ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Number Theory 110 (2005) 178–198

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

Inertia groups and abelian surfaces

A. Silverberg[a,*], Yu. G. Zarhin[b,c]

[a] *Department of Mathematics, Ohio State University, 231 W. 18 Avenue, Columbus, OH 43210–1174, USA*

[b] *Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA*

[c] *Institute for Mathematical Problems in Biology, Russian Academy of Sciences, Pushchino, Moscow Region, Russia*

Received 19 October 2003; revised 15 May 2004

Communicated by D. Goss

Available online 11 November 2004

Dedicated to the memory of Arnold Ross

Abstract

This paper classifies the finite groups that occur as inertia groups associated to abelian surfaces. These groups can be viewed as Galois groups for the smallest totally ramified extension over which an abelian surface over a local field acquires semistable reduction. The results extend earlier elliptic curves results of Serre and Kraus.

Keywords: Abelian varieties; Inertia groups; Semistable reduction

1. Introduction and statements of main results

In this paper we classify the finite groups that occur as inertia groups associated to abelian surfaces. We first prove a group theoretic result, Theorem 1.3, that does not involve the theory of abelian varieties. Namely, we define a class of groups that are inertia groups in the sense of having a unique Sylow p-subgroup with cyclic quotient,

* Corresponding author.

E-mail addresses: silver@math.ohio-state.edu (A. Silverberg), zarhin@math.psu.edu (Yu. G. Zarhin).

0022-314X/$ - see front matter © 2004 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2004.05.015

and also have a compatible system of representations into $\mathrm{GL}_\tau(\mathbb{Z}) \times \mathrm{Sp}_{2\alpha}(\mathbb{Q}_\ell)$ for all $\ell \neq p$ (with τ and α fixed), where $\mathrm{Sp}_{2\alpha}(R)$ denotes the group of $2\alpha \times 2\alpha$ symplectic matrices over R. We determine exactly which groups can occur when $\tau + \alpha \leqslant 2$. In Theorems 1.7 and 1.8 we show that these groups are exactly the groups that occur as inertia groups associated to abelian surfaces over local fields as in [6] (see pp. 354–355; see also Section 4 of [24]). This extends earlier elliptic curve results of Serre and Kraus (see Remark 1.5). The proofs in this paper use results from [24] (see also [25] for related results), which were heavily influenced by the theory of Grothendieck and Serre.

Definition 1.1. We say G is (p, τ, α)-*inertial* if G is a finite group, either $p = 0$ or p is a prime, and τ and α are non-negative integers that satisfy:

(i) if $p = 0$ then G is cyclic; if $p > 0$ then G is an extension of a cyclic group of order prime to p by a p-group;
(ii) for all primes $\ell \neq p$ there is an injection

$$G \hookrightarrow \mathrm{GL}_\tau(\mathbb{Z}) \times \mathrm{Sp}_{2\alpha}(\mathbb{Q}_\ell)$$

such that the projection map onto the first factor is independent of ℓ, and the characteristic polynomial of the projection of any element onto the second factor has integer coefficients independent of ℓ.

Note that (i) implies that G is solvable, and has a unique Sylow p-subgroup if $p > 0$. Note that (ii) implies that the character associated to the representation of G on $\mathbb{Q}_\ell^{2\alpha}$ takes integer values and is independent of ℓ ($\neq p$); it follows that the dimension of the space $(\mathbb{Q}_\ell^{2\alpha})^G$ of G-invariants is independent of ℓ.

Next we define notation for finite groups of small order. Let C_n denote the cyclic group of order n, let D_8 (respectively, Q_8) denote the dihedral (respectively, quaternion) group of order 8, and let T_{12} denote the nontrivial semidirect product of C_3 by C_4. Let H_{24} denote the nontrivial semidirect product of C_3 by C_8. Let H_{20} denote the semidirect product of C_5 by C_4 where a generator of C_4 acts on C_5 as an automorphism of order 2. Let H_{40} denote the semidirect product of C_5 by C_8 where a generator of C_8 acts on C_5 as an automorphism of order 4. (Note that H_{20} is a (normal) subgroup of H_{40}.) Let H_{36} denote the semidirect product of $C_3 \times C_3$ by C_4 where a generator of C_4 takes elements of $C_3 \times C_3$ to their inverses. Let H_{72} denote the semidirect product of $C_3 \times C_3$ by C_8 where a generator of C_8 acts on $C_3 \times C_3$ as an automorphism of order 4. Let H_{128} denote the semidirect product of $Q_8 \times Q_8$ by C_2, with C_2 acting by exchanging the factors. Let H_{160} denote the nontrivial semidirect product of H_{32} by C_5, where H_{32} is the subgroup of H_{128} generated by the C_2, the diagonal $Q_8 \subset Q_8 \times Q_8$, and the center ($\cong C_2 \times C_2$) of the $Q_8 \times Q_8$. Let $\mathcal{S}_{128}$ denote the set of subgroups ($\neq 1$) of H_{128}. Let $\mathcal{S}_4(5)$ denote the set of subgroups of $\mathrm{Sp}_4(\mathbb{F}_5)$ that are nontrivial semidirect products of a subgroup of H_{128} by C_3 and have no elements of order 24.

Note that $\mathrm{SL}_2(\mathbb{F}_3)$ is the only nontrivial semidirect product of Q_8 by C_3.

Definition 1.2. Suppose either $p = 0$ or p is a prime. Define finite sets of finite groups as follows:

$\Sigma_p(0,0) = \{1\}$;
$\Sigma_p(1,0) = \{C_2\}$,

$$\Sigma(0,1) = \{C_2, C_3, C_4, C_6\},$$

$\Sigma_2(0,1) = \Sigma(0,1) \cup \{Q_8, \mathrm{SL}_2(\mathbb{F}_3)\}$,
$\Sigma_3(0,1) = \Sigma(0,1) \cup \{T_{12}\}$,
$\Sigma_p(0,1) = \Sigma(0,1)$ otherwise;

$\Sigma_2(1,1) = \Sigma_2(0,1) \cup \{C_2 \times C_2, C_2 \times C_4, C_2 \times C_6, C_2 \times Q_8, C_2 \times \mathrm{SL}_2(\mathbb{F}_3)\}$,
$\Sigma_p(1,1) = \Sigma_p(0,1)$ otherwise;

$\Sigma_2(2,0) = \Sigma(0,1) \cup \{C_2 \times C_2, D_8\}$,
$\Sigma_3(2,0) = \Sigma(0,1) \cup \{S_3\}$,
$\Sigma_p(2,0) = \Sigma(0,1)$ otherwise;

$$\Sigma(0,2) = \Sigma(0,1) \cup \{C_5, C_8, C_{10}, C_{12}\},$$

$\Sigma_2(0,2) = \Sigma(0,2) \cup$
$\{C_2 \times C_6, C_4 \times C_6, C_3 \times Q_8, C_3 \times D_8, C_6 \times Q_8, H_{160}\} \cup \mathcal{S}_{128} \cup \mathcal{S}_4(5)$,
$\Sigma_3(0,2) = \Sigma(0,2) \cup \{C_3 \times C_3, C_3 \times C_6, S_3, C_3 \times S_3, T_{12}, C_3 \times T_{12}, H_{24}, H_{36}, H_{72}\}$,
$\Sigma_5(0,2) = \Sigma(0,2) \cup \{H_{20}, H_{40}\}$,
$\Sigma_p(0,2) = \Sigma(0,2)$ otherwise.

Note that if $G \in \Sigma_p(\tau, \alpha)$, then G is (p, τ, α)-inertial. (We show in Section 4 that if $G \in \Sigma_p(0,2)$, then $G \subset \mathrm{GL}_2(\mathbb{H}_p) \subset \mathrm{Sp}_4(\mathbb{Q}_\ell)$ for every prime $\ell \neq p$, where $\mathbb{H}_p$ is the quaternion algebra over $\mathbb{Q}$ ramified exactly at p and ∞.) The following result, which we prove in Section 3, gives a converse, under the hypothesis $\tau + \alpha \leqslant 2$.

Theorem 1.3. *If G is (p, τ, α)-inertial, $G \neq 1$, and $\tau + \alpha \leqslant 2$, then $G \in \Sigma_p(\tau, \alpha)$.*

Remark 1.4. The set $\mathcal{S}_4(5)$ consists of the groups

$$\mathrm{SL}_2(\mathbb{F}_3), \mathrm{SL}_2(\mathbb{F}_3) \times C_2, \mathrm{SL}_2(\mathbb{F}_3) \times C_4, \mathrm{SL}_2(\mathbb{F}_3) \times Q_8,$$

and the groups that the computational group theory program GAP [5] calls

$$[48, 28], [48, 29], [48, 33], [96, 67], [96, 191], [96, 202], [192, 1022], [384, 618],$$

where $[a, b]$ denotes the bth group on GAP's list of groups of order a. Note that $[384, 618]$ is the normalizer in $\mathrm{Sp}_4(\mathbb{F}_5)$ of its Sylow 2-subgroup H_{128}, and $\mathrm{SL}_2(\mathbb{F}_3)$, $\mathrm{SL}_2(\mathbb{F}_3) \times C_2$, $[48, 33]$, $[96, 202]$, and $[192, 1022]$ are subgroups of it.

Next, we apply Theorem 1.3 to inertia groups associated with abelian surfaces. Throughout this paper, A is a d-dimensional abelian variety over a field F, v is a discrete valuation on F of residue characteristic $p \geqslant 0$ with perfect residue field, and ℓ is a prime different from p. Fix an extension $\bar{v}$ of v to a separable closure F^s of F, and write $\mathcal{I}_v$ for the inertia subgroup in $\mathrm{Gal}(F^s/F)$ for $\bar{v}$. Let

$$\rho_{\ell,A} : \mathrm{Gal}(F^s/F) \to \mathrm{GL}(V_\ell(A))$$

be the ℓ-adic representation, where $V_\ell(A)$ is the ℓ-adic Tate module. Let $G_{v,A}$ denote the (finite) group of connected components of the Zariski closure of $\rho_{\ell,A}(\mathcal{I}_v)$ in $\mathrm{GL}(V_\ell(A))$. In [6] (see pp. 354–355), Grothendieck defined a subgroup $\mathcal{I}'$ of $\mathcal{I}_v$ with the property that A has semistable reduction at the restriction w of $\bar{v}$ to a finite separable extension of F if and only if $\mathcal{I}_w \subseteq \mathcal{I}'$. In particular, if $\tilde{F}$ denotes the maximal unramified extension of the completion of F at v, then $\mathcal{I}'$ cuts out the smallest Galois extension of $\tilde{F}$ over which A has semistable reduction. We denote the group $\mathcal{I}'$ by $\mathcal{I}_{v,A}$ because of its dependence on A and v. Then $G_{v,A} = \mathcal{I}_v/\mathcal{I}_{v,A}$ (see Theorem 4.2 of [24]), and the finite group $G_{v,A}$ encodes information about the extensions over which A acquires semistable reduction. See Section 6 (especially Corollary 4.1) of [12] for a discussion of $G_{v,A}$ when A is a Jacobian.

Remark 1.5. As shown in [18] (p. 312) and [11], if E is an elliptic curve with non-semistable (i.e., additive) reduction, then $G_{v,E} \in \Sigma_p(0,1)$ if the reduction is potentially good, and $G_{v,E} \in \Sigma_p(1,0)$ if the reduction is potentially multiplicative. Conversely, if $G \in \Sigma_p(0,1)$ (resp., $\Sigma_p(1,0)$), then there are a discrete valuation field F with residue characteristic p and an elliptic curve E over F with additive and potentially good (resp., potentially multiplicative) reduction such that $G_{v,E} \cong G$.

In Theorems 1.7 and 1.8 below we use Theorem 1.3 to extend this elliptic curve result to the case of abelian surfaces. Theorem 1.7 implies, for example, that if A has purely additive and potentially multiplicative reduction, then either $G_{v,A}$ is a cyclic group of order 2, 3, 4, or 6, or $p = 2$ and $G_{v,A}$ is $C_2 \times C_2$ or D_8, or $p = 3$ and $G_{v,A}$ is S_3, while Theorem 1.8 says that all these groups occur.

If w is the restriction of $\bar{v}$ to a finite separable extension L of F, let A_w denote the special fiber of the Néron model of A at w. If A has semistable reduction at w, let $a(A)$ and $t(A)$ (respectively, $a_v(A)$ and $t_v(A)$) denote the abelian and toric ranks of A_w (respectively, A_v). As in [6], we denote them by a, t, a_v, and t_v when the dependence on A is clear. Note that a and t are independent of the valuation w above v at which A has semistable reduction, and we have $t + a = d$. The abelian variety A has semistable reduction at v (i.e., $G_{v,A} = 1$) if and only if $(t - t_v, a - a_v) = (0,0)$. Remark 1.5 implies that if E is an elliptic curve, then $G_{v,E} \in \Sigma_p(t - t_v, a - a_v)$.

Lemma 1.6. *If A is an abelian variety as above, then $G_{v,A}$ is $(p, t-t_v, a-a_v)$-inertial.*

Proof. Definition 1.1(i) is satisfied for $G_{v,A}$ and p, as can be seen by replacing F by the maximal unramified extension of the completion of F at v, looking at the extension

cut out by $\mathcal{I}_{v,A}$, taking its maximal tamely ramified subextension, and applying Section 8 of [4]. By Theorem 5.2(i) of [24], Definition 1.1(ii) is satisfied. □

Conversely, Theorems 1.7, 1.8, and 1.3 together give the list of groups that can occur as a $G_{v,A}$ for abelian surfaces A, and imply in particular that given p, t_v, t, a_v, a with $t + a = 2$, all $(p, t - t_v, a - a_v)$-inertial groups do in fact occur as $G_{v,A}$'s, for some v and abelian surface A with the given p, t_v, t, a_v, a.

Theorem 1.7. *If A is an abelian surface, then $G_{v,A} \in \Sigma_p(t - t_v, a - a_v)$.*

Proof. Apply Lemma 1.6 and Theorem 1.3. □

We prove the following result in Section 5 below.

Theorem 1.8. *Suppose $G \in \Sigma_p(\tau_2 - \tau_1, \alpha_2 - \alpha_1)$, with $\tau_1, \tau_2, \alpha_1, \alpha_2 \in \mathbb{Z}$, $0 \leqslant \tau_1 \leqslant \tau_2$, $0 \leqslant \alpha_1 \leqslant \alpha_2$, and $\tau_2 + \alpha_2 = 2$. Then there are a field F with a discrete valuation v of residue characteristic p and an abelian surface A over F such that $G \cong G_{v,A}$ and $(t_v, t, a_v, a) = (\tau_1, \tau_2, \alpha_1, \alpha_2)$.*

Remark 1.9. If a finite group can be realized as a group $G_{v,A}$ for some A and v, then so can each of its subgroups (for the same abelian variety A, and for the restriction of $\bar{v}$ to the subfield of L cut out by the subgroup, where L is the smallest Galois extension of $\tilde{F}$ over which A has semistable reduction; note that t_v and a_v might increase).

It is natural to ask whether analogues of Theorems 1.7 and 1.8 hold for abelian varieties in arbitrary dimension, i.e., does the set of non-trivial $(p, t - t_v, a - a_v)$-inertial groups G coincide with the set of $G_{v,A}$'s for abelian varieties A with the given p, t_v, t, a_v, a? The answer turns out to be no, as can be seen from Example 1.12 below, which shows the necessity of imposing additional restrictions on G.

Definition 1.10. We say G is *strongly (p, τ, α)-inertial* if G is (p, τ, α)-inertial, and the G-invariants $(\mathbb{Z}^\tau)^G$ and $(\mathbb{Q}_\ell^{2\alpha})^G$ coming from Definition 1.1(ii) are zero.

As pointed out after Definition 1.1, the dimension of $(\mathbb{Q}_\ell^{2\alpha})^G$ is independent of ℓ.

Lemma 1.11. *If A is an abelian variety, then $G_{v,A}$ is strongly $(p, t-t_v, a-a_v)$-inertial.*

Proof. By Lemma 1.6, $G_{v,A}$ is $(p, t-t_v, a-a_v)$-inertial. Let w be an extension of v at which A has semistable reduction, and let $\mathcal{T}_w$ (resp., $\mathcal{T}_v$) denote the maximal subtorus of A_w (respectively, A_v). Without loss of generality, suppose $F = \tilde{F}$. Over an algebraic closure of the residue field, there are exact sequences

$$0 \to \mathcal{T}_w \to A_w^0 \to \mathcal{B}_w \to 0, \qquad 0 \to U_v \times \mathcal{T}_v \to A_v^0 \to \mathcal{B}_v \to 0,$$

where $\mathcal{B}_w$ and $\mathcal{B}_v$ are abelian varieties, U_v is a unipotent group, and the superscript 0 denotes the identity component (see Section 2.1 of [6]). We have $t_v = \dim(\mathcal{T}_v)$,

$t = \dim(\mathcal{T}_w)$, $a_v = \dim(\mathcal{B}_v)$, $a = \dim(\mathcal{B}_w)$, and $(V_\ell(\mathcal{T}_w))^{G_{v,A}} = V_\ell(\mathcal{T}_v)$. Let $\mathcal{T}'$ denote the image of $\mathcal{T}_v$ in $\mathcal{T}_w$, and let $\mathcal{T} = \mathcal{T}_w/\mathcal{T}'$. Then $\mathcal{T}' = (\mathcal{T}_w^{G_{v,A}})^0$, so $\mathcal{T}^{G_{v,A}}$ is finite. Thus $(\mathbb{Z}^{t-t_v})^{G_{v,A}} = 0$. Similarly, letting $\mathcal{B}'$ denote the image of $\mathcal{B}_v \to \mathcal{B}_w$ and letting $\mathcal{B} = \mathcal{B}_w/\mathcal{B}'$, then $V_\ell(\mathcal{B}_w)^{G_{v,A}} = V_\ell(\mathcal{B}_v)$, $\mathcal{B}' = (\mathcal{B}_w^{G_{v,A}})^0$, $\mathcal{B}^{G_{v,A}}$ is finite, and $(\mathbb{Q}_\ell^{2(a-a_v)})^{G_{v,A}} = 0$. □

Theorems 1.7, 1.8, and 1.3 and Lemma 1.11 imply in particular that the strongly (p, τ, α)-inertial groups are the same as the (p, τ, α)-inertial groups, when $\tau + \alpha \leqslant 2$.

Example 1.12. Suppose that either $p = 0$ or p is a prime. Then C_3 is $(p, 3, 0)$-inertial but is not strongly $(p, 3, 0)$-inertial, as can be seen as follows. For every embedding $f : C_3 = \langle g \rangle \hookrightarrow \mathrm{GL}_3(\mathbb{Z})$, the characteristic polynomial of $f(g)$ is $x^3 - 1$, so $(\mathbb{Z}^3)^{C_3} \neq 0$. By Lemma 1.11, there does not exist a three-dimensional abelian variety A with purely additive and potentially multiplicative reduction such that $G_{v,A} \cong C_3$. Similarly, C_5 is $(p, 0, 3)$-inertial but is not strongly $(p, 0, 3)$-inertial (as follows). We have $C_5 \subset \mathrm{Sp}_4(\mathbb{Q}) \subset \mathrm{Sp}_6(\mathbb{Q})$. For $\ell \equiv 2$ or $3 \pmod 5$, we have that for every embedding $f : C_5 = \langle g \rangle \hookrightarrow \mathrm{Sp}_6(\mathbb{Q}_\ell)$, the characteristic polynomial of $f(g)$ is $(x^5 - 1)(x - 1)$, so $(\mathbb{Q}_\ell^6)^{C_5} \neq 0$. By Lemma 1.11, there does not exist a 3-dimensional abelian variety A with purely additive and potentially good reduction such that $G_{v,A} \cong C_5$.

The answer to the following question is yes when $\tau_1 + \tau_2 \leqslant 2$ (by the results in this paper), but is open when $\tau_1 + \tau_2 \geqslant 3$.

Question 1.13. If G is strongly $(p, \tau_2 - \tau_1, \alpha_2 - \alpha_1)$-inertial with $\tau_1, \tau_2, \alpha_1, \alpha_2 \in \mathbb{Z}$, $0 \leqslant \tau_1 \leqslant \tau_2$, and $0 \leqslant \alpha_1 \leqslant \alpha_2$, do there exist a field F with a discrete valuation v of residue characteristic p and an abelian variety A over F such that $G \cong G_{v,A}$ and $(t_v, t, a_v, a) = (\tau_1, \tau_2, \alpha_1, \alpha_2)$?

In Section 2 we prove some lemmas that are used in Section 3 to prove Theorem 1.3. In Section 4 we prove lemmas that are used in Section 5 to prove Theorem 1.8. Our examples are mostly in the equicharacteristic case. It would be desirable to find examples also in mixed characteristic.

2. Lemmas for Section 3

Let Φ_m denote the mth cyclotomic polynomial (of degree $\varphi(m)$).

Lemma 2.1. *If K is a field of characteristic zero, and $\mathrm{GL}_n(K)$ has an element of order $r > 1$ whose characteristic polynomial has rational coefficients, then we can write $r = \prod_{i=1}^t m_i$ with pairwise relatively prime integers $m_i > 1$ such that $\sum_{i=1}^t \varphi(m_i) \leqslant n$. In particular, if $n = 2$ then r divides 4 or 6, and if $n = 4$ then r divides 8, 10, or 12.*

Proof. If g has order r, then $x^r - 1$ is divisible by the minimal polynomial $f(x)$ of g over $\mathbb{Q}$. Then $f = \Phi_{d_1} \cdots \Phi_{d_s}$ for some $d_1, \ldots, d_s$ where $r = \mathrm{lcm}\{d_i\}$. Take

pairwise relatively prime $n_i \in \mathbb{Z}^+$ such that $n_i \mid d_i$ and $r = \prod_{i=1}^{s} n_i$, and let $\{m_1, \ldots, m_t\}$ be the subset of $\{n_1, \ldots, n_s\}$ of elements $\neq 1$. Then $r = \prod_{i=1}^{t} m_i$ and $\sum_{i=1}^{t} \varphi(m_i) \leqslant \sum_{i=1}^{s} \varphi(d_i) = \deg(f) \leqslant n$. □

Lemma 2.2. *There does not exist a faithful four-dimensional symplectic representation of D_{10} in characteristic zero whose character has only rational values.*

Proof. This is easy to check, using the list of irreducible representations of D_{10} (see for example Section 5.3 of [19] with $n = 5$). □

Lemma 2.3. *If ℓ is prime and $\ell \equiv \pm 3 \pmod 8$, then the Sylow 2-subgroups of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ are isomorphic to H_{128}.*

Proof. The Sylow 2-subgroups of $\mathrm{SL}_2(\mathbb{F}_\ell)$ are isomorphic to Q_8. We have $Q_8 \times Q_8 \subset \mathrm{SL}_2(\mathbb{F}_\ell) \times \mathrm{SL}_2(\mathbb{F}_\ell) \subset \mathrm{Sp}_4(\mathbb{F}_\ell)$. The subgroup of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ generated by $Q_8 \times Q_8$ and $\left(\begin{smallmatrix} 0 & I_2 \\ I_2 & 0 \end{smallmatrix}\right)$ is isomorphic to H_{128}. Since the order of the Sylow 2-subgroups of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ is $2^7 = 128$, we are done. □

Lemma 2.4. *Suppose that G is a finite subgroup of $\mathrm{Sp}_4(\mathbb{Q}_5)$, and $S \subseteq G$ is a 2-group. If there is a short exact sequence $1 \to S \to G \to C_5 \to 1$, then either $G \cong C_5$, or $G \cong C_{10}$, or $G \cong H_{160}$ and $S \cong H_{32}$.*

Proof. By Theorem 5.1 of [26], $G \hookrightarrow \mathrm{Sp}_4(\mathbb{F}_5)$, so $S \hookrightarrow H_{128}$. Fix $c \in G \subset \mathrm{Sp}_4(\mathbb{Q}_5)$ of order 5. Then $V := \mathbb{Q}_5^4$ is a one-dimensional vector space over $\mathbb{Q}_5(\zeta_5) \cong \mathbb{Q}_5[c]$, and $\mathrm{End}_{\mathbb{Q}_5[c]}(V) = \mathbb{Q}_5[c]$. Thus every element of $GL(V)$ of finite order that commutes with c is of the form ac^j where $j \in \mathbb{Z}$, $a \in \mathbb{Q}_5$, and $a^4 = 1$. Since $c \in G \subset \mathrm{Sp}_4(\mathbb{Q}_5)$, and ± 1 are the only scalars in $\mathrm{Sp}_4(\mathbb{Q}_5)$, the elements of G that commute with c are the elements $\pm c^j$. Thus the centralizer of c in S lies in $\{\pm 1\} \subset \mathrm{Sp}_4(\mathbb{F}_5)$. If c commutes with S then $S \subseteq \{\pm 1\}$, so $G \cong C_5$ or C_{10}.

Assume now that c does not commute with S. (Using GAP we can show that every subgroup of H_{128} with an automorphism of order 5 is isomorphic to H_{32}; however, we also give below a theoretical proof of what we need.) Since $S \subset \mathrm{Sp}_4(\mathbb{F}_5)$, $C_2 \times C_2 \times C_2$ is not a subgroup of S. Thus the center Z of S is either cyclic or a product of two cyclic groups. If $S \neq 1$ then $Z \neq 1$, since S is a 2-group. Let Z_2 be the subgroup of Z of elements of order $\leqslant 2$. Then $cZ_2c^{-1} = Z_2$ and $Z_2 \cong C_2$ or $C_2 \times C_2$. Since neither group has an automorphism of order 5, c commutes with Z_2. Thus $Z_2 = \{\pm 1\} \subset S \subset \mathrm{Sp}_4(\mathbb{F}_5)$, and Z_2 is the centralizer of c in S. Write $\#S = 2^r \leqslant 2^7$. Since c does not commute with S, we have $S \neq Z_2$, so $r > 1$. Since conjugation by c has no fixed points on $S - Z_2$, 5 divides $\#(S - Z_2) = 2^r - 2$. Thus $r = 5$, i.e., $\#S = 32$.

If S is abelian then $S = Z$. Since Z_2 is cyclic, $Z = S$ is also cyclic and thus has an element of order 32. But H_{128} has no elements of order 32. So S is non-abelian.

Conjugation by c stabilizes Z, and $\#Z$ divides 128. If $Z \neq Z_2$ then as above, $\#(Z - Z_2)$ is divisible by 5 and $\#Z = 32 = \#S$, so $S = Z$ is abelian. This contradiction shows that $Z = Z_2 = \{\pm 1\}$.

Let $S' = S/Z$, let Z' ($\neq 1$) be the center of S', let Z'_2 be the subgroup of Z' of elements of order $\leqslant 2$, and let H be the preimage of Z'_2 in S. As above, $\#H = 32$. Thus $S = H$ and $S/Z = Z'_2 \cong (C_2)^4$. Since S/Z is abelian, $[S, S] = Z = \{\pm 1\}$. Thus S is an extra-special 2-group (see Section 31 of [1]). By Lemmas 31.2–31.4 of [1], $S \cong Q_8 * Q_8$ or $Q_8 * D_8$, where $*$ denotes the "central product". The number of non-central elements of order 2 in $Q_8 * Q_8$ is 18, which is not divisible by 5, so $Q_8 * Q_8$ has no automorphism of order 5 whose set of fixed points is the center. Thus $S \cong Q_8 * D_8 \cong H_{32}$. □

The next result follows from Proposition 3.3 of [24].

Theorem 2.5. *Suppose that G is a finite group, ℓ is a prime that does not divide $\#G$, and there is an injection*

$$f : G \hookrightarrow \mathrm{GL}_\tau(\mathbb{Z}) \times \mathrm{Sp}_{2\alpha}(\mathbb{Q}_\ell).$$

Then there is an injection

$$G \hookrightarrow \mathrm{GL}_\tau(\mathbb{Z}) \times \mathrm{Sp}_{2\alpha}(\mathbb{Z}_\ell)$$

such that the projection map onto the first factor is the same as that for f, and the characteristic polynomial of the projection onto the second factor is the same as that for f.

Let [ ] denote the greatest integer function, let

$$s(n, q) = \sum_{j=0}^{\infty} \left[\frac{n}{q^j(q-1)} \right], \qquad J(n) = \prod_q q^{s(n,q)},$$

where in the definition of $J(n)$, q runs over the prime numbers. Note that the prime divisors of $J(n)$ are the primes $q \leqslant n+1$. For example, $J(0) = 1$, $J(1) = 2$, $J(2) = 24$, and $J(4) = 2^7 3^2 5$. The method of Minkowski and Serre ([15] and pp. 119–121 of [20]; see also Formula 3.1 of [23]) shows that, for all $N \geqslant 3$, $J(2m)$ is the greatest common divisor of the orders of the groups $\mathrm{Sp}_{2m}(\mathbb{F}_\ell)$, for primes $\ell \geqslant N$. Further (see p. 3 of [21]), $J(n)$ is the least common multiple of the orders of the finite subgroups of $\mathrm{GL}_n(\mathbb{Q})$ (or equivalently, of $\mathrm{GL}_n(\mathbb{Z})$). For the finite subgroups of maximum order for general linear groups over $\mathbb{Q}$ and over cyclotomic fields, see [3]. Let

$$r_p(\tau, \alpha) = s(\tau, p) + s(2\alpha, p), \qquad M(\tau, \alpha) = \max\{\tau, 2\alpha\},$$

and for all primes q such that $p \neq q \leqslant M(\tau, \alpha) + 1$ let

$$r_q(\tau, \alpha) = 1 + \left[\log_q \left(\frac{M(\tau, \alpha)}{q-1} \right) \right].$$

Let

$$N_p(\tau,\alpha)=\prod q^{r_q(\tau,\alpha)},$$

where the product runs over all prime numbers $q\leqslant M(\tau,\alpha)+1$ (this might include $q=p$). The following result follows from the proof of Corollary 6.3 of [24] (see also Proposition 3.1 of [13]).

Theorem 2.6. *If G is (p,τ,α)-inertial, then the largest prime divisor of $\#G$ is at most $M(\tau,\alpha)+1$, and $\#G$ divides $N_p(\tau,\alpha)$ and $J(\tau)J(2\alpha)$.*

3. Proof of Theorem 1.3

If $(\tau,\alpha)=(1,0)$, the result follows immediately from Definition 1.1(ii).

If $(\tau,\alpha)=(0,1)$, we have $G\subset \mathrm{SL}_2(\mathbb{Z}_\ell)$ for all sufficiently large primes ℓ, by Definition 1.1(ii) and Theorem 2.5. This case can be handled the same way as Remark 1.5, where the allowable groups were already known.

The case $(\tau,\alpha)=(1,1)$ follows from the case $(\tau,\alpha)=(0,1)$.

If $(\tau,\alpha)=(2,0)$, we have $G\subset \mathrm{GL}_2(\mathbb{Z})$. By p. 125 of [17], the finite subgroups of $\mathrm{SL}_2(\mathbb{Z})$ are the cyclic groups of order 1, 2, 3, 4, and 6. Therefore $\#G=2$, 3, 4, 6, 8, or 12. Using Definition 1.1(i) and elementary facts about $GL_2(\mathbb{Z})$, it is easy to obtain the list of allowable groups.

From now on, suppose $(\tau,\alpha)=(0,2)$. We have $G\subset \mathrm{Sp}_4(\mathbb{Z}_\ell)$ for all sufficiently large primes ℓ. By Lemma 2.1 (with $n=4$ and $K=\mathbb{Q}_\ell$), if G has a cyclic subgroup of order r then r divides 8, 10, or 12. In particular, G has no elements of order 24. By Theorem 2.6, $\#G$ divides $J(4)=2^7 3^2 5$, and divides $2^3 3^2 5$ if $p=3$ or 5. Suppose from now on that G is not cyclic. Then $p=2$, 3, or 5, and by Definition 1.1(i), there is an exact sequence $0\to S\to G\to C\to 0$ where S ($\neq 1$) is the Sylow p-subgroup of G and C is cyclic.

3.1. Suppose $p=5$. Then $S\cong C_5$ and $\ker[C\to \mathrm{Aut}(S)]\subseteq C_2$. Thus $C\cong C_2$, C_4, or C_8. Suppose $C\cong C_2$. By Lemma 2.2, G does not have a subgroup isomorphic to D_{10}. Thus $G\cong C_{10}$. Suppose now that $C\cong C_4$. Since G does not have a subgroup isomorphic to D_{10}, the subgroup $C_2\subset C$ acts trivially on S. Since G is not C_{20}, we conclude that C acts nontrivially on S, and $G\cong H_{20}$. The remaining case is that $C_8\cong C\twoheadrightarrow \mathrm{Aut}(S)=C_4$, so $G\cong H_{40}$.

3.2. Suppose $p=3$. Then $S\cong C_3$ or $C_3\times C_3$, and $\ker[C\to \mathrm{Aut}(S)]\subseteq C_4$.

Suppose $S\cong C_3$. Then $C\cong C_2$, C_4, or C_8. If $C\cong C_2$, then $G\cong S_3$ or C_6. If $C\cong C_4$, then $G\cong T_{12}$ or C_{12}. If $C\cong C_8$, then $G\cong H_{24}$.

Suppose now that $S\cong C_3\times C_3$. Since $\#\mathrm{Aut}(S)=\#\mathrm{GL}_2(\mathbb{F}_3)=2^4 3$, we again have $C\cong C_2$, C_4, or C_8.

Suppose $C\cong C_2$. If C acts trivially on S, then $G\cong C_3\times C_6$. If there is an isomorphism $S\cong C_3\times C_3$ such that a generator of C acts on S by $(x,y)\mapsto(x^{-1},y)$,

then $G \cong S_3 \times C_3$. The remaining case is that a generator of C acts as the inverse map on $S \cong C_3 \times C_3$. Then S has four subgroups $A_1, \ldots, A_4$ of order 3 such that $G/A_i \cong S_3$. Thus G has two one-dimensional (orthogonal) representations of $G/S \cong C_2$ and a two-dimensional irreducible (orthogonal) representation of $G/A_i \cong S_3$ for each $i \in \{1, 2, 3, 4\}$. Since $\#G = 18 = 2 \times 1^2 + 4 \times 2^2$, these are the only irreducible representations of G (see Corollary 2 in Section 2.4 of [19]). Thus G does not have a faithful symplectic four-dimensional representation in characteristic zero, contradicting Definition 1.1(ii).

Suppose now that $C \cong C_4$.

If C acts trivially on S, then $C_3 \times C_{12} \cong G \subset \mathrm{Sp}_4(\mathbb{Q}_3)$. However, $\mathrm{Sp}_4(\mathbb{Q}_3)$ does not have a subgroup isomorphic to $C_3 \times C_{12}$, as can be seen as follows. If c is a generator of $C_{12} \subset \mathrm{Sp}_4(\mathbb{Q}_3)$, then $\mathbb{Q}_3[c] \cong \mathbb{Q}_3(\zeta_{12})$ or $\mathbb{Q}_3(\zeta_3) \times \mathbb{Q}_3(\zeta_4)$, and $\mathbb{Q}_3^4$ can be viewed as a free rank one module over $\mathbb{Q}_3[c]$. Thus

$$C_3 \times C_{12} \subset \mathrm{Aut}_{\mathbb{Q}_3[c]}(\mathbb{Q}_3^4) = (\mathbb{Q}_3[c])^*.$$

However, neither $\mathbb{Q}_3(\zeta_{12})$ nor $\mathbb{Q}_3(\zeta_3) \times \mathbb{Q}_3(\zeta_4)$ has a multiplicative subgroup isomorphic to $C_3 \times C_{12}$.

If a generator of C acts on S as the inverse map, then $G \cong H_{36}$.

If there is an isomorphism $S \cong C_3 \times C_3$ such that a generator of C acts on S by $(x, y) \mapsto (x^{-1}, y)$, then $G \cong T_{12} \times C_3$.

The remaining case is that a generator of C acts on S as an automorphism of order 4. Then the element of order 2 in C takes an element of S to its inverse. Thus G has an index two subgroup that is an extension of C_2 by $S \cong C_3 \times C_3$, where the generator of C_2 acts as the inverse map on S. We showed above that this does not occur.

Suppose $C \cong C_8$. Since C_{24} is not a subgroup of G, it follows that C cannot act trivially on any subgroup of S of order 3.

Suppose that a generator c of C acts as the inverse map on S. Then c^2 generates the center of G. Since the cyclotomic polynomial $\Phi_8(t) = t^4 + 1$ is irreducible over $\mathbb{Q}_2$, it is the minimal polynomial of $c \in G \subset \mathrm{GL}_4(\mathbb{Q}_2)$, and $c^4 = -1 \in \mathrm{GL}_4(\mathbb{Q}_2)$. Thus $\mathbb{Q}_2[c^2] \cong \mathbb{Q}_2(\sqrt{-1}) = \mathbb{Q}_2(i)$ and so

$$C_3 \times C_3 \cong S \subset G \subset \mathrm{Aut}_{\mathbb{Q}_2[c^2]}(\mathbb{Q}_2^4) \cong \mathrm{GL}_2(\mathbb{Q}_2(i)).$$

Since every homomorphism from $C_3 \times C_3$ to $\mathbb{Q}_2(i)^*$ is trivial, we have $C_3 \times C_3 \subset \mathrm{SL}_2(\mathbb{Q}_2(i))$, which is false (every abelian subgroup of SL_2 over a characteristic 0 field is cyclic), so this case cannot occur.

If a generator of C acts on S as an automorphism of order 4, then $G \cong H_{72}$.

Lastly, if a generator of C acts on S as an automorphism of order 8, then the element of order 2 in C takes every element of S to its inverse. Thus G has a subgroup of index four that is an extension of C_2 by S, and the generator of C_2 takes an element of S to its inverse. We saw above that this cannot occur.

3.3. Suppose $p = 2$. For all but finitely many primes ℓ, there is an embedding $G \subset \mathrm{Sp}_4(\mathbb{F}_\ell)$. By Lemma 2.3, $S \subset H_{128}$.

If $C = C_5$, then $G \cong C_5$, C_{10}, or H_{160} by Lemma 2.4.

Suppose $C = C_3$. Let $c \in G$ be an element of order 3, and suppose c centralizes S. Then $G \cong S \times C_3$. Since C_{24} is not a subgroup of G, there are no elements of order 8 in G. By Definition 1.1(ii), we have $G \subset \mathrm{Sp}_4(\mathbb{Q}_3)$. Since c is symplectic, 1 has multiplicity 0 or 2 as an eigenvalue of c.

First suppose the multiplicity is 2. Let $W_1 = \{x \in \mathbb{Q}_3^4 \mid cx = x\}$. Write $\mathbb{Q}_3^4 = W_1 \oplus W_2$, where W_2 is an S-invariant and c-invariant subspace (as is W_1). Then $\dim(W_1) = \dim(W_2) = 2$. Let I denote the image of $S \to \mathrm{GL}(W_1)$. Since the restriction of the alternating form to W_1 is non-degenerate, $I \subset \mathrm{SL}(W_1) \cong \mathrm{SL}_2(\mathbb{Q}_3)$. Choosing an I-invariant $\mathbb{Z}_3$-lattice in W_1 and reducing modulo $\sqrt{-3}$ gives $I \subset \mathrm{SL}_2(\mathbb{F}_3)$ (since $2 \neq 3$). Thus $I \subseteq Q_8$. Let c_2 be the image of c in $\mathrm{GL}(W_2)$. Then ${c_2}^2 + c_2 + 1 = 0$ in $\mathrm{End}_{\mathbb{Q}_3}(W_2)$. Thus $\mathbb{Q}_3[c_2] \cong \mathbb{Q}_3(\sqrt{-3})$, and W_2 can be viewed as a one-dimensional vector space over $\mathbb{Q}_3(\sqrt{-3})$. Since the image of $S \to \mathrm{GL}(W_2) \cong \mathbb{Q}_3(\sqrt{-3})^*$ is a finite 2-group, it is in $\{\pm 1\}$. Thus $S \subseteq Q_8 \times \{\pm 1\}$, and $G \subseteq Q_8 \times \{\pm 1\} \times C_3 = Q_8 \times C_6$.

Suppose now that 1 is not an eigenvalue of c. Then $c^2 + c + 1 = 0$ in $M_4(\mathbb{Q}_3)$, $\mathbb{Q}_3[c] \cong \mathbb{Q}_3(\sqrt{-3})$, and $\mathbb{Q}_3^4$ can be viewed as a two-dimensional vector space over $\mathbb{Q}_3(\sqrt{-3})$. Thus $S \subset \mathrm{GL}_2(\mathbb{Q}_3(\sqrt{-3}))$. Choosing an S-invariant $\mathbb{Z}_3[\sqrt{-3}]$-lattice in $\mathbb{Q}_3(\sqrt{-3})^2$ and reducing modulo 3 gives $S \subset \mathrm{GL}_2(\mathbb{F}_3)$. Since S has no elements of order 8, the group $\mathrm{GL}_2(\mathbb{F}_3)$ does, and the Sylow 2-subgroups of $\mathrm{GL}_2(\mathbb{F}_3)$ have order 16, it follows that $\#S$ divides 8. Therefore S is C_2, C_4, $C_2 \times C_2$, $C_2 \times C_4$, Q_8, or D_8. Thus $G \cong C_6 \times C_2$, $C_6 \times C_4$, $C_3 \times Q_8$, or $C_3 \times D_8$.

Suppose now that c does not centralize S. By Definition 1.1, we have reduced to the case where $G \in \mathcal{S}_4(5)$.

4. Lemmas for Section 5

Grothendieck gave the assertion of Theorem 4.1 below as the definition of $\mathcal{I}_{v,A}$. See Theorem 4.2 of [24] for a proof of the following.

Theorem 4.1. $\mathcal{I}_{v,A} = \{\sigma \in \mathcal{I}_v : \sigma \text{ acts unipotently on } V_\ell(A)\}$.

Remark 4.2. If $B = A^m$, then $G_{v,A}$ and $G_{v,B}$ are canonically isomorphic. Further, A has purely additive and potentially good reduction if and only if B does. If $m \in \mathbb{Z}^+$ and either $p = 0$ or p is a prime, then by Remark 1.5, for every group $G \in \Sigma_p(0, 1)$ there is an m-dimensional abelian variety B over a discrete valuation field of residue characteristic p with purely additive and potentially good reduction and with $G_{v,B} \cong G$.

Recall that $\tilde{F}$ denotes the maximal unramified extension of the completion of F at v.

Theorem 4.3. *Suppose B is an abelian variety over $\tilde{F}$ with semistable reduction, all the endomorphisms of B are defined over $\tilde{F}$, L is a finite Galois extension of $\tilde{F}$,*

and $G = \mathrm{Gal}(L/\tilde{F})$. *If there is an injective homomorphism* $i : G \hookrightarrow \mathrm{Aut}(B)$, *then* $G \cong G_{v,A}$, *where* A *is the twist of* B *by the cocycle* c *defined by the composition*

$$\mathrm{Gal}(\tilde{F}^s/\tilde{F}) \twoheadrightarrow \mathrm{Gal}(L/\tilde{F}) = G \hookrightarrow \mathrm{Aut}(B).$$

Suppose further that B *has good reduction. Then* $B^{i(G)}$ *is finite if and only if* A *has purely additive reduction* (*i.e.*, $a_v(A) = t_v(A) = 0$).

Proof. Note that $\mathrm{Gal}(\tilde{F}^s/\tilde{F}) = \mathcal{I}_v$. By the definition of the twist, there is an isomorphism $f : B \xrightarrow{\sim} A$ such that $c(\sigma) = \sigma(f)^{-1} f$ for every $\sigma \in \mathrm{Gal}(\tilde{F}^s/\tilde{F})$. We then have $\rho_{\ell,A}(\sigma) = \sigma(f)\rho_{\ell,B}(\sigma) f^{-1}$. Therefore,

$$\begin{aligned}\mathcal{I}_{v,A} &= \{\sigma \in \mathcal{I}_v : \sigma(f)\rho_{\ell,B}(\sigma) f^{-1} \text{ is unipotent}\}\\ &= \{\sigma \in \mathcal{I}_v : \rho_{\ell,B}(\sigma) c(\sigma)^{-1} \text{ is unipotent}\} = \{\sigma \in \mathcal{I}_v : c(\sigma) \text{ is unipotent}\} = \ker(c),\end{aligned}$$

where the first equality follows from Theorem 4.1, the second after conjugating by $\sigma(f)$, the third since $\rho_{\ell,B}(\sigma)$ is unipotent, and the fourth since $c(\sigma)$ has finite order. Therefore,

$$G_{v,A} = \mathcal{I}_v/\mathcal{I}_{v,A} = \mathcal{I}_v/\ker(c) \cong \mathrm{Gal}(L/\tilde{F}) = G.$$

Now suppose that B has good reduction. Then $\mathcal{I}_v$ acts as the identity on $V_\ell(B)$. Further, A has purely additive reduction if and only if $V_\ell(A)^{\mathcal{I}_v} (\cong V_\ell(A_v)) = 0$. Recall that $c(\sigma) = \sigma(f)^{-1} f \in \mathrm{Aut}(B) \subset \mathrm{Aut}(V_\ell(B))$. Then

$$\begin{aligned}V_\ell(A)^{\mathcal{I}_v} &= \{x \in V_\ell(A) : \sigma(f)\rho_{\ell,B}(\sigma) f^{-1}(x) = x \text{ for all } \sigma \in \mathcal{I}_v\}\\ &= f(\{y \in V_\ell(B) : \sigma(y) = \sigma(f)^{-1} f(y) \text{ for all } \sigma \in \mathcal{I}_v\})\\ &= f(\{y \in V_\ell(B) : y = c(\sigma)(y) \text{ for all } \sigma \in \mathcal{I}_v\}).\end{aligned}$$

Further, $\{y \in B : y = c(\sigma)(y) \text{ for all } \sigma \in \mathcal{I}_v\} = B^{i(G)}$. Therefore,

$$V_\ell(A)^{\mathcal{I}_v} = V_\ell(B^{i(G)}).$$

Clearly, if $\dim(B^{i(G)}) > 0$ then $B^{i(G)}$ has an abelian subvariety of positive dimension and therefore $V_\ell(B^{i(G)}) \neq 0$. Thus $B^{i(G)}$ is finite if and only if $V_\ell(A)^{\mathcal{I}_v} = 0$. □

Remark 4.4. If A has potentially good reduction then $V_\ell(A)^{\mathcal{I}_v} = V_\ell(A)^{G_{v,A}}$. Hence A has purely additive reduction if and only if $V_\ell(A)^{G_{v,A}} = 0$.

The following lemma gives evidence for the sharpness of Theorem 2.6.

Lemma 4.5. *Suppose either $p = 0$ or p is a prime. If $n > 2$, then there exist a field K with a discrete valuation v of residue characteristic p, and an abelian variety A over K of dimension $\varphi(n)/2$, with purely additive and potentially good reduction at v and with $G_{v,A} \cong C_n$. Further, if n is the order of an element of finite order in $\mathrm{GL}_{2d'}(\mathbb{Z})$, then $\dim(A) \leqslant d'$. If $2d+1$ is a prime, then there exists a d-dimensional abelian variety A such that $G_{v,A} \cong C_{2d+1}$ and $Q_{v,A} = M(t - t_v, a - a_v) + 1 = 2d + 1$.*

Proof. Choose an abelian variety B of dimension $\varphi(n)/2$ with complex multiplication by $\mathbb{Z}[\zeta_n]$ and with good reduction over $\tilde{F}$, where F is a sufficiently large extension of $\mathbb{Q}_p(\zeta_n)$ if p is prime, and $F = \tilde{F} = \mathbb{C}((t))$ if $p = 0$ (see Sections 4–5 of [22]). Let L be a totally ramified cyclic extension of $\tilde{F}$ of degree n. Let A be the twist of B by the cocycle induced by the composition

$$\mathrm{Gal}(\tilde{F}^s/\tilde{F}) \twoheadrightarrow \mathrm{Gal}(L/\tilde{F}) \cong C_n \hookrightarrow \mathrm{Aut}(B).$$

By Theorem 4.3, A is an abelian variety over $\tilde{F}$ of dimension $\varphi(n)/2$ with potentially good reduction, and $G_{v,A} \cong \mathrm{Gal}(L/\tilde{F}) \cong C_n$. Since $1 - \zeta_n$ is an isogeny, it has finite kernel, so B^{μ_n} is finite and A has purely additive reduction (and so $M(t - t_v, a - a_v) = 2\dim(A)$). □

We next prove results that will be used to prove Theorem 4.11 below.

Suppose G is a finite group, and K is a field complete with respect to a discrete valuation v with valuation ring $\mathcal{O}$, maximal ideal $\mathfrak{m}$, and residue field k. Suppose $\#G$ is not divisible by the characteristic of k. By Proposition 43 in Section 15.5 of [19], every finite-dimensional representation $\bar{\rho}\colon G \to \mathrm{Aut}_k(W)$ can be lifted in a unique way (up to isomorphism) to $\rho\colon G \to \mathrm{Aut}_{\mathcal{O}}(T)$, where T is a free $\mathcal{O}$-module with $T/\mathfrak{m}T = W$, and $\bar{\rho}$ is ρ modulo $\mathfrak{m}$. The lifting of a trivial G-module is also a trivial G-module. A bilinear form $e\colon T \times T \to \mathcal{O}$ is called *perfect* if the induced homomorphisms $T \to \mathrm{Hom}(T, \mathcal{O})$ are bijective.

Lemma 4.6. *With notation and assumptions as above, suppose $\bar{\rho}$ is symplectic, i.e., there exists a non-degenerate alternating G-invariant bilinear form*

$$\bar{e}\colon W \times W \to k.$$

Then there exists a perfect alternating G-invariant $\mathcal{O}$-bilinear form

$$e\colon T \times T \to \mathcal{O}$$

that is a lift of $\bar{e}$.

Proof. Since $\#G$ is not divisible by $\mathrm{char}(k)$, by Maschke's theorem there exists a $k[G]$-module $\bar{S}$ such that

$$\mathrm{Hom}_k(\wedge_k^2(W), k) = (\mathrm{Hom}_k(\wedge_k^2(W), k))^G \oplus \bar{S}.$$

Let (projective $\mathcal{O}[G]$-modules) U and S be the liftings of $(\mathrm{Hom}_k(\wedge^2_k(W), k))^G$ and $\bar{S}$, respectively. Then U is a trivial G-module. We have

$$\mathrm{Hom}_{\mathcal{O}}(\wedge^2_{\mathcal{O}}(T), \mathcal{O}) = U \oplus S,$$

since both sides are liftings of $\mathrm{Hom}_k(\wedge^2_k(W), k)$. Choose

$$e \in U \subset (\mathrm{Hom}_{\mathcal{O}}(\wedge^2_{\mathcal{O}}(T), \mathcal{O}))^G$$

such that the reduction of e is $\bar{e}$. The non-degeneracy of $\bar{e}$ implies that e is perfect. □

If p is a prime, let $\mathbb{H}_p$ denote the quaternion algebra over $\mathbb{Q}$ ramified exactly at p and ∞.

Theorem 4.7. *Suppose G is a finite group that is a semidirect product of a normal Sylow p-subgroup by a cyclic group. Suppose that χ is a faithful irreducible character of G of degree d.*

(i) *If χ takes values in an imaginary quadratic field $E \subset \mathbb{H}_p$, then G is isomorphic to a subgroup of* $\mathrm{GL}_d(\mathbb{H}_p)$.
(ii) *If χ is symplectic and takes values in $\mathbb{Q}$, then G is isomorphic to a subgroup of* $\mathrm{GL}_{d/2}(\mathbb{H}_p)$.

Proof. Write $\mathbb{Q}(\chi)$ (resp., $E(\chi)$) for the subfield of $\mathbb{C}$ obtained by adjoining to $\mathbb{Q}$ (respectively, to E) all values of χ. In case (i) we have $\mathbb{Q}(\chi) = \mathbb{Q}$ or E, and $E(\chi) = E$; in case (ii) we have $\mathbb{Q}(\chi) = \mathbb{Q}$.

Let V be a faithful irreducible $\mathbb{C}[G]$-module with character χ. Write the (semisimple) $\mathbb{Q}(\chi)$-algebra $\mathbb{Q}(\chi)[G]$ as a direct sum

$$\mathbb{Q}(\chi)[G] = \oplus_{i=1}^{s} A_i$$

of simple $\mathbb{Q}(\chi)$-algebras A_i. By Lemma 24.7 of [1], there is exactly one $j \in \{1, \ldots, s\}$ such that $A_j V \neq 0$, and the center of A_j is $\mathbb{Q}(\chi)$. The central simple $\mathbb{C}$-algebra $A_{j,\mathbb{C}} := A_j \otimes_{\mathbb{Q}(\chi)} \mathbb{C}$ is a direct summand of $\mathbb{C}[G]$, and $A_{j,\mathbb{C}} V \neq 0$. By the same lemma, these properties define $A_{j,\mathbb{C}}$ uniquely. Explicitly, the unit of $A_{j,\mathbb{C}}$ is

$$e_\chi := \frac{\chi(1)}{\#G} \sum_{g \in G} \chi(g^{-1}) g \in \mathbb{Q}(\chi)[G].$$

Identifying A_j with $A_j \otimes 1 \subset A_{j,\mathbb{C}}$, then $A_j = e_\chi(\mathbb{Q}(\chi)[G])$, so $D_\chi := A_j$ determines χ uniquely. Note that e_χ acts on V as the identity map. We have $\dim_{\mathbb{Q}(\chi)} D_\chi = \chi(1)^2 = d^2$ (see [1], proof of Theorem 24.12(4)).

Clearly, D_χ is a central simple $\mathbb{Q}(\chi)$-algebra and thus there exist a central division algebra B over $\mathbb{Q}(\chi)$ and a positive integer n such that $D_\chi \cong \mathrm{M}_n(B)$. We have $d^2 = n^2 \dim_{\mathbb{Q}(\chi)}(B)$. The $\mathbb{Q}(\chi)$-vector space B^n is naturally a faithful simple $D_\chi = \mathrm{M}_n(B)$-module. Via the projection map $\mathbb{Q}(\chi)[G] \twoheadrightarrow D_\chi$ defined by $x \mapsto x \cdot e_\chi$, we can view B^n as a simple $\mathbb{Q}(\chi)[G]$-module with e_χ acting as the identity map. Thus $B^n \otimes_{\mathbb{Q}(\chi)} \mathbb{C} \cong V^{s(\chi)}$, where $s(\chi)$ is the Schur index of χ, i.e., $s(\chi)^2 = \dim_{\mathbb{Q}(\chi)}(B)$ ([1, Theorem 24.14). Since V is a faithful $\mathbb{C}[G]$-module, B^n is a faithful $\mathbb{Q}(\chi)[G]$-module, i.e., $\rho\colon G \to \mathrm{Aut}_{\mathbb{Q}(\chi)}(B^n)$ is injective. Since $B^{\mathrm{op}} = \mathrm{End}_{\mathbb{Q}(\chi)[G]}(B^n) = \mathrm{End}_{\mathrm{M}_n(B)}(B^n)$, we have an embedding

$$\rho\colon G \hookrightarrow \mathrm{GL}_n(B^{\mathrm{op}}).$$

Note that $B^{\mathrm{op}} \cong B$ if either $B = \mathbb{Q}(\chi)$ or B is a quaternion algebra over $\mathbb{Q}(\chi)$.

If K is an arbitrary field containing $\mathbb{Q}(\chi)$, then χ is realizable over K if and only if D_χ splits over K ([1, Theorem 24.8(b)]). Thus χ is realizable over K if and only if B^{op} splits over K.

Let ℓ be a prime different from p. Serre [16] proved that, for G a semidirect product of a normal Sylow p-subgroup by a cyclic group, the group algebra $\mathbb{Q}_\ell[G]$ is a direct sum of matrix algebras over (commutative) fields. Thus if $\mathbb{Q}_\ell \subseteq K$, then $K[G]$ is also a direct sum of matrix algebras over fields, so every character with values in K is realizable over K. Thus D_χ, and therefore B^{op}, is unramified at all non-archimedean places of $\mathbb{Q}(\chi)$ with residue characteristic different from p.

Suppose $\mathbb{Q}(\chi) = E$. Then

$$\mathbb{Q}(\chi) \otimes_{\mathbb{Q}} \mathbb{Q}_p = E \otimes_{\mathbb{Q}} \mathbb{Q}_p \subset \mathbb{H}_p \otimes_{\mathbb{Q}} \mathbb{Q}_p,$$

so $E \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a field. Thus there is exactly one place of E with residue characteristic p, and B^{op} is unramified away from this place. Since E is an imaginary quadratic field, it follows that B^{op} is unramified everywhere. Thus $B = \mathbb{Q}(\chi) = E$, $n = d$, and $\rho\colon G \hookrightarrow \mathrm{GL}_d(E) \subset \mathrm{GL}_d(\mathbb{H}_p)$.

Suppose $\mathbb{Q}(\chi) = \mathbb{Q}$. Then B^{op} is unramified outside p and ∞. Thus either $B^{\mathrm{op}} = \mathbb{Q}(\chi) = \mathbb{Q}$ and $n = d$, or $B^{\mathrm{op}} = \mathbb{H}_p$ and $n = d/2$. We have

$$\rho\colon G \hookrightarrow \mathrm{GL}_d(\mathbb{Q}) \subset \mathrm{GL}_d(\mathbb{H}_p)$$

or

$$\rho\colon G \hookrightarrow \mathrm{GL}_{d/2}(\mathbb{H}_p),$$

respectively.

If χ is symplectic then it is not realizable over $\mathbb{R}$ ([19], Section 13.2, Proposition 38), so B^{op} is ramified at ∞, so $B^{\mathrm{op}} \neq \mathbb{Q}$. $\square$

Lemma 4.8. *Suppose H is a subgroup of $\mathrm{Sp}_4(\mathbb{F}_5)$ of order 2^m3^n that does not have any elements of order 24. Then the values of the character of its lifting*

$$H \hookrightarrow \mathrm{Sp}_4(\mathbb{Q}_5) \subset \mathrm{GL}_4(\mathbb{Q}_5)$$

all lie in $\mathbb{Q}$.

Proof. Since the order of H is prime to 5, there is exactly one lifting $H \hookrightarrow \mathrm{GL}_4(\mathbb{Q}_5)$ of $H \subset \mathrm{Sp}_4(\mathbb{F}_5) \subset \mathrm{GL}_4(\mathbb{F}_5)$. By Lemma 4.6, this lifting is symplectic and thus we have a faithful symplectic representation

$$\rho\colon H \hookrightarrow \mathrm{Sp}_4(\mathbb{Q}_5) \subset \mathrm{GL}_4(\mathbb{Q}_5).$$

Suppose that d is the order of some element $x \in H$. Then d is a divisor of 8 or 12. Since ρ is self-dual, the values of its character χ all lie in $\mathbb{R}$, and thus $\chi(x)$ is in the totally real subfield of $\mathbb{Q}(\zeta_d)$. If $d \in \{1, 2, 3, 4, 6\}$, then $\chi(x) \in \mathbb{Q}$. The remaining cases are $d = 8$ and $d = 12$.

Suppose first that $\rho(x)$ has a primitive dth root of unity γ as an eigenvalue. Then $\gamma \notin \mathbb{Q}_5$. Since $\rho(x)$ is "defined" over $\mathbb{Q}_5$, γ^5 is another eigenvalue of $\rho(x)$. Since $\rho(x)$ is symplectic, γ^{-1} and γ^{-5} are eigenvalues of $\rho(x)$. By counting arguments (i.e., since $\varphi(d) = 4$), the spectrum of $\rho(x)$ is the set of primitive dth roots of unity (each with multiplicity one). Thus the characteristic polynomial of $\rho(x)$ is Φ_d, so the trace $\chi(x) = 0 \in \mathbb{Q}$.

The remaining case to consider is when $\rho(x)$ has an eigenvalue i that is a primitive fourth root of unity and an eigenvalue ω that is a primitive sixth or cube root of unity. Since $\rho(x)$ is symplectic, the spectrum of $\rho(x)$ is $\{i, -i, \omega, \omega^{-1}\}$ (each with multiplicity one) and the trace $\chi(x) = \omega + \omega^{-1} = -1$ or 1. □

As pointed out to us by Klaus Lux, the table on p. 146 of [9] shows that the degree four Brauer character φ_{16} of $\mathrm{Sp}_4(\mathbb{F}_5)$ takes rational values on the elements of order $\leqslant 12$, and this observation may be used to obtain a different proof of Lemma 4.8.

Theorem 4.9. *Suppose G is a finite group with a normal Sylow 2-subgroup of index 3. Suppose χ is a degree 2 faithful character of G. Assume that either*:

(i) *G is non-abelian and χ is symplectic, or*
(ii) *G is non-abelian and the values of χ are all in $\mathbb{Q}$, or*
(iii) *χ is symplectic and the values of χ are all in $\mathbb{Q}$.*

Then G is isomorphic to a subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$.

Proof. Suppose first that G is abelian and χ is symplectic. Then G is cyclic, since G is a finite subgroup of $\mathrm{SL}_2(\mathbb{C})$. If further the values of χ are all in $\mathbb{Q}$, then $\#G$ divides 4 or 6. Since $3 \mid \#G$, we have $G \cong C_3$ or C_6. Note that $C_3 \subset C_6 \subset \mathrm{SL}_2(\mathbb{F}_3)$.

We may therefore suppose that G is not abelian. Then χ is irreducible.

Assume first that χ is symplectic. Inspecting the list of finite subgroups of $\mathrm{SL}_2(\mathbb{C})$ ([28], Case I of Theorem 6.17 on p. 404), we conclude that either $G \cong \mathrm{SL}_2(\mathbb{F}_3)$, or

$$G \cong \mathcal{H}_{4r} = < x, y \mid x^r = y^2, yxy^{-1} = x^{-1} >,$$

the generalized quaternion group of order $4r$, for some positive integer r. Assume $G \cong \mathcal{H}_{4r}$. Since y has order 4, it is in the kernel of every homomorphism $f : G \to C_3$. Thus $f(x)^{-1} = f(yxy^{-1}) = f(x)$, so $f(x) = 1$. Thus every homomorphism $G \to C_3$ is trivial, contradicting our first assumption on G.

Now assume instead that the values of χ are all in $\mathbb{Q}$. Since the values of χ are all real, χ is either symplectic or orthogonal. We dealt with the symplectic case above, so we may assume that χ is orthogonal. Then χ is realizable over $\mathbb{R}$ (by the Frobenius–Schur theorem) and $G \subset O_2(\mathbb{R})$, the orthogonal group. Every element of G has order dividing 6 or 4. Let $G_0 = G \cap SO_2(\mathbb{R})$. Then $[G : G_0] = 1$ or 2, so $3 \mid \#G_0$. Since every finite subgroup of $SO_2(\mathbb{R})$ is cyclic, G_0 is cyclic of order 3 or 6. If $\#G_0 = 3$, then $G \cong S_3$, which does not have a normal Sylow 2-subgroup. Thus $G_0 = C_6$, and $G \cong T_{12}$. But the Sylow 2-subgroups of T_{12} are not normal. □

Lemma 4.10. *If $\mathcal{O}$ is a maximal order of $\mathbb{H}_p$, G is a finite subgroup of $\mathrm{GL}_r(\mathbb{H}_p)$, and $r > 1$, then there is an embedding $G \hookrightarrow \mathrm{GL}_r(\mathcal{O})$.*

Proof. Let $\Lambda \subseteq \mathbb{H}_p^r$ be a left G-stable $\mathcal{O}$-lattice (for example, start with any lattice Λ' and let $\Lambda = \sum_{g \in G} \Lambda' g$). Since $r > 1$, $\Lambda \cong \mathcal{O}^r$ by a result of Eichler ([2]; see also Corollary 2.2 of [7]). Thus $G \hookrightarrow \mathrm{Aut}_{\mathcal{O}}(\Lambda) \cong \mathrm{GL}_r(\mathcal{O})$. □

Theorem 4.11. *Suppose G is a non-abelian subgroup of $\mathrm{Sp}_4(\mathbb{F}_5)$ whose Sylow 2-subgroup is normal of index 3 in G. Suppose G has no elements of order 24. Then there is an embedding $G \hookrightarrow \mathrm{GL}_2(\mathcal{O})$ where $\mathcal{O}$ is the maximal order in the Hamilton quaternions $\mathbb{H}_2$.*

Proof. By Lemma 4.8, there exists a faithful symplectic complex character χ of G of degree 4 whose values are all rational. By Lemma 4.10, it suffices to check that there is an embedding $G \hookrightarrow \mathrm{GL}_2(\mathbb{H}_2)$. If χ is irreducible then this follows from Theorem 4.7(ii). Assume now that χ is reducible. Since G is non-abelian, χ is not a sum of one-dimensional characters. Thus χ is a sum $\chi_1 + \chi_2$ of two-dimensional characters, where we can assume χ_2 is irreducible. For $i = 1, 2$, let $\rho_i : G \to \mathrm{SL}_2(\mathbb{C})$ be a corresponding representation with character χ_i, and let $H_i = \rho_i(G)$. Since χ is symplectic, either χ_1 and χ_2 are symplectic, or χ_1 and χ_2 are complex conjugates of each other.

If χ_1 is the complex conjugate of χ_2, then $\ker(\rho_1) = \ker(\rho_2) \subseteq \ker(\rho_1 \oplus \rho_2)$. Since χ is faithful, so are χ_1 and χ_2. Since $\chi = \chi_1 + \chi_2$, the Galois orbit of χ_2 is $\{\chi_2\}$ or $\{\chi_1, \chi_2\}$. Thus χ_2 takes values in an imaginary quadratic field. Applying Theorem 4.7(i) to G and χ_2, we have $G \hookrightarrow \mathrm{GL}_2(\mathbb{H}_2)$.

Assume now that χ_1 and χ_2 are symplectic. Since χ takes values in $\mathbb{Q}$, either χ_1 and χ_2 both take values in $\mathbb{Q}$, or χ_1 and χ_2 take values in a real quadratic field and χ_1 is the Galois conjugate of χ_2.

Suppose first that χ_1 and χ_2 take values in a real quadratic field and χ_1 is the Galois conjugate of χ_2. Then $\ker(\rho_1) = \ker(\rho_2)$, so χ_1 and χ_2 are faithful. Applying Theorem 4.9(i) to G and χ_2, we have $G \subseteq \mathrm{SL}_2(\mathbb{F}_3) \subset \mathbb{H}_2^*$.

Suppose instead that χ_1 and χ_2 both take values in $\mathbb{Q}$. If $\#H_i$ is divisible by 3, then $H_i \subseteq \mathrm{SL}_2(\mathbb{F}_3)$ by Theorem 4.9(iii). Suppose $\#H_2$ is not divisible by 3. If d is

the exponent of H_2 then χ_2 is realizable over $\mathbb{Q}(\zeta_d)$ (see the Corollary to Theorem 24 in Section 12.3 of [19]), so there is an absolutely irreducible faithful representation $H_2 \hookrightarrow \mathrm{SL}_2(\mathbb{Q}(\zeta_d)) \subset \mathrm{SL}_2(\mathbb{Q}_3(\zeta_d))$. Let Ω be the ring of integers of $\mathbb{Q}_3(\zeta_d)$. Choosing an H_2-stable Ω-lattice in $\mathbb{Q}_3(\zeta_d)^2$ gives an embedding $\rho_3 : H_2 \hookrightarrow \mathrm{SL}_2(\Omega)$. Since $\#H_2$ is prime to 3, reduction modulo 3 gives an absolutely irreducible faithful representation $\bar{\rho}_3 : H_2 \hookrightarrow \mathrm{SL}_2(\Omega/3\Omega)$ such that the character $\bar{\chi}_3$ of $\bar{\rho}_3$ is the reduction mod 3 of χ_2. Since χ_2 takes values in $\mathbb{Q}$, it takes values in $\mathbb{Z}$, so $\bar{\chi}_3$ takes values in $\mathbb{F}_3$. By Theorem 24.10 of [1], $\bar{\rho}_3$ is realizable over $\mathbb{F}_3$, so there is an embedding $H_2 \hookrightarrow \mathrm{SL}_2(\mathbb{F}_3)$. If χ_1 is irreducible, then similarly $H_1 \hookrightarrow \mathrm{SL}_2(\mathbb{F}_3)$. If χ_1 is a sum of two characters of degree one, then $H_1 \subset \mathrm{SL}_2(\mathbb{C})$ is abelian, so is cyclic, and by Lemma 2.1 either $H_1 \subseteq C_4 \subset \mathrm{SL}_2(\mathbb{F}_3)$ or $H_1 \subseteq C_6 \subset \mathrm{SL}_2(\mathbb{F}_3)$. Thus

$$G \hookrightarrow H_1 \times H_2 \hookrightarrow \mathrm{SL}_2(\mathbb{F}_3) \times \mathrm{SL}_2(\mathbb{F}_3) \subset \mathbb{H}_2^* \times \mathbb{H}_2^* \hookrightarrow \mathrm{GL}_2(\mathbb{H}_2). \qquad \square$$

5. Proof of Theorem 1.8

Lemma 5.1. *If k is an algebraically closed field of prime characteristic p, then every (p, τ, α)-inertial group G can be realized as a Galois group $\mathrm{Gal}(L/k((t))$ for a (totally ramified) Galois extension L of $k((t))$.*

Proof. Our proof follows [14]. Let H denote the absolute Galois group of $k((t))$, and let $\hat{\mu}$ denote the character group of the group of all roots of unity in k. Then $\hat{\mu} \cong \prod_{\ell \neq p} \mathbb{Z}_\ell$. By Theorem 1 in Section 2 of [14] (see also [10]), H is a semidirect product of a (normal) subgroup W by $\hat{\mu}$, where W contains an infinite set J with the following universal property. If S is a pro-p-group with a continuous homomorphism $\hat{\mu} \to \mathrm{Aut}(S)$, then every map $J \to S$ that sends all but finitely many elements of J to the identity extends uniquely to a continuous homomorphism $W \to S$ that commutes with the actions of $\hat{\mu}$.

Now let S denote the Sylow p-subgroup of G. Fixing any surjective map $J \twoheadrightarrow S$ that sends all but finitely many elements of J to the identity, the universal property gives a continuous homomorphism $W \twoheadrightarrow S$ that commutes with the actions of $\hat{\mu}$. Thus there is a continuous surjective homomorphism $H \twoheadrightarrow T$, where T is the semidirect product of S by $\hat{\mu}$. Since G/S is a finite cyclic p'-group, there is a continuous surjective homomorphism $\pi : \hat{\mu} \twoheadrightarrow G/S$. Let $U = \ker(\pi)$, and view U as a closed normal subgroup of T. Then we have $H \twoheadrightarrow T \twoheadrightarrow T/U \cong G$. $\square$

Note that $G_{v,A} = 1$ (i.e., A has semistable reduction) if and only if $(t_v, t, a_v, a) = (0, 0, 2, 2)$, $(2, 2, 0, 0)$, or $(1, 1, 1, 1)$. Products of elliptic curves with good and/or multiplicative reduction give such abelian varieties.

Suppose $G \in \Sigma_p(\tau_2 - \tau_1, \alpha_2 - \alpha_1)$, with $0 \leqslant \tau_1 \leqslant \tau_2$, $0 \leqslant \alpha_1 \leqslant \alpha_2$.

If $(\tau_1, \tau_2, \alpha_1, \alpha_2) = (0, 1, 1, 1)$, $(1, 2, 0, 0)$, $(0, 0, 1, 2)$, $(1, 1, 0, 1)$, $(0, 1, 0, 1)$ (i.e., $\max\{\tau_2 - \tau_1, \alpha_2 - \alpha_1\} = 1$), then it is easy (using Remark 1.5) to find a product A of two elliptic curves such that $G \cong G_{v,A}$ and $(t_v, t, a_v, a) = (\tau_1, \tau_2, \alpha_1, \alpha_2)$. For example, let E_1 be an elliptic curve over $F = \mathbb{Q}_2^{nr}$ (the maximal unramified extension of $\mathbb{Q}_2$) such that $G_{v,E_1} \cong \mathrm{SL}_2(\mathbb{F}_3)$ (and therefore E_1 has additive, potentially good

reduction). Let L be the smallest extension of $\tilde{F}$ over which E_1 acquires good reduction (so $\mathrm{Gal}(L/\tilde{F}) \cong G_{v,E_1}$). Let $K/\tilde{F}$ be a quadratic extension disjoint from L (there exist infinitely many). Let E_2' be an elliptic curve over $\tilde{F}$ with multiplicative reduction and let E_2 be the twist of E_2' by the quadratic character associated to $K/\tilde{F}$. Then E_2 has additive, potentially multiplicative reduction, and K is the smallest extension of $\tilde{F}$ over which E_2 has semistable reduction, by Theorem 4.3. Therefore KL is the smallest extension of $\tilde{F}$ over which $A = E_1 \times E_2$ has semistable reduction, so $G_{v,A} \cong \mathrm{Gal}(KL/\tilde{F}) \cong C_2 \times \mathrm{SL}_2(\mathbb{F}_3)$.

If $(\tau_1, \tau_2, \alpha_1, \alpha_2) = (0, 2, 0, 0)$, let E be an elliptic curve over $\tilde{F}$ with multiplicative reduction and let $B = E^2$. Then $\mathrm{GL}_2(\mathbb{Z}) \subseteq \mathrm{Aut}(B)$. The groups C_2, C_3, C_4, C_6, $C_2 \times C_2$, D_8, and S_3 can all be embedded in $\mathrm{GL}_2(\mathbb{Z})$ (embed C_2 so that the generator goes to -1). By Theorem 4.3, for each such G, there is a twist A of B such that $G_{v,A} \cong G$ and v has residue characteristic p. There is a $g \in G$ such that $g - 1$ is in $\mathrm{GL}_2(\mathbb{Q})$, and thus induces an isogeny on B. Thus B^G is finite, so A has purely additive and potentially multiplicative reduction.

From now on, assume $(\tau_1, \tau_2, \alpha_1, \alpha_2) = (0, 0, 0, 2)$. By Lemma 4.5 with $n = 5$, 8, 10, or 12, we can realize all cyclic groups of order dividing 8, 10, or 12. By Remark 4.2, if $G \in \Sigma_p(0, 1)$, then G can be realized as a $G_{v,A}$ for some abelian surface A with purely additive and potentially good reduction over some $\tilde{F}$ with residue characteristic p. So we may assume that $G \in \Sigma_p(0, 2) - \Sigma_p(0, 1) - \Sigma(0, 2)$.

Let $p = 2$. To realize H_{160}, consider the hyperelliptic curve $C : y^2 - y = x^5$ of genus 2 over the local field $\tilde{F} = \bar{\mathbb{F}}_2((t))$ and let J be the Jacobian of C. Then C and J have good reduction. The maps $(x, y) \mapsto (\gamma x + a, y + a^8\gamma^2 x^2 + a^4\gamma x + b)$ with $\gamma, a, b \in \mathbb{F}_{16}$, $\gamma^5 = 1$, and $b^2 - b = a^5$ allow one to view H_{160} as $\mathrm{Aut}(C) \subset \mathrm{Aut}(J)$ (see [8], pp. 616 and 645–646). Restricting to $\gamma = 1$ gives the normal subgroup H_{32}. The (only) nontrivial central element is $(x, y) \mapsto (x, y + 1)$. Apply Theorem 4.3 and Lemma 5.1.

Consider $E : y^2 - y = x^3$ over the local field $\bar{\mathbb{F}}_2((t))$. Then E has good reduction. It is well-known that $\mathrm{Aut}(E) = \mathrm{SL}_2(\mathbb{F}_3)$ (see [29] and Appendix A of [27]). The groups $C_2 \times C_6$, $C_4 \times C_6$, $C_3 \times Q_8$, $C_3 \times D_8$, and $C_6 \times Q_8$ all lie in $\mathcal{O}^* \times \mathcal{O}^* \subset \mathrm{GL}_2(\mathcal{O}) = \mathrm{Aut}(E^2)$, where $\mathcal{O}$ is the maximal order in $\mathbb{H}_2$. If $G \in \mathcal{S}_4(5)$, then by Theorem 4.11, $G \subset \mathrm{GL}_2(\mathcal{O}) = \mathrm{Aut}(E^2)$. Let H denote the semidirect product of $\mathrm{SL}_2(\mathbb{F}_3) \times \mathrm{SL}_2(\mathbb{F}_3)$ by C_2, with C_2 acting by interchanging the factors (this is the wreath product $\mathrm{SL}_2(\mathbb{F}_3)$ wr C_2). Then $H \subset \mathrm{Aut}(E^2)$, and H_{128} is the Sylow 2-subgroup of H. Every subgroup of H of order dividing $2^7 3$ is a Galois group over $\tilde{F}$. Apply Lemma 5.1 and Theorem 4.3 with $B = E^2$.

Let $p = 3$. From now on, let E be the elliptic curve $y^2 = x^3 - x$ over the field $\bar{\mathbb{F}}_3((t))$. The maps $(x, y) \mapsto (a^2 x + b, ay)$ for $b \in \mathbb{F}_3$ and $a \in \mathbb{F}_9 \subset \bar{\mathbb{F}}_3$ with $a^4 = 1$ allow one to realize T_{12} explicitly as a subgroup of $\mathrm{Aut}(E)$. In fact, $\mathrm{Aut}(E) = T_{12}$ (see Appendix A of [27]). Let $B = E^2$. Then $T_{12} \times T_{12} \subset \mathrm{Aut}(B)$. Note that $C_3 \times T_{12}$ and H_{36} are subgroups of $T_{12} \times T_{12}$. Choose $\omega \in \mathrm{Aut}(E)$ of order 3. Then $\begin{pmatrix} \omega & 0 \\ 0 & \omega \end{pmatrix} \in \mathrm{Aut}(B)$, $S_3 \subset \mathrm{GL}_2(\mathbb{Z}) \subset \mathrm{Aut}(B)$, and $C_3 \times S_3 \subset \mathrm{Aut}(B)$. By Theorem 4.3 and Lemma 5.1, we can realize T_{12}, $C_3 \times T_{12}$, H_{36}, S_3, and $C_3 \times S_3$.

To realize H_{24}, fix $a \in \mathbb{F}_9$ with $a^2 = -1$ and define $u \in \mathrm{Aut}(E)$ by $u(x, y) = (-x, ay)$. Then $u^2 = -1$ and $\mathbb{Z}[u] \cong \mathbb{Z}[i]$. Note that $H_{24} \subset \mathrm{GL}_2(\mathbb{Z}[i]) \subset \mathrm{Aut}(B)$,

since $\left(\begin{smallmatrix} 0 & -1 \\ -1 & -1 \end{smallmatrix}\right)$ is an element of order 3 whose subgroup is normalized by the element $\left(\begin{smallmatrix} -1 & \mathrm{i} \\ 1+\mathrm{i} & 1 \end{smallmatrix}\right)$ of order 8. Apply Theorem 4.3 and Lemma 5.1.

To realize H_{72} (and therefore also its subgroups $C_3 \times C_3$ and $C_3 \times C_6$), note that H_{72} is isomorphic to the subgroup of $\mathrm{Aut}(B)$ generated by $C_3 \times C_3$ and $\left(\begin{smallmatrix} 0 & 1 \\ u & 0 \end{smallmatrix}\right)$, and apply Theorem 4.3 and Lemma 5.1.

Let $p = 5$. To realize H_{40} (and therefore also H_{20}), let C be the hyperelliptic curve $y^2 = x^5 - x$ of genus 2 over the local field $\bar{\mathbb{F}}_5((t))$, and let J be the Jacobian of C. Then C and J have good reduction. The maps $(x, y) \mapsto (a^2 x + b, ay)$ for $b \in \mathbb{F}_5$ and $a \in \mathbb{F}_{25}$ with $a^8 = 1$ allow one to view H_{40} as a subgroup of $\mathrm{Aut}(C) \subset \mathrm{Aut}(J)$. Apply Theorem 4.3 and Lemma 5.1.

The above abelian varieties A have potentially good reduction (i.e., $(t, a) = (0, 2)$). Since $G_{v,A} \notin \Sigma_p(0, 1)$, A has purely additive reduction by Theorem 1.7.

Acknowledgments

The authors thank B. Eick and P. Brooksbank for help with GAP, K. Lux for helpful comments on an earlier version of the text, I. R. Shafarevich and S.V. Vostokov for useful conversations about the inverse Galois problem, and the referee for helpful comments that improved the final version of the paper. Silverberg thanks the NSA and NSF for financial support.

Corrigendum: As pointed out by the referee, the hypothesis that the residue field is perfect should have been included in [24].

References

[1] L. Dornhoff, Group Representation Theory, Part A, Marcel Dekker Inc., New York, 1971.
[2] M. Eichler, Über die Idealklassenzahl hyperkomplexer Systeme, Math. Z. 43 (1938) 481–494.
[3] W. Feit, Orders of finite linear groups, in: T. Foguel, J. Minty (Eds.), Proceedings of the First Jamaican Conference on Group Theory and its Applications (Kingston, 1996), University of West Indies, Kingston, 1996, pp. 9–11.
[4] A. Fröhlich, Local fields, in: J.W.S. Cassels, A. Fröhlich (Eds.), Algebraic Number Theory, Thompson Book Company, Washington, 1967, pp. 1–41.
[5] GAP—Groups, Algorithms and Programming, computational discrete algebra system, http://www-gap.dcs.st-and.ac.uk/~gap.
[6] A. Grothendieck, Modèles de Néron et monodromie, in: A. Grothendieck (Ed.), Groupes de monodromie en géométrie algébrique, SGA7 I, Lecture Notes in Mathematics, vol. 288, Springer, Berlin, 1972, pp. 313–523.
[7] T. Ibukiyama, T. Katsura, F. Oort, Supersingular curves of genus two and class numbers, Compositio Math. 57 (1986) 127–152.
[8] J. Igusa, Arithmetic variety of moduli for genus two, Ann. Math. 72 (2) (1960) 612–649.
[9] C. Jansen, K. Lux, R. Parker, R. Wilson, An Atlas of Brauer Characters, London Mathematical Society Monographs, vol. 11, The Clarendon Press, Oxford University Press, New York, 1995.
[10] H. Koch, Über die Galoissche Gruppe der algebraischen Abschliessung eines Potenzreihenkörpers mit endlichem Konstantenkörper, Math. Nachr. 35 (1967) 323–327.

[11] A. Kraus, Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive, Manuscripta Math. 69 (1990) 353–385.
[12] Q. Liu, Courbes stables de genre 2 et leur schéma de modules, Math. Ann. 295 (1993) 201–222.
[13] D. Lorenzini, Groups of components of Néron models of Jacobians, Compositio Math. 73 (1990) 145–160.
[14] O.V. Mel'nikov, A.A. Sharomet, The Galois group of a multidimensional local field of positive characteristic Mat. Sb. 180 (1989) 1132–1147, 1152; Math. USSR Sbornik 67 (1990) 595–610.
[15] H. Minkowski, Gesammelte Abhandlungen, Bd. I, Leipzig, 1911, pp. 212–218 (Zur Theorie der positiven quadratischen Formen, J. Reine Angew. Math. 101 (1887) 196–202).
[16] J-P. Serre, Sur la rationalité des représentations d'Artin, Ann. Math. 72 (1960) 405–420.
[17] J-P. Serre, Lie algebras and Lie groups, Benjamin Publication, New York, 1965; second ed.: Lecture Notes in Mathematics, vol. 1500, Springer, Berlin, 1992.
[18] J-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. 15 (1972) 259–331.
[19] J-P. Serre, Représentations linéaires des groupes finis, third revised ed., Hermann, Paris, 1978.
[20] J-P. Serre, Arithmetic groups, in: C.T.C. Wall (Ed.), Homological Group Theory, LMS Lecture Note Series, vol. 36, Cambridge University Press, Cambridge, 1979, pp. 105–136.
[21] J-P. Serre, Finite subgroups of Lie groups, Moursund Lectures 1998, http://darkwing.uoregon.edu/~math/serre/serre_notes.pdf.
[22] J-P. Serre, J. Tate, Good reduction of abelian varieties, Ann. Math. 88 (2) (1968) 492–517.
[23] A. Silverberg, Fields of definition for homomorphisms of abelian varieties, J. Pure Appl. Algebra 77 (1992) 253–262.
[24] A. Silverberg, Yu.G. Zarhin, Subgroups of inertia groups arising from abelian varieties, J. Algebra 209 (1998) 94–107.
[25] A. Silverberg, Yu.G. Zarhin, Symplectic representations of inertia groups, J. Algebra 238 (2001) 400–410.
[26] A. Silverberg, Yu.G. Zarhin, Polarizations on abelian varieties and self-dual ℓ-adic representations of inertia groups, Compositio Math. 126 (2001) 25–45.
[27] J. Silverman, The Arithmetic of Elliptic Curves, Springer, New York, 1986.
[28] M. Suzuki, Group Theory I, Springer, New York, 1982.
[29] J. Tate, Algebraic Formulas in Arbitrary Characteristic, Appendix 1 in S. Lang, Elliptic Functions, second ed., Springer, New York, 1987.