quaternionic multiplication: A is absolutely simple and $\mathrm{End}_{\overline{K}}(A)$ is an order in a quaternion division algebra over $\mathbb{Q}$;

4. Type IV, complex multiplication: A is absolutely simple and admits complex multiplication by a quartic CM field;

5. Non-simple case: $A_{\overline{K}}$ is isogenous to the product of two elliptic curves.

We focus here on the first three possibilities; the case of complex multiplication (in arbitrary dimension) is treated in [Lom15c], and that of a product of an arbitrary number of elliptic curves without complex multiplication is studied in [Lom15a]. It should be possible to combine these results to treat any finite product of elliptic curves (in which some factors admit CM and others do not); this would in particular cover case (5) above.

1.1 Notation and statement of the result

We are interested in the Galois representations attached to A: the natural action of $\mathrm{Gal}\left(\overline{K}/K\right)$ on the Tate modules $T_\ell(A)$ gives rise to a family of representations

$$\rho_{\ell^\infty} : \mathrm{Gal}\left(\overline{K}/K\right) \to \mathrm{GL}(T_\ell(A))$$

which will be our main object of study. We will also need to consider the residual mod-ℓ representations, which we similarly denote by $\rho_\ell : \mathrm{Gal}\left(\overline{K}/K\right) \to \mathrm{GL}(A[\ell])$; we shall write G_{ℓ^∞} (resp. G_ℓ) for the image of ρ_{ℓ^∞} (resp. ρ_ℓ). Most of our estimates will be given in terms of the following function:

Definition 1.2 Let $\alpha(g) = 2^{10} g^3$ and define $b(d, g, h) = \left((14g)^{64g^2} d \max\left(h, \log d, 1\right)^2 \right)^{\alpha(g)}$. If K is a number field and A is an abelian variety over K, we shall use the shorthand $b(A/K)$ to denote $b([K : \mathbb{Q}], \dim A, h(A))$.

We are now ready to state our main results.

Theorem 1.3 Let A/K be an abelian surface with $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$. The equality $G_{\ell^\infty} = \mathrm{GSp}_4(\mathbb{Z}_\ell)$ holds for every prime ℓ that satisfies the following three conditions:

- $\ell > b(2[K : \mathbb{Q}], 4, 2h(A))^{1/4}$;

- there exists a place of K of characteristic ℓ at which A has semistable reduction;

- ℓ is unramified in K.

For the case of real multiplication we treat the more general situation of abelian varieties of GL_2-type:

Theorem 1.4 *Let A/K be an abelian variety of dimension g. Suppose that $\operatorname{End}_{\overline{K}}(A)$ is an order in a totally real field E of degree g over $\mathbb{Q}$ (that is, A is of GL_2-type), and that all the endomorphisms of A are defined over K. Let ℓ be a prime unramified both in K and in E and strictly larger than $\max\left\{b(A/K)^g,\ b(2[K:\mathbb{Q}], 2\dim(A), 2h(A))^{1/2}\right\}$: then we have*

$$G_{\ell^\infty} = \left\{x \in \operatorname{GL}_2\left(\mathcal{O}_E \otimes \mathbb{Z}_\ell\right) \mid \det_{\mathcal{O}_E} x \in \mathbb{Z}_\ell^\times \right\}.$$

The case of abelian surfaces with real multiplication then follows as an immediate consequence:

Corollary 1.5 *Let A/K be an abelian surface. Suppose that $R = \operatorname{End}_{\overline{K}}(A)$ is an order in a real quadratic field E and that all the endomorphisms of A are defined over K. Let ℓ be a prime unramified both in K and in E and strictly larger than $b(2[K:\mathbb{Q}], 4, 2h(A))^{1/2}$: then we have*

$$G_{\ell^\infty} = \left\{x \in \operatorname{GL}_2\left(\mathcal{O}_E \otimes \mathbb{Z}_\ell\right) \mid \det_{\mathcal{O}_E} x \in \mathbb{Z}_\ell^\times \right\}.$$

Remark 1.6 When A is a surface, the group $H_{\ell^\infty} := \left\{x \in \operatorname{GL}_2\left(\mathcal{O}_E \otimes \mathbb{Z}_\ell\right) \mid \det_{\mathcal{O}_E} x \in \mathbb{Z}_\ell^\times\right\}$ appearing in this statement admits the following concrete description. When ℓ is split in E, the ring $\mathcal{O}_E \otimes \mathbb{Z}_\ell$ is isomorphic to $\mathbb{Z}_\ell \oplus \mathbb{Z}_\ell$, and we have $H_{\ell^\infty} = \left\{(h_1, h_2) \in \operatorname{GL}_2(\mathbb{Z}_\ell)^2 \mid \det h_1 = \det h_2\right\}$. If, on the other hand, ℓ is inert in E, then $\mathcal{O}_E \otimes \mathbb{Z}_\ell$ is a domain that contains a canonical copy of $\mathbb{Z}_\ell$ (namely $\mathbb{Z} \otimes \mathbb{Z}_\ell$), and we have $H_{\ell^\infty} = \left\{x \in \operatorname{GL}_2(\mathcal{O}_E \otimes \mathbb{Z}_\ell) \mid \det x \in \mathbb{Z}_\ell^\times\right\}$, where now det is the usual determinant (since $\mathcal{O}_E \otimes \mathbb{Z}_\ell$ is a domain). More generally, if A is of dimension g and ℓ is unramified in E, then

$$H_{\ell^\infty} = \left\{(x_\lambda) \in \prod_{\lambda \mid \ell} \operatorname{GL}_2(\mathcal{O}_\lambda) \mid \det x_{\lambda_1} = \det x_{\lambda_2} \in \mathbb{Z}_\ell^\times \quad \forall \lambda_1, \lambda_2 \mid \ell\right\},$$

where the product is over the places of E dividing ℓ.

Finally, we come to the case of quaternionic multiplication:

Theorem 1.7 *Let A/K be an abelian surface such that $R = \operatorname{End}_{\overline{K}}(A)$ is an order in an indefinite quaternion division algebra over $\mathbb{Q}$, and let Δ be the discriminant of R. Suppose that all the endomorphisms of A are defined over K. If ℓ is larger than $b(2[K:\mathbb{Q}], 4, 2h(A))^{1/2}$, does not divide Δ, and is unramified in K, then the equality $G_{\ell^\infty} = (R \otimes \mathbb{Z}_\ell)^\times$ holds.*

Remark 1.8 In the case of real and quaternionic multiplication we have assumed that the endomorphisms of A are defined over K, but this is not a severe restriction, since we may reduce to this case at the expenses of a controlled extension of the base field K. More precisely, it is known that there exists a minimal (and automatically normal) extension K' of K such that $\operatorname{End}_{K'}(A) = \operatorname{End}_{\overline{K}}(A)$ (see [Sil92, Proposition 2.2] and its proof), and the degree $[K':K]$ can be bounded purely in terms of the dimension of A. Moreover, K'/K is unramified away from the places of K at which A has bad, non-semistable reduction ([Sil92, p. 262]); this enables us to also control the discriminant of K'. In particular, when A is a surface, it is known that K'/K can be taken to be of degree at most 2 for the case of real multiplication ([Sil92, Proposition 4.3]), and at most 12 for the quaternionic case ([DR04, Prop. 2.1]); more complicated (but still explicit) bounds on the degree K'/K are also available in case A is of GL_2-type, cf. again [Sil92]. One can then apply our methods to A/K' to obtain a description of $\rho_{\ell^\infty}\left(\operatorname{Gal}\left(\overline{K'}/K'\right)\right)$ for all sufficiently large ℓ, and deduce a description of $\rho_{\ell^\infty}\left(\operatorname{Gal}\left(\overline{K}/K\right)\right)$ as an extension of $\operatorname{Gal}\left(K'/K\right)$ by $\rho_{\ell^\infty}\left(\operatorname{Gal}\left(\overline{K'}/K'\right)\right)$ (for all ℓ larger than some explicit bound).

Before proceeding with the proof of the three main statements a few more comments are in order. Consider the hypothesis that there is a place of K of characteristic ℓ at which A has semistable reduction (this assumption appears in the statement of theorem 1.3). Without any assumption on A, this condition cannot be turned into an inequality only involving $h(A)$: indeed, the set of primes of unstable reduction of A/K is certainly not invariant under extensions of scalars,

so it cannot be controlled just in terms of the *stable* Faltings height; this is really an arithmetical condition that is hard to avoid. On the plus side, the primes which fail to meet this restriction are often easy to determine in practice, especially when A is explicitly given as the Jacobian of a genus 2 curve.

Also note that in many intermediate lemmas we give estimates in terms of the best possible isogeny bound (cf. section 2.2), thus avoiding to use the specific form of the function $b(A/K)$. However, in order to make the final results more readable, we have chosen to express them in a form that only involves the function b; this also has the merit of giving completely explicit bounds.

Let us also briefly review previous work in the area. As already mentioned, Serre [Ser86] proved that for a large class of abelian varieties (that includes surfaces with $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$) there exists a number $\ell_1(A, K)$ such that $G_{\ell^\infty} = \mathrm{GSp}_{2\dim A}(\mathbb{Z}_\ell)$ for every ℓ larger than $\ell_1(A, K)$; his result, however, is not effective, in the sense that the proof does not give any bound on $\ell_1(A, K)$. Similarly, Ribet proved in [Rib76] an open image result for abelian varieties of GL_2-type that includes surfaces with real multiplication as a particular case, but that is again non-effective. The case of surfaces with quaternionic multiplication was treated independently in [Oht74] and in [Jac74] by extending the techniques Serre used to prove his celebrated open image theorem for elliptic curves in [Ser72], but once again these results were not effective. Furthermore, many other big monodromy results have been proven for classes of abelian varieties that satisfy various combinations of hypotheses on their dimension, endomorphism algebra, and reduction type at places of K, see for example the work of Pink [Pin98], Chi [Chi92], and Hall [Hal11]. All these results are non-effective as stated (even though [Zyw15] makes Hall's criterion effective in some cases).

In a slightly different direction, Dieulefait [Die02] considers abelian surfaces $A/\mathbb{Q}$ that satisfy $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$, and gives sufficient conditions for the equality $G_{\ell^\infty} = \mathrm{GSp}_4(\mathbb{Z}_\ell)$ to hold for a fixed prime ℓ; the form of these conditions, however, is again such that they do not yield a bound for the largest prime for which the equality $G_\ell = \mathrm{GSp}_4(\mathbb{Z}_\ell)$ fails to hold. Nonetheless, the treatment we give of case 2 of theorem 3.3 has been inspired by Dieulefait's paper. Finally, [Die02, Theorem 5.8] gives an explicit example of a 2-dimensional Jacobian over $\mathbb{Q}$ for which the equality $G_{\ell^\infty} = \mathrm{GSp}_4(\mathbb{Z}_\ell)$ holds for every prime $\ell \geq 3$ (the result was conditional on Serre's modularity conjecture, which has subsequently been proved by Khare and Wintenberger, cf. [KW09a] and [KW09b]). An analogous example, for which the equality $G_{\ell^\infty} = \mathrm{GSp}_4(\mathbb{Z}_\ell)$ holds for all primes ℓ, is given in [JR10, Proposition 6.5]. Notice however that even in this last example the *adelic* representation $\prod_\ell \rho_{\ell^\infty} : \mathrm{Gal}\left(\overline{K}/K\right) \to \prod_\ell \mathrm{GSp}_4(\mathbb{Z}_\ell) = \mathrm{GSp}_4(\hat{\mathbb{Z}})$ is not surjective: indeed there exists no principally polarized abelian surface over $\mathbb{Q}$ with surjective adelic representation, cf. [Zyw15, Proposition 2.5].

It is tempting to conjecture that bounds $\ell_0(A, K)$ as above can be taken to be independent of A (albeit obviously not of K), but very little is known in this direction: the analogous question for elliptic curves, often called "Serre's uniformity problem", is still open even for $K = \mathbb{Q}$. We do know, however, that such bounds must necessarily depend on the dimension of A: for example, Theorem 1.4 of [GP12] shows that for infinitely many primes p there exists a $\mathbb{Q}$-abelian variety A_p of GL_2-type and of dimension at most $\frac{(p-5)(p-7)}{24}$ such that the associated modulo-p representation ρ_p is not surjective; in particular, a uniform bound for $\ell_0(A, \mathbb{Q})$, if it exists, must grow at least as fast as $\sqrt{\dim A}$.

To conclude this introduction let us give a brief overview of the organisation of the paper and of the proof methods. Theorems 1.3, 1.4, and 1.7 will be shown in sections 3, 4, and 5 respectively.

The main input for the proof in the case of trivial endomorphism ring comes from group theory, complemented by an application of some nontrivial results of Raynaud. After reducing the problem to that of showing the equality $G_\ell = \mathrm{GSp}_4(\mathbb{F}_\ell)$ for ℓ large enough, we recall the classification of the maximal proper subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ and proceed to show that each of them cannot occur as the image of the Galois representation on $A[\ell]$, at least for ℓ large enough. In most cases, this follows from the so-called isogeny theorem of Masser and Wüstholz [MW93c] [MW93b] (theorem 2.2 below): in many circumstances, if G_ℓ is not maximal, then the Galois module $A[\ell]$ (or $A[\ell] \times A[\ell]$)

is nonsimple, a fact that gives rise to minimal isogenies of high degree, eventually contradicting the isogeny theorem for ℓ large enough. In some exceptional cases, however, the representations $A[\ell]$ and $A[\ell] \times A[\ell]$ can be irreducible even if G_ℓ is comparatively very small, and it is to exclude this possibility that we need to invoke Raynaud's results. These same results of Raynaud also lead to the following lower bound on the order of $\mathbb{P}G_\ell$ (the projective image of G_ℓ), which might have some independent interest:

Proposition 1.9 *(Proposition 3.15) Let A/K be any abelian variety of dimension g. Let ℓ be a prime such that there is a place of K of residual characteristic ℓ at which A has either good or bad semistable reduction. If ℓ is unramified in K and not less than $g + 2$, then $|\mathbb{P}G_\ell| \geq \ell - 1$.*

For the case of real multiplication our method is quite different from that of [Rib76]: by appealing to group theory more than it is done in [Rib76], we can completely avoid the use of Chebotarev's theorem, which would be the main obstacle in making Ribet's method effective. We show again that if G_ℓ is smaller than it could conceivably be (given the restrictions imposed by the Weil pairing and by the action of $\mathrm{End}_{\overline{K}}(A)$), then A admits minimal isogenies of high degree: combined with the isogeny theorem, this gives the desired result.

As for the case of quaternionic multiplication, there is a general philosophy suggesting that – at the level of Galois representations – an abelian variety of dimension $2g$ with quaternionic multiplication by an algebra with center L should behave as an abelian variety of dimension g admitting multiplication by L, and indeed the case of section 5 turns out to be the easiest, the argument being very similar to that for elliptic curves without complex multiplication. More precisely, the Tate module decomposes as two copies of a 2-dimensional Galois representation, and we can apply techniques that are an essentially straightforward generalisation of those employed to show analogous results for elliptic curves, and that go back to Serre [Ser72] (cf. also [MW93a]).

Finally, in appendix A we show how to bound the index of $\mathrm{End}_{\overline{K}}(A)$ in any order in which it is contained, a result that is needed in the course of the proof of theorems 1.4 and 1.7.

2 Preliminaries

We collect in this section a number of results that are essentially well-known and that will form the basis for all our further discussion. Specifically, we recall a few fundamental properties of Galois representations attached to abelian varieties and an explicit form (due to Gaudron and Rémond) of the so-called Isogeny Theorem, first proved by Masser and Wüstholz in a seminal series of papers, cf. especially [MW93c] and [MW93b].

2.1 Weil pairing, the multiplier of the Galois action

We fix once and for all a minimal K-polarization of A. This choice equips the Tate module $T_\ell(A)$ with the Weil pairing, a skew-symmetric, Galois-equivariant form

$$\langle \cdot, \cdot \rangle : T_\ell(A) \times T_\ell(A) \to \mathbb{Z}_\ell(1),$$

where $\mathbb{Z}_\ell(1)$ is the 1-dimensional Galois module the action on which is given by the cyclotomic character $\chi_\ell : \mathrm{Gal}\left(\overline{K}/K\right) \to \mathbb{Z}_\ell^\times$. The Weil pairing is known to be nondegenerate on $A[\ell]$ as long as ℓ does not divide the degree of the given polarization. We know by [GR14a, Théorème 1.1] that the degree of a minimal K-polarization on A is at most $b(A/K)$: since all the bounds given in the main theorems are strictly larger than this number, we can restrict ourselves to primes that *do not* divide the degree of our fixed polarization, and for which the Weil pairing is therefore nondegenerate. From now on, therefore, we assume that the choice of a minimal polarization has been made:

Convention. We assume implicitly that a minimal K-polarization of A has been chosen. We only consider primes ℓ larger than $b(A/K)$, so the Weil pairing induced on $A[\ell]$ by this polarization is nondegenerate.

The fact that $\langle \cdot, \cdot \rangle$ is Galois-equivariant means that G_{ℓ^∞} is a subgroup of $\mathrm{GSp}(T_\ell(A), \langle \cdot, \cdot \rangle)$, the group of symplectic similitudes of $T_\ell(A)$ with respect to the Weil pairing, which we will also simply denote $\mathrm{GSp}(T_\ell(A))$. Choosing a $\mathbb{Z}_\ell$-basis of $T_\ell(A)$ we can then consider G_{ℓ^∞} (resp. G_ℓ) as being a subgroup of $\mathrm{GSp}_4(\mathbb{Z}_\ell)$ (resp. $\mathrm{GSp}_4(\mathbb{F}_\ell)$).

Our interest in the Weil pairing stems from its relationship with the determinant (or, more precisely, the multiplier) of the Galois action. Let us describe the connection. Recall that if $\langle \cdot, \cdot \rangle$ is a skew-symmetric form, the **multiplier** of a symplectic similitude B is the only scalar $\nu(B)$ such that $\langle Bv, Bw \rangle = \nu(B)\langle v, w \rangle$ for every v, w. The association $B \mapsto \nu(B)$ is then a homomorphism, whose kernel is the group $\mathrm{Sp}(\langle \cdot, \cdot \rangle)$ of symplectic isometries. In the case at hand, the Galois-equivariance of the Weil pairing implies that the composition

$$\mathrm{Gal}\left(\overline{K}/K\right) \xrightarrow{\rho_{\ell^\infty}} \mathrm{GSp}\left(T_\ell(A)\right) \xrightarrow{\nu} \mathbb{Z}_\ell^\times$$

coincides with the cyclotomic character $\chi_\ell : \mathrm{Gal}\left(\overline{K}/K\right) \to \mathbb{Z}_\ell^\times$, and it follows that G_{ℓ^∞} is all of $\mathrm{GSp}(T_\ell(A))$ if and only if it contains $\mathrm{Sp}(T_\ell(A))$ and $\mathrm{Gal}\left(\overline{K}/K\right) \xrightarrow{\chi_\ell} \mathbb{Z}_\ell^\times$ is surjective. This latter condition is very easy to check:

Lemma 2.1 *Suppose ℓ does not ramify in K: then $\mathrm{Gal}\left(\overline{K}/K\right) \xrightarrow{\chi_\ell} \mathbb{Z}_\ell^\times$ is surjective. In particular, if G_ℓ (resp. G_{ℓ^∞}) contains $\mathrm{Sp}(A[\ell])$ (resp. $\mathrm{Sp}(T_\ell(A))$) and ℓ does not divide the discriminant of K, the equality $G_\ell = \mathrm{GSp}(A[\ell])$ (resp. $G_{\ell^\infty} = \mathrm{GSp}(T_\ell(A))$) holds.*

Proof. The claim is equivalent to the fact that the equality $[K(\mu_{\ell^n}) : K] = \varphi(\ell^n)$ holds for all $n \geq 1$. In particular it suffices to show that K and $\mathbb{Q}(\mu_{\ell^n})$ are linearly disjoint over $\mathbb{Q}$, and since $\mathbb{Q}(\mu_{\ell^n})/\mathbb{Q}$ is Galois it suffices to show that they intersect trivially. Set $L := K \cap \mathbb{Q}(\mu_{\ell^n})$. Now on the one hand ℓ is unramified in K, so it is *a fortiori* unramified in L; on the other hand, every prime different from ℓ is unramified in $\mathbb{Q}(\mu_{\ell^n})$, so it is also unramified in L: it follows that L is unramified everywhere, that is, $L = \mathbb{Q}$ as claimed. The second statement is immediate. ∎

2.2   The isogeny theorem

For future reference we introduce here the main tool that will make all the explicit estimates possible. The crucial result is the isogeny theorem of Masser and Wüstholz [MW93c] [MW93b], in the following completely explicit form proved by Gaudron and Rémond:

Theorem 2.2 *(Isogeny Theorem, [GR14a, Theorem 1.4]) Let $b(A/K)$ be as in definition 1.2. For every K-abelian variety A and for every K-abelian variety A^* that is K-isogenous to A, there exists a K-isogeny $A^* \to A$ whose degree is bounded by $b(A/K)$.*

It is very likely that the function $b(A/K)$ of definition 1.2 is not the best possible one. Let us then introduce another function $b_0(A/K)$, which is by definition the best possible isogeny bound:

Definition 2.3 *For A/K an abelian variety, let $b_0(A/K)$ be the smallest natural number such that, for every abelian variety A^*/K that is K-isogenous to A, there exists a K-isogeny $A^* \to A$ of degree at most $b_0(A/K)$. Also let $b_0(A/K; d) = \max_{[K':K] \leq d} b_0(A/K')$, where the maximum is taken over the extensions of K of degree at most d.*

It is clear that the isogeny theorem implies that $b_0(A/K)$ and $b_0(A/K; d)$ are finite, and that $b_0(A/K; d) \leq b(d[K : \mathbb{Q}], \dim A, h(A))$. Whenever possible, we will state our results in terms of b_0 instead of b: in some situations, however, in order to avoid cumbersome expressions involving maxima we simply give bounds in terms of the function b.

2.3 Serre's lifting lemma

We conclude this section of preliminaries with a well-known lemma of Serre. To state it, we introduce the following useful notation:

Notation 2.4 *If G is a finite group (resp. a topological group) we denote by G' its derived subgroup (resp. the topological closure of its derived subgroup).*

Lemma 2.5 *Let n be a positive integer, $\ell \geq 5$ be a prime, and H be a closed subgroup of $\mathrm{Sp}_{2n}(\mathbb{Z}_\ell)$ whose projection modulo ℓ contains $\mathrm{Sp}_{2n}(\mathbb{F}_\ell)$: then $H = \mathrm{Sp}_{2n}(\mathbb{Z}_\ell)$. Likewise, let G be a closed subgroup of $\mathrm{GSp}_{2n}(\mathbb{Z}_\ell)$ whose projection modulo ℓ contains $\mathrm{Sp}_{2n}(\mathbb{F}_\ell)$: then $G' = \mathrm{Sp}_{2n}(\mathbb{Z}_\ell)$.*

Proof. The first statement is [Ser00, Lemme 1 on p. 52]. The second part follows from applying the first to $G = H'$: indeed, the image modulo ℓ of H' contains the derived subgroup of $\mathrm{Sp}_{2n}(\mathbb{F}_\ell)$, which (since $\ell \geq 5$) is again $\mathrm{Sp}_{2n}(\mathbb{F}_\ell)$, and the claim follows. ∎

3 Type I – Trivial endomorphisms

In this section we prove theorem 1.3, that is, we establish an explicit surjectivity result under the assumption that A/K is an abelian surface with $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$. The material is organized as follows. In the first paragraph we recall classical results on the maximal subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$; notice that – thanks to lemmas 2.1 and 2.5 – showing theorem 1.3 essentially amounts to proving that G_ℓ is not contained in any maximal proper subgroup of $\mathrm{GSp}_4(\mathbb{F}_\ell)$. In the second paragraph we collect information about the action of inertia that allows us to conclude that some exceptional subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ cannot arise as images of Galois representations. Theorem 1.3 then follows easily, as shown in the last paragraph.

3.1 Group theory for $\mathrm{GSp}_4(\mathbb{F}_\ell)$

We start by recalling the classification of the maximal subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$. The result was first proved by Mitchell in [Mit14] (see also King's article in [Web05] for a more modern account of the result), but we shall instead follow the approach of Aschbacher, who, in [Asc84], proved a general classification result for the maximal subgroups of the finite classical matrix groups. These maximal subgroups are classified into two categories: "geometric" subgroups, in turn subdivided into 8 classes $\mathcal{C}_1, \ldots, \mathcal{C}_8$, and "exceptional" (or "class $\mathcal{S}$") subgroups. Among the geometric classes introduced by Aschbacher we will only need to deal with $\mathcal{C}_1, \mathcal{C}_2$ and $\mathcal{C}_3$:

Definition 3.1 *A subgroup G of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ is said to be of class*

- *$\mathcal{C}_1$, if it stabilizes a (totally singular or non-singular) subspace;*

- *$\mathcal{C}_2$, if there exist 2-dimensional subspaces V_1, V_2 of $\mathbb{F}_\ell^4$ such that $\mathbb{F}_\ell^4 \cong V_1 \oplus V_2$, and*

$$G = \left\{ A \in \mathrm{GSp}_4(\mathbb{F}_\ell) \mid \exists \sigma \in S_2 \ s.t. \ AV_i \subseteq V_{\sigma(i)} \ for \ i = 1, 2 \right\},$$

  where S_2 is the group of permutations of the two indices $1, 2$.

- *$\mathcal{C}_3$, if there exists a $\mathbb{F}_{\ell^2}$-structure on $\mathbb{F}_\ell^4$ such that*

$$G = \left\{ A \in \mathrm{GSp}_4(\mathbb{F}_\ell) \mid \exists \sigma \in \mathrm{Gal}\left(\mathbb{F}_{\ell^2}/\mathbb{F}_\ell\right) : \forall \lambda \in \mathbb{F}_{\ell^2}, \forall v \in \mathbb{F}_\ell^4 \quad A(\lambda * v) = \sigma(\lambda) * Av \right\},$$

  where we denote by $*$ the multiplication map $\mathbb{F}_{\ell^2} \times \mathbb{F}_\ell^4 \to \mathbb{F}_\ell^4$. In this case, the set

$$\left\{ A \in \mathrm{GSp}_4(\mathbb{F}_\ell) \mid \forall \lambda \in \mathbb{F}_{\ell^2}, \forall v \in \mathbb{F}_\ell^4 \quad A(\lambda * v) = \lambda * Av \right\}$$

  is a subgroup of G of index 2 which acts $\mathbb{F}_{\ell^2}$-linearly on $\mathbb{F}_\ell^4$ (for the $\mathbb{F}_{\ell^2}$-structure $*$).

For completeness, we also include a precise definition of the exceptional class $\mathcal{S}$ (for more details cf. [BHRD13, Definition 2.1.3]):

Definition 3.2 *A subgroup H of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ is said to be of class $\mathcal{S}$ if and only if all of the following hold:*

1. *$\mathbb{P}H$ is almost simple;*

2. *H does not contain $\mathrm{Sp}_4(\mathbb{F}_\ell)$;*

3. *$H^\infty := \bigcap_{i \geq 1} H^{(i)}$ acts absolutely irreducibly on $\mathbb{F}_\ell^4$.*

A complete list of maximal subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ can be read off [BHRD13, Tables 8.13 and 8.14]:

Theorem 3.3 *Let $\ell > 7$ be a prime number. Let G be a maximal proper subgroup of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ not containing $\mathrm{Sp}_4(\mathbb{F}_\ell)$. One of the following holds:*

1. *G is of class $\mathcal{C}_1$, $\mathcal{C}_2$ or $\mathcal{C}_3$;*

2. *G is of class $\mathcal{S}$; it contains a subgroup H isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)$ such that $\mathbb{P}G = \mathbb{P}H$;*

3. *the projective image $\mathbb{P}G$ of G has order at most 3840.*

Being of class $\mathcal{S}$ in Aschbacher's classification, maximal subgroups of type (2) do not fit in a general geometric picture, but they can still be described in considerable detail. The following lemma follows immediately from the arguments of [BHRD13, §5.3]:

Lemma 3.4 *Let $\ell > 7$ be a prime and G be a maximal subgroup of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ of type (2) in the above list. For every $g \in G$, the eigenvalues of g can be written as $\lambda \cdot \lambda_1^3, \lambda \cdot \lambda_1^2 \lambda_2, \lambda \cdot \lambda_1 \lambda_2^2, \lambda \cdot \lambda_2^3$, where λ is an element of $\mathbb{F}_\ell^\times$ and λ_1, λ_2 are the roots of a second-degree polynomial with coefficients in $\mathbb{F}_\ell$.*

Proof. We know that G contains a subgroup H isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)$ such that $\mathbb{P}G = \mathbb{P}H$. For any element g of G there exist a scalar $\lambda \in \mathbb{F}_\ell^\times$ and an $h \in H$ such that $g = \lambda h$, so it suffices to show that the eigenvalues of any $h \in H$ are of the form $\lambda_1^3, \lambda_1^2 \lambda_2, \lambda_1 \lambda_2^2, \lambda_2^3$ for some λ_1, λ_2 as in the statement of the lemma. By [BHRD13, Proposition 5.3.6] we know that H is conjugated to the image of

$$\sigma_4 : \mathrm{GL}_2(\mathbb{F}_\ell) \to \mathrm{GSp}_4(\mathbb{F}_\ell),$$

where σ_4 is the third symmetric power of the standard representation of $\mathrm{GL}_2(\mathbb{F}_\ell)$. Now for every $\gamma \in \mathrm{GL}_2(\mathbb{F}_\ell)$ the eigenvalues of $\sigma_4(\gamma)$ are $\lambda_1^3, \lambda_1^2 \lambda_2, \lambda_1 \lambda_2^2, \lambda_2^3$, where λ_1, λ_2 are the eigenvalues of γ, and since H is conjugated to the image of σ_4 the claim follows. ∎

Remark 3.5 Maximal subgroups of type (2) can be interpreted in terms of morphisms of algebraic groups: the unique irreducible 4-dimensional representation of the algebraic group SL_2 is symplectic, so it gives rise to an embedding $\mathrm{SL}_2 \hookrightarrow \mathrm{Sp}_4$ with weights $-3, -1, 1, 3$. This representation extends to a representation $\mathrm{GL}_2 \to \mathrm{GSp}_4$, and subgroups of type (2) are generated by the $\mathbb{F}_\ell$-points of the image of this representation together with the homotheties.

3.2   The action of inertia

For the whole section λ is a fixed place of $\mathcal{O}_K$ at which A has *semistable* reduction. We write ℓ for the rational prime below λ and e for the (absolute) ramification index of λ over $\mathbb{Q}$. We also let I be the inertia group at λ and I^t be the corresponding *tame* inertia group, that is, the quotient of I by its pro-ℓ Sylow subgroup. The action of I on $A[\ell]$ is described by the following celebrated result of Raynaud:

8

Theorem 3.6 *([Ray74, Corollaire 3.4.4]) Let V be a simple Jordan-Hölder quotient of $A[\ell]$ (as a module over I). Suppose that V has dimension n over $\mathbb{F}_\ell$. The action of I on $A[\ell]$ factors through I^t. Moreover, there exist integers $e_1, \ldots, e_n$ such that:*

- *V has a structure of $\mathbb{F}_{\ell^n}$-vector space*

- *the action of I^t on V is given by a character $\psi : I^t \to \mathbb{F}_{\ell^n}^\times$*

- *$\psi = \varphi_1^{e_1} \ldots \varphi_n^{e_n}$, where $\varphi_1, \ldots, \varphi_n$ are the fundamental characters of I^t of level n*

- *for every $i = 1, \ldots, n$ the inequality $0 \le e_i \le e$ holds*

Remark 3.7 Raynaud's theorem is usually stated for places of *good* reduction. However, as it was shown in [LV14, Lemma 4.9], the extension to the semistable case follows easily upon applying results of Grothendieck [Gro].

In this section we only consider $A[\ell]$ as an I^t-module; in particular, by a Jordan-Hölder quotient of $A[\ell]$ we implicitly mean "under the action of I^t". Notice that, in view of Raynaud's theorem, the map $\rho_\ell : \mathrm{Gal}\left(\overline{K}/K\right) \to \mathrm{Aut}\, A[\ell]$ induces a map $I^t \to \mathrm{Aut}\, A[\ell]$, which for simplicity of notation we still denote by ρ_ℓ. Recall furthermore that the norm, taken from $\mathbb{F}_{\ell^n}$ to $\mathbb{F}_\ell$, of a fundamental character of level n is the unique fundamental character of level 1; when ℓ is unramified in K, this fundamental character of level 1 is χ_ℓ, the cyclotomic character mod ℓ.

Recall the following fact (a consequence of the definition of the fundamental characters):

Lemma 3.8 *If $\varphi : I^t \to \mathbb{F}_{\ell^n}^\times$ is any fundamental character of level n, then φ is surjective, hence in particular its image is a cyclic group of order $\ell^n - 1$.*

Lemma 3.9 *Let W be a simple Jordan-Hölder quotient of $A[\ell]$ of dimension n and let ψ be the associated character $I^t \to \mathbb{F}_{\ell^n}^\times \subset \overline{\mathbb{F}_\ell}^\times$. Let k be a positive integer and suppose that the image of ψ is contained in $\mathbb{F}_{\ell^k}^\times \subset \overline{\mathbb{F}_\ell}^\times$: then $n \le k$.*

Proof. Let σ be a generator of $\mathrm{Gal}\left(\mathbb{F}_{\ell^k}/\mathbb{F}_\ell\right)$. The hypothesis implies that the action of I^t on W can be diagonalized over $\mathbb{F}_{\ell^k}$, so we can find a vector $v \in W \otimes_{\mathbb{F}_\ell} \mathbb{F}_{\ell^k}$ that is a common eigenvector for the action of I^t. The $\mathbb{F}_{\ell^k}$-vector subspace of $W \otimes_{\mathbb{F}_\ell} \mathbb{F}_{\ell^k}$ spanned by $v, \sigma v, \ldots, \sigma^{k-1} v$ is by construction σ-stable, hence it descends to a $\mathbb{F}_\ell$-subspace W' of W, and it is clear by construction that W' is also stable under the action of I^t. As W is irreducible and W' is nontrivial we must have $W' = W$, and since $\dim W' \le k$ we have $n = \dim W \le k$. ∎

Lemma 3.10 *Let $\ell > 7$, and suppose G_ℓ is contained in a maximal subgroup of type (2) in the sense of theorem 3.3. Then every simple Jordan-Hölder quotient W of $A[\ell]$ has dimension at most 2.*

Proof. The hypothesis and lemma 3.4 imply that all the eigenvalues of every element of G_ℓ lie in $\mathbb{F}_{\ell^2}$, hence in particular the same is true for the eigenvalues of the action of I^t. It follows that the image of the character ψ associated with W is entirely contained in $\mathbb{F}_{\ell^2}$, and lemma 3.9 shows that W is of dimension at most 2. ∎

Corollary 3.11 *Suppose $\ell > 7$ is unramified in K and G_ℓ is contained in a maximal subgroup of type (2) in the sense of theorem 3.3. Let W be an n-dimensional Jordan-Hölder quotient of $A[\ell]$. The following are the only possibilities:*

- *$n = 1$ and I^t acts trivially on W;*

- *$n = 1$ and I^t acts on W through χ_ℓ;*

- *$n = 2$ and I^t acts on W through a fundamental character of level 2.*

Proof. Lemma 3.10 implies $n \leq 2$, and theorem 3.6 classifies all simple Jordan-Hölder quotients of dimension at most 2 (notice that ℓ is unramified in K, so $e = 1$). ∎

From now on we suppose that $\ell > 7$ is unramified in K and that G_ℓ is contained in a maximal subgroup of type (2) in the sense of theorem 3.3. We fix a Jordan-Hölder filtration of the I^t-module $A[\ell]$, and we denote by $W_1, \ldots, W_k$ the simple subquotients of the filtration.

Furthermore, we let m_0, m_1, m_2 be the number of W_i on which the action of I^t is respectively trivial, given by χ_ℓ, or given by a fundamental character of level 2. Clearly, by comparing dimensions, we must have

$$m_0 + m_1 + 2m_2 = \dim_{\mathbb{F}_\ell} A[\ell] = 4. \tag{3.1}$$

Considering the determinant of the Galois action gives a second numerical relation:

Lemma 3.12 *We have $m_1 + m_2 = 2$.*

Proof. Let W be a simple Jordan-Hölder subquotient of $A[\ell]$. The determinant of the action of $g \in I^t$ on W is either 1 (if the action is trivial) or $\chi_\ell(g)$ (if the action is given by χ_ℓ or by a fundamental character of level 2). On the other hand, the determinant of the Galois action of $g \in I^t$ on $A[\ell]$ is $\chi_\ell(g)^2$ by the properties of the Weil pairing, so we must have

$$\prod_{W_i} \det \left(\rho_\ell(g) : W_i \to W_i \right) = \chi_\ell(g)^2 \quad \forall g \in I^t,$$

or in another words $\chi_\ell^{m_1 + m_2 - 2}(g) = 1$ for all $g \in I^t$. Since $\chi_\ell(I^t)$ is a cyclic group of order $\ell - 1$, this implies $\ell - 1 \mid m_1 + m_2 - 2$, and since $|m_1 + m_2 - 2| \leq 2 < \ell - 1$ we must in fact have $m_1 + m_2 - 2 = 0$, as claimed. ∎

Corollary 3.13 *Suppose $\ell > 7$ is unramified in K and G_ℓ is contained in a maximal subgroup of type (2) in the sense of theorem 3.3. For every $g \in I^t$ the multiset of eigenvalues of $\rho_\ell(g)$ is one of the following, where we denote by φ_1 and $\varphi_2 = \varphi_1^\ell$ the two fundamental characters of level 2:*

1. $\{\chi_\ell(g), \chi_\ell(g), 1, 1\}$

2. $\{\varphi_1(g), \varphi_2(g), \chi_\ell(g), 1\}$

3. $\{\varphi_1(g), \varphi_2(g), \varphi_1(g), \varphi_2(g)\}$

Proof. The multiset of eigenvalues of $\rho_\ell(g)$ is the union of the multisets of values taken by the characters that give the action of g on the simple Jordan-Hölder factors W_i. In turn, these characters and their multiplicities are determined by the three numbers m_0, m_1, m_2, which by equation (3.1) and the previous lemma satisfy $m_1 = m_0$ and $m_2 = 2 - m_0$. The three cases in the statement correspond to the three possibilities $m_0 = 0$, $m_0 = 1$, and $m_0 = 2$. ∎

We can now show that groups of type (2) do not arise as images of Galois representations (at least when $\ell > 7$ is unramified in K):

Proposition 3.14 *Let $\ell > 7$ be a prime unramified in K. Suppose there is a place λ of K of characteristic ℓ at which A has semistable reduction: then G_ℓ is not contained in a group of type (2) in the sense of theorem 3.3.*

Proof. Suppose on the contrary that G_ℓ is contained in a group of type (2). By lemma 3.4, for any $g \in \mathrm{Gal}\left(\overline{K}/K\right)$ the eigenvalues of $\rho_\ell(g)$ are of the form $\{\lambda a^3, \lambda a^2 d, \lambda a d^2, \lambda d^3\}$ for certain $\lambda \in \mathbb{F}_\ell^\times$ and $a, d \in \mathbb{F}_{\ell^2}^\times$. This applies in particular to the tame inertia group I^t: for every g in I^t, the eigenvalues of $\rho_\ell(g)$ lie in $\mathbb{F}_{\ell^2}^\times$, and – taken in some order $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ – they satisfy the system of equations

$$\lambda_1 \lambda_4 = \lambda_2 \lambda_3, \ \lambda_2 \lambda_4 = \lambda_3^2, \ \lambda_1 \lambda_3 = \lambda_2^2. \tag{3.2}$$

We now go through the cases listed in corollary 3.13 and check that (for a suitably chosen $g \in I^t$) there is no way to renumber the multiset of eigenvalues of $\rho_\ell(g)$ in such a way that the

three equations above are all satisfied together, a contradiction that shows the result. Consider case 1. By lemma 3.8, the condition $\ell > 7$ implies that the order of $\chi_\ell(I^t)$ is at least 10, so there exists a $g \in I^t$ with $\chi_\ell(g) \neq \pm 1$. Consider equations (3.2) for this specific g. If either λ_2 or λ_3 is 1, then one of the last two equations reads $\chi_\ell(g)^d = 1$ with $d = 1$ or 2, which contradicts $\chi_\ell(g) \neq 1, -1$. But if neither λ_2 nor λ_3 is 1 then the only possibility is $\lambda_1 = \lambda_4 = 1$, $\lambda_2 = \lambda_3 = \chi_\ell(g)$, for which none of the three equations is satisfied. Likewise, in case 3 we can choose a $g \in I^t$ such that $\varphi_1(g)$ is of order $\ell^2 - 1$, and – independently of the numbering of the eigenvalues – from equations (3.2) we obtain $(\varphi_1(g))^2 = (\varphi_2(g))^2$, which using $\varphi_2 = (\varphi_1)^\ell$ implies $\varphi_1(g)^{2(\ell-1)} = 1$, a contradiction. Finally, if we are in case 2, then taking the norm from $\mathbb{F}_{\ell^2}$ to $\mathbb{F}_\ell$ of the three equations (3.2) we find that for all $g \in I^t$ there exists a positive integer $d \leq 3$ such that $\chi_\ell(g)^d = 1$, which again contradicts the fact that $\chi_\ell(I^t)$ has order at least 10. $\blacksquare$

Considering the action of inertia also allows us to exclude groups of type (3) in the list of theorem 3.3. The following proposition (which applies to abelian varieties of arbitrary dimension and with arbitrary endomorphism ring) gives a linear lower bound on the order of $\mathbb{P}G_\ell$:

Proposition 3.15 *Let A/K be any abelian variety of dimension g. Let ℓ be a prime such that there is a place λ of K of residual characteristic ℓ at which A has either good or bad semistable reduction. If ℓ is unramified in K and not less than $g + 2$, then $|\mathbb{P}G_\ell| \geq \ell - 1$.*

Proof. We let again $W_1, \ldots, W_k$ be the simple Jordan-Hölder subquotients of $A[\ell]$ under the action of the tame inertia group at λ (denoted by I^t), and we write ψ_i $(i = 1, \ldots, k)$ for the character giving the action of I^t on W_i. Let N be the order of $|\mathbb{P}G_\ell|$, and notice that for every $y \in G_\ell$ the projective image of y^N is trivial, that is, y^N is a scalar, and in particular has a unique eigenvalue of multiplicity $2g$. Since for $x \in I^t$ the eigenvalues of $\rho_\ell(x)$ are given by the Galois conjugates of the various $\psi_i(x)$, this implies that for all $i, j = 1, \ldots, k$, for all integers $t \geq 0$, and for all $x \in I^t$ we have

$$\psi_i(x)^{\ell^t N} = \psi_j(x)^N. \tag{3.3}$$

Notice that if W is a one-dimensional Jordan-Hölder subquotient of $A[\ell]$, then the action of I^t on W is given either by the trivial character or by χ_ℓ: this follows from theorem 3.6 and the assumption that ℓ is unramified in K (in the notation of theorem 3.6 we have $e = 1$). Thus we are necessarily in one of the following three cases: at least one W_i has dimension at least 2; all the W_i are 1-dimensional, and both 1 and χ_ℓ appear among the ψ_i; all the W_i are 1-dimensional, and the ψ_i are either all trivial or all equal to χ_ℓ.

1. At least one of the W_i's is of dimension ≥ 2: without loss of generality, we can assume that $n := \dim W_1$ is at least 2. Let ψ be the associated character. By Raynaud's theorem, there are integers $e_0, \ldots, e_{n-1} \in \{0, 1\}$ such that $\psi = \varphi^{\sum_{i=0}^{n-1} e_i \ell^i}$, where φ is a fundamental character of level n. Note that we cannot have $e_i = 1$ for all $i = 0, \ldots, n-1$, for otherwise we would have $\psi = \chi_\ell$, which contradicts the fact that W_1 is of dimension $n > 1$ (lemma 3.9). In particular, since for all integers $t \geq 0$ the character φ^{ℓ^t} is a Galois conjugate of φ, replacing φ with φ^{ℓ^t} for a suitable t we can assume that $e_{n-1} = 0$ (notice that replacing φ with φ^ℓ has the effect of permuting cyclically the integers e_i, at least one of which is zero). Now φ has exact order $\ell^n - 1$, so $\psi = \varphi^{\sum_{i=0}^{n-1} e_i \ell^i}$ has order at least

$$\frac{\ell^n - 1}{\sum_{i=0}^{n-1} e_i \ell^i} \geq \frac{\ell^n - 1}{\sum_{i=0}^{n-2} \ell^i} = \frac{(\ell^n - 1)(\ell - 1)}{(\ell^{n-1} - 1)} \geq \ell(\ell - 1),$$

that is to say, there is an $x \in I^t$ such that $\psi(x)$ has order at least $\ell(\ell - 1)$. Consider now equation (3.3) for this specific x, for $\psi_i = \psi_j = \psi$ and for $t = 1$: it gives $\psi(x)^{(\ell-1) \cdot N} = 1$, so $\psi(x)$ has order at most $(\ell - 1) \cdot N$. Thus we obtain $(\ell - 1) \cdot N \geq \ell(\ell - 1)$, that is $N \geq \ell > \ell - 1$ as claimed.

2. All the W_i's are of dimension 1, for at least one index i we have $\psi_i = 1$, and for at least one index j we have $\psi_j = \chi_\ell$: then for all $x \in I^t$ we have $\psi_j(x)^N = \psi_i(x)^N$, that is, $\chi_\ell(x)^N = 1$ for all $x \in I^t$. As χ_ℓ has exact order $\ell - 1$, this implies $N \geq \ell - 1$.

3. All the W_i's are of dimension 1 and all characters ψ_i are equal to each other (and in particular are either all trivial or all equal to the cyclotomic character χ_ℓ): in this case there are exactly $k = 2g$ simple Jordan-Hölder quotients, and from the equality

$$\chi_\ell(x)^g = \det \rho_\ell(x) = \prod_{i=1}^{2g} \psi_i(x) = \begin{cases} 1, & \text{if } \psi_i = 1 \text{ for every } i \\ \chi_\ell(x)^{2g}, & \text{if } \psi_i = \chi_\ell \text{ for every } i \end{cases}$$

we find $\chi_\ell(x)^g = 1$ for all $x \in I^t$, which contradicts the fact that the order of χ_ℓ is $\ell - 1 > g$.

∎

Remark 3.16 The proof shows that case 3 is impossible under the hypotheses of the previous proposition. By contrast, cases 1 and 2 do happen: the former is the generic situation, while the latter occurs for example for elliptic curves over $\mathbb{Q}$ having a rational ℓ-torsion point (with $\ell \geq g + 2 = 3$).

3.3 The surjectivity result

We are almost ready to prove theorem 1.3: the last ingredients we are missing are two isogeny estimates which form the subject of lemmas 3.17 and 3.18 below. The strategy of proof of these lemmas is a variant of the approach of [MW93a] – cf. especially lemmas 3.1 and 3.2 of *op. cit.*

Lemma 3.17 *Let A/K be an abelian variety of dimension g with $\mathrm{End}_K(A) = \mathbb{Z}$. Suppose that the G_ℓ-module $A[\ell]$ is reducible: then the inequality $\ell \leq b_0(A/K)$ holds.*

Proof. Let H be a nontrivial proper subspace of $A[\ell]$ stable under the action of G_ℓ. As H is a proper $\mathbb{F}_\ell$-subspace of $A[\ell] \cong \mathbb{F}_\ell^{2g}$, its order divides ℓ^{2g-1}. Consider now the abelian variety $A^* = A/H$, which is defined over K (since H is), and let $\Psi : A^* \to A$ be an isogeny of degree at most $b_0(A/K)$. Let $\pi : A \to A^*$ be the canonical projection, of degree $|H| \leq \ell^{2g-1}$, and consider the composition $\Psi \circ \pi : A \to A$. By the hypothesis $\mathrm{End}_K(A) = \mathbb{Z}$ this composition must be multiplication by m for a certain nonzero integer m. Comparing degrees we see that $m^{2g} = \deg(\Psi) \deg(\pi) \leq b_0(A/K)\ell^{2g-1}$, and on the other hand $\Psi \circ \pi$ kills H (since this is true even for π alone), so $mH = 0$. Every nonzero element of H has order ℓ, so m must be divisible by ℓ, which implies $\ell^{2g} \leq b_0(A/K)\ell^{2g-1}$, i.e. $\ell \leq b_0(A/K)$ as claimed. ∎

Lemma 3.18 *Let A/K be an abelian variety of dimension g with $\mathrm{End}_K(A) = \mathbb{Z}$. If the centralizer of G_ℓ in $\mathrm{End}(A[\ell])$ strictly contains $\mathbb{F}_\ell$, then ℓ does not exceed $b_0(A^2/K)^{1/2g}$.*

Proof. Choose an element $\alpha \in \mathrm{End}(A[\ell])$ lying in the centralizer of G_ℓ but not in $\mathbb{F}_\ell$. Consider the abelian variety $B = A^2$ and the subgroup of B given by $\Gamma = \{(x, \alpha x) \mid x \in A[\ell]\}$. Notice that Γ is defined over K: indeed α commutes with all of $\rho_\ell(\mathrm{Gal}\left(\overline{K}/K\right))$, so an operator $h \in \mathrm{Gal}\left(\overline{K}/K\right)$ sends $(x, \alpha x)$ to

$$(\rho_\ell(h)x, \rho_\ell(h)\alpha x) = (\rho_\ell(h)x, \alpha(\rho_\ell(h)x)) \in \Gamma.$$

Let $B^* = B/\Gamma$, $\pi : B \to B^*$ be the natural projection, and $\psi : B^* \to B$ be an isogeny satisfying $\deg(\psi) \leq b_0(A^2/K)$. The endomorphism $\psi \circ \pi$ of B kills Γ, and thanks to the hypothesis $\mathrm{End}_K(A) = \mathbb{Z}$ it can be represented by a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathrm{End}_K(A)) = \mathrm{M}_2(\mathbb{Z})$ with nonzero determinant. By definition we must have $ax + b\alpha x = cx + d\alpha x = 0$ for every $x \in A[\ell]$. Suppose that one among a, b, c, d is not divisible by ℓ (and for the sake of simplicity let us assume it is b, the other cases being analogous): then we have $\alpha(x) = -b^{-1}ax$ for every x in $A[\ell]$, which shows that α coincides with the multiplication by an element of $\mathbb{F}_\ell$, contradiction. Therefore a, b, c, d are all divisible by ℓ, and the degree of $\psi \circ \pi$, which is $\left(\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right)^{2g}$, is divisible by ℓ^{4g}. On the other hand, the degree of π is $|\Gamma| = |A[\ell]| = \ell^{2g}$, so we deduce

$$\ell^{4g} \leq \deg(\psi \circ \pi) = \deg \psi \cdot \ell^{2g} \leq \ell^{2g} b_0(A^2/K),$$

that is, $\ell \leq b_0(A^2/K)^{1/2g}$ as claimed. ∎

Theorem 3.19 *(Theorem 1.3) Let A/K be an abelian surface with $\text{End}_{\overline{K}}(A) = \mathbb{Z}$. The equality $G_{\ell^\infty} = \text{GSp}_4(\mathbb{Z}_\ell)$ holds for every prime ℓ that satisfies the following three conditions:*

- $\ell > b(2[K : \mathbb{Q}], 4, 2h(A))^{1/4}$;

- *there exists a place of K of characteristic ℓ at which A has semistable reduction;*

- *ℓ is unramified in K.*

Proof. We claim that G_ℓ contains $\text{Sp}_4(\mathbb{F}_\ell)$. If this is not the case, then G_ℓ is contained in one of the maximal proper subgroups of $\text{GSp}_4(\mathbb{F}_\ell)$ listed in theorem 3.3. Let us go through this list.

Firstly, since $\ell > b(2[K : \mathbb{Q}], 4, 2h(A))^{1/4} > b_0(A/K)$, lemma 3.17 implies that G_ℓ is not contained in a maximal subgroup of class $\mathcal{C}_1$. Suppose next that G_ℓ is contained in a maximal subgroup of class $\mathcal{C}_2$: then there exists a (normal) subgroup H_ℓ of G_ℓ, of index at most 2, that does not act irreducibly on $A[\ell]$. Consider the morphism

$$\text{Gal}\left(\overline{K}/K\right) \to G_\ell \to G_\ell/H_\ell :$$

the fixed field of its kernel is a certain extension K' of K, of degree at most 2, such that $\rho_\ell\left(\text{Gal}\left(\overline{K'}/K'\right)\right) = H_\ell$ does not act irreducibly on $A[\ell]$. Applying lemma 3.17 to A/K' we find $\ell \leq b_0(A/K') \leq b(2[K : \mathbb{Q}], 4, 2h(A))^{1/4}$, contradiction. Consider now the case of G_ℓ being contained in a maximal subgroup of class $\mathcal{C}_3$: there is a (normal) subgroup H_ℓ of G_ℓ, of index at most 2, and a structure of $\mathbb{F}_{\ell^2}$-vector space on $A[\ell]$, such that the action of H_ℓ on $A[\ell]$ is compatible with the $\mathbb{F}_{\ell^2}$-structure. As above, let K'' be the fixed field of $\ker\left(\text{Gal}\left(\overline{K}/K\right) \to G_\ell \to G_\ell/H_\ell\right)$, and notice that K'' is a (at most) quadratic extension of K such that the centralizer of $\rho_\ell(\text{Gal}\left(\overline{K''}/K''\right))$ contains a copy of $\mathbb{F}_{\ell^2}$: this contradicts lemma 3.18, since $\ell > b(2[K : \mathbb{Q}], 4, 2h(A))^{1/4} \geq b_0(A^2/K')^{1/4}$, so we cannot be in this case either. Finally, case (2) is impossible by proposition 3.14, and case (3) is excluded by proposition 3.15: indeed we clearly have $\ell > 3842$, so proposition 3.15 implies that $|\mathbb{P}G_\ell| > 3840$. It follows as claimed that G_ℓ contains $\text{Sp}_4(\mathbb{F}_\ell)$, hence G_{ℓ^∞} contains $\text{Sp}_4(\mathbb{Z}_\ell)$ by lemma 2.5; lemma 2.1 finally implies the desired equality $G_{\ell^\infty} = \text{GSp}_4(\mathbb{Z}_\ell)$. ∎

4 Type I – Real multiplication

We consider now the case of GL_2-varieties, which includes abelian surfaces with real multiplication as a special case. Recall (definition 1.1) that an abelian variety A is said to be of GL_2-type when it is absolutely simple and $R = \text{End}_{\overline{K}}(A)$ is an order in a totally real number field E of degree equal to $\dim A$. We shall assume that the action of R is defined over K. For every ℓ we set $\mathcal{O}_\ell = \mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$, and if λ is a place of E we let $\mathcal{O}_\lambda$ be the completion of $\mathcal{O}_E$ at λ. We have $\mathcal{O}_\ell \cong \prod_{\lambda | \ell} \mathcal{O}_\lambda$, where the product is over the places of E dividing ℓ. An implicit convention will always be in force, that if λ is a place of E then ℓ denotes its residual characteristic.

Definition 4.1 *Following Ribet's paper [Rib76] we say that a rational prime ℓ is **good** for A if it does not divide the index $[\mathcal{O}_E : R]$.*

As $[\mathcal{O}_E : R]$ is finite, all but finitely many primes are good for A. It is a general fact that $[\mathcal{O}_E : R]$ can be bounded in terms of K and $h(A)$, cf. appendix A. We obtain from proposition A.5 the following estimate, which enables us to assume that all the primes we work with are good:

Proposition 4.2 *The index $[\mathcal{O}_E : R]$ is bounded by $b\left([K : \mathbb{Q}], \dim A, h(A)\right)^{\dim A}$. In particular, any prime strictly larger than this quantity is good.*

From now on we only consider *good* primes that do not ramify in E – this only excludes finitely many primes. Notice that in the case of surfaces, in view of the last proposition and of the obvious inequality $b(2[K : \mathbb{Q}], 2\dim A, 2h(A))^{1/2} > b\left([K : \mathbb{Q}], \dim A, h(A)\right)^2$, all the primes considered in corollary 1.5 are good for A. For any good prime ℓ we have $R_\ell := R \otimes \mathbb{Z}_\ell \cong \mathcal{O}_E \otimes \mathbb{Z}_\ell$, and furthermore for such primes the structure of $T_\ell(A)$ is well understood:

Proposition 4.3 *([Rib76, Proposition 2.2.1]) If ℓ is good for A, then $T_\ell(A)$ is a free R_ℓ-module of rank 2; equivalently, it is a free $\mathcal{O}_\ell$-module of rank 2.*

When ℓ is good and λ is a place of E of characteristic ℓ we put $T_\lambda(A) = T_\ell(A) \otimes_{\mathcal{O}_\ell} \mathcal{O}_\lambda$: this makes sense since $\mathcal{O}_\ell = R \otimes \mathbb{Z}_\ell$. The Galois action on $T_\ell(A)$ is $\mathcal{O}_\ell$-linear, and we thus obtain canonical decompositions $T_\ell(A) \cong \prod_{\lambda|\ell} T_\lambda(A)$; the $\mathcal{O}_\ell$-linear morphism ρ_{ℓ^∞} then amounts to a family of $\mathcal{O}_\lambda$-linear maps

$$\rho_{\lambda^\infty} : \mathrm{Gal}\left(\overline{K}/K\right) \to \mathrm{GL}(T_\lambda(A)) \cong \mathrm{GL}_2\left(\mathcal{O}_\lambda\right).$$

We also have isomorphisms $\mathrm{Aut}\, T_\ell(A) \cong \mathrm{GL}_2(\mathcal{O}_E \otimes \mathbb{Z}_\ell) \cong \prod_{\lambda|\ell} \mathrm{GL}_2\left(\mathcal{O}_\lambda\right)$, and we regard the ℓ-adic Galois representation on $T_\ell(A)$ as a group morphism

$$\rho_{\ell^\infty} : \mathrm{Gal}\left(\overline{K}/K\right) \to \prod_{\lambda|\ell} \mathrm{GL}_2\left(\mathcal{O}_\lambda\right)$$

whose components are the ρ_{λ^∞}. It is also natural to consider λ-adic residual representations:

Definition 4.4 *If λ is a place of E above a good prime ℓ that is furthermore unramified in E, we write G_λ for the image of the residual representation modulo λ, namely the image of the map ρ_λ given by the composition*

$$\mathrm{Gal}\left(\overline{K}/K\right) \xrightarrow{\rho_{\ell^\infty}} \prod_{\lambda|\ell} \mathrm{GL}_2\left(\mathcal{O}_\lambda\right) \to \mathrm{GL}_2\left(\mathcal{O}_\lambda\right) \to \mathrm{GL}_2\left(\mathcal{O}_\lambda/\lambda\right).$$

The determinant of ρ_{λ^∞} is easy to describe:

Lemma 4.5 *([Rib76, Lemma 4.5.1]) For every place λ of E dividing a good prime ℓ, the function*

$$\det \rho_{\lambda^\infty} : \mathrm{Gal}\left(\overline{K}/K\right) \to \mathcal{O}_\lambda^\times$$

coincides with the ℓ-adic cyclotomic character $\chi_\ell : \mathrm{Gal}\left(\overline{K}/K\right) \to \mathbb{Z}_\ell^\times \hookrightarrow \mathcal{O}_\lambda^\times$.

Observe that for a good prime ℓ the ℓ-adic representation lands in $\mathrm{Aut}_{\mathcal{O}_\ell}(T_\ell(A))$. If we regard $\mathbb{Z}_\ell$ as being embedded in $\mathcal{O}_\ell$ (the latter is naturally a $\mathbb{Z}_\ell$-algebra), then by the previous lemma we have $\det_{\mathcal{O}_\ell} \rho_{\ell^\infty}(g) = \chi_\ell(g) \in \mathbb{Z}_\ell^\times \subset \mathcal{O}_\ell^\times$, and applying lemma 2.1 we find

Lemma 4.6 *If ℓ is good and unramified in K then $\det_{\mathcal{O}_\ell} : G_{\ell^\infty} \to \mathbb{Z}_\ell^\times$ is surjective.*

4.1 The intersection $G_{\ell^\infty} \cap \mathrm{SL}_2(\mathcal{O}_\ell)$

The key step in proving the surjectivity of the Galois representation for ℓ large enough lies in understanding the intersection $G_{\ell^\infty} \cap \mathrm{SL}_2(\mathcal{O}_\ell)$. A remarkable simplification of the problem comes from the fact that we only need to prove surjectivity for the residual mod-ℓ representation instead of the full ℓ-adic system: this is made possible by the following 'lifting' result, analogous to lemma 2.5.

Proposition 4.7 *([Rib97, Proposition 4.2]) Let $\mathcal{O}$ be the ring of integers of a number field E, $\lambda_1, \lambda_2, \ldots, \lambda_r$ distinct primes of $\mathcal{O}$ above ℓ and H a closed subgroup of $\mathrm{SL}_2(\mathcal{O}_{\lambda_1}) \times \cdots \times \mathrm{SL}_2(\mathcal{O}_{\lambda_r})$ whose projection to $\mathrm{SL}_2(\mathbb{F}_{\lambda_1}) \times \cdots \times \mathrm{SL}_2(\mathbb{F}_{\lambda_r})$ is surjective. If ℓ is unramified in E and $\ell \geq 5$, then H is all of $\mathrm{SL}_2(\mathcal{O}_{\lambda_1}) \times \cdots \times \mathrm{SL}_2(\mathcal{O}_{\lambda_r})$. Under the same assumptions on ℓ, if G is a closed subgroup of $\mathrm{GL}_2(\mathcal{O}_{\lambda_1}) \times \cdots \times \mathrm{GL}_2(\mathcal{O}_{\lambda_r})$ whose projection to $\mathrm{GL}_2(\mathbb{F}_{\lambda_1}) \times \cdots \times \mathrm{GL}_2(\mathbb{F}_{\lambda_r})$ contains $\mathrm{SL}_2(\mathbb{F}_{\lambda_1}) \times \cdots \times \mathrm{SL}_2(\mathbb{F}_{\lambda_r})$, then $G' = \mathrm{SL}_2(\mathcal{O}_{\lambda_1}) \times \cdots \times \mathrm{SL}_2(\mathcal{O}_{\lambda_r})$.*

4.1.1 A little group theory

We briefly review the group-theoretic results we are going to use, starting with the following sufficient criterion for a group to be a direct product:

Lemma 4.8 *([Rib76, Lemma 5.2.2]) Let $S_1, \ldots, S_k$ $(k > 1)$ be finite groups with no nontrivial abelian quotients. Let G be a subgroup of $S_1 \times \cdots \times S_k$ such that each projection $G \to S_i \times S_j$ $(1 \leq i < j \leq k)$ is surjective. Then $G = S_1 \times \cdots \times S_k$.*

We will also need the following version of [MW93a, Lemma 5.1]; note that our formulation is slightly different from that of [MW93a], but the same proof applies equally well.

Lemma 4.9 *([MW93a, Lemma 5.1]) Let $\ell \geq 5$ be a prime, $\mathbb{F}$ a finite field of characteristic ℓ, and*

$$D = \left\{ (b, b') \in \mathrm{GL}_2(\mathbb{F}) \times \mathrm{GL}_2(\mathbb{F}) \mid \det(b) = \det(b') \in \mathbb{F}_\ell^\times \right\}.$$

Let H be a subgroup of D whose projections on the two factors $\mathrm{GL}_2(\mathbb{F})$ contain $\mathrm{SL}_2(\mathbb{F})$. Then either H contains $\mathrm{SL}_2(\mathbb{F}) \times \mathrm{SL}_2(\mathbb{F})$, or else there exist an isomorphism $f : \mathbb{F}^2 \to \mathbb{F}^2$ (of $\mathbb{F}$-vector spaces), a character $\chi : H \to \{\pm 1\}$, and a field automorphism σ of $\mathbb{F}$ such that

$$H \subseteq \left\{ (b, b') \in \mathrm{GL}_2(\mathbb{F}) \times \mathrm{GL}_2(\mathbb{F}) \mid b' = \chi((b, b'))\, \sigma\left(fbf^{-1}\right) \right\}.$$

Finally, we will need a description of the subgroups of $\mathrm{GL}_2(\mathbb{F}_{\ell^\beta})$ for $\beta \geq 1$:

Theorem 4.10 *(Dickson, [Blo67, Theorem 3.4]) Let p be a prime number, β be a positive integer, $q = p^\beta$ be a power of p, and G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_q)$. Then, up to conjugacy in $\mathrm{GL}_2(\mathbb{F}_q)$, one of the following occurs:*

1. *G is cyclic;*

2. *G is a subgroup of the Borel group $\left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \mid x, z \in \mathbb{F}_q^\times, y \in \mathbb{F}_q \right\}$;*

3. *G contains (as a subgroup of index 2) a cyclic subgroup of order u, where u divides $q^2 - 1$;*

4. *G contains (as a subgroup of index 2) a subgroup consisting entirely of diagonal matrices;*

5a. *there is an $\alpha \in \mathbb{N}_{>0}$ dividing β such that G is generated by $\mathrm{SL}_2(\mathbb{F}_{p^\alpha})$ and by a scalar matrix V (in this case $p^\alpha > 3$);*

5b. *there exist an α dividing β, a generator ε of $\mathbb{F}_{p^\alpha}^\times$ (as a multiplicative group), and an element $b \in \mathbb{F}_{p^\beta}^\times$, such that G is generated by $\mathrm{SL}_2(\mathbb{F}_{p^\alpha})$, a scalar matrix V, and the diagonal matrix $\mathrm{diag}(b, b\varepsilon)$; the subgroup generated by $\mathrm{SL}_2(\mathbb{F}_{p^\alpha})$ and V is of type 5a, and has index 2 in G (and again the inequality $p^\alpha > 3$ holds);*

6. *$G/\{\pm \mathrm{Id}\}$ is isomorphic to $S_4 \times \frac{\mathbb{Z}}{u\mathbb{Z}}$, $A_4 \times \frac{\mathbb{Z}}{u\mathbb{Z}}$ or $A_5 \times \frac{\mathbb{Z}}{u\mathbb{Z}}$, where $\frac{\mathbb{Z}}{u\mathbb{Z}}$ is identified with the subgroup generated by a scalar matrix in $\mathrm{GL}_2(\mathbb{F}_q)/\{\pm \mathrm{Id}\}$.*

7. *G is not of type (6), but $G/\{\pm \mathrm{Id}\}$ contains $A_4 \times \frac{\mathbb{Z}}{u\mathbb{Z}}$ as a subgroup of index 2, and A_4 as a subgroup with cyclic quotient group; $\frac{\mathbb{Z}}{u\mathbb{Z}}$ is as in type (6) with u even.*

Definition 4.11 *In cases (5a) or (5b) the number α will be called the **level** of the group G.*

4.1.2 Isogeny estimates

Let λ be a place of E. We write $\mathbb{F}_\lambda$ for the residue field at λ and $f = [\mathbb{F}_\lambda : \mathbb{F}_\ell]$ for its inertia degree; recall that we have introduced the residual representation G_λ in definition 4.4. The following two lemmas are simple variants of lemmas 3.17 and 3.18 respectively; we give a complete argument only for the former:

Lemma 4.12 *Let ℓ be a good prime for A unramified in E, and let λ be a place of E above ℓ. Suppose that G_λ fixes a 1-dimensional $\mathbb{F}_\lambda$-subspace Γ of $T_\lambda(A)/\lambda T_\lambda(A) \cong \mathbb{F}_\lambda^2$: then we have $\ell \leq b_0(A/K)$.*

Proof. The finite group Γ is fixed by G_λ and therefore defined over K. Consider the K-variety $A^* = A/\Gamma$, which comes equipped with a natural isogeny $\pi : A \twoheadrightarrow A^*$ of degree $|\Gamma| = |\mathbb{F}_\lambda| = \ell^f$. Choose a K-isogeny $\psi : A^* \to A$ of degree $b \leq b_0(A/K)$. The composition $\psi \circ \pi$ is an endomorphism of A, so by hypothesis it is given by a certain $e \in \mathrm{End}(A) \subseteq \mathcal{O}_E$. Notice now that e kills Γ, and on the other hand the action of e on $T_\lambda(A)/\lambda T_\lambda(A)$ is through multiplication by the class of e in $\mathcal{O}_E/\lambda \cong \mathbb{F}_\lambda$. It follows that e reduces to 0 in $\mathbb{F}_\lambda$, that is, e belongs to the ideal λ; hence $\deg(e) = N_{E/\mathbb{Q}}(e)^2$ (for this equality cf. [BL04], Chapter 5, Corollary 1.3) is divisible by $N_{E/\mathbb{Q}}(\lambda)^2$, which is just $|\mathbb{F}_\lambda|^2 = \ell^{2f}$. Comparing degrees we have $\ell^{2f} \mid \deg(e) = b\ell^f$, so ℓ^f divides b which, in turn, is at most $b_0(A/K)$. ∎

Lemma 4.13 *Let ℓ and λ be as in the previous lemma. If G_λ is abelian, then the inequality $\ell^2 \leq b_0\left(A^2/K\right)$ holds.*

The group H_ℓ of the following definition is the natural candidate for the image of ρ_ℓ, for $\ell \gg 0$: it is the largest (connected) group whose elements are simultaneously symplectic similitudes for the Weil pairing and contained in the centralizer of the action of E.

Definition 4.14 *Let ℓ be a good prime that does not ramify in E. We set*

$$
H_\ell = \left\{ (h_\lambda)_{\lambda|\ell} \in \prod_{\lambda|\ell} \mathrm{GL}_2(\mathbb{F}_\lambda) \;\middle|\; \det(h_{\lambda_1}) = \det(h_{\lambda_2}) \in \mathbb{F}_\ell^\times \quad \forall \lambda_1, \lambda_2|\ell \right\},
$$

where the product is over the places of E that divide ℓ.

Lemma 4.15 *If ℓ is a good prime unramified in E, the group G_ℓ is contained in H_ℓ.*

Proof. The determinant of every ρ_λ agrees with the cyclotomic character (lemma 4.5), so any two h_λ have the same determinant. ∎

To ease the notation we introduce the following definition:

Definition 4.16 *Let A/K be an abelian variety. We set*

$$
M(A/K) := b(2[K:\mathbb{Q}], 2\dim(A), 2h(A))^{1/2}.
$$

Lemma 4.17 *Let ℓ be a good prime unramified in E and let λ be a place of E above ℓ. Suppose that no $\mathrm{GL}_2(\mathbb{F}_\lambda)$-conjugate of G_λ contains $\mathrm{SL}_2(\mathbb{F}_\ell)$: then the inequality $\ell \leq M(A/K)$ holds.*

Proof. By the Dickson classification (theorem 4.10; cf. also [Ser72, §2]) we know that if G_λ does not contain $\mathrm{SL}_2(\mathbb{F}_\ell)$ (up to conjugacy in $\mathrm{GL}_2(\mathbb{F}_\lambda)$), then one of the following holds:

(I) G_λ is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\lambda)$: by definition, such a subgroup fixes a line, therefore we have $\ell \leq b_0(A/K)$ by lemma 4.12.

(II) G_λ is contained in the normalizer of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\lambda)$: let C be this Cartan subgroup and N its normalizer. By the Dickson classification, the index $[N : C]$ is 2, so the morphism

$$\mathrm{Gal}\left(\overline{K}/K\right) \to G_\lambda \to \frac{G_\lambda}{G_\lambda \cap C} \hookrightarrow \frac{N}{C}$$

induces a quadratic character of $\mathrm{Gal}\left(\overline{K}/K\right)$. Let K' be the fixed field of the kernel of this character: we have $[K' : K] \le |N/C| = 2$, and by construction the image of $\mathrm{Gal}\left(\overline{K'}/K'\right)$ in $\mathrm{Aut}\left(A[\lambda]\right)$ is contained in C. Applying lemma 4.13 to $A_{K'}$ we see that ℓ is at most $b_0 \left(A^2/K'\right)^{1/2}$.

(III) The projective image $\mathbb{P}G_\lambda$ of G_λ is a finite group of order at most 60: by lemma 4.12 we have $\ell \le b_0(A/K'')$, where K'' is the fixed field of the kernel of $\mathrm{Gal}\left(\overline{K}/K\right) \to G_\lambda \to \mathbb{P}G_\lambda$.

It is immediate to check that the three bounds we have found – namely $b_0(A/K)$, $b_0(A^2/K')^{1/2}$, and $b_0(A/K'')$ – do not exceed $M(A/K)$, and this concludes the proof. ∎

Let ℓ be a good prime unramified in E, and write $\ell \mathcal{O}_E = \prod_{i=1}^n \lambda_i$ for its factorization in $\mathcal{O}_E$. We now aim to show that, when ℓ is large enough, the group G_{λ_i} contains $\mathrm{SL}_2(\mathbb{F}_{\lambda_i})$ for every λ_i lying above ℓ. We already know that for ℓ large enough G_{λ_i} contains $\mathrm{SL}_2(\mathbb{F}_\ell)$ up to conjugacy, so we focus on this case. Fix a place λ_i of E above ℓ and let $\beta_i = [\mathbb{F}_{\lambda_i} : \mathbb{F}_\ell]$, so that ℓ^{β_i} is the order of the residue field at λ_i. Suppose that (up to conjugacy) the group G_{λ_i} contains $\mathrm{SL}_2(\mathbb{F}_\ell)$; this immediately implies that G_{λ_i} must be of type (5a) or (5b) in the notation of theorem 4.10. In this situation we have the following result:

Lemma 4.18 *Let ℓ be a good prime unramified in E, and suppose that G_{λ_i} is of type (5a) or (5b). Let α_i be the level of G_{λ_i}. There exists an extension K' of K, of degree at most 4, such that – up to conjugacy – the image of $\rho_{\lambda_i} : \mathrm{Gal}\left(\overline{K'}/K'\right) \to \mathrm{GL}_2\left(\mathbb{F}_{\lambda_i}\right)$ is contained in $\mathrm{GL}_2\left(\mathbb{F}_{\ell^{\alpha_i}}\right)$.*

Proof. Suppose first G_{λ_i} is of type (5a), generated (up to conjugacy) by $\mathrm{SL}_2\left(\mathbb{F}_{\ell^{\alpha_i}}\right)$ and by a scalar matrix $V = \mu \cdot \mathrm{Id}$. Since the determinant of any element in G_{λ_i} lies in $\mathbb{F}_\ell^\times$ we know that $\det V = \mu^2$ is an element of $\mathbb{F}_\ell$, hence $V^2 \in \mathrm{GL}_2(\mathbb{F}_\ell)$. In particular, G_{λ_i} contains a subgroup of index 2 which (up to conjugacy) is contained in $\mathrm{GL}_2(\mathbb{F}_{\ell^{\alpha_i}})$: it is the subgroup T_1 generated by $\mathrm{SL}_2\left(\mathbb{F}_{\ell^{\alpha_i}}\right)$ and V^2. One can then take K' to be the fixed field of $\rho_{\lambda_i}^{-1}(T_1)$.

On the other hand, if G_{λ_i} is of type (5b), then it contains a group of type (5a) as a subgroup of index 2. The same argument as above now shows that there exists a subgroup T_2 of G_{λ_i} that is contained in $\mathrm{GL}_2(\mathbb{F}_{\ell^{\alpha_i}})$ (up to conjugacy) and satisfies $[G_{\lambda_i} : T_2] = 4$. We can again take K' to be the fixed field of $\rho_{\lambda_i}^{-1}(T_2)$. ∎

Next we show that – at least for ℓ large enough – the level α_i must necessarily equal β_i, the degree $[\mathbb{F}_{\lambda_i} : \mathbb{F}_\ell]$:

Lemma 4.19 *Let ℓ be a good prime unramified in E. Suppose that, up to conjugacy in $\mathrm{GL}_2(\mathbb{F}_{\lambda_i})$, the group G_{λ_i} is contained in $\mathrm{GL}_2\left(\mathbb{F}_{\ell^{\alpha_i}}\right)$ for some $\alpha_i < \beta_i$. Then $\ell \le b_0(A/K)^{1/2}$.*

Proof. For every place λ of E above ℓ we can identify $A[\lambda]$ with $\mathbb{F}_\lambda^2$, and for the factor $A[\lambda_i]$ the hypothesis allows us to choose coordinates in such a way that the image of ρ_{λ_i} is contained in $\mathrm{GL}_2\left(\mathbb{F}_{\ell^{\alpha_i}}\right)$. Consider now the subspace of $A[\ell]$ given by

$$\Gamma = \left\{ (x_\lambda) \in \prod_{\lambda | \ell} A[\lambda] \cong \prod_{\lambda | \ell} \mathbb{F}_\lambda^2 \mid x_{\lambda_i} \in \left(\mathbb{F}_{\ell^{\alpha_i}}\right)^2, x_\lambda = 0 \text{ for } \lambda \ne \lambda_i \right\}.$$

By construction, Γ is Galois-stable: indeed for any $g \in \mathrm{Gal}\left(\overline{K}/K\right)$ and every $(x_\lambda) \in \Gamma$ we have

$$(\rho_\lambda(g) \cdot x_\lambda)_{\lambda_i} = \rho_{\lambda_i}(g) \cdot x_{\lambda_i} \in \left(\mathbb{F}_{\ell^{\alpha_i}}\right)^2,$$

since both the coefficients of the vector x_{λ_i} and those of the matrix $\rho_{\lambda_i}(g)$ lie in $\mathbb{F}_{\ell^{\alpha_i}}$. It follows that the abelian variety $A' = A/\Gamma$ is defined over K, and there are isogenies $\pi : A \to A'$ (the

canonical projection, of degree $\ell^{2\alpha_i}$) and $\psi : A' \to A$ (which can be chosen to be of degree at most $b_0(A/K)$). Notice now that the endomorphism $e := \psi \circ \pi \in \mathcal{O}_E$ of A kills Γ; since the action of e on $A[\lambda_i]$ is given by the class $[e]$ of e in $\mathbb{F}_{\lambda_i}$, it follows that $[e] = 0$, that is, e belongs to the ideal λ_i. Thus we see that the degree of $\psi \circ \pi$ satisfies

$$\ell^{2\beta_i} = N_{E/\mathbb{Q}}(\lambda_i)^2 \mid N_{E/\mathbb{Q}}(e)^2 \mid \deg(\psi \circ \pi) = \ell^{2\alpha_i} \deg \psi \le \ell^{2\alpha_i} b_0(A/K),$$

and therefore we have $\ell^2 \le \ell^{2(\beta_i - \alpha_i)} \le b_0(A/K)$. ∎

Combining the previous two lemmas we find

Corollary 4.20 *Let ℓ be a good prime unramified in E, and let λ be a place of E above ℓ. Suppose that the image of the representation $\rho_\lambda : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{F}_\lambda)$ does not contain $\mathrm{SL}_2(\mathbb{F}_\lambda)$: then $\ell \le M(A/K)$.*

Proof. Suppose first that no $\mathrm{GL}_2(\mathbb{F}_\lambda)$-conjugate of G_λ contains $\mathrm{SL}_2(\mathbb{F}_\ell)$: then by lemma 4.17 we have $\ell \le M(A/K)$ and we are done. We can therefore assume that G_λ contains $\mathrm{SL}_2(\mathbb{F}_\ell)$ up to conjugacy, so that in particular G_λ is of type (5a) or (5b) in the sense of theorem 4.10. Let α be the level of G_λ and $\beta = [\mathbb{F}_\lambda : \mathbb{F}_\ell]$, and notice that the hypothesis implies $\alpha < \beta$. By lemma 4.18, passing to an extension K' of K of degree at most 4 we can assume that (up to conjugacy) the image of $\rho_\lambda : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}\, A[\lambda]$ is contained in $\mathrm{GL}_2(\mathbb{F}_{\ell^\alpha})$. The corollary then follows from lemma 4.19 (applied to A/K') and the obvious inequality $b_0(A/K')^{1/2} \le b(A/K')^{1/2} < M(A/K)$. ∎

Lemma 4.21 *Let ℓ be a good prime for A and λ_1, λ_2 be two distinct places of $\mathcal{O}_E$ above ℓ. Suppose ℓ is unramified in E and the image of $\mathrm{Gal}(\overline{K}/K) \xrightarrow{\rho_{\lambda_1} \times \rho_{\lambda_2}} G_{\lambda_1} \times G_{\lambda_2}$ does not contain $\mathrm{SL}_2(\mathbb{F}_{\lambda_1}) \times \mathrm{SL}_2(\mathbb{F}_{\lambda_2})$: then $\ell \le M(A/K)$.*

Proof. Let S be the image of G_ℓ in $G_{\lambda_1} \times G_{\lambda_2}$. For the sake of simplicity write $S_i = \mathrm{SL}_2(\mathbb{F}_{\lambda_i})$ for $i = 1, 2$, set $S^1 = S \cap (S_1 \times S_2)$, and write π_1, π_2 for the two projections $S \to \mathrm{GL}_2(\mathbb{F}_{\lambda_i})$. Suppose first that $\pi_1(S)$ (resp. $\pi_2(S)$) does not contain S_1 (resp. S_2): then by corollary 4.20 we have $\ell \le M(A/K)$ and we are done. We can therefore assume that $\pi_i(S)$ contains S_i, and we claim that this implies $\pi_1(S^1) = S_1$. Indeed, under the assumption $\pi_1(S) \supseteq S_1$, for every $g_1 \in \mathrm{SL}_2(\mathbb{F}_{\lambda_1})$ there exists in S an element of the form (g_1, g_2) for some $g_2 \in G_{\lambda_2}$. On the other hand, we know from lemma 4.5 that $\det(g_2) = \det(g_1) = 1$, so (g_1, g_2) actually belongs to S^1, which therefore projects surjectively onto $\mathrm{SL}_2(\mathbb{F}_{\lambda_1}) = S_1$. The same argument also shows $\pi_2(S^1) = S_2$. Now notice that the hypotheses of the lemma imply that the inclusion $S^1 \subseteq S_1 \times S_2$ is strict, because S^1 contains $S_1 \times S_2$ if and only if S does. Since S^1 maps surjectively onto S_1 and S_2 but $S^1 \ne S_1 \times S_2$, by Goursat's lemma there exist *proper* normal subgroups N_1, N_2 (of S_1, S_2 respectively) and an isomorphism $\varphi : S_1/N_1 \to S_2/N_2$ such that S^1 projects to the graph of φ in $S_1/N_1 \times S_2/N_2$. Comparing the orders of S_1/N_1 and S_2/N_2 (or, more precisely, their valuations at ℓ) easily gives $\mathbb{F}_{\lambda_1} \cong \mathbb{F}_{\lambda_2}$. We now have all that we need to apply lemma 4.9 to the group S (notice that we have $M(A/K) > 3$ by definition, so we can safely assume $\ell \ge 5$). We find that there exist an isomorphism $f : \mathbb{F}_{\lambda_1}^2 \to \mathbb{F}_{\lambda_2}^2$, a character $\chi : S \to \{\pm 1\}$, and an automorphism σ of $\mathbb{F}_{\lambda_1} = \mathbb{F}_{\lambda_2}$ such that $g_2 = \chi((g_1, g_2))\sigma(fg_1f^{-1})$ for all (g_1, g_2) in S. Assume first that χ is the trivial character: then the subspace

$$\Gamma := \left\{ (x_\lambda) \in \prod_{\lambda \mid \ell} \mathbb{F}_\lambda^2 \cong \prod_{\lambda \mid \ell} A[\lambda] \mid x_{\lambda_2} = \sigma(fx_{\lambda_1}),\ x_\lambda = 0 \text{ for } \lambda \ne \lambda_1, \lambda_2 \right\}$$

is Galois invariant, so the abelian variety $A^* := A/\Gamma$ is defined over K. Let $\pi : A \to A^*$ be the canonical projection and $\psi : A^* \to A$ be an isogeny of degree at most $b_0(A/K)$. As in the previous lemma, we see that since $e := \psi \circ \pi \in \mathcal{O}_E$ kills Γ we must have $e \in \lambda_1$ and $e \in \lambda_2$.

Since λ_1, λ_2 are *distinct*, hence relatively prime (as ideals), this implies that $N_{E/\mathbb{Q}}(e)$ is divisible by $N_{E/\mathbb{Q}}(\lambda_1)N_{E/\mathbb{Q}}(\lambda_2)$; thus if β denotes the common degree $[\mathbb{F}_{\lambda_1} : \mathbb{F}_\ell] = [\mathbb{F}_{\lambda_2} : \mathbb{F}_\ell]$ we have

$$\ell^{4\beta} = N_{E/\mathbb{Q}}(\lambda_1\lambda_2)^2 \leq \deg e = \deg(\psi \circ \pi) = \ell^{2\beta} \deg \psi \leq \ell^{2\beta} b_0(A/K),$$

whence $\ell \leq b_0(A/K)^{1/2} \leq M(A/K)$ as desired. If, on the other hand, χ is not the trivial character, then the kernel of $\mathrm{Gal}\left(\overline{K}/K\right) \to G_\ell \to S \xrightarrow{\chi} \{\pm 1\}$ defines a quadratic extension K' of K, and repeating the same argument over K' we find $\ell \leq b_0(A/K')^{1/2} \leq M(A/K)$. ∎

We are now ready to prove theorem 1.4, whose statement we reproduce here for the reader's convenience:

Theorem 4.22 *(Theorem 1.4) Let A/K be an abelian variety of dimension g. Suppose that $\mathrm{End}_{\overline{K}}(A)$ is an order in a totally real field E of degree g over $\mathbb{Q}$ (that is, A is of GL_2-type), and that all the endomorphisms of A are defined over K. Let ℓ be a prime unramified both in K and in E and strictly larger than $\max\left\{b(A/K)^g, b(2[K:\mathbb{Q}], 2\dim(A), 2h(A))^{1/2}\right\}$: then we have*

$$G_{\ell^\infty} = \left\{x \in \mathrm{GL}_2\left(\mathcal{O}_E \otimes \mathbb{Z}_\ell\right) \mid \det_{\mathcal{O}_E} x \in \mathbb{Z}_\ell^\times\right\}.$$

Proof. Notice first that ℓ is a good prime by proposition 4.2. By lemma 4.21, the inequality $\ell > M(A/K)$ guarantees that for every pair of distinct places λ_1, λ_2 of E lying above ℓ the image of

$$\mathrm{Gal}\left(\overline{K}/K\right) \xrightarrow{\rho_{\lambda_1} \times \rho_{\lambda_2}} \mathrm{GL}_2(\mathbb{F}_{\lambda_1}) \times \mathrm{GL}_2(\mathbb{F}_{\lambda_2})$$

contains $\mathrm{SL}_2(\mathbb{F}_{\lambda_1}) \times \mathrm{SL}_2(\mathbb{F}_{\lambda_2})$. Let $S := G_\ell \cap \prod_{\lambda|\ell} \mathrm{SL}_2(\mathbb{F}_\lambda)$. By lemma 4.15 and what we just remarked we see that for every pair λ_1, λ_2 of distinct places of E dividing ℓ the group S projects surjectively onto $\mathrm{SL}_2(\mathbb{F}_{\lambda_1}) \times \mathrm{SL}_2(\mathbb{F}_{\lambda_2})$. We have $\ell \geq b(A/K) \geq 5$, so a group of the form $\mathrm{SL}_2(\mathbb{F}_\lambda)$ has no nontrivial abelian quotients (since $\mathrm{SL}_2(\mathbb{F}_\lambda)$ is quasi-simple, cf. [BHRD13, Proposition 1.10.3]): lemma 4.8 then implies $S = \prod_{\lambda|\ell} \mathrm{SL}_2(\mathbb{F}_\lambda)$, and by proposition 4.7 the group G_{ℓ^∞} contains $\mathrm{SL}_2(\mathcal{O}_E \otimes \mathbb{Z}_\ell)$. Since furthermore the map $\det_{\mathcal{O}_E \otimes \mathbb{Z}_\ell} : G_{\ell^\infty} \to \mathbb{Z}_\ell^\times$ is surjective by lemma 4.6 we conclude that G_{ℓ^∞} contains $\left\{x \in \mathrm{GL}_2\left(\mathcal{O}_E \otimes \mathbb{Z}_\ell\right) \mid \det_{\mathcal{O}_E} x \in \mathbb{Z}_\ell^\times\right\}$. The opposite inclusion is proved as in lemma 4.15, so these two groups are equal as claimed. ∎

Remark 4.23 It is not hard to show that when g is large enough we have $M(A/K) < b(A/K)^g$; in fact, $g \geq 33$ suffices.

The case of abelian surfaces follows at once:

Corollary 4.24 *(Corollary 1.5) Let A/K be an abelian surface. Suppose that $R = \mathrm{End}_{\overline{K}}(A)$ is an order in a real quadratic field E and that all the endomorphisms of A are defined over K. Let ℓ be a prime unramified both in K and in E and strictly larger than $b(2[K:\mathbb{Q}], 4, 2h(A))^{1/2}$: then we have*

$$G_{\ell^\infty} = \left\{x \in \mathrm{GL}_2\left(\mathcal{O}_E \otimes \mathbb{Z}_\ell\right) \mid \det_{\mathcal{O}_E} x \in \mathbb{Z}_\ell^\times\right\}.$$

Proof. Immediate from the previous theorem and the (easy) inequality $M(A/K) > b(A/K)^2$. ∎

5   Type II – Quaternionic multiplication

In this section we establish the surjectivity result when $R = \mathrm{End}_{\overline{K}}(A)$ is an order in an indefinite (division) quaternion algebra D over $\mathbb{Q}$, and the action of R is defined over K. We let Δ be the discriminant of R, and we fix a maximal order $\mathcal{O}_D$ of D which contains R. For the whole section we only consider primes ℓ strictly larger than $b(2[K:\mathbb{Q}], 4, 2h(A))^{1/2}$.

Remark 5.1 We know from proposition A.5 that the index $[\mathcal{O}_D : R]$ does not exceed $b(A/K)^4$. It is easy to check that $b(A/K)^4 < b(2[K:\mathbb{Q}], 4, 2h(A))^{1/2}$, and thus for all the primes ℓ we consider we have $\ell \nmid [\mathcal{O}_D : R]$.

We start by recalling a result from [BGK06], which we state only in the special case we need (abelian surfaces with quaternionic multiplication):

Theorem 5.2 *([BGK06, Theorem 5.4]) Let $\mathcal{O}_D$ be a maximal order of $\mathrm{End}_{\overline{K}}(A)$ containing R. Let ℓ be a prime dividing neither Δ nor the index $[\mathcal{O}_D : R]$. Suppose that ℓ does not divide the degree of a fixed K-polarization of A. There exists a $\mathrm{Gal}\left(\overline{K}/K\right)$-equivariant isomorphism*

$$T_\ell(A) \cong W_{\ell^\infty} \oplus W_{\ell^\infty},$$

where W_{ℓ^∞} is a simple $\mathrm{Gal}\left(\overline{K}/K\right)$-module, free of rank 2 over $\mathbb{Z}_\ell$, equipped with a nondegenerate, $\mathrm{Gal}\left(\overline{K}/K\right)$-equivariant bilinear form

$$\langle\cdot,\cdot\rangle_{QM} : W_{\ell^\infty} \times W_{\ell^\infty} \to \mathbb{Z}_\ell(1).$$

Notation. We write W_ℓ for $W_{\ell^\infty}/\ell W_{\ell^\infty}$. It is a $\mathrm{Gal}\left(\overline{K}/K\right)$-module, free of rank 2 over $\mathbb{F}_\ell$.

Theorem 5.2 says in particular that $T_\ell A$ decomposes as the direct sum of two isomorphic 2-dimensional representations. Thus choosing bases for W_{ℓ^∞} and W_ℓ we have:

Lemma 5.3 *If ℓ divides neither Δ nor $[\mathcal{O}_D : R]$, then G_ℓ can be identified with a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ acting on $A[\ell] \cong \mathbb{F}_\ell^4 \cong \mathrm{M}_2(\mathbb{F}_\ell)$ on the right. Similarly, G_{ℓ^∞} can be identified with a subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ acting on $T_\ell(A) \cong \mathbb{Z}_\ell^4 \cong \mathrm{M}_2(\mathbb{Z}_\ell)$ on the right.*

From now on we use the description of G_ℓ given by the previous lemma, namely we consider it as a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ acting on $\mathbb{F}_\ell^4$ as two copies of the standard representation.

Lemma 5.4 *Let ℓ be a prime which divides neither Δ nor $[\mathcal{O}_D : R]$. Under the above identification $T_\ell(A) \cong \mathrm{M}_2(\mathbb{Z}_\ell)$, the action of $R\otimes\mathbb{Z}_\ell \cong \mathrm{M}_2(\mathbb{Z}_\ell)$ on $T_\ell(A)$ is the natural multiplication of matrices (with $R \otimes \mathbb{Z}_\ell$ acting on the left).*

Proof. Notice first that $R \otimes \mathbb{Z}_\ell \cong \mathrm{M}_2(\mathbb{Z}_\ell)$ since $\ell \nmid \Delta$. Next by [Chi92, Theorem 7.3] we know that G_{ℓ^∞} is open in $\mathrm{GL}_2(\mathbb{Z}_\ell)$; in particular, G_{ℓ^∞} is Zariski-dense in $\mathrm{M}_2(\mathbb{Z}_\ell)$. Let φ be any element of $R\otimes\mathbb{Z}_\ell$: then G_{ℓ^∞} commutes with φ, and since the property of commuting with a fixed element is Zariski-closed we see that φ commutes with *any* element of $\mathrm{M}_2(\mathbb{Z}_\ell)$ (acting on $T_\ell(A) \cong \mathrm{M}_2(\mathbb{Z}_\ell)$ by right multiplication). Since this holds for every $\varphi \in R \otimes \mathbb{Z}_\ell$, it follows that the left action of $R\otimes\mathbb{Z}_\ell$ on $T_\ell(A)$ commutes with the right action of $\mathrm{M}_2(\mathbb{Z}_\ell)$. Since $T_\ell(A)$ is a free one-dimensional right module over $\mathrm{M}_2(\mathbb{Z}_\ell)$, this implies that φ acts on $T_\ell(A)$ as *left* multiplication by an element of $\mathrm{M}_2(\mathbb{Z}_\ell)$. ∎

Lemma 5.5 *Suppose ℓ divides neither Δ nor $[\mathcal{O}_D : R]$. If the group G_ℓ does not contain $\mathrm{SL}_2(\mathbb{F}_\ell)$ under the above identification, then $\ell \leq b(2[K : \mathbb{Q}], 4, 2h(A))^{1/2}$.*

Proof. This is a very minor variant of lemmas 4.12 and 4.13, so we only sketch the proof. If G_ℓ does not contain $\mathrm{SL}_2(\mathbb{F}_\ell)$, then Dickson's classification (theorem 4.10) implies that one of the following holds:

- G_ℓ is contained in a Borel subgroup: we can find a line $\Gamma \subseteq W_\ell$ that is stable under the action of G_ℓ. Using the previous lemma and applying an obvious variant of the argument of lemma 4.12 to the isogeny $A \to \dfrac{A}{\Gamma \oplus \Gamma}$ we find $\ell^2 \leq b_0(A/K) \leq b(A/K)$.

- The projective image of G_ℓ has cardinality at most 60: upon replacement of K with an extension of degree at most 60 we are back to the previous case, hence we find that the inequality $\ell^2 \leq b(60[K : \mathbb{Q}], 2, h(A))$ holds.

- Up to replacing K with an extension K' of degree at most 2, G_ℓ is commutative, but does not entirely consist of scalars (this case being covered by the first one). We can choose an $\alpha \in G_\ell$ which is not a scalar, and apply a variant the argument of lemma 4.13 to the isogeny given by the natural projection from $A \times A$ to its quotient by the subgroup

$$\left\{ (x_1, y_1, x_2, y_2) \in W_\ell \oplus W_\ell \oplus W_\ell \oplus W_\ell \cong A[\ell] \times A[\ell] \mid x_2 = \alpha x_1, \ y_1 = y_2 = 0 \right\}.$$

The conclusion is now $\ell^2 \leq b_0(A^2/K') \leq b(2[K:\mathbb{Q}], 4, 2h(A))$.

Comparing the various bounds thus obtained we see that $b(2[K:\mathbb{Q}], 4, 2h(A))^{1/2}$ is much larger than any of the others, thus establishing the lemma. ∎

Lemma 5.6 *Suppose ℓ is a prime that divides neither Δ nor $[\mathcal{O}_D : R]$, so that $R \otimes \mathbb{Z}_\ell \cong \mathrm{M}_2(\mathbb{Z}_\ell)$. Suppose furthermore that ℓ does not divide the degree of a minimal K-polarization of A. For every $g \in \mathrm{Gal}\left(\overline{K}/K\right)$ the determinant of $\rho_\ell(g)$, thought of as an element of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ (and not of $\mathrm{GSp}(T_\ell(A))$), is $\chi_\ell(g)$.*

Proof. This is the same argument as for elliptic curves. If we fix a basis e_1, e_2 of W_{ℓ^∞} and write $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ for the matrix representing the action of $\rho_{\ell^\infty}(g)$ in this basis, we obtain

$$\begin{aligned}
\chi_\ell(g)\langle e_1, e_2 \rangle_{QM} &= \langle \rho_{\ell^\infty}(g)e_1, \rho_{\ell^\infty}(g)e_2 \rangle_{QM} \\
&= \langle ae_1 + ce_2, be_1 + de_2 \rangle_{QM} \\
&= ad\langle e_1, e_2 \rangle + bc\langle e_2, e_1 \rangle_{QM} \\
&= (ad - bc)\langle e_1, e_2 \rangle_{QM},
\end{aligned}$$

and since $\langle e_1, e_2 \rangle_{QM}$ does not vanish we obtain $\chi_\ell(g) = (ad - bc) = \det \rho_\ell(g)$ as claimed. ∎

Theorem 5.7 *(Theorem 1.7) Let A/K be an abelian surface such that $R = \mathrm{End}_{\overline{K}}(A)$ is an order in an indefinite quaternion division algebra over $\mathbb{Q}$, and let Δ be the discriminant of R. Suppose that all the endomorphisms of A are defined over K. If ℓ is larger than $b(2[K:\mathbb{Q}], 4, 2h(A))^{1/2}$, does not divide Δ, and is unramified in K, then the equality $G_{\ell^\infty} = (R \otimes \mathbb{Z}_\ell)^\times$ holds.*

Proof. As $b(2[K:\mathbb{Q}], 4, 2h(A))^{1/2} > b(A/K)$, by [GR14a, Théorème 1] we see that ℓ does not divide the degree of a minimal polarization of A. Combining this fact with remark 5.1, we see from theorem 5.2 that there exist well-defined modules W_{ℓ^∞}, W_ℓ and a nondegenerate bilinear form $\langle \cdot, \cdot \rangle_{QM}$ on W_{ℓ^∞}.

By lemma 5.5 the inequality imposed on ℓ guarantees that G_ℓ contains $\mathrm{SL}_2(\mathbb{F}_\ell)$. It follows that G_{ℓ^∞} is a closed subgroup of $(R \otimes_\mathbb{Z} \mathbb{Z}_\ell)^\times \cong \mathrm{GL}_2(\mathbb{Z}_\ell)$ whose projection modulo ℓ contains $\mathrm{SL}_2(\mathbb{F}_\ell)$. Since we certainly have $\ell \geq 5$, it follows from lemma 2.5 that G_{ℓ^∞} contains $\mathrm{SL}_2(\mathbb{Z}_\ell)$. On the other hand, the previous lemma and the condition that ℓ is unramified in K ensure that $\det : G_{\ell^\infty} \to \mathbb{Z}_\ell^\times$ is onto, so $G_{\ell^\infty} = \mathrm{GL}_2(\mathbb{Z}_\ell)$ as claimed. ∎

Let us make a few closing remarks on this case. It is a general philosophy that – at the level of Galois representations – an abelian variety of dimension $2g$ with quaternionic multiplication by an algebra D (whose center is the number field L) should behave like two copies of an abelian variety of dimension g and endomorphism algebra L. The proof we have just given shows that this philosophy is very much correct in the case of surfaces, and indeed from lemma 5.5 onward this is virtually the same proof as for elliptic curves (cf. for example [MW93a]). Even more precisely, write the bound we obtained for a QM surface in the form $b(2[K:\mathbb{Q}], 2\dim(A), 2h(A))^{1/2}$; for an elliptic curve E/K without (potential) complex multiplication, the Galois representation is surjective onto $\mathrm{GL}_2(\mathbb{Z}_\ell)$ for every prime ℓ that does not ramify in K and is larger than $b(2[K:\mathbb{Q}], 2\dim E, 2h(E))^{1/2}$ (cf. [MW93a]), which is formally the same expression. On the other hand, the actual numerical dependence of the present result on the height of A is much worse than the analogous one for elliptic curves, due to the strong dependence of the function $b([K:\mathbb{Q}], \dim A, h(A))$ on the parameter $\dim A$.

Remark 5.8 In the light of this discussion, it is reasonable to think that the methods of [Lom15b] might be generalized to give results on the index of the *adelic* representation attached to A. We do not attempt this here, for doing so would entail giving a classification of the integral Lie subalgebras of *any* $\mathbb{Z}_\ell$-form of $\mathfrak{sl}_2$: indeed, these algebras appear when we try to study the precise structure of G_{ℓ^∞} for those ℓ that divide Δ. Such a classification task seems rather daunting, given that the easier problem of studying the $\mathbb{Q}_\ell$-forms of $\mathfrak{sl}_2$ is already highly nontrivial.

A The index of the endomorphism ring

Let A/K be an absolutely simple abelian variety. Its endomorphism ring $R = \operatorname{End}_{\overline{K}}(A)$ is an order in a finite-dimensional division algebra D over $\mathbb{Q}$, and we are interested in giving a bound on the index of R in any maximal order $\mathcal{O}_D$ containing it. Note that when D is a field there is a unique maximal order, namely its ring of integers, but when D is not commutative the index $[\mathcal{O}_D : R]$ might a priori depend on the choice of $\mathcal{O}_D$. The following proposition shows that this is not the case:

Proposition A.1 *Let L be a number field, D a central simple algebra over L, and R an order of D. Let $\mathcal{O}_D$ be a maximal order in D containing R. The index $[\mathcal{O}_D : R]$ does not depend on the choice of $\mathcal{O}_D$.*

Proof. Note first that any maximal order of D is stable under multiplication by $\mathcal{O}_L$ (indeed if S is a subring of D then the $\mathcal{O}_L$-module generated by S is again a subring of D), so the order R' generated by R and $\mathcal{O}_L$ is again contained in $\mathcal{O}_D$. We have $[\mathcal{O}_D : R] = [\mathcal{O}_D : R'][R' : R]$, and since $[R' : R]$ clearly does not depend on $\mathcal{O}_D$ we can assume that $R = R'$, i.e. that R is an $\mathcal{O}_L$-order. Under this additional assumption we have

$$\mathcal{O}_D/R \cong \bigoplus_{v \text{ finite place of } L} \frac{\mathcal{O}_D \otimes_{\mathcal{O}_L} \mathcal{O}_{Lv}}{R \otimes_{\mathcal{O}_L} \mathcal{O}_{Lv}},$$

so that $[\mathcal{O}_D : R] = \prod_{v \text{ finite place of } L}[\mathcal{O}_D \otimes \mathcal{O}_{Lv} : R_v]$, where $R_v = R \otimes_{\mathcal{O}_L} \mathcal{O}_{Lv}$. The order $\mathcal{O}_D \otimes \mathcal{O}_{Lv}$ is maximal in $\mathcal{O}_D \otimes L_v$ ([Rei03, Corollary 11.2 and Theorem 11.5]), so it is enough to prove that at every finite place the index $[\mathcal{O}_D \otimes \mathcal{O}_{Lv} : R_v]$ is independent of the choice of $\mathcal{O}_D$. We are thus reduced to the complete local case: by Theorem 17.3 of [Rei03] all maximal orders in $\mathcal{O}_D \otimes L_v$ are conjugated. We now write the index $[\mathcal{O}_D \otimes \mathcal{O}_{Lv} : R_v]$ as the ratio $\dfrac{\operatorname{covol}(R_v)}{\operatorname{covol}(\mathcal{O}_D \otimes \mathcal{O}_{Lv})}$, where the covolume is taken with respect to any Haar measure (on $\mathcal{O}_D \otimes L_v$): as the Haar measure is invariant under conjugation, this quantity does not depend on $\mathcal{O}_D$. ∎

In order to simplify matters it is convenient to assume that all the endomorphisms of A are defined over K. This condition is completely harmless, since it can be achieved at the expenses of a controllable extension of K:

Lemma A.2 *([Sil92, Theorem 4.1]) There exists a number field K', with $[K' : K]$ bounded only in terms of $g = \dim(A)$, such that all the endomorphisms of A are defined over K'. We can take $[K' : K] \leq 2 \cdot (9g)^{2g}$.*

From now on we will therefore assume that all the endomorphisms of A are defined over K. In order to get estimates in the case of noncommutative endomorphism algebras we will need the following lemma, which is essentially [Wil98, Proposition 2.5.4]: even though the latter was stated only for commutative endormorphism rings, the proof works equally well in the general case.

Lemma A.3 *([Wil98, Proposition 2.5.4]) Let D be a division algebra, $R \subseteq S$ be orders in D and A/K be an abelian variety with $\operatorname{End}_K(A) = R$. There exists an abelian variety B/K, isogenous to A over K, such that $\operatorname{End}_K(B) \supseteq S$.*

Corollary A.4 *Let A/K be an abelian variety with endomorphism ring R. Write $D = R \otimes \mathbb{Q}$, and let $\mathcal{O}_D$ be any maximal order of D containing R. Suppose that all the endomorphisms of A are defined over K. There exists an abelian variety A'/K and two isogenies $\varepsilon_1 : A \to A', \varepsilon_2 : A' \to A$, defined over K, such that $\mathrm{End}_K(A') = \mathcal{O}_D$ and $\max\{\deg(\varepsilon_1), \deg(\varepsilon_2)\} \leq b(A/K)$.*

Proof. Lemma A.3 shows the existence of a K-variety A' having $\mathcal{O}_D$ as its endomorphism ring, so the claim follows from [GR14a, Theorem 1.4] (which is a symmetric version of theorem 2.2, bounding the degrees of minimal isogenies both from A to A' and from A' to A). ∎

We can now deduce the desired bound on $[\mathcal{O}_D : R]$:

Proposition A.5 *The inequality $[\mathcal{O}_D : R] \leq b(A/K)^{\dim_{\mathbb{Q}}(D)}$ holds.*

Proof. Let $A', \varepsilon_1, \varepsilon_2$ be as in the above corollary. Consider the following linear map:

$$\varphi : \quad \mathrm{End}_K(A') \quad \to \quad \mathrm{End}_K(A) \quad \hookrightarrow \quad \mathrm{End}_K(A')$$
$$e \quad \mapsto \quad \varepsilon_2 \circ e \circ \varepsilon_1,$$

where the second embedding is given by the fact that $R = \mathrm{End}_K(A)$ is an order in D and $\mathrm{End}_K(A') = \mathcal{O}_D$ is a maximal order containing R. Note that $\mathrm{End}_K(A)$ is endowed with a positive-definite quadratic form given by the degree. We consider both $\mathrm{End}_K(A)$ and $\mathrm{End}_K(A')$ as lattices sitting inside $D_{\mathbb{R}} = \mathrm{End}_K(A') \otimes_{\mathbb{Z}} \mathbb{R}$, and observe that the degree map extends naturally to a positive-definite quadratic form on $D_{\mathbb{R}}$. This makes $D_{\mathbb{R}}$ into an Euclidean space, which in particular comes equipped with a natural (Lebesgue) measure. Denote by r the $\mathbb{R}$-dimension of $D_{\mathbb{R}}$, which is also the dimension of D as a $\mathbb{Q}$-vector space. Since the equality $\deg(e_1 \circ e_2) = \deg(e_1) \cdot \deg(e_2)$ holds for any pair of isogenies between abelian varieties, we have

$$\deg(\varphi(e)) = \deg(\varepsilon_2 \circ e \circ \varepsilon_1) = \deg(\varepsilon_1)\deg(\varepsilon_2)\deg(e) \leq b(A/K)^2 \deg(e).$$

Extend φ by linearity to an endomorphism of $D_{\mathbb{R}}$ (which we still denote by φ) and fix a deg-orthonormal basis $\gamma_1, \ldots, \gamma_r$ of $D_{\mathbb{R}}$. By construction the inclusion $\varphi(\mathcal{O}_D) \subseteq R$ holds, so we have the inequality

$$[\mathcal{O}_D : R] = \frac{\mathrm{covol}(R)}{\mathrm{covol}(\mathcal{O}_D)} \leq \frac{\mathrm{covol}(\varphi(\mathcal{O}_D))}{\mathrm{covol}(\mathcal{O}_D)} = \frac{\det(\varphi)\,\mathrm{covol}(\mathcal{O}_D)}{\mathrm{covol}(\mathcal{O}_D)} = \det(\varphi).$$

Write $\varphi(\gamma_i) = \sum_{j=1}^{r} a_{ij}\gamma_j$ with $a_{ij} \in \mathbb{R}$ for the matrix representing φ in the basis of the γ_j. Let $\lambda(\cdot, \cdot)$ be the bilinear form associated with deg. Using the inequality $\deg(\varphi(e)) \leq b(A/K)^2 \deg(e)$ we deduce

$$\deg\left(\sum_j a_{ij}\gamma_j\right) = \deg(\varphi(\gamma_i)) \leq b(A/K)^2 \deg(\gamma_i) = b(A/K)^2 \quad \forall i = 1, \ldots, r,$$

so

$$b(A/K)^2 \geq \lambda\left(\sum_j a_{ij}\gamma_j, \sum_k a_{ik}\gamma_k\right) = \sum_{j,k} a_{ij}a_{ik}\lambda(\gamma_j, \gamma_k) = \sum_j a_{ij}^2 \quad \forall i = 1, \ldots, r :$$

equivalently, the L^2-norm of each row of the matrix (a_{ij}) is bounded by $b(A/K)$. Hadamard's inequality then gives

$$[\mathcal{O}_D : R] \leq \det(\varphi) \leq \prod_{i=1}^{r} \|a_i\|_{L^2} \leq b(A/K)^r,$$

which is the desired estimate. ∎

References

[Asc84]   M. Aschbacher. On the maximal subgroups of the finite classical groups. *Invent. Math.*, 76(3):469–514, 1984.

[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.*, (Extra Vol.):35–75 (electronic), 2006.

[BHRD13] J. N. Bray, D. F. Holt, and C. M. Roney-Dougal. *The maximal subgroups of the low-dimensional finite classical groups*, volume 407 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2013. With a foreword by Martin Liebeck.

[BL04]   C. Birkenhake and H. Lange. *Complex Abelian Varieties*. Springer, 2004.

[Blo67]   D. M. Bloom. The subgroups of PSL(3, q) for odd q. *Trans. Amer. Math. Soc.*, 127:150–178, 1967.

[Chi92]   W. C. Chi. ℓ-adic and λ-adic representations associated to abelian varieties defined over number fields. *Amer. J. Math.*, 114(2):315–353, 1992.

[Die02]   L. V. Dieulefait. Explicit determination of the images of the Galois representations attached to abelian surfaces with $\mathrm{End}(A) = \mathbb{Z}$. *Experiment. Math.*, 11(4):503–512 (2003), 2002.

[DR04]   L. V. Dieulefait and V. Rotger. The arithmetic of QM-abelian surfaces through their Galois representations. *J. Algebra*, 281(1):124–143, 2004.

[GP12]   E. Ghate and P. Parent. On uniform large Galois images for modular abelian varieties. *Bull. Lond. Math. Soc.*, 44(6):1169–1181, 2012.

[GR14a]   É. Gaudron and G. Rémond. Polarisations et isogénies. *Duke Math. J.*, 163(11):2057–2108, 2014.

[GR14b]   É. Gaudron and G. Rémond. Théorème des périodes et degrés minimaux d'isogénies. *Comment. Math. Helv.*, 89(2):343–403, 2014.

[Gro]   A. Grothendieck. Modèles de Néron et monodromie. In *Séminaire de Géométrie Algébrique, Volume 7, Esposé 9*.

[Hal11]   C. Hall. An open-image theorem for a general class of abelian varieties. *Bull. Lond. Math. Soc.*, 43(4):703–711, 2011. With an appendix by Emmanuel Kowalski.

[Jac74]   M. I. Jacobson. Variétés abéliennes de dimension deux ayant pour algèbre d'endomorphismes une algèbre de quaternions indéfinie (in Russian). *Uspekhi Mat. Nauk*, 29:185–186, 1974.

[JR10]   R. Jones and J. Rouse. Galois theory of iterated endomorphisms. *Proc. Lond. Math. Soc. (3)*, 100(3):763–794, 2010. Appendix A by Jeffrey D. Achter.

[Kaw03]   T. Kawamura. The effective surjectivity of mod ℓ Galois representations of 1- and 2-dimensional abelian varieties with trivial endomorphism ring. *Comment. Math. Helv.*, 78(3):486–493, 2003.

[KW09a]   C. Khare and J.-P. Wintenberger. Serre's modularity conjecture. I. *Invent. Math.*, 178(3):485–504, 2009.

[KW09b]   C. Khare and J.-P. Wintenberger. Serre's modularity conjecture. II. *Invent. Math.*, 178(3):505–586, 2009.

[Lom15a]   D. Lombardo. An explicit open image theorem for products of elliptic curves. *ArXiv e-prints*, January 2015.

[Lom15b]   D. Lombardo. Bounds for Serre's open image theorem for elliptic curves over number fields. *Algebra & Number Theory*, 9-10:2347–2395, 2015.

[Lom15c]   D. Lombardo. Galois representations attached to abelian varieties of CM type. *ArXiv e-prints*, June 2015.

[LV14]   E. Larson and D. Vaintrob. Determinants of subquotients of Galois representations associated with abelian varieties. *J. Inst. Math. Jussieu*, 13(3):517–559, 2014. With an appendix by B. Conrad.

[Mit14]   H. H. Mitchell. The subgroups of the quaternary abelian linear group. *Trans. Amer. Math. Soc.*, 15(4):379–396, 1914.

[Mum70]   D. Mumford. Abelian varieties. In *Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research*, 1970.

[MW93a]   D. W. Masser and G. Wüstholz. Galois properties of division fields of elliptic curves. *Bull. London Math. Soc.*, 25(3):247–254, 1993.

[MW93b]   D. W. Masser and G. Wüstholz. Isogeny estimates for abelian varieties, and finiteness theorems. *Ann. of Math. (2)*, 137(3):459–472, 1993.

[MW93c]   D. W. Masser and G. Wüstholz. Periods and minimal abelian subvarieties. *Ann. of Math. (2)*, 137(2):407–458, 1993.

[Oht74]   M. 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.

[Pin98]   R. Pink. ℓ-adic algebraic monodromy groups, cocharacters, and the Mumford-Tate conjecture. *J. reine angew. Math*, (495), 1998.

[Ray74]   M. Raynaud. Schémas en groupes de type $(p, \ldots, p)$. *Bull. Soc. Math. France*, 102:241–280, 1974.

[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.

[Rib76]   K. A. Ribet. Galois action on division points of Abelian varieties with real multiplications. *Amer. J. Math.*, 98(3):751–804, 1976.

[Rib97]   K. A. Ribet. Images of semistable Galois representations. *Pacific J. Math.*, Special Issue:277–297, 1997. Olga Taussky-Todd: in memoriam.

[Ser72]   J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Ser86]   J.-P. Serre. Résumé des cours de 1985-1986, Annuaire du Collège de France, 1986.

[Ser00]   J.-P. Serre. Letter to M-F. Vigneras, January 1st, 1983. In *Œuvres. Collected papers. IV.* Springer-Verlag, Berlin, 2000.

[Sil92]   A. Silverberg. Fields of definition for homomorphisms of abelian varieties. *J. Pure Appl. Algebra*, 77(3):253–262, 1992.

[Web05]   B. S. Webb, editor. *Surveys in combinatorics 2005*, volume 327 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2005. Papers from the 20th British Combinatorial Conference held at the University of Durham, Durham, July 10–15, 2005.

[Wil98]   J. Wilson. Curves of genus 2 with real multiplication by a square root of 5. *PhD Thesis*, 1998. Available at `http://eprints.maths.ox.ac.uk/32/`.

[Zyw15]   D. Zywina. An explicit Jacobian of dimension 3 with maximal Galois action. *ArXiv e-prints*, August 2015.