Canad. J. Math. Vol. 74 (1), 2022 pp. 266–298
http://dx.doi.org/10.4153/S0008414X20000759


# Divisibility of torsion subgroups of abelian surfaces over number fields

John Cullinan and Jeffrey Yelton

*Abstract.* Let $A$ be a two-dimensional abelian variety defined over a number field $K$. Fix a prime number $\ell$ and suppose $\#A(\mathbf{F}_\mathfrak{p}) \equiv 0 \pmod{\ell^2}$ for a set of primes $\mathfrak{p} \subset \mathcal{O}_K$ of density 1. When $\ell = 2$ Serre has shown that there does not necessarily exist a $K$-isogenous $A'$ such that $\#A'(K)_{\text{tor}} \equiv 0 \pmod 4$. We extend those results to all odd $\ell$ and classify the abelian varieties that fail this divisibility principle for torsion in terms of the image of the mod-$\ell^2$ representation.

## 1 Introduction

### 1.1 Background

Let $A$ be an abelian variety defined over a number field $K$. If $\mathfrak{p}$ is a prime of good reduction for $A$ and $m$ is a positive integer, then we say that $A$ *locally has a subgroup of order* $m$ at $\mathfrak{p}$ if $\#A(\mathbf{F}_\mathfrak{p}) \equiv 0 \pmod m$. If $\mathfrak{p}$ has absolute ramification index $e_\mathfrak{p} < p - 1$, then by, [3, Appendix], the reduction-modulo- $\mathfrak{p}$ map is injective on torsion:

$$A(K)_{\text{tor}} \hookrightarrow A(\mathbf{F}_\mathfrak{p}).$$

It follows that if $A(K)$ has a subgroup of order $m$ then it locally has a subgroup of order $m$ for a set of primes $\mathfrak{p}$ of density 1. On the other hand, if $A$ locally has a subgroup of order $m$ for a set of primes of density 1, then it is not necessarily true that $A(K)$ has a global subgroup of order $m$. For example, the elliptic curve with LMFDB label 11.a1 [7] locally has a subgroup of order 5 for all $p \neq 11$, but has trivial Mordell–Weil group over $\mathbf{Q}$. Lang asked whether any abelian variety that locally has a subgroup of order $m$ for a set of primes of density 1 must be $K$-isogenous to one with a global subgroup of order $m$:

***Question 1*** (Lang) Let $A$ be an abelian variety defined over a number field $K$. Suppose that $m \mid \#A_\mathfrak{p}(\mathbf{F}_\mathfrak{p})$ for a set of primes $\mathfrak{p}$ of $K$ of density 1. Does there exist a $K$-isogenous $A'$ such that $m \mid \#A'(K)_{\text{tor}}$?

Note that if $m_1$ and $m_2$ are relatively prime integers and the answer to the above question is positive for a given abelian variety $A$, both when we take $m = m_1$ and when we take $m = m_2$, then the answer is positive for $A$ when we take $m = m_1 m_2$. It, therefore, suffices to consider the question only in the case that $m$ is a prime power.

Received by the editors January 18, 2020; revised October 11, 2020.
Published online on Cambridge Core October 28, 2020.
AMS subject classification: **11G10, 12R32, 20G25.**
Keywords: Abelian variety, torsion points, $\ell$-adic representation.

In [3], Katz showed that the answer to Question 1 is affirmative when $A$ is an elliptic curve, when $m$ is a prime number $\ell$, and when $A$ is an abelian surface. However, he showed by explicit construction that when $\dim A \geq 3$ and $m$ is odd, the answer is negative (the degree $[K : \mathbf{Q}]$ of the field $K$ of definition of $A$ may be very large). In [2], the first author considered the special case of $m = 2$ and showed that the answer to Question 1 is affirmative when $\dim A = 3$ and negative when $\dim A \geq 4$. While we expect the answer when $\dim A = 4$ and $m$ is a higher power of 2 to be negative as well, we do not pursue that question in this paper. More generally, it may be of interest to determine whether a negative answer to Question 1 for fixed $\dim A$ and modulus $\ell^n$ implies a negative answer for modulus $\ell^m$ when $m > n$.

On the other hand, among all moduli $m = \ell^n$ and among all positive integers $\dim A$, there are two main cases where the answer to Question 1 is unknown: the case $\dim A = 3$ and $m = 2^n$ $(n > 1)$, and the case $\dim A = 2$ and $m$ composite. In all of these cases where there is a negative answer, it would be interesting to construct explicit examples of such abelian varieties where the degree $[K : \mathbf{Q}]$ of the field of definition of $A$ is minimized. We refer to this as the *realization* problem and briefly address it at the end of this section.

Returning to the open cases of Question 1, we focus exclusively on the situation where $m$ is composite and $\dim A = 2$ in this paper. In an unpublished letter to Katz [11], Serre constructed a counterexample for the modulus 4—that is, he showed there exists an abelian surface $A$ that locally has a subgroup of order 4 for a set of primes of density 1 and no surface in the $K$-isogeny class of $A$ has a global subgroup of order 4. More precisely, Serre constructed an open subgroup $H$ of the symplectic similitude group $\mathrm{GSp}_4(\mathbf{Z}_2)$ such that any abelian surface whose 2-adic image equals $H$ is one where Question 1 has a negative answer. However, Serre's construction does not immediately generalize to odd, composite moduli. This is the starting point of our paper.

It is enough to answer Question 1 for prime-power moduli and in [3, Introduction], Katz shows that Question 1 is equivalent to Question 2 below (which in Katz's paper is [3, Problem 1 (bis)]). In order to state this equivalent version, we introduce some further notation. Write $m = \ell^n$ for a prime number $\ell$ and a positive integer $n$. Following Katz, we write $\mathrm{T}_\ell(A)$ for the $\ell$-adic Tate module of $A$ and $\rho_\ell : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(\mathrm{T}_\ell(A))$ for the associated $\ell$-adic representation of $A$. Now Question 1 is equivalent to the following.

***Question 2*** (Katz) Let $A$ be an abelian variety over a number $K$, $\ell$ a prime number, and $\rho_\ell : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(\mathrm{T}_\ell(A))$ its $\ell$-adic representation. Suppose we have

$$\det(\rho_\ell(\gamma) - 1) \equiv 0 \pmod{\ell^n} \qquad \text{for all } \gamma \in \mathrm{Gal}(\overline{K}/K).$$

Do there exist $\mathrm{Gal}(\overline{K}/K)$-stable lattices $\mathcal{L} \supset \mathcal{L}'$ in $\mathrm{T}_\ell(A)$ such that the quotient $\mathcal{L}/\mathcal{L}'$ has order $\ell^n$, and such that $\mathrm{Gal}(\overline{K}/K)$ acts trivially on $\mathcal{L}/\mathcal{L}'$?

Our main result is that the answer to Question 2 (and hence to Question 1) is *negative* for all moduli $\ell^2$ when $A$ is an abelian surface. Our argument is purely group-theoretic; in the following section, we develop our general group-theoretic set-up.

## 1.2 Restriction of the image

Before stating our main theorem, we give a more detailed overview of our approach in this subsection.

Let $\mathcal{T}$ be a free $\mathbf{Z}_\ell$-module of rank 4, which we equip with a nondegenerate alternating bilinear form

$$\langle\, , \,\rangle : \mathcal{T} \times \mathcal{T} \to \mathbf{Z}_\ell.$$

Two groups of invertible operators on $\mathcal{T}$ that concern us are the group of symplectic similitudes, defined as

$$\mathrm{GSp}(\mathcal{T}) := \{g \in \mathrm{Aut}(\mathcal{T}) \mid \langle g.v, g.w\rangle = m_g \langle v, w\rangle\},$$

for some $m_g \in \mathbf{Z}_\ell^\times$ depending on $g$, and the symplectic group, defined as

$$\mathrm{Sp}(\mathcal{T}) := \{g \in \mathrm{Aut}(\mathcal{T}) \mid \langle g.v, g.w\rangle = \langle v, w\rangle\} \subset \mathrm{GSp}(\mathcal{T}).$$

We may identify $\mathrm{GSp}(\mathcal{T})$ and $\mathrm{Sp}(\mathcal{T})$ with $\mathrm{GSp}_4(\mathbf{Z}_\ell)$ and $\mathrm{Sp}_4(\mathbf{Z}_\ell)$, respectively, by fixing a symplectic basis of $\mathrm{T}_\ell(A)$ (see Definition 2.1 below).

We will be particularly interested in subgroups of $\mathrm{Sp}(\mathcal{T})$ satisfying a certain determinant condition, motivating us to define

$$\mathrm{Fix}(\ell^n) := \{\text{subgroups } G \subset \mathrm{Sp}(\mathcal{T}) \mid \det(g-1) \equiv 0 \pmod{\ell^n} \text{ for all } g \in G\}.$$

***Remark 1.1*** Our motivation for the above notation is that a subgroup $G \subset \mathrm{Sp}_4(\mathcal{T})$ lies in $\mathrm{Fix}(\ell^n)$ for some $n$ if and only if $G$ fixes an order- $\ell^n$ submodule of $\mathcal{T}$ under the induced mod-$\ell^n$ action. Indeed, the latter condition is equivalent to saying that under this action, for each $g \in G$, the operator $g - 1 \in \mathrm{Sp}_4(\mathcal{T})$ kills a submodule of $(\mathcal{T}/\ell^n\mathcal{T})$ of order $\ell^n$. We may assume that the image of $g - 1$ modulo $\ell^n$ is a diagonal matrix in $\mathrm{End}(\mathcal{T}/\ell^n\mathcal{T})$ after performing a series of invertible row and column operations on it. It is then easy to see that in order for $g - 1$ to kill an order- $\ell^n$ submodule of $\mathcal{T}/\ell^n\mathcal{T}$, the product of its diagonal elements must be divisible by $\ell^n$, and so $\det(g - 1) \equiv 0 \pmod{\ell^n}$, which is the defining criterion for membership in $\mathrm{Fix}(\ell^n)$.

We will show that the hypothesis that $G \in \mathrm{Fix}(\ell^2)$ is so strong that, with only a few exceptions, it forces the existence of pairs of $G$-stable lattices of relative index $\ell^2$ with trivial $G$-action on the quotient. We will refer to these "exceptions" using the following terminology.

***Definition 1.1*** Given any free $\mathbf{Z}_\ell$-module $\mathcal{T}$ of rank 4, we call any $G \in \mathrm{Fix}(\ell^2)$ for which there do not exist $G$-stable lattices $\mathcal{L}' \subset \mathcal{L} \subset \mathcal{T}$ with $[\mathcal{L} : \mathcal{L}'] = \ell^2$ and trivial $G$-action on the quotient $\mathcal{L}/\mathcal{L}'$ a *counterexample*.

In the context of our investigation of Question 2, the $\mathbf{Z}_\ell$-module $\mathcal{T}$ is the $\ell$-adic Tate module $T_\ell(A)$ of an abelian variety $A$ over a number field $K$ for some prime $\ell$. After possibly replacing $A$ with an isogenous abelian variety, we assume that $A$ is principally polarized so that we may define the Weil pairing as a skew-symmetric form on $\mathrm{T}_\ell(A)$. It is well known that the Weil pairing $\langle\, , \,\rangle$ on $T_\ell(A)$ is equivariant with respect to the action of the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ on $\mathrm{T}_\ell(A)$. (See [8, §16] for more details on the Weil pairing.) The image of the natural $\ell$-adic Galois

https://doi.org/10.4153/S0008414X20000759 Published online by Cambridge University Press

representation $\rho_\ell : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(\mathrm{T}_\ell(A))$ is, therefore, contained in $\mathrm{GSp}(T_\ell(A))$. The following proposition explains our choice of the term "counterexample" in Definition 1.1 by showing that any counterexample $G$ in the sense of Definition 1.1 gives a counterexample for Question 2 (and hence to Question 1).

***Proposition 1.1*** *Let $G \in \mathrm{Fix}(\ell^2)$ be a counterexample in the sense of* Definition 1.1. *Then, there is an abelian surface $A$ over a number field $K$, which provides a counterexample for* Question 2 *such that, taking $\mathcal{T}$ to be $T_\ell(A)$, we have $\mathrm{im}(\rho_\ell) \cap \mathrm{Sp}(\mathcal{T}) = G$.*

**Proof** It is well known that for any prime $\ell$, there exists an abelian surface $A$ over $\mathbf{Q}$ such that the image of its natural $\ell$-adic Galois representation coincides with $\mathrm{GSp}(T_\ell(A))$. In fact, we quote the stronger result of [5, Theorem 1.3] that the image of the $\ell$-adic representation $\rho_\ell : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}(\mathrm{T}_\ell(A))$ of the hyperelliptic Jacobian defined by

$$y^2 = x^6 + 7471225x^5 + 16548721x^4 + 6639451x^3 + 16857421x^2 + 20754195x + 9508695$$

is maximal for all $\ell$.

Now, let $\Gamma'(\ell^2) \subset \mathrm{GSp}(\mathcal{T})$ be the subgroup consisting of all symplectic similitudes $g \in \mathrm{GSp}(\mathcal{T})$ such that $g \equiv 1 \pmod{\ell^2}$, and let $G' \subset \mathrm{GSp}(T_\ell(A))$ be the subgroup generated by $G$ and $\Gamma'(\ell^2)$. Let $K/\mathbf{Q}$ be the extension fixed by $\rho_\ell^{-1}(G')$; since $G'$ contains the finite-index subgroup $\Gamma'(\ell^2) \subset \mathrm{GSp}(T_\ell(A))$ and is, therefore, an open subgroup of $\mathrm{GSp}(T_\ell(A))$, the field extension $K/\mathbf{Q}$ is finite and so $K$ is a number field. Now, we consider $A$ as an abelian surface over $K$ and restrict $\rho_\ell$ to the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ of $K$; it is clear that we still have $\det(\rho_\ell(\gamma) - 1) \equiv 0 \pmod{\ell^2}$ for all $\gamma \in \mathrm{Gal}(\overline{K}/K)$. Meanwhile, since $G' \supset G$ and $G$ is a counterexample, there do not exist $\mathrm{Gal}(\overline{K}/K)$-stable lattices $\mathcal{L} \supset \mathcal{L}'$ in $\mathrm{T}_\ell(A)$ such that the quotient $\mathcal{L}/\mathcal{L}'$ has order $\ell^2$, and such that $\mathrm{Gal}(\overline{K}/K)$ acts trivially on $\mathcal{L}/\mathcal{L}'$, and we have, therefore, found a counterexample to Question 2 by taking $n = 2$. ■

By the discussion of [3, pp. 482–483], given an abelian surface $A$ arising from a counterexample $G \subset \mathrm{Sp}(\mathcal{T})$ via Proposition 1.1, after possibly replacing $A$ with an isogenous abelian surface, we may assume that its associated mod-$\ell$ Galois representation has a trivial one-dimensional subrepresentation. In fact, we will see from Proposition 2.1 below that this property implies that the semisimplification of the mod-$\ell$ reduction $\overline{G}$ of a counterexample $G$ always has at least two one-dimensional factors. We further distinguish between the following two cases: subgroups $G \subset \mathrm{Sp}(\mathcal{T})$ for which the semisimplification of the mod-$\ell$ reduction either

(1) has four one-dimensional factors, two of which are trivial, or
(2) has an irreducible two-dimensional factor and two trivial one-dimensional factors.

We remark that Serre's original counterexample for Question 2 in [11] had four one-dimensional factors and we will review this counterexample in Section 3 below.

Furthermore, we will only mainly consider subgroups $G$ of $\mathrm{Sp}(\mathcal{T})$ where the kernel of reduction modulo $\ell$ is as large as possible (to be made precise below). As we will see in Section 2.2, this assumption gives us a simple criterion for checking which lattices are $G$-stable and, therefore, whether there are any quotients of order $\ell^2$ with trivial $G$-action.

To summarize, in this paper, for the purpose of finding and classifying counterexamples, we will only consider subgroups $G \subset \mathrm{Sp}(\mathcal{T})$ such that

- $\overline{G}$ fixes a subspace of $\mathcal{T}/\ell\mathcal{T}$ of dimension 1; and
- the kernel of the natural projection $G$ to its reduction modulo $\ell$ is as large as possible; for us, this will mean $G$ contains the full kernel $\Gamma(\ell)$ of the reduction-mod-$\ell$ map from $\mathrm{Sp}(\mathcal{T})$ to $\mathrm{Sp}(\mathcal{T}/\ell\mathcal{T})$ or contains a certain index-$\ell$ subgroup of $\Gamma(\ell)$.

What we will show using group theory is that, even under these added hypotheses, counterexamples $G \in \mathrm{Fix}(\ell^2)$ do exist; more specifically, counterexamples satisfying property A exist for any $\ell$, and counterexamples satisfying property B exist when $\ell = 2$. This, in particular, implies a negative answer to Question 2.

## 1.3 Statement of the results

With this motivation and background in place, we now state our main results. For clarity of exposition, we only give the *maximal* counterexamples in this statement of the main theorem; while in the course of proving the results, we give the minimal requirements that a counterexample must meet.

***Theorem 1.2*** *Let $\ell$ be a prime number; let $\mathcal{T}$ be a free $\mathbf{Z}_\ell$-module of rank 4 equipped with a nondegenerate alternating pairing; and suppose $G \subset \mathrm{Sp}(\mathcal{T})$ satisfies*

(i) $\det(g-1) \equiv 0 \pmod{\ell^2}$ *for all $g \in G$, and*
(ii) *there do not exist $G$-stable lattices $\mathcal{L}' \subset \mathcal{L} \subset \mathcal{T}$ of relative index $\ell^2$ with trivial $G$-action on the quotient $\mathcal{L}/\mathcal{L}'$, and*
(iii) *$G$ is maximal among subgroups of $\mathrm{Sp}(\mathcal{T})$ satisfying (i) and (ii).*

*Then, one of the following holds.*

(a) *We have $\ell = 2$, the image of $G$ modulo 2 is isomorphic to $D_4 \times C_2$ or $S_3 \times C_2$, and we have $[\Gamma(2) : G \cap \Gamma(2)] = 2$. In the former case, the semisimplification of the mod-2 representation consists of four one-dimensional factors and in the latter it consists of two one-dimensional factors and a two-dimensional factor.*
(b) *We have $\ell = 2$, and $G$ is the full preimage in $\mathrm{Sp}(\mathcal{T})$ of a subgroup of $\mathrm{Sp}(\mathcal{T}/\ell\mathcal{T})$ isomorphic to $S_3$. In this case, the semisimplification of the mod-2 representation consists of two one-dimensional factors and a two-dimensional factor.*
(c) *We have $\ell \geq 3$, and $G$ is the full preimage in $\mathrm{Sp}(\mathcal{T})$ of a subgroup of $\mathrm{Sp}(\mathcal{T}/\ell\mathcal{T})$ of isomorphism type $\mathbf{Z}/\ell \rtimes (\mathbf{Z}/\ell)^\times$ or $\mathbf{Z}/\ell \times (\mathbf{Z}/\ell \rtimes (\mathbf{Z}/\ell)^\times)$. In this case, the semisimplification of the mod-$\ell$ representation consists of four one-dimensional factors.*

In the course of proving Theorem 1.2, we give explicit representations, including the dimensions of the factors in the semisimplifications, of all of the groups that occur. In Section 2.1, we give a more detailed exposition of how the group theoretic result of Theorem 1.2 implies the following corollary, answering Lang's original Question 1.

***Corollary 1.3*** *For all square moduli, the answer to* Question 2*, and hence to* Question 1*, is negative. In addition, when the modulus is 4, there are counterexamples to* Question 1 *realized by absolutely simple abelian surfaces.*

Our paper proceeds as follows. In Section 2, we review the relevant background on symplectic groups and representation theory, and we give an explicit description of the stable lattice structure. The classification of the maximal counterexamples then amounts to a group theory argument. We break this argument up over the ensuing three sections. In Section 3, we classify the counterexamples for which $G$ is contained in a maximal pro-$\ell$ subgroup of $\mathrm{Sp}(\mathcal{T})$; we show that counterexamples of this type exist when $\ell = 2$ and do not exist for $\ell \geq 3$. This is where we will recall Serre's original counterexample. Then, in Section 4 we classify the counterexamples for which $G$ lies in the Iwahori subgroup of $\mathrm{Sp}(\mathcal{T})$; this is where the semisimplification of the mod-$\ell$ representation consists of four one-dimensional factors. Finally, Section 5 is where we consider the case where the semisimplification of the mod-$\ell$ representation contains an irreducible two-dimensional factor. There we show that no such counterexamples exist when $\ell \geq 3$ and classify the ones that do when $\ell = 2$.

## 1.4 The realization problem

Our main theorem shows, from the point of view of group theory, that the answer to Question 1 is negative for abelian surfaces. A follow-up question, which we call the *realization problem*, is to construct abelian surfaces with these $\ell$-adic images. By the Galois-theoretic argument in the proof of Proposition 1.1, we can construct such an abelian surface $A$ over a number field $K$ with $[K : \mathbf{Q}]$ large. We, therefore, pose the following question.

***Question 3*** Fix a prime number $\ell$. What is the minimum degree $[K : \mathbf{Q}]$ such that there exists an abelian variety $A/K$ with $\ell$-adic Galois image equal to one of the groups in Theorem 1.2?

We do not pursue the realization problem in this paper, though we mention that the LMFDB's current database of over 68,000 genus-2 curves is a natural place to search for potential examples [1]. In particular, by sampling at a large number of primes, one can find examples of surfaces that have a local subgroup of (say) order $\ell^2$ but a global subgroup of order $\ell$. For example, the isogeny class 1270.a contains the hyperelliptic curve with label 1270.a.325120.1 . By sampling a large number of primes, this Jacobian experimentally has a subgroup of order 4 (but a global subgroup of order 2), and the 2-torsion field has Galois group $S_3 \times S_2$. Furthermore, the semisimplification of the mod-2 representation contains an irreducible two-dimensional factor and the Jacobian is absolutely simple over $\mathbf{Q}$.

In order to rigorously determine whether or not a Jacobian defines a counterexample, one would need to determine both the mod-$\ell$ and mod-$\ell^2$ images of the $\ell$-adic representation. A related question for future exploration would be to employ known estimates on the distribution of eigenvalues of Frobenius for genus-2 curves to determine how many primes one should sample to be "reasonably" certain (in a precise sense) that an isogeny class consists entirely of Jacobians with a local subgroup of order $\ell^2$.

https://doi.org/10.4153/S0008414X20000759 Published online by Cambridge University Press

### 1.5 Group theory notation

Given any prime $\ell$, suppose we have a free $\mathbf{Z}_\ell$-module $\mathcal{T}$ of rank 4 equipped with a nondegerate alternating pairing $\langle\ ,\ \rangle$. Throughout this paper, for any integer $n \geq 1$, we denote the kernel of the reduction-modulo- $\ell^n$ map from $\mathrm{Sp}(\mathcal{T})$ to $\mathrm{Sp}(\mathcal{T}/\ell^n\mathcal{T})$ by

$$\Gamma(\ell^n) := \{g \in \mathrm{Sp}(\mathcal{T}) \mid g \equiv 1 \pmod{\ell^n}\}.$$

The form $\langle\ ,\ \rangle$ induces a nondegenerate alternating pairing on $\mathcal{T}/\ell^n\mathcal{T}$ via reduction modulo $\ell^n$ for each $n \geq 1$. We have (surjective) homomorphisms $\pi_{\ell^n}$ : $\mathrm{Sp}(\mathcal{T}) \to \mathrm{Sp}(\mathcal{T}/\ell^n\mathcal{T})$ for all $n \geq 1$, as well as (surjective) homomorphisms $\pi_{\ell^n \to \ell^m}$ : $\mathrm{Sp}(\mathcal{T}/\ell^n\mathcal{T}) \to \mathrm{Sp}(\mathcal{T}/\ell^m\mathcal{T})$ for any integers $n > m \geq 1$.

We use both the notations, $C_n$ and $\mathbf{Z}/n$, for a cyclic group of order $n$ depending on whether we are emphasizing a multiplicative or additive group structure, respectively. The notations $S_n$ and $A_n$ refer to the symmetric and alternating groups on $n$ letters, respectively. We use $D_n$ to denote the dihedral group of order $2n$.

## 2 Symplectic groups

The basic definitions and background on symplectic groups are widely available in the literature: see [9] for a general development or [4] for concise definitions, especially for symplectic groups over general commutative rings. We will be content with a very brief overview here. Let $\ell$ be a prime number and $\mathcal{T}$ be a free rank-4 $\mathbf{Z}_\ell$-module equipped with a nondegenerate alternating bilinear form $\langle\ ,\ \rangle$ as in Section 1.2. Many of our explicit group-theoretic arguments are performed in coordinates and so we make the following formal definition.

***Definition 2.1*** A *symplectic* basis of $\mathcal{T}$ is an ordered basis $\{e_1, e_2, e_3, e_4\}$ that satisfies $\langle e_1, e_4\rangle = \langle e_2, e_3\rangle = 1$ and $\langle e_1, e_2\rangle = \langle e_1, e_3\rangle = \langle e_4, e_2\rangle = \langle e_4, e_3\rangle = 0$.

To ease notation, write

$$\overline{G} := \pi_\ell(G)$$

for any subgroup $G \subset \mathrm{Sp}(\mathcal{T})$; this reduction $\overline{G}$ acts naturally on the four-dimensional symplectic $\mathbf{F}_\ell$-vector space $\mathcal{T}/\ell\mathcal{T}$. Note that $\Gamma(\ell) \triangleleft \mathrm{Sp}(\mathcal{T})$ is the kernel of $\pi_\ell$. Some of the counterexamples $G$ of Theorem 1.2 are maximal in the sense that $\Gamma(\ell) \subset G$; such a subgroup $G$ can be described simply as the inverse image under $\pi_\ell$ of $\overline{G}$.

### 2.1 The mod-$\ell$ representation

We now determine the "shape" of $\overline{G}$, where $G \in \mathrm{Fix}(\ell^2)$ is a counterexample satisfying the assumptions given in Section 1.2.

***Proposition 2.1*** *Let $G \in \mathrm{Fix}(\ell^2)$ be a counterexample whose reduction $\overline{G}$ acts trivially on a one-dimensional subspace of $\mathcal{T}/\ell\mathcal{T}$. Then, with respect to the reduction of a suitable symplectic basis of $\mathcal{T}$, the elements of $\overline{G}$ are all matrices of the form*

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ * & * & * & 0 \\ * & * & * & 0 \\ * & * & * & 1 \end{pmatrix}. \tag{2.1}$$

https://doi.org/10.4153/S0008414X20000759 Published online by Cambridge University Press

**Proof** The statement amounts to asserting that there exists a $\overline{G}$-invariant subspace $\overline{W} \subset \mathcal{T}/\ell\mathcal{T}$ of dimension 3 such that $\overline{G}$ acts trivially on the quotient $(\mathcal{T}/\ell\mathcal{T})/\overline{W}$. We now construct a symplectic basis $\{e_1, e_2, e_3, e_4\}$ of $\mathcal{T}$ such that the reduction $\overline{e}_4 \in \mathcal{T}/\ell\mathcal{T}$ of $e_4$ generates the one-dimensional subspace, which is fixed by $\overline{G}$. Since the symplectic pairing is nondegenerate, there is an element $e_1 \in \mathcal{T}$ such that $\langle e_1, e_4 \rangle = 1$. Let $V$ be the span of $\{e_1, e_4\}$. Since the sum of the dimensions of any subspace of $\mathcal{T}$ and its orthogonal complement must equal the dimension of $\mathcal{T}$, we get that the orthogonal complement $V^\perp$ of $V$ has dimension 2. Now, clearly there is a nondegenerate symplectic pairing on $V/(V \cap V^\perp)$ induced by $\langle\, , \rangle$, so $V/(V \cap V^\perp)$ must have even dimension; since $\langle\, , \rangle$ is nontrivial on $V$, we must have $V^\perp \neq V$ and so $V \cap V^\perp = \{0\}$. Then, since $V \oplus V^\perp = \mathcal{T}$, the pairing $\langle\, , \rangle$ cannot be trivial on $V^\perp$, and any ordered basis $\{e_2, e_3\}$ satisfies $\langle e_2, e_3 \rangle = 1$ after appropriate scaling of one of the elements. Thus, we have an ordered set $\{e_1, e_2, e_3, e_4\}$, which is a symplectic basis of $\mathcal{T}$.

Now, let $W \subset \mathcal{T}$ be the span of $\{e_2, e_3, e_4\}$. It is clear that $W$ is the orthogonal complement of the subspace spanned by $e_4$. It now follows from the $G$-invariance of the symplectic pairing that since $\overline{G}$ fixes the element $\overline{e}_4$, the reduction $\overline{W}$ of $W$ is invariant under the action of $\overline{G}$. Note further that for any $g \in G$, we have $\langle g(e_1), g(e_4) \rangle = \langle e_1, e_4 \rangle = 1$. It follows that since $g(e_4) \equiv e_4 \pmod{\ell}$, we have $\langle g(e_1), e_4 \rangle \equiv 1 \pmod{\ell}$ and therefore $g(e_1) \equiv e_1 + w \pmod{\ell}$ for some $w \in W$. Since $\overline{W}$ and the image of $\overline{e}_1$ modulo $\ell$ generate $\mathcal{T}/\ell\mathcal{T}$, we get the desired statement. ∎

Given any counterexample $G \in \mathrm{Fix}(\ell^2)$ satisfying the hypothesis of the above proposition, we fix a symplectic basis $\{e_1, e_2, e_3, e_4\}$ of $\mathcal{T}$ such that, with respect to its reduction modulo $\ell$ (which we denote by $\{\overline{e}_1, \overline{e}_2, \overline{e}_3, \overline{e}_4\}$ and which is a basis of $\mathcal{T}/\ell\mathcal{T}$), the elements of the group $\overline{G}$ are matrices of the form given in (2.1). (Note that since $G \subset \mathrm{Sp}(\mathcal{T})$, there are additional constraints placed on the off-diagonal entries by $\langle\, , \rangle$.)

In order to classify possible counterexamples $G \in \mathrm{Fix}(\ell^2)$, we will now introduce three subgroups $\mathrm{S}_\ell \subset \mathrm{B}_\ell \subset \mathrm{P}_\ell \subset \mathrm{Sp}(\mathcal{T})$. We first define $\mathrm{P}_\ell$ to be the subgroup of matrices whose reductions modulo $\ell$ are of the lower block-triangular form given in (2.1). According to Proposition 2.1 above, any counterexample $G \in \mathrm{Fix}(\ell^2)$ is conjugate, in $\mathrm{Sp}(\mathcal{T})$, to a subgroup of $\mathrm{P}_\ell$.

For any element of $\mathrm{P}_\ell$, we highlight the off-diagonal lower entries in the matrix form of its reduction modulo $\ell$ as

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ \alpha & * & * & 0 \\ \beta & \gamma & * & 0 \\ \delta & \beta' & \alpha' & 1 \end{pmatrix}, \tag{2.2}$$

and we let $\alpha, \alpha', \beta, \beta', \gamma, \delta : \mathrm{P}_\ell \to \mathbf{Z}/\ell$ be the maps given by taking an element $g \in \mathrm{P}_\ell$ to the corresponding entries of $\pi_\ell(g)$ shown in (2.2). (These maps are not homomorphisms in general.) Noting from (2.2) that the (1,4) entry $g_{1,4}$ of any element $g \in \mathrm{P}_\ell$ is divisible by $\ell$, we also define a map

$$f : \mathrm{P}_\ell \to \mathbf{Z}/\ell, \quad g \mapsto \pi_\ell(g_{1,4}/\ell).$$

It is easy to verify that this map $f$ is a homomorphism.

https://doi.org/10.4153/S0008414X20000759 Published online by Cambridge University Press

The *Iwahori subgroup* $\mathrm{B}_\ell \subset \mathrm{Sp}(\mathcal{T})$ is the subgroup consisting of all matrices whose reduction modulo $\ell$ is lower-triangular. We write $\mathrm{S}_\ell \subset \mathrm{B}_\ell$ for the (maximal pro-$\ell$-) *Sylow subgroup* of $\mathrm{B}_\ell$; it is the subgroup of $\mathrm{B}_\ell$ consisting of those triangular matrices whose reduction modulo $\ell$ has all 1's along the diagonal. Given a group $G \in \mathrm{Fix}(\ell)$, we write $G \subset \mathrm{B}_\ell$ (resp. $G \subset \mathrm{S}_\ell$) if there is a basis $\{e_1, e_2, e_3, e_4\}$ with the properties given above with respect to which $G$ is contained in $\mathrm{B}_\ell$ (resp. $\mathrm{S}_\ell$). With respect to this chosen basis, a calculation with $\langle\, ,\, \rangle$ shows that if we let $\varepsilon : \mathrm{B}_\ell \to (\mathbf{Z}/\ell)^\times$ be the map taking an element $g \in \mathrm{B}_\ell$ to the $(2,2)$ entry of $\pi_\ell(g)$, the $(3,3)$ entry of $\pi_\ell(g)$ is given by $1/\varepsilon(g)$, and that we have the formulas below:

$$\begin{aligned} \alpha'(g) &= -\alpha(g)/\varepsilon(g) \\ \beta'(g) &= \beta(g)\varepsilon(g) - \alpha(g)\gamma(g). \end{aligned} \tag{2.3}$$

We note that the map $\varepsilon : \mathrm{B}_\ell \to (\mathbf{Z}/\ell)^\times$ is a homomorphism whose kernel coincides with $\mathrm{S}_\ell$. For any $g \in \mathrm{B}_\ell$, the determinant $\det(g-1)$ satisfies

$$\det(g-1) \equiv \left(\gamma(g)\alpha(g)^2 + \frac{\beta(g)\alpha(g)(1-\varepsilon(g)^2)}{\varepsilon(g)} + \frac{\delta(g)(1-\varepsilon(g))^2}{\varepsilon(g)}\right) f(g)\ell \pmod{\ell^2}. \tag{2.4}$$

We further note that when we restrict to $\mathrm{S}_\ell$, the maps $\alpha, \beta : \mathrm{S}_\ell \to \mathbf{Z}/\ell$ become homomorphisms, and we get the simplified formulas from (2.3) below:

$$\begin{aligned} \alpha'(g) &= -\alpha(g) \\ \beta'(g) &= \beta(g) - \alpha(g)\gamma(g). \end{aligned} \tag{2.5}$$

In this special case, the determinant formula (2.4) simplifies to

$$\det(g-1) \equiv \alpha(g)^2\gamma(g)f(g)\ell \pmod{\ell^2}. \tag{2.6}$$

## 2.2 Lattices

As we see from the conditions given in Question 2, in order to determine whether a given group $G \in \mathrm{Sp}(\mathcal{T})$ is a counterexample, it is crucial to understand the stable lattice structure of $\mathcal{T}$ under the action of $G$. The following proposition will allow us to essentially work with the mod-$\ell$ representation and search for pairs of stable subspaces of $\mathcal{T}/\ell\mathcal{T}$ whose quotients admit trivial $G$-action rather than search through all sublattices of $\mathcal{T}$.

***Proposition 2.2*** *Assume that $G \in \mathrm{Fix}(\ell^2)$ contains $\Gamma(\ell) \cap \ker(f)$ and that $f$ is not trivial on $G$. Let $\mathcal{L} \subset \mathcal{T}$ be a $G$-stable lattice. Then, we have $\mathcal{L} \subset \ell\mathcal{T}$ or $\mathcal{L} \supset \ell\mathcal{T}$.*

In order to prove the above proposition, we first need a lemma.

***Lemma 2.1*** *Choose a vector $v \in \mathcal{T}\backslash\ell\mathcal{T}$.*

a) *For any integer $n \geq 1$, the orbit of $v$ under the action of the subgroup $\Gamma(\ell^n) \subset \mathrm{Sp}(\mathcal{T})$ coincides with the coset $v + \ell^n\mathcal{T}$.*

https://doi.org/10.4153/S0008414X20000759 Published online by Cambridge University Press

b) *Let $W \subset \mathcal{T}$ be the submodule consisting of vectors $w$ such that $\langle w, e_4\rangle \in \ell\mathbf{Z}_\ell$. The orbit of $v$ under the action of the subgroup $\Gamma(\ell) \cap \ker(f) \subset \mathrm{Sp}(\mathcal{T})$ coincides with the coset $v + W$ (resp. $v + \ell\mathcal{T}$) if $v$ is (resp. is not) a (unit) scalar multiple of $e_4 \in \mathcal{T}$.*

**Proof** In order to prove part (a), we first show that for any integer $m \geq 1$, the orbit of any vector $v \in \mathcal{T}/\ell^{m+1}\mathcal{T}$ under the action of the subgroup $\Gamma(\ell^m)/\Gamma(\ell^{m+1}) \subset \mathrm{Sp}(\mathcal{T}/\ell^{m+1}\mathcal{T})$ consists of all vectors $v' \in \mathcal{T}/\ell^{m+1}\mathcal{T}$ equivalent to $v$ modulo $\ell^m$. (Below we abuse notation slightly and write $\langle\ ,\ \rangle$ for the pairing on $\mathcal{T}/\ell^{m+1}\mathcal{T}$ induced by reducing the symplectic pairing on $\mathcal{T}$ modulo $\ell^{m+1}$; it takes values in $\mathbf{Z}/\ell^{m+1}$.) In order to do this, we define, for any vector $u \in \mathcal{T}/\ell^{m+1}\mathcal{T}$, the (unipotent) operator $T_u \in \Gamma(\ell^m)/\Gamma(\ell^{m+1})$ given by $w \mapsto w + \ell^m\langle w, u\rangle u$ for $w \in \mathcal{T}/\ell^{m+1}\mathcal{T}$. Now choose $a \in (\mathcal{T}\backslash\ell\mathcal{T})/\ell^{m+1}\mathcal{T}$; we proceed to show that $v + \ell^m a$ lies in the orbit of $v$ under $\Gamma(\ell^m)/\Gamma(\ell^{m+1})$. First assume that $\langle v, a\rangle \not\equiv 0 \pmod{\ell}$. In this case, we clearly have $T_u^{\langle v,a\rangle^{-1}}(v) = v + \ell^m a$ and we are done. Now assume that $\langle v, a\rangle \equiv 0 \pmod{\ell}$. Then, one sees from a simple dimension-counting argument that there is a vector $b \in (\mathcal{T}\backslash\ell\mathcal{T})/\ell^{m+1}\mathcal{T}$ satisfying $\langle v, b\rangle \equiv 1 \pmod{\ell}$ and $\langle b, a\rangle \not\equiv 0 \pmod{\ell}$. Now, we compute $(T_{a+b}^{\langle b,a\rangle^{-1}} T_b^{-1})(v) = v + \ell^m a$, and we are done proving our claim about the orbit of $v$ under $\Gamma(\ell^m)$ modulo $\ell^{m+1}$.

Now, we fix $n \geq 1$ and claim that for any $n' > n \geq 1$ the orbit of any $v \in \mathcal{T}/\ell^{n'}\mathcal{T}$ under the action of the subgroup $\Gamma(\ell^n)/\Gamma(\ell^{n'}) \subset \mathrm{Sp}(\mathcal{T}/\ell^{n'}\mathcal{T})$ consists of all vectors $v' \in \mathcal{T}/\ell^{n'}\mathcal{T}$ equivalent to $v$ modulo $\ell^{n'}$. We prove this claim by performing induction on $n'$, noting that we get the $n' = n + 1$ case by applying the statement we proved in the last paragraph with $m = n$. Now, if our claim is true for a particular $n' > n$, we see that it holds for $n' + 1$ as well: indeed, for any vectors $v, w \in \mathcal{T}/\ell^{n'+1}\mathcal{T}$ with $v \equiv w \pmod{\ell^{n'}}$, the inductive assumption provides an operator $g \in \Gamma(\ell^n)/\Gamma(\ell^{n'+1})$, which takes $v$ to some $w'$, which is equivalent to $w$ modulo $\ell^{n'}$; then by applying the statement, we proved in the last paragraph with $m = n'$ we get an operator $h \in \Gamma(\ell^{n'})/\Gamma(\ell^{n'+1}) \subset \Gamma(\ell^n)/\Gamma(\ell^{n'+1})$ that takes $w'$ to $w$. Therefore, $w$ is in the orbit of $v$ under the action of $\Gamma(\ell^n)/\Gamma(\ell^{n'+1})$, and our claim is proved. Now, by moving to the inverse limit of the groups $\Gamma(\ell^n)/\Gamma(\ell^{n'})$ and the modules $\mathcal{T}/\ell^{n'}\mathcal{T}$, we get the statement of part (a).

Now, by applying part (a) for $n = 2$, it is clear that in order to prove part (b), it suffices only to consider the orbit of a vector $v \in (\mathcal{T}\backslash\ell\mathcal{T})/\ell^2\mathcal{T}$ under the action of the subgroup $(\Gamma(\ell) \cap \ker(f))/\Gamma(\ell^2)$. First, assume that $v$ is (the image modulo $\ell^2$ of) a scalar multiple of $e_4$. Then, it follows immediately from the definition of $f$ that an operator $T \in \Gamma(\ell)/\Gamma(\ell^2)$ lies in $\ker(f)/\Gamma(\ell^2)$ if and only if $\langle v, T(v)\rangle = \langle v, T(v) - v\rangle = 0$, or equivalently, if $T(v) = v + \ell w$ for some $w \in W$, whence the first statement of (b). Now, assume that $v$ is not (the image modulo $\ell^2$ of) a scalar multiple of $e_4$. Then, there exists a vector $b \in (\mathcal{T}\backslash\ell\mathcal{T})/\ell^{n+1}\mathcal{T}$ satisfying $\langle e_4, b\rangle \not\equiv 0 \pmod{\ell}$ and $\langle v, b\rangle \equiv 0 \pmod{\ell}$; the first condition implies that $T_b \notin (\Gamma(\ell) \cap \ker(f))/\Gamma(\ell^2)$, while the second condition implies that $T_b$ fixes $v$. We know from part (a) that there exists an operator $T \in \Gamma(\ell)/\Gamma(\ell^2)$ such that $T(v) = v + \ell a$ for any given vector $a \in (\mathcal{T}\backslash\ell\mathcal{T})/\ell^2\mathcal{T}$. Since $\Gamma(\ell)/\Gamma(\ell^2)$ is cyclically generated over $(\Gamma(\ell) \cap \ker(f))/\Gamma(\ell^2)$, the operator $TT_b^m$ lies in $(\Gamma(\ell) \cap \ker(f))/\Gamma(\ell^2)$; the second claim of part (b) follows from the fact that $(TT_b^m)(v) = T(v) = v + \ell a$. ∎

https://doi.org/10.4153/S0008414X20000759 Published online by Cambridge University Press

**Proof of Proposition 2.2** We assume that $\mathcal{L} \not\subset \ell\mathcal{T}$ and proceed to show that $\mathcal{L}$ must contain $\ell\mathcal{T}$. Choose a vector $v \in \mathcal{L}\backslash\ell\mathcal{T}$. Since we have $\Gamma(\ell) \cap \ker(f) \subset G$ by hypothesis, we may apply Lemma 2.1(b) to get that $v + W \subset \mathcal{L}$ (resp. $v + \ell\mathcal{T} \subset \mathcal{L}$) if $v$ is (resp. is not) a scalar multiple of $e_4$, where $W \subset \mathcal{T}$ is as defined in the statement of the lemma. Since $\mathcal{L}$ is closed under addition, we immediately get $\mathcal{L} \supset \ell W$ (resp. $\mathcal{L} \supset \ell\mathcal{T}$, in which case we are done). Now, suppose that we are in the former case; we assume without loss of generality that $v = e_4$. Since $f$ is nontrivial on $G$, we may choose some element $y \in G\backslash\ker(f)$. As $G$ has the block-upper-triangular structure described above, we have that $y(e_4) - e_4 \in \ell\mathcal{T}$; the fact that $f(y) \neq 0$ then implies that we have $y(e_4) - e_4 \in \ell\mathcal{T}\backslash W$. Since $\mathcal{T}$ is generated over $W$ by any element in $\mathcal{T}\backslash W$, we get the desired inclusion $\mathcal{L} \supset \ell\mathcal{T}$. ∎

Let $G$ be a group in $\mathrm{Fix}(\ell^2)$, and for $0 \leq i \leq 3$, define the sublattice

$$L_i := \mathrm{span}_{\mathbf{Z}_\ell}\{\ell e_1, \dots, \ell e_i, e_{i+1}, \dots, e_4\} \subset \mathcal{T}. \tag{2.7}$$

The following proposition will be useful below for determining whether a given $G \in \mathrm{Fix}(\ell^2)$ is a counterexample or not.

***Proposition 2.3***

a) *The sublattices $L_1$ and $L_3$ are always $G$-stable. Moreover, the quotient $L_3/\ell L_1$ is fixed under the induced $G$-action if and only if the homomorphism $f : G \to \mathbf{Z}/\ell$ is trivial. Thus, if $G$ is a counterexample, then $f$ is nontrivial on $G$.*

b) *If we have $G \subset \mathrm{B}_\ell$, then $L_2$ is also a $G$-invariant sublattice. Suppose further that we have $G \subset \mathrm{S}_\ell$. Then, the quotient $L_1/L_3$ (resp. the quotients $L_0/L_2$ and $L_2/\ell L_0$) is fixed under the induced $G$-action if and only if the homomorphism $\gamma : G \to \mathbf{Z}/\ell$ (resp. $\alpha : G \to \mathbf{Z}/\ell$) is trivial. Thus, if $G \subset \mathrm{S}_\ell$ is a counterexample, then both $\alpha$ and $\gamma$ are nontrivial on $G$.*

c) *In order to verify that $G$ is a counterexample, it suffices to verify that for any $G$-invariant sublattices $\mathcal{L}' \subset \mathcal{L} \subset \mathcal{T}$ both containing $\ell\mathcal{T}$ and with quotient of order $\ell^2$, the induced action of $G$ on the quotients $\mathcal{L}/\mathcal{L}'$ and $\mathcal{L}'/\ell\mathcal{L}$ is not trivial.*

**Proof** The statements of parts (a) and (b) can be verified straightforwardly from the discussion and definitions in Section 2.1.

We proceed to prove part (c). Choose any group $G \in \mathrm{Fix}(\ell^2)$ such that there exist $G$-invariant lattices $\mathcal{M}' \subset \mathcal{M} \subset \mathcal{T}$ whose quotient $\mathcal{M}/\mathcal{M}'$ has order $\ell^2$ and is fixed under the induced action by $G$. If we have $\mathcal{M} \subset \ell\mathcal{T}$, then we may replace $\mathcal{M}$ and $\mathcal{M}'$ with $1/\ell\mathcal{M}$ and $1/\ell\mathcal{M}'$, respectively, without changing the induced action of $G$ on their quotient. We, therefore, assume that $\mathcal{M} \not\subset \ell\mathcal{T}$, which by part (a) combined with Proposition 2.2 implies that $\mathcal{M} \supsetneq \ell\mathcal{T}$. If we also have $\mathcal{M}' \not\subset \ell\mathcal{T}$, then we similarly get $\mathcal{M}' \supsetneq \ell\mathcal{T}$. In this case, we let $\mathcal{L} = \mathcal{M}$ and $\mathcal{L}' = \mathcal{M}'$, and we are done.

Now, assume that $\mathcal{M}' \subset \ell\mathcal{T}$. Then, it follows from considering the order of the quotient $\mathcal{M}/\mathcal{M}'$ that we certainly have $\mathcal{M}' \not\subset \ell^2\mathcal{T}$, implying that $1/\ell\mathcal{M}' \not\subset \ell\mathcal{T}$. Now, by part (a) combined with Proposition 2.2, this implies that $1/\ell\mathcal{M}' \supsetneq \ell\mathcal{T}$ and so we have the inclusions $\ell^2\mathcal{T} \subsetneq \mathcal{M}' \subset \ell\mathcal{T}$. Suppose that $\mathcal{M}/\mathcal{M}' \cong \mathbf{Z}/\ell^2$, so that there exists an element $v \in \mathcal{M}\backslash\ell\mathcal{T}$ whose image modulo $\mathcal{M}'$ generates $\mathcal{M}/\mathcal{M}'$. If $v \equiv e_4 \pmod{\ell}$, then one verifies directly from the definition of $f$ that since $v$ is fixed modulo $\mathcal{M}'$ by $G$, the homomorphism $f$ must be trivial on $G$; then by part (a) we may take $\mathcal{L} = L_3$

https://doi.org/10.4153/S0008414X20000759 Published online by Cambridge University Press

and $\mathcal{L}' = \ell L_1$ and we are done. If, on the other hand, we have $v \not\equiv e_4 \pmod{\ell}$, we may take $\mathcal{L}$ to be generated by $\ell\mathcal{T}$ and the elements $v$ and $e_4$; it is immediate to check that $G$ acts trivially on $\mathcal{L}/\mathcal{L}'$ and again we are done. Now finally, suppose that $\mathcal{M}/\mathcal{M}' \cong \mathbf{Z}/\ell \oplus \mathbf{Z}/\ell$. In this case, we clearly have $\mathcal{M} \subset 1/\ell\mathcal{M}' \subset \mathcal{T}$ and can, therefore, take $\mathcal{L} = \mathcal{M}'$ and $\mathcal{L}' = 1/\ell\mathcal{M}$, finishing the proof of part (c). ∎

The following lemma will be useful in both Section 3 and Section 4.

***Lemma 2.2*** *Let $G$ be any subgroup of $\mathrm{B}_\ell$ such that the homomorphisms $\alpha$ and $\gamma$ are nontrivial on $G$. Then, the only proper $G$-stable sublattices of $\mathcal{T}$, which properly contain $\ell\mathcal{T}$ are $L_0$, $L_1$, $L_2$, $L_3$, where the sublattices $L_i$ are as in (2.7). Moreover, if $G \in \mathrm{Fix}(\ell^2)$ and the homomorphism $f$ is also trivial on $G$, then $G$ is a counterexample.*

**Proof** For $i = 0, 1, 2, 3$, we write $\overline{e}_i \in \mathcal{T}/\ell\mathcal{T}$ for the reduction modulo $\ell$ of $e_i \in \mathcal{T}$ and $\overline{L}_i \subset \mathcal{T}/\ell\mathcal{T}$ for the $\overline{G}$-invariant subspace given by $L_i/\ell\mathcal{T}$, so that $\overline{L}_i = \langle \overline{e}_{i+1}, \dots, \overline{e}_4 \rangle$. The first statement of the lemma is equivalent to saying that the only nontrivial $\overline{G}$-invariant subspaces of $\mathcal{T}/\ell\mathcal{T}$ are the $\overline{L}_i$'s. We prove this by showing that for $i = 0, 1, 2$, given a vector $v \in \overline{L}_i \backslash \overline{L}_{i+1}$, the minimal $\overline{G}$-invariant subspace containing $v$ is $\overline{L}_i$. We start by choosing $v \in \overline{L}_2 \backslash \overline{L}_3$; on choosing some $g \in G \backslash \ker(\alpha)$, we get that $\varepsilon(g)^{-1}v - \pi_\ell(g).v \in \langle \overline{e}_4 \rangle = \overline{L}_3$. Any $\overline{G}$-invariant subspace containing $v$ therefore contains the subspace generated by $\overline{L}_3$ and $v$, which coincides with $\overline{L}_2$. We have thus proved that the minimal $\overline{G}$-invariant subspace containing $v$ is $\overline{L}_2$. We now show that for $v \in \overline{L}_1 \backslash \overline{L}_2$, the minimal $\overline{G}$-invariant subspace containing $v$ is $\overline{L}_1$, using a similar argument where this time we choose some $g \in G \backslash \ker(\gamma)$ and take $\varepsilon(g)v - \pi_\ell(g).v$. Finally we show that for $v \in \overline{L}_0 \backslash \overline{L}_1$, the minimal $\overline{G}$-invariant subspace containing $v$ coincides with $\overline{L}_0$ in the same way, this time choosing some $g \in G \backslash \ker(\alpha)$ and taking $v - \pi_\ell(g).v$.

The second statement now follows easily by applying all three parts of Proposition 2.3. ∎

## 3 The Sylow subgroup $\mathrm{S}_\ell$

In this section, we consider subgroups $G \subset \mathrm{S}_\ell$ that belong to $\mathrm{Fix}(\ell^2)$. Throughout this section, by fixing an appropriate symplectic basis of our free rank-4 $\mathbf{Z}_\ell$-module $\mathcal{T}$, we identify $\mathrm{S}_\ell$ with the subgroup of $\mathrm{Sp}_4(\mathbf{Z}_\ell)$ whose reduction modulo $\ell$ consists of lower-triangular matrices with only 1's on the diagonal.

We have two main results: that there are no counterexamples when $\ell \geq 3$, and that there exist counterexamples when $\ell = 2$.

***Theorem 3.1*** *Suppose $G \subset \mathrm{S}_\ell$ with $G \in \mathrm{Fix}(\ell^2)$.*

a) *If $\ell \geq 3$, then one of $\alpha$, $\gamma$, or $f$ is trivial on $G$, i.e., there are no counterexamples when $\ell \geq 3$ and $G \subset \mathrm{S}_\ell$.*
b) *Let $G \subset \mathrm{S}_2$ be a counterexample. Then, we have either $\overline{G} = \overline{\mathrm{S}}_2 \cong C_2 \times D_4$ or $\overline{G} \cong D_4$. In either case, for any $H \subset \Gamma(2) \cap \ker(f)$, the subgroup of $\mathrm{Sp}_4(\mathcal{T})$ generated by $G$ and $H$ is also a counterexample. In particular, if $G$ is a maximal counterexample, then we have $\overline{G} = D_4 \times C_2$ and $G \cap \Gamma(2) = \Gamma(2) \cap \ker(f)$.*

*Moreover, there do exist counterexamples satisfying $\overline{G} = \overline{\mathrm{S}}_2$ and counterexamples satisfying $\overline{G} = D$ for any subgroup $D \subset \overline{\mathrm{S}}_2$ isomorphic to $D_4$.*

https://doi.org/10.4153/S0008414X20000759 Published online by Cambridge University Press

Because of the difference in techniques of the two cases of Theorem 3.1, we separate our argument into multiple subsections. We begin with a short description of the structure of $\overline{\mathrm{S}}_\ell \subset \mathrm{Sp}_4(\mathbf{Z}/\ell)$ that we will use extensively throughout this section.

### 3.1 The structure of $\mathrm{S}_\ell$

Let $\mathrm{S}_\ell$ be the $\ell$-Sylow subgroup of $\mathrm{B}_\ell$ and $\overline{\mathrm{S}}_\ell$ the $\ell$-Sylow subgroup of $\overline{\mathrm{B}}_\ell$. We define the following four elements of $\overline{\mathrm{S}}_\ell$ that we will use extensively in the rest of the paper:

$$x_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{pmatrix} \quad x_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$
$$x_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \quad x_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

The group $\overline{\mathrm{S}}_\ell$ is nonabelian of order $\ell^4$ and the following facts are easily verified to hold for all $\ell$. It is straightforward to compute directly that the order-$\ell$ elements $x_2, x_3, x_4$ commute and so $\langle x_2, x_3, x_4 \rangle$ defines an elementary abelian subgroup of $\overline{\mathrm{S}}_\ell$ of order $\ell^3$. We also have the commutation relations

$$[x_1, x_2] = x_3^{-1} x_4^{-1}$$
$$[x_1, x_3] = x_4^{-2},$$

which show that $x_1 \notin \langle x_2, x_3, x_4 \rangle$ because it does not commute with $x_2$ or $x_3$. Therefore, $\langle x_1, x_2, x_3, x_4 \rangle = \overline{\mathrm{S}}_\ell$ since it must have maximal order $\ell^4$. It is then a calculation to see that the element $x_4$ lies in the center of $\overline{\mathrm{S}}_\ell$. By the commutation relations, the center of $\overline{\mathrm{S}}_\ell$ is $\langle x_4 \rangle$, while the center of $\overline{\mathrm{S}}_2$ is $\langle x_3, x_4 \rangle$. We can simplify the generating set even more: when $\ell$ is odd we have $\overline{\mathrm{S}}_\ell = \langle x_1, x_2 \rangle$, while $\overline{\mathrm{S}}_2 = \langle x_1, x_2, x_4 \rangle$.

For $\ell \geq 5$, $\overline{\mathrm{S}}_\ell$ has exponent $\ell$, while for $\ell \in \{2, 3\}$ $\overline{\mathrm{S}}_\ell$ has exponent $\ell^2$ (this is a special case of a general fact about the Sylow subgroups of classical groups in defining characteristic [12, Corollary 0.5]). In these two special cases, the $\ell$-Sylow subgroups have isomorphism type $\overline{\mathrm{S}}_2 \simeq C_2 \times D_4$ and $\overline{\mathrm{S}}_3 \simeq C_3 \wr C_3$ (the wreath product of $C_3$ and $C_3$ with respect to a nontrivial permutation action). We now seek an explicit description of the subgroups of $\overline{\mathrm{S}}_\ell$ of order $\ell^3$, which will be used in the proof of Proposition 3.1.

To make the notation less cumbersome in the next lemma, we define the homomorphisms

$$\overline{\alpha}, \overline{\gamma} : \overline{\mathrm{S}}_\ell \to \mathbf{Z}/\ell$$

to be the ones induced by factoring $\alpha$ and $\gamma$, respectively, through $\pi_\ell|_{\mathrm{S}_\ell} : \mathrm{S}_\ell \to \overline{\mathrm{S}}_\ell$; i.e., given an element $g \in \overline{\mathrm{S}}_\ell$, the images $\overline{\alpha}(g)$ and $\overline{\gamma}(g)$ are its $(2,1)$-entry and its $(3,2)$-entry, respectively.

https://doi.org/10.4153/S0008414X20000759 Published online by Cambridge University Press

***Lemma 3.2*** *Let $\ell$ be an odd prime. There are exactly $\ell$ nonabelian subgroups of $\overline{\mathrm{S}}_\ell$ of order $\ell^3$, and these are given explicitly by*

$$\langle x_1 x_2^k, x_3 \rangle_{k=0,\ldots,\ell-1}. \tag{3.1}$$

**Proof** It is routine to verify that the groups $\langle x_1 x_2^k, x_3\rangle_{k=0,\ldots,\ell-1}$ are distinct, nonabelian, and of order $\ell^3$. In addition, observe that $\langle x_2, x_3, x_4\rangle$ coincides with the kernel of $\overline{\alpha}$ and is the unique abelian subgroup of $\overline{\mathrm{S}}_\ell$ of order $\ell^3$. Therefore, if $H \subset \overline{\mathrm{S}}_\ell$ is a nonabelian subgroup of order $\ell^3$, then $\overline{\alpha}(H) \neq 0$.

Because $H$ is an $\ell$-group, it has nontrivial center. Let $h \in H$ be such that $\overline{\alpha}(h) \neq 0$. Then, $h$ only commutes with powers of $x_4$. Thus, $H$ contains $\langle x_4\rangle$. Since $h$ and $x_4$ each have order $\ell$ and commute, we have $\langle h, x_4\rangle \simeq C_\ell^2$, hence $H$ contains another element $g$ so that $H = \langle g, h, x_4\rangle$. Since $H$ is nonabelian we must have $H = \langle g, h\rangle$ since otherwise $\langle g, h\rangle \simeq C_\ell^2$ and then $H$ would be elementary abelian.

Next, observe that $H \cap \langle x_2, x_3, x_4\rangle$ has order $\ell^2$. Since $\langle x_4\rangle \subset H$, it must be the case that $H$ contains a subgroup $K$ of $\langle x_2, x_3\rangle$ of order $\ell$, whence we can write $K = \langle x_2^c x_3^b\rangle$ for some $b, c$. If $c \neq 0$, then we claim that the group generated by $h$, $x_4$, and $K$ is all of $\overline{\mathrm{S}}_\ell$. This claim can be verified by checking that the commutator $[h, x_2^c x_3^b]$ equals a nontrivial power of $x_3$ times a power of $x_4$, thus ensuring that the group generated by $h, x_4$, and $K$ contains $\ker(\overline{\alpha})$; since $h \notin \ker(\overline{\alpha})$, this group coincides with $\overline{\mathrm{S}}_\ell$. So in fact we can take $c = 0$ and have $K = \langle x_3\rangle$.

Thus, $G$ contains the order-$\ell^2$ subgroup $\langle x_3, x_4\rangle$, and also contains the element $h$. By multiplying $h$ by suitable powers of $x_3$ and $x_4$, we can take $h$ to be $x_1^a x_2^c$ for some $a, c$. By raising $x_1^a x_2^c$ to a suitable power and re-multiplying by suitable powers of $x_3$ and $x_4$, we can take $h$ to be of the form $x_1 x_2^k$, for some $k \in \{0, \ldots, \ell-1\}$, as claimed. ∎

## 3.2 The case $\ell \geq 3$

We now show that there are no counterexamples $G \subset \mathrm{S}_\ell$ when $\ell \geq 3$ by proving that if $G \in \mathrm{Fix}(\ell^2)$ then one of the homomorphisms $\alpha, \gamma, f$ is trivial on $G$ and applying Proposition 2.3.

**Proof of Theorem 3.1(a)** Let $\ell$ be an odd prime and $G \subset \mathrm{S}_\ell$ with $G \in \mathrm{Fix}(\ell^2)$. We argue case by case based on the order of $\overline{G}$.

<u>$\overline{G}$ has order $\ell^4$.</u> In this case, $\overline{G} = \overline{\mathrm{S}}_\ell = \langle x_1, x_2\rangle$. For $i \in \{1, 2\}$ let $g_i \in G$ be any element such that $g_i \equiv x_i \pmod{\ell}$. Observe that $\alpha$ and $\gamma$ are each nonzero on $g_1 g_2$ and on $g_1 g_2^2$, whence $f(g_1 g_2) = f(g_1 g_2^2) = 0$; it then follows easily that $f(g_1) = f(g_2) = 0$. Because $g_1$ and $g_2$ were chosen arbitrarily, it follows that $f$ is trivial on all of $G$.

<u>$\overline{G}$ has order $\ell^3$.</u> There are $\ell + 1$ subgroups of $\overline{\mathrm{S}}_\ell$ of order $\ell^3$. One of these subgroups is elementary abelian and the remaining $\ell$ are nonabelian by Lemma 3.2. If $\overline{G}$ is elementary abelian, then $\overline{G} = \langle x_2, x_3, x_4\rangle$ and so $\alpha(G) = 0$.

For the nonabelian groups, we appeal to the classification of Lemma 3.2. Fix an index $k \in \{0, \ldots \ell - 1\}$ and suppose $G$ is such that

$$\overline{G} = \langle x_1 x_2^k, x_3\rangle.$$

https://doi.org/10.4153/S0008414X20000759 Published online by Cambridge University Press

If $k = 0$ then visibly $\gamma(G) = 0$. If $k \neq 0$, then let x and y be any elements of $G$ such that $\mathrm{x} \equiv x_1 x_2^k \pmod{\ell}$ and $\mathrm{y} \equiv x_3 \pmod{\ell}$. Then, $\alpha$ and $\gamma$ are nontrivial on x and xy, so $f(\mathrm{x}) = f(\mathrm{xy}) = 0$ and thus $f(\mathrm{y}) = 0$. Since x and y were chosen arbitrarily, $f(G) = 0$.

$\overline{G}$ has order $\ell^2$ or $\ell$. Since $G \in \mathrm{Fix}(\ell^2)$, for every $g \in G$ one of $\alpha(g), \gamma(g)$, or $f(g)$ must be trivial. If $\overline{G}$ is cyclic and $g \in G$ is such that $\pi_\ell(g)$ generates $\overline{G}$, then whichever of $\alpha, \gamma$, or $f$ is trivial on $g$ must also be trivial on $G$. This takes care of every group $G$ for which $\overline{G}$ has order $\ell$, as well as the special case of cyclic subgroups of $\overline{G}_3$ of order 9. We will now assume $\overline{G}$ is elementary abelian of order $\ell^2$.

Suppose $\overline{G}$ contains an element $g$ on which $\overline{\alpha}$ and $\overline{\gamma}$ are both nontrivial. Because $\overline{G}$ is abelian, and such $g$ only commute with powers of $x_4$, then $\overline{G} = \langle x_4, g\rangle$. But then $\overline{G}$ is also generated by $\langle g x_4, g\rangle$, and $\overline{\alpha}$ and $\overline{\gamma}$ are both nontrivial on these elements. By the same reasoning as in the previous cases this implies $f(G) = 0$.

If $\overline{G}$ contains an element $g \in \ker \overline{\alpha}$ then $g$ will not commute with any element of $\overline{\mathrm{S}}_\ell$ on which $\overline{\alpha}$ is nontrivial. Therefore, $\overline{G} \subset \ker \overline{\alpha}$ and so $G \subset \ker \alpha$.

If $\overline{G}$ contains an element $g \in \ker \overline{\gamma}$, let $h \in \overline{G}$ lie outside $\langle g\rangle$ so that $\overline{G}$ is generated by $g$ and $h$. If $h \in \ker \overline{\gamma}$ then we are done. If not, then both $g$ and $h$ must belong to $\ker \overline{\alpha}$ or else $g$ and $h$ would not commute and so $G \subset \ker \alpha$. ∎

### 3.3 The case $\ell = 2$

In contrast to the previous section, there do exist counterexamples $G \subset \mathrm{S}_2$, as we now show.

**Proof of Theorem 3.1(b)** We begin by noting, from the discussion above, that $\overline{\mathrm{S}}_2 = \langle x_1, x_2, x_4\rangle$ and that each pair of these generators commutes except that we have $x_1 x_2 x_1^{-1} x_2^{-1} = x_3 x_4$; moreover, each of these generators commutes with $x_3$. It is then straightforward to check that $\overline{\mathrm{S}}_2$ decomposes as a direct product of $\langle x_4\rangle \cong C_2$ with $\langle x_1, x_2\rangle \cong D_4$. From evaluating $\overline{\alpha}$ and $\overline{\gamma}$ on generators, it is clear that the order-8 elementary abelian group $\langle x_2, x_3, x_4\rangle$ (resp. $\langle x_1, x_3, x_4\rangle$) is contained in the kernel of $\overline{\alpha}$ (resp. $\overline{\gamma}$); moreover on checking orders we see that these containments are equalities. It follows that the center of $\overline{\mathrm{S}}_2$ coincides with $Z := \langle x_3, x_4\rangle = \ker(\overline{\alpha}) \cap \ker(\overline{\gamma})$.

We first prove that if $G \subset \mathrm{S}_2$ is a counterexample then we must have $\overline{G} = \overline{\mathrm{S}}_2$ or $\overline{G} \cong D_4$. To show this, we start by claiming that if $\overline{G}$ is abelian then $\overline{G}$ cannot be a counterexample. Suppose that $\overline{G}$ is an abelian subgroup of $\overline{\mathrm{S}}_2$. Since neither $\overline{\alpha}$ nor $\overline{\gamma}$ can be trivial on $G$, there must exist (not necessarily distinct) elements $w, y \in \overline{G}$ such that $w \notin \ker(\overline{\alpha})$ and $y \notin \ker(\overline{\gamma})$. If $w \in \ker(\overline{\gamma}) \setminus \ker(\overline{\alpha})$, then $w \equiv x_1 \pmod{Z}$, and the relations given above imply that $w$ cannot commute with anything not lying in $\ker(\overline{\gamma})$; this contradiction implies that $w \notin \ker(\overline{\alpha}) \cup \ker(\overline{\gamma})$. By an analogous argument, we also have $y \notin \ker(\overline{\alpha}) \cup \ker(\overline{\gamma})$, and indeed, any element $g \in \overline{G} \setminus Z$ must satisfy $g \notin \ker(\overline{\alpha}) \cup \ker(\overline{\gamma})$, i.e., $\alpha(\tilde{g}) = \gamma(\tilde{g}) = 1$ for any $\tilde{g} \in G$ with $\pi_2(\tilde{g}) = g$. Now if we assume that $G$ is a counterexample, for any $\tilde{g} \in G$ we must have $-\alpha(\tilde{g})^2 \gamma(\tilde{g}) f(\tilde{g}) \equiv 0 \pmod{2}$ by (2.6) and, therefore, $f(\tilde{g}) = 0$ for each $\tilde{g} \in \pi_2^{-1}(\overline{G} \setminus Z)$. Then, since $\overline{G} \setminus Z$ clearly generates $\overline{G}$, we get that $f$ is trivial on $G$, thus contradicting our assumption and proving our claim.

We now assume that $\overline{G}$ is a proper nonabelian subgroup of $\overline{\mathrm{S}}_2$ (and therefore of order 8) and show that it is isomorphic to $D_4$. Note that since both $\ker(\overline{\alpha})$ and $\ker(\overline{\gamma})$ are elementary abelian 2-groups, any order-4 element of $\overline{G}$ must lie in $\overline{\mathrm{S}}_2 \setminus (\ker(\overline{\alpha}) \cup$

$\ker(\overline{\gamma})$). By considering the quotient $\overline{\mathrm{S}}_2/Z$ using the generators and relations given above, we see that any element of $\overline{\mathrm{S}}_2\backslash(\ker(\overline{\alpha}) \cup \ker(\overline{\gamma}))$ must be equivalent modulo $Z$ to $x_1x_2$. It follows that any two such elements commute, and so $\overline{G}$ has the property that any two of its order-4 elements commute. Since the only nonabelian group of order 8 with that property is $D_4$, we get $\overline{G} \cong D_4$ as claimed.

Now for any counterexample $G \subset \mathrm{S}_2$, we claim that $\langle G, H\rangle \in \mathrm{Fix}(4)$ for any subgroup $H \subset \Gamma(2) \cap \ker(f)$. This follows directly from the formula (2.6) and the fact that replacing any element $g \in G$ with its translation by an element in $H$ clearly does not change $\alpha(g)$, $\beta(g)$, or $f(g)$. Since we have $\langle G, H\rangle \supset G$, the fact that $G$ satisfies the lattice condition in Question 2 automatically implies that $\langle G, H\rangle$ satisfies it as well, and so $\langle G, H\rangle$ is also a counterexample.

Now, that we have shown that any counterexample $G$ satisfies that $\overline{G}$ contains a subgroup isomorphic to $D_4$, we set out to prove the converse: that a counterexample subgroup $G \subset \mathrm{S}_2$ can be constructed satisfying that $\overline{G} = \overline{\mathrm{S}}_2$ or that $\overline{G}$ coincides with any given subgroup of $\overline{\mathrm{S}}_2$, which is isomorphic to $D_4$. We start by letting $D \subset \overline{\mathrm{S}}_2$ be any subgroup isomorphic to $D_4$, generated by an order-4 element $\mathrm{x}$ and an order-2 element $\mathrm{y} \neq \mathrm{x}^2$. Now, suppose that $G = \langle \tilde{\mathrm{x}}, \tilde{\mathrm{y}}, \Gamma(2) \cap \ker(f)\rangle$, where $\tilde{\mathrm{x}}$ and $\tilde{\mathrm{y}}$ are elements of $\mathrm{S}_2$ lying in the inverse images $\pi_2^{-1}(\mathrm{x})$ and $\pi_2^{-1}(\mathrm{y})$, respectively, and satisfying $f(\tilde{\mathrm{x}}) = 0$ and $f(\tilde{\mathrm{y}}) = 1$. Then, by construction we have $\overline{G} = \langle \mathrm{x}, \mathrm{y}\rangle = D$. We now show that every element of $G$ satisfies the determinant condition required for $G$ to lie in $\mathrm{Fix}(4)$, for which we make use of the formula (2.6). First of all, if $g \in G$ lies in $\pi_2^{-1}(\langle \mathrm{x}\rangle)$, then we clearly have $f(g) = 0$ and so $\det(g - 1) \equiv 0 \pmod 4$. Now, choose $g \in G\backslash\pi_2^{-1}(\langle \mathrm{x}\rangle)$, so that $\pi_2(g) \in D \cong D_4$ has order 2. If we assume that $g \in \mathrm{S}_2\backslash(\ker(\overline{\alpha}) \cup \ker(\overline{\gamma}))$, then it is easily verified, using the fact that the only nontrivial commutator in $\overline{\mathrm{S}}_2$ lies in $Z$, that $\pi_2(g) \equiv x_1x_2 \pmod Z$ and so $\pi_2(g)^2 = x_3x_4 \neq 1$, contradicting the fact that $\pi_2(g)$ has order 2. We therefore have $\pi_2(g) \in \ker(\overline{\alpha}) \cup \ker(\overline{\gamma})$. We then get $\det(g - 1) \equiv 0$ (mod 4) from the fact that $\alpha(g) = 0$ or $\gamma(g) = 0$. It follows that $G \in \mathrm{Fix}(4)$.

Suppose that we replace $G$ with $\langle G, \tilde{x}_4\rangle$ for some element $\tilde{x}_4 \in \mathrm{S}_2$ satisfying $\pi_2(\tilde{x}_4) = x_4$ and $f(\tilde{x}_4) = 0$. We know from the group structure of $\overline{\mathrm{S}}_2$ that it is a direct product of $\langle x_4\rangle$ and any of its subgroups isomorphic to $D_4$; therefore, we have $\overline{G} = \overline{\mathrm{S}}_2$. Now given any $g \in G\backslash\langle \tilde{\mathrm{x}}, \tilde{\mathrm{y}}, \Gamma(2) \cap H\rangle$, we have $g = g'x_4$ for some $g' \in \langle \tilde{\mathrm{x}}, \tilde{\mathrm{y}}, \Gamma(2) \cap H\rangle$. We have already shown that $\det(g' - 1) \cong 0 \pmod 4$; now it is clear that $\det(g - 1) \equiv 0 \pmod 4$ also, using (2.6) and the fact that the homomorphisms $\alpha$, $\beta$, and $f$ each take the same value on $g'$ and $g'x_4$. Thus, again we have $G \in \mathrm{Fix}(4)$.

Now, using the fact that the maps $\alpha$, $\gamma$, and $f$ are each nontrivial on $G$ in any of the above cases, we apply Lemma 2.2 to get that $G$ is a counterexample. We have thus proven the existence of counterexamples $G$ with $\overline{G} = \overline{\mathrm{S}}_2$ or $\overline{G} \cong D_4$. ■

## 3.4 Serre's counterexample

Because the reference [11] does not appear in the literature, and because it was the genesis of this paper, we give a brief description of Serre's original counterexample. Let $\ell = 2$ and consider the subgroup $H$ of $\mathrm{S}_2$ consisting of all $g$ such that

$$\alpha(g) + \gamma(g) + f(g) = 0.$$

https://doi.org/10.4153/S0008414X20000759 Published online by Cambridge University Press

This ensures that the product $\alpha^2\gamma f$ is zero on $H$ (when $\ell = 2$ we have $\alpha = \alpha'$) and hence that $H \in \mathrm{Fix}(4)$ by (2.6). Now consider the elements

$$g_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{pmatrix} \quad g_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad g_3 = \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

and set $A = g_1g_2$, $B = g_1g_3$, and $C = g_2g_3$. Then, one of $\alpha$, $\gamma$, or $f$ is nontrivial on each of $A$, $B$, and $C$ and, in addition, $A$, $B$, and $C$ each belong to $H$. This makes $H \subset \mathrm{Sp}_4(\mathbf{Z}_2)$ a counterexample by Lemma 2.3 and Proposition 2.2. We now replace $H$ by $\pi_4^{-1}(\pi_4(H))$, so that the image modulo 4 is the same, but $H$ now contains $\Gamma(4)$. This enlarged group is then open in $\mathrm{GSp}_4(\mathbf{Z}_2)$, belongs to $\mathrm{Fix}(4)$, and does not stabilize any additional lattices; it is therefore a counterexample. Since there exists an abelian surface over $\mathbf{Q}$ with full 2-adic image $\mathrm{GSp}_4(\mathbf{Z}_2)$, one can enlarge the field of definition to produce an abelian surface over a number field with the desired mod-4 image, which produces a counterexample to Question 1.

## 4 The Iwahori subgroup

Throughout this section, by fixing an appropriate symplectic basis of our free rank-4 $\mathbf{Z}_\ell$-module $\mathcal{T}$, we identify $\mathrm{B}_\ell$ with the subgroup of $\mathrm{Sp}_4(\mathbf{Z}_\ell)$ whose reduction modulo $\ell$ is the full subgroup of lower-triangular matrices. Note that $\mathrm{S}_\ell \subset \mathrm{B}_\ell$. If $G \subset \mathrm{B}_\ell$ also belongs to $\mathrm{Fix}(\ell^2)$, then the elements of $G$ can be explicitly described in terms of the maps $\alpha, \beta, \gamma, \delta, \varepsilon$ as outlined in Section 2.1. The main result of this section is the following theorem, which classifies the counterexamples $G \subset \mathrm{B}_\ell$. Because $\mathrm{B}_2 = \mathrm{S}_2$, in this section we only consider primes $\ell \geq 3$.

***Theorem 4.1*** *Suppose that $\ell \geq 3$ and that $G \in \mathrm{Fix}(\ell^2)$ is a counterexample such that $G \subset \mathrm{B}_\ell$ but $G \not\subset \mathrm{S}_\ell$. Then $G$ satisfies the following:*

(i) *$\alpha(G \cap \mathrm{S}_\ell) = 0$ and $\overline{(G \cap \mathrm{S}_\ell)}$ has order $\ell$ or $\ell^2$; or*

(ii) *$\gamma(G \cap \mathrm{S}_\ell) = 0$ and $\overline{(G \cap \mathrm{S}_\ell)}$ has order $\ell$.*

*In either case, for any $H \subset \Gamma(\ell)$, the subgroup of $\mathrm{Sp}_4(\mathbf{Z}/\ell^2)$ generated by $G$ and $H$ is also a counterexample.*

*In particular, if $G$ is a maximal counterexample, then $\Gamma(\ell) \subset G$ and $\overline{G}$ has isomorphism type $\mathbf{Z}/\ell \times (\mathbf{Z}/\ell \rtimes (\mathbf{Z}/\ell)^\times)$ or $\mathbf{Z}/\ell \rtimes (\mathbf{Z}/\ell)^\times$, depending on whether $\alpha(G \cap \mathrm{S}_\ell) = 0$ or $\gamma(G \cap \mathrm{S}_\ell) = 0$, respectively.*

*Moreover, there do exist counterexamples satisfying (i) and counterexamples satisfying (ii).*

Observe that if $G \in \mathrm{Fix}(\ell^2)$ then $G \cap \mathrm{S}_\ell \in \mathrm{Fix}(\ell^2)$ as well. By our work in Section 3, one of $\alpha$, $\gamma$, or $f$ must be trivial on $G \cap \mathrm{S}_\ell$. Starting with $f$, we will consider the effect on $G$ of $\alpha$, $\gamma$, or $f$ being trivial on $G \cap \mathrm{S}_\ell$.

***Lemma 4.2*** *Suppose $G \in \mathrm{Fix}(\ell^2)$, $G \subset \mathrm{B}_\ell$, and $f(G \cap \mathrm{S}_\ell) = 0$. Then $f(G) = 0$ and therefore, by* Proposition 2.3, *$G$ is not a counterexample.*

**Proof** The fact that $G \cap \mathrm{S}_\ell \lhd G$ and the hypothesis $f(G \cap \mathrm{S}_\ell) = 0$ together imply $f$ induces a homomorphism $G/G \cap \mathrm{S}_\ell \to \mathbf{Z}/\ell$. But elements in $G/G \cap \mathrm{S}_\ell$ have order coprime to $\ell$, whence such a homomorphism is trivial and so is $f$. ∎

In contrast to Lemma 4.2, we do get counterexamples when $\alpha(G \cap \mathrm{S}_\ell) = 0$ and when $\gamma(G \cap \mathrm{S}_\ell) = 0$, as claimed in Theorem 4.1. Our first step in each classification is to show that if $G$ is a maximal counterexample, then $\overline{(G \cap \mathrm{S}_\ell)}$ has order $\ell^2$ when $\alpha(G \cap \mathrm{S}_\ell) = 0$ and order $\ell$ when $\gamma(G \cap \mathrm{S}_\ell) = 0$.

We start with a computation that will be used in both cases. In order for $G$ to be a counterexample, $f : G \to \mathbf{Z}/\ell$ must be nontrivial and, therefore, surjective. If $g \in G$ and $f(g) \neq 0$, our determinant formula (2.4) directly implies

$$\gamma(g)\alpha(g)^2 + \frac{\beta(g)\alpha(g)(1-\varepsilon(g)^2)}{\varepsilon(g)} + \frac{\delta(g)(1-\varepsilon(g))^2}{\varepsilon(g)} \equiv 0 \pmod{\ell}. \tag{4.1}$$

***Remark 4.3*** Even though we will not need it for the work that follows, one can prove that if the mod-$\ell$ images of the entries of $g$ satisfy (4.1), and if $\varepsilon(g) \in (\mathbf{Z}/\ell)^\times$ has order $m$, then $g^m \equiv 1 \pmod{\ell}$.

Now, we consider the effect of $\alpha$ and $\gamma$ being trivial on $G \cap \mathrm{S}_\ell$. If either $\alpha(G \cap \mathrm{S}_\ell) = 0$ or $\gamma(G \cap \mathrm{S}_\ell) = 0$, then $\overline{(G \cap \mathrm{S}_\ell)}$ cannot be the full $\ell$-Sylow subgroup of $\mathrm{Sp}_4(\mathbf{Z}/\ell)$. We will now show, among other things, that $\overline{(G \cap \mathrm{S}_\ell)}$ cannot have order $\ell^3$ either. To do this, we will argue separately for $\alpha$ versus $\gamma$. Because neither $\alpha$ nor $\gamma$ extends to a homomorphism of $G$, our arguments will be different from those for Lemma 4.2.

***Lemma 4.4*** *Suppose $G \subset \mathrm{B}_\ell$ lies in* $\mathrm{Fix}(\ell^2)$ *and that $f|_G$ is nontrivial. Suppose further that $\alpha(G \cap \mathrm{S}_\ell) = 0$. Then $\overline{(G \cap \mathrm{S}_\ell)}$ has order dividing $\ell^2$.*

**Proof** Recall that $\ker \overline{\alpha} = \langle x_2, x_3, x_4 \rangle$ is the unique elementary abelian subgroup of $\overline{(G \cap \mathrm{S}_\ell)}$ of order $\ell^3$. Fix $g \in G \backslash G \cap \mathrm{S}_\ell$ and suppose $\det(g-1) \equiv 0 \pmod{\ell^2}$, so that either $f(g) = 0$ or (4.1) holds.

Let $s \in G \cap \mathrm{S}_\ell$. Then, direct computation in coordinates reveals that

$$\det(gs-1) \equiv (\star)(f(g)+f(s))\ell \pmod{\ell},$$

where the expression $(\star)$ is given by

$$\star = \frac{\alpha(g)^2\gamma(s) + (1-\varepsilon(g))^2\delta(s) + 2\alpha(g)(1-\varepsilon(g))\beta(s)}{\varepsilon(g)}.$$

Thus, for every $s \in G \cap \mathrm{S}_\ell$, we must have either

$$\alpha(g)^2\gamma(s) + (1-\varepsilon(g))^2\delta(s) + 2\alpha(g)(1-\varepsilon(g))\beta(s) \equiv 0 \pmod{\ell} \tag{4.2}$$

or $f(s) + f(g) \equiv 0 \pmod{\ell}$.

For fixed $g$, we claim that it is not the case that every $s \in \ker \alpha$ satisfies (4.2) or $f(s) + f(g) \equiv 0 \pmod{\ell}$. To see this, note that the subset

$$\{(\beta(s), \gamma(s), \delta(s))\}_{s \in \ker \alpha \cap \mathrm{S}_\ell} \subset (\mathbf{Z}/\ell)^3$$

defines a three-dimensional $\mathbf{F}_\ell$-vector space E. Indeed, it is easy to verify from the discussion in Section 3.1 that the maps $\overline{\beta}$, $\overline{\gamma}$, $\overline{\delta} : \overline{\mathrm{S}}_\ell \to \mathbf{Z}/\ell$ are homomorphisms and

https://doi.org/10.4153/S0008414X20000759 Published online by Cambridge University Press

form a dual basis $\{\overline{\beta}, \overline{\gamma}, \overline{\delta}\}$ to the basis $\{x_2, x_3, x_4\}$ of the three-dimensional $\mathbf{F}_\ell$-space $\ker \overline{\alpha} \cap \overline{\mathrm{S}}_\ell$. Since $g$ is fixed and $\varepsilon(g) \neq 1$, the congruence (4.2) defines a codimension-1 subspace V of E.

Then, every $s$ such that $(\beta(s), \gamma(s), \delta(s))$ lies outside V must have $f(s) = -f(g)$. If $f(g) = 0$, then $f(s) = 0$ for all $s \notin \pi_\ell^{-1}(G \cap \mathrm{S}_\ell)$. This implies $f(G) = 0$ because the complement of $\pi_\ell^{-1}(G \cap \mathrm{S}_\ell)$ generates $G$, and contradicts the hypothesis $f|_G$ is nontrivial. If $f(g) \neq 0$, then we have

$$f(s) = f(s^2) = -f(g),$$

which is impossible since $f(s^2) = 2f(s)$. If follows that $\overline{(G \cap \mathrm{S}_\ell)}$ cannot have order $\ell^3$ and so must have order dividing $\ell^2$. ∎

Lemma 4.4 constrains the order of $\overline{(G \cap \mathrm{S}_\ell)}$ to be at most $\ell^2$. We now show that counterexamples exist when the order equals $\ell^2$. While it is possible that counterexamples may exist when the order of $\overline{(G \cap \mathrm{S}_\ell)}$ equals $\ell$, they would come from subgroups of the order-$\ell^2$ counterexamples. Because of this, it will satisfy us to describe only the maximal counterexamples.

***Remark 4.5*** In the extreme case, where $\overline{(G \cap \mathrm{S}_\ell)}$ is trivial, then $G$ cannot be a counterexample, since $\overline{G}$ is then cyclic (if a generator fixes an order-$\ell^2$ submodule, then the entire group will fix the same).

***Proposition 4.1*** *Fix an element $g \in \mathrm{B}_\ell \backslash \mathrm{S}_\ell$ satisfying $\det(g-1) \equiv 0 \pmod{\ell^2}$. Let $\mathcal{S}$ be the subgroup of $\ker \alpha$ satisfying (4.2) relative to the coordinates of $g$. Then, the subgroup $G$ of $\mathrm{B}_\ell$ generated by the element $g$ and the subgroups $\mathcal{S}$ and $\Gamma(\ell)$ is a counterexample.*

**Proof** By hypothesis $\det(g-1) \equiv 0 \pmod{\ell^2}$, and $\det(gs-1) \equiv 0 \pmod{\ell^2}$ for all $s \in G \cap \mathrm{S}_\ell$ because of (4.2). Therefore, the coset $g(G \cap \mathrm{S}_\ell)$ consists entirely of elements $\sigma$ satisfying $\det(\sigma - 1) \equiv 0 \pmod{\ell^2}$. We claim that this is enough to conclude that $G \in \mathrm{Fix}(\ell^2)$. To see this, we use the fact that $G/(G \cap \mathrm{S}_\ell)$ is cyclic, generated by $g(G \cap \mathrm{S}_\ell)$ and, for fixed $n \geq 1$, evaluate the expression $(\star)$ of Lemma 4.4 on elements $g^n s$:

$$(\star)' : \frac{\alpha(g^n)^2 \gamma(s) + (1 - \varepsilon(g^n))^2 \delta(s) + 2\alpha(g^n)(1 - \varepsilon(g^n))\beta(s)}{\varepsilon(g^n)}.$$

We have $\varepsilon(g^n) = \varepsilon(g)^n$ because $\varepsilon : G \to (\mathbf{Z}/\ell)^\times$ is a homomorphism. It is easy to show that

$$\alpha(g^n) = \frac{1 - \varepsilon(g)^n}{1 - \varepsilon(g)} \alpha(g).$$

Then, applying the expressions for $\alpha(g^n)$ and $\varepsilon(g^n)$ to $(\star)'$ and using (4.2), algebraic manipulation reveals that $(\star)' = 0$. Therefore, every coset $g^n(G \cap \mathrm{S}_\ell)$ consists of $\sigma$ with $\det(\sigma - 1) \equiv 0 \pmod{\ell^2}$ and so $G \in \mathrm{Fix}(\ell^2)$.

To see that $G$ is a counterexample, we apply Propositions 2.3 and 2.2. Our assumption that $\Gamma(\ell) \subset G$ means that $f|_G$ is nontrivial, satisfying Proposition 2.3(a). If $\alpha|_G$ and $\gamma|_G$ are nonzero, then Proposition 2.2 shows that the only proper $G$-stable lattices we need to check for quotients with trivial $G$-action are $L_0$, $L_1$, $L_2$, and $L_3$. But any pair of these with relative index $\ell^2$ visibly has nontrivial $G$-action due to the nontriviality of $\varepsilon$. There is one exceptional case to check by hand.

If $\alpha(G) = 0$, then $\delta(s) = 0$ for all $s \in G \cap \mathrm{S}_\ell$ by (4.2). If, in addition, $\gamma(G) \neq 0$, then an argument in the vein of the proof of Proposition 2.3 shows that the only new $G$-stable lattices to include among $L_0$, $L_1$, $L_2$, and $L_3$ are:

- the lattice $\widetilde{L}_1$ generated by $\ell\mathfrak{T}$ and $e_3$, and
- the lattice $\widetilde{L}_2$ generated by $\ell\mathfrak{T}$ and $e_1$, $e_3$, and $e_4$.

The nontriviality of $\varepsilon$ again shows that the action on any quotient of order $\ell^2$ is nontrivial.

If $\gamma(G) = 0$, (in particular $\gamma(s) = 0$ for all $s \in G \cap \mathrm{S}_\ell$), then (4.2) imposes an additional linear condition on the entries of $\overline{G \cap \mathrm{S}_\ell}$ and so $G \cap \mathrm{S}_\ell$ has order dividing $\ell$. Since we only classify maximal counterexamples in this proposition, we can safely omit this case.

This completes the classification of maximal counterexamples and finishes the proof. ∎

We can produce counterexamples that are as large as possible within the constraints of Proposition 4.1, as the following example shows.

***Example 4.6*** Suppose $\alpha(g) = 0$ so that $(\star)$' simplifies to

$$(1 - \varepsilon(g)^n)^2\delta(s).$$

for all $s$. In particular, $(1 - \varepsilon(g)^n)^2\delta(s)$ must equal 0 for all powers of $n$, including those for which $\varepsilon(g)^n \neq 1$, whence $\delta(s) = 0$ for all $s$. The maximal subgroup satisfying all of these conditions is then seen to be the preimage in $\mathrm{Sp}_4(\mathbf{Z}_\ell)$ of the group

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \varepsilon & 0 & 0 \\ \beta & \gamma & 1/\varepsilon & 0 \\ 0 & \beta\varepsilon & 0 & 1 \end{pmatrix} \subset \mathrm{Sp}_4(\mathbf{Z}/\ell),$$

where $\beta, \gamma \in \mathbf{Z}/\ell$ and $\varepsilon \in (\mathbf{Z}/\ell)^\times$.

Finally, we consider the case where $\gamma(G \cap \mathrm{S}_\ell) = 0$. Similar to when $\alpha(G \cap \mathrm{S}_\ell) = 0$, we will show that if $G$ is a counterexample, then $\overline{(G \cap \mathrm{S}_\ell)}$ cannot have order $\ell^3$; in fact, we will show that $\overline{(G \cap \mathrm{S}_\ell)}$ must have order $\ell$.

***Lemma 4.7*** *Suppose $G \subset \mathrm{B}_\ell$ lies in $\mathrm{Fix}(\ell^2)$ and that $f|_G$ is nontrivial. Suppose further that $\gamma(G \cap \mathrm{S}_\ell) = 0$. Then $\overline{(G \cap \mathrm{S}_\ell)}$ has order dividing $\ell$.*

**Proof** The proof strategy is nearly identical to that of Lemma 4.4. Fix $g \in G \backslash G \cap \mathrm{S}_\ell$ with $\det(g - 1) \equiv 0 \pmod{\ell}$. For all $s \in G \cap \mathrm{S}_\ell$, we must have $\det(gs - 1) \equiv 0 \pmod{\ell}$ and a direct calculation reveals that

$$\det(gs - 1) \equiv \big(\star\star\big)(f(g) + f(s))\ell,$$

where the expression $(\star\star)$ is given by

$$\gamma(g)\alpha(s)^2 + 2(\beta(g)(1 - \varepsilon(g)) + \alpha(g)\gamma(g))\alpha(s) +$$
$$2\alpha(g)(1/\varepsilon(g) - 1)\beta(s) + (1/\varepsilon(g) - 1)\alpha(s)\beta(s) + (\varepsilon(g) + 1/\varepsilon(g) - 2)\delta(s).$$

Therefore, for every $s \in G \cap \mathrm{S}_\ell$ it must be the case that either

$$\begin{aligned}(4.3)\quad & \gamma(g)\alpha(s)^2 + 2(\beta(g)(1-\varepsilon(g)) + \alpha(g)\gamma(g))\alpha(s) + \\ & 2\alpha(g)(1/\varepsilon(g)-1)\beta(s) + (1/\varepsilon(g)-1)\alpha(s)\beta(s) + (\varepsilon(g)+1/\varepsilon(g)-2)\delta(s) = 0\end{aligned}$$

or $f(s) + f(g) = 0$.

Not every triple $(\alpha(s), \beta(s), \delta(s)) \in (\mathbf{Z}/\ell)^3$ satisfies (4.3) (for example, $(0,0,1)$ does not), and those that do not need not satisfy $f(s) + f(g) = 0$ by the same reasoning in the proof of Lemma 4.4. Therefore, the group $\overline{(G \cap \mathrm{S}_\ell)}$ cannot have order $\ell^3$, and hence has order dividing $\ell^2$. We will now show that the order must in fact divide $\ell$.

While the group $\ker \overline{\gamma}$ is not elementary abelian, any subgroup of order dividing $\ell^2$ is. We will show that the set

$$\{(\alpha(s), \beta(s), \delta(s)) \in \mathbf{F}_\ell{}^3\}$$

taken over all $s \in G \cap \mathrm{S}_\ell$ that satisfy (4.3) does not contain a two-dimensional linear space. Suppose it did. Let $s \in G \cap \mathrm{S}_\ell$ so that $s^2 \in G \cap \mathrm{S}_\ell$ as well. Apply the condition (4.3) to $s^2$ and subtract twice the relation (4.3) applied to $s$ to obtain the new condition

$$(4.4)\qquad \alpha(s)\big(\gamma(g)\alpha(s) + (1/\varepsilon(g)-1)\beta(s)\big) = 0.$$

If $\alpha(s) = 0$ then substituting into (4.3) shows

$$(4.5)\qquad 2\alpha(g)(1/\varepsilon(g)-1)\beta(s) + (\varepsilon(g)+1/\varepsilon(g)-2)\delta(s) = 0$$

whence the linear space is at most one-dimensional.

On the other hand, if $\gamma(g)\alpha(s) + (1/\varepsilon(g)-1)\beta(s) = 0$, then substituting into (4.3) additionally shows that

$$(4.6)\qquad 2\beta(g)(1-\varepsilon(g))\alpha(s) + (\varepsilon(g)+1/\varepsilon(g)-2)\delta(s) = 0$$

as well, whence the linear space is at most one-dimensional.

In all cases, we see that $\overline{G \cap S}$ has order dividing $\ell$, which completes the proof of the lemma. ■

We now show that there exist counterexamples $G \subset \mathrm{B}_\ell$ where $\overline{(G \cap \mathrm{S}_\ell)}$ has order $\ell$.

***Proposition 4.2*** *Fix an element* $g \in \mathrm{B}_\ell \backslash \mathrm{S}_\ell$ *with* $\det(g-1) \equiv 0 \pmod{\ell^2}$. *Let* $\mathscr{S}$ *be any subgroup of* $\ker \gamma$ *satisfying* (4.3) *such that* $\overline{\mathscr{S}}$ *has order* $\ell$. *Then, the subgroup G of* $\mathrm{B}_\ell$ *generated by g,* $\mathscr{S}$*, and* $\Gamma(\ell)$ *is a counterexample.*

**Proof** The proof of Lemma 4.7 showed that there are two ways for $\overline{G \cap \mathrm{S}_\ell}$ to have order $\ell$; see equation (4.4), which yields the two cases (4.5) and (4.6). We will consider these case by case.

*Case* 1. Suppose $\alpha(s) = 0$ for all $s \in G \cap \mathrm{S}_\ell$. Then, by (4.3), we have

$$(4.7)\qquad 2\alpha(g)(1-\varepsilon(g))\beta(s) + (\varepsilon(g)+1/\varepsilon(g)-2)\delta(s) = 0$$

and so $g(G \cap \mathrm{S}_\ell)$ consists entirely of elements $\sigma$ such that $\det(\sigma - 1) \equiv 0 \pmod{\ell^2}$. Fix a positive integer $n > 1$ such that $g^n \notin G \cap \mathrm{S}_\ell$ and consider the coset $g^n(G \cap \mathrm{S}_\ell)$.

https://doi.org/10.4153/S0008414X20000759 Published online by Cambridge University Press

Because

$$\gamma(g^n) = \frac{(1-\varepsilon(g)^{2n})}{(1-\varepsilon(g)^2)\varepsilon(g)^{n-2}}\gamma(g),$$

the determinant condition $\det(g^n s - 1) \equiv 0 \pmod{\ell^2}$, under the assumption that $\alpha(s) = 0$ and making the substitution $g \mapsto g^n$ in (4.3) reduces to

$$2\alpha(g^n)(1-\varepsilon(g^n))\beta(s) + (\varepsilon(g^n) + 1/\varepsilon(g^n) - 2)\delta(s) \equiv 0 \pmod{\ell},$$

which simplifies to

$$2\alpha(g)\beta(s)(1-\varepsilon(g)^n)^2 \frac{(1-1/\varepsilon(g)^{(n-1)})}{1-\varepsilon(g)} \equiv 0 \pmod{\ell}$$

for all $s \in G \cap S_\ell$. If $\beta(s) = 0$ for all $g \in S_\ell$, then by (4.7) we have $\delta(s) = 0$ for all $s \in S_\ell$ as well, and so $\overline{G \cap S_\ell}$ is trivial, violating the hypothesis that it have order $\ell$. We also assume that $\varepsilon(g^n)$ and $\varepsilon(g^{n-1})$ are nontrivial, and thus we are left with $\alpha(g) = 0$.

If $\alpha(g) = 0$ then $\alpha(G) = 0$, and then it is immediate to check that (4.3) is satisfied for all nontrivial cosets $g^n(G \cap S_\ell)$.

*Case* 2. Here, we assume

$$\gamma(g)a(s) + (1/\varepsilon(g) - 1)\beta(s) = 2\beta(g)(1-\varepsilon(g))\alpha(s) + (\varepsilon(g) + 1/\varepsilon(g) - 2)\delta(s) = 0 \tag{4.8}$$

for all $s \in G \cap S_\ell$. Now, we proceed in an identical fashion to the previous case to determine conditions for an arbitrary coset $g^n(G \cap S_\ell)$ to consist of elements $\sigma$ with $\det(\sigma - 1) \equiv 0 \pmod{\ell^2}$. If $\gamma(g) \neq 0$, then a similar argument to the one above shows that we are forced to take $\alpha(s) = 0$ for all $s$. But the linearity conditions then show $\beta(s) = \delta(s) = 0$ for all $s$ as well, whence $\overline{G \cap S_\ell}$ is trivial, a contradiction. On the other hand, if $\gamma(g) = 0$, then $\gamma(G) = 0$; and then a straightforward argument, similar to the one above, shows (substituting $g \mapsto g^n$ in the formula (4.8)) that $\det(g^n s - 1) \equiv 0 \pmod{\ell^2}$ for all $s \in G \cap S_\ell$ and so $G \in \mathrm{Fix}(\ell^2)$.

We see that either $\alpha|_G = 0$ or $\gamma|_G = 0$, so we cannot apply Proposition 2.2 directly. In the case $\alpha|_G = 0$ but $\gamma|_G \neq 0$, then the only lattices to check in addition to the $L_i$ are the $\widetilde{L}_1$ and $\widetilde{L}_2$ of the proof of Proposition 4.1. Similarly, due to the nontriviality of $\varepsilon$, there do not exist quotients of order $\ell^2$ with trivial $G$-action.

If $\gamma|_G = 0$ but $\alpha|_G \neq 0$, then the only additional stable lattice to check is the lattice $\widetilde{L}_3$ generated by $\ell\mathcal{T}$ and the elements $e_2$ and $e_4$. As in all other cases, the nontriviality of $\varepsilon$ means that none of the quotients of order $\ell^2$ have trivial $G$-action.

This completes the proof. ∎

As with Proposition 4.1, we can use Proposition 4.2 to produce maximal counterexamples. That is, we can find $G \in \mathrm{Fix}(\ell^2)$ such that $\Gamma(\ell) \subset G$ and such that $\overline{G}$ has order $(\ell - 1)\ell$. The following example has $G \cap S_\ell \subset \ker\gamma$ and is distinct from the ones classified by Proposition 4.1.

https://doi.org/10.4153/S0008414X20000759 Published online by Cambridge University Press

***Example 4.8*** Let $G \subset B_\ell$ be the full preimage of the group

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ \alpha & \varepsilon & 0 & 0 \\ 0 & 0 & 1/\varepsilon & 0 \\ 0 & 0 & -\alpha/\varepsilon & 1 \end{pmatrix} \subset \mathrm{Sp}_4(\mathbf{Z}/\ell),$$

where $\alpha \in \mathbf{Z}/\ell$ and $\varepsilon \in (\mathbf{Z}/\ell)^\times$. One can check that this group falls into the classification of the counterexamples given above.

## 5 Subgroups with an irreducible two-dimensional factor

Now, we suppose that the subgroup $G \subset \mathrm{Sp}(\mathcal{T})$ is such that the semisimplification of the action of $\overline{G}$ on $\mathcal{T}/\ell\mathcal{T}$ contains an irreducible two-dimensional factor. Throughout this section, by fixing an appropriate symplectic basis $\{e_1, e_2, e_3, e_4\}$ of our free rank-4 $\mathbf{Z}_\ell$-module $\mathcal{T}$ (in which we require that $\overline{e}_4$ be fixed by all of $\overline{G}$), we identify $\mathrm{P}_\ell$ with a particular subgroup of $\mathrm{Sp}_4(\mathbf{Z}_\ell)$ whose reduction is lower block-triangular. We recall the maps $\alpha, \beta, \beta', \alpha' : \mathrm{P}_\ell \to \mathbf{Z}/\ell$, as well as their induced maps $\overline{\alpha}, \overline{\beta}, \overline{\alpha}', \overline{\beta}' : \overline{\mathrm{P}}_\ell \to \mathbf{Z}/\ell$ defined in Section 2.1. Each element of $\overline{\mathrm{P}}_\ell$ is a lower-block-diagonal matrix that fixes $\overline{e}_4$ and whose middle block is a $2 \times 2$ submatrix reflecting how that operator acts on the component corresponding to the span of $\{\overline{e}_2, \overline{e}_3\}$ in the semisimplification of $\mathcal{T}/\ell\mathcal{T}$. There is, therefore, a homomorphism $\overline{\pi} : \overline{\mathrm{P}}_\ell \to \mathrm{SL}_2(\mathbf{Z}/\ell)$ given by sending a matrix in $\overline{\mathrm{P}}_\ell$ to its middle block, which is a matrix in $\mathrm{SL}_2(\mathbf{Z}/\ell)$. Composing this with $\pi_\ell$ gives us a homomorphism $\pi : G \to \mathrm{SL}_2(\mathbf{Z}/\ell)$.

When the image under $\pi$ of a subgroup $G \subset \mathrm{P}_\ell$ is reducible, via an appropriate change of symplectic bases of $\mathcal{T}$, it can be simultaneously conjugated to a group of lower-triangular matrices in $\mathrm{SL}_2(\mathbf{F}_\ell)$ (without affecting the block-diagonal structure of $\overline{G}$), and, therefore, we are in the situation dealt with in Section 3 and Section 4. In this section, we are concerned with the case that $\overline{\pi}(\overline{G})$ is an irreducible subgroup of $\mathrm{SL}_2(\mathbf{F}_\ell)$, i.e., there is no nontrivial subspace of $\mathbf{F}_\ell^2$ fixed by the whole group $\pi(G)$.

We now show how the vector $(\beta', \alpha')(g) = (\beta'(g), \alpha'(g)) \in {\mathbf{F}_\ell}^2$ is determined by $(\alpha, \beta)(g)$ and $\pi(g)$. The group $\mathrm{SL}_2(\mathbf{F}_\ell)$ injects into $\overline{\mathrm{P}}_\ell$ as the subgroup of all block-diagonal matrices whose first and last blocks are trivial; this injection $\mathrm{SL}_2(\mathbf{F}_\ell) \hookrightarrow \overline{\mathrm{P}}_\ell$ is a section of the surjective map $\overline{\pi}$. Given any matrix $g \in \mathrm{P}_\ell$, we may multiply its reduction $\pi_\ell(g) \in \overline{\mathrm{P}}_\ell$ on the right by the block-diagonal matrix in $\overline{\mathrm{P}}_\ell$ corresponding to the image of $\pi(g)^{-1}$ to get a matrix $x \in \overline{\mathrm{P}}_\ell$ lying in $\ker(\overline{\pi})$. We have seen in Section 2 that then we have $(\overline{\beta}', \overline{\alpha}')(x) = (\overline{\beta}, -\overline{\alpha})(x)$. One then checks directly through the operation of matrix multiplication that $(\alpha, \beta)(g) = (\overline{\alpha}, \overline{\beta})(\pi_\ell(g)) = (\overline{\alpha}, \overline{\beta})(x)$ and that we have the formula

$$(\beta', \alpha')(g) = \big(\beta(g) - \alpha(g)\big)\pi(g). \tag{5.1}$$

We are now ready to present the main result of this section, which states that, under the hypotheses of this section, there are no counterexamples for $\ell \geq 3$ and which roughly classifies the counterexamples that exist for $\ell = 2$. For notational convenience, we switch to using $\mathbf{F}_\ell$ for $\mathbf{Z}/\ell$ to emphasize the fact that we are doing linear algebra rather than considering an image of reduction modulo $\ell$.

https://doi.org/10.4153/S0008414X20000759 Published online by Cambridge University Press

***Theorem 5.1*** *Let $G \subset \mathrm{Sp}(\mathcal{T})$ be a counterexample satisfying that $\pi(G) \subset \mathrm{SL}_2(\mathbf{F}_\ell)$ is an irreducible subgroup. Then we have $\ell = 2$; i.e., there are no counterexamples satisfying the above property when $\ell \geq 3$. When $\ell = 2$, we have that $G \subset \mathrm{Sp}(\mathcal{T})$ satisfies either*

(i) $\overline{G}_2 \cong \pi(G) \times C_2$; *or*
(ii) $\overline{G}_2 \cong \pi(G) \cong \mathrm{SL}_2(\mathbf{F}_2)$.

*In case (i), for any $H \subset \Gamma(2) \cap \ker(f)$, the subgroup of $\mathrm{Sp}(\mathcal{T})$ generated by $G$ and $H$ is also a counterexample. In case (ii), for any $H \subset \ker(\pi_2)$, the subgroup of $\mathrm{Sp}(\mathcal{T})$ generated by $G$ and $H$ is also a counterexample (in particular, the full inverse image $\pi_2^{-1}(\overline{G}_2)$ is a maximal counterexample).*

*Moreover, there do exist counterexamples satisfying (i) and counterexamples satisfying (ii).*

The rest of this section is dedicated to proving the above theorem. Throughout the following arguments, we will freely use the fact that if a subgroup $G \subset \mathrm{Sp}(\mathcal{T})$ is a counterexample, then $f$ must be nontrivial on $G$, by Proposition 2.3(a).

## 5.1 Restricting the possible images of counterexamples

In this subsection, we will show that under the assumption of an irreducible two-dimensional factor, which was established at the beginning of this section, a counterexample $G$ must satisfy $\overline{G} \cong \pi(G) \times C_\ell$ or $\overline{G} \cong \pi(G)$. We first need to provide some basic results concerning the properties of the classical groups $\mathrm{SL}_2(\mathbf{F}_\ell)$ and their irreducible subgroups, as in the below proposition.

For the statement below and the arguments given throughout the rest of the section, recall that a *unipotent* operator $x$ is one satisfying $(x-1)^n = 0$ for some $n \geq 1$. In our situation where $x$ belongs to $\mathrm{SL}_2(\mathbf{F}_\ell)$ for some prime $\ell$, this is equivalent to satisfying that $(x-1)^2 = 0$; that $x - 1$ is noninvertible; that $x$ fixes some nontrivial vector $v \in \mathbf{F}_\ell^2$; or that the only eigenvalue of $x$ is 1.

In what follows, an *irreducible* subgroup of $\mathrm{SL}_2(\mathbf{F}_\ell)$ is one that acts irreducibly on $\mathbf{F}_\ell^2$.

***Proposition 5.1*** *Let $\ell$ be a prime. The following facts hold.*

a) (i) *If $\ell \geq 5$, then there is no nontrivial homomorphism from $\mathrm{SL}_2(\mathbf{F}_\ell)$ to $\mathbf{Z}/\ell$.*
   (ii) *The only normal subgroup of $\mathrm{SL}_2(\mathbf{F}_3)$ of index 3 is the subgroup $Q_8 \triangleleft \mathrm{SL}_2(\mathbf{F}_3)$ coinciding with the subset of all elements whose orders are not divisible by 3 and which is isomorphic to the quaternion group; there are thus only two nontrivial homomorphisms from $\mathrm{SL}_2(\mathbf{F}_3)$ to $\mathbf{Z}/3$, both having kernel $Q_8$.*
   (iii) *Since $\mathrm{SL}_2(\mathbf{F}_2)$ is isomorphic to the symmetric group $S_3$, the only nontrivial homomorphism from $\mathrm{SL}_2(\mathbf{F}_2)$ to $\mathbf{Z}/2$ is the one whose kernel is the order-3 subgroup $A_3 \triangleleft \mathrm{SL}_2(\mathbf{F}_2)$ corresponding to the alternating group.*

b) *An element of $\mathrm{SL}_2(\mathbf{F}_\ell)$ is unipotent if and only if it has order dividing $\ell$.*
c) *The order of any proper irreducible subgroup of $\mathrm{SL}_2(\mathbf{F}_\ell)$ is not divisible by $\ell$; thus there is no nontrivial homomorphism from a proper irreducible subgroup of $\mathrm{SL}_2(\mathbf{F}_\ell)$ to $\mathbf{Z}/\ell$.*
d) *Assume that $\ell \geq 3$, and let $H \subsetneq \mathrm{SL}_2(\mathbf{F}_\ell)$ be a proper irreducible subgroup. The group $\mathrm{SL}_2(\mathbf{F}_\ell)$ is generated by set of nonunipotent matrices lying in $\mathrm{SL}_2(\mathbf{F}_\ell) \backslash H$.*
e) *If $\ell \geq 3$, each irreducible subgroup of $\mathrm{SL}_2(\mathbf{F}_\ell)$ has nontrivial center.*

https://doi.org/10.4153/S0008414X20000759 Published online by Cambridge University Press

**Proof** If $\ell \geq 3$, any homomorphism from $\mathrm{SL}_2(\mathbf{F}_\ell)$ to $\mathbf{Z}/\ell\mathbf{Z}$ must kill the scalar $-1$, since the order of this element is never divisible by $\ell$. Such a homomorphism, therefore, factors through the projective linear group $\mathrm{SL}_2(\mathbf{F}_\ell)/\{\pm 1\}$. According to [10, Section IV.3.4, Lemma 1], this group is simple as long as $\ell \geq 5$. Such a homomorphism must therefore be trivial, proving part (a)(i). The statements of (a)(ii) and (a)(iii) are evident from direct verification.

Parts (c) and (b) are precisely the statement of [6, Theorem XI.2.2] (see also [10, Section IV.3.2, Lemma 2] and the unnamed statement appearing right before it in [6, Section XI.2] respectively.

Now assume that $\ell \geq 3$, and let $H \subsetneq \mathrm{SL}_2(\mathbf{F}_\ell)$ be a proper irreducible subgroup. Consider the subset $S \subset \mathrm{SL}_2(\mathbf{F}_\ell)$ consisting of all matrices $x$ such that $-x$ is nontrivial and unipotent. Since each operator in $S$ has $-1$ as its only eigenvalue, there are no unipotent matrices in $S$. Moreover, given any element $x \in S$, since $\ell$ is odd and $-x \neq 1$ is unipotent and so has order $\ell$, we have $x^{\ell+1} = (-x)^{\ell+1} = -x$. This proves both that $S \cap H = \varnothing$ (because otherwise $H$ would contain the unipotent matrix $-x$ for each $x \in S$; it follows from parts (b) and (c) that this contradicts the fact that $H$ is proper and irreducible) and that $S$ generates the set of all unipotent matrices in $\mathrm{SL}_2(\mathbf{F}_\ell)$, which are well known to generate all of $\mathrm{SL}_2(\mathbf{F}_\ell)$. Thus, part (d) is proved.

Now retaining our assumption that $\ell \geq 3$, the group $\mathrm{SL}_2(\mathbf{F}_\ell)$ itself has nontrivial center since it contains the scalar $-1$. Let $N \subsetneq \mathrm{SL}_2(\mathbf{F}_\ell)$ be a proper irreducible subgroup. By part (c), the order of $N$ is not divisible by $\ell$ and so we may apply [6, Theorem XI.2.3] to get that $N/(N \cap \{\pm 1\})$ is isomorphic to a dihedral group or to $A_4$, $S_4$, or $A_5$. One verifies through straightforward computation that the only element of order 2 in $\mathrm{SL}_2(\mathbf{F}_\ell)$ is the scalar $-1$. It follows that if $N$ has even order, then $N$ has nontrivial center. We therefore assume that $N$ has odd order. Then, we have that $N \cong N/(N \cap \{\pm 1\})$ itself must be an odd-order subgroup of a dihedral group or of $A_4$, $S_4$, or $A_5$. We claim that the only odd-order subgroups of these groups are abelian, thus proving that $N$ still has nontrivial center. Indeed, the only odd-order elements of a dihedral group lie in its index- 2 cyclic subgroup and thus can only generate a cyclic subgroup, while we see by looking at the orders of $A_4$, $S_4$, and $A_5$ that their odd-order subgroups must have order dividing 15, and all such groups are abelian. Thus, part (e) is proved. ∎

***Lemma 5.2*** *Let $\ell$ be any prime and $G$ be any group in* $\mathrm{Fix}(\ell^2)$.

*a) For each nontrivial element $g \in G$ with $f(g) \neq 0$, there exists a vector $w_g = ((w_g)_1, (w_g)_2) \in \mathbf{F}_\ell^2$ such that $(\alpha, \beta)(g) = \pi(g).w_g - w_g$. If $f(g) \neq 0$ and $\pi(g)$ is not unipotent, then $\pi_\ell(g)$ fixes the vector $(-1, (w_g)_1, (w_g)_2, 0) \in \mathbf{F}_\ell^4$ and we have the formula*

$$\delta(g) = \begin{pmatrix} \beta(g) & -\alpha(g) \end{pmatrix} (\pi(g) - 1)^{-1} \begin{pmatrix} \alpha(g) \\ \beta(g) \end{pmatrix}.$$

*b) Suppose that the maps $\alpha$ and $\beta$ both vanish on the subgroup $G \cap \ker(\pi)$. Then, there exists a vector $w = (w_1, w_2) \in \mathbf{F}_\ell^2$ (depending only on $G$) such that $(\alpha(g), \beta(g)) = \pi(g)w - w$ for every element $g \in G$. For those elements $g \in G$ such that $f(g) \neq 0$ and $\pi(g)$ is not unipotent, we have that $\pi_\ell(g)$ fixes the vector $(-1, w_1, w_2, 0) \in \mathbf{F}_\ell^4$.*

**Proof** Let $g \in G$ be an element such that $f(g) \neq 0$. Since $G \in \mathrm{Fix}(\ell^2)$, it follows from Remark 1.1 that $\pi_{\ell^2}(g) \in \mathrm{Sp}_4(\mathbf{Z}/\ell^2)$ fixes a submodule of $\mathcal{T}/\ell^2\mathcal{T}$ of order $\ell^2$. It is already clear that $\pi_{\ell^2}(g)$ fixes the mod-$\ell^2$ image of $\ell e_4$; it must, therefore, be the case that $\pi_{\ell^2}(g)$ fixes a vector $u \in \mathcal{T}/\ell^2\mathcal{T}$ such that $\ell e_4$ modulo $\ell^2$ is $\ell u$ (that is, $u = (\ell u_1, \ell u_2, \ell u_3, u_4)$ with $u_4 \neq 0$) or that there is a vector $v \in \mathcal{T}/\ell^2\mathcal{T}$ with $\ell v \neq \ell\pi_{\ell^2}(e_4)$ such that $g$ fixes $\ell v$. The first case is impossible, as one verifies easily that the first entry of $g.u$ equals the first entry of $u$ plus $f(g)u_4 \neq 0$. We, therefore, have a vector $v \in \mathcal{T}/\ell^2\mathcal{T}$ such that $\ell g.v = \ell v$, or equivalently, such that the image modulo $\ell$ of $v$ is fixed under multiplication by $\pi_{\ell^2\to\ell}(g)$. Write $\overline{v} = (v_1, v_2, v_3, v_4) \in \mathbf{F}_\ell^4$ for the image modulo $\ell$ of $v$. We observe that the second and third entries of $\pi_\ell(g)\overline{v}$ are given by the vector $v_1(\alpha(g), \beta(g)) + \pi(g).(v_2, v_3)$. The fact that $\pi_\ell(g).\overline{v} = \overline{v}$ now implies

$$(v_2, v_3) = v_1(\alpha(g), \beta(g)) + \pi(g).(v_2, v_3). \tag{5.2}$$

If $v_1 \neq 0$, then it follows that $(\alpha, \beta)(g) = -v_1^{-1}(\pi(g)\,(v_2, v_3) - (v_2, v_3))$, and we get the first claim of part (a) when we take $w_g = -v_1^{-1}(v_2, v_3)$. We, therefore, assume that $v_1 = 0$. In this case, the above equation implies that $(v_2, v_3)$ is invariant under multiplication by $\pi(g)$ (in particular, this implies that $\pi(g)$ is unipotent). It follows from the above discussion that the final entry of $\pi_2(g).\overline{v}$ is equal to

$$\begin{pmatrix}\beta - \alpha\end{pmatrix} \pi(g) \begin{pmatrix} v_2 \\ v_3 \end{pmatrix} + v_4 = \begin{pmatrix}\beta & -\alpha\end{pmatrix} \begin{pmatrix} v_2 \\ v_3 \end{pmatrix} + v_4.$$

Since we have $\pi_2(g).\overline{v} = \overline{v}$, it follows that $\begin{pmatrix}\beta - \alpha\end{pmatrix}\begin{pmatrix} v_2 \\ v_3 \end{pmatrix} = 0$. It is now clear that the vector $(\beta, -\alpha) \in \mathbf{F}_\ell^2$ must be a scalar multiple of $(v_3, -v_2)$, and so $(\alpha, \beta)(g)$ is a scalar multiple of $(v_2, v_3)$. Then, we take $w_g$ to be any vector in the subspace $\langle \overline{e}_2, \overline{e}_3 \rangle$ that is *not* a scalar multiple of $(v_2, v_3)$. Since the operator $\pi(g)$ is not the identity, it cannot also fix $w_g$. It is now easily verified that $\pi(g).w_g - w_g$ is a nontrivial scalar multiple of $(v_2, v_3)$ and thus also of $(\alpha(g), \beta(g))$; after replacing $w_g$ with a suitable multiple of itself, we even get $\pi(g).w_g - w_g = (\alpha(g), \beta(g))$, and the first claim of part (a) follows.

Now, suppose that $f(g) \neq 0$ and $\pi(g)$ is not unipotent. We have seen above that $\pi_\ell(g)$ fixes a vector $(v_1, v_2, v_3, v_4) \in \mathbf{F}_\ell^4$ and that we must have $v_1 \neq 0$, because otherwise $\pi(g)$ would be unipotent. We have shown that in this case, we may take $w_g = -v_1^{-1}(v_2, v_3)$. Since $\pi(g)$ fixes both $-v_1^{-1}(v_1, v_2, v_3, v_4) = (-1, (w_g)_1, (w_g)_2, -v_1^{-1}v_4)$ and $(0,0,0,1)$, we get the claim that $(-1, (w_g)_1, (w_g)_2, 0)$ is fixed by $\pi(g)$. Now, the final entry of $\pi(g)(-1, (w_g)_1, (w_g)_2, 0)$ is given by

$$0 = -\delta(g) + \beta'(g)(w_g)_1 + \alpha'(g)(w_g)_2 = -\delta(g) + \begin{pmatrix}\beta'(g) \alpha'(g)\end{pmatrix} \begin{pmatrix} (w_g)_1 \\ (w_g)_2 \end{pmatrix}. \tag{5.3}$$

Since from the discussion at the start of this section we have $(\beta', \alpha')(g) = \big(\beta(g) - \alpha(g)\big)\pi(g)$and we have shown above that $(\alpha, \beta)(g) = (\pi(g) - 1).w_g$, we get

$$\delta(g) = \begin{pmatrix}\beta(g) & -\alpha(g)\end{pmatrix} \pi(g)(\pi(g) - 1)^{-1} \begin{pmatrix} \alpha(g) \\ \beta(g) \end{pmatrix}. \tag{5.4}$$

Now, one sees that the above is equivalent to the formula claimed in part (a) by noting that $\pi(g)(\pi(g) - 1)^{-1} = (\pi(g) - 1)^{-1} + 1$ and $\begin{pmatrix}\beta(g) & -\alpha(g)\end{pmatrix}\begin{pmatrix}\alpha(g) & \beta(g)\end{pmatrix}^{\top} = 0$.

We now assume the hypothesis of part (b), which implies that the map $(\alpha, \beta) : G \to \mathbf{F}_\ell^2$ induces a map $(\hat{\alpha}, \hat{\beta}) : \pi(G) \to \mathbf{F}_\ell^2$. We observe directly from multiplying matrices that we have the identity

$$(\hat{\alpha}, \hat{\beta})(xy) = (\hat{\alpha}, \hat{\beta})(x) + x.(\hat{\alpha}, \hat{\beta})(y) \tag{5.5}$$

for any $x, y \in \pi(G)$. The map $(\hat{\alpha}, \hat{\beta})$ is, therefore, a cocycle with respect to the obvious action of $\pi(G)$ on $\mathbf{F}_\ell^2$. The claim of part (b) is equivalent to saying that $(\hat{\alpha}, \hat{\beta})$ is also a coboundary, so it suffices to prove that the first group cohomology of $\pi(G)$ with coefficients in the $\pi(G)$-module $\mathbf{F}_\ell^2$ is trivial. We first assume that we do not have $\ell = 2$ and $\pi(G) = \mathrm{SL}_2(\mathbf{F}_2)$ and prove the vanishing of the first group cohomology by appealing to Sah's Lemma [6, Lemma VI.10.2], which implies as an immediate corollary that if a group $A$ acting on a module $M$ has a central element $x$ such that $x - 1$ acts as an automorphism on $M$, then the first group homology $H^1(A, M)$ vanishes. In our case, we need to show that $\pi(G)$ has a central element $x$ such that the operator $x - 1$ is invertible. Either we have $\ell = 2$ and $\pi(G) = A_3$ (which is a nontrivial abelian group), or we have $\ell \geq 3$ and then Proposition 5.1(e) implies that $\pi(G)$ has a nontrivial central element. In either case, choose an element $x \neq 1$ lying in the center of $\pi(G)$. Since a unipotent operator cannot lie in the center of an irreducible subgroup of $\mathrm{SL}_2(\mathbf{F}_\ell)$, the operator $x - 1$ must be invertible, and we have proved part (b) except in the exceptional case that $\ell = 2$ and $\pi(G) = \mathrm{SL}_2(\mathbf{F}_2)$. In this case, we consider the values that $(\overline{\alpha}, \overline{\beta})$ takes on the elements $u_1 := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $u_2 := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, noting that together these elements generate $\mathrm{SL}_2(\mathbf{F}_2)$. It follows from part (a) that there exist scalars $c_1, c_2 \in \mathbf{F}_2$ such that $(\hat{\alpha}, \hat{\beta})(u_1) = c_1(1, 0)$ and $(\hat{\alpha}, \hat{\beta})(u_2) = c_2(0, 1)$. Taking $w = (c_2, c_1) \in \mathbf{F}_2^2$, we get the desired statement. ∎

***Lemma 5.3*** *If $G$ is a counterexample, then the maps $\alpha$ and $\beta$ vanish on the subgroup $G \cap \ker(\pi)$.*

**Proof** Suppose that there is an element $g \in G \cap \ker(\pi)$ with $(\alpha, \beta)(g) \neq (0, 0)$. Using the identity in (5.5), it is easy to verify that for any $h \in G$ we have $(\alpha(hgh^{-1}), \beta(hgh^{-1})) = \pi(h)(\alpha, \beta)(g)$. Since $\pi(G)$ is irreducible, there is some $h \in G$ such that the set $\{\pi(h).(\alpha, \beta)(g), (\alpha, \beta)(g)\}$ is linearly independent. We note that the map $(\alpha, \beta)$ is a homomorphism when restricted to $G \cap \ker(\pi)$ thanks to the identity (5.5). It follows that given any vector $(\alpha_0, \beta_0) \in \mathbf{F}_\ell^2$, there is an element $g \in G \cap \ker(\pi)$ with $(\alpha, \beta)(g) = (\alpha_0, \beta_0)$. We shall show that for any $g \in G \cap \ker(\pi)$ such that $(\alpha, \beta)(g) \neq (0, 0)$, we have $f(g) \neq 0$. Under the assumption that such an element $g$ exists, this implies an obvious contradiction and thus will prove the statement in the lemma.

In order to prove our claim that $f(g) \neq 0$ for any $g \in G \cap \ker(\pi)$ such that $(\alpha, \beta)(g) \neq (0, 0)$, we consider the cases $\pi(G) = \mathrm{SL}_2(\mathbf{F}_\ell)$ and $\pi(G) \subsetneq \mathrm{SL}_2(\mathbf{F}_\ell)$ separately. We first assume that $\pi(G) = \mathrm{SL}_2(\mathbf{F}_\ell)$. Assume that there exists an element $h \in G \cap \ker(\pi)$ with $(\alpha, \beta)(h) \neq (0, 0)$ and $f(h) = 0$. Let $y \in \mathbf{F}_\ell^2$ be a vector that is not a scalar multiple of $(\alpha, \beta)(h)$. Then, $\pi(G)$ contains a nontrivial unipotent operator $u$, which fixes $y$, so that $uw - w$ is a scalar multiple of $y$ for each $w \in \mathbf{F}_\ell^2$. There exists some $g \in \pi^{-1}(u) \subset G$ with $f(g) \neq 0$, because otherwise, the fact that any nontrivial unipotent operator in $\mathrm{SL}_2(\mathbf{F}_\ell)$ normally generates all of $\mathrm{SL}_2(\mathbf{F}_\ell)$ implies that $f$ is trivial on all of $G$. Now, Lemma 5.2(a) implies that $(\alpha,\beta)(g)$ is a scalar multiple of $y$. We have $\pi(hg)=u$ and $f(hg)\neq 0$, while the identity (5.5) implies that $(\alpha,\beta)(hg)=(\alpha,\beta)(h)+(\alpha,\beta)(g)$, which is not a scalar multiple of $y$, thus contradicting Lemma 5.2(a).

We now assume that $\pi(G)\subsetneq \mathrm{SL}_2(\mathbf{F}_\ell)$. Assume again that there exists an element $h\in G\cap\ker(\pi)$ with $(\alpha,\beta)(h)\neq(0,0)$ and $f(h)=0$. Since the set of all such elements is clearly closed under conjugation and group multiplication, this implies that in fact for every vector $(\alpha_0,\beta_0)\in\mathbf{F}_\ell^2$ there is an element $h\in G\cap\ker(\pi)$ with $(\alpha,\beta)(h)=(\alpha_0,\beta_0)$ and $f(h)=0$. There exists an element $g\in G\setminus\ker(\pi)$ with $f(g)\neq 0$, because otherwise $f$ would be trivial on $G$. Since $\pi(G)$ is a proper irreducible subgroup of $\mathrm{SL}_2(\mathbf{F}_\ell)$, we know that $\pi(g)$ is not unipotent by Lemma 5.2(b), (c), and so we may apply Lemma 5.2(a) to get the formula given there for $\delta(g)$. We may do the same to get a formula for $\delta(hg)$ for any $h\in G\cap\ker(\pi)\cap\ker(f)$ since then $\pi(hg)=\pi(g)$ and $f(hg)=f(g)\neq 0$. Using the previously noted fact that $(\alpha,\beta)(hg)=(\alpha,\beta)(h)+(\alpha,\beta)(g)$ along with the easily verified fact that $\delta(hg)=\delta(h)+\delta(g)$, we get the below general formula for $\delta(hg)$.

$$\delta(hg)=\left(\begin{pmatrix}\beta(h) & -\alpha(h)\end{pmatrix}+\begin{pmatrix}\beta(g) & -\alpha(g)\end{pmatrix}\right)(\pi(g)-1)^{-1}\left(\begin{pmatrix}\alpha(h)\\ \beta(h)\end{pmatrix}+\begin{pmatrix}\alpha(g)\\ \beta(g)\end{pmatrix}\right). \tag{5.6}$$

We now expand the above formula, use the easily verified fact that $\delta(hg)=\delta(h)+\delta(g)$, and subtract the formula for $\delta(g)$ from (5.6) to get

$$\begin{aligned}\delta(h)=\begin{pmatrix}\beta(h) & -\alpha(h)\end{pmatrix}(\pi(g)-1)^{-1}\begin{pmatrix}\alpha(g)\\ \beta(g)\end{pmatrix}+\begin{pmatrix}\beta(g) & -\alpha(g)\end{pmatrix}(\pi(g)-1)^{-1}\begin{pmatrix}\alpha(h)\\ \beta(h)\end{pmatrix}\\ +\begin{pmatrix}\beta(h) & -\alpha(h)\end{pmatrix}(\pi(g)-1)^{-1}\begin{pmatrix}\alpha(h)\\ \beta(h)\end{pmatrix}.\end{aligned} \tag{5.7}$$

We now use the fact that the final term on the right-hand side of (5.7) is in some sense "quadratic" while the other terms in (5.7) are "linear" in order to derive a contradiction. More precisely, we consider the cases when $\ell\geq 3$ and $\ell=2$ separately as follows. We note in either case that $(\alpha,\beta,\delta)(h^2)=2(\alpha,\beta,\delta)(h)$ for any $h\in G\cap\ker(\pi)$. If $\ell\geq 3$, then choose an element $h\in G\cap\ker(\pi)$ such that $(\alpha(h),\beta(h))$ is not an eigenvector of $\pi(g)-1$, which ensures that

$$\begin{pmatrix}\beta(h) & -\alpha(h)\end{pmatrix}(\pi(g)-1)^{-1}\begin{pmatrix}\alpha(h)\\ \beta(h)\end{pmatrix}\neq 0. \tag{5.8}$$

Then, applying the formula (5.7) to $h^2$ and subtracting (5.6), we get

$$2\begin{pmatrix}\beta(h) & -\alpha(h)\end{pmatrix}(\pi(g)-1)^{-1}\begin{pmatrix}\alpha(h)\\ \beta(h)\end{pmatrix}=0, \tag{5.9}$$

which contradicts (5.8). Now if $\ell=2$, we deduce from the relations given in Section 3 that $\alpha$, $\beta$, and $\delta$ are all homomorphisms when restricted to $G\cap\ker(\pi)$. Noting that

$\pi(g) \in \left\{ \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$, we now compute

$$\begin{pmatrix} \beta(h) & -\alpha(h) \end{pmatrix} (\pi(g) - 1)^{-1} \begin{pmatrix} \alpha(h) \\ \beta(h) \end{pmatrix} = \alpha(h)^2 + \alpha(h)\beta(h) + \beta(h)^2.$$

Choosing elements $h_1, h_2 \in G \cap \ker(\pi)$ such that $(\alpha, \beta)(h_1) = (1, 0)$ and $(\alpha, \beta)(h_2) = (0, 1)$, putting $h = h_1 + h_2$ into (5.7) and then subtracting the formula (5.7) for $h_1$ and for $h_2$ yields the desired contradiction. ∎

***Corollary 5.4*** *Let $G \subset \mathrm{Sp}(\mathcal{T})$ be a counterexample satisfying that $\pi(G) \subset \mathrm{SL}_2(\mathbf{F}_\ell)$ is an irreducible subgroup. We then have $\overline{G} \cong \pi(G) \times C_\ell$ or $\overline{G} \cong \pi(G)$.*

**Proof** Clearly, $\overline{G}$ is an extension of $\pi(G)$ by $\overline{G}_\ell \cap \pi_\ell(\ker(\pi))$. Since Lemma 5.3 says that the maps (homomorphisms) $\alpha$ and $\beta$ vanish on the latter, we get that $\overline{G} \cap \pi_\ell(\ker(\pi)) \subset \langle x_4 \rangle \cong C_\ell$, where $x_4$ is the element defined in Section 3. Moreover, it follows from the discussion there that $x_4$ commutes with everything in $\pi_\ell(\ker(\pi)) \subset \mathrm{Sp}_4(\mathcal{T}/\ell\mathcal{T})$, which directly implies the desired statement. ∎

## 5.2 The nonexistence of counterexamples for $\ell \geq 3$

We assume throughout this subsection that $\ell \geq 3$ and proceed to prove the first statement of Theorem 5.1.

**Proof of Theorem 5.1 for $\ell \geq 3$** We first consider the case that $\overline{G} \cong \mathrm{SL}_2(\mathbf{F}_\ell) \times C_\ell$. In this case, we claim that $f$ is trivial on $G \cap \ker(\pi_\ell)$. To see this, assume that $f$ is nontrivial on $G \cap \ker(\pi_\ell)$. Let $g \in G$ be an element such that $\pi(g)$ is not unipotent, and let $h \in G$ be an element such that $\pi_\ell(h) = x_4$. Then, after possibly translating $g$ or $h$ by an element of $G \cap \ker(\pi_\ell) \setminus \ker(f) \neq \varnothing$, we get that $f(g) = f(hg) \neq 0$. Since $h \in \ker(\pi)$, we have already seen that $(\alpha, \beta)(hg) = (\alpha, \beta)(g)$; meanwhile, one verifies in a straightforward manner that $\delta(hg) = \delta(g) + 1$. Then, putting $hg$ into the formula given by Lemma 5.2(a) yields the desired contradiction.

The fact that the homomorphism $f$ is trivial on $G \cap \ker(\pi_\ell)$ implies that it induces a homomorphism $\overline{f} : \overline{G}_\ell \to \mathbf{Z}/\ell\mathbf{Z}$. Write $\overline{G}_\ell = S \times \langle x_4 \rangle$, where $S$ is a component isomorphic to $\pi(G)$. It follows from Proposition 5.1(a) that $\overline{f}$ is trivial on $S$ except in the case that $\ell = 3$ and $S \cong \mathrm{SL}_2(\mathbf{F}_3)$. Assume for the moment that we are not in that exceptional case. Then we must have $\overline{f}_3(x_4) \neq 0$, because otherwise $f$ would be trivial on $G$. Let $g, h \in G$ be elements such that $\pi_\ell(h) = x_4$, $\pi_\ell(g) \in S$, and $\pi(g)$ is not unipotent. Then $f(hg) = 1 \in \mathbf{Z}/\ell$, so that we may apply Lemma 5.2(a) to get the formula given there for $\delta(hg)$. Since $\ell \geq 3$, we have $f(h^2 g) = 2 \neq 0 \in \mathbf{Z}/\ell$, and since again $\delta(h^2 g) = \delta(hg) + 1$ and $(\alpha, \beta)(h^2 g) = (\alpha, \beta)(hg)$, the formula given by Proposition 5.2(a) applied to $\delta(h^2 g)$ implies a contradiction. It follows that there is no counterexample for these cases.

We now assume that $\ell = 3$ and $S \cong \mathrm{SL}_2(\mathbf{F}_3)$. We claim that there is a subgroup $S' \subset \overline{G}_3$ with $\overline{G}_3 = S' \times \langle x_4 \rangle$ such that $\overline{f}$ is trivial on $S'$, so that the above argument works in this case also by replacing $S$ with $S'$. If $\overline{f}$ is trivial on $S$, then we take $S' = S$ and are done, so we assume that $\overline{f}$ is not trivial on $S$. Note that there exists $g \in S$ with $\overline{f}(g) \neq 0$ such that $\pi(g)$ is not unipotent, since by Proposition 5.1(a)(ii) we have $\ker(\overline{f}) \cap \pi(G) \subset Q_8$

and certainly there are nonunipotent matrices in $\mathrm{SL}_2(\mathbf{F}_3)\backslash Q_8$. Now, again letting $h \in G$ be an element such that $\pi_3(h) = x_4$, if we assume that $\overline{f}(h) = 0$ and apply a similar argument as was used above to the formula for $\delta(hg)$ given by Proposition 5.2(a), we get a contradiction. Therefore, the homomorphism $\overline{f}$ is nontrivial on $\langle x_4 \rangle$ and we may define $S'$ to be $\{x_4^{-\overline{f}_3(y)\overline{f}(x_4)^{-1}} y \mid y \in S\}$; it is easy to check that $S' \subset \overline{G}_3$ is a subgroup contained in the kernel of $\overline{f}$ and satisfying $\overline{G} = S' \times \langle x_4 \rangle$. We have thus shown that there are no counterexamples in the case that $\overline{G} \cong \mathrm{SL}_2(\mathbf{F}_\ell) \times C_\ell$.

We now consider the case that $\overline{G}_\ell \cong \pi(G)$. First suppose that there is an element $h \in G \cap \ker(\pi_\ell)$ with $f(h) \neq 0$. We shall show that $\overline{G}$ fixes a two-dimensional subspace of $\mathcal{T}/\ell\mathcal{T}$, and that therefore $G$ is not a counterexample by Proposition 2.3(c). Let $x \in \overline{G} \cong \pi(G)$ be any nonunipotent operator and lift it to an element $g \in G$ with $\pi_\ell(g) = x$. If $f(g) = 0$, we let $g' = hg$, and we let $g' = g$ otherwise, so that $f(g') \neq 0$. Now by Lemma 5.2(b), there is a vector $w = (w_1, w_2) \in \mathbf{F}_\ell^2$ such that $x = \pi_\ell(g')$ fixes the vector $(-1, w_1, w_2, 0) \in \mathbf{F}_\ell^4$. Now, Proposition 5.1(d) says that the subset of nonunipotent operators in $\pi(G)$ generates $\pi(G)$; it follows that the whole group $\overline{G}$ fixes $(-1, w_1, w_2, 0)$. Since the group $\overline{G}_\ell$ also fixes $(0,0,0,1)$, it fixes the two-dimensional subspace generated by these two vectors and so $G$ is not a counterexample.

Now, suppose that the homomorphism $f$ is trivial on $G \cap \ker(\pi_\ell)$, so that $f$ induces a homomorphism $\overline{f} : \overline{G} \to \mathbf{Z}/\ell$. We know that $\overline{f}$ cannot be trivial on $\overline{G} \cong \pi(G)$, because otherwise $f$ would be trivial on all of $G$, so we are left with the only possibility being that $\ell = 3$ and $\overline{G}_3 \cong \mathrm{SL}_2(\mathbf{F}_3)$ with the induced homomorphism $\overline{f} : \mathrm{SL}_2(\mathbf{F}_3) \to \mathbf{Z}/3$ being a surjection whose kernel is $Q_8$. There exist nonunipotent operators in $\mathrm{SL}_2(\mathbf{F}_3)\backslash \ker(\overline{f}_3)$, which generate all of $\mathrm{SL}_2(\mathbf{F}_3)$ by Proposition 5.1(d). Then, the argument proceeds in a similar fashion: we know from Lemma 5.2(b) that there is a vector $w = (w_1, w_2) \in \mathbf{F}_3^2$ such that $x \in \overline{G}_3\backslash \ker(\overline{f}_3)$ fixes the vector $(-1, w_1, w_2, 0) \in \mathbf{F}_\ell^4$ if $x$ is not unipotent; since the set of such elements generates all of $\overline{G}_3$, we get that the whole group $\overline{G}_3$ fixes the two-dimensional subspace spanned by $\{(-1, w_2, w_3, 0), (0,0,0,1)\}$ and, therefore, $G$ is not a counterexample. ∎

## 5.3 Classifying counterexamples for $\ell = 2$

In this subsection, we assume that $\ell = 2$ and finish the proof of Theorem 5.1. We first present the following useful lemma.

***Lemma 5.5*** *Let $S \subset \overline{\mathrm{S}}_2$ be the subgroup isomorphic to $S_3$, which fixes the subspace $\langle \overline{e}_1, \overline{e}_4 \rangle \subset \mathcal{T}/\ell\mathcal{T}$ and acts as $\mathrm{SL}_2(\mathbf{F}_2)$ on its complement subspace $\langle \overline{e}_2, \overline{e}_3 \rangle \subset \mathcal{T}/\ell\mathcal{T}$, and let $x_4 \in \overline{\mathrm{S}}_2$ be the element defined in* Section 3. *Suppose that $G \subset \mathrm{S}_2$ is a subgroup satisfying one of the following:*

(i) $\overline{G} = \langle x_4 \rangle \times S$;
(ii) $\overline{G} \subset \langle x_4 \rangle \times S$ *is the subgroup isomorphic to $A_3 \times C_2$; or*
(iii) $\overline{G} \subset \langle x_4 \rangle \times S$ *is the subgroup given by $\{(x, \phi(x)) \in S \times \langle x_4 \rangle \mid x \in S\}$, where $\phi : S \to \langle x_4 \rangle$ is the unique surjective homomorphism.*

*Then, the only nontrivial $G$-invariant sublattices of $\mathcal{T}$ that properly contain $\ell\mathcal{T}$ are $M_1 := \langle \ell\mathcal{T}, e_1, e_4 \rangle$, $M_2 := \langle \ell\mathcal{T}, e_2, e_3 \rangle$, $L_1$ and $L_3$, where the $L_i$'s are as in* (2.7).

https://doi.org/10.4153/S0008414X20000759 Published online by Cambridge University Press

**Proof** We write $\overline{M}_1$, $\overline{M}_2$, $\overline{L}_1$, and $\overline{L}_3$ for the subspaces of $\mathcal{T}/2\mathcal{T}$ given by the quotients by $2\mathcal{T}$ of $M_1$, $M_2$, $L_1$, and $L_3$, respectively. The statement of the lemma is equivalent to saying that the only proper, nontrivial $\overline{G}_2$-invariant subspaces of $\mathcal{T}/2\mathcal{T}$ are $\overline{M}_1$, $\overline{M}_2$, $\overline{L}_1$, and $\overline{L}_3$.

Note that in cases (i), (ii), and (iii) of the statement, the only proper nontrivial $\overline{G}_2$-invariant subspace of $\overline{M}_1$ is $\langle \overline{e}_4 \rangle = L_3$, while $\overline{M}_2$ has no proper, nontrivial $\overline{G}_2$-invariant subspaces. Choose any vector $v \in \mathcal{T}/\ell\mathcal{T}$, and let $\overline{L} \in \mathcal{T}/\ell\mathcal{T}$ be the smallest $\overline{G}_2$-invariant subspace containing $v$. Since the vector space $\mathcal{T}/\ell\mathcal{T}$ can be decomposed as the direct sum $\overline{M}_1 \oplus \overline{M}_2$, we may write $v = m_1 + m_2$ for some vectors $m_1 \in \overline{M}_1$ and $m_2 \in \overline{M}_2$.

We claim that $\overline{L} = \overline{L}_1 \oplus \overline{L}_2$, where $\overline{L}_i$ is the smallest $\overline{G}_2$-invariant subspace of $\overline{M}_i$ containing $m_i$ for $i = 1, 2$. If $m_1 = 0$ or $m_2 = 0$, this is trivially true, so we assume that $m_1, m_2 \neq 0$. It is straightforward to check for cases (i), (ii), and (iii) given in the statement that given any element $m_2' \in \overline{M}_2 \backslash \{0, m_2\}$, there is an element of $\overline{G}_2$, which sends $v = m_1 + m_2$ to $m_1 + m_2'$; taking their difference, we get that $0 \neq m_2 - m_2' \in \overline{M}_2$ lies in $L$. Since in all of the cases in the statement, $\overline{G}_2$ acts irreducibly on $\overline{M}_2$, we get $\overline{L}_2 = \overline{M}_2 \subsetneq L$. Now since $m_2 \in \overline{L}$, we have $v - m_2 = m_1 \in \overline{L}$, so that $\overline{L}_1$ by definition is contained in $\subset \overline{L}$. We, therefore, have $\overline{L}_1 \oplus \overline{L}_2 \subset \overline{L}$, and since $\overline{L}_1 \oplus \overline{L}_2$ is a $\overline{G}_2$-invariant subspace containing $v$, this inclusion of subspaces is in fact an equality, whence our claim. The statement of the lemma follows now from the observation that $\overline{L}_1 = \overline{M}_2 \oplus \overline{L}_3$. ■

**Proof of Theorem 5.1 for $\ell = 2$** We first consider the case that $\overline{G} \cong \pi(G) \times C_2$. Here, we have that $f$ is trivial on $G \cap \ker(\pi_2)$ by the exact same argument we used in Section 3 under the case that $\ell = 3$ and $\overline{G} \cong \pi(G) \times C_\ell$, so we again have an induced homomorphism $\overline{f} : \overline{G} \to \mathbf{Z}/2$. As before, we write $\overline{G} = S \times \langle x_4 \rangle$, where $S \cong \pi(G)$. We also have that $f(x_4) \neq 0$ by the same argument as was used under Case 1. Fix an element $h \in G$ with $\pi_2(h) = x_4$. We now claim that $G$ is a counterexample if and only if for each element $g \in G$ such that $\pi(g)$ is not unipotent, we have either (i) $f(g) = 1$ and $\delta(g)$ is equal to the expression in terms of $(\alpha, \beta)(g)$ in the formula given in Lemma 5.2(a), or (ii) $f(g) = 0$ and $\delta(g)$ is *not* equal to the expression in terms of $(\alpha, \beta)(g)$ in the formula given in Lemma 5.2(a). Indeed, if such an element $g \in G$ satisfies neither (i) nor (ii), then either $g$ or $hg$ clearly violates the conclusion of Lemma 5.2(a), which contradicts the fact that $G \in \mathrm{Fix}(4)$. Suppose conversely that either (i) or (ii) holds for all such elements $g \in G$; we will show that now $G$ is a counterexample. For each element $g \in G$ such that $\pi(g)$ is unipotent and fixes a nontrivial vector $v = (v_1, v_2) \in \mathbf{F}_2^2$, we have that $\pi_2(g)$ fixes the two-dimensional subspace of $\mathcal{T}/2\mathcal{T}$ spanned by $\{(0, v_1, v_2, 0), (0, 0, 0, 1)\}$. Meanwhile, for each $g \in G$ such that $\pi(g) = \pi(hg)$ is not unipotent, Lemma 5.2(b) says that for some vector $w = (w_1, w_2) \in \mathbf{F}_2^2$, either $\pi_2(g)$ or $\pi_2(hg)$ fixes the vector $(-1, w_1, w_2, 0) \in \mathcal{T}/2\mathcal{T}$. An easy computation shows that if $\pi_2(g)$ fixes $(-1, w_1, w_2, 0)$, then $\pi_2(hg)$ does not fix $(-1, w_1, w_2, 0)$ but $hg$ does fix $(2, 2, 2, 1) \in \mathcal{T}/2\mathcal{T}$, and vice versa. Moreover, the subspace of $\mathcal{T}/2\mathcal{T}$ fixed by $\pi_2(g)$ contains the vector $(0, 0, 0, 1)$ but can have dimension at most 2 (otherwise $\pi(g) - 1$ would be noninvertible so that $\pi(g)$ would be unipotent). It follows that there is no two-dimensional subspace of $\mathcal{T}/2\mathcal{T}$ fixed by the whole group $\overline{G}$. Since, of course, $f$ is not trivial on $G$, we get that $G$ is a counterexample by Proposition 2.3(c) and by a quick check of quotients of the $G$-stable sublattices provided by Lemma 5.5. Now, it is clear that for any subgroup $H \subset \ker(\pi_2) \cap \ker(f)$, the group generated by the subgroups $G$ and $H$ is also a counterexample since multiplying by elements in $H$ will not affect their images under $\alpha$, $\beta$, $\delta$, or $f$.

We now consider the case that $\ell = 2$ and $\overline{G} \cong \pi(G)$. We first eliminate the possibility that $\overline{G} \cong \pi(G) = A_3$. Indeed, if we have $\overline{G} \cong \pi(G) = A_3$, then the group $\overline{G} \cong \pi(G)$ is cyclic and there is some element $g \in G$ with $f(g) \neq 0$ such that $\pi_2(g)$ generates $\overline{G}$ (otherwise $f$ would be trivial on $G$). Then, by Lemma 5.2(a), the operator $\pi_2(g)$ fixes a vector of the form $(-1, w_1, w_2, 0) \in \mathcal{T}/2\mathcal{T}$, implying that all of $\overline{G}$ fixes the subspace of $\mathcal{T}/2\mathcal{T}$ spanned by $\{(-1, w_1, w_2, 0), (0, 0, 0, 1)\}$ and so $G$ is not a counterexample.

We, therefore, assume that $\overline{G} \cong \pi(G) = \mathrm{SL}_2(\mathbf{F}_2)$. Let $w = (w_1, w_2) \in \mathbf{F}_2^2$ be the vector provided by Lemma 5.2(b) applied to $G$, and let $S \subset \overline{G}_2 \times \langle x_4 \rangle$ be the subgroup that fixes the vector $(-1, w_1, w_2, 0)$. A straightforward calculation similar to the ones done in the proof of Lemma 5.2(a) shows that the first three entries of $(-1, w_1, w_2, 0)$ are fixed under multiplication by every matrix in $\overline{G} \times \langle x_4 \rangle$; meanwhile, it is immediate that $x_4$ acts by changing the final entry of any vector in $\mathcal{T}/\ell\mathcal{T}$ whose first entry is nontrivial. It follows that for each $y \in \overline{G}_2$ we have $y \in S$ or $x_4 y \in S$ and so $S \cong \mathrm{SL}_2(\mathbf{F}_2)$. If $\overline{G}_2 = S$, then $\overline{G}_2$ is not a counterexample by Proposition 2.3(c) because it fixes the subspace of $\mathcal{T}/\ell\mathcal{T}$ spanned by $\{(-1, w_1, w_2, 0), (0, 0, 0, 1)\}$. The only alternative is that $\overline{G}_2 = \{x_4^{\phi(x)} y \mid y \in S\}$ where $\phi$ is the surjection from $\mathrm{SL}_2(\mathbf{F}_2)$ to $\mathbf{Z}/2$. In this case, since not everything in $\overline{G}_2$ fixes $(-1, w_1, w_2, 0)$; the unipotent elements already each fix some two-dimensional subspace; and the nonunipotent elements do fix the two-dimensional subspace spanned by $\{(-1, w_1, w_2, 0), (0, 0, 0, 1)\}$ but cannot fix a larger subspace (as was argued above), we get that $\overline{G}$ does not fix a two-dimensional subspace of $\mathcal{T}/\ell\mathcal{T}$. Therefore, as long as $f$ is not trivial on $G$ (which means that either $f$ is nontrivial on $G \cap \ker(\pi_2)$ or that it factors through the only nontrivial homomorphism from $\overline{G} \cong \mathrm{SL}_2(\mathbf{F}_2)$ to $\mathbf{Z}/2$), we have that $G$ is a counterexample by Proposition 2.3(c) and by a quick check of quotients of the $G$-stable sublattices provided by Lemma 5.5. Now, it is clear as before that for any subgroup $H \subset \ker(\pi_2) \cap \ker(f)$, the group generated by the subgroups $G$ and $H$ is also a counterexample because multiplying by elements in $H$ will not affect images under $\alpha$, $\beta$, and $\delta$; since each element of $\overline{G}_2$ fixes a two-dimensional subgroup of $\mathbf{F}_2^4$, we do not need $f$ to take a certain value on any particular element of $\overline{G}_2$. ∎

**Acknowledgment** The authors would like to extend their gratitude to J.-P. Serre for providing J.C. with his (unpublished) letter to Katz [11] which in large part inspired this whole project, and for graciously giving permission to discuss it in this work. We would also like to thank Drew Sutherland for helpful comments and to thank the anonymous referees for many helpful comments and clarifications.

## References

[1] A. Booker, J. Sijsling, A. Sutherland, J. Voight, and D. Yasaki, *A database of genus-2 curves over the rational numbers*. LMS J. Comput. Math. **19**(2016), suppl. A, 235–254.

[2] J. Cullinan, *A computational approach to the 2-torsion structure of abelian threefolds*. Math. Comput. **78**(2009), no. 267, 1825–1836.

[3] N. Katz, *Galois properties of torsion points on abelian varieties*. Invent. Math. **62**(1981), 481–502.

https://doi.org/10.4153/S0008414X20000759 Published online by Cambridge University Press

[4] A. Landesman, A. Swaminathan, J. Tao, and Y. Xu, *Lifting subgroups of symplectic groups over* $\mathbf{Z}/\ell Z$. Res. Number Theory 3(2017), no. 14, 12 pp.
[5] A. Landesman, A. Swaminathan, J. Tao, and Y. Xu, *Hyperelliptic curves with maximal Galois action on the torsion points of their Jacobians*. Preprint, 2017. https://arxiv.org/pdf/1705.08777.pdf
[6] S. Lang, *Algebra*. Revised 3rd ed., Graduate Texts in Mathematics, 211, Springer-Verlag, New York, NY, 2002.
[7] The LMFDB Collaboration, *The L-functions and modular forms database*. 2019. http://www.lmfdb.org
[8] J. S. Milne, *Abelian varieties*. In: Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, NY, 1986, pp. 103–150.
[9] O. T. O'Meara, *Symplectic groups, mathematical surveys. Vol. 16*. Amer. Math. Soc., Providence, RI, 1978.
[10] J.-P. Serre, *Abelian l-adic representations and elliptic curves*. Research Notes in Mathematics, 7, A K Peters, Ltd., Wellesley, MA, 1998.
[11] J.-P. Serre, *Letter to N. Katz.* Unpublished.
[12] D. Testerman, *$A_1$-type overgroups of elements of orderpin semisimple algebraic groups and the associated finite groups*. J. Algebra 177(1995), no. 1, 34–76.

*Department of Mathematics, Bard College, Annandale-On-Hudson, NY 12401, USA*
*e-mail*: cullinan@bard.edu

*Department of Mathematics and Computer Science, Emory University, Atlanta, GA 30322, USA*
*e-mail*: jeffrey.yelton@emory.edu