Selecta Mathematica (2024) 30:18
https://doi.org/10.1007/s00029-023-00908-0

Selecta Mathematica
New Series

On the local-global principle for isogenies of abelian surfaces

Davide Lombardo[1] · **Matteo Verzobio**[2]

Accepted: 10 December 2023
© The Author(s) 2024

Abstract
Let ℓ be a prime number. We classify the subgroups G of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ and $\mathrm{GSp}_4(\mathbb{F}_\ell)$ that act irreducibly on $\mathbb{F}_\ell^4$, but such that every element of G fixes an $\mathbb{F}_\ell$-vector subspace of dimension 1. We use this classification to prove that a local-global principle for isogenies of degree ℓ between abelian surfaces over number fields holds in many cases—in particular, whenever the abelian surface has non-trivial endomorphisms and ℓ is large enough with respect to the field of definition. Finally, we prove that there exist arbitrarily large primes ℓ for which some abelian surface $A/\mathbb{Q}$ fails the local-global principle for isogenies of degree ℓ.

Keywords Local-global principle · Abelian surfaces · Galois representations · Isogeny · Matrix groups

Mathematics Subject Classification Primary 11F80; Secondary 20C33 · 14K15 · 11G10

1 Introduction

Let K be a number field and A be an abelian variety over K. For all primes v of K we denote by $\mathbb{F}_v$ the residue field at v, and—if A has good reduction at v—we write A_v for the reduction of A modulo v. If A/K has some kind of global level structure (say, a K-rational isogeny or a K-rational torsion point), then so do all the reductions A_v. Local-global principles ask about the converse: if A_v has some level structure for (almost) all v, is the same true for A/K? A question of this form was first raised

✉ Davide Lombardo
davide.lombardo@unipi.it

Matteo Verzobio
matteo.verzobio@gmail.com

[1] Dipartimento di Matematica, Università di Pisa, Largo Bruno Pontecorvo 5, Pisa, Italy

[2] IST Austria, Am Campus 1, Klosterneuburg, Austria

Published online: 26 January 2024

by Katz [12], who considered the property $|E(K)_{\text{tors}}| \equiv 0 \pmod{m}$ when E is an elliptic curve and m is a fixed positive integer (if $m = \ell$ is prime, this is equivalent to asking that $E(K)$ contains a non-trivial ℓ-torsion point). He showed that this property does not satisfy the local-global principle, but also proved [12, Theorem 2] that, if $|E(K_v)_{\text{tors}}| \equiv 0 \pmod{m}$ for almost all v, then E is isogenous over K to an elliptic curve E' with $|E'(K)_{\text{tors}}| \equiv 0 \pmod{m}$.

Seen in this light, the local-global principle for the existence of isogenies is perhaps more natural, because the existence of isogenies is itself an isogeny invariant. In this paper, we consider in particular the local-global problem for (prime-degree) isogenies of abelian surfaces. The analogous question for abelian varieties of dimension one, namely elliptic curves, has received much attention in recent years [1, 3, 29, 31], and is now essentially well-understood. In the setting of abelian surfaces much less is known: the recent work [2] gives examples showing that the local-global principle does not always hold, even for abelian surfaces over $\mathbb{Q}$, but no general theory seems to have been developed to study this phenomenon. In the present work, we address completely the group-theoretic aspects of the question and make significant progress on its arithmetic aspects. Formally, the question we consider may be stated as follows:

Question 1.1 Let A/K be an abelian surface and let ℓ be a prime number. Suppose that, for all places v of K with at most finitely many exceptions, the abelian variety A_v admits an ℓ-isogeny defined over $\mathbb{F}_v$.

- Does A admit an ℓ-isogeny defined over K?
- Less restrictively, is the group of ℓ-torsion points $A[\ell]$ reducible as a $\text{Gal}\left(\overline{K}/K\right)$-module?

We will say that the pair (A, ℓ) is a **weak counterexample** (to the local-global principle for cyclic isogenies) if A does not admit any ℓ-isogenies defined over K, but for all places v of K (with at most finitely many exceptions) the abelian variety A_v admits an ℓ-isogeny defined over $\mathbb{F}_v$. We say that (A, ℓ) is a **strong counterexample** if, in addition, $A[\ell]$ is an irreducible $\text{Gal}(\overline{K}/K)$-module.

Question 1.1 may be reformulated in the language of Galois representations. The group $A[\ell]$ of ℓ-torsion points of $A(\overline{K})$ is an $\mathbb{F}_\ell$-vector space of dimension 4, and there is an action of $G_K := \text{Gal}\left(\overline{K}/K\right)$ on $A[\ell]$, which we denote by $\rho_\ell : G_K \to \text{Aut}(A[\ell])$. Let v be a place of K of characteristic $\neq \ell$ at which A has good reduction. The representation ρ_ℓ is then unramified at ℓ. Choosing a Frobenius element at v, denoted by $\text{Frob}_v \in G_K$, the condition that A_v admits an ℓ-isogeny defined over $\mathbb{F}_v$ may be interpreted as the condition that $\rho_\ell(\text{Frob}_v)$ acts on $A[\ell] \cong \mathbb{F}_\ell^4$ fixing an $\mathbb{F}_\ell$-line. By Chebotarev's theorem, every element in the finite group $G_\ell = \rho_\ell(G_K)$ is of the form Frob_v for infinitely many places v, so we arrive at the following characterisation (see also [1, 29]):

Lemma 1.2 *The pair (A, ℓ) is a weak counterexample if and only if the action of G_ℓ on $A[\ell]$ leaves no line invariant, but every $g \in G_\ell$ admits an $\mathbb{F}_\ell$-rational eigenvalue. Moreover, (A, ℓ) is a strong counterexample if and only if the action of G_ℓ on $A[\ell]$ is irreducible, but every $g \in G_\ell$ admits an $\mathbb{F}_\ell$-rational eigenvalue.*

Thus, the study of the local-global principle for isogenies of abelian surfaces naturally splits into two sub-problems:

(1) characterise the subgroups G of $\mathrm{GL}_4(\mathbb{F}_\ell)$ having the properties described in Lemma 1.2 (we will call *Hasse subgroups* the groups corresponding to strong counterexamples, see Definition 3.1). We will show below that, if one is only interested in strong counterexamples, it suffices to classify the Hasse subgroups of the smaller group $\mathrm{GSp}_4(\mathbb{F}_\ell)$, the general symplectic group with respect to a suitable antisymmetric bilinear form (cf. Corollary 2.5).
(2) understand whether these groups may in fact arise as the image of the mod-ℓ Galois representation attached to some abelian surface over a fixed number field K.

Concerning (1), previous work [6] claims to give a classification of the (maximal) Hasse subgroups of $\mathrm{Sp}_4(\mathbb{F}_\ell)$, and that this classification may be extended easily to $\mathrm{GSp}_4(\mathbb{F}_\ell)$. Unfortunately, it seems that there are several problems with the arguments in that paper: at the beginning of our investigations, we used the algebra software MAGMA to explicitly list the maximal Hasse subgroups of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ for several small primes ℓ, and found that the results did not agree with the main theorem of [6]. Moreover, it was not clear to us how to obtain the classification of Hasse subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ starting from the corresponding classification for $\mathrm{Sp}_4(\mathbb{F}_\ell)$. Concerning (2), in the case of elliptic curves [1] shows that—for a fixed number field K—there are only finitely many primes ℓ for which there exists an elliptic curve E/K such that (E, ℓ) is a counterexample to the local-global principle for isogenies. One of our main motivations for the present work was the desire to understand to what extent the same holds for abelian surfaces.

In this paper, we make progress on both sub-problems (1) and (2), focusing on *strong* counterexamples. One reason for this choice comes from group theory: if (A, ℓ) is merely a weak counterexample (and not a strong one), $A[\ell]$ admits a 2-dimensional irreducible subspace. Up to semi-simplification, G_ℓ is then contained in $\mathrm{GL}_2(\mathbb{F}_\ell) \times \mathrm{GL}_2(\mathbb{F}_\ell)$, so (from the group-theoretic point of view) in this case one can to a certain extent rely on the study of Hasse subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$, see [1, 29] and especially [2] for the case of $\mathrm{GL}_2(\mathbb{F}_\ell) \times \mathrm{GL}_2(\mathbb{F}_\ell)$. Another reason is the obvious point that strong counterexamples constitute a more substantial violation of the local-global principle than weak ones.

We now describe our main results, starting with group theory. In Theorem 3.2 we classify the maximal Hasse subgroups of $\mathrm{Sp}_4(\mathbb{F}_\ell)$, correcting and completing the arguments in [6]. Notice that the list given in Table 1, which agrees with our computations in MAGMA for all primes up to 100, is significantly different from the table of Theorem 1 in [6]. In particular, our results justify Remarks 2.6 and 2.7 in [2]. Secondly, we use this result, combined with several additional arguments, to obtain a classification of the maximal Hasse subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ (see Theorem 5.5). Together, these results completely settle the group-theoretic sub-problem (1).

Concerning the more genuinely arithmetic problem (2), we formulate a conjecture about the 'uniform boundedness of counterexamples' in the setting of abelian surfaces (see Conjecture 2.2) and make some progress towards establishing it. In particular, we obtain several restrictions on the existence of strong counterexamples, depending on the endomorphism algebra of A (see Sect. 6). We summarise some consequences of this analysis in the following corollary; see Theorem 6.1 for a more detailed statement.

Corollary 1.3 (Corollary 6.2) *Let K be a number field. There exists a constant $C = C(K)$, depending only on K, such that the following holds: there exists no strong counterexample (A, ℓ) where A/K is an abelian surface with $\mathrm{End}_K(A) \neq \mathbb{Z}$ and $\ell > C$. The constant C can be taken to be $\max\{2^9 \cdot 3^3 \cdot 5^2 \cdot [K : \mathbb{Q}] + 1, \Delta_K\}$, where Δ_K is the discriminant of K.*

We also show that *semistable* abelian surfaces over the rational numbers (and other number fields of small discriminant) do not yield any strong counterexamples for any prime ℓ, with the possible exception of the prime 5:

Theorem 1.4 (Theorem 6.31) *Let K be a number field such that every non-trivial extension L/K ramifies at least at one finite place (for example $K = \mathbb{Q}$). Let A/K be a semistable abelian surface and let $\ell \neq 5$ be a prime. The pair $(A/K, \ell)$ is not a strong counterexample to the local-global principle for isogenies.*

On the other hand, we also show that—if one does not make any assumptions on the endomorphism ring—there exist strong counterexamples $(A/\mathbb{Q}, \ell)$ with ℓ unbounded:

Proposition 1.5 (Proposition 6.28) *Let $\ell > 5$ be a prime with $\ell \equiv 5 \pmod 8$. There exists an abelian surface A, defined over $\mathbb{Q}$ and geometrically isogenous to the square of a CM elliptic curve, such that (A, ℓ) is a strong counterexample.*

Thus, the situation for abelian surfaces is strikingly different from that of elliptic curves, for which [1] provides a uniform bound for every fixed number field. In addition to showing that no such uniform bound exists in the case of abelian surfaces, Proposition 6.28 is significant also for another reason, namely, it helps explaining where the difficulty lies in proving Conjecture 2.2. Indeed, the latter is a statement about Galois representations, and in order to prove it one should in particular show that—for ℓ large enough—the mod-ℓ Galois representation attached to a non-CM abelian surface A/K is non-isomorphic to the Galois representation attached to certain CM abelian surfaces. This is a notoriously difficult problem, so we suspect that a full solution to Conjecture 2.2 is out of reach at present.

Computer calculations. While writing this paper, we have often relied on the computer algebra software MAGMA to double-check our results. However, our proofs are independent of computer calculations, except for the precise list of groups given in Table 1 and for the proof of Theorem A.1 in the Appendix. All the MAGMA scripts to verify these results are available online [19]. The same repository also contains tables of the maximal Hasse subgroups of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ for $\ell < 100$. These tables are obtained by a direct computation independent of the results in this paper, and agree in all cases with Table 1.

1.1 Notation

Throughout the paper, K denotes a number field and A an abelian surface over K. We write G_K for the absolute Galois group of K, and denote by G_ℓ the image of the natural Galois representation

$$\rho_\ell : G_K \to \mathrm{Aut}(A[\ell]),$$

where we will usually fix an $\mathbb{F}_\ell$-basis of $A[\ell]$ and therefore identify $\mathrm{Aut}(A[\ell])$ with $\mathrm{GL}_4(\mathbb{F}_\ell)$. We let $\chi_\ell : G_K \to \mathbb{F}_\ell^\times$ denote the mod-ℓ cyclotomic character.

Let k be a field and n be a positive integer. For a subgroup G of $\mathrm{GL}_n(k)$, we denote by $\mathbb{P}G$ the image of G under the canonical projection $\mathrm{GL}_n(k) \to \mathrm{PGL}_n(k)$. Given a matrix $M \in \mathrm{GL}_n(k)$, we write M^{-T} for the inverse of the transpose of M. As is well-known, this is also the transpose of the inverse of M.

We say that a matrix $M \in \mathrm{GL}_4(\mathbb{F}_\ell)$ is **block-diagonal** if it is of the form $M = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$ with $x, y \in \mathrm{GL}_2(\mathbb{F}_\ell)$. If M is block-diagonal and x and y are scalar multiples of the identity, then we say that M is **block-scalar**. Moreover, we say that M is **block-anti-diagonal** if it is of the form $M = \begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix}$ with $x, y \in \mathrm{GL}_2(\mathbb{F}_\ell)$.

Definition 1.6 For a choice of a symplectic form on $\mathbb{F}_\ell^4$, represented by a matrix J, we set

$$\mathrm{GSp}_4(\mathbb{F}_\ell) = \left\{ M \in \mathrm{GL}_4(\mathbb{F}_\ell) \mid \exists k \in \mathbb{F}_\ell^\times \text{ such that } M^T J M = kJ \right\}.$$

Given $M \in \mathrm{GSp}_4(\mathbb{F}_\ell)$, there is a unique $k \in \mathbb{F}_\ell^\times$ such that $M^T J M = kJ$: we call it the **multiplier** of M, and denote it by $\lambda(M)$. The map $M \mapsto \lambda(M)$ is a group homomorphism, whose kernel is denoted $\mathrm{Sp}_4(\mathbb{F}_\ell)$.

We will use several choices of symplectic forms. The two main ones correspond to the matrices

$$\begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \tag{1}$$

and

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}. \tag{2}$$

1.2 Structure of the paper

In Sect. 2 we collect some preliminary observations about counterexamples to the local-global principle for isogenies between abelian surfaces and formulate a conjecture about the boundedness of counterexamples for a given number field. We also briefly review some well-known facts about $\mathrm{GL}_2(\mathbb{F}_\ell)$ and its subgroups. In Sect. 3 we classify the maximal Hasse subgroups of $\mathrm{Sp}_4(\mathbb{F}_\ell)$, and in Sect. 4 we study the Hasse subgroups H of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ with the property that $H \cap \mathrm{Sp}_4(\mathbb{F}_\ell)$ acts reducibly. Combining these results, in Sect. 5 we obtain a classification of the maximal Hasse subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$. Finally, Sect. 6 contains our main arithmetical results about

abelian surfaces: we give sufficient conditions (in terms of the field of definition of the endomorphisms of A) that ensure that (A, ℓ) is not a strong counterexample, and provide an infinite family of counterexamples $(A/\mathbb{Q}, \ell)$ with ℓ unbounded.

2 Preliminaries

2.1 Endomorphism rings and algebraic monodromy groups

Let A be an abelian surface over a number field K. By the classification of the geometric endomorphism algebras of abelian surfaces, one of the following holds:

(1) A is geometrically irreducible:

- (a) Trivial endomorphisms: $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$.
- (b) Real multiplication: $\mathrm{End}_{\overline{K}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a real quadratic field.
- (c) Quaternion multiplication: $\mathrm{End}_{\overline{K}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a non-split quaternion algebra over $\mathbb{Q}$.
- (d) Complex multiplication: $\mathrm{End}_{\overline{K}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a quartic CM field.

(2) A is geometrically reducible:

- (e) $A_{\overline{K}}$ is isogenous to the product of two non-isogenous elliptic curves E_1 and E_2. This gives rise to three sub-cases, according to whether none, one, or both of E_1, E_2 have CM.
- (f) $A_{\overline{K}}$ is isogenous to the square of an elliptic curve without CM.
- (g) $A_{\overline{K}}$ is isogenous to the square of an elliptic curve with CM.

We now describe certain predictions on strong counterexamples $(A/K, \ell)$ that follow from well-established conjectures on Galois representations. Denote by $T_\ell A = \varprojlim_n A[\ell^n]$ the ℓ-adic Tate module of A, and by $\mathcal{G}_\ell$ the ℓ-adic monodromy group of A, namely, the Zariski closure inside $\mathrm{GL}_{T_\ell(A)\otimes\mathbb{Q}_\ell}$ of the image of the ℓ-adic Galois representation $\mathrm{Gal}\left(\overline{K}/K\right) \xrightarrow{\rho_{\ell^\infty}} \mathrm{Aut}(T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)$. The endomorphism ring of $A_{\overline{K}}$ determines the structure of $\mathcal{G}_\ell^0$, the connected component of the identity, see [8]. In particular, the dimension of $\mathcal{G}_\ell^0$ is as follows:

Case	(a)	(b)	(c)	(d)	(e)	(f)	(g)
$\dim \mathcal{G}_\ell^0$	11	7	4	3	7 or 5 or 3	4	2

where the three possibilities in (e) correspond to the three sub-cases listed above. By general conjectures on Galois representations, one expects $|G_\ell|$ to differ at most by a fixed multiplicative constant from $[\mathcal{G}_\ell : \mathcal{G}_\ell^0]\ell^{\dim \mathcal{G}_\ell^0}$. More precisely, G_ℓ is by definition a subgroup of $\mathcal{G}_\ell(\mathbb{F}_\ell)$, which for $\ell > 2$ is a group of order $[\mathcal{G}_\ell : \mathcal{G}_\ell^0] \cdot |\mathcal{G}_\ell^0(\mathbb{F}_\ell)|$, and one knows that asymptotically $|\mathcal{G}_\ell^0(\mathbb{F}_\ell)| \sim \ell^{\dim \mathcal{G}_\ell^0}$, see [11, Proposition 2.2]. In particular,

we see that the ratio

$$\frac{|G_\ell|}{[\mathcal{G}_\ell : \mathcal{G}_\ell^0] \cdot \ell^{\dim \mathcal{G}_\ell^0}}$$

is bounded above by a universal constant; it is also bounded away from zero because the Mumford-Tate conjecture holds for abelian surfaces (see [24] for the case of geometrically simple abelian surfaces and [16] and the references there for the case of a product of two elliptic curves). One may then conjecture that, for a fixed number field K, there exists a uniform lower bound $c(K)$ such that for *every* abelian surface A/K and every prime ℓ we have

$$|G_\ell| \geq c(K) \cdot [\mathcal{G}_\ell : \mathcal{G}_\ell^0] \cdot \ell^{\dim \mathcal{G}_\ell^0}. \tag{3}$$

Remark 2.1 This conjecture does not seem to appear in print in this form. However, at least in the case of abelian surfaces, the results of [14, 15, 17] imply that the existence of $c(K)$ would follow from the uniform boundedness of the degrees of minimal isogenies for abelian varieties of a fixed dimension over a number field of fixed degree. This latter statement has been conjectured by many authors, and is closely related to many other well-known uniformity conjectures, see [25].

On the other hand, if $(A/K, \ell)$ is a strong counterexample to the local-global principle for cyclic isogenies of abelian surfaces, Lemma 1.2 and Theorem 5.5 show that $|G_\ell|$ is bounded above by an absolute constant f times ℓ^3: if we assume that (3) holds, we obtain

$$f \cdot \ell^3 \geq |G_\ell| \geq c(K) \cdot [\mathcal{G}_\ell : \mathcal{G}_\ell^0] \cdot \ell^{\dim \mathcal{G}_\ell^0},$$

which is only possible if ℓ is 'small' (that is, bounded above by a constant depending only on K) or $\dim \mathcal{G}_\ell^0 \leq 3$. In turn, this latter inequality is satisfied only in cases (d), (e) and (g), and we show in Theorem 6.23 and Lemma 6.24 that—for a fixed number field K—counterexamples in cases (d) and (e) arise only for finitely many primes ℓ (in fact, case (e) gives no counterexamples at all). This suggests the following conjecture:

Conjecture 2.2 For every number field K there is a constant $b = b(K)$ such that, for all primes $\ell > b(K)$ and for all strong counterexamples (A, ℓ) to the local-global principle for isogenies of prime degree between abelian surfaces, A is geometrically isogenous to the square of an elliptic curve with complex multiplication.

We make some progress on this conjecture in Theorem 6.1, and show in Proposition 6.28 that the case of A being geometrically isogenous to the square of a CM elliptic curve does need to be excluded if we aim for a uniform bound on ℓ. We remark explicitly that, while we make significant headway on this conjecture for all cases when $\mathrm{End}_{\overline{K}}(A) \neq \mathbb{Z}$, our methods do not allow us to say much for *generic* surfaces

(that is, those with $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$). It should be pointed out that even finding *examples* of violations of the local-global principle for isogenies of generic abelian surfaces seems very hard, and the examples in [2] are all non-generic.

2.2 Invariance under isogeny

We now show that the property of being a *strong counterexample* is an isogeny invariant.

Lemma 2.3 *Let $(A/K, \ell)$ be a strong counterexample to the local-global principle for isogenies of abelian surfaces. Let B/K be an abelian surface that is K-isogenous to A. There exists an isogeny $\phi : A \to B$ with $\ell \nmid \deg \phi$.*

Proof Let $\psi : A \to B$ be an isogeny of minimal degree. If $\ell \nmid \deg \psi$ we are done; otherwise, $\ker \psi$ contains a point of order ℓ, so $\ker \psi \cap A[\ell]$ is a non-zero Galois-stable subspace of $A[\ell]$. By assumption, $A[\ell]$ is irreducible, so we have $\ker \psi \cap A[\ell] = A[\ell]$, which implies that $\psi = [\ell] \circ \psi'$ for some isogeny $\psi' : A \to B$ with $\deg \psi' < \deg \psi$. This contradicts the minimality of ψ. □

Corollary 2.4 *Let K be a number field and A/K be an abelian surface. Suppose that (A, ℓ) is a strong counterexample and that B/K is an abelian variety K-isogenous to A: then (B, ℓ) is also a strong counterexample.*

Proof By Lemma 2.3, there exists an isogeny $\varphi : A \to B$ of degree not divisible by ℓ. It induces an isomorphism $A[\ell] \cong B[\ell]$ of G_K-modules. Since the property of being a strong counterexample depends only on the image of the mod-ℓ Galois representation (Lemma 1.2), the claim follows. □

In particular, we obtain that, when (A, ℓ) is a strong counterexample, G_ℓ preserves a non-trivial symplectic form, even if A is not principally polarised:

Corollary 2.5 *Suppose that $(A/K, \ell)$ is a strong counterexample. The image G_ℓ of the mod-ℓ Galois representation is contained in $\mathrm{GSp}_4(\mathbb{F}_\ell)$ with respect to a suitable symplectic form on $A[\ell]$.*

Proof As is well-known, the dual abelian surface $A^\vee$ is isogenous to A over K. By Lemma 2.3, there exists a K-isogeny $\varphi : A \to A^\vee$ of degree prime to ℓ. Via φ, the Weil pairing $A[\ell] \times A^\vee[\ell] \to \mu_\ell$ induces the desired non-degenerate, Galois-invariant, antisymmetric form $A[\ell] \times A[\ell] \to \mathbb{F}_\ell$. For more details on the Weil pairing, the reader is referred to [20]. In particular, [20, Lemma 16.2(e)] shows that the Weil pairing on $T_\ell(A)$ constructed from any polarisation $\varphi : A \to A^\vee$ is an element of $\mathrm{Hom}\left(\Lambda^2 T_\ell(A), \mathbb{Z}_\ell(1)\right)$, that is, an antisymmetric form. The same statement then holds for its reduction modulo ℓ. □

2.3 Group theory

We briefly review some basic group theory we will need in the rest of the paper. We begin with a rather standard definition and a simple lemma, which we will use repeatedly in the rest of the paper:

Definition 2.6 Let I and J be arbitrary groups. We say that $G \leq I \times J$ is a sub-direct product of I and J if G projects surjectively onto both I and J.

Lemma 2.7 *The following hold:*

(1) An element $g \in \mathrm{GL}_2(\mathbb{F}_\ell)$ has an $\mathbb{F}_\ell$-rational eigenvalue if and only if both its eigenvalues are $\mathbb{F}_\ell$-rational.
(2) An element $g \in \mathrm{GL}_n(\mathbb{F}_\ell)$ has an $\mathbb{F}_\ell$-rational eigenvalue if and only if 1 is an eigenvalue of $g^{\ell-1}$.
(3) Let $g \in \mathrm{GL}_n(\mathbb{F}_\ell)$ have order prime to ℓ. The eigenvalues of g are all $\mathbb{F}_\ell$-rational if and only if $g^{\ell-1} = \mathrm{Id}$. This applies in particular to all elements of any subgroup $G < \mathrm{GL}_n(\mathbb{F}_\ell)$ with $\ell \nmid |G|$.

2.3.1 Subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$

We will have to make extensive use of the classification of the maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$, so we briefly recall it here. The result is classical and goes back to Dickson [7]; see also [26, §2].

Theorem 2.8 *Let $\ell \geq 2$ be a prime and let G be a maximal proper subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. One of the following holds:*

(1) G contains $\mathrm{SL}_2(\mathbb{F}_\ell)$.
(2) Borel: up to conjugacy, G is contained in the subgroup of upper-triangular matrices.
(3) Normaliser of Split Cartan: G is conjugate to the group

$$\left\{ \begin{pmatrix} a & \\ & b \end{pmatrix}, \begin{pmatrix} & a \\ b & \end{pmatrix} : a, b \in \mathbb{F}_\ell^\times \right\},$$

of order $2(\ell-1)^2$.
(4) Normaliser of non-split Cartan: let $d \in \mathbb{F}_\ell^\times \setminus \mathbb{F}_\ell^{\times 2}$. The group G is conjugate to the group $\left\{ \begin{pmatrix} a & bd \\ b & a \end{pmatrix}, \begin{pmatrix} a & bd \\ -b & -a \end{pmatrix} : a, b \in \mathbb{F}_\ell \right\}$, of order $2(\ell^2-1)$.
(5) Exceptional: G contains the scalars, and $\mathbb{P}G$ is isomorphic to A_4, S_4 or A_5.

Variants of the same classification also hold for $\mathrm{SL}_2(\mathbb{F}_\ell)$ and $\mathrm{PGL}_2(\mathbb{F}_\ell)$, see Tables 8.1 and 8.2 of [4] for a modern reference. In particular, the exceptional maximal subgroups G of $\mathrm{SL}_2(\mathbb{F}_\ell)$ are as follows: according to whether they have projective image A_4, S_4 or A_5, they are isomorphic respectively to $\mathrm{SL}_2(\mathbb{F}_3)$, $\widehat{S_4}$ or $\mathrm{SL}_2(\mathbb{F}_5)$, where $\widehat{S_4}$, the group with GAP identifier (48, 28), is a Schur double cover of the symmetric group S_4.

We will be especially interested in the maximal subgroup of $\mathrm{SL}_2(\mathbb{F}_\ell)$ given by the intersection of the normaliser of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ with $\mathrm{SL}_2(\mathbb{F}_\ell)$. This is a *generalised quaternion group*, which we now describe in more detail. The generalised quaternion group Q_{4n} of order $4n$ is generated by an element of order $2n$, that we will denote by r, and by an element of order 4, that we will denote by s and we will call a symmetry, subject to the relations $s^2 = r^n$ and $s^{-1}rs = r^{-1}$. Up to

conjugacy, there is a unique maximal subgroup of $\mathrm{SL}_2(\mathbb{F}_\ell)$ isomorphic to $Q_{2(\ell-1)}$. A representative of the conjugacy class is generated by the matrices

$$r = \begin{pmatrix} \delta & 0 \\ 0 & \delta^{-1} \end{pmatrix} \quad \text{and} \quad s = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

with δ a generator of $\mathbb{F}_\ell^\times$. We will denote this specific subgroup of $\mathrm{SL}_2(\mathbb{F}_\ell)$, which is the normaliser of a split Cartan subgroup of $\mathrm{SL}_2(\mathbb{F}_\ell)$, by $N(C_s)$. When considering the group Q_{4n}, we denote by $\mathbb{Z}/(2n)\mathbb{Z}$ the subgroup generated by r. This subgroup is unique if $n \neq 2$. If $j \mid 2n$, we then denote by $\mathbb{Z}/j\mathbb{Z}$ the unique subgroup of $\mathbb{Z}/(2n)\mathbb{Z} < Q_{4n}$ of order j.

3 Hasse subgroups of $\mathrm{Sp}_4(\mathbb{F}_\ell)$

Let us formally define the group-theoretic objects we are interested in:

Definition 3.1 A subgroup G of $\mathrm{GL}_n(\mathbb{F}_\ell)$ is said to have property (E) (for 'eigenvalues') if every $g \in G$ possesses an $\mathbb{F}_\ell$-rational eigenvalue. We further say that G is Hasse if it has property (E) and acts irreducibly on $\mathbb{F}_\ell^n$.

Our objective in this section is to classify the maximal Hasse subgroups of $\mathrm{Sp}_4(\mathbb{F}_\ell)$. The result is as follows:

Theorem 3.2 *Let G be a subgroup of $\mathrm{Sp}_4(\mathbb{F}_\ell)$. If G is Hasse, then $\ell \equiv 1 \pmod 4$ and up to conjugacy it is contained in one of the following groups:*

(1) An extension of degree 2 of the normaliser of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. For a full description, see Eq. (4).
(2) A subgroup of order $2(\ell-1)^2$ or $4(\ell-1)^2$ of an extension of degree 2 of $Q_{2(\ell-1)} \times Q_{2(\ell-1)}$. In particular, the maximal groups of this form contain the subgroup given in Eq. (5).
(3) An extension of degree 2 of an extension of the cyclic group of order $(\ell-1)/2$ by a finite group of order at most 240.
(4) A finite group of order that divides $2^9 \cdot 3^2 \cdot 5^2$.

In Table 1 we give an exhaustive list containing all maximal Hasse subgroups of $\mathrm{Sp}_4(\mathbb{F}_\ell)$. More precisely, the table lists Hasse subgroups that are maximal within a given maximal subgroup of $\mathrm{Sp}_4(\mathbb{F}_\ell)$. We do not make any statement about possible containments between (conjugates of) subgroups that are contained in maximal subgroups of different types (first column). The only exception to this is in Remark 3.20, where we show that (a conjugate of) the group in the first line of the table is always contained in the groups of the fifth or sixth line.

Remark 3.3 In order to obtain the list of groups given in Table 1 we made extensive use of the computer algebra software MAGMA. However, note that we prove Theorem 3.2 as stated, without the explicit list of finite groups that may arise in case (4), without relying on any computer calculations. We use the detailed classification of the maximal Hasse subgroups of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ only in order to prove a fine point of the classification of the Hasse subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$, see Theorem A.1.

Table 1 Maximal Hasse subgroups of $\mathrm{Sp}_4(\mathbb{F}_\ell)$

Type	Group	Condition	Order	Max. subgroup
$\mathcal{C}_2$	$(N_{\mathrm{GL}_2(\mathbb{F}_\ell)}(C_s)).2$	$\ell \equiv 1 \pmod 4$	$2(\ell-1)^2$	$\mathrm{GL}_2(\mathbb{F}_\ell).2$
$\mathcal{C}_2$	$(C_{(\ell-1)/2}.\mathrm{SL}_2(\mathbb{F}_3)).2$	$\ell \equiv 13 \pmod{24}$, $\ell \not\equiv 1 \pmod 5$	$24(\ell-1)$	$\mathrm{GL}_2(\mathbb{F}_\ell).2$
$\mathcal{C}_2$	$(C_{(\ell-1)/2}.\widehat{S_4}).2$	$\ell \equiv 1 \pmod{24}$	$48(\ell-1)$	$\mathrm{GL}_2(\mathbb{F}_\ell).2$
$\mathcal{C}_2$	$(C_{(\ell-1)/2}.\mathrm{SL}_2(\mathbb{F}_5)).2$	$\ell \equiv 1 \pmod{60}$	$120(\ell-1)$	$\mathrm{GL}_2(\mathbb{F}_\ell).2$
$\mathcal{C}_2$	$G < (Q_{2(\ell-1)} \times Q_{2(\ell-1)}).C_2$	$\ell \equiv 1 \pmod 8$	$4(\ell-1)^2$	$\mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$
$\mathcal{C}_2$	$G < (Q_{2(\ell-1)} \times Q_{2(\ell-1)}).C_2$	$\ell \equiv 5 \pmod 8$	$2(\ell-1)^2$	$\mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$
$\mathcal{C}_2$	$C_4.C_2^3$	$\ell \equiv 5 \pmod{24}$	32	$\mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$
$\mathcal{C}_2$	$D_4.A_4$	$\ell \equiv 13 \pmod{24}$	96	$\mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$
$\mathcal{C}_2$	$\widehat{S_4} \wr S_2$	$\ell \equiv 1 \pmod{48}$	4608	$\mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$
$\mathcal{C}_2$	$C_4^2.C_2^4.C_2$	$\ell \equiv 17 \pmod{48}$	512	$\mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$
$\mathcal{C}_2$	$(C_3 : C_4) \wr C_2$	$\ell \equiv 25 \pmod{48}$	288	$\mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$
$\mathcal{C}_2$	$C_4^2.C_2^3.C_2$	$\ell \equiv 25 \pmod{48}$	256	$\mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$
$\mathcal{C}_2$	$Q_8^2.S_3^2$	$\ell \equiv 25 \pmod{48}$	2304	$\mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$
$\mathcal{C}_2$	$Q_8^2.C_2^2$	$\ell \equiv 25, 41 \pmod{48}$	256	$\mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$
$\mathcal{C}_2$	$C_4^2.C_2^3.C_2$	$\ell \equiv 41 \pmod{48}$	256	$\mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$
$\mathcal{C}_2$	$\mathrm{SL}_2(\mathbb{F}_5) \wr S_2$	$\ell \equiv 1 \pmod{120}$	28800	$\mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$
$\mathcal{C}_2$	$C_4.C_2^3$	$\ell \equiv 29, 101 \pmod{120}$	32	$\mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$

Table 1 continued

Type	Group	Condition	Order	Max. subgroup
$\mathcal{C}_2$	$Q_8^2.C_2$	$\ell \equiv 41, 89 \pmod{120}$	128	$\mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$
$\mathcal{C}_2$	$C_5^2 : (C_4 \wr C_2)$	$\ell \equiv 41 \pmod{120}$	800	$\mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$
$\mathcal{C}_2$	$(C_3 : C_4) \wr C_2$	$\ell \equiv 49 \pmod{120}$	288	$\mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$
$\mathcal{C}_2$	$C_2^2.(A_4 \wr C_2)$	$\ell \equiv 49 \pmod{120}$	1152	$\mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$
$\mathcal{C}_2$	$C_5 : D_4 : D_5$	$\ell \equiv 61, 101 \pmod{120}$	400	$\mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$
$\mathcal{C}_2$	$D_6 : S_3 : C_2$	$\ell \equiv 61, 109 \pmod{120}$	144	$\mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$
$\mathcal{C}_2$	$D_4.A_5$	$\ell \equiv 61 \pmod{120}$	480	$\mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$
$\mathcal{C}_2$	$D_4.A_4$	$\ell \equiv 109 \pmod{120}$	96	$\mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$
$\mathcal{C}_3$	$\mathrm{SL}_2(\mathbb{F}_3)$	$\ell \equiv 5 \pmod{24}$	24	$\mathrm{GU}_2(\mathbb{F}_\ell).2$
$\mathcal{C}_3$	$\widehat{S_4}$	$\ell \equiv 17 \pmod{24}$	48	$\mathrm{GU}_2(\mathbb{F}_\ell).2$
$\mathcal{C}_6$	$2_-^{1+4}.O_4(2)$	$\ell \equiv 1 \pmod{120}$	3840	$2_-^{1+4}.O_4(2)$
$\mathcal{C}_6$	$C_2.D_4^2.C_2$	$\ell \equiv 17, 41, 89, 113 \pmod{120}$	256	$2_-^{1+4}.O_4(2)$
$\mathcal{C}_6$	$D_4.A_4.C_2^2$	$\ell \equiv 49, 73, 97 \pmod{120}$	384	$2_-^{1+4}.O_4(2)$
$\mathcal{C}_6$	$Q_8^2.D_6$	$\ell \equiv 49, 73, 97 \pmod{120}$	768	$2_-^{1+4}.O_4(2)$
$\mathcal{C}_6$	$2_-^{1+4}.F_5$	$\ell \equiv 41 \pmod{120}$ or $\ell = 5$	640	$2_-^{1+4}.O_4(2)$
$\mathcal{C}_6$	$D_4.A_4$	$\ell \equiv 13, 37, 61, 109 \pmod{120}$	96	$2_-^{1+4}.\Omega_4^-(2)$

Table 1 continued

Type	Group	Condition	Order	Max. subgroup
$\mathcal{C}_6$	$C_4.C_2^3$	$\ell \equiv 29, 53, 77 \pmod{120}$	32	$2_-^{1+4}.\Omega_4^-(2)$
$\mathcal{C}_6$	$(C_4.C_2^3) : C_5$	$\ell \equiv 61, 101 \pmod{120}$	160	$2_-^{1+4}.\Omega_4^-(2)$
$\mathcal{S}$	$\widehat{S_4}$	$\ell \equiv 17, 41, 89, 113 \pmod{120}$	48	$2.A_6$
$\mathcal{S}$	$\mathrm{SL}_2(\mathbb{F}_3)$	$\ell \equiv 29, 53, 77 \pmod{120}$	24	$2.A_6$
$\mathcal{S}$	$\mathrm{SL}_2(\mathbb{F}_5)$	$\ell \equiv 41, 101 \pmod{120}$ or $\ell = 5$	120	$2.A_6$
$\mathcal{S}$	$2.S_6$	$\ell \equiv 1 \pmod{120}$	1440	$2.S_6$
$\mathcal{S}$	$D_6 : S_3$	$\ell \equiv 13, 37, 61, 109 \pmod{120}$	72	$2.S_6$
$\mathcal{S}$	$\mathrm{GL}_2(\mathbb{F}_3) : C_2$	$\ell \equiv 49, 73, 97 \pmod{120}$	96	$2.S_6$
$\mathcal{S}$	$\mathrm{SL}_2(\mathbb{F}_3).C_2^2$	$\ell \equiv 49, 73, 97 \pmod{120}$	96	$2.S_6$
$\mathcal{S}$	$C_3^2 : Q_8 : C_2$	$\ell \equiv 49, 73, 97 \pmod{120}$	144	$2.S_6$
$\mathcal{S}$	$\mathrm{SL}_2(\mathbb{F}_5)$	$\ell \equiv 61 \pmod{120}$	120	$2.S_6$
$\mathcal{S}$	$\mathrm{SL}_2(\mathbb{F}_3)$	$\ell \equiv 29 \pmod{60}$	24	$\mathrm{SL}_2(\mathbb{F}_\ell)$
$\mathcal{S}$	$\widehat{S_4}$	$\ell \equiv 1, 17 \pmod{24}$	48	$\mathrm{SL}_2(\mathbb{F}_\ell)$
$\mathcal{S}$	$\mathrm{SL}_2(\mathbb{F}_5)$	$\ell \equiv 1, 41 \pmod{60}$	120	$\mathrm{SL}_2(\mathbb{F}_\ell)$

For a description of the data in the table see Remark 3.5

Remark 3.4 Primes $\ell \leq 7$ cannot be handled by our methods, both because the technique of Sect. 3.2, which we use to analyse certain small groups H, requires the assumption $\ell \nmid |H|$, and because the classification of the maximal subgroups of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ is slightly different for small ℓ. However, a direct computation reveals that $\mathrm{Sp}_4(\mathbb{F}_\ell)$ and $\mathrm{GSp}_4(\mathbb{F}_\ell)$ contain no Hasse subgroups at all for $\ell = 2, 3$. Moreover, one can check that Theorems 3.2, 5.5, and 4.6 all hold for $\ell \leq 7$. Hence, from now on, we will tacitly assume that $\ell > 7$.

Remark 3.5 Table 1 is organised as follows. Every line corresponds to a Hasse subgroup G of $\mathrm{Sp}_4(\mathbb{F}_\ell)$, maximal among the Hasse subgroups contained in a given maximal subgroup of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ (given in the last column). The second column gives a description of the structure of G, and the third column gives congruence conditions under which the group G exists, is Hasse, and is maximal in the sense above. The fourth column gives the order of G.

For a classification of the maximal subgroup of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ see Table 2. In both tables, the column 'Type' refers to the Aschbacher type of the maximal subgroup of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ (for a definition see for example [4]).

3.1 Preliminary lemmas

Lemma 3.6 *Let $G < \mathrm{GL}_2(\mathbb{F}_\ell)$ be a Hasse subgroup such that every matrix in G is diagonal or anti-diagonal. Let $M \in \mathrm{GL}_2(\mathbb{F}_\ell)$ be a matrix that normalises G and such that MM^{-T} is diagonal or anti-diagonal. Then, at least one of the following holds:*

- *M is diagonal or anti-diagonal. There exists $g \in G$ such that gM is diagonal.*
- *$\mathbb{P}G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and there exists $g \in G$ such that gM is symmetric. This case is only possible if $\ell \equiv 1 \pmod 4$.*

Proof Write $M = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$. Note that G contains a diagonal matrix $D = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$ with $a \neq d$, because otherwise $\mathbb{P}G$ would have order ≤ 2 and G would not act irreducibly.

Let $D = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in G$ be a diagonal matrix that is not a multiple of the identity. If MDM^{-1} is diagonal, then by direct computation we have $xy = zw = 0$, so M is diagonal or anti-diagonal. By irreducibility, G contains an anti-diagonal matrix g; if M is anti-diagonal, gM is diagonal, and we are done.

Otherwise, we may suppose that MDM^{-1} is anti-diagonal for all diagonal matrices $D = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in G$ with $a \neq d$. The condition that MDM^{-1} is anti-diagonal gives $xaw - ydz = wdx - zay = 0$, which in particular implies $a = -d$ and $xw = -yz$. Thus we have $a = \pm d$ for all diagonal matrices $D = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$ in G. By irreducibility, not all diagonal matrices in G are scalars, so G contains some diagonal matrix D_0 with $a = -d$. Again by irreducibility, G also contains anti-diagonal matrices. Combined with the condition $a = \pm d$ for all diagonal matrices, this yields $\mathbb{P}G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

If MM^{-T} is diagonal, we have $x(y - z) = w(y - z) = 0$, which gives that M is anti-diagonal or symmetric. If MM^{-T} is anti-diagonal, then $xw - y^2 = xw - z^2 = 0$,

which implies $y = \pm z$. If $z = y$, then M is symmetric, and if $z = -y$ then $D_0 M$ is symmetric. Finally, we prove that ℓ is congruent to 1 modulo 4. Let $g \in G$ be an anti-diagonal matrix, with characteristic polynomial $t^2 + \det(g)$. The condition that g has rational eigenvalues implies that $-\det(g)$ is a square. The matrix $D_0 g$ is anti-diagonal, and the condition that $-\det(D_0 g) = (-a^2)(-\det g)$ is a square implies that -1 is a square modulo ℓ, so $\ell \equiv 1 \pmod 4$. □

Lemma 3.7 *Let $G < \mathrm{SL}_2(\mathbb{F}_\ell)$ be a Hasse subgroup of $N(C_s)$ and let $M \in \mathrm{GL}_2(\mathbb{F}_\ell)$ normalise G. One of the following holds:*

- *M is diagonal or anti-diagonal. There exists $g \in G$ such that gM is diagonal;*
- *$G \cong Q_8$.*

Proof If $|G| > 8$, the subgroup of diagonal matrices is characteristic in G, hence M normalises it. This forces M to be diagonal or anti-diagonal; the conclusion follows easily. □

Remark 3.8 Let $A \in \mathrm{GL}_4(\mathbb{F}_\ell)$ be a block-anti-diagonal matrix of the form $\begin{pmatrix} 0 & g_1 \\ g_2 & 0 \end{pmatrix}$ with $g_1, g_2 \in \mathrm{GL}_2(\mathbb{F}_\ell)$. The eigenvalues of A are given by $\pm\sqrt{\lambda_1}, \pm\sqrt{\lambda_2}$, where λ_1, λ_2 are the eigenvalues of $g_1 g_2$. In particular, A admits an $\mathbb{F}_\ell$-rational eigenvalue if and only if one of the eigenvalues of $g_1 g_2$ is a square in $\mathbb{F}_\ell^\times$. If $\det(g_1 g_2) = \lambda_1 \lambda_2$ is a square in $\mathbb{F}_\ell^\times$, then A has an $\mathbb{F}_\ell$-rational eigenvalue if and only if all of its eigenvalues are $\mathbb{F}_\ell$-rational.

We now briefly describe the general strategy of proof of Theorem 3.2, which is inspired by [6], even though the details are significantly different. The idea is to recursively explore the lattice of subgroups of $\mathrm{Sp}_4(\mathbb{F}_\ell)$, starting with the maximal ones and considering smaller and smaller subgroups as needed. More precisely, given a subgroup $G \leq \mathrm{Sp}_4(\mathbb{F}_\ell)$, one of the following holds:

(1) G is Hasse, in which case we add it to the list of Hasse subgroups of $\mathrm{Sp}_4(\mathbb{F}_\ell)$;
(2) G acts reducibly, in which case it contains no Hasse subgroups;
(3) G acts irreducibly, but it contains elements without any $\mathbb{F}_\ell$-rational eigenvalues. We then consider each maximal subgroup of G, and iterate the same analysis.

At the top level, we start with $G = \mathrm{Sp}_4(\mathbb{F}_\ell)$ itself, which contains elements without $\mathbb{F}_\ell$-rational eigenvalues. Thus, we need to consider the maximal proper subgroups of $\mathrm{Sp}_4(\mathbb{F}_\ell)$, which are as in Table 2 (see [4] for the notion of Aschbacher type of a maximal subgroup and Tables 8.12 and 8.13 of *op. cit.* for the classification). We exclude from our list the groups of type $\mathcal{C}_1$, since these act reducibly by definition.

The cases corresponding to each of these maximal subgroups will be considered in turn in Sects. 3.4 to 3.7. It is useful to point out at the outset that most groups H in this list have the property that all maximal subgroups of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ isomorphic to H are conjugate inside $\mathrm{Sp}_4(\mathbb{F}_\ell)$, so that—for our purposes—we may work with a single, fixed maximal subgroup in the given isomorphism class. More precisely, this property holds for all the groups but $2_-^{1+4}.O_4^-(2)$ and $2.S_6$, for which two conjugacy classes exist (these groups will be handled using the methods of Sect. 3.2 and cause no difficulties).

Table 2 Maximal subgroups of $\mathrm{Sp}_4(\mathbb{F}_\ell)$

Type	Group
$\mathcal{C}_2$	$\mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$
$\mathcal{C}_2$	$\mathrm{GL}_2(\mathbb{F}_\ell).2$
$\mathcal{C}_3$	$\mathrm{SL}_2(\mathbb{F}_{\ell^2}).2$
$\mathcal{C}_3$	$\mathrm{GU}_2(\mathbb{F}_\ell).2$
$\mathcal{C}_6$	$2_-^{1+4}.O_4^-(2)$ or $2_-^{1+4}.\Omega_4^-(2)$
$\mathcal{S}$	$\mathrm{SL}_2(\mathbb{F}_\ell)$
$\mathcal{S}$	$2.S_6$ or $2.A_6$

3.2 Handling the 'small' groups

In this section we describe a computational technique to classify the Hasse subgroups of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ that are isomorphic to a subgroup of a fixed abstract group G, as ℓ varies among the primes that do not divide $|G|$. The technique is based on basic representation theory, so we only give a sketch, but we point out that we have implemented the algorithm resulting from the arguments in this section as a MAGMA script. Since there is nothing specific about $\mathrm{Sp}_4(\mathbb{F}_\ell)$, we actually consider more generally subgroups of arbitrary matrix groups over finite fields.

Notice first that since $\ell \nmid |G|$ all representations of G in characteristic ℓ are semi-simple (Maschke's theorem) and come by reduction from representations defined in characteristic 0, so that we have at our disposal all the usual machinery of characters and representation theory in characteristic 0. In particular, for a fixed $k \geq 1$ we can describe all representations $G \hookrightarrow \mathrm{GL}_k(\mathbb{F}_{\ell^e})$ (and even $G \hookrightarrow \mathrm{Sp}_k(\mathbb{F}_{\ell^e})$):

(1) we construct all k-dimensional representations of G by looking at complex characters;
(2) by [27, Theorem 24, p. 109], the representation corresponding to each complex character can be realised over the number field $K := \mathbb{Q}(\zeta_{|G|})$. The prime ℓ is unramified in this field, so by reducing modulo a place $\mathfrak{p}$ of K of characteristic ℓ we obtain a corresponding representation defined over a finite extension of $\mathbb{F}_\ell$;
(3) we may also determine the minimal extension of $\mathbb{F}_\ell$ over which a given representation is defined: by [27, Corollaire on p. 108], since the Brauer group of any finite field vanishes, a representation ρ over $\overline{\mathbb{F}_\ell}$ is defined over the finite field $\mathbb{F}_{\ell^e}$ if and only if $\mathbb{F}_{\ell^e}$ contains the field generated by the image of the character of ρ (which we obtain by reducing the corresponding complex character modulo the place $\mathfrak{p}$);
(4) finally, when the dimension k is even, in order to test whether a given representation V has image in $\mathrm{Sp}_k(\mathbb{F}_{\ell^e})$ (that is, whether V admits an invariant alternating bilinear form), it suffices to test whether $\Lambda^2 V^*$ contains a copy of the trivial representation. This can also be understood in terms of characters: the character of V determines the character of $\Lambda^2 V^*$, and in order to check whether $\Lambda^2 V$ contains a copy of the trivial representation we simply need to take the scalar product of this character with the trivial character. An obvious variant of this procedure, using $\mathrm{Sym}^2 V^*$, can be used to test whether a representation is orthogonal.

Suppose now that we wish to know for which primes ℓ (not dividing $|G|$) there exist

- an embedding $\overline{\rho} : G \hookrightarrow \mathrm{Sp}_k(\mathbb{F}_\ell)$
- a subgroup H of G

such that $\rho(H)$ is a Hasse subgroup. The inclusion $\overline{\rho}$ gives in particular a symplectic representation of G on a k-dimensional space, which comes by reduction from a faithful representation $\rho : G \hookrightarrow \mathrm{GL}_k(K)$. Since we can list all irreducible k-dimensional representations of G, we may assume that the representation ρ is fixed. We may then proceed as follows:

(1) for each subgroup H of G, we restrict ρ to H;
(2) we decompose $\rho|_H$ as a direct sum of representations of H, using character theory;
(3) for each sub-representation W of $\rho|_H$ we test whether W is defined over $\mathbb{F}_\ell$. Notice that this amounts to testing whether ℓ splits completely in the sub-field of K generated by the traces of the character of $\rho|_H$. Since the field K is cyclotomic, by class field theory (or even just the Kronecker-Weber theorem) this amounts to some congruence conditions on ℓ. If no non-trivial sub-representation W of $\rho|_H$ is defined over $\mathbb{F}_\ell$, then $\rho|_H$ is irreducible over $\mathbb{F}_\ell$;
(4) for each $h \in H$ we compute the characteristic polynomial of $\rho(h)$. Its roots are all roots of unity, of orders (say) $n_1, \ldots, n_k$. The condition that $\rho(h)$ has an $\mathbb{F}_\ell$-rational eigenvalue again translates into a congruence condition: ℓ must be congruent to 1 modulo at least one of the integers $n_1, \ldots, n_k$.

The output of this algorithm is a collection of pairs (H, congruence conditions on ℓ): the Hasse subgroups of $\rho(G) < \mathrm{Sp}_k(\mathbb{F}_\ell)$ are precisely the $\rho(H)$ for which the corresponding congruence conditions on ℓ are met. Notice that each subgroup H of G will correspond to different conditions in general, and for some subgroups the conditions will correspond to the empty set of prime numbers. Naturally we can also list the *maximal* Hasse subgroups by checking for inclusions between the various subgroups. We shall use this procedure repeatedly to handle cases when the relevant subgroups of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ to be studied have order independent of the prime ℓ.

3.3 Further input from representation theory

Let G be a finite group and let ℓ be a prime such that $\ell \nmid |G|$. As recalled in the previous section, there is a bijective correspondence between irreducible representations of G over $\overline{\mathbb{F}_\ell}$ and over $\mathbb{C}$.

Proposition 3.9 *Let G and ℓ be as above, let G_0 be a subgroup of G of index 2, and let $\rho : G \to \mathrm{GL}_n(\mathbb{F}_\ell)$ be a representation. Suppose that, for every $g \in G$, all eigenvalues of $\rho(g)$ are $\mathbb{F}_\ell$-rational. Then the following hold:*

(1) ρ is irreducible if and only if it is absolutely irreducible.
(2) Let χ be the character of the complex representation lifting ρ. Then ρ is irreducible if and only if $\langle \chi, \chi \rangle_G = 1$, where $\langle \cdot, \cdot \rangle_G$ is the usual scalar product on characters.
(3) Suppose that the restriction of ρ to G_0 decomposes as the direct sum of two isomorphic representations over $\mathbb{F}_\ell$. Then ρ is reducible.

Proof (1) One implication is trivial. For the other, let χ be the character of the complex representation lifting ρ, and let χ_1 be an irreducible character appearing as a summand of χ. For every $g \in G$, the reduction modulo ℓ of $\chi_1(g)$ is a sum of eigenvalues of g, hence is $\mathbb{F}_\ell$-rational. By [27, Corollaire on p. 108], the representation ρ_1 with character (the reduction modulo ℓ of) χ_1 is defined over $\mathbb{F}_\ell$ and is a subrepresentation of ρ.

(2) Follows combining (1), the correspondence between representations over $\mathbb{C}$ and $\overline{\mathbb{F}_\ell}$, and the well-known fact that a complex representation is irreducible if and only if its character has norm 1 with respect to the natural scalar product.

(3) Let χ be as above. The assumption yields $\langle \chi, \chi \rangle_{G_0} = \frac{1}{|G_0|} \sum_{g_0 \in G_0} |\chi(g_0)|^2 \geq 4$, since $\chi|_{G_0}$ is the sum of two copies of the same representation. Hence

$$\langle \chi, \chi \rangle_G = \frac{1}{|G|} \sum_{g \in G} |\chi(g)|^2 \geq \frac{1}{2|G_0|} \sum_{g \in G_0} |\chi(g)|^2 \geq 2,$$

so the representation ρ is reducible by (2).

□

3.4 *G* of type $\mathcal{C}_2$: $G < \mathrm{GL}_2(\mathbb{F}_\ell).2$

In this section we prove:

Proposition 3.10 *Let $G < \mathrm{Sp}_4(\mathbb{F}_\ell)$ be a Hasse group contained in a group isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell).2$. Then, one of the following holds:*

- *$\ell \equiv 1 \pmod 4$ and G is contained (up to conjugacy) in G', the group described in Eq. (4).*
- *G is contained in one of the groups of Proposition 3.17.*

The group $\mathrm{GL}_2(\mathbb{F}_\ell).2$ sits in the exact sequence

$$1 \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell) \xrightarrow{i} \mathrm{GL}_2(\mathbb{F}_\ell).2 \xrightarrow{\pi} S_2 \longrightarrow 0$$

and up to conjugacy in $\mathrm{Sp}_4(\mathbb{F}_\ell)$, considered as the group of isometries of the symplectic form given in (1), we have

$$\mathrm{GL}_2(\mathbb{F}_\ell).2 = \left\{ \begin{pmatrix} A & 0 \\ 0 & A^{-T} \end{pmatrix}, \begin{pmatrix} 0 & B \\ -B^{-T} & 0 \end{pmatrix} \mid A, B \in \mathrm{GL}_2(\mathbb{F}_\ell) \right\},$$

see the beginning of [6, Section 3.1]. Let $G < \mathrm{GL}_2(\mathbb{F}_\ell).2$ be a Hasse subgroup and let $G_0 := G \cap \ker \pi$: every element of G_0 can be written as $\begin{pmatrix} A & 0 \\ 0 & A^{-T} \end{pmatrix}$. Then we can identify G_0 to a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ via the isomorphism $\begin{pmatrix} A & 0 \\ 0 & A^{-T} \end{pmatrix} \mapsto A$.

Since there are elements of $\mathrm{GL}_2(\mathbb{F}_\ell)$ that do not have any rational eigenvalues, G_0 is a proper subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. By Theorem 2.3.1, G_0 contains $\mathrm{SL}_2(\mathbb{F}_\ell)$ or is

contained in the normaliser of a Cartan subgroup, in a Borel subgroup, or in groups that have projective image A_4, S_4, or A_5. Observe that there are elements of $\mathrm{SL}_2(\mathbb{F}_\ell)$ without a rational eigenvalue: it follows that G_0 does not contain $\mathrm{SL}_2(\mathbb{F}_\ell)$, hence it is a subgroup of one of the groups above.

3.4.1 Case G_0 in the normaliser of a split Cartan subgroup

In a suitable basis, the normaliser NC_s of a split Cartan can be written as

$$NC_s = \left\{ \begin{pmatrix} \delta^i & 0 \\ 0 & \delta^j \end{pmatrix}, \begin{pmatrix} 0 & \delta^i \\ \delta^j & 0 \end{pmatrix} \mid \delta \text{ generates } \mathbb{F}_\ell^\times, i, j = 0, \ldots, \ell - 2 \right\}.$$

G is Hasse and then contains a block-anti-diagonal matrix $\begin{pmatrix} 0 & M \\ -M^{-T} & 0 \end{pmatrix}$ with $M \in \mathrm{GL}_2(\mathbb{F}_\ell)$ that normalises G_0. The possible matrices M are described in Lemma 3.6.

If we are in the second case of Lemma 3.6, then $\mathbb{P}G_0 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and $\ell \equiv 1 \pmod 4$. It follows that G_0 is exceptional, and we will study this case in Sect. 3.4.4.

If we are in the first case of Lemma 3.6, then M is diagonal or anti-diagonal. Put $A(i, j) = \begin{pmatrix} \delta^i & 0 \\ 0 & \delta^j \end{pmatrix}$ and $B(i, j) = \begin{pmatrix} 0 & \delta^i \\ \delta^j & 0 \end{pmatrix}$, so that

$$G \leq \left\{ \begin{pmatrix} A(i,j) & 0 \\ 0 & A(i,j)^{-T} \end{pmatrix}, \begin{pmatrix} 0 & A(i,j) \\ -A(i,j)^{-T} & 0 \end{pmatrix}, \begin{pmatrix} B(i,j) & 0 \\ 0 & B(i,j)^{-T} \end{pmatrix}, \begin{pmatrix} 0 & B(i,j) \\ -B(i,j)^{-T} & 0 \end{pmatrix} \right\}.$$

Since G is Hasse, it must contain matrices of all four types above (for otherwise it would stabilise a 2-dimensional subspace). In particular, the set $G \setminus G_0$ is non-empty and contains an element of the form $\begin{pmatrix} 0 & A(i,j) \\ -A(i,j)^{-T} & 0 \end{pmatrix}$. A matrix of this form has characteristic polynomial $(t^2 + 1)^2$, so it has a rational eigenvalue if and only if -1 is a square modulo ℓ. Hence, in order for every element of G to have a rational eigenvalue, we need $\ell \equiv 1 \pmod 4$, which we assume from now on. As above, G_0 contains at least one element of the form $B(i_0, j_0)$. The matrix $B(i, j)$ has a rational eigenvalue if and only if δ^{i+j} is a square, hence $i_0 + j_0$ is even. Since $A(i, j)B(i_0, j_0) = B(i + i_0, j + j_0)$ is also an element of G, we must have $i + i_0 + j + j_0 \equiv 0 \pmod 2$. So $i + j$ is even and

$$G_0 \leq \left\{ A(i, j), B(i, j) \mid i + j \equiv 0 \pmod 2 \right\}.$$

Moreover, G contains an element of the form $\begin{pmatrix} 0 & B(i,j) \\ -B(i,j)^{-T} & 0 \end{pmatrix}$. The characteristic polynomial of this matrix is $(t^2 + \delta^{i-j})(t^2 + \delta^{j-i})$, so it has a rational

eigenvalue if and only if $i - j \equiv 0 \pmod 2$ (recall that -1 is a square modulo $\ell \equiv 1 \pmod 4$). We conclude that $G \leq G'$, where

$$G' = \left\{ \begin{pmatrix} A(i,j) & 0 \\ 0 & A(i,j)^{-T} \end{pmatrix}, \begin{pmatrix} 0 & A(i,j) \\ -A(i,j)^{-T} & 0 \end{pmatrix}, \begin{pmatrix} B(i,j) & 0 \\ 0 & B(i,j)^{-T} \end{pmatrix}, \begin{pmatrix} 0 & B(i,j) \\ -B(i,j)^{-T} & 0 \end{pmatrix} \Big| i + j \equiv 0 \pmod 2 \right\}. \tag{4}$$

On the other hand, if $\ell \equiv 1 \pmod 4$ one checks immediately that the group G' is a (necessarily maximal) Hasse subgroup.

3.4.2 Case G_0 in the normaliser of a non-split Cartan subgroup

Up to conjugacy, the normaliser NC_{ns} of a non-split Cartan is

$$N(C_{ns}) := \left\{ \begin{pmatrix} a & \delta b \\ b & a \end{pmatrix}, \begin{pmatrix} a & \delta b \\ -b & -a \end{pmatrix} \mid (a,b) \neq (0,0) \in \mathbb{F}_\ell^2 \right\},$$

where δ is a non-square in $\mathbb{F}_\ell^\times$, see Sect. 2.3.1. The group G contains a matrix with $b \neq 0$, since otherwise it would not act irreducibly. For $b \neq 0$ the matrix $\begin{pmatrix} a & \delta b \\ b & a \end{pmatrix}$ does not have a rational eigenvalue, because its characteristic polynomial is $(t-a)^2 - \delta b^2$. Moreover, by direct computation, the product of two different matrices of the form $\begin{pmatrix} a & \delta b \\ -b & -a \end{pmatrix}$ does not have a rational eigenvalue, unless the two matrices differ by a scalar. Hence, if G_0 contains a matrix M of the form $\begin{pmatrix} a & \delta b \\ -b & -a \end{pmatrix}$ for $b \neq 0$, then this is the only element of G_0 of this form up to scalars. It follows that G_0 is contained in the group generated by the scalar matrices and by M. In particular, G_0 fixes the eigenspaces of M, so G_0 is contained in a Borel subgroup, which we treat next.

3.4.3 Case G_0 in a Borel subgroup

Let $\langle v \rangle$ be a line in $\mathbb{F}_\ell^4$ fixed by G_0. Let $g \in G \setminus G_0$ and consider the two-dimensional subspace $V = \langle v, gv \rangle$: one checks immediately that V is G-invariant, hence G does not act irreducibly.

3.4.4 Cases $\mathbb{P}G_0 \leq A_4$, $\mathbb{P}G_0 \leq S_4$, and $\mathbb{P}G_0 \leq A_5$

Lemma 3.11 *Let H be a Hasse subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell).2$. Consider the subgroup H_1 of $\mathrm{GL}_2(\mathbb{F}_\ell).2$ consisting of the matrices of the form $\begin{pmatrix} \lambda \,\mathrm{Id} & 0 \\ 0 & \lambda^{-1} \,\mathrm{Id} \end{pmatrix}$ for $\lambda \in \mathbb{F}_\ell^\times$. The subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell).2$ generated by H and H_1 is Hasse.*

Proof One can see that $HH_1 = H_1H$, hence that HH_1 is a group. We check that HH_1 is Hasse. By assumption every $h \in H$ has at least one $\mathbb{F}_\ell$-rational eigenvalue. If h is block-diagonal, then it is easy to see that any element of the form hh_1 for $h_1 \in H_1$ has at least one $\mathbb{F}_\ell$-rational eigenvalue. On the other hand, if $h = \begin{pmatrix} 0 & B \\ -B^{-T} & 0 \end{pmatrix}$ is block-anti-diagonal, then we know that h has $\mathbb{F}_\ell$-rational eigenvalues if and only if $-BB^{-T}$ admits an eigenvalue which is a square in $\mathbb{F}_\ell^\times$ (see Remark 3.8). Let $h_1 = \begin{pmatrix} \lambda^{-1}\,\mathrm{Id} & 0 \\ 0 & \lambda\,\mathrm{Id} \end{pmatrix}$ be any element of H_1. Therefore, multiplying the off-diagonal blocks of the product $hh_1 = \begin{pmatrix} 0 & \lambda B \\ -\lambda^{-1}B^{-T} & 0 \end{pmatrix}$ we get again $-BB^{-T}$, which by assumption has an eigenvalue that is a square in $\mathbb{F}_\ell^\times$, so hh_1 has at least one $\mathbb{F}_\ell$-rational eigenvalue, as desired. Finally, since H acts irreducibly on $\mathbb{F}_\ell^4$, then a fortiori so does HH_1, hence HH_1 is Hasse as claimed. □

Corollary 3.12 *Every subgroup of* $\mathrm{GL}_2(\mathbb{F}_\ell).2$*, maximal among Hasse subgroups, contains the group* H_1 *of the previous lemma.*

Corollary 3.13 *Let* $\ell > 3$ *be a prime and let* H *be a subgroup of* $\mathrm{GL}_2(\mathbb{F}_\ell).2$ *that contains* H_1*. Let* $H_0 = H \cap \ker\pi$ *and assume* $H \neq H_0$*. If* $H_0 \leq \mathrm{GL}_2(\mathbb{F}_\ell)$ *acts irreducibly on* $\mathbb{F}_\ell^2$*, then* H *acts irreducibly on* $\mathbb{F}_\ell^4$*.*

Proof Let W be a subspace of $\mathbb{F}_\ell^4$ stable under the action of H. We will show that either $W = \{0\}$ or $W = \mathbb{F}_\ell^4$. We write V_1 (resp. V_2) for the $\mathbb{F}_\ell$-span of the first two (resp. last two) basis vectors of $\mathbb{F}_\ell^4$. First we observe that $W = (W \cap V_1) \oplus (W \cap V_2)$. To see this, simply notice that W is stable under the action of H_1, hence in particular under the action of

$$\frac{1}{\lambda - \lambda^{-1}}\left(\begin{pmatrix} \lambda\,\mathrm{Id} & 0 \\ 0 & \lambda^{-1}\,\mathrm{Id} \end{pmatrix} - \lambda^{-1}\,\mathrm{Id}\right),$$

which—for $\lambda \neq \pm 1$ (and there is such an element in $\mathbb{F}_\ell^\times$, since $\ell > 3$)—is the projector on V_1; one reasons similarly for the projection on V_2. The subspace $W \cap V_1$ is stable under the action of H_0, so by assumption it is either trivial or all of V_1 (and the same applies to $W \cap V_2$). Finally, since H contains an element that exchanges V_1 with V_2, the subspaces $W \cap V_1$ and $W \cap V_2$ are either both trivial or both 2-dimensional. In the two cases, one obtains $W = \{0\}$ or $W = \mathbb{F}_\ell^4$. □

It is clear that if $H \leq \mathrm{GL}_2(\mathbb{F}_\ell).2$ is a Hasse subgroup, then $H_0 = H \cap \ker\pi$ is a Hasse subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$: the condition on rational eigenvalues is satisfied, and if $\mathbb{F}_\ell^2$ were reducible under the action of H_0, then H_0 would be contained in a Borel subgroup, which contradicts the arguments of Sect. 3.4.3.

By [29, Lemma 1] we see that if $\mathbb{P}H_0$ is not contained in $\mathrm{PSL}_2(\mathbb{F}_\ell)$, then $\mathbb{P}H_0$ cannot be an exceptional group, so we fall back into the cases of the previous sections. Hence we may assume that $\mathbb{P}H_0$ is contained in $\mathrm{PSL}_2(\mathbb{F}_\ell)$. By [1, Lemma 3.5] we then obtain that ℓ is 1 modulo 4 and $\mathbb{P}H_0$ is isomorphic to one among A_4, S_4, A_5.

Notice that $\mathrm{GL}_2^{\square}(\mathbb{F}_\ell) := \{g \in \mathrm{GL}_2(\mathbb{F}_\ell) \mid \det(g) \in \mathbb{F}_\ell^{\times 2}\}$ coincides with the subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ generated by $\mathrm{SL}_2(\mathbb{F}_\ell)$ and the scalar matrices. We record what we have just shown as a lemma:

Lemma 3.14 *If $H < \mathrm{GL}_2(\mathbb{F}_\ell).2$ is a maximal Hasse subgroup, then we have $\ell \equiv 1 \pmod 4$ and $H_0 < \mathrm{GL}_2^{\square}(\mathbb{F}_\ell)$, where $H_0 := H \cap \ker \pi$. Moreover, H_0 contains $\mathbb{F}_\ell^{\times}$ Id.*

We now recover H from H_0 using that H normalises it.

Lemma 3.15 *Let $\ell \equiv 1 \pmod 4$ be a prime. Let H_0 be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, contained in $\mathrm{GL}_2^{\square}(\mathbb{F}_\ell)$ and containing $\mathbb{F}_\ell^{\times}$ Id.*

(1) Suppose that H_0 has projective image isomorphic to S_4 or A_5. Then the normaliser N of H_0 in $\mathrm{GL}_2(\mathbb{F}_\ell).2$ satisfies $[N : H_0] = 2$, and an element of the non-trivial coset is given by $J' := \begin{pmatrix} & J_2 \\ -J_2 & \end{pmatrix}$, where $J_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

(2) Suppose that H_0 has projective image isomorphic to A_4. Then the normaliser N of H_0 in $\mathrm{GL}_2(\mathbb{F}_\ell).2$ satisfies $[N : H_0] = 4$, and representatives of the three non-trivial cosets are given by J', $\begin{pmatrix} \sigma & 0 \\ 0 & \sigma^{-T} \end{pmatrix}$, $J'\begin{pmatrix} \sigma & 0 \\ 0 & \sigma^{-T} \end{pmatrix}$, where $\sigma \in \mathrm{GL}_2(\mathbb{F}_\ell)$ is such that $\langle H_0, \sigma \rangle$ has projective image S_4.

(3) With notation as in (2), assume that $\mathbb{P}H_0 \cong A_4$ is a maximal subgroup of $\mathrm{PSL}_2(\mathbb{F}_\ell)$. The coset $J'\begin{pmatrix} \sigma & 0 \\ 0 & \sigma^{-T} \end{pmatrix} H_0$ contains matrices that do not have $\mathbb{F}_\ell$-rational eigenvalues.

Proof We begin by noticing the following matrix identity: for every $A \in \mathrm{GL}_2(\mathbb{F}_\ell)$ one has

$$-J_2 A^{-T} J_2 = \frac{1}{\det A} A.$$

(1) The normaliser N_0 of H_0 in $\mathrm{GL}_2(\mathbb{F}_\ell)$ is H_0 itself: indeed, $\mathbb{P}N_0$ is a subgroup of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ containing $\mathbb{P}H_0$, and S_4, A_5 are maximal subgroups of $\mathrm{PGL}_2(\mathbb{F}_\ell)$, so we have $\mathbb{P}N_0 = \mathbb{P}H_0$, which – since H_0 contains all the scalars—implies $N_0 = H_0$. Now let $g_1, g_2 \in \mathrm{GL}_2(\mathbb{F}_\ell).2 \setminus \mathrm{GL}_2(\mathbb{F}_\ell)$ both normalise H_0. Then $g_1 g_2$ is in $\mathrm{GL}_2(\mathbb{F}_\ell)$ and normalises H_0, so it is in H_0. This proves that $[N : H_0] \leq 2$. The fact that J' is in N follows from a simple calculation using the above matrix identity.

(2) The group $\mathrm{PGL}_2(\mathbb{F}_\ell)$ contains a subgroup isomorphic to S_4 for all $\ell > 2$ (see [26, Remarque on page 281]). The inverse image $\tilde{H}$ in $\mathrm{GL}_2(\mathbb{F}_\ell)$ of this subgroup contains H_0 with index 2. Let σ be a representative of the non-trivial coset of H_0 inside $\tilde{H}$, as in the statement. It is clear that both $\begin{pmatrix} \sigma & 0 \\ 0 & \sigma^{-T} \end{pmatrix}$ and J' normalise H_0. On the other hand, $\tilde{H}$ is a maximal subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, so—reasoning as in the previous part—we see that $[N : \tilde{H}] \leq 2$. This shows $[N : H_0] \leq 4$, from which the claim follows.

(3) Observe that $\det(\sigma)$ is not a square in $\mathbb{F}_\ell^\times$, for otherwise $\mathbb{P}\langle H_0, \sigma\rangle$ would be a proper overgroup of $\mathbb{P}H_0$ in $\mathrm{PSL}_2(\mathbb{F}_\ell)$. Let $\begin{pmatrix} A & 0 \\ 0 & A^{-T} \end{pmatrix}$ be an element in H_0 and notice that

$$J' \begin{pmatrix} \sigma & 0 \\ 0 & \sigma^{-T} \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & A^{-T} \end{pmatrix} = \begin{pmatrix} 0 & J_2\sigma^{-T}A^{-T} \\ -J_2\sigma A & 0 \end{pmatrix}.$$

By Remark 3.8, in order to check if this matrix has $\mathbb{F}_\ell$-rational eigenvalues, we need to test whether the matrix $-J_2\sigma^{-T}A^{-T}J_2\sigma A$ has an eigenvalue that is a square in $\mathbb{F}_\ell^\times$. Using the matrix identity at the beginning of the proof, we need to understand whether $\frac{1}{\det(\sigma A)}(\sigma A)^2$ admits an eigenvalue in $\mathbb{F}_\ell^{\times 2}$. We may choose A in such a way that σA represents a transposition in S_4. Notice that $\det(A)$ is a square (since this is true for all elements in H_0). From the choice of A it follows that $(\sigma A)^2 = \mathrm{Id}$, so the eigenvalues of $\frac{1}{\det(\sigma A)}(\sigma A)^2$ are all equal to $\frac{1}{\det(\sigma A)}$, which is not a square (since $\det(A) \in \mathbb{F}_\ell^{\times 2}$ but $\det\sigma \notin \mathbb{F}_\ell^{\times 2}$).

□

Corollary 3.16 *Let $\ell \equiv 1 \pmod 4$ be a prime. Let H_0 be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, contained in $\mathrm{GL}_2^{\square}(\mathbb{F}_\ell)$ and containing $\mathbb{F}_\ell^\times \mathrm{Id}$. Suppose that H_0 is Hasse.*

(1) Suppose that one of the following holds:

(a) $\mathbb{P}H_0 \cong S_4$;
(b) $\mathbb{P}H_0 \cong A_5$;
(c) $\mathbb{P}H_0 \cong A_4$ and $\mathbb{P}H_0$ is maximal in $\mathrm{PSL}_2(\mathbb{F}_\ell)$.

Then $H := \langle H_0, J'\rangle$ is Hasse and is the unique maximal Hasse subgroup $G < \mathrm{GL}_2(\mathbb{F}_\ell).2$ such that $G_0 = H_0$.

(2) Suppose that $\mathbb{P}H_0 \cong A_4$ and that $\mathbb{P}H_0$ is contained in a maximal subgroup of $\mathrm{PSL}_2(\mathbb{F}_\ell)$ isomorphic to S_4. Then there is no maximal Hasse subgroup G of $\mathrm{GL}_2(\mathbb{F}_\ell).2$ for which $G_0 = H_0$.

Proof (1) All matrices in $H \setminus H_0$ are of the form

$$\begin{pmatrix} A & 0 \\ 0 & A^{-T} \end{pmatrix} \begin{pmatrix} & J_2 \\ -J_2 & \end{pmatrix} = \begin{pmatrix} 0 & AJ_2 \\ -A^{-T}J_2 & 0 \end{pmatrix}$$

for some $A \in H_0$. Such a matrix has an $\mathbb{F}_\ell$-rational eigenvalue if and only if the product $(AJ_2)(-A^{-T}J_2)$ has an $\mathbb{F}_\ell$-rational eigenvalue that is a square in $\mathbb{F}_\ell^\times$. Writing $A = \lambda B$ with $\det(B) = 1$ and using the matrix identity in the proof of Lemma 3.15 one checks easily that $(AJ_2)(-A^{-T}J_2) = B^2$. Since by assumption A (and hence also B) has an $\mathbb{F}_\ell$-rational eigenvalue, this matrix has an $\mathbb{F}_\ell$-rational eigenvalue that is a square. Combining this observation with Corollary 3.13 we see that H is Hasse.
Now, if G is any Hasse subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell).2$ such that $G_0 = H_0$, then H_0 is normal in G, so G is contained in N, the normaliser of H_0 in $\mathrm{GL}_2(\mathbb{F}_\ell).2$.

In the cases $\mathbb{P}H_0 \cong S_4$ or A_5, it follows immediately from the previous lemma that either $G = H_0$ (which, however, is not Hasse, since H_0 obviously stabilizes two 2-dimensional subspaces) or $G = N = H$, as claimed.
If $\mathbb{P}H_0 \cong A_4$, then $[N : H_0] = 4$, and G is a union of H_0-cosets of N. By part (3) of Lemma 3.15 we see that G cannot meet the coset represented by $J'\begin{pmatrix}\sigma & 0\\ 0 & \sigma^{-T}\end{pmatrix}$. This implies $[G : H_0] \leq 2$, and since H_0 itself is not Hasse we must have $[G : H_0] = 2$. If the non-trivial coset of H_0 in G were represented by $\begin{pmatrix}\sigma & 0\\ 0 & \sigma^{-T}\end{pmatrix}$ the action of G on $\mathbb{F}_\ell^4$ would be reducible, contradiction, so we must have $G = \langle H_0, J'\rangle = H$ as claimed.

(2) Consider the normaliser N of H_0 in $\mathrm{GL}_2(\mathbb{F}_\ell).2$. By Lemma 3.15 we know that $N = (H_0 \sqcup \begin{pmatrix}\sigma & 0\\ 0 & \sigma^{-T}\end{pmatrix} H_0) \sqcup (H_0 \sqcup \begin{pmatrix}\sigma & 0\\ 0 & \sigma^{-T}\end{pmatrix} H_0)J'$, where $\det(\sigma)$ is a square in $\mathbb{F}_\ell^\times$, because by assumption $\mathbb{P}H_0$ extends to a subgroup of $\mathrm{PSL}_2(\mathbb{F}_\ell)$ isomorphic to S_4. Note that this happens only if $\ell \equiv \pm 1 \pmod 8$, and since $\ell \equiv 1 \pmod 4$ we obtain $\ell \equiv 1 \pmod 8$. Reasoning as in the proof of part (3) of Lemma 3.15 we see easily that N is Hasse (notice that the elements of $S_4 \setminus A_4$ have order dividing 4, so their lifts to $\mathrm{SL}_2(\mathbb{F}_\ell)$ have order dividing 8; it follows that the elements of the coset $H_0\sigma$ have $\mathbb{F}_\ell$-rational eigenvalues since $\ell \equiv 1 \pmod 8$). If G is a group with $G_0 = H_0$, then H_0 is normal in G and hence $G \leq N$. By maximality of G we should have $G = N$, but $N_0 \neq H_0$, as desired.

□

Combining the previous lemmas we obtain:

Proposition 3.17 *Let G' be a maximal subgroup of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell).2$. The maximal Hasse subgroups G of G' with $\mathbb{P}G_0$ isomorphic to A_4, S_4 or A_5 are as follows:*

Group	Condition
$(C_{(\ell-1)/2}.\mathrm{SL}_2(\mathbb{F}_3)).2$	$\ell \equiv 13 \pmod{24}$, $\ell \not\equiv 1 \pmod 5$
$(C_{(\ell-1)/2}.\widehat{S_4}).2$	$\ell \equiv 1 \pmod{24}$
$(C_{(\ell-1)/2}.\mathrm{SL}_2(\mathbb{F}_5)).2$	$\ell \equiv 1 \pmod{60}$

Proof Let G be a Hasse subgroup of G' and such that $\mathbb{P}G_0$ is isomorphic to A_4, S_4 or A_5. If G is maximal with such properties, then by Corollary 3.12 we know that it contains the group H_1. By Lemma 3.14, we have $\ell \equiv 1 \pmod 4$ and $\mathbb{P}G_0$ is contained in $\mathrm{PSL}_2(\mathbb{F}_\ell)$, so G_0 is contained in $\mathrm{GL}_2^{\square}(\mathbb{F}_\ell)$ and contains $\mathbb{F}_\ell^\times \mathrm{Id}$. The hypotheses imply that G_0 has elements of order 3, so the condition that every element of G_0 has $\mathbb{F}_\ell$-rational eigenvalues implies $\ell \equiv 1 \pmod{12}$. Consider the following cases:

(1) if $\ell \equiv 1 \pmod 5$, then by [4, Table 8.2] the group $\mathrm{SL}_2(\mathbb{F}_\ell)$ contains a maximal subgroup isomorphic to $\mathrm{SL}_2(\mathbb{F}_5)$ with projective image A_5. This group satisfies

the assumptions of Corollary 3.16, so we get a maximal subgroup isomorphic to

$$\langle \mathrm{SL}_2(\mathbb{F}_5), \mathbb{F}_\ell^\times \mathrm{Id}, J' \rangle = (C_{(\ell-1)/2}.\mathrm{SL}_2(\mathbb{F}_5)).2.$$

From the previous discussion it is clear that the conditions $\ell \equiv 1 \pmod{60}$ are necessary and sufficient in order for this subgroup to be Hasse. Moreover, in this case we do not get any Hasse maximal subgroup X such that $\mathbb{P}X_0 \cong A_4$: this is proven exactly as in part (2) of Corollary 3.16, using the fact that in this case $\mathbb{P}X_0$ extends to a subgroup isomorphic to A_5.

(2) if $\ell \equiv 1 \pmod 8$, then $\mathrm{SL}_2(\mathbb{F}_\ell)$ contains a maximal subgroup isomorphic to $\widehat{S_4}$, and reasoning as above we find a maximal Hasse subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell).2$ isomorphic to $(C_{(\ell-1)/2}.\widehat{S_4}).2$. Moreover, by Corollary 3.16 (2) we see that $\mathrm{GL}_2(\mathbb{F}_\ell).2$ cannot contain maximal subgroups X with $\mathbb{P}X_0 \cong A_4$.

(3) if $\ell \not\equiv 1 \pmod 5$ and $\ell \equiv 5 \pmod 8$, then $\mathrm{SL}_2(\mathbb{F}_\ell)$ contains a maximal subgroup isomorphic to $\mathrm{SL}_2(\mathbb{F}_3)$ whose projective image is a maximal subgroup of $\mathrm{PSL}_2(\mathbb{F}_\ell)$ isomorphic to A_4. This group satisfies the assumptions of Corollary 3.16 (1), so we get a maximal Hasse subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell).2$ isomorphic to $\langle \mathrm{SL}_2(\mathbb{F}_3), \mathbb{F}_\ell^\times, J' \rangle \cong (C_{(\ell-1)/2}.\mathrm{SL}_2(\mathbb{F}_3)).2$.

□

3.5 G of type C_2: $G < \mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$

In this section we prove:

Proposition 3.18 *Let $G < \mathrm{Sp}_4(\mathbb{F}_\ell)$ be a Hasse group contained (up to conjugacy) in $\mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$. Then, one of the following holds:*

- $\ell \equiv 1 \pmod 4$ *and G is contained in a group that is isomorphic to $(Q_{2(\ell-1)} \times Q_{2(\ell-1)}).C_2$.*
- *G is contained in one of the groups described in Sect. 3.5.5.*

Let $\pi : \mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2 \to S_2$ be the natural projection and consider $\ker \pi \cong \mathrm{SL}_2(\mathbb{F}_\ell) \times \mathrm{SL}_2(\mathbb{F}_\ell)$. We write elements of $\mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$ as triples (g, h, ε) with $g, h \in \mathrm{SL}_2(\mathbb{F}_\ell)$ and $\varepsilon \in \{\pm 1\}$, where $(g, h, 1)$ denotes the matrix $\begin{pmatrix} g & 0 \\ 0 & h \end{pmatrix}$ and $(g, h, -1)$ denotes $\begin{pmatrix} 0 & g \\ h & 0 \end{pmatrix}$. If $\pi(G) = \{1\}$, then G is a subgroup of $\mathrm{SL}_2(\mathbb{F}_\ell) \times \mathrm{SL}_2(\mathbb{F}_\ell)$ and does not act irreducibly. Therefore, $\pi(G) = \{\pm 1\}$. Let $(g, h, -1) \in G$ and let G_1 (resp. G_2) be the projection of $G_0 = \ker \pi \cap G$ to the first (resp. second) factor $\mathrm{SL}_2(\mathbb{F}_\ell)$. Note that

$$(g, h, -1)(g_1, g_2, 1)(g, h, -1)^{-1} = (gg_2g^{-1}, hg_1h^{-1}, 1),$$

so the map $\varphi_h : G_1 \to G_2$ given by $\varphi(g_1) = hg_1h^{-1}$ is well-defined and bijective, with inverse $g_2 \mapsto h^{-1}g_2h$. Thus, G_1 and G_2 are conjugate inside $\mathrm{SL}_2(\mathbb{F}_\ell)$. Up to a change of basis via the (symplectic) matrix $\begin{pmatrix} \mathrm{Id} & 0 \\ 0 & h \end{pmatrix}$, we can assume that $G_1 = G_2$. Hence, G_0 is a sub-direct product of $\mathrm{SL}_2(\mathbb{F}_\ell)$ with itself or is contained in $M \times M$ with

M a maximal subgroup of $\mathrm{SL}_2(\mathbb{F}_\ell)$. By the classification of the maximal subgroups of $\mathrm{SL}_2(\mathbb{F}_\ell)$ we have that (up to conjugacy) M can be $Q_{2(\ell-1)}$, $Q_{2(\ell+1)}$, a Borel subgroup, or E, where E is a group such that $\mathbb{P}E$ is A_4, A_5, or S_4. Recalling that the only non-trivial normal subgroup of $\mathrm{SL}_2(\mathbb{F}_\ell)$ is $\{\pm 1\}$ and applying Goursat's Lemma, one sees that every non-trivial sub-direct product of $\mathrm{SL}_2(\mathbb{F}_\ell)$ with itself is contained in $\mathcal{G} = \{(g, \pm g, \pm 1) \mid g \in \mathrm{SL}_2(\mathbb{F}_\ell)\}$.

3.5.1 Case $G_0 < \mathcal{G}$

Since $\mathrm{SL}_2(\mathbb{F}_\ell)$ contains matrices without a rational eigenvalue, G_0 cannot be all of $\mathcal{G}$. Hence G_0 is contained in a group of the form $\{(g, \pm g, 1) \mid g \in M\}$ for a certain proper maximal subgroup M of $\mathrm{SL}_2(\mathbb{F}_\ell)$. In particular, G_0 is a subgroup of $M \times M$ with M a maximal subgroup of $\mathrm{SL}_2(\mathbb{F}_\ell)$, so this case is included in one of the cases below.

3.5.2 Case M Borel

Recall that $G_0 = G \cap \ker \pi$. The group G_0 fixes a line $\langle v \rangle$, and G does not act irreducibly by the same argument as in Sect. 3.4.3, so G is not Hasse.

3.5.3 Case $M \cong Q_{2(\ell+1)}$

Assume first that $\ell \equiv 3 \pmod 4$. Every element of G_0 has order that divides $(\ell + 1)$. Any element $(q_1, q_2, 1) \in G_0$ has a rational eigenvalue, hence q_1 or q_2 has a rational eigenvalue and therefore its order divides $\ell - 1$. Hence, at least one between q_1 and q_2 has order that divides $\gcd(\ell - 1, \ell + 1) = 2$. The only elements in $Q_{2(\ell+1)}$ of order that divides 2 are ± 1. Therefore, G_0 is contained in $\{(q, \pm 1, 1) \mid q \in Q_{2(\ell+1)}\} \cup \{(\pm 1, q, 1) \mid q \in Q_{2(\ell+1)}\}$, hence $G_0 \leq Q_{2(\ell+1)} \times \mathbb{Z}/2\mathbb{Z}$ or $G_0 \leq \mathbb{Z}/2\mathbb{Z} \times Q_{2(\ell+1)}$. In both cases, G_0 fixes a line and G does not act irreducibly, contradiction. The case $\ell \equiv 1 \pmod 4$ is similar: one proves that q_1 or q_2 has order that divides 4, hence $G_0 \leq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, and this subgroup fixes a line. So, G is not Hasse.

3.5.4 Case $M \cong Q_{2(\ell-1)}$

Recall the description of the group Q_{4n} from Sect. 2.3.1. Assume first $\ell \equiv 3 \pmod 4$. Observe that G_0 cannot contain an element $(s_1, s_2, 1)$ with $s_1, s_2 \notin \mathbb{Z}/(\ell - 1)\mathbb{Z}$ since such an element does not have a rational eigenvalue as $\mathrm{ord}(s_1) = \mathrm{ord}(s_2) = 4 \nmid \ell - 1$. Therefore, $G_0 \subseteq \{\mathbb{Z}/(\ell - 1)\mathbb{Z} \times Q_{2(\ell-1)}\} \cup \{Q_{2(\ell-1)} \times \mathbb{Z}/(\ell - 1)\mathbb{Z}\}$. Proceeding as in the previous case we conclude that G does not act irreducibly.

Assume now that $\ell \equiv 1 \pmod 4$. We start by showing that the exponent of G divides $\ell - 1$. The elements of G_0 have order dividing $\ell - 1$. Let $g \in G \setminus G_0$. Its characteristic polynomial is of the form $x^4 + bx^2 + 1$, hence its eigenvalues are of the form $\pm\lambda^{\pm 1}$. If one such eigenvalue is rational, then they all are, and it follows as desired that the order of g divides $\ell - 1$. Let $\mathcal{H}$ be the set of subgroups of $\mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$ with exponent that divides $\ell - 1$, that act irreducibly, and such that the intersection

with $\ker\pi$ is contained in $Q_{2(\ell-1)} \times Q_{2(\ell-1)}$. Observe that (up to conjugacy) G is contained in a maximal element of $\mathcal{H}$ with respect to inclusion. We want to classify these maximal elements. Let H be a maximal element of $\mathcal{H}$, let $H_0 = H \cap \ker\pi$ and $(z, w, -1) \in H \setminus H_0$.

Assume that each of z and w is diagonal or anti-diagonal. Let H' be the subgroup of $Q_{2(\ell-1)} \wr S_2$ defined by

$$H' := \{(x, y, 1) \mid x, y \in Q_{2(\ell-1)} \text{ and } xy \in \mathbb{Z}/((\ell-1)/2)\mathbb{Z}\}. \tag{5}$$

The group H' is normalised by H, so $\langle H, H'\rangle = HH'$. One can easily show that, given $g \in H$ with $\mathrm{ord}(g) \mid \ell - 1$, we have $\mathrm{ord}(gh') \mid \ell - 1$ and $\mathrm{ord}(h'g) \mid \ell - 1$ for all $h' \in H'$. Therefore, $\langle H, H'\rangle$ is in $\mathcal{H}$ and hence $H' \leq H$.

Otherwise, assume that at least one between z and w is neither diagonal nor anti-diagonal. By Lemma 3.7 we have $H_0 \cong Q_8 \times Q_8$.

In conclusion, the maximal groups in $\mathcal{H}$ are isomorphic to $(Q_8 \times Q_8).C_2$ or contain H'. Since G is Hasse, it is contained in a maximal subgroup in $\mathcal{H}$. If $G \leq (Q_8 \times Q_8).C_2$, then $G_0 \leq Q_8 \times Q_8$ and it is contained in $(E \times E)$, where $\mathbb{P}E \cong S_4$. We study this case in Sect. 3.5.5. If G is contained in a maximal group H of $\mathcal{H}$ that contains H', then $\ell \equiv 1 \pmod 4$. Since H' has index 4 in $Q_{2(\ell-1)} \times Q_{2(\ell-1)}$, we have that H has order $2(\ell-1)^2$ or $4(\ell-1)^2$. Observe that $\mathcal{H}$ is non-empty for all $\ell \equiv 1 \pmod 4$ since it contains $\langle H', (\mathrm{Id}, \mathrm{Id}, -1)\rangle$.

Remark 3.19 Let H be a maximal Hasse subgroup that contains H'. Note that H' is normal in $Q_{2(\ell-1)} \wr S_2$ and $(Q_{2(\ell-1)} \wr S_2)/H' \cong (\mathbb{Z}/2\mathbb{Z})^3$. So, H corresponds to a subgroup $\overline{H}$ of $(Q_{2(\ell-1)} \wr S_2)/H' \cong (\mathbb{Z}/2\mathbb{Z})^3$. Let X_{-1} be the subset of $(Q_{2(\ell-1)} \wr S_2)/H'$ given by the classes of elements of the form $(x, y, -1)$. Since H is Hasse, $\overline{H}$ contains an element in X_{-1}. If $\ell \equiv 5 \pmod 8$, the only class in X_{-1} that can belong to $\overline{H}$ is the class of $(\mathrm{Id}, \mathrm{Id}, -1)H'$, since the other classes contain elements without a rational eigenvalue. Hence, $H = \langle H', (\mathrm{Id}, \mathrm{Id}, -1)\rangle$ and $|H| = 2(\ell-1)^2$. If $\ell \equiv 1 \pmod 8$, three of the four classes in X_{-1} have the property that every element in the class has a rational eigenvalue. By maximality we obtain that $\overline{H}$ is generated by two of these three classes, hence that it has order 4. It follows that there are 3 possible choices of $\overline{H}$, each leading to a maximal subgroup H of order $4(\ell-1)^2$.

Remark 3.20 Let G' be the maximal Hasse subgroup described in Eq. (4), that is, the group listed in the first line of Table 1. The base change corresponding to $M := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$ takes the symplectic form of Eq. (1) into the symplectic form of Eq. (2). Simultaneously, it conjugates G' into a subgroup G'' of $Q_{2(\ell-1)} \wr S_2$ which, in the notation of this section, is $G'' = \langle H', (\mathrm{Id}, \mathrm{Id}, -1)\rangle$. Hence, the group $(N_{\mathrm{GL}_2(\mathbb{F}_\ell)}(C_s)).2$ of the first line of Table 1 is always contained (up to conjugacy) in the groups of the fifth or sixth line of the table.

3.5.5 Case $M \cong E$

All these cases can be treated using the algorithm of Sect. 3.2. The results are listed in Table 1 and correspond to (part of) Proposition 2 in [6].

3.6 G of type $\mathcal{C}_3$

The goal of this section is to prove the following.

Proposition 3.21 *Let G' be a maximal subgroup of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ of type $\mathcal{C}_3$, hence isomorphic to $\mathrm{SL}_2(\mathbb{F}_{\ell^2}).2$ or $\mathrm{GU}_2(\mathbb{F}_\ell).2$. In the first case, G' does not contain Hasse subgroups. In the second case, the maximal Hasse subgroups of G' are as follows:*

Group	Condition
$\mathrm{SL}_2(\mathbb{F}_3)$	$\ell \equiv 5 \pmod{24}$
$\widehat{S}_4$	$\ell \equiv 17 \pmod{24}$

This result follows from Propositions 3.25 and 3.27 below. We start by describing explicitly the two (conjugacy classes of) maximal subgroups of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ of type $\mathcal{C}_3$. Table 8.12 in [4] shows that all the maximal subgroups of type $\mathcal{C}_3$ that are abstractly isomorphic form a single conjugacy class, so it suffices to study a specific subgroup of each type.

A subgroup G of type $\mathcal{C}_3$ consists of all transformations in $\mathrm{Sp}_4(\mathbb{F}_\ell)$ that act either $\mathbb{F}_{\ell^2}$-linearly or $\mathbb{F}_{\ell^2}$-anti-linearly for a given $\mathbb{F}_{\ell^2}$-vector space structure on $\mathbb{F}_\ell^4$. In order to construct such groups we start with the vector space $V_2 = \mathbb{F}_{\ell^2}^2$, whose basis vectors we denote by $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. We denote by σ the non-trivial element of $\mathrm{Gal}(\mathbb{F}_{\ell^2}/\mathbb{F}_\ell)$ and equip V_2 with one of the following forms:

(1) the symplectic form characterised by $\langle e_1, e_2 \rangle = 1$;
(2) the Hermitian form characterised by $\langle e_1, e_1 \rangle_H = \langle e_2, e_2 \rangle_H = 0$ and $\langle e_1, e_2 \rangle_H = \sqrt{d}$.

Remark 3.22 Recall that a Hermitian form on $V_2 \cong \mathbb{F}_{\ell^2}^2$ is a map $\langle \cdot, \cdot \rangle : V_2 \times V_2 \to \mathbb{F}_{\ell^2}$ that is $\mathbb{F}_{\ell^2}$-linear in the first argument and satisfies $\langle v_2, v_1 \rangle = \sigma(\langle v_1, v_2 \rangle)$ for all $v_1, v_2 \in V_2$.

We fix once and for all $d \in \mathbb{F}_\ell^\times$ a non-square; in case ℓ is congruent to 3 modulo 4, we take $d = -1$. Setting $e_3 = \sqrt{d}e_1$ and $e_4 = \sqrt{d}e_2$, we obtain that e_1, e_2, e_3, e_4 is an $\mathbb{F}_\ell$-basis of V_2. We will represent $\mathbb{F}_\ell$-linear transformations of V_2 in the basis $e_1, \ldots, e_4$. In particular, we let

$$\tau := \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & -1 & \\ & & & -1 \end{pmatrix} \tag{6}$$

denote the matrix giving the natural action of σ on V_2. We are now ready to describe the maximal subgroups of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ of type $\mathcal{C}_3$.

The subgroup $\mathrm{SL}_2(\mathbb{F}_{\ell^2}).2$. Consider the subgroup $\mathrm{SL}_2(\mathbb{F}_{\ell^2})$ of $\mathrm{GL}_2(\mathbb{F}_{\ell^2})$. An element

$$g = \begin{pmatrix} a_{11} + b_{11}\sqrt{d} & a_{12} + b_{12}\sqrt{d} \\ a_{21} + b_{21}\sqrt{d} & a_{22} + b_{22}\sqrt{d} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_{\ell^2})$$

acts on $\mathbb{F}_\ell^4$ (with respect to our coordinates) via

$$\iota(g) = \begin{pmatrix} a_{11} & a_{12} & db_{11} & db_{12} \\ a_{21} & a_{22} & db_{21} & db_{22} \\ b_{11} & b_{12} & a_{11} & a_{12} \\ b_{21} & b_{22} & a_{21} & a_{22} \end{pmatrix}, \tag{7}$$

and it is easy to check that the condition $\det(g) = 1$ implies that $\iota(g)$ preserves the symplectic form with matrix $\begin{pmatrix} & 1 & & \\ -1 & & & \\ & & & d \\ & & -d & \end{pmatrix}$. Notice that this is the $\mathbb{F}_\ell$-bilinear form obtained as $\mathrm{tr}_{\mathbb{F}_{\ell^2}/\mathbb{F}_\ell}(\langle\cdot,\cdot\rangle)$. The subgroup $\iota(\mathrm{SL}_2(\mathbb{F}_{\ell^2}))$ of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ is normalised by τ, and we write $\mathrm{SL}_2(\mathbb{F}_{\ell^2}).2$ for the group generated by $\iota(\mathrm{SL}_2(\mathbb{F}_{\ell^2}))$ and by τ. This subgroup preserves the bilinear form just described. From now on, we shall identify $\mathrm{SL}_2(\mathbb{F}_{\ell^2})$ with its image via ι. For a subgroup G of $\mathrm{SL}_2(\mathbb{F}_{\ell^2}).2$, we denote by G_0 the intersection of G with $\mathrm{SL}_2(\mathbb{F}_{\ell^2})$.

Remark 3.23 Let $g \in \mathrm{SL}_2(\mathbb{F}_{\ell^2})$ that has eigenvalues $\lambda, 1/\lambda$. So, the eigenvalues of $\iota(g)$ are $\lambda, \sigma(\lambda), \lambda^{-1}, \sigma(\lambda)^{-1}$. In particular, $\iota(g)$ has an $\mathbb{F}_\ell$-rational eigenvalue if and only if all of its eigenvalues are $\mathbb{F}_\ell$-rational. Moreover, $\tau\iota(g)$ has characteristic polynomial of the form $t^4 + at^2 + 1$ for some $a \in \mathbb{F}_\ell$, so its eigenvalues are of the form $\pm\mu, \pm\mu^{-1}$. It follows that an element in $\mathrm{SL}_2(\mathbb{F}_{\ell^2}).2$ has an $\mathbb{F}_\ell$-rational eigenvalue if and only if all of its eigenvalues are $\mathbb{F}_\ell$-rational.

The subgroup $\mathrm{GU}_2(\mathbb{F}_\ell).2$. Let $\mathrm{GU}_2(\mathbb{F}_\ell) \subseteq \mathrm{GL}_2(\mathbb{F}_{\ell^2})$ be the isometry group of $\langle\cdot,\cdot\rangle_H$, that is, the subgroup of $\mathrm{GL}_2(\mathbb{F}_{\ell^2})$ consisting of those g that satisfy

$$\langle gv_1, gv_2\rangle_H = \langle v_1, v_2\rangle_H \quad \forall v_1, v_2 \in V_2,$$

or equivalently, ${}^t g \begin{pmatrix} 0 & \sqrt{d} \\ -\sqrt{d} & 0 \end{pmatrix} \sigma(g) = \begin{pmatrix} 0 & \sqrt{d} \\ -\sqrt{d} & 0 \end{pmatrix}$.

Lemma 3.24 *Let $\mu \in \mathbb{F}_{\ell^2}^\times$ be an element of norm -1 and let H be the group*

$$\left\{\lambda g : g \in \mathrm{SL}_2(\mathbb{F}_\ell), \lambda \in \ker\left(N_{\mathbb{F}_{\ell^2}/\mathbb{F}_\ell} : \mathbb{F}_{\ell^2}^\times \to \mathbb{F}_\ell^\times\right)\right\}.$$

The group $\mathrm{GU}_2(\mathbb{F}_\ell)$ coincides with $H \sqcup H \cdot \begin{pmatrix} \mu/\sqrt{d} & 0 \\ 0 & \mu\sqrt{d} \end{pmatrix}$. In particular, $\mathrm{GU}_2(\mathbb{F}_\ell)$ is contained in $\mathbb{F}_{\ell^2}^\times \mathrm{Id} \cdot \mathrm{GL}_2(\mathbb{F}_\ell)$, and $\mathbb{P}\,\mathrm{GU}_2(\mathbb{F}_\ell)$ coincides with $\mathrm{PGL}_2(\mathbb{F}_\ell)$.

Proof One checks that all the elements given in the statement preserve $\langle \cdot, \cdot \rangle_H$, hence that they are in $\mathrm{GU}_2(\mathbb{F}_\ell)$. On the other hand, by [4, Theorem 1.6.22] we have

$$|\mathrm{GU}_2(\mathbb{F}_\ell)| = 2 \cdot \frac{\ell+1}{2} \cdot \ell(\ell^2-1) = \left| H \sqcup H \begin{pmatrix} \mu/\sqrt{d} & 0 \\ 0 & \mu\sqrt{d} \end{pmatrix} \right|,$$

which concludes the proof. □

The $\mathbb{F}_\ell$-bilinear form on $V_2 \cong \mathbb{F}_\ell^4$ given by

$$\langle v, w \rangle := \frac{\langle v, w \rangle_H - \langle w, v \rangle_H}{2\sqrt{d}}$$

is anti-symmetric and invariant under the action of $\mathrm{GU}_2(\mathbb{F}_\ell)$ by definition of this group. We consider $\mathrm{Sp}_4(\mathbb{F}_\ell)$ and $\mathrm{GSp}_4(\mathbb{F}_\ell)$ as the groups of transformations that preserve (resp. preserve up to scalars) this symplectic form. We denote by $\mathrm{GU}_2(\mathbb{F}_\ell).2$ the subgroup of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ generated by $\iota(\mathrm{GU}_2(\mathbb{F}_\ell))$ and τ (this latter element normalises $\iota(\mathrm{GU}_2(\mathbb{F}_\ell))$). For a subgroup G of $\mathrm{GU}_2(\mathbb{F}_\ell).2$, we denote by G_0 the intersection of G with $\iota(\mathrm{GU}_2(\mathbb{F}_\ell))$.

3.6.1 Subgroups of $\mathrm{SL}_2(\mathbb{F}_{\ell^2}).2$

Let G be a maximal Hasse subgroup of $\mathrm{SL}_2(\mathbb{F}_{\ell^2}).2$. We consider $G_0 = G \cap \iota(\mathrm{SL}_2(\mathbb{F}_{\ell^2}))$ as a subgroup of $\mathrm{SL}_2(\mathbb{F}_{\ell^2})$. We now distinguish cases according to which maximal subgroups of $\mathrm{SL}_2(\mathbb{F}_{\ell^2})$ contain G_0; we rely on Table 8.1 of [4].

(1) $G_0 = \mathrm{SL}_2(\mathbb{F}_{\ell^2})$. It is clear that G_0 contains elements that do not have $\mathbb{F}_\ell$-rational eigenvalues, so G cannot be Hasse.

(2) G_0 is contained in a Borel subgroup. Using the fact that all the eigenvalues of the elements of G_0 are rational (Remark 3.23), we see that the group $G_0 \subseteq \mathrm{Sp}_4(\mathbb{F}_\ell)$ stabilises a 1-dimensional subspace V of $\mathbb{F}_\ell^4$. If $G \neq G_0$, let g be an element of $G \setminus G_0$: then g normalises G_0 (since $[G : G_0] = 2$) and the subspace $W = V + gV$, of dimension at most 2, is stable under the action of G. Thus G cannot be Hasse.

(3) G_0 is contained in $Q_{2(\ell^2+1)}$. An element $g \in G_0$ has one $\mathbb{F}_\ell$-rational eigenvalue if and only if both its eigenvalues are $\mathbb{F}_\ell$-rational (their product is 1), if and only if $g^{\ell-1} = \mathrm{Id}$. This implies that the order of every $g \in G_0$ divides $(\ell^2+1, \ell-1) = 2$, so G_0 is either $\mathbb{Z}/2\mathbb{Z}$ or $(\mathbb{Z}/2\mathbb{Z})^2$. In both cases, G_0 stabilizes a line in $\mathbb{F}_{\ell^2}^2$ and we are reduced to the previous case. The conclusion is that G cannot be Hasse.

(4) G_0 is contained in $Q_{2(\ell^2-1)}$. Reasoning as in the previous case, we obtain that G_0 is contained in $Q_{2(\ell-1)}$, which—up to conjugacy—is a subgroup of $\mathrm{SL}_2(\mathbb{F}_\ell)$. More generally, we prove that G_0 cannot be (conjugate to) a subgroup of $\mathrm{SL}_2(\mathbb{F}_\ell)$. Indeed, if this is the case, $\iota(G_0)$ stabilizes the non-trivial subspaces $\langle e_1, e_2 \rangle_{\mathbb{F}_\ell}$ and $\langle e_3, e_4 \rangle_{\mathbb{F}_\ell}$ of $\mathbb{F}_\ell^4$. Moreover, it acts on both subspaces with the same character. Proposition 3.9 (3), which we can apply by Remark 3.23, implies that G cannot be Hasse.

(5) G_0 is isomorphic to a subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$, $\widehat{S_4}$, or $\mathrm{SL}_2(\mathbb{F}_5)$. In the first two cases, the subgroup G_0 is conjugate to a subgroup of $\mathrm{SL}_2(\mathbb{F}_\ell)$, and by what we proved in the previous case we obtain that G cannot be Hasse. In the case $\mathrm{SL}_2(\mathbb{F}_5)$, either G_0 is again conjugate to a subgroup of $\mathrm{SL}_2(\mathbb{F}_\ell)$, or $\ell \equiv \pm 3 \pmod{10}$, see [4, Table 8.2]. However, in the latter case no element of G_0 of order 5 can have $\mathbb{F}_\ell$-rational eigenvalues, so $5 \nmid |G_0|$. Any such G_0 is conjugate to a subgroup of $\widehat{S_4}$, so we obtain a contradiction as above.

(6) G_0 is contained in $\mathrm{SL}_2(\mathbb{F}_\ell).2$. Let G_{00} be the intersection of G_0 with $\mathrm{SL}_2(\mathbb{F}_\ell)$. If the order of G_{00} is not divisible by ℓ, then $\ell \nmid |G_0|$ and G_0 is contained in a subgroup maximal among those of order not divisible by ℓ, which are covered by the previous points. On the other hand, if $\ell \mid |G_{00}|$, then by the classification of the subgroups of $\mathrm{SL}_2(\mathbb{F}_\ell)$ we know that either $G_{00} = \mathrm{SL}_2(\mathbb{F}_\ell)$ or G_{00} is contained in a Borel subgroup. In the former case, G_{00} contains elements that do not have $\mathbb{F}_\ell$-rational eigenvalues, which is impossible since G is assumed to be Hasse. In the latter case, G_{00} is normal inside G_0, of index at most 2. Since G_{00} fixes precisely one line $\langle w \rangle$ in $\mathbb{F}_\ell^2$ (any element of order ℓ in $\mathrm{SL}_2(\mathbb{F}_\ell)$ has this property, and we know that $\ell \mid |G_{00}|$), by normality we obtain that G_0 also fixes that line (let g be a representative of the possible non-trivial coset of G_{00} inside G_0. Then $g\langle w \rangle$ is G_{00}-stable, hence it must coincide with $\langle w \rangle$). This implies that G stabilizes a non-trivial subspace, contradiction. The conclusion is that G cannot be Hasse, unless it is already covered by one of the previous cases. But since no Hasse subgroup existed for any of the previous cases, putting everything together we have established:

Proposition 3.25 *The maximal subgroups of* $\mathrm{Sp}_4(\mathbb{F}_\ell)$ *isomorphic to* $\mathrm{SL}_2(\mathbb{F}_{\ell^2}).2$ *contain no Hasse subgroups.*

3.6.2 Subgroups of $\mathrm{GU}_2(\mathbb{F}_\ell).2$

Let G be a maximal Hasse subgroup of $\mathrm{GU}_2(\mathbb{F}_\ell).2$. We consider G_0 as subgroup of $\mathrm{GU}_2(\mathbb{F}_\ell)$, hence of $\mathbb{F}_{\ell^2}^\times \cdot \mathrm{GL}_2(\mathbb{F}_\ell)$. We will show below that the group G fixes a non-trivial subspace of $\mathbb{F}_\ell^4$ (of dimension at most 2) whenever G_0 fixes a line in $\mathbb{F}_{\ell^2}^2$. Therefore, if G is a maximal Hasse subgroup of $\mathrm{GU}_2(\mathbb{F}_\ell).2$, then all the elements in G_0 have $\mathbb{F}_\ell$-rational eigenvalues and G_0 does not stabilize any line in $\mathbb{F}_{\ell^2}^2$. We now distinguish cases according to the structure of $\mathbb{P}G_0$, relying on the classification of the maximal subgroups of $\mathrm{PGL}_2(\mathbb{F}_\ell) = \mathbb{P}\,\mathrm{GU}_2(\mathbb{F}_\ell)$, see Sect. 2.3.1.

(1) Assume $\mathbb{P}G_0 = \mathrm{PSL}_2(\mathbb{F}_\ell)$ or $\mathbb{P}G_0 = \mathrm{PGL}_2(\mathbb{F}_\ell)$. The derived subgroup $(G_0)' \subseteq \mathrm{SL}_2(\mathbb{F}_\ell)$ satisfies $\mathbb{P}((G_0)') = (\mathbb{P}G_0)' = (\mathrm{PSL}_2(\mathbb{F}_\ell))' = \mathrm{PSL}_2(\mathbb{F}_\ell)$. It is easy to show that the only subgroup of $\mathrm{SL}_2(\mathbb{F}_\ell)$ that projects onto $\mathrm{PSL}_2(\mathbb{F}_\ell)$ is $\mathrm{SL}_2(\mathbb{F}_\ell)$ itself. But this would imply that $(G_0)'$ (hence also G_0) contains $\mathrm{SL}_2(\mathbb{F}_\ell)$, contradicting the fact that every element of G_0 has $\mathbb{F}_\ell$-rational eigenvalues.

(2) $\mathbb{P}G_0$ is contained in a Borel subgroup. Then (up to conjugating by a matrix in $\mathrm{GL}_2(\mathbb{F}_\ell)$) all matrices in G_0 are of the form $\lambda \begin{pmatrix} \mu_1 & \star \\ 0 & \mu_2 \end{pmatrix}$ with $\mu_1, \mu_2 \in \mathbb{F}_\ell^\times$ and $\lambda \in \mathbb{F}_{\ell^2}^\times$. Such a matrix admits a rational eigenvalue if and only if λ is in fact in

$\mathbb{F}_\ell^\times$. This implies that G_0 is contained in $\mathrm{GL}_2(\mathbb{F}_\ell)$, so it stabilises an $\mathbb{F}_\ell$-line $\langle v\rangle$. As $[G : G_0] \leq 2$, this implies that G stabilises a subspace of dimension at most 2, contradiction.

(3) $\mathbb{P}G_0$ is contained in the normaliser of a split Cartan subgroup. Up to conjugacy, G_0 is then contained in

$$\left\{\lambda\begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix} : \alpha, \beta \in \mathbb{F}_\ell^\times, \lambda \in \mathbb{F}_{\ell^2}^\times\right\} \cup \left\{\lambda\begin{pmatrix}0 & \alpha\\ \beta & 0\end{pmatrix} : \alpha, \beta \in \mathbb{F}_\ell^\times, \lambda \in \mathbb{F}_{\ell^2}^\times\right\}.$$

A matrix of the form $\lambda\begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix}$ has $\mathbb{F}_\ell$-rational eigenvalues if and only if $\lambda\alpha$ or $\lambda\beta$ are in $\mathbb{F}_\ell$; since α, β are in $\mathbb{F}_\ell^\times$, this implies that λ is also in $\mathbb{F}_\ell^\times$. On the other hand, consider a matrix of the form $\lambda\begin{pmatrix}0 & \alpha\\ \beta & 0\end{pmatrix}$. The condition of rational eigenvalues translates to the fact that $\lambda^2\alpha\beta$ is in $\mathbb{F}_\ell^{\times 2}$. Since α, β are in $\mathbb{F}_\ell^\times$, this implies that λ is either in $\mathbb{F}_\ell^\times$ or in $\mathbb{F}_\ell^\times\sqrt{d}$.

Notice that the set of matrices of the form $\lambda\begin{pmatrix}0 & \alpha\\ \beta & 0\end{pmatrix}$ is a coset for the subgroup

$$\left\{\lambda\begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix} : \alpha, \beta \in \mathbb{F}_\ell^\times, \lambda \in \mathbb{F}_\ell^\times\right\},$$

all of whose elements have $\mathbb{F}_\ell$-rational coefficients. This shows that either all elements $\lambda\begin{pmatrix}0 & \alpha\\ \beta & 0\end{pmatrix}$ satisfy $\lambda \in \mathbb{F}_\ell^\times$ (case 1), or they all satisfy $\lambda \in \mathbb{F}_\ell^\times\sqrt{d}$ (case 2). In case (2), applying ι we see that G_0 acts on $\mathbb{F}_\ell^4$ via the matrices

$$\iota\left(\lambda\begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix}\right) = \lambda\begin{pmatrix}\alpha & & & \\ & \beta & & \\ & & \alpha & \\ & & & \beta\end{pmatrix}, \quad \iota\left(\lambda\begin{pmatrix}0 & \alpha\\ \beta & 0\end{pmatrix}\right) = \frac{\lambda}{\sqrt{d}}\begin{pmatrix} & & & d\alpha\\ & & d\beta & \\ & \alpha & & \\ \beta & & & \end{pmatrix}.$$

From this description we see that $V_1 = \langle e_1, e_4\rangle$ and $V_2 = \langle e_2, e_3\rangle$ are stable under the action of G_0, and that the characters of G_0 on V_1 and V_2 are equal. By Proposition 3.9, we conclude that G does not act irreducibly, contradiction. Note that, in order to apply Proposition 3.9, we need that all eigenvalues of every matrix of G_0 are rational. All the eigenvalues of the diagonal matrices are rational. The matrices $\iota\left(\lambda\begin{pmatrix}0 & \alpha\\ \beta & 0\end{pmatrix}\right)$ have eigenvalues $\pm\sqrt{\lambda^2\alpha\beta}$ (with multiplicity 2), that are $\mathbb{F}_\ell$-rational since, as we noted before, $\lambda^2\alpha\beta$ is a square. In case (1) the proof is similar, but simpler.

(4) $\mathbb{P}G_0$ is contained in the normaliser N of a non-split Cartan subgroup C, which is the maximal cyclic subgroup of N.
Suppose first that $\mathbb{P}G_0$ is contained in C. This implies in particular that $\mathbb{P}G_0$ is cyclic, say generated by the projective image of $g \in G_0$. Since the kernel of

$G_0 \to \mathbb{P}G_0$ consists of scalars that lie in $\mathbb{F}_{\ell^2}^\times$ and have both $\mathbb{F}_\ell$-rational eigenvalues and norm equal to 1, we see that this kernel is contained in $\{\pm \mathrm{Id}\}$ (and in fact, by maximality of G, equal to it). This implies that G is generated by $\iota(g)$, $\iota(-\mathrm{Id})$, and any element h in $G \setminus G_0$ (assuming $G \neq G_0$). Notice that $h^2 \in G_0$ and that by assumption $g \in \mathrm{GU}_2(\mathbb{F}_\ell)$ has at least one $\mathbb{F}_\ell$-rational eigenvalue, so $\iota(g)$ possesses that same eigenvalue. Letting $v \in \mathbb{F}_\ell^4$ denote a corresponding eigenvector, one checks easily that $\langle v, hv\rangle_{\mathbb{F}_\ell}$ is a non-trivial subspace of $\mathbb{F}_\ell^4$ stable under the action of G, contradiction.

Suppose now that $\mathbb{P}G_0$ meets $N \setminus C$, the non-trivial coset of the cyclic group C inside the dihedral group N. Recall from Sect. 2.3.1 that—up to conjugacy in $\mathrm{PGL}_2(\mathbb{F}_\ell)$—elements in $N \setminus C$ are (projective classes of) matrices of the form $\begin{pmatrix} \alpha & d\beta \\ -\beta & -\alpha \end{pmatrix}$ with $\alpha, \beta \in \mathbb{F}_\ell$. Any lift of such a matrix is of the form $\lambda \begin{pmatrix} \alpha & d\beta \\ -\beta & -\alpha \end{pmatrix}$, with characteristic polynomial $t^2 - \lambda^2(-\alpha^2 + d\beta^2)$, hence eigenvalues $\pm\lambda\sqrt{-\alpha^2 + d\beta^2}$. Since $-\alpha^2 + d\beta^2$ is in $\mathbb{F}_\ell$, we see that λ is either in $\mathbb{F}_\ell^\times$ or in $\mathbb{F}_\ell^\times\sqrt{d}$. Now consider *two* elements of G_0 that project to classes lying in $N \setminus C$. The group G_0 contains their product:

$$\lambda_1 \begin{pmatrix} \alpha_1 & d\beta_1 \\ -\beta_1 & -\alpha_1 \end{pmatrix} \lambda_2 \begin{pmatrix} \alpha_2 & d\beta_2 \\ -\beta_2 & -\alpha_2 \end{pmatrix} = \lambda_1\lambda_2 \begin{pmatrix} \alpha_1\alpha_2 - d\beta_1\beta_2 & d(\alpha_1\beta_2 - \alpha_2\beta_1) \\ -\alpha_2\beta_1 + \alpha_1\beta_2 & \alpha_1\alpha_2 - d\beta_1\beta_2 \end{pmatrix}.$$

The eigenvalues of this matrix are

$$\lambda_1\lambda_2\Big((\alpha_1\alpha_2 - d\beta_1\beta_2) \pm \sqrt{d}(\alpha_1\beta_2 - \alpha_2\beta_1)\Big),$$

where $\lambda_1\lambda_2$ is in $\mathbb{F}_\ell^\times$ or in $\mathbb{F}_\ell^\times\sqrt{d}$. In particular, there can be an $\mathbb{F}_\ell$-rational eigenvalue only if we have

$$\alpha_1\alpha_2 - d\beta_1\beta_2 = 0 \quad \text{or} \quad \alpha_1\beta_2 - \alpha_2\beta_1 = 0. \tag{8}$$

Suppose now that for at least one element of $\mathbb{P}G_0 \cap (N \setminus C)$ we have $\beta_1 \neq 0$ (otherwise, $\mathbb{P}G_0 \cap (N \setminus C)$ consists of at most one element, the projective class of $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, hence $|\mathbb{P}G_0| = 2$. We will rule out below the possibility that $|\mathbb{P}G_0| \mid 4$). Then the Eq. (8) imply the equality

$$\begin{aligned} \beta_1 \begin{pmatrix} \alpha_2 & d\beta_2 \\ -\beta_2 & -\alpha_2 \end{pmatrix} &= \begin{pmatrix} \beta_1\alpha_2 & d\beta_1\beta_2 \\ -\beta_1\beta_2 & -\beta_1\alpha_2 \end{pmatrix} \\ &= \begin{pmatrix} \beta_1\alpha_2 & \alpha_1\alpha_2 \\ -\frac{1}{d}\alpha_1\alpha_2 & -\beta_1\alpha_2 \end{pmatrix} \text{ or } \begin{pmatrix} \beta_2\alpha_1 & d\beta_1\beta_2 \\ -\beta_1\beta_2 & -\beta_2\alpha_1 \end{pmatrix}, \end{aligned}$$

which—at the level of projective classes—means

$$\begin{pmatrix} \alpha_2 & d\beta_2 \\ -\beta_2 & -\alpha_2 \end{pmatrix} = \begin{pmatrix} \beta_1 & \alpha_1 \\ -\frac{1}{d}\alpha_1 & -\beta_1 \end{pmatrix} \text{ or } \begin{pmatrix} \alpha_1 & d\beta_1 \\ -\beta_1 & -\alpha_1 \end{pmatrix}.$$

Since $\begin{pmatrix} \alpha_2 & d\beta_2 \\ -\beta_2 & -\alpha_2 \end{pmatrix}$ is an arbitrary element in $\mathbb{P}G_0 \cap (N \setminus C)$, this shows that $\mathbb{P}G_0 \cap (N \setminus C)$ consists of at most 2 elements, so $\mathbb{P}G_0$ has cardinality at most 4 and all elements of order at most 2. It follows that $\mathbb{P}G_0$ is isomorphic to a subgroup of $(\mathbb{Z}/2\mathbb{Z})^2$. Since any subgroup of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$ acts on $\mathbb{P}(\mathbb{F}_\ell^2)$ with a fixed point, this implies that (up to conjugacy in $\mathrm{PGL}_2(\mathbb{F}_\ell)$) the group $\mathbb{P}G_0$ is contained in a Borel subgroup, contradicting what we already proved.

(5) $\mathbb{P}G_0$ is contained in an exceptional subgroup isomorphic to A_4, S_4 or A_5. As observed above, the kernel of the projection map $G_0 \to \mathbb{P}G_0$ is $\{\pm 1\}$, so G_0 is a central extension of degree 2 of a subgroup of one among A_4, S_4, and A_5. In fact, one checks easily that if $\mathbb{P}G_0$ is a proper subgroup of A_4, or a proper subgroup of S_4 distinct from A_4, or a proper subgroup of A_5 distinct from A_4, then $\mathbb{P}G_0$ falls in one of the previous cases, so we may assume $\mathbb{P}G_0 \in \{A_4, S_4, A_5\}$.

Lemma 3.26 *The following hold:*

(a) $\mathbb{P}G_0 \cong A_4$;
(b) $\ell \equiv 1 \pmod 4$;
(c) $\ell \equiv 2 \pmod 3$.

Proof Notice that $\mathbb{P}((G_0)') = (\mathbb{P}G_0)'$. In particular, if $\mathbb{P}G_0 \cong A_5$ we have $(\mathbb{P}G_0)' \cong A_5$, and if $\mathbb{P}G_0 \cong S_4$ then $(\mathbb{P}G_0)' \cong A_4$. Also notice that $(G_0)'$ is a subgroup of $\mathrm{SL}_2(\mathbb{F}_\ell)$ (which, by Lemma 3.24, is the derived subgroup of $\mathrm{GU}_2(\mathbb{F}_\ell)$). In the case $\mathbb{P}(G_0)' \cong A_5$ we obtain that $(G_0)'$ is an extension of degree 2 of A_5 (so by cardinality reasons) $(G_0)' = G_0$. This shows in particular that $G_0 < \mathrm{SL}_2(\mathbb{F}_\ell).2$, so G cannot be Hasse by the work done for the case of $\mathrm{SL}_2(\mathbb{F}_{\ell^2}).2$.

Next suppose that $\mathbb{P}G_0 \cong S_4$. Then reasoning as above we obtain that $(G_0)'$ is a subgroup of $\mathrm{SL}_2(\mathbb{F}_\ell)$ having projective image the exceptional subgroup A_4, so $(G_0)' \cong \mathrm{SL}_2(\mathbb{F}_3)$. Since elements in $(G_0)' < \mathrm{SL}_2(\mathbb{F}_\ell)$ have one $\mathbb{F}_\ell$-rational eigenvalue if and only if they have all their eigenvalues in $\mathbb{F}_\ell$, and since $\mathrm{SL}_2(\mathbb{F}_3)$ contains elements of order 3 and 4, we obtain $\ell \equiv 1 \pmod{12}$. Take an element $\overline{g}$ in $\mathbb{P}G_0$ that under the isomorphism $\mathbb{P}G_0 \cong S_4$ corresponds to a transposition. The element $\overline{g}$ has exactly two lifts $\pm g$ in $\mathrm{GL}_2(\mathbb{F}_\ell)$ with order 4. Since $4 \mid \ell - 1$, the elements $\pm g$ have all their eigenvalues in $\mathbb{F}_\ell$. It follows that no multiple λg with $\lambda \in \mathbb{F}_{\ell^2} \setminus \mathbb{F}_\ell$ has any $\mathbb{F}_\ell$-rational eigenvalues, hence the elements of G_0 that project to $\overline{g}$ must be precisely $\pm g \in \mathrm{GL}_2(\mathbb{F}_\ell)$. Since transpositions generate S_4, it follows that all elements of G_0 are contained in $\mathrm{GL}_2(\mathbb{F}_\ell)$. Reasoning as in the case of $\mathrm{SL}_2(\mathbb{F}_\ell).2$, this gives a contradiction to the fact that G acts irreducibly on $\mathbb{F}_\ell^4$. Having excluded the possibilities $\mathbb{P}G_0 \cong S_4, A_5$, this concludes the proof of (a).

Suppose now that $\mathbb{P}G_0 \cong A_4$, hence $\mathbb{P}((G_0)') \cong (\mathbb{Z}/2\mathbb{Z})^2$. It is easy to see that $(G_0)'$ contains elements of order 4: otherwise, the 2-Sylow subgroup would only have

elements of order 2 and would therefore be commutative. Since elements of order 2 are diagonalisable, and they all commute, all matrices in the 2-Sylow of $(G_0)'$ would be simultaneously diagonalisable in $\mathrm{GL}_2(\mathbb{F}_{\ell^2})$; but there are only 4 diagonal elements of order at most 2 in $\mathrm{GL}_2(\mathbb{F}_{\ell^2})$, while the 2-Sylow of $(G_0)'$ has order 8. Reasoning as above we then obtain that $\ell \equiv 1 \pmod 4$, that is, (b). Finally, suppose by contradiction $\ell \equiv 1 \pmod 3$. Any element $\overline{g}$ of $\mathbb{P}G_0$ has a lift g in $\mathrm{GL}_2(\mathbb{F}_\ell)$, and such an element has order dividing 6 or 4. Since $\ell \equiv 1 \pmod{12}$, the element g has both its eigenvalues in $\mathbb{F}_\ell^\times$, so no multiple of g by a scalar in $\mathbb{F}_{\ell^2} \setminus \mathbb{F}_\ell$ has any $\mathbb{F}_\ell$-rational eigenvalues. It follows that the elements of G_0 whose projective image is $\overline{g}$ are precisely $\pm g$, hence that $G_0 \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$. Reasoning as above, this gives a contradiction to the fact that G acts irreducibly on $\mathbb{F}_\ell^4$. □

The above analysis shows that $|G| = 48$, that G contains a subgroup G_0 isomorphic to $\mathrm{SL}_2(\mathbb{F}_3)$, and that $\ell \equiv 2 \pmod 3$. The problem can now be handled by the methods of Sect. 3.2, and the result is as follows:

Proposition 3.27 *Let G' be a maximal subgroup of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ isomorphic to $\mathrm{GU}_2(\mathbb{F}_\ell).2$. The maximal Hasse subgroups G of G' are as follows:*

Group	Condition
$\mathrm{SL}_2(\mathbb{F}_3)$	$\ell \equiv 5 \pmod{24}$
$\widehat{S_4}$	$\ell \equiv 17 \pmod{24}$

3.7 G of type $\mathcal{C}_6$ and $\mathcal{S}$

These cases can be handled by the algorithm in Sect. 3.2. For groups of class $\mathcal{S}$, one also needs to contend with certain subgroups of $\mathrm{SL}_2(\mathbb{F}_\ell)$ whose order depends on ℓ, but these can be excluded using the arguments in [6, Proposition 4]. The results are listed in Table 1 and correspond to Propositions 3 and 4 and Lemmas 2 and 3 of [6].

4 Hasse subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ that become reducible upon intersection with $\mathrm{Sp}_4(\mathbb{F}_\ell)$

Let G be a Hasse subgroup of $\mathrm{GSp}_4(\mathbb{F}_\ell)$.

Definition 4.1 Let G be a subgroup of $\mathrm{GL}_n(\mathbb{F}_\ell)$. The **saturation** G^{sat} of G is the subgroup of $\mathrm{GL}_n(\mathbb{F}_\ell)$ generated by G and by $\mathbb{F}_\ell^\times \cdot \mathrm{Id}$. We say that G is **saturated** if $G = G^{\mathrm{sat}}$.

The following lemma is obvious:

Lemma 4.2 *Let G be a subgroup of $\mathrm{GL}_n(\mathbb{F}_\ell)$.*

(1) The groups G and G^{sat} (acting on $\mathbb{F}_\ell^n$) have the same invariant subspaces. In particular, G acts irreducibly if and only if G^{sat} does.

(2) G has property (E) if and only if G^{sat} does.
(3) G is Hasse if and only if G^{sat} is.

We note the following formal consequence of the above:

Corollary 4.3 *Every maximal Hasse subgroup of* $\mathrm{GSp}_4(\mathbb{F}_\ell)$ *satisfies* $G = G^{\mathrm{sat}}$.

Remark 4.4 Let G be a saturated subgroup of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ and let $G^1 := G \cap \mathrm{Sp}_4(\mathbb{F}_\ell)$. Then $(G^1)^{\mathrm{sat}}$ coincides with

$$G^{\square} := \ker\left(G \xrightarrow{\lambda} \mathbb{F}_\ell^\times \to \mathbb{F}_\ell^\times/\mathbb{F}_\ell^{\times 2}\right),$$

the subgroup of G consisting of elements having square multiplier, which has index at most 2 in G.

Lemma 4.5 *Let G be a maximal Hasse subgroup of* $\mathrm{GSp}_4(\mathbb{F}_\ell)$ *such that* $G \cap \mathrm{Sp}_4(\mathbb{F}_\ell)$ *is reducible. Then,* $\lambda(G) = \mathbb{F}_\ell^\times$.

Proof By Corollary 4.3 we have $(\mathbb{F}_\ell^\times)^2 \subseteq \lambda(G)$. If $(\mathbb{F}_\ell^\times)^2 = \lambda(G)$, then $G = (G^1)^{\mathrm{sat}}$ and so G^1 acts irreducibly, contradiction. So, there is $\delta \in \mathbb{F}_\ell^\times \setminus (\mathbb{F}_\ell^\times)^2$ in the image of $\lambda(G)$. Hence, $\lambda(G) = \mathbb{F}_\ell^\times$. □

Given a Hasse subgroup G of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ there are two possibilities: either $G^1 = G \cap \mathrm{Sp}_4(\mathbb{F}_\ell)$ is irreducible, in which case it is one of the groups described in Theorem 3.2, or G^1 is reducible, and is then described by the following result.

Theorem 4.6 *Let G be a maximal Hasse subgroup of* $\mathrm{GSp}_4(\mathbb{F}_\ell)$ *such that* $G^1 := G \cap \mathrm{Sp}_4(\mathbb{F}_\ell)$ *acts reducibly. One of the following holds:*

- $\ell \equiv 1 \pmod 4$ *and G is conjugate to* $(C_{(\ell-1)/2}.G^1).2$, *where G^1 is a subgroup of* $N(C_s) \times N(C_s) \cong Q_{2(\ell-1)} \times Q_{2(\ell-1)}$. *Under the action of G^1, the module* $\mathbb{F}_\ell^4$ *decomposes as the direct sum of two non-singular subspaces of dimension 2.*
- $\ell \equiv 3 \pmod 4$ *and G is conjugate to* $(C_{(\ell-1)/2}.H).2$, *where H is a subgroup of* $N_{\mathrm{GL}_2(\mathbb{F}_\ell)}(C_s)$ *of index 2. Under the action of G^1, the module* $\mathbb{F}_\ell^4$ *decomposes as the direct sum of two totally isotropic subspaces of dimension 2.*
- $|\mathbb{P}G| \leq 2^7 \cdot 3^2 \cdot 5^2$.

We split the proof into several lemmas. Theorem 4.6 follows from Lemmas 4.12 and 4.13 below, which also give a more explicit description of the groups in question.

Remark 4.7 In the third case of the Theorem, one can prove that $\mathbb{P}G$ has order dividing $2^9 \cdot 3^2 \cdot 5^2$.

Remark 4.8 Let G be a maximal Hasse subgroup such that G^1 acts reducibly and corresponds to one of the groups of the first two cases of the theorem. In both cases, G has a subgroup of index 2 that decomposes the module $\mathbb{F}_\ell^4$ as the direct sum of two non-singular subspaces of dimension 2. In the same way, G has a subgroup of index 2 that decomposes $\mathbb{F}_\ell^4$ as the direct sum of two isotropic subspaces of dimension 2. This follows easily from the description of the groups given in Lemmas 4.12 and 4.13. In

both cases, the base change that exchanges the two non-singular spaces with the two isotropic spaces is the same as in Remark 3.20. The main difference between the two cases is that, when $\ell \equiv 1 \pmod 4$, then $G^{\square}$ (that has index 2) decomposes $\mathbb{F}_\ell^4$ in two non-singular subspaces, and, when $\ell \equiv 3 \pmod 4$, then $G^{\square}$ decomposes $\mathbb{F}_\ell^4$ in two isotropic subspaces.

Lemma 4.9 *Let G be a maximal Hasse subgroup of $\mathrm{GSp}_4(\mathbb{F}_\ell)$. Suppose that G^1 acts reducibly: then there exist two subspaces V_1, V_2 of $\mathbb{F}_\ell^4$, both of dimension 2 and irreducible under the action of G^1, such that $\mathbb{F}_\ell^4 \cong V_1 \oplus V_2$ and with the property that for every $g \in G \setminus G^{\square}$ one has $g(V_i) = V_{3-i}$ for $i = 1, 2$. Finally, either the restriction of the symplectic form to both V_1 and V_2 is trivial, or the restriction of the symplectic form to both V_1 and V_2 is non-degenerate.*

Proof By Corollary 4.3 we know that G is saturated. By Lemma 4.2 (1) we know that G^1 and $(G^1)^{\mathrm{sat}} = G^{\square}$ have the same invariant subspaces, so it suffices to prove the result with G^1 replaced by $G^{\square}$. Since $[G : G^{\square}] \leq 2$, it follows from Clifford's theorem that the irreducible G-module $\mathbb{F}_\ell^4$ either stays irreducible upon restriction to $G^{\square}$ or splits as the direct sum of two irreducible sub-modules of the same dimension. As the first possibility is ruled out by the assumption of the lemma, the first claim follows. As G acts irreducibly, there is an element in $G \setminus G^{\square}$ that exchanges V_1 and V_2 (hence the same holds for every element in $G \setminus G^{\square}$). Let ω be the anti-symmetric bilinear form we consider on $\mathbb{F}_\ell^4$. The radical of $\omega|_{V_i}$ is a $G^{\square}$-submodule of the irreducible module V_i, hence (for each $i = 1, 2$) it is either trivial or all of V_i. Since any element of $G \setminus G^{\square}$ exchanges V_1 with V_2, the same case must happen for both representations V_i. □

Lemma 4.10 *Let G be a maximal Hasse subgroup of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ such that G^1 acts reducibly. Write $\mathbb{F}_\ell^4 = V_1 \oplus V_2$ as in the previous lemma.*

(1) If V_1, V_2 are both non-singular, then up to conjugacy in $\mathrm{GL}_4(\mathbb{F}_\ell)$ the group G is contained in the group

$$G_{ns} := \left\{ \begin{pmatrix} g_1 & 0 \\ 0 & g_2 \end{pmatrix}, \begin{pmatrix} 0 & g_1 \\ g_2 & 0 \end{pmatrix} \mid g_1, g_2 \in \mathrm{GL}_2(\mathbb{F}_\ell), \det(g_1) = \det(g_2) \right\}.$$

This group preserves the symplectic form of Eq. (2).

(2) If V_1, V_2 are both totally isotropic, then up to conjugacy in $\mathrm{GL}_4(\mathbb{F}_\ell)$ the group G is contained in

$$G_s := \left\{ \begin{pmatrix} g & 0 \\ 0 & \lambda g^{-T} \end{pmatrix}, \begin{pmatrix} 0 & g \\ -\lambda g^{-T} & 0 \end{pmatrix} \mid g \in \mathrm{GL}_2(\mathbb{F}_\ell), \lambda \in \mathbb{F}_\ell^\times \right\}.$$

This group preserves the symplectic form of Eq. (1).

The following hold:

(a) for $h = \begin{pmatrix} g_1 & 0 \\ 0 & g_2 \end{pmatrix} \in G_{ns}$ or $h = \begin{pmatrix} 0 & g_1 \\ g_2 & 0 \end{pmatrix} \in G_{ns}$ we have $\lambda(h) = \det(g_1) = \det(g_2)$;

(b) for $h = \begin{pmatrix} g & 0 \\ 0 & \lambda g^{-T} \end{pmatrix} \in G_s$ *or* $h = \begin{pmatrix} 0 & g \\ -\lambda g^{-T} & 0 \end{pmatrix} \in G_s$ *we have* $\lambda(h) = \lambda$*;*

(c) given a subgroup G *of* $\left\{ \begin{pmatrix} g_1 & 0 \\ 0 & g_2 \end{pmatrix}, \begin{pmatrix} 0 & g_1 \\ g_2 & 0 \end{pmatrix} \mid g_1, g_2 \in \mathrm{GL}_2(\mathbb{F}_\ell) \right\}$*, denote by* G_0 *the subgroup of* G *consisting of block-diagonal matrices. If* G *is as in the statement of the lemma, all matrices* $h \in G_0$ *satisfy* $\lambda(h) \in \mathbb{F}_\ell^{\times 2}$*, and all matrices* $h \in G \setminus G_0$ *satisfy* $\lambda(h) \in \mathbb{F}_\ell^\times \setminus \mathbb{F}_\ell^{\times 2}$*.*

Proof Let $e_1, \dots, e_4$ be the standard basis of $\mathbb{F}_\ell^4$. Up to conjugacy, we may assume that the invariant subspaces are $\langle e_1, e_2 \rangle$, and $\langle e_3, e_4 \rangle$. The claim is then easy to check by direct computation, taking into account the fact that every $h \in G$ either stabilizes both V_1, V_2 or exchanges them. Part (c) follows from the fact that, by Lemma 4.9, $(G^1)^{\mathrm{sat}} = G^\square$ is precisely the subgroup of matrices that send each V_i into itself. □

Lemma 4.11 *Let* I *be a subgroup of* $Q_{2(\ell-1)}$ *not contained in the subgroup generated by* r *(see Sect. 2.3.1). Let* $G \leq I \times I$ *be a sub-direct product of* I *by itself. The group* G *contains an element of the form* (s_1, s_2) *with* s_1 *and* s_2 *symmetries of* $Q_{2(\ell-1)}$*.*

Proof As I is not contained in $\langle r \rangle$, the group G contains two elements of the form $g_1 = (s_1', q_1)$ and $g_2 = (q_2, s_2')$, where s_1', s_2' are symmetries. One of the elements $g_1, g_2, g_1 g_2$ satisfies the conclusion of the lemma. □

Recall that we defined $G^1 = G \cap \mathrm{Sp}_4(\mathbb{F}_\ell)$. We now set $G_0^1 = G_0 \cap G^1$, where G_0 is as in Lemma 4.10.

Lemma 4.12 *Let* G *be a maximal Hasse subgroup of* $\mathrm{GSp}_4(\mathbb{F}_\ell)$*. Suppose that* G^1 *acts reducibly on* $\mathbb{F}_\ell^4$ *and that we are in case 1 of Lemma 4.10. Then,* $\ell \equiv 1 \pmod 4$*. Moreover, one of the following holds:*

(1) G^1 *is conjugate to a subgroup of* $Q_{2(\ell-1)} \times Q_{2(\ell-1)}$*. The matrices with multiplier a square are block-diagonal with blocks diagonal or anti-diagonal. The matrices with multiplier not a square are block-anti-diagonal with blocks diagonal or anti-diagonal.*
(2) $\mathbb{P}G$ *has order smaller than* $2^7 \cdot 3^2 \cdot 5^2$

In case (1), one of the following holds:

(i) $G \setminus G_0$ *contains a block-anti-diagonal matrix* $M = \begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix}$ *with both* x *and* y *diagonal.*
(ii) The fourth power of any block-anti-diagonal matrix is a scalar.

Proof By definition we have $G_0^1 < \mathrm{SL}_2(\mathbb{F}_\ell) \times \mathrm{SL}_2(\mathbb{F}_\ell)$. Let I (resp. J) be the projection of G_0^1 on the first (resp. second) factor $\mathrm{SL}_2(\mathbb{F}_\ell)$, and let δ be a fixed generator of $\mathbb{F}_\ell^\times$. Since G acts irreducibly on $\mathbb{F}_\ell^4$, it contains an element of the form $M = \begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix}$ with $x, y \in \mathrm{GL}_2(\mathbb{F}_\ell)$ and, by Lemma 4.5, we have $\det x = \det y \notin \mathbb{F}_\ell^{\times 2}$. Multiplying the matrix M by a rational constant (recall that G contains all matrices $\lambda\,\mathrm{Id}$ for $\lambda \in \mathbb{F}_\ell^\times$), we can assume $\det x = \det y = \delta$. The group G_0 has index 2 in G, so it is normal in it,

and M belongs to $N_G(G_0)$. The map $\varphi_x : J \to I$ defined as $\varphi_x(j) = xjx^{-1}$ induces an isomorphism $I \to J$.

We now proceed as in Sect. 3.5. The group G_0^1 cannot be a sub-direct product of $\mathrm{SL}_2(\mathbb{F}_\ell)$ by itself, hence $G_0^1 \leq I \times J$ with $I \cong J$ proper subgroups of $\mathrm{SL}_2(\mathbb{F}_\ell)$.

- If I is contained in a Borel subgroup, then G_0^1 fixes a line and G does not act irreducibly on $\mathbb{F}_\ell^4$, contradiction. Note that $(G_0^1)^{\mathrm{sat}} = G_0$ by part (3) of Lemma 4.10.
- If I is contained in $Q_{2(\ell+1)}$, then imposing that all of its elements have an $\mathbb{F}_\ell$-rational eigenvalue yields that G does not act irreducibly, unless $|I| \leq 8$, in which case $|\mathbb{P}G|$ is smaller than $2^7 \cdot 3^2 \cdot 5^2$. This follows from arguments very similar to those in Sect. 3.5.
- If I is exceptional, then $\mathbb{P}G$ has cardinality that divides $2(|I|)^2$. We know that $|I|$ has order at most 120, which implies $|\mathbb{P}G| \leq 2^7 \cdot 3^2 \cdot 5^2$.
- If $I \leq Q_{2(\ell-1)}$ and $\ell \equiv 3 \pmod 4$, then we can prove that G is not Hasse reasoning as in Sect. 3.5. So, we only need to treat the case $I \leq Q_{2(\ell-1)}$ and $\ell \equiv 1 \pmod 4$.
  Assume that $\mathbb{P}G$ is greater than $2^7 \cdot 3^2 \cdot 5^2$. Thanks to Lemma 3.7, x and y are diagonal or anti-diagonal.
  Note that I is not cyclic since otherwise G would not act irreducibly. By Lemma 4.11, G contains a matrix of the form (s_1, s_2). If the blocks x and y of M are both anti-diagonal, then multiplying M by (s_1, s_2) we find that G contains a block-anti-diagonal matrix with x and y diagonal. Thus, the following are equivalent:

  (a) G contains no block-anti-diagonal matrix $\begin{pmatrix} 0 & x' \\ y' & 0 \end{pmatrix}$ with x' and y' both diagonal;

  (b) for every $A = \begin{pmatrix} 0 & x' \\ y' & 0 \end{pmatrix}$ in $G \setminus G_0$ we have that x' is diagonal and y' is anti-diagonal, or vice-versa.

  Assume that property (i) in the statement of the lemma does not hold. Then (a) is true, hence so is (b). Let $A \begin{pmatrix} 0 & x' \\ y' & 0 \end{pmatrix}$ be any element in $G \setminus G_0$. By (b), $x'y' \det(x')^{-1}$ is an anti-diagonal matrix in $Q_{2(\ell-1)}$, so its square is scalar. We conclude that A^4 is a scalar, that is, (ii) holds.

□

Lemma 4.13 *Let G be a maximal Hasse subgroup of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ and suppose that we are in case (2) of Lemma 4.10. Then we have $\ell \equiv 3 \pmod 4$ and up to conjugacy in $\mathrm{GSp}_4(\mathbb{F}_\ell)$ the group G is given by*

$$\left\{ \mu \begin{pmatrix} A & 0 \\ 0 & A^{-T} \end{pmatrix}, \mu \begin{pmatrix} 0 & A \\ A^{-T} & 0 \end{pmatrix} \mid \mu \in \mathbb{F}_\ell^\times, A \in H \right\},$$

where H is a subgroup of index 2 of $N_{\mathrm{GL}_2(\mathbb{F}_\ell)}(C_s)$. In particular, G has order $(\ell-1)^3$.

Proof Observe that the group G_0^1 is of the form $\left\{ \begin{pmatrix} g & 0 \\ 0 & g^{-T} \end{pmatrix} \mid g \in H \right\}$, with H a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. Proceeding as in the case $\mathrm{GL}_2(\mathbb{F}_\ell).2$, we can easily show that $H \leq N(C_s)$ or H is exceptional. Note that the diagonal matrix $\begin{pmatrix} g & 0 \\ 0 & g^{-T} \end{pmatrix}$ has an $\mathbb{F}_\ell$-rational eigenvalue if and only if $g \in \mathrm{GL}_2(\mathbb{F}_\ell)$ does.

We consider first the case when H is exceptional. We will show that no Hasse subgroups arise in this case. If $\ell \equiv 3 \pmod 4$, then H cannot contain any elements of order 4, because such elements would not have $\mathbb{F}_\ell$-rational eigenvalues. It is easy to check that a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ of exceptional type and without elements of order 4 has cyclic projective image, hence it acts reducibly on $\mathbb{F}_\ell^2$, contradiction.

Suppose now that $\ell \equiv 1 \pmod 4$. Arguing as in Corollary 3.12, we may assume that H contains all the scalars. By the assumption that we are in case (2) of Lemma 4.10 and the surjectivity of the symplectic multiplier (Lemma 4.5) we know that, for every $\mu \in \mathbb{F}_\ell^\times \setminus \mathbb{F}_\ell^{\times 2}$, there exists in G an element of the form $M := \begin{pmatrix} 0 & x \\ -\mu x^{-T} & 0 \end{pmatrix}$ that normalises $G^\square$. This implies that the matrix $v = \begin{pmatrix} 0 & x \\ -x^{-T} & 0 \end{pmatrix}$, which is in the subgroup $\mathrm{GL}_2(\mathbb{F}_\ell).2$ of $\mathrm{Sp}_4(\mathbb{F}_\ell)$, normalises H^{sat}. Notice that v is not in G (its multiplier is 1, but v is not block-diagonal). We have described the normaliser of a group like H^{sat} inside $\mathrm{GL}_2(\mathbb{F}_\ell).2$ in Lemma 3.15. With notation as in that lemma, this allows us to conclude that $x = gJ_2$ or $x = gJ_2\sigma^{-T}$. Multiplying M by $\begin{pmatrix} g & 0 \\ 0 & g^{-T} \end{pmatrix}^{-1} \in H$, we obtain an element of G of the form

$$u' = \begin{pmatrix} 0 & J_2 \\ -\mu J_2 & 0 \end{pmatrix} \quad \text{or} \quad u'' = \begin{pmatrix} 0 & J_2\sigma^{-T} \\ -\mu J_2\sigma & 0 \end{pmatrix},$$

where the second case can only arise if $\mathbb{P}H$ is isomorphic to A_4 and $\mathbb{P}A_4$ is not maximal in $\mathrm{PSL}_2(\mathbb{F}_\ell)$ (see Lemma 3.15 (3)). In particular, H^{sat} is normalised by an element $\sigma \in \mathrm{SL}_2(\mathbb{F}_\ell)$ with $\mathbb{P}\sigma$ representing a transposition in $\mathbb{P}(\langle H, \sigma \rangle) \cong S_4$. Note that $\sigma^2 = -\mathrm{Id}$.

If G contains an element of the form u' (which is automatic if $\mathbb{P}H \not\cong A_4$), then we get a contradiction: it is clear that u' does not have $\mathbb{F}_\ell$-rational eigenvalues, since the product of the off-diagonal blocks is $-\mu J_2^2 = \mu$, whose eigenvalues are not squares in $\mathbb{F}_\ell^\times$ (see Remark 3.8). If instead G contains an element of the form u'' (hence in particular $\mathbb{P}H \cong A_4$), then similarly $-\mu J_2\sigma^{-T}J_2\sigma = -\mu\frac{\sigma^2}{\det\sigma} = \mu$, contradiction. Hence H cannot be an exceptional subgroup.

So we may assume that H is a subgroup of $N(C_s)$ and $H = H^{\mathrm{sat}}$. In particular, the condition that every element of H has an $\mathbb{F}_\ell$-rational eigenvalue gives

$$H \leq \{A(i,j), B(i,j) \mid i + j \equiv 0 \pmod 2\},$$

where $A(i,j) = \begin{pmatrix} \delta^i & 0 \\ 0 & \delta^j \end{pmatrix}$ and $B(i,j) = \begin{pmatrix} 0 & \delta^i \\ \delta^j & 0 \end{pmatrix}$ and δ is a generator of $\mathbb{F}_\ell^\times$.

Let $M = \begin{pmatrix} 0 & x \\ -\mu x^{-T} & 0 \end{pmatrix}$ be as above. Since M^2 belongs to G^0, we have $xx^{-T} \in H$. If x is not diagonal or anti-diagonal, then we are in the second case of Lemma 3.6 and $\ell \equiv 1 \pmod 4$. In this case, up to multiplying M by an element of G_0^1, we can then assume that x is symmetric, which implies $M^2 = -\mu$. Therefore, $M^{\ell-1} = (-\mu)^{(\ell-1)/2} = -\mathrm{Id}$ since μ is not a square, which is absurd since M must have a rational eigenvalue. Otherwise, if we are in the first case of Lemma 3.6, up to multiplying M by an element of G_0^1 we can assume

$$M = \begin{pmatrix} 0 & A(i_1, j_1) \\ -\mu A(i_1, j_1)^{-T} & 0 \end{pmatrix}.$$

Observe that $M^2 = (-\mu)$ and $M^{\ell-1} = (-\mu)^{(\ell-1)/2}$. If -1 is a square mod ℓ, then $M^{\ell-1} = -\mathrm{Id}$ and M does not have a rational eigenvalue, contradiction. Therefore, -1 must not be a square, that is, $\ell \equiv 3 \pmod 4$, and we can take $\mu = -1$. One checks that $\begin{pmatrix} 0 & B(i,j) \\ B(i,j)^{-T} & 0 \end{pmatrix}$ has $\mathbb{F}_\ell$-rational eigenvalues iff $i + j$ is even, hence $G \leq \mathbb{F}_\ell^\times \cdot G'$, where

$$G' = \left\{ \begin{pmatrix} A(i,j) & 0 \\ 0 & A(i,j)^{-T} \end{pmatrix}, \begin{pmatrix} 0 & A(i,j) \\ A(i,j)^{-T} & 0 \end{pmatrix}, \begin{pmatrix} B(i,j) & 0 \\ 0 & B(i,j)^{-T} \end{pmatrix}, \begin{pmatrix} 0 & B(i,j) \\ B(i,j)^{-T} & 0 \end{pmatrix} \mid i + j \equiv 0 \pmod 2 \right\}. \tag{9}$$

If we show that G' is Hasse, then necessarily $G = \mathbb{F}_\ell^\times \cdot G'$ since G is maximal. The fact that G' acts irreducibly follows from the character formula, similarly to the case $\mathrm{GL}_2(\mathbb{F}_\ell).2$. The fact that every matrix has a rational eigenvalue follows from the fact that every matrix has order that divides $\ell - 1$. □

5 Hasse subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$

The goal of this section is to describe all maximal Hasse subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ having surjective multiplier.

Definition 5.1 Let G^1 be a Hasse subgroup of $\mathrm{Sp}_4(\mathbb{F}_\ell)$. If G^1 is not contained in one of the groups of the first three cases of Theorem 3.2, then we say that G^1 is exceptional.

Lemma 5.2 *Let G be a subgroup of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ containing the scalar multiples of* Id *and such that $\lambda(G) = \mathbb{F}_\ell^\times$. Let $G^1 = G \cap \mathrm{Sp}_4(\mathbb{F}_\ell)$. The index $[\mathbb{P}G : \mathbb{P}G^1]$ is at most 2.*

Proof The kernel of the projection $\pi : G \to \mathbb{P}G$ has order $|\mathbb{F}_\ell^\times| = \ell - 1$, while $G^1 \to \mathbb{P}G^1$ has kernel of order $k \leq 2$ (the only scalar matrices in $\mathrm{Sp}_4(\mathbb{F}_\ell)$ are $\pm\mathrm{Id}$). On the other hand, $|G|/|G^1| = |\lambda(G)| = \ell - 1$. It follows that $[\mathbb{P}G : \mathbb{P}G^1] = \frac{|\pi(G)|}{|\pi(G^1)|} = \frac{|G|/(\ell-1)}{|G^1|/k} = k \leq 2$. □

Lemma 5.3 *Let G be a maximal Hasse subgroup of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ with $\lambda(G) = \mathbb{F}_\ell^\times$ such that $G^1 = G \cap \mathrm{Sp}_4(\mathbb{F}_\ell)$ acts irreducibly. One of the following holds:*

- *G^1 is of class $\mathcal{C}_2$. In particular, as in Sect. 3.5 we can choose a basis of $\mathbb{F}_\ell^4$ with respect to which all elements in G are either block-diagonal or block-anti-diagonal.*
- *G^1 is exceptional.*

Proof As G^1 acts irreducibly, it is a Hasse subgroup of $\mathrm{Sp}_4(\mathbb{F}_\ell)$. The assumption $\lambda(G) = \mathbb{F}_\ell^\times$ implies that $\mathbb{P}G$ is not contained in $\mathbb{P}\,\mathrm{Sp}_4(\mathbb{F}_\ell)$. Thus there exists a maximal subgroup $\overline{M}$ of $\mathbb{P}\,\mathrm{GSp}_4(\mathbb{F}_\ell)$ with $\overline{M} \neq \mathbb{P}\,\mathrm{Sp}_4(\mathbb{F}_\ell)$ and $\overline{M}$ containing $\mathbb{P}G$. We let M be the inverse image of $\overline{M}$ in $\mathrm{GSp}_4(\mathbb{F}_\ell)$. The maximal subgroups $\overline{M}$ of $\mathbb{P}\,\mathrm{GSp}_4(\mathbb{F}_\ell)$ are classified in [4, Tables 8.12 and 8.13].

(1) Suppose first that M is of Aschbacher type $\mathcal{C}_i$ for some $i \neq 2$, or lies in class $\mathcal{S}$. Then by definition G^1 is contained in a maximal subgroup of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ of the same Aschbacher type, or is of class $\mathcal{S}$. By Theorem 3.2, Table 1, and Definition 5.1, G^1 is exceptional.

(2) Suppose instead that M is of Aschbacher type $\mathcal{C}_2$. By definition, M (hence also G) preserves a decomposition of $\mathbb{F}_\ell^4$ as the direct sum of two 2-dimensional subspaces: thus, in a suitable basis, all matrices in M are either block-diagonal or block-anti-diagonal. Note that by Theorem 3.2 we know that G^1 is contained in a maximal subgroup isomorphic to $\mathrm{SL}_2(\mathbb{F}_\ell) \wr S_2$ and the present choice of basis is compatible with that of Sect. 3.5.

□

Lemma 5.4 *Let G be a Hasse subgroup of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ such that $\lambda(G) = \mathbb{F}_\ell^\times$. If G^1 is not exceptional, then it acts reducibly.*

Proof Suppose by contradiction that G^1 acts irreducibly. Up to conjugacy, G^1 is contained in a maximal Hasse subgroup of one of the first three types listed in Theorem 3.2. In particular, we have $\ell \equiv 1 \pmod 4$. By Lemma 5.3, we can assume that every matrix in G is block-diagonal or block-anti-diagonal. We will find a contradiction by showing that G contains a matrix without rational eigenvalues. Note that we can assume that G contains all the scalars.

(1) Assume $G^1 \leq (Q_{2(\ell-1)} \times Q_{2(\ell-1)}).C_2$. As we did in Sect. 3.5, we write elements of $(Q_{2(\ell-1)} \times Q_{2(\ell-1)}).C_2$ as triples $(g, h, \pm 1)$. As above, G^1 contains a block-anti-diagonal matrix. Let $M \in G$ be an operator with $\lambda(M) = \delta$. Multiplying if necessary M by a block-anti-diagonal matrix in G^1, we can assume that M is block-diagonal. So, $M = \begin{pmatrix} M_1 & 0 \\ 0 & M_2 \end{pmatrix}$ with $\det(M_1) = \det(M_2) = \delta$. If M_1 or M_2 is neither diagonal nor anti-diagonal, then $G^1 \leq (Q_8 \times Q_8).C_2$ thanks to Lemma 3.7. In this case G^1 is exceptional, contradiction. So, we can assume that M_1 and M_2 are diagonal or anti-diagonal. By Lemma 4.11, we can assume that $M' = (s_1, s_2, 1)$ is in G^1. So, without loss of generality, we can assume that M_1 is diagonal. If M_2 is diagonal, then $M'M$ does not have a rational eigenvalue and G is not Hasse. If M_2 is anti-diagonal, then $M^2 = \delta(r^a, \pm 1, 1)$ with a

odd. Let $M_3 \in G^1 \setminus G_0^1$. As we showed in Sect. 3.5.4, $M_3 = (q_1, q_2, -1)$ with $q_1, q_2 \in Q_{2(\ell-1)}$. There are three possible cases:

- $M_3 = (r^c, r^d, -1)$. Under the assumption that M_3 has a rational eigenvalue, the order of M_3 divides $\ell-1$ and $c+d$ is even. So, $M^2M_3 = \delta(r^{a+c}, \pm r^d, -1)$ does not have a rational eigenvalue since $a + c + d$ is odd. Hence, G is not Hasse.
- $M_3 = (s_3, s_4, -1)$ with s_3 and s_4 symmetries. Then, $M_3' = M'M_3$ is of the form $(r^c, r^d, -1)$. So, one between M_3' and M^2M_3' does not have a rational eigenvalue, as we proved in the previous case.
- $M_3 = (q_1, q_2, -1)$ with q_1q_2 a symmetry. Multiplying by M, we see that G contains an element of the form $N = \begin{pmatrix} 0 & N_1 \\ N_2 & 0 \end{pmatrix}$ with $\det(N_1) = \det(N_2) = \delta$ and N_1 and N_2 both diagonal. Since N has a rational eigenvalue, we have $(N_1N_2)^{(\ell-1)/2} = 1$. In this case, M^2N does not have a rational eigenvalue, contradiction.

(2) Assume that $G^1 \leq (N_{\mathrm{GL}_2(\mathbb{F}_\ell)(C_s)}.2)$. By Remark 3.20, the group G^1 is contained in a maximal group of the previous case and so the lemma holds.

(3) Assume $G^1 \leq (C_{(\ell-1)/2}.E).2$ with E exceptional. We know that G_0^1 has projective image A_4, A_5, or S_4.
Assume G_0^1 has projective image A_5 or S_4. Proceeding as above, we obtain that G contains an element of the form $N = \begin{pmatrix} 0 & x \\ -\delta x^{-T} & 0 \end{pmatrix}$. Observe that x normalises G_0^1, so, as we pointed out in the proof of Lemma 3.15, x is in G_0^1 (when we see it as a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$). So, $M = \begin{pmatrix} x & 0 \\ 0 & x^{-T} \end{pmatrix}$ belongs to G. Letting $M' = M^{-1}N \in G$, by direct computation one has $M'^2 = -\delta$ and $(M')^{\ell-1} = -\mathrm{Id}$, so M' does not have a rational eigenvalue.
Assume that G_0^1 has projective image A_4. The normaliser of G_0^1 in $\mathrm{GL}_2(\mathbb{F}_\ell)$, that we denote with G', has projective image contained in S_4. Since G^1 acts irreducibly, it contains a matrix of the form $M_2 = \begin{pmatrix} 0 & y \\ -y^{-T} & 0 \end{pmatrix}$, and since $\lambda(G) = \mathbb{F}_\ell^\times$ the group G contains a matrix of the form $M_1 = \begin{pmatrix} 0 & x \\ -\delta x^{-T} & 0 \end{pmatrix}$ (notice that, up to multiplication by M_2, we can assume that M_1 is block-anti-diagonal). Since x normalises G_0^1, it belongs to G'. If $x \in G_0^1$, we conclude as in the case projective image A_5 or S_4. Otherwise, we may assume that $\mathbb{P}G' = S_4$ and that x is an element of $G' \setminus G_0^1$. Since $[G' : G_0^1] = 2$ all elements in $G' \setminus G_0^1$ appear as x for some choice of M_1 (simply multiply by a suitable element in G_0^1). Since $M_1^2 = -\delta \begin{pmatrix} xx^{-T} & 0 \\ 0 & x^{-T}x \end{pmatrix}$ we have $xx^{-T} \in G'$, hence x^{-T} is in G' for all $x \in G' \setminus G_0^1$. Every element z of G_0^1 is the product of two elements $x, x' \in G' \setminus G_0^1$, hence $z^{-T} = (xx')^{-T} = x^{-T}(x')^{-T} \in G'$. Thus $x \mapsto x^{-T}$ gives an automorphism of G'. Passing to the projective quotient, this induces an automorphism φ of order ≤ 2 of $\mathbb{P}G' \cong S_4$. All automorphisms of S_4 are inner, so φ is conjugation by some

element $w \in S_4$ of order ≤ 2. In particular, $\varphi(w) = w$, so if $x \in G' \setminus G_0^1$ lifts w we have $x^{-T} = \pm x$ and $xx^{-T} = \pm \mathrm{Id}$. Now for this x we have $M_1^2 = \pm\delta\,\mathrm{Id}$, hence $M_1^{\ell-1} = -\mathrm{Id}$ and M_1 does not have any rational eigenvalues, contradiction.

□

Theorem 5.5 *Let G be a maximal Hasse subgroup of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ with $\lambda(G) = \mathbb{F}_\ell^\times$. Let $G^1 = G \cap \mathrm{Sp}_4(\mathbb{F}_\ell)$. One of the following holds:*

- *G^1 acts reducibly, $\ell \equiv 1 \pmod 4$, and G^1 is a subgroup of $Q_{2(\ell-1)} \times Q_{2(\ell-1)}$.*
- *G^1 acts reducibly, $\ell \equiv 3 \pmod 4$, and $G = C_{(\ell-1)/2}.(H.2)$, where H is a subgroup of $N_{\mathrm{GL}_2(\mathbb{F}_\ell)}(C_s)$ of index 2.*
- *$|\mathbb{P}G| \leq 2^7 \cdot 3^2 \cdot 5^2$ and $|\mathbb{P}G|$ divides $2^9 \cdot 3^2 \cdot 5^2$.*

Proof By Lemma 5.4, G^1 acts reducibly or is exceptional. In the first case, we conclude by using Theorem 4.6. In the second case G^1 has order smaller than $2^7 \cdot 3^2 \cdot 5^2$ and dividing $2^9 \cdot 3^2 \cdot 5^2$ by Theorem 3.2 (see Table 1 and Remark 4.7). Note that $|G| = 2|G^\square| = 2(\ell-1)/2|G^1|$ and $|G| = (\ell-1)|\mathbb{P}G|$ since G contains $\mathbb{F}_\ell^\times \cdot \mathrm{Id}$. So, $|\mathbb{P}G| = |G^1| \leq 2^7 \cdot 3^2 \cdot 5^2$ and $|\mathbb{P}G|$ divides $2^9 \cdot 3^2 \cdot 5^2$. □

Remark 5.6 In "Appendix A" we will prove a slightly stronger version of this theorem, showing that, for *any* Hasse subgroup G of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ with $\lambda(G) = \mathbb{F}_\ell^\times$, the subgroup G^1 acts reducibly.

Remark 5.7 With more work in the style of Sect. 3, one could probably improve the bound on the order of $|\mathbb{P}G|$ in the third case of the theorem, and also classify the groups of the form $\mathbb{P}G$ that arise from the Hasse subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$. We have decided not to pursue this, since the qualitative form of the result given above will be enough for our applications.

Remark 5.8 The assumption $\lambda(G) = \mathbb{F}_\ell^\times$ is less restrictive than it may seem: indeed, by Corollary 4.3 we know that for every maximal Hasse subgroup G of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ the multiplier group $\lambda(G)$ contains $\lambda(\mathbb{F}_\ell^\times\,\mathrm{Id}) = \mathbb{F}_\ell^{\times 2}$. The assumption $\lambda(G) = \mathbb{F}_\ell^\times$ is then equivalent to the requirement that G contains an element whose multiplier is not a square. If this is not the case, then G is simply the saturation of G^1, which is a Hasse subgroup of $\mathrm{Sp}_4(\mathbb{F}_\ell)$. These cases are therefore already covered by Theorem 3.2.

6 Strong counterexamples

6.1 Statement of the main result

Theorem 6.1 *Let A be an abelian surface defined over a number field K. There exists a constant C_1, depending only on K, such that the following hold for all primes $\ell > C_1$.*

- *If $\mathrm{End}_{\overline{K}}(A)$ is an order $\mathcal{O}$ in a real quadratic field, then there exists an extension K'/K, of degree at most 2, such that $\mathrm{End}_{\overline{K}}(A) = \mathrm{End}_{K'}(A)$. If ℓ is unramified in K', then (A, ℓ) is not a strong counterexample. In particular, if all the endomorphisms of A are defined over K, then (A, ℓ) is not a strong counterexample.*

- *If $A_{\overline{K}}$ is isogenous to the square of an elliptic curve E without CM, then there exists an extension K'/K of degree at most 3 such that $A_{K'}$ is either isogenous to the product of two elliptic curves or satisfies that $\mathrm{End}_{K'}(A) \otimes \mathbb{Q}$ is a quadratic field. If $[K' : K] = 1$ or 3, then (A, ℓ) is not a strong counterexample. If $[K' : K] = 2$ and ℓ is unramified in K', then (A, ℓ) is not a strong counterexample.*
- *If $\mathrm{End}_{\overline{K}}(A)$ is an order in a (nonsplit) quaternion algebra and $\mathrm{End}_K(A)$ is an order in a quaternion algebra or an order in a quadratic field, then (A, ℓ) is not a strong counterexample. If $\mathrm{End}_K(A) = \mathbb{Z}$, then there is a field extension K'/K of degree 2 such that $\mathrm{End}_{K'}(A)$ is an order in a quadratic field. If ℓ is unramified in K', then (A, ℓ) is not a strong counterexample.*
- *If $\mathrm{End}_{\overline{K}}(A)$ is an order in a CM field, then (A, ℓ) is not a strong counterexample.*

Strong counterexamples (A, ℓ) for which A is geometrically isogenous to the square of an elliptic curve with CM are not bounded in the same sense as in the above theorem. Indeed, as we will show in Proposition 6.28, we can find infinitely many ℓ such that there exists an abelian surface defined over $\mathbb{Q}$ and geometrically isogenous to the square of an elliptic curve with CM such that (A, ℓ) is a strong counterexample.

We will also obtain the following consequence of Theorem 6.1:

Corollary 6.2 *Let A be an abelian surface over a number field K. Assume that $\mathrm{End}_K(A) \neq \mathbb{Z}$. There exists a constant C_1, depending only on K, such that (A, ℓ) is not a strong counterexample for $\ell > C_1$.*

We will make the following assumptions on ℓ:

- ℓ is unramified in K.
- $\ell > 2^9 \cdot 3^3 \cdot 5^2 \cdot [K : \mathbb{Q}] + 1$. By Theorem 6.6, this implies $|\mathbb{P}G_\ell| > 2^7 \cdot 3^2 \cdot 5^2$.

These assumptions clearly hold if

$$\ell > C_1 := \max\{2^9 \cdot 3^3 \cdot 5^2 \cdot [K : \mathbb{Q}] + 1, \Delta_K\},$$

where Δ_K is the discriminant of K. Recall that G_ℓ is defined in Sect. 1.1 as the image of the Galois representation $\rho_\ell : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(A[\ell])$.

6.2 Lower bounds on the image of Galois

We shall need the following result, proven in [30]:

Theorem 6.3 *Let A be an abelian surface over a number field K, and let v be a place of K. Let L be a minimal extension of K over which A acquires semistable reduction at a place w above v. Suppose that the residue characteristic of v is at least 7: then the ramification index $e(w|v)$ is bounded by 12.*

From now on, we will always assume that $\ell \geq 7$, so that the previous theorem applies.

Theorem 6.4 ([22, Corollaire 3.4.4]) *Let A be an abelian variety over a number field K and let v be a finite place of K of characteristic ℓ at which A has semistable reduction. Let $I_v = I_v(\overline{K}/K)$ be the inertia group at v and I_v^t be its tame quotient.*

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

- *V has a structure of an $\mathbb{F}_{\ell^n}$-vector space;*
- *the action of I_v^t on V is given by a character $\psi : I_v^t \to \mathbb{F}_{\ell^n}^\times$;*
- *$\psi = \varphi_1^{e_1} \ldots \varphi_n^{e_n}$, where $\varphi_1, \ldots, \varphi_n$ are the fundamental characters of I_v^t of level n;*
- *for every $i = 1, \ldots, n$ the inequality $0 \leq e_i \leq e$ holds.*

Remark 6.5 Raynaud's theorem is usually stated for places of *good* reduction. However, as shown in [18, Lemma 4.9], the extension to the semi-stable case follows easily upon applying results of Grothendieck [9].

Theorem 6.6 *Let A/K be an abelian surface over a number field K. Given a finite group G, we write $\exp(G) = \operatorname{lcm}\{\operatorname{ord}(g) : g \in G\}$.*

(1) Let $\ell > 2[K : \mathbb{Q}]$ be a prime. If A has semi-stable reduction at a place v of K of characteristic ℓ, then $\exp(\mathbb{P}G_\ell) \geq \dfrac{\ell - 1}{[K : \mathbb{Q}]}$.

(2) Without the assumption of semi-stable reduction, we have

$$\exp(\mathbb{P}G_\ell) \geq \frac{1}{12} \frac{\ell - 1}{[K : \mathbb{Q}]}$$

for every prime $\ell > 24[K : \mathbb{Q}]$.

Proof We first show that the first statement implies the second. Let L/K be a minimal extension of K over which A acquires semi-stable reduction at some place of characteristic ℓ. Since $\ell > 5$, by Theorem 6.3 we have $[L : K] \leq 12$ (hence $[L : \mathbb{Q}] \leq 12[K : \mathbb{Q}]$), and since clearly $\exp(\mathbb{P}\rho_\ell(G_K)) \geq \exp(\mathbb{P}\rho_\ell(G_L))$ the claim follows from part (1) applied to A/L.

We now prove part 1. Consider the action of an inertia group I_v at v on $A[\ell]$. If the wild inertia subgroup (which is pro-ℓ) acts non-trivially, then G_ℓ contains an element of order ℓ, and since $\ker(G_\ell \to \mathbb{P}G_\ell)$ has order prime to ℓ we see that $\mathbb{P}G_\ell$ contains an element of order ℓ, so that $\exp(\mathbb{P}G_\ell) \geq \ell$ and we are done. We may therefore assume that the wild inertia subgroup acts trivially, hence that the action of I_v on $A[\ell]$ factors through I_v^t, the tame inertia quotient. Recall that this is a pro-cyclic group, hence all its finite homomorphic images are cyclic.

The representation ρ_ℓ induces, by restriction to I_v and then passage to the quotient I_v^t, a group homomorphism (which we still denote by ρ_ℓ) from I_v^t to G_ℓ. By composing with the projection $G_\ell \to \mathbb{P}G_\ell$, we obtain a map $\phi : I_v^t \to \mathbb{P}G_\ell$, and it suffices to show that the image of this map has order at least $\frac{\ell-1}{[K:\mathbb{Q}]}$. Indeed, the image of this map is cyclic, hence $\exp(\mathbb{P}G_\ell) \geq \exp(\phi(I_v^t)) = |\phi(I_v^t)|$. Since $|\phi(I_v^t)| = [I_v^t : \ker\phi]$, we now want to study the kernel of ϕ. Furthermore, since $[K : \mathbb{Q}] \geq e(v|\ell)$, it suffices to show the theorem with $[K : \mathbb{Q}]$ replaced by the ramification index $e := e(v|\ell)$.

If $\sigma \in I_v^t$ lies in the kernel of ϕ, then $\rho_\ell(\sigma)$ is a scalar matrix. Notice that $A[\ell]$ is a semisimple I_v^t-module, because $\rho_\ell(I_v)$ has no elements of order ℓ. Write $A[\ell] \cong$

$\bigoplus W_i$, where W_i is irreducible and of dimension l_i. By Theorem 6.4, the eigenvalues of $\rho_\ell(\sigma)|_{W_i}$ are given by the conjugates of $\psi_i = \varphi_{l_i}^{a_i}$, where φ_{l_i} is a fundamental character of level l_i and if we write $a_i = a_{i,0} + a_{i,1}\ell + \cdots + a_{i,l_i-1}\ell^{l_i-1}$ we have $0 \le a_{i,j} \le e$. Moreover, if $i > 1$ then we cannot have $a_{i,0} = \ldots = a_{i,l_i-1}$ (otherwise, $\psi_i = \chi_\ell^{a_{i,0}}$ would take values in $\mathbb{F}_\ell^\times$ and W_i would not be irreducible, see also [15, Proposition 3.15]). We distinguish several cases:

(1) **At least one l_i is 2 or more.** Without loss of generality, assume that $l_1 \ge 2$, and let $\varphi^b = \varphi_{l_1}^{a_1}$ be a character giving one of the eigenvalues of the action of inertia. Write for simplicity $\varphi := \varphi_l$ and $b := a_1 = b_0 + b_1\ell + \cdots + b_{l-1}\ell^{l-1}$, with every b_i in $\mathbb{N} \cap [0, e]$ and $l = l_1$.
Notice that $\varphi(\sigma)^b$ and $\varphi(\sigma)^{\ell b}$ are both eigenvalues of $\rho_\ell(\sigma)$, so if $\rho_\ell(\sigma)$ is a scalar we must have $\varphi(\sigma)^{b(\ell-1)} = 1$. Since I_v^t is a pro-cyclic group, the subgroup $H = \{\sigma \in I_v^t : \varphi(\sigma)^b = \varphi(\sigma)^{b\ell}\}$ is also pro-cyclic, and its index in I_v^t is

$$\frac{\ell^l - 1}{\left(b(\ell-1), \ell^l - 1\right)} = \frac{\ell^l - 1}{(\ell-1)\left(b_0 + b_1\ell + \cdots + b_{l-1}\ell^{l-1}, 1 + \ell + \cdots + \ell^{l-1}\right)}. \tag{10}$$

Now $\left(b_0 + b_1\ell + \cdots + b_{l-1}\ell^{l-1}, 1 + \ell + \cdots + \ell^{l-1}\right)$ is equal to

$$\left((b_0 - b_{l-1}) + (b_1 - b_{l-1})\ell + \cdots + (b_{l-2} - b_{l-1})\ell^{l-2}, 1 + \ell + \cdots + \ell^{l-1}\right),$$

where $(b_0 - b_{l-1}) + (b_1 - b_{l-1})\ell + \cdots + (b_{l-2} - b_{l-1})\ell^{l-2}$ is non-zero since we already remarked that the b_i cannot all be equal. It follows that the denominator of (10) is at most $e(1 + \ell + \cdots + \ell^{l-2}) = e\frac{\ell^{l-1}-1}{\ell-1}$, and therefore $|(I_v^t/H)| \ge \frac{1}{e}\frac{(\ell^l-1)(\ell-1)}{\ell^{l-1}-1} \ge \frac{1}{e}\ell(\ell-1)$. It follows in particular that $\mathbb{P}\rho_\ell(I_v)$ has order at least $\frac{\ell(\ell-1)}{e} > \frac{\ell-1}{e}$.

(2) **All l_i are equal to 1, at least one character ψ_i is trivial, and at least one character ψ_j is non-trivial.** Write $\psi_j = \chi_\ell^b$ with $b > 0$. For every $\sigma \in I_v^t$ the endomorphism $\rho_\ell(\sigma)$ admits 1 as an eigenvalue, and therefore $\ker\phi$ is contained in $\{\sigma \in I_v^t : \chi_\ell^b(\sigma) = 1\}$, which has index $(\ell - 1, b)$ in I. Since $b \le e$, the claim follows.

(3) **All l_i are equal to 1, and there are two indices i, j such that $a_i \ne a_j$.** Write $b_1 = a_i$ and $b_2 = a_j$. We have $\ker\phi \subseteq \{\sigma \in I_v : \chi_\ell(\sigma)^{b_1-b_2} = 1\}$, which again has index at least $\frac{\ell-1}{(\ell-1,b_1-b_2)} \ge \frac{\ell-1}{e}$ in I_v^t.

(4) **All l_i are equal to 1 and all the a_i are equal to each other.** We show that this case cannot arise for $\ell > 2[K : \mathbb{Q}]$. All the characters $\varphi_{l_i}^{a_i}$ are equal to χ_ℓ^b for some b with $0 \le b \le e$. Then for every $\sigma \in I_v^t$ we have $\chi_\ell(\sigma) = \lambda(\rho_\ell(\sigma)) = \chi_\ell^{2b}(\sigma)$, whence $\ell - 1 \mid 2b - 1 \le 2e - 1 \le 2[K : \mathbb{Q}] - 1$, contradicting our assumption $\ell > 2[K : \mathbb{Q}]$.

□

Corollary 6.7 *Let $\ell \geq C_1$ be a prime. Using the notation of Theorem 6.4, let $I = \rho_\ell(I_v(\overline{K}/K))$. Suppose that all elements of I have four $\mathbb{F}_\ell$-rational eigenvalues. There exists $e \leq 12$ such that, for all $\sigma \in I_v(\overline{K}/K)$, the automorphism $\rho_\ell(\sigma^e)$ has eigenvalues $1, 1, \chi_\ell(\sigma^e)$, and $\chi_\ell(\sigma^e)$.*

Proof In the notation of Theorem 6.3, let e be the ramification index of v in L/K. Given $\sigma \in I_v(\overline{K}/K)$ we have $\sigma^e \in I_w := I_w(\overline{L}/L)$, hence, by Theorem 6.4, $\rho_\ell(\sigma^e)$ acts with eigenvalues that are (products of) fundamental characters of level at most 4. Since $\rho_\ell(\sigma^e)$ has four rational eigenvalues for every σ, the fundamental characters are all of level 1, so the eigenvalues are of the form $\chi_\ell^{a_1}(\sigma^e), \ldots, \chi_\ell^{a_4}(\sigma)$ for some exponents $0 \leq a_i \leq e$ independent of σ. Choosing σ so that $\chi_\ell(\sigma)$ generates $\mathbb{F}_\ell^\times$ we obtain $\det \rho_\ell(\sigma^e) = \chi_\ell(\sigma)^{2e} = \chi_\ell(\sigma)^{e\sum a_i}$, which (since $\ell \geq C_1$) implies $\sum_{i=1}^4 a_i = 2$. Finally, up to renumbering, the eigenvalues $\lambda_1, \ldots, \lambda_4$ of a matrix in $\mathrm{GSp}_4(\mathbb{F}_\ell)$ satisfy $\lambda_1\lambda_4 = \lambda_2\lambda_3$, which then forces $a_1 = a_2 = 0, a_3 = a_4 = 1$ (up to reordering). □

6.3 Preliminary lemmas

For simplicity of notation, from now on we write ρ instead of ρ_ℓ. We choose a place v of K of characteristic ℓ and let $I_v < \mathrm{Gal}\left(\overline{K}/K\right)$ be a corresponding inertia group.

Lemma 6.8 *Let A be an abelian surface defined over a number field K. Let $\ell > C_1$ be a prime and let $G = \rho(\mathrm{Gal}(\overline{K}/K))$. Assume that (A, ℓ) is a strong counterexample, so that G is Hasse. The order of $\mathbb{P}G$ is strictly greater than $2^7 \cdot 3^2 \cdot 5^2$. Up to conjugacy, G contains only block-diagonal and block-anti-diagonal matrices, with blocks that are diagonal or anti-diagonal. The matrices whose multiplier is a square are block-diagonal, and the matrices whose multiplier is not a square are block-anti-diagonal. Moreover,*

- *If $\ell \equiv 1 \pmod 4$, then G is contained in a group as in Lemma 4.12, case (1).*
- *If $\ell \equiv 3 \pmod 4$, then G is contained in the group described in Lemma 4.13.*

Every element of G has four rational eigenvalues and $\lambda(G) = \mathbb{F}_\ell^\times$. Finally, G contains a matrix M of the form $\begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix}$ such that the following all hold: x and y are either both diagonal or both anti-diagonal, $\lambda(M)$ generates $\mathbb{F}_\ell^\times$, and M^4 is not a scalar.

Proof Since ℓ is unramified in K by the assumption $\ell > C_1$, we have that the multiplier of G is $\chi_\ell(\mathrm{Gal}\left(\overline{K}/K\right)) = \mathbb{F}_\ell^\times$. As (A, ℓ) is a strong counterexample, it follows that up to conjugacy G is contained in one of the groups described in Theorem 5.5. By Theorem 6.6, the order of $\mathbb{P}G$ is greater than $2^7 \cdot 3^2 \cdot 5^2$ since $\ell > C_1$. So, if $\ell \equiv 3 \pmod 4$, then G is necessarily contained in the group described in Lemma 4.13. If $\ell \equiv 1 \pmod 4$, then G is contained in a group as in Lemma 4.12, case (1). From these explicit descriptions the first part of the lemma follows easily.

Let $M = \rho(\sigma)$ be an element in $\rho(I_v)$ such that $\lambda(M)$ generates $\mathbb{F}_\ell^\times$. Such an element exists because ℓ is unramified in K (since $\ell > C_1$). By Corollary 6.7, M^{4e} is not a scalar, hence M^4 is not a scalar. Since the multiplier of M is not a square, M is a block-anti-diagonal matrix of the form $\begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix}$. By what we already proved,

x and y are diagonal or anti-diagonal. We just need to show that it is impossible for x to be diagonal and y anti-diagonal (or vice-versa). If this were the case, by direct computation M^4 would be a scalar, contradiction. □

Lemma 6.9 *Let G be as in Lemma 6.8 and let M be as in the conclusion of that lemma. The matrix M has four different eigenvalues.*

Proof The characteristic polynomial of M is $x^4 + cx^2 + \det(x)\det(y)$ for some $c \in \mathbb{F}_\ell$. By Lemma 4.10, $\det(x)\det(y) = \lambda^2$ with $\lambda \notin (\mathbb{F}_\ell^\times)^2$. Letting x_0 be a rational eigenvalue of M, the eigenvalues are $\pm x_0, \pm\lambda/x_0$. Note that $x_0 \neq -x_0$ and $x_0 \neq \lambda/x_0$ since λ is not a square. If $x_0 \neq -\lambda/x_0$, then M has four different eigenvalues. If $x_0 = -\lambda/x_0$, then $x_0 = \pm\sqrt{-\lambda}$ and the eigenvalues are $\pm\sqrt{-\lambda}$ with multiplicity 2. Hence $M^2 = -\lambda$, contradicting the fact that M^2 is not a scalar. □

Given a ring R, we will denote by $\mathrm{Nilrad}(R)$ the ideal of nilpotent elements.

Lemma 6.10 *Let $R = \mathrm{End}_{\overline{K}}(A)$ be an order in a field. If ℓ is ramified in $R \otimes \mathbb{Q}$ or it divides the conductor of R, then $\mathrm{Nilrad}(R \otimes \mathbb{F}_\ell)$ is non-trivial and $\mathrm{Gal}(\overline{K}/K)$-invariant.*

Proof The assumptions imply that $R \otimes \mathbb{F}_\ell$ is not a product of fields. The ring $R \otimes \mathbb{F}_\ell$ is finite, hence Artinian. Every Artinian ring can be written as a product of Artinian local rings. Hence, $R \otimes \mathbb{F}_\ell$ is isomorphic to $\prod A_i$, where at least one of the A_i is not a field, hence contains a non-trivial non-invertible element. Since $\mathrm{Nilrad}(R \otimes \mathbb{F}_\ell) = \prod_i \mathrm{Nilrad}(A_i)$, the claim follows from the well-known fact that a finite local Artinian ring A with a non-zero non-invertible element has non-trivial nilradical. Therefore, $\mathrm{Nilrad}(R \otimes \mathbb{F}_\ell)$ is $\mathrm{Gal}(\overline{K}/K)$-invariant because the condition $x^n = 0$ clearly is. □

Lemma 6.11 *Any group G as in Lemma 6.8 contains at most $4(\ell-1)^2$ diagonal matrices having at most 3 distinct eigenvalues.*

Proof Assume $\ell \equiv 3 \pmod 4$, so that G is contained in the group described in Lemma 4.13. Then, the eigenvalues of a diagonal matrix are $\mu\delta^{\pm i}, \mu\delta^{\pm j}$ where $\mu \in \mathbb{F}_\ell^\times$, the number $i + j$ is even, and δ is a generator of $\mathbb{F}_\ell^\times$. If a 4×4 matrix has at most three different eigenvalues, then two of them are equal.

If $\delta^i = \delta^j$, then we have $\ell - 1$ choices for i, one choice for j and $(\ell-1)/2$ choices for μ (up to sign). So, there are $(\ell-1)^2/2$ matrices such that $\delta^i = \delta^j$. The same holds for every other pair of eigenvalues. Since there are 6 pairs to consider, there are at most $3(\ell-1)^2$ diagonal matrices with at most three different eigenvalues.

If instead $\ell \equiv 1 \pmod 4$, then G is in particular contained in a group as in Lemma 4.12, case (1) . Then, the eigenvalues of a diagonal matrix are $\mu\delta^{\pm a}, \mu\delta^{\pm b}$. Reasoning as above we see that there are at most $(\ell-1)^2/2$ matrices such that $\delta^{\pm a} = \delta^{\pm b}$. Moreover, we have at most $(\ell-1)^2$ matrices such that $\delta^a = \delta^{-a}$, and at most $(\ell-1)^2$ matrices such that $\delta^b = \delta^{-b}$. In conclusion, there are at most $4(\ell-1)^2$ matrices with at most three different eigenvalues. □

Lemma 6.12 *Let $\rho : G \to \mathrm{GL}(V)$ be a 4-dimensional representation of a group G. Assume that V splits as $V = V_1 \oplus V_2$, where V_1 and V_2 are two-dimensional G-invariant subspaces. Suppose that there is $\lambda \neq 0, 1$ and an element g of G such that*

$\rho(g)(v_1) = v_1$ for all $v_1 \in V_1$ and $\rho(g)(v_2) = \lambda v_2$ for all $v_2 \in V_2$. Then at least one of the following holds:

(1) V_1 and V_2 are the only G-invariant subspaces of dimension 2;
(2) there exists a G-invariant subspace of dimension 1.

Proof The assumptions imply that g commutes with every $h \in G$: the restrictions of g, h to V_1, V_2 commute since $g|_{V_i}$ is a scalar. Notice that V_1, V_2 are the eigenspaces of g. Since g is in the center, every element of G preserves the eigenspaces of g, hence every G-invariant subspace W splits as $(W \cap V_1) \oplus (W \cap V_2)$, which easily implies the statement. □

Lemma 6.13 *Let G be a group as in Lemma 6.8. The subgroup D of diagonal matrices in G is normal. If $\ell \equiv 3 \pmod 4$, then $G/D \cong (\mathbb{Z}/2\mathbb{Z})^2$. If $\ell \equiv 1 \pmod 4$, then $G/D \cong D_4$ or $G/D \cong (\mathbb{Z}/2\mathbb{Z})^2$.*

Proof First note that if M is a 2×2 diagonal matrix and N is a 2×2 diagonal or anti-diagonal matrix, then NMN^{-1} is diagonal. From this it follows easily that D is normal in G. Assume $\ell \equiv 3 \pmod 4$. In this case, D has index 4, with cosets represented by

$$\begin{pmatrix} A & 0 \\ 0 & A^{-T} \end{pmatrix}, \begin{pmatrix} 0 & A \\ A^{-T} & 0 \end{pmatrix}, \begin{pmatrix} B & 0 \\ 0 & B^{-T} \end{pmatrix}, \begin{pmatrix} 0 & B \\ B^{-T} & 0 \end{pmatrix}$$

with A (resp. B) diagonal (resp. anti-diagonal). Note that every one of these cosets must appear since G acts irreducibly. Therefore, G/D has order 4 and every element has order that divides 2, so $G/D \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Assume now $\ell \equiv 1 \pmod 4$. As we showed at the end of the proof of Lemma 4.12, there are eight possible cosets, namely

$$\begin{pmatrix} r_1 & 0 \\ 0 & r_2 \end{pmatrix}, \begin{pmatrix} 0 & xr_1 \\ yr_2 & 0 \end{pmatrix}, \begin{pmatrix} s_1 & 0 \\ 0 & s_2 \end{pmatrix}, \begin{pmatrix} 0 & xs_1 \\ ys_2 & 0 \end{pmatrix}$$
$$\begin{pmatrix} r_1 & 0 \\ 0 & s_2 \end{pmatrix}, \begin{pmatrix} 0 & xr_1 \\ ys_2 & 0 \end{pmatrix}, \begin{pmatrix} s_1 & 0 \\ 0 & r_2 \end{pmatrix}, \begin{pmatrix} 0 & xs_1 \\ yr_2 & 0 \end{pmatrix}$$

with r_i diagonal, s_i anti-diagonal, and x and y diagonal. As we observed in Lemmas 4.12 and 6.8, G must contain elements from each of the first 4 cosets since it acts irreducibly. From this it follows easily that either G/D has order 4, in which case $G/D \cong (\mathbb{Z}/2\mathbb{Z})^2$, or it has order 8, and is then isomorphic to D_4. □

Lemma 6.14 *Let G be a group as in Lemma 6.8 and let G' be a subgroup of index 2 of G such that G' acts reducibly on $A[\ell]$. Let $D < G$ be the subgroup of diagonal matrices of G and $D' \leq G'$ be the subgroup of diagonal matrices of G'. Assume that G' contains a block-anti-diagonal matrix whose square is not a scalar. Then, $[G' : D'] = 2$.*

Proof We assume that $[G' : D'] \neq 2$ and aim for a contradiction. By Lemma 6.13 we have $[G : D] = 4$ or 8, so $[G' : D'] = 4$ or 8. In both cases one can easily check

that G' contains a matrix of the form $M = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$ with x and y both anti-diagonal. Let $V_1 = \langle e_1, e_2 \rangle$ and $V_2 = \langle e_3, e_4 \rangle$. Let $H' < G'$ be the subgroup of block-diagonal matrices and consider the action of H' on V_1 and on V_2. There are two possibilities: H' acts reducibly on both V_1 and V_2, or it does not.

- Assume that H' acts reducibly on V_1 and V_2. We have $V_1 = V_{1,1} \oplus V_{1,2}$, with each of the two 1-dimensional subspaces invariant under the action of H'. Denote by H'_1 the projection of H' to $\mathrm{GL}(V_1) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$. All elements in H'_1 are simultaneously diagonalisable by the assumption that H' acts reducibly on V_1, hence in particular H'_1 is commutative. Since anti-diagonal matrices commute if and only if they differ by a scalar, every diagonal matrix in H'_1 is a scalar. The same holds for V_2, so the diagonal matrices in H' (hence also in G') are block-scalar.
  Suppose first that $\ell \equiv 1 \pmod 4$. All the diagonal matrices in G are of the form

$$M = \mu \begin{pmatrix} \delta^a & 0 & 0 & 0 \\ 0 & \delta^{-a} & 0 & 0 \\ 0 & 0 & \delta^b & 0 \\ 0 & 0 & 0 & \delta^{-b} \end{pmatrix}$$

  where δ is a generator of $\mathbb{F}_\ell^\times$. Since $M \in G'$ must be block-scalar, then necessarily a and b are equal to 0 or $(\ell - 1)/2$. Hence $|\mathbb{P}D'| \leq 2$ and $|\mathbb{P}D| \leq 4$ since $[D : D'] \leq 2$. So, $|\mathbb{P}G| \leq 32$ since $[G : D] \leq 8$ (see Lemma 6.13), contradiction.
  Suppose instead that $\ell \equiv 3 \pmod 4$. Let $M \in G'$ be a block-anti-diagonal matrix. Using Eq. (9) one can easily check that, if M^2 is block-scalar, then it is a scalar. So, the square of every block-anti-diagonal matrix in G' is a scalar. This contradicts the hypothesis.
- Without loss of generality, assume that H' acts irreducibly on V_1. Let χ be the character of the representation of G on $A[\ell]$. By Lemma 6.8, all the eigenvalues of every element of G are $\mathbb{F}_\ell$-rational, hence by Proposition 3.9 we have $\langle \chi, \chi \rangle_G = 1$. Since $[G : G'] = 2$ we have $\langle \chi, \chi \rangle_{G'} \leq 2$ and since G' acts reducibly we have $\langle \chi, \chi \rangle_{G'} = 2$. Observe that $\chi(g') = 0$ for all $g' \in G' \setminus H'$ and $2|H'| = |G'|$. Therefore, $\langle \chi, \chi \rangle_{H'} = 4$. Let χ_1, χ_2 be the characters of the action of H' on V_1, V_2, so that $\chi|_{H'} = \chi_1 + \chi_2$. The assumption that H' acts irreducibly on V_1 gives $\langle \chi_1, \chi_1 \rangle_{H'} = 1$. Combined with $\langle \chi_1 + \chi_2, \chi_1 + \chi_2 \rangle_{H'} = 4$, this gives $\langle \chi_1, \chi_2 \rangle_{H'} > 0$, which implies $\chi_1 = \chi_2$. In particular, H' acts irreducibly also on V_2.
  Assume first $\ell \equiv 3 \pmod 4$. Every diagonal matrix of H' is of the form

$$M(i, j) := \mu \begin{pmatrix} A(i, j) & 0 \\ 0 & A(i, j)^{-T} \end{pmatrix}.$$

  So, $\chi_1(M) = \delta^i + \delta^j$ and $\chi_2(M) = \delta^{-i} + \delta^{-j}$. We have $\chi_1(M) = \chi_2(M)$ and $\chi_1(M^2) = \chi_2(M^2)$ and this happens only if $2(i + j) \equiv 0 \pmod{\ell - 1}$. Observe that $i + j \not\equiv (\ell - 1)/2 \pmod{\ell - 1}$ since $(\ell - 1)/2$ is odd and $i + j$ is even by Eq. (9). Hence, $i + j \equiv 0 \pmod{\ell - 1}$. So, the matrices in H' are of the form $M(i, -i)$.

Let H be the subgroup of block-diagonal matrices of G, so that H' has index ≤ 2 in H. If all the diagonal matrices in H are of the form $M(i, -i)$, then using the character formula as above shows that G acts reducibly on $A[\ell]$, contradiction. So, H contains a diagonal matrix of the form $M(i_0, j_0)$ with $i_0 + j_0 \not\equiv 0 \pmod{\ell - 1}$. Since H' has index ≤ 2 in H, we have $M^2(i_0, j_0) \in H'$ and then $2i_0 + 2j_0 \equiv 0 \pmod{\ell - 1}$. This happens only if $i_0 + j_0 \equiv (\ell - 1)/2 \pmod{\ell - 1}$, which is absurd as already noticed.

Assume now $\ell \equiv 1 \pmod 4$. Note that, since $\chi_1 = \chi_2$, the group H' contains no matrices of the form $\begin{pmatrix} r^a & \\ & s_1 \end{pmatrix}$ where s_1 is a symmetry in $Q_{2(\ell-1)}$, unless H' is a sub-direct product of $Q_8 \times Q_8$. In this case, $|G| = 4|H'| \leq 2^8$, contradicting Lemma 6.8. Therefore, the block-anti-diagonal matrices in G' are of the form $M = \begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix}$ with x and y both diagonal or both anti-diagonal. Hence, $[G' : D'] = 4$. We will denote by $\mathrm{diag}(a, b, c, d)$ the diagonal matrix with diagonal entries a, b, c, d. Let $M_1 = \begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix}$ be a matrix in G' with x and y diagonal, and $\det x = \det y \notin \mathbb{F}_\ell^2$. Such a matrix exists since $[G' : D'] = 4$. If M_1^2 is a scalar, say $M_1^2 = \lambda$, then $\lambda^2 = \det x \det y$. But $\det x \det y = (\det x)^2 \notin \mathbb{F}_\ell^{\times 4}$, while λ^2 is a fourth power since λ is an eigenvalue of xy, which is a square by Remark 3.8. So, M_1^2 cannot be a scalar. Hence, $M_1^2 = \mathrm{diag}(a, b, a, b)$ with $a \neq b$. Similarly, G contains a matrix $M_2 = \begin{pmatrix} 0 & x_2 \\ y_2 & 0 \end{pmatrix}$ with x_2 and y_2 anti-diagonal and $M_2^2 = \mathrm{diag}(a, b, b, a)$ with $a \neq b$. Note that $M^2 \in G'$ for all $M \in G$ since G' is normal of index 2. Let $v = (x', y', z', w')^T$ be a non-zero vector in a G'-invariant subspace W of dimension ≤ 2 (in fact, $\dim W = 2$ by Clifford's theorem). The subspace spanned by v, $\mathrm{diag}(a, b, a, b)v$ and $\mathrm{diag}(a, b, b, a)v$ contains at least one of the basis vectors e_i. We assume $e_1 \in W$, the other cases being identical. Multiplying e_1 by a block-diagonal but non-diagonal matrix in G' we have that $e_2 \in W$. So, $W = \langle e_1, e_2 \rangle$. Multiplying e_1 by an anti-block-diagonal we have that $e_3 \in W$ or $e_4 \in W$, contradiction.

□

Lemma 6.15 *Let K be a number field and let (A, ℓ) be a strong counterexample with $\ell > C_1$. Assume that there exists a degree-2 extension K' of K such that $\rho(\mathrm{Gal}(\overline{K}/K'))$ acts reducibly. Assume that ℓ is unramified in K'. The following hold:*

- *There exist precisely two $\rho(\mathrm{Gal}(\overline{K}/K'))$-invariant subspaces V_1 and V_2 of dimension 2.*
- *Let $v_{K'}$ be a place of K' and let L be a minimal extension of K' over which A acquires semi-stable reduction at a place above $v_{K'}$. Let v_L be a place of L above $v_{K'}$ and $e = e(v_L \mid v_{K'}) \leq 12$ be its ramification index. Choose σ in an inertia group corresponding to $v_{K'}$ with the property that $\chi_\ell(\sigma)$ generates $\mathbb{F}_\ell^\times$ and let $M = \rho(\sigma) \in \mathrm{Gal}(\overline{K}/K')$. Up to exchanging V_1 and V_2, we have $M_{|V_1}^{2e} = \mathrm{Id}$ and $M_{|V_2}^{2e} = \chi_\ell(\sigma^{2e})$.*

Proof Up to conjugacy, the group $G = \rho(\mathrm{Gal}(\overline{K}/K))$ satisfies the assumptions of Lemma 6.8. We set $G' = \rho(\mathrm{Gal}(\overline{K}/K'))$. Assume first $\ell \equiv 3 \pmod 4$. By Corollary 6.7, the eigenvalues of M^{2e} are $1, 1, \chi_\ell(\sigma^{2e}), \chi_\ell(\sigma^{2e})$ (in some order). The structure of the group described in Lemma 4.13 implies that M^{2e} must be diagonal, because the square of a block-anti-diagonal matrix is diagonal and $2e$ is even. Consider the diagonal entries of M^{2e} (that is, its eigenvalues, taken in a specific order). Assume that the first two diagonal entries of M^{2e} are equal. If $M = \mu \begin{pmatrix} 0 & B(i,j) \\ B(i,j)^{-T} & 0 \end{pmatrix}$, then $2(i-j) \equiv 0 \pmod{\ell - 1}$ and M^{2e} is a scalar. If $M = \mu \begin{pmatrix} 0 & A(i,j) \\ A(i,j)^{-T} & 0 \end{pmatrix}$, then M^{2e} is a scalar. This is a contradiction since $\ell - 1 > 24 \geq 2e$ and the eigenvalues are $1, 1, \chi_\ell(\sigma^{2e}), \chi_\ell(\sigma^{2e})$. So, we can assume that M^{2e} is diagonal with eigenvalues $1, \chi_\ell(\sigma^{2e}), \chi_\ell(\sigma^{2e}), 1$ or $\chi_\ell(\sigma^{2e}), 1, 1, \chi_\ell(\sigma^{2e})$. Lemma 6.14 implies that the matrices in G' are either diagonal or block-anti-diagonal with anti-symmetric matrices as blocks (indeed, in the notation of that lemma we have $[G' : D'] = 2$. If the non-trivial coset consisted of block-anti-diagonal matrices whose blocks are diagonal, M^2 would be a scalar). This implies that $V_1 = \langle e_1, e_4 \rangle$ and $V_2 = \langle e_2, e_3 \rangle$ are G'-invariant. We are in the hypotheses of Lemma 6.12, and there is no invariant subspace of dimension 1 since G acts irreducibly and G' has index 2 in it. Hence V_1 and V_2 are the only two invariant subspaces of dimension 2. Moreover, the eigenvalues of M^{2e} on V_1 are either $1, 1$ or $\chi_\ell(\sigma^{2e}), \chi_\ell(\sigma^{2e})$. The case $\ell \equiv 1 \pmod 4$ is similar. □

6.4 Real multiplication

Theorem 6.16 *Let A be an abelian surface over a number field K. The following hold:*

(1) Assume that $\mathrm{End}_{\overline{K}}(A) = \mathcal{O}$ with $\mathcal{O}$ an order in the real quadratic field $L = \mathbb{Q}(\sqrt{d})$. Let $\ell > C_1$ be a prime. There exists an extension K'/K, of degree at most 2, such that $\mathrm{End}_{\overline{K}}(A) = \mathrm{End}_{K'}(A)$. If ℓ is unramified in K', then (A, ℓ) is not a strong counterexample. In particular, if all the endomorphisms of A are defined over K and $\ell > C_1$, then (A, ℓ) is not a strong counterexample.

(2) Assume that $\mathrm{End}_K(A)$ contains an order $\mathcal{O}$ in the (not necessarily real) quadratic field $L = \mathbb{Q}(\sqrt{d})$. If $\ell > C_1$, then (A, ℓ) is not a strong counterexample.

Proof We begin with the proof of part (1). Let c be the conductor of $\mathcal{O}$ inside $\mathcal{O}_L$. Define $\mathcal{O}_\ell = \mathcal{O} \otimes \mathbb{F}_\ell$.

- If ℓ divides c or is ramified in $\mathcal{O}_\ell$, then by Lemma 6.10 we have that $\mathrm{Nilrad}(\mathcal{O}_\ell) \subset \mathcal{O}_\ell$ is nontrivial and Galois-stable, hence so is the subspace $\mathrm{Nilrad}(\mathcal{O}_\ell) \cdot A[\ell]$ of $A[\ell]$. Thus (A, ℓ) is not a strong counterexample.
- If $\ell \nmid c$ splits in L, then $\mathcal{O}_\ell \cong \mathbb{F}_\ell \times \mathbb{F}_\ell$. Let π_1, π_2 be the idempotents of $\mathcal{O}_\ell$ corresponding to the idempotents $(1, 0), (0, 1)$ of $\mathbb{F}_\ell \times \mathbb{F}_\ell$. The non-trivial subspaces $V_1 = \pi_1 A[\ell]$ and $V_2 = \pi_2 A[\ell]$ are $\mathrm{Gal}(\overline{K}/K')$-stable. If $K' = K$ we immediately have a contradiction. Otherwise, by Lemma 6.15 there is an element $M^{2e} = \rho(\sigma^{2e})$ in $\rho(\mathrm{Gal}\left(\overline{K'}/K'\right))$ that acts on V_1, V_2 with eigenvalues $1, 1$ and δ^{2e}, δ^{2e} (or vice-versa), where δ is a generator of $\mathbb{F}_\ell^\times$ and $e \leq 12$. On the other hand, by [23, Lemma

4.5.1], we have that $\det(\rho(\sigma^{2e}) \mid V_1) = \det(\rho(\sigma^{2e}) \mid V_2) = \chi_\ell(\sigma^{2e}) = \delta^{2e}$. Thus we have $\delta^{2e} = 1$, which contradicts the fact that $0 < 2e \leq 24 < \ell - 1$.

- If $\ell \nmid c$ is inert in L we have $\mathcal{O}_\ell \cong \mathbb{F}_{\ell^2}$ and the natural action of $\mathcal{O}_\ell$ on $A[\ell]$ endows it with the structure of an $\mathbb{F}_{\ell^2}$-vector space of dimension 2. Fix an isomorphism $j : A[\ell] \to \mathbb{F}_{\ell^2}^2$. For every matrix $M \in \mathrm{GL}_4(\mathbb{F}_\ell)$ that acts $\mathbb{F}_{\ell^2}$-linearly on $A[\ell]$, we also denote by $j(M)$ the corresponding matrix in $\mathrm{GL}_2(\mathbb{F}_{\ell^2})$.
  Let $G' = \rho(\mathrm{Gal}\left(\overline{K'}/K'\right))$ be the subgroup (of index ≤ 2) of G that acts $\mathbb{F}_{\ell^2}$-linearly on $A[\ell]$. Let $M \in G'$ and let $v \in A[\ell]$ be an eigenvector with eigenvalue λ. Observe that $\lambda \in \mathbb{F}_\ell$ by Lemma 6.8 and that $j(M) \cdot j(v) = \lambda j(v)$, so each eigenvalue of M is also an eigenvalue of $j(M)$. Thus, M has at most two different eigenvalues.
  Assume that (A, ℓ) is a strong counterexample. Up to conjugacy we may then assume that G is as in Lemma 6.8. Let M be the element of G whose existence is assured by that result: by Lemma 6.9, M has four different eigenvalues, contradiction.

For part (2), in the first two cases we immediately get nontrivial Galois-invariant subspaces defined over K, while the third case is handled exactly as above. □

6.5 Squares of elliptic curves

We will need the following lemma, that is contained in [8, Proposition 4.7]:

Lemma 6.17 *Let K be a number field and let A/K be an abelian surface such that $A_{\overline{K}}$ is isogenous to the square of an elliptic curve E without CM. There exists an extension K'/K of degree at most 3 such that $A_{K'}$ is either isogenous to the product of two elliptic curves or satisfies that $\mathrm{End}_{K'}(A) \otimes \mathbb{Q}$ is a quadratic field. Moreover, this quadratic field can be taken to be either real or equal to $\mathbb{Q}(\zeta_n)$ with $n \in \{3, 4, 6\}$.*

Lemma 6.18 *In the setting of the previous lemma, suppose that $R = \mathrm{End}_{K'}(A)$ is an order in a quadratic field. Let $\ell > 2$ be a prime that does not divide the conductor of R and splits in $R \otimes \mathbb{Q}$. The action of $R \otimes \mathbb{F}_\ell \cong \mathbb{F}_\ell^2$ decomposes $A[\ell]$ as the direct sum of two 2-dimensional sub-modules W_1, W_2, corresponding to the non-trivial idempotents of $\mathbb{F}_\ell^2$. The determinant of the action of $\mathrm{Gal}\left(\overline{K'}/K'\right)$ on each of W_1, W_2 is the product of the cyclotomic character with a character of order dividing 4 or 6.*

Similarly, if ℓ divides the conductor of R or ramifies in $R \otimes \mathbb{Q}$, let x be a non-trivial nilpotent element in $R \otimes \mathbb{F}_\ell$. Let V be the kernel of the action of x on $A[\ell]$. Then V is a 2-dimensional subspace with the following property: for all $\sigma \in \mathrm{Gal}\left(\overline{K'}/K'\right)$, the determinant of $\rho(\sigma \mid V)$ is $\chi_\ell(\sigma)\varepsilon(\sigma)$ for some character ε of order dividing 4 or 6.

Proof When $R \otimes \mathbb{Q} = \mathbb{Q}(\sqrt{d})$ is a real quadratic field, this follows (in a stronger form) from [23, Lemma 4.5.1], see also the comments on page 784 of [23]. For the general case, note that W_1, W_2 are the reduction modulo ℓ of $\mathbb{Z}_\ell$-sub-modules $\mathcal{W}_1$, $\mathcal{W}_2$ (each of rank 2) of $T_\ell(A)$, coming from the decomposition $R \otimes \mathbb{Z}_\ell \cong \mathbb{Z}_\ell^2$, so it suffices to prove that the determinant of the action of $\sigma \in \mathrm{Gal}\left(\overline{K}/K\right)$ on $\mathcal{W}_i$ is given by the

product of the ℓ-adic cyclotomic character and a character of order dividing 4 or 6. Since $T_\ell(A)$ embeds into $T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell =: V_\ell(A)$, it suffices to work with the latter. Let $\mathbb{W}_1, \mathbb{W}_2$ be the subspaces of $V_\ell(A)$ corresponding to $\mathcal{W}_1, \mathcal{W}_2$.

Let L be the minimal (Galois) extension of K over which all the endomorphisms of A are defined. By [8, Theorem 3.4 and Table 8], the degree $[L : K]$ divides 8 or 12, and $[L : K']$ divides 4 or 6 (indeed, if $[L : K] = 12$ or 8, then K'/K is a non-trivial extension). There exists an L-isogeny $A \to E^2$, which induces an isomorphism $\psi : V_\ell(A) \to V_\ell(E^2) = V_\ell(E)^2$. We will use ψ to identify $\mathbb{W}_1, \mathbb{W}_2$ to subspaces of $V_\ell(E^2)$ that we still denote by the same symbol. Note that ψ is equivariant for the action of the absolute Galois group of L.

The hypothesis that ℓ splits in $\mathbb{Q}(\sqrt{d})$ implies that d is a square in $\mathbb{Q}_\ell$, say $d = \beta^2$ with $\beta \in \mathbb{Q}_\ell^\times$. Let $M \in \mathrm{End}(V_\ell(E^2)) \cong \mathrm{Mat}_{2\times 2}(\mathrm{End}(V_\ell E))$ be the endomorphism induced by the action of $\sqrt{d} \in \mathrm{End}(E^2) \otimes \mathbb{Q}$. Since E does not have complex multiplication, the endomorphisms of E^2 are given by $\mathrm{Mat}_{2\times 2}(\mathbb{Z})$, so M is of the form $\begin{pmatrix} \lambda_{11}\,\mathrm{Id} & \lambda_{12}\,\mathrm{Id} \\ \lambda_{21}\,\mathrm{Id} & \lambda_{22}\,\mathrm{Id} \end{pmatrix}$, where the λ_{ij} are rational numbers.

The subspaces $\mathbb{W}_1, \mathbb{W}_2$ can be described as the kernels of $M - \beta, M + \beta$. The kernel of $M - \beta = \begin{pmatrix} \lambda_{11} - \beta & \lambda_{12} \\ \lambda_{21} & \lambda_{22} - \beta \end{pmatrix}$ is the set of $(x, y) \in V_\ell(E) \oplus V_\ell(E)$ that satisfy $(\lambda_{11} - \beta)x + \lambda_{12} y = 0$. Now observe that β cannot be a rational number (since d is not a square in $\mathbb{Q}$), so $\lambda_{11} - \beta$ is non-zero. This shows that $\mathbb{W}_1 = \ker(M - \beta)$ is the graph of the $(\mathrm{Gal}\left(\overline{L}/L\right)$-equivariant) map

$$\begin{aligned} V_\ell(E) &\to V_\ell(E) \oplus V_\ell(E) \\ y &\mapsto \left(-\tfrac{\lambda_{12}}{\lambda_{11} - \beta} y, y \right), \end{aligned}$$

so the determinant of the action of $\mathrm{Gal}(\overline{L}/L)$ on $\mathbb{W}_1$ is the same as the determinant of the action on $V_\ell(E)$, namely, the cyclotomic character. A similar argument applies to $\mathbb{W}_2$, and shows that for $i = 1, 2$ one has $\det(\sigma \mid \mathbb{W}_i) = \chi_\ell(\sigma)$ for all $\sigma \in \mathrm{Gal}(\overline{L}/L)$. Finally, consider the character $\varepsilon_i(\sigma) = \det(\sigma \mid \mathbb{W}_i) \cdot \chi_\ell(\sigma)^{-1}$, defined on all of $\mathrm{Gal}\left(\overline{K'}/K'\right)$. By the above, ε is trivial on $\mathrm{Gal}(\overline{L}/L)$, so its image has order dividing $[\mathrm{Gal}(\overline{K'}/K') : \mathrm{Gal}(\overline{K'}/L)] = [L : K']$. As already observed, this quantity divides 4 or 6, which proves the lemma.

The second half of the statement is proved in the same way. □

Theorem 6.19 *Let K be a number field and let A/K be an abelian surface such that $A_{\overline{K}}$ is isogenous to the square of an elliptic curve E without CM. Let K' be as in Lemma 6.17. If ℓ is unramified in K' and $\ell > C_1$, then (A, ℓ) is not a strong counterexample.*

Proof Assume first that $A_{K'}$ is isogenous to the product of two elliptic curves. Then, $G' = \rho(\mathrm{Gal}(\overline{K}/K'))$ acts reducibly. If $[K' : K]$ is equal to 1 or 3, then by Clifford's theorem $A[\ell]$ must be reducible, contradiction. If $[K' : K] = 2$, let $\psi : E \hookrightarrow A_{K'}$ be an elliptic curve defined over K' and contained in $A_{K'}$. The map ψ induces an injection $E[\ell] \hookrightarrow A[\ell]$ that gives a 2-dimensional G'-invariant subspace V of $A[\ell]$

on which the determinant of the Galois action is the mod-ℓ cyclotomic character. By Lemma 6.15, there exists $M = \rho(\sigma) \in G'$ with $\lambda(M) = \delta$ that generates $\mathbb{F}_\ell^\times$ and such that $\det\left(\rho(\sigma^{2e}) \mid V\right) = 1$ or δ^{4e}. But $\det\left(\rho(\sigma^{2e}) \mid V\right) = \chi_\ell(\sigma)^{2e} = \delta^{2e}$, so $\delta^{2e} = 1$, which contradicts the fact that $0 < 2e < \ell - 1$.

Assume now that $R = \mathrm{End}_{K'}(A)$ is an order in a quadratic field. If ℓ ramifies in R or divides its conductor, Lemma 6.10 implies that $A[\ell]$ is reducible under the action of $\mathrm{Gal}(\overline{K}/K')$. If $[K' : K]$ is equal 1 or 3, then we conclude as above by Clifford's theorem. If $[K' : K] = 2$, then we are in the hypotheses of Lemma 6.15. Reasoning as in the proof of Theorem 6.16, but replacing [23, Lemma 4.5.1] with Lemma 6.18, we find that there are a 2-dimensional subspace V of $A[\ell]$, an element $M^{2e} = \rho(\sigma^{2e})$, and an element $\zeta \in \mathbb{F}_\ell^\times$ of order dividing 12 such that

$$\det\left(\rho(\sigma^{2e}) \mid V\right) = \zeta\delta^{2e} = 1 \text{ or } \delta^{4e}.$$

Raising to the 12th power, this implies $\delta^{24e} = 1$, which contradicts the fact that $0 < 24e \leq 24 \cdot 12 < \ell - 1$. The same argument applies if ℓ does not divide the conductor of R and splits in $R \otimes \mathbb{Q}$. Finally, if ℓ is inert, the proof is identical to the proof of Theorem 6.16 in the inert case. □

6.6 Quaternion algebra

Theorem 6.20 *Let A be an abelian surface over a number field K. Assume that $\mathrm{End}_{\overline{K}}(A)$ is an order in a quaternion algebra and that $\ell > C_1$. If $\mathrm{End}_K(A)$ is an order in a quaternion algebra or an order in a quadratic field, then (A, ℓ) is not a strong counterexample. If $\mathrm{End}_K(A) = \mathbb{Z}$, then there is a field extension K'/K of degree 2 such that $\mathrm{End}_{K'}(A)$ is an order in a quadratic field. If ℓ is unramified in K', then (A, ℓ) is not a strong counterexample.*

Proof Assume by contradiction that (A, ℓ) is a strong counterexample. Let $\overline{R} = \mathrm{End}_{\overline{K}}(A)$ and $R = \mathrm{End}_K(A)$ be the endomorphism rings of A over $\overline{K}$ and over K. Write $\overline{R}_\ell = \overline{R} \otimes \mathbb{F}_\ell$ and $R_\ell = R \otimes \mathbb{F}_\ell$. If $R \neq \mathbb{Z}$ we are done by Theorem 6.16. Assume instead that $R = \mathbb{Z}$. Table 8 in [8] then shows that the Sato-Tate group of A/K must be of type $J(E_n)$ for some $n \in \{2, 3, 4, 6\}$. In this case, there exists a quadratic extension K'/K such that the Sato-Tate group of A over K' is of type E_n, and from [8, Table 8] we see that $\mathrm{End}_{K'}(A) \otimes \mathbb{Q}$ is an (imaginary) quadratic number field. Let $R' = \mathrm{End}_{K'}(A)$ and $R'_\ell = R' \otimes \mathbb{F}_\ell$.

If the Jacobson radical $J := \mathrm{rad}(\overline{R}_\ell)$ of $\overline{R}_\ell$ is non-trivial, then J is a Galois-invariant ideal in $\overline{R}_\ell$, hence $A[\ell][J] := \{x \in A[\ell] : jx = 0 \quad \forall j \in J\}$ is a non-trivial, Galois-invariant subspace of $A[\ell]$ defined over K. This cannot happen since we are assuming that (A, ℓ) is a strong counterexample, hence we may assume that $J = (0)$. The condition $J = (0)$ implies that $\overline{R}_\ell$ is semisimple, that is, it is a direct product of simple algebras. However, a simple algebra of dimension at most 3 is commutative, and the product of commutative algebras is commutative, so $\overline{R}_\ell$ cannot be a non-trivial product. Therefore, $\overline{R}_\ell$ is simple. As the Brauer group of finite fields is trivial,

this implies that $\overline{R}_\ell$ is a matrix algebra over some finite field $\mathbb{F}_{\ell^k}$. Combined with $\dim_{\mathbb{F}_\ell} \overline{R}_\ell = 4$, this yields $\overline{R}_\ell \cong \mathrm{Mat}_2(\mathbb{F}_\ell)$. There are three cases:

- If ℓ divides the conductor of R'_ℓ or is ramified in $R'_\ell \otimes \mathbb{Q}$, let $x \in R'_\ell$ be a non-trivial nilpotent element (which exists by Lemma 6.10). Let $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and note that $\sigma(x) \in R'_\ell$. Indeed, for all $\tau \in \mathrm{Gal}(\overline{K}/K')$, we have $\tau(\sigma(x)) = \sigma(x)$ since $\sigma^{-1}\tau\sigma \in \mathrm{Gal}(\overline{K}/K')$ and x is defined over K'. So, $\sigma(x)$ is a nilpotent element in R'_ℓ, which implies $\sigma(x) = b_\sigma x$ for some $b_\sigma \in \mathbb{F}_\ell^\times$ (notice that the nilpotent elements in R_ℓ form a proper $\mathbb{F}_\ell$-subspace of R'_ℓ, that has dimension 2). This shows that the ideal (x) is stable under $\mathrm{Gal}\left(\overline{K}/K\right)$, hence $\ker(x) \subseteq A[\ell]$ is a nonzero proper subspace of $A[\ell]$ defined over K, contradiction.
- If $R'_\ell \cong \mathbb{F}_{\ell^2}$, we proceed as in the proof of Theorem 6.16. $A[\ell]$ acquires the structure of an $\mathbb{F}_{\ell^2}$-vector space of dimension 2 and $\mathrm{Gal}(\overline{K}/K')$ acts $\mathbb{F}_{\ell^2}$-linearly on it. So, each matrix in $\rho(\mathrm{Gal}(\overline{K}/K'))$ has at most two rational eigenvalues. Choose $M \in G'$ such that $\lambda(M)$ generates $\mathbb{F}_\ell^\times$. Proceeding as in the proof of Lemma 6.9, we show that M^2 is a scalar since it has at most two rational eigenvalues. This contradicts Corollary 6.7.
- If $R'_\ell \cong \mathbb{F}_\ell \times \mathbb{F}_\ell$, then R'_ℓ contains a non-trivial idempotent x. Note that $x \in R'_\ell \subseteq \overline{R}_\ell \cong \mathrm{Mat}_2(\mathbb{F}_\ell)$ and, after a change of basis, we can assume $x = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ since $x^2 - x = 0$. Let $y = 1 - x$, and put $W_1 = xA[\ell]$ and $W_2 = yA[\ell]$. So $W_1 \oplus W_2 = A[\ell]$ and W_1, W_2 are $\mathrm{Gal}(\overline{K}/K')$-invariant. Let L be the smallest field such that $\mathrm{End}_{\overline{K}}(A) = \mathrm{End}_L(A)$. From [8, Table 8], we have $[L : K'] \mid 12$. Now, we want to show that $\det(\rho(\sigma) \mid W_1) = \chi_\ell(\sigma)$ for each σ in $\mathrm{Gal}(\overline{K}/L)$.
  Let $\langle \cdot, \cdot \rangle$ be the Weil pairing and assume that $\langle \cdot, \cdot \rangle_{|W_1}$ is non-degenerate. So, if P_1, P_2 is a basis of W_1, then $\langle P_1, P_2 \rangle = \zeta_\ell$ for ζ_ℓ a primitive ℓ-th root of unity. For each $\sigma \in \mathrm{Gal}(\overline{K}/L)$ we have

$$\zeta_\ell^{\chi_\ell(\sigma)} = \sigma(\zeta_\ell) = \langle P_1, P_2 \rangle^\sigma = \langle P_1, P_2 \rangle^{\det(\rho(\sigma)|W_1)} = \zeta_\ell^{\det(\rho(\sigma)|W_1)}. \quad (11)$$

  Assume now that $\langle \cdot, \cdot \rangle_{|W_1}$ is degenerate. Let $s = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{F}_\ell) \cong \overline{R_\ell}$. Define a bilinear form ψ on W_1 by the formula $\psi(\cdot, \cdot) = \langle \cdot, s\cdot \rangle$. Observe that the multiplication by s gives an isomorphism from W_1 to W_2, so $\psi_{|W_1}$ is non-degenerate, since otherwise the Weil paring on $A[\ell]$ would be degenerate. Proceeding as in the proof of Lemma 3.3 of [5] (see in particular Step 3), one can show that $\langle v, sw \rangle = \langle sv, w \rangle$ for all $v, w \in A[\ell]$. Hence, given $v_1, w_1 \in W_1$, we have $\psi(v_1, w_1) = \langle v_1, sw_1 \rangle = \langle sw_1, v_1 \rangle^{-1} = \langle w_1, sv_1 \rangle^{-1} = \psi(w_1, v_1)^{-1}$, since the Weil pairing is anti-symmetric. Let P_1, P_2 be a basis of W_1, so that $\psi(P_1, P_1) = 1$ and $\psi(P_1, P_2)$ is a primitive ℓ-th root of unity since ψ is non-degenerate on W_1. Note that $\psi(P_1, P_2)^\sigma = \psi(P_1^\sigma, P_2^\sigma)$ for each σ in $\mathrm{Gal}(\overline{K}/L)$ because s is defined over L. Proceeding as in Eq. (11), we conclude that $\det(\rho(\sigma) \mid W_1) = \chi_\ell(\sigma)$ for each σ in $\mathrm{Gal}(\overline{K}/L)$.
  In conclusion, $\det(\rho(\sigma) \mid W_1) = \chi_\ell(\sigma)$ for each σ in $\mathrm{Gal}(\overline{K}/L)$, independently of whether $\langle \cdot, \cdot \rangle_{|W_1}$ is degenerate or not. Given $\sigma \in \mathrm{Gal}(\overline{K}/K')$, we have $\sigma^{12} \in$

$\mathrm{Gal}(\overline{K}/L)$ since $[L : K'] \mid 12$ and then $\det(\rho(\sigma^{12}) \mid W_1) = \chi_\ell(\sigma^{12})$. Therefore, for each $\sigma \in \mathrm{Gal}(\overline{K}/K')$, there is a root of unity ζ of order dividing 12 such that $\det(\rho(\sigma) \mid W_1) = \zeta\chi_\ell(\sigma)$.

We now conclude as in the proof of Theorem 6.19. Let $M = \rho(\sigma) \in \rho(\mathrm{Gal}(\overline{K}/K'))$ with $\lambda(M) = \delta$ that generates $\mathbb{F}_\ell^\times$, which exists because ℓ is unramified in K'. So, $\det(\rho(\sigma) \mid W_1) = \zeta\delta$ with ζ a root of unity of order dividing 12. By Lemma 6.15, W_1 and W_2 are the only $\mathrm{Gal}(\overline{K}/K')$-invariant subspaces of dimension 2 of $A[\ell]$, and $\det(\rho(\sigma^{2e}) \mid W_1) = 1$ or δ^{4e}, where $e \leq 12$. Hence, $\delta^{12e} = 1$, which contradicts the hypothesis $\ell > C_1$.

□

6.7 Complex multiplication by a quartic CM field

Lemma 6.21 *Let k be a field and let G' be an abelian subgroup of $\mathrm{GL}_n(k)$. If G' contains a diagonal matrix whose eigenvalues are all distinct, then G' consists entirely of diagonal matrices.*

Proof Basic linear algebra. □

Lemma 6.22 *Let A be an abelian surface defined over a number field K. Assume that $\mathrm{End}_{\overline{K}}(A) = R$ is an order in a quartic CM field. Assume that ℓ is not ramified in $R \otimes \mathbb{Q}$ and does not divide the conductor of R. If $\ell > C_1$, then (A, ℓ) is not a strong counterexample.*

Proof Let K' be a cyclic extension of K such that $\mathrm{End}_{K'}(A) = R$ with $[K' : K] \mid 4$ (see [8, §4.3]) and let $\rho(\mathrm{Gal}(\overline{K}/K')) = G'$. Let $\mathrm{MT}(A)(\mathbb{F}_\ell) = \{x \in (R \otimes \mathbb{F}_\ell)^\times : \sigma(x)x \in \mathbb{F}_\ell^\times\}$ be the group of $\mathbb{F}_\ell$-rational points of the Mumford Tate group of A, where σ denotes the automorphism of $(R \otimes \mathbb{F}_\ell)^\times$ induced by complex conjugation on R. Theorem 1.3 (2) in [17] gives

$$[\mathrm{MT}(A)(\mathbb{F}_\ell) : \mathrm{MT}(A)(\mathbb{F}_\ell) \cap G'] \leq C_K,$$

where C_K is a constant that depends only on K. In the notation of [17], we have $[K : E^*] \leq [K : \mathbb{Q}]$ and $|F| = 1$, as noticed in [17, §6.4]. We also have $\mu^* \leq 12$, because a field of degree 4 cannot contain more than 12 roots of unity. Thus we may take $C_K = 12[K : \mathbb{Q}]$. By our assumptions on ℓ, the ring $R \otimes \mathbb{F}_\ell$ is a product of fields.

- If $R \otimes \mathbb{F}_\ell = \mathbb{F}_\ell^4$, then up to reordering the factors $\mathbb{F}_\ell$ we have $\sigma(a, b, c, d) = (b, a, d, c)$. In particular, $\sigma(x)x \in \mathbb{F}_\ell^\times$ if and only if $ab = cd \neq 0$, so $|\mathrm{MT}(A)(\mathbb{F}_\ell)| = (\ell - 1)^3$.

  Suppose by contradiction that (A, ℓ) is a strong counterexample, so that—up to conjugacy—we may assume that $G = \rho(\mathrm{Gal}\left(\overline{K}/K\right))$ is as in Lemma 6.8. In particular, the subgroup of diagonal matrices in G has index at most 8. Let D' be the subgroup of diagonal matrices in G'. We have $|D' \cap \mathrm{MT}(A)(\mathbb{F}_\ell)| \geq \frac{1}{8}|G' \cap \mathrm{MT}(A)(\mathbb{F}_\ell)| \geq |\mathrm{MT}(A)(\mathbb{F}_\ell)|/(8C_K) = (\ell - 1)^3/(8C_K)$. By Lemma 6.11, the group D' contains at most $4(\ell-1)^2$ matrices having at most three distinct

eigenvalues. Since $\ell > C_1$, we have $(\ell-1)^3/(8C_K) > 4(\ell-1)^2$. Therefore, there is a matrix $M \in D' \cap \mathrm{MT}(A)(\mathbb{F}_\ell)$ having four different eigenvalues. Moreover, G' is abelian by the theory of complex multiplication (see for example [28, Corollary 2 on p. 502]), so $G' = D'$ by Lemma 6.21. Let D be the group of diagonal matrices in G. We have shown $G' \leq D$. Moreover, since $[G : G'] \leq 4$ and $[G : D] \geq 4$ by Lemma 6.21, we have $G' = D$. Hence, $G/D = G/G' \cong \mathrm{Gal}(K'/K)$, which is a contradiction, because the extension K'/K is cyclic but the group G/D is not (see Lemma 6.21).

- If $R \otimes \mathbb{F}_\ell = \mathbb{F}_{\ell^4}$, then $\mathrm{MT}(A)(\mathbb{F}_\ell) = \{x \in \mathbb{F}_{\ell^4}^\times : N_{\mathbb{F}_{\ell^4}/\mathbb{F}_{\ell^2}}(x) \in \mathbb{F}_\ell^\times\}$. Suppose by contradiction that (A, ℓ) is a strong counterexample. Letting $H = \{x \in \mathrm{MT}(A)(\mathbb{F}_\ell) : x \in \mathbb{F}_\ell^\times\}$, we have $[\mathrm{MT}(A)(\mathbb{F}_\ell) : H] \geq \ell - 1$. Note that $G' \cap \mathrm{MT}(A)(\mathbb{F}_\ell) \leq H$ since every matrix in G' has a rational eigenvalue, and the eigenvalues of $x \in \mathbb{F}_{\ell^4}^\times$ acting on $A[\ell]$ are given by the $\mathbb{F}_{\ell^4}/\mathbb{F}_\ell$-conjugates of x. It follows that $[\mathrm{MT}(A)(\mathbb{F}_\ell) : G' \cap \mathrm{MT}(A)(\mathbb{F}_\ell)] \geq \ell - 1$, which contradicts $\ell > C_1 > C_K$.
- If $R \otimes \mathbb{F}_\ell = \mathbb{F}_{\ell^2} \times \mathbb{F}_{\ell^2}$, then

$$\mathrm{MT}(A)(\mathbb{F}_\ell) = \{(x, y) \in \mathbb{F}_{\ell^2}^\times \times \mathbb{F}_{\ell^2}^\times : N_{\mathbb{F}_{\ell^2}/\mathbb{F}_\ell}(x) = N_{\mathbb{F}_{\ell^2}/\mathbb{F}_\ell}(y)\}$$

if σ fixes the two primes of $R \otimes \mathbb{Q}$ above ℓ and

$$\mathrm{MT}(A)(\mathbb{F}_\ell) = \{(x, y) \in \mathbb{F}_{\ell^2}^\times \times \mathbb{F}_{\ell^2}^\times : xy \in \mathbb{F}_\ell^\times\}$$

if σ swaps them. Let $H = \{(x, y) \in \mathrm{MT}(A)(\mathbb{F}_\ell) : x \in \mathbb{F}_\ell^\times, y \in \mathbb{F}_\ell^\times\}$ and notice that we have $[\mathrm{MT}(A)(\mathbb{F}_\ell) : H] \geq \ell - 1$. As above we have $G' \leq H$, and we conclude as in the previous case.

□

Theorem 6.23 *Let A be an abelian surface over a number field K. Assume that $\mathrm{End}_{\overline{K}}(A) = R$ is an order in a CM field. If $\ell > C_1$, then (A, ℓ) is not a strong counterexample.*

Proof If ℓ is unramified in $\mathrm{End}_{\overline{K}}(A)$ and does not divide the conductor of this order, we conclude using Lemma 6.22. Otherwise, we use Lemma 6.10. □

6.8 Proof of the main results

We can now easily conclude the proof of our main results.

Proof of Theorem 6.1 If $\mathrm{End}_{\overline{K}}(A)$ is an order in a real quadratic field, the claim follows from Theorem 6.16. If $A_{\overline{K}}$ is isogenous to the square of an elliptic curve without CM, we conclude using Theorem 6.19. If $\mathrm{End}_{\overline{K}}(A)$ is an order in a quaternion algebra, we apply Theorem 6.20. Finally, if $\mathrm{End}_{\overline{K}}(A)$ is an order in a quartic CM field, the conclusion follows from Theorem 6.23. □

Lemma 6.24 *Let A be an abelian surface over a number field K. If $\mathrm{End}_K(A) \otimes \mathbb{Q} \supseteq \mathbb{Q}^2$, then (A, ℓ) is not a strong counterexample.*

Proof The assumption $\mathrm{End}_K(A) \otimes \mathbb{Q} \supseteq \mathbb{Q}^2$ implies that A is isogenous (over K) to the product of two elliptic curves E_1 and E_2. By Corollary 2.4, this implies that $(E_1 \times E_2, \ell)$ is a strong counterexample, but this is obviously a contradiction since $(E_1 \times E_2)[\ell] \cong E_1[\ell] \oplus E_2[\ell]$ is not irreducible. □

Proof of Corollary 6.2 If $\mathrm{End}_K(A)$ is larger than $\mathbb{Z}$, then it contains an order in a quadratic field or in $\mathbb{Q}^2$ (see Sect. 2.1, and notice that a quartic CM field contains a real quadratic field). The claim follows from Theorem 6.16 and Lemma 6.24. □

6.9 Squares of CM elliptic curves

The goal of this section is to construct infinitely many strong counterexamples $(A/\mathbb{Q}, \ell)$ with A geometrically isogenous to the square of a CM elliptic curve and ℓ unbounded. Such examples will be obtained as twists of E^2, where $E/\mathbb{Q}$ is the elliptic curve with Weierstrass equation $y^2 = x^3 + x$. The construction is reminiscent of Katz's examples in [12] that show that the local-global principle for the existence of torsion points fails in dimension ≥ 3.

We begin by finding suitable Galois extensions of $\mathbb{Q}$ with Galois group D_8 (the dihedral group with 16 elements), which we will then use to construct our twists. The following is a special case of [13, Theorems 5 and 6].

Theorem 6.25 *Let F be a field of characteristic different from 2. Let a and b in F be such that the following hold:*

- *a, b, and ab are not squares in F;*
- *$b = a - 1$;*
- *the equation $X^2 - aY^2 - 2Z^2 - 2abV^2 = 0$ has a solution in F with $(X, Y) \neq (0, 0)$.*

There exists $q \in F^*$ such that the Galois extension $F(\sqrt{a}, \sqrt{b}, \sqrt{2q(a + \sqrt{a})})/F$ has Galois group D_4 and can be embedded in a D_8-extension, cyclic over $F(\sqrt{b})$.

Lemma 6.26 *Let $\ell \equiv 1 \pmod 4$ be a prime. There exists a Galois extension $L/\mathbb{Q}$ such that:*

- $\mathrm{Gal}(L/\mathbb{Q}) \cong D_8 = \langle r, s \mid r^8 = s^2 = 1, srs = r^{-1} \rangle$;
- *$\sqrt{\ell}$ and i are in L;*
- *$r(i) = -i$, $s(i) = i$, $r(\sqrt{\ell}) = -\sqrt{\ell}$, and $s(\sqrt{\ell}) = -\sqrt{\ell}$.*

Proof By Fermat's theorem on sums of two squares there exist integers X_1 and X_2 such that $X_1^2 + X_2^2 = \ell$. Let $a = -X_2^2/X_1^2$ and $b = -\ell/X_1^2 = a - 1$. The equation

$$X^2 - aY^2 - 2Z^2 - 2abV^2 = 0$$

has the solution $(X, Y, Z, V) = (X_2/X_1, 1, X_2/X_1, 0)$. Hence, by Theorem 6.25, there exists a Galois extension $L/\mathbb{Q}$ such that $\mathrm{Gal}(L/\mathbb{Q}) \cong D_8$, the three quadratic sub-extensions of $L/\mathbb{Q}$ are $\mathbb{Q}(\sqrt{\pm\ell})$ and $\mathbb{Q}(i)$, and $\mathrm{Gal}(L/\mathbb{Q}(\sqrt{-\ell}))$ is cyclic.

There is only one cyclic subgroup of order 8 of D_8, hence only one quadratic field $E \subset L$ such that L/E is cyclic. We know $E = \mathbb{Q}(\sqrt{-\ell})$. Let r be an element of order

8 in $\mathrm{Gal}(L/\mathbb{Q})$. If r fixes $\sqrt{\ell}$, then $\mathbb{Q}(\sqrt{\ell}) \subseteq L^{\langle r\rangle} = E$, contradiction. The same holds for i. Hence, $r(\sqrt{\ell}) = -\sqrt{\ell}$ and $r(i) = -i$. Let s' be an element of $\mathrm{Gal}(L/\mathbb{Q})$ that is not a power of r. If s' fixes $\sqrt{-\ell}$, then the whole of $\mathrm{Gal}(L/\mathbb{Q})$ fixes this element, which is impossible since $\sqrt{-\ell} \notin \mathbb{Q}$. So we have $s'(\sqrt{-\ell}) = -\sqrt{-\ell}$, hence $s'(i) = -i$ and $s'(\sqrt{\ell}) = \sqrt{\ell}$, or $s'(i) = i$ and $s'(\sqrt{\ell}) = -\sqrt{\ell}$. In the two cases, we take respectively $s = s'r$ and $s = s'$. □

Example 6.27 Take $\ell = 13$, $X_1 = 3$ and $X_2 = 2$, so that $b = -13/9$ and $a = -4/9$. Theorem 6.25 applies with $q = 9/2$: the field

$$L' = \mathbb{Q}(\sqrt{-4/9}, \sqrt{-13/9}, \sqrt{2 \cdot (9/2) \cdot (-4/9 + 2i/3)}) = \mathbb{Q}(i, \sqrt{13}, \sqrt{4 - 6i})$$

is a D_4-extension of $\mathbb{Q}$, and embeds in the D_8-extension L given by the splitting field of $x^8 - 96x^6 - 1280x^4 + 227328x^2 + 8998912$. One can check that $L/\mathbb{Q}(\sqrt{-b})$ is cyclic.

Proposition 6.28 *Let $\ell > 5$ be a prime with $\ell \equiv 5 \pmod 8$. There exists an abelian surface A, defined over $\mathbb{Q}$ and geometrically isogenous to the square of a CM elliptic curve, such that (A, ℓ) is a strong counterexample.*

Proof Let E be the elliptic curve $y^2 = x^3 + x$. The prime ℓ (which is in particular congruent to 1 modulo 4) splits in $\mathbb{Z}[i]$, so, up to a choice of basis for $E[\ell]$, the action of the automorphism $[i] : (x, y) \mapsto (-x, iy)$ of $E_{\overline{\mathbb{Q}}}$ on $E[\ell]$ is represented by $N = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, where i is one of the two primitive fourth roots of unity in $\mathbb{F}_\ell^\times$. By [17, Theorem 1.3], the image G_ℓ of the mod-ℓ Galois representation attached to $E/\mathbb{Q}$ is the normaliser of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. In particular, in the basis above G_ℓ is given by the set $\{A(a, b), B(a, b) : a, b \in \mathbb{F}_\ell^\times\}$, where

$$A(a, b) = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, \quad B(a, b) = \begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix}.$$

The subgroup $\rho_{E,\ell}\left(\mathrm{Gal}\left(\overline{\mathbb{Q}(i)}/\mathbb{Q}(i)\right)\right)$ is given by those Galois automorphisms that commute with the action of $[i]$, that is, $\{A(a, b) : a, b \in \mathbb{F}_\ell^\times\}$. In other words, $\rho_E(\sigma)$ is of the form $A(a, b)$ for suitable a, b if $\sigma(i) = i$, and it is of the form $B(a, b)$ otherwise. Moreover, in the two cases one has

$$\chi_\ell(\sigma) = \det \rho_{E,\ell}(\sigma) = \pm ab;$$

since -1 is a square modulo ℓ, the quantity $ab \in \mathbb{F}_\ell^\times$ is a square if and only if $\chi_\ell(\sigma)$ is a square, if and only if σ fixes $\sqrt{\ell}$.

We now construct the desired abelian surface A as a twist of E^2. Let L be as in Lemma 6.26 and identify $\mathrm{End}(E^2_{\overline{\mathbb{Q}}})$ with $\mathrm{Mat}_{2\times 2}(\mathrm{End}(E_{\overline{\mathbb{Q}}}))$. We define a cocycle $c : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E^2_{\overline{\mathbb{Q}}}) \subset \mathrm{End}(E^2_{\overline{\mathbb{Q}}})$ as the composition of the canonical projection

$$\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to \mathrm{Gal}(L/\mathbb{Q}) \cong \langle r, s \mid r^8 = s^2 = 1, srs = r^{-1}\rangle$$

with the unique cocycle of $\mathrm{Gal}(L/\mathbb{Q})$ mapping r to $\begin{pmatrix} 0 & \mathrm{Id} \\ [i] & 0 \end{pmatrix}$ and s to $\begin{pmatrix} 0 & \mathrm{Id} \\ \mathrm{Id} & 0 \end{pmatrix}$. One checks easily that these conditions do in fact define a cocycle. Let now A denote the twist of E^2 by the class of c in $H^1(\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right), \mathrm{Aut}(E^2_{\overline{\mathbb{Q}}}))$, so that for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we have

$$\rho_{A,\ell}(\sigma) = c(\sigma)\rho_{E^2,\ell}(\sigma).$$

We now show that (A, ℓ) is a strong counterexample. We start by checking that $\rho_{A,\ell}(\sigma)$ admits at least one $\mathbb{F}_\ell$-rational eigenvalue for every $\sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$, distinguishing cases according to the image $\sigma_{|L}$ of σ in $\mathrm{Gal}(L/\mathbb{Q})$. Recall that we denote by $N = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ the matrix giving the action of $[i]$ on $E[\ell]$. If $\sigma_{|L} = r$, then $\sigma(i) = -i$, so for suitable $a, b \in \mathbb{F}_\ell^\times$ we have

$$\rho_{A,\ell}(\sigma) = \begin{pmatrix} 0 & \mathrm{Id} \\ N & 0 \end{pmatrix} \begin{pmatrix} B(a,b) & 0 \\ 0 & B(a,b) \end{pmatrix} = \begin{pmatrix} 0 & B(a,b) \\ NB(a,b) & 0 \end{pmatrix}.$$

Here ab is not a square in $\mathbb{F}_\ell^\times$, because by construction r (hence also σ) does not fix $\sqrt{\ell}$. Thus $\rho_{A,\ell}(\sigma)$ has the rational eigenvalue $\sqrt{iab}$: note that iab is a square since i and ab are not (here we use $\ell \equiv 5 \pmod 8$ to deduce that i is not a square modulo ℓ). We may reason similarly for all other cases. If $\sigma_{|L} = s$, then $\sigma(i) = i$, so

$$\rho_{A,\ell}(\sigma) = \begin{pmatrix} 0 & \mathrm{Id} \\ \mathrm{Id} & 0 \end{pmatrix} \begin{pmatrix} A(a,b) & 0 \\ 0 & A(a,b) \end{pmatrix} = \begin{pmatrix} 0 & A(a,b) \\ A(a,b) & 0 \end{pmatrix}$$

has the $\mathbb{F}_\ell$-rational eigenvalues $\pm a, \pm b$. If $\sigma_{|L} = sr$, then $\sigma(\sqrt{\ell}) = \sqrt{\ell}$ and $\sigma(i) = -i$, so

$$\rho_{A,\ell}(\sigma) = \begin{pmatrix} N & 0 \\ 0 & \mathrm{Id} \end{pmatrix} \begin{pmatrix} B(a,b) & 0 \\ 0 & B(a,b) \end{pmatrix} = \begin{pmatrix} NB(a,b) & 0 \\ 0 & B(a,b) \end{pmatrix}$$

with $ab \in \mathbb{F}_\ell^{\times 2}$, so that $\rho_{A,\ell}(\sigma)$ has the rational eigenvalues $\pm\sqrt{ab}$. If $\sigma_{|L} = 1$, then $\rho_{A,\ell}(\sigma)$ is represented by a diagonal matrix, hence admits $\mathbb{F}_\ell$-rational eigenvalues.

For the other cases, note that every element of D_8 can be written as a power of r^2 times an element of the set $\{1, r, s, sr\}$. From this and the fact that $c(r^2)$ is a diagonal matrix with diagonal entries equal to $\pm i$, it is easy to conclude that $\rho_{A,\ell}(\sigma)$ has an $\mathbb{F}_\ell$-rational eigenvalue for every $\sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$.

Let $G = \rho_{A,\ell}\Big(\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)\Big)$ and let $H < G$ be the subgroup of block-diagonal matrices. Let χ_1 (resp. χ_2) be the character of the representation of H on $V_1 = \langle e_1, e_2\rangle$ (resp. $V_2 = \langle e_3, e_4\rangle$). Then, $\langle \chi_1, \chi_1\rangle_H = \langle \chi_2, \chi_2\rangle_H = 1$ since H acts absolutely irreducibly on V_1 and V_2. Let σ be such that $\sigma_{|L} = r^2$ and such that $\rho_{E,\ell}(\sigma) = A(a,b)$ with $a \neq b$. To see that such an element exists, consider the set $S := \{\rho_{E,\ell}(\sigma_0\sigma') :$

$\sigma' \in \mathrm{Gal}(\overline{\mathbb{Q}}/L)\}$, where σ_0 is any element of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ restricting to r^2 on L. This is in bijection with $\rho_{E,\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/L))$, which has order at least

$$\frac{1}{[L:\mathbb{Q}]}|\rho_{E,\ell}(\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right))| = \frac{1}{8}(\ell-1)^2 > \ell - 1,$$

so S must contain some matrix $A(a,b)$ with $a \neq b$ (notice that r^2 fixes i, so every matrix in S is diagonal). On the other hand, any $\sigma_0\sigma'$ as in the definition of S restricts to r^2 on L. So, $M = \rho_{A,\ell}(\sigma) = \begin{pmatrix} \overline{N}A(a,b) & 0 \\ 0 & NA(a,b) \end{pmatrix}$ is in H and $\chi_1(M) \neq \chi_2(M)$. Therefore, $\langle \chi_1, \chi_2 \rangle_H = 0$ and $\langle \chi_1 + \chi_2, \chi_1 + \chi_2 \rangle_H = 2$. Let χ be the character of the representation of G. Then,

$$\langle \chi, \chi \rangle_G = \frac{1}{2}\langle \chi, \chi \rangle_H = \frac{1}{2}\langle \chi_1 + \chi_2, \chi_1 + \chi_2 \rangle_H = 1$$

and so, thanks to Proposition 3.9, G acts irreducibly. By Lemma 1.2, (A, ℓ) is a strong counterexample. □

Remark 6.29 With more work, the construction given in the proof can be adapted to $y^2 = x^3 + 1$, and probably to all elliptic curves over $\mathbb{Q}$ with potential CM (in each case, one would get a different congruence condition on the prime ℓ).

Remark 6.30 A variant of the same construction can be used to obtain weak counterexamples over many number fields K. Let $E/\mathbb{Q}$ be a CM elliptic curve, with CM by an order in the quadratic imaginary field F, and let E_K denote the base-change of E to K. Suppose that K does not contain F. For ℓ sufficiently large and split in F, the image of $\rho_{E_K,\ell}$ is the full normaliser of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. Let $L = \mathbb{Q}(\sqrt{\ell^*})$ be the quadratic subfield of $\mathbb{Q}(\zeta_\ell)$ and let $A = \mathrm{Res}_{KL/K}(E_L)$, where Res denotes the Weil restriction of scalars. Using the fact that the mod-ℓ Galois representations attached to the abelian surface A/K are given by $\mathrm{Ind}_{G_{KL}}^{G_K}(\rho_{E,\ell})$, one checks easily that (A, ℓ) is a weak counterexample to the local-global principle for isogenies.

6.10 The semistable case for $K = \mathbb{Q}$

To finish our discussion of strong counterexamples, we will show the following non-existence result for *semistable* counterexamples over the rational numbers (and other fields of small discriminant):

Theorem 6.31 *Let K be a number field such that every non-trivial extension L/K ramifies at least at one finite place (for example $K = \mathbb{Q}$). Let A/K be a semistable abelian surface and let $\ell \neq 5$ be a prime. The pair $(A/K, \ell)$ is not a strong counterexample to the local-global principle for isogenies.*

The idea is that such a counterexample would lead to the existence of an everywhere unramified extension of K. The proof relies on the following theorem:

Theorem 6.32 (Grothendieck [10, Exposé IX, Proposition 3.5]) *Let A be an abelian variety over the number field K with semistable reduction at v, a place of characteristic p. Let $I_v \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ denote a choice of inertia group at v. The action of I_v on the ℓ^n-division points of A for $\ell \neq p$ is rank two unipotent, that is, for $\sigma \in I_v$ we have $(\sigma - 1)^2 A[\ell^n] = 0$. In particular, I_v acts through its maximal pro-ℓ quotient, which is procyclic.*

Proof of Theorem 6.31 By Remark 3.4 and the assumption $\ell \neq 5$ we may assume that $\ell \geq 7$. Since A is a strong counterexample, the group G_ℓ is a Hasse subgroup of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ (here we also use Corollary 2.5 to deduce that G_ℓ is contained in $\mathrm{GSp}_4(\mathbb{F}_\ell)$). By Theorem 5.5 we have $|G_\ell| \not\equiv 0 \pmod{\ell}$. Theorem 6.32 then implies that for every prime $p \neq \ell$ the inertia group at p acts trivially on $A[\ell]$. Moreover, the assumption of semistability implies that the action of I_ℓ, the inertia group at ℓ, factors through the pro-cyclic quotient I_ℓ^t (see Theorem 6.4), so $\rho_\ell(I_\ell)$ is cyclic. Let $L = K(A[\ell])$. The extension L/K is Galois with group G_ℓ. The fact that K has no everywhere unramified extensions implies that G_ℓ is generated by its inertia subgroups (indeed, let H be the subgroup generated by all the inertia subgroups. The subfield of L fixed by H is an unramified extension of K, hence it is K itself, and by Galois theory this implies $H = G_\ell$). The only non-trivial inertia subgroup corresponds to the prime ℓ and is cyclic, so G_ℓ is cyclic, say generated by g. The condition that (A, ℓ) is a strong counterexample gives that g stabilises a non-trivial subspace of $A[\ell]$, but then so does all of G_ℓ, contradiction. □

Remark 6.33 It is well known that the field of rational numbers satisfies the hypothesis of the previous theorem. Other examples include quadratic imaginary fields of class number one, real quadratic fields with conductor less than 67, and cyclotomic fields with class number one: in all cases, this follows from the Odlyzko bounds on root discriminants [21].

Acknowledgements It is a pleasure to thank Samuele Anni for his interest in this project and for several discussions on the topic of this paper, which led in particular to Remark 6.30 and to a better understanding of the difficulties with [6]. We also thank John Cullinan for correspondence about [6] and Barinder Banwait for his many insightful comments on the first version of this paper. Finally, we thank the referee for their thorough reading of the manuscript.

Funding Open access funding provided by Università di Pisa within the CRUI-CARE Agreement. The authors have been partially supported by MIUR (Italy) through PRIN 2017 "Geometric, algebraic and analytic methods in arithmetic" and PRIN 2022 "Semiabelian varieties, Galois representations and related Diophantine problems", and by the University of Pisa through PRA 2018-19 and 2022 "Spazi di moduli, rappresentazioni e strutture combinatorie". The first author is a member of the INdAM group GNSAGA.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

Appendix

The goal of this appendix is to prove following stronger version of Theorem 5.5.

Theorem A.1 *Let $G < \mathrm{GSp}_4(\mathbb{F}_\ell)$ be a Hasse group with $\lambda(G) = \mathbb{F}_\ell^\times$. The subgroup $G^1 = G \cap \mathrm{Sp}_4(\mathbb{F}_\ell)$ acts reducibly.*

Recall that exceptional Hasse groups are defined in Definition 5.1. From Lemma 5.4, we know that if G^1 is not exceptional, then it acts reducibly. Thus, we just need to prove that G^1 cannot be an exceptional Hasse group.

The set of exceptional groups is finite and fully classified in Table 1. In particular, exceptional groups have cardinality bounded independently of ℓ. Given a group G, we denote by $\mathrm{Aut}(G)$ its automorphism group, by $\mathrm{Inn}(G)$ the subgroup of inner automorphisms, and by $\mathrm{Out}(G)$ the quotient $\mathrm{Aut}(G)/\mathrm{Inn}(G)$.

Definition A.2 Let $G^1 < \mathrm{Sp}_4(\mathbb{F}_\ell)$. We say that G^1 has property (P1) if the following holds. For all $[\varphi] \in \mathrm{Out}(G^1)$ of order 2 there exists a representative $\varphi \in \mathrm{Aut}(G^1)$ of $[\varphi]$ such that one of the following holds:

- $\varphi^2 = \mathrm{Id}$;
- for all $g_1 \in G^1$ such that φ^2 is conjugation by g_1, there exists $g_1' \in G^1$ such that all the eigenvalues λ of $\varphi(g_1')\varphi^2(g_1')g_1$ satisfy $\lambda^{(\ell-1)/2} \neq -1$.

Definition A.3 Let $G^1 < \mathrm{Sp}_4(\mathbb{F}_\ell)$ and let $\tilde{G}^1$ be the natural immersion of G^1 in $\mathrm{Sp}_4(\mathbb{F}_{\ell^2})$. We say that G^1 has property (P2) if for all groups $\tilde{G} \subseteq \mathrm{Sp}_4(\mathbb{F}_{\ell^2})$ such that $[\tilde{G} : \tilde{G}^1] = 2$, there exists g in $\tilde{G} \setminus \tilde{G}^1$ such that each eigenvalue μ of g has multiplicative order k with $v_2(k) \neq v_2(\ell - 1) + 1$.

Let G be a Hasse subgroup of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ with $\lambda(G) = \mathbb{F}_\ell^\times$. We will show that $G \cap \mathrm{Sp}_4(\mathbb{F}_\ell)$ satisfies neither (P1) nor (P2). Then, we will show that each exceptional group has property (P1) or (P2), and so $G \cap \mathrm{Sp}_4(\mathbb{F}_\ell)$ cannot be an exceptional group.

Lemma A.3 *Let G^1 be a Hasse subgroup of $\mathrm{Sp}_4(\mathbb{F}_\ell)$. The center $Z(G^1)$ is contained in $\{\pm \mathrm{Id}\}$.*

Proof Let $g_1 \in Z(G^1)$ and let μ be one of its rational eigenvalues. As g_1 commutes with G^1, the kernel of $g_1 - \mu\,\mathrm{Id}$ is a non-trivial G^1-invariant subspace of $\mathbb{F}_\ell^4$. Since G^1 is Hasse, we have $\ker(g_1 - \mu\,\mathrm{Id}) = \mathbb{F}_\ell^4$ and $g_1 = \mu\,\mathrm{Id}$. From $1 = \lambda(g_1) = \mu^2$ we obtain $\mu = \pm 1$. □

Lemma A.4 *Let $G \leq \mathrm{GSp}_4(\mathbb{F}_\ell)$ be a group with $\lambda(G) = \mathbb{F}_\ell^\times$ and $G = G^{\mathrm{sat}}$. Assume that $G^1 = G \cap \mathrm{Sp}_4(\mathbb{F}_\ell)$ satisfies* (P1) *and is a Hasse subgroup of $\mathrm{Sp}_4(\mathbb{F}_\ell)$. Then, G is not Hasse.*

Proof Let $x \in G$ be an element whose multiplier δ generates $\mathbb{F}_\ell^\times$. Then, x normalises G^1 and conjugation by x, that we denote by φ_x, is an automorphism of G^1.

Assume first that φ_x is an inner automorphism, so that there exists $g_1 \in G^1$ such that $\varphi_x = \varphi_{g_1}$ and hence $\varphi_{g_1^{-1}x} = \mathrm{Id}$. Put $x' = g_1^{-1}x$ and notice that $(x')^2/\delta$ is in the center of G^1, since conjugation by x' is the identity. By Lemma A.3 we have

$(x')^2 = \pm\delta$, so $(x')^{\ell-1} = -1$ (recall that $\mathrm{Sp}_4(\mathbb{F}_\ell)$ admits Hasse subgroups only for $\ell \equiv 1 \pmod 4$, see Theorem 3.2, so $(\ell-1)/2$ is even). Therefore, $x' \in G$ does not have a rational eigenvalue and G is not Hasse.

Assume that φ_x is not an inner automorphism. We have $x^2/\delta = g \in G^1$ and $\varphi_x^2 = \varphi_{x^2} = \varphi_g$ is an inner automorphism of G^1. Thus, φ_x has order 2 in $\mathrm{Out}(G^1)$. Let $\varphi \in \mathrm{Aut}(G^1)$ be the representative of the class of φ_x in $\mathrm{Out}(G^1)$ given in Definition A.2. We have $\varphi = \varphi_x\varphi_h$ for some $h \in G^1$. Let $y = xh \in G$, so that $\varphi_y = \varphi$ and $y^2 = \delta g_1$ for some $g_1 \in G^1$. If $\varphi^2 = \mathrm{Id}$, then $g_1 = \pm\mathrm{Id}$ and $y^2 = \pm\delta$. Then $y^{\ell-1} = -\mathrm{Id}$, so y does not have a rational eigenvalue and G is not Hasse. It remains to study the case $\varphi^2 \neq \mathrm{Id}$. Let $g_1' \in G^1$ be as in Definition A.2. Letting $x' = yg_1' \in G$ we have

$$(x')^2 = yg_1'yg_1' = yg_1'(y)^{-1}(y)^2g_1'(y)^{-2}y^2 = \delta\varphi_y(g_1')\varphi_{y^2}(g_1')g_1.$$

Using the fact that $\delta^{(\ell-1)/2} = -1$ and the property of g_1' given in Definition A.2, we see that $(x')^{\ell-1}$ does not have 1 as an eigenvalue. It follows that x' does not have a rational eigenvalue, hence G is not Hasse. □

Lemma A.5 *Let $G \leq \mathrm{GSp}_4(\mathbb{F}_\ell)$ be a group with $\lambda(G) = \mathbb{F}_\ell^\times$ and $G = G^{\mathrm{sat}}$. Assume that the group $G^1 = G \cap \mathrm{Sp}_4(\mathbb{F}_\ell)$ has property* (P2) *and is a Hasse subgroup of $\mathrm{Sp}_4(\mathbb{F}_\ell)$. Then, G is not Hasse.*

Proof Let $x \in G$ be an element whose multiplier δ generates $\mathbb{F}_\ell^\times$. Clearly $x' := x/\sqrt{\delta}$ has coefficients in $\mathbb{F}_{\ell^2}$ and satisfies $\lambda(x') = \frac{1}{\delta}\lambda(x) = 1$, so x' is in $\mathrm{Sp}_4(\mathbb{F}_{\ell^2})$. Furthermore, $(x')^2$ is in G^1 and normalises G^1, so $\tilde{G} = G^1 \cdot \langle x' \rangle$ is a subgroup of $\mathrm{Sp}_4(\mathbb{F}_{\ell^2})$ and has order $|G^1| \cdot |\langle x' \rangle| / |G^1 \cap \langle x' \rangle| = 2|G^1|$. Let $g \in \tilde{G} \setminus G^1$ be as in Definition A.3. So, $g_1 = \sqrt{\delta}g \in G$ and $g_1^{\ell-1} = -g^{\ell-1}$. By definition of g we know that $g^{\ell-1}$ does not have -1 as eigenvalue, so $g_1^{\ell-1}$ does not have 1 as eigenvalue. Hence, g_1 does not have a rational eigenvalue and G is not Hasse. □

Lemma A.6 *Every exceptional Hasse subgroup G^1 of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ satisfies at least one among* (P1) *and* (P2).

Proof By Theorem 3.2 and Table 1, there is only a finite number of groups to check, which we do case by case by a computer calculation. Note that it is not enough to consider the groups appearing in Table 1, but we also need to check all of their subgroups. We briefly explain how our MAGMA script works.

We first check which exceptional groups have property (P1). This happens for the vast majority of the exceptional groups. Then, for the remaining groups, we check that they satisfy (P2). Note that checking if a group has (P2) is computationally more expensive than checking if a group has (P1). To check if G^1 has (P1) we use the following algorithm.

- Let G^1 be one of the exceptional groups that arise from the classification in Theorem 3.2 with the condition $\ell \equiv m \pmod M$. The group G^1 is equipped with a character χ on a 4-dimensional vector space V.

- Let $g_1 \in G^1$ and let k be the order of one of its eigenvalues λ. The condition $\lambda^{(\ell-1)/2} = -1$ implies $v_2(\ell-1) = v_2(k)$, so we check a sufficient condition that ensures $v_2(k) \neq v_2(\ell-1)$. If $v_2(m-1) < v_2(M)$, then $v_2(\ell-1) = v_2(m-1)$ and we check directly if $v_2(m-1) \neq v_2(k)$. If $v_2(m-1) \geq v_2(M)$, then $v_2(\ell-1) \geq v_2(m-1) = v_2(M)$ and we check if $v_2(M) > v_2(k)$.
- For all exceptional groups G^1 and every class of order 2 in $\mathrm{Out}(G^1)$, we select a representative φ of the class and $f \in G^1$ such that φ^2 is conjugation by f. Note that the choice of f is unique up to multiplication by ± 1 thanks to Lemma A.3. If $\varphi^2 \neq \mathrm{Id}$, we then check that there exists an element $g' \in G^1$ such that the 2-adic valuation of the order of all eigenvalues of $\varphi(g')\varphi^2(g')f$ is different from $v_2(\ell-1)$. We make use of the fact that $\lambda = \pm 1$ is a square mod ℓ since exceptional subgroups only exist for $\ell \equiv 1 \pmod 4$.

To check if G^1 has (P2) we use the following algorithm.

- Let G^1 be one of the exceptional groups that arise from the classification in Theorem 3.2 with the condition $\ell \equiv m \pmod M$. The group G^1 is equipped with a character χ on a 4-dimensional vector space V.
- We list all pairs $(\tilde{G}, \tilde{\chi})$ such that $\tilde{G}$ is an (abstract) group containing a subgroup of index 2 isomorphic to G^1, and $\tilde{\chi}$ is a character such that $\tilde{\chi}_{|G^1} = \chi$.
- Given a pair $(\tilde{G}, \tilde{\chi})$, we check if there exists an element $g \in \tilde{G} \setminus G$ such that for each eigenvalue μ, the multiplicative order k of μ is such that $v_2(k) \leq \min\{v_2(m-1), v_2(M)\}$. Note that $v_2(\ell-1) \geq \min\{v_2(m-1), v_2(M)\}$.

□

Proposition A.8 *Let G be a maximal Hasse subgroup of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ with $\lambda(G) = \mathbb{F}_\ell^\times$. Then, $G^1 = G \cap \mathrm{Sp}_4(\mathbb{F}_\ell)$ is not an exceptional group.*

Proof Assume by contradiction that G^1 is exceptional. Note that G^{sat} is Hasse and $(G^{\mathrm{sat}})^1$ is exceptional. So, we just need to prove the proposition for $G = G^{\mathrm{sat}}$. By Lemma A.6, the group G^1 satisfies (P1) or (P2). If G has (P1), we conclude using Lemma A.4. If it has (P2), we conclude using Lemma A.5. □

Proof of Theorem A.1 Follows from Proposition A.8 and Lemma 5.4. □

References

1. Anni, S.: A local-global principle for isogenies of prime degree over number fields. J. Lond. Math. Soc. (2) **89**(3), 745–761 (2014)
2. Banwait, B.S.: Examples of abelian surfaces failing the local-global principle for isogenies. Res. Number Theory **7**(3), 55 (2021)
3. Banwait, B.S., Cremona, J.: Tetrahedral elliptic curves and the local-global principle for isogenies. Algebra Number Theory **8**(5), 1201–1229 (2014)
4. Bray, J.N., Holt, D.F., Roney-Dougal, C.M.: The Maximal Subgroups of the Low-Dimensional Finite Classical Groups. London Mathematical Society Lecture Note Series, vol. 407. Cambridge University Press, Cambridge (2013). (**With a foreword by Martin Liebeck**)
5. Chi, W.: On the Tate modules of absolutely simple abelian varieties of type II. Bull. Inst. Math. Acad. Sin. **18**, 85–95 (1990)

6. Cullinan, J.: Symplectic stabilizers with applications to abelian varieties. Int. J. Number Theory **8**(2), 321–334 (2012)
7. Dickson, L.E.: Linear groups: With an Exposition of the Galois Field Theory. B. G. Teubner, Stuttgart (1901)
8. Fité, F., Kedlaya, K.S., Rotger, V., Sutherland, A.V.: Sato–Tate distributions and Galois endomorphism modules in genus 2. Compos. Math. **148**(5), 1390–1442 (2012)
9. Grothendieck, A.: Modeles de Néron et monodromie. Sém. de Géom. 7, Exposé IX, Lecture Notes in Mathematics, vol. 288 (1971)
10. Grothendieck, A., Raynaud, M., Rim, D. S.: Groupes de monodromie en géométrie algébrique. I, Lecture Notes in Mathematics, vol. 288, Springer-Verlag, 1972, Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I)
11. Hindry, M., Ratazzi, N.: Points de torsion sur les variétés abéliennes de type GSp. J. Inst. Math. Jussieu **11**(1), 27–65 (2012)
12. Katz, N.M.: Galois properties of torsion points on abelian varieties. Invent. Math. **62**(3), 481–502 (1981)
13. Kiming, I.: Explicit classifications of some 2-extensions of a field of characteristic different from 2. Can. J. Math. **42**(5), 825–855 (1990)
14. Lombardo, D.: An explicit open image theorem for products of elliptic curves. J. Number Theory **168**, 386–412 (2016)
15. Lombardo, D.: Explicit surjectivity of Galois representations for abelian surfaces and GL_2-varieties. J. Algebra **460**, 26–59 (2016)
16. Lombardo, D.: On the ℓ-adic Galois representations attached to nonsimple abelian varieties. Ann. Inst. Fourier (Grenoble) **66**(3), 1217–1245 (2016)
17. Lombardo, D.: Galois representations attached to abelian varieties of CM type. Bull. Soc. Math. France **145**(3), 469–501 (2017)
18. Larson, E., Vaintrob, D.: 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**)
19. Lombardo, D., Verzobio, M.: Computations with Hasse subgroups. https://github.com/DavideLombardoMath/local-global-surfaces (2022)
20. Milne, J.S.: Abelian Varieties, Arithmetic Geometry (Storrs, Conn., 1984), pp. 103–150. Springer, New York (1986)
21. Odlyzko, A.M.: Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results. Sém. Théor. Nombres Bordeaux (2) **2**(1), 119–141 (1990)
22. Raynaud, M.: Schémas en groupes de type $(p, \ldots, p)$. Bull. Soc. Math. France **102**, 241–280 (1974)
23. Ribet, K.A.: Galois action on division points of abelian varieties with real multiplications. Am. J. Math. **98**(3), 751–804 (1976)
24. Ribet, K.A.: Hodge classes on certain types of abelian varieties. Am. J. Math. **105**, 523–538 (1983)
25. Rémond, G.: Conjectures uniformes sur les variétés abéliennes. Q. J. Math. **69**(2), 459–486 (2018)
26. Serre, J.-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. **15**(4), 259–331 (1972)
27. Serre, J.-P.: Représentations linéaires des groupes finis, 5th edn. Hermann, Paris (1998)
28. Serre, J.-P., Tate, J.: Good reduction of abelian varieties. Ann. Math. (2) **88**, 492–517 (1968)
29. Sutherland, A.V.: A local-global principle for rational isogenies of prime degree. J. Théor. Nr. Bordx. **24**(2), 475–485 (2012)
30. Silverberg, A., Zarhin, Y.G.: Inertia groups and abelian surfaces. J. Number Theory **110**(1), 178–198 (2005)
31. Vogt, I.: A local-global principle for isogenies of composite degree. Proc. Lond. Math. Soc. (3) **121**(6), 1496–1530 (2020)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.