Math. Res. Lett.
Volume 22, Number 3, 803–839, 2015

GL_2-representations with maximal image

Nathan Jones

For a matrix group $\mathcal{G}$, consider a Galois representation

$$\varphi\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathcal{G}(\hat{\mathbb{Z}})$$

which extends the cyclotomic character. For a broad class of matrix groups $\mathcal{G}$, we prove a theorem characterizing when such a representation has image which is "as large as possible" inside a fixed open subgroup $G \subseteq \mathcal{G}(\hat{\mathbb{Z}})$. As applications, we obtain such a characterization for the Galois representation on the torsion of a simple principally polarized k-dimensional abelian variety A defined over $\mathbb{Q}$ (where $\mathcal{G} = \mathrm{GSp}_{2k}$) and also for the Galois representation on the torsion of a product of k elliptic curves over $\mathbb{Q}$ (where $\mathcal{G} = \{(g_1, \dots, g_k) \in \mathrm{GL}_2^k : \det g_1 = \cdots = \det g_k\}$). Our results are motivated by open image theorems for classes of abelian varieties initiated by Serre in the 1960s.

1. Introduction

Let K be a number field and let E be an elliptic curve defined over K. Consider the action of $G_K := \mathrm{Gal}(\overline{K}/K)$ on the n-torsion $E[n]$ of E, which gives rise to a Galois representation

$$\varphi_{E_K,n}\colon G_K \longrightarrow \mathrm{Aut}(E[n]) \simeq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

Taking the inverse limit over all $n \geq 1$ (ordered by divisibility), one may consider the action of G_K on

$$E_{\mathrm{tors}} := \bigcup_{n=1}^{\infty} E[n],$$

obtaining a continuous homomorphism

$$\varphi_{E_K}: G_K \longrightarrow \mathrm{Aut}(E_{\mathrm{tors}}) \simeq \mathrm{GL}_2(\hat{\mathbb{Z}}),$$

where $\mathrm{GL}_2(\hat{\mathbb{Z}}) = \varprojlim \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. As discussed in [14], it is of interest to understand the image of φ_{E_K}. For example, if $K = \mathbb{Q}$, the image $\varphi_E(G_{\mathbb{Q}})$[1] plays a crucial role in a conjecture of Lang and Trotter which counts primes with fixed Frobenius trace. (This conjecture is still open, although average versions (see [5] and [4]) have been obtained.)

Serre [18] proved that, when E has no complex multiplication, the image of φ_{E_K} is open in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ (i.e. has finite index in $\mathrm{GL}_2(\hat{\mathbb{Z}})$). He also noted that φ_{E_K} can never be surjective when $K = \mathbb{Q}$, because of the following "cyclotomic obstruction."

Let us introduce the notation

$$\begin{aligned} K(E[n]) &:= \overline{K}^{\ker \varphi_{E_K,n}} = K(\text{the } x \text{ and } y\text{-coordinates of all } P \in E[n]), \\ K(E_{\mathrm{tors}}) &:= \overline{K}^{\ker \varphi_{E_K}} = K(\text{the } x \text{ and } y\text{-coordinates of all } P \in E_{\mathrm{tors}}). \end{aligned}$$

Serre noticed that if $K = \mathbb{Q}$, then for some positive integer $d = d_E \geq 1$ we have

$$\begin{aligned} \mathbb{Q}(\sqrt{\Delta_E}) &\subseteq \mathbb{Q}(E[2]) \cap \mathbb{Q}(\mu_d) \\ &\subseteq \mathbb{Q}(E[2]) \cap \mathbb{Q}(E[d]), \end{aligned}$$

where Δ_E denotes the discriminant of any Weierstrass model of E and $\mathbb{Q}(\mu_d)$ denotes the d-th cyclotomic field. By Galois theory, this forces $\varphi_E(G_{\mathbb{Q}}) \subsetneq \mathrm{GL}_2(\hat{\mathbb{Z}})$. More precisely, it implies that

$$\varphi_E(G_{\mathbb{Q}}) \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})_{\chi=\varepsilon} := \left\{ g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : \chi(g) = \varepsilon(g) \right\}, \tag{1}$$

where the "signature"

$$\begin{aligned} \varepsilon \colon \mathrm{GL}_2(\hat{\mathbb{Z}}) &\longrightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \\ &\longrightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})/[\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})] \simeq \{\pm 1\} \end{aligned} \tag{2}$$

is the unique non-trivial character of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ pre-composed with reduction modulo 2 and

$$\chi \colon \mathrm{GL}_2(\hat{\mathbb{Z}}) \longrightarrow \hat{\mathbb{Z}}^\times \longrightarrow \{\pm 1\}$$

[1] When $K = \mathbb{Q}$, we will denote the Galois representation on E_{tors} (resp. on $E[n]$) simply by φ_E (resp. by $\varphi_{E,n}$).

is defined by $\chi(g) = \left(\frac{\Delta_E}{\det g}\right)$, with $\left(\frac{\Delta_E}{\cdot}\right)$ the Kronecker symbol, i.e. the unique character which satisfies $\mathrm{Frob}_p(\sqrt{\Delta_E}) = \left(\frac{\Delta_E}{\mathrm{Frob}_p}\right)\sqrt{\Delta_E}$ for each prime p not dividing d.

Serre also gave examples of elliptic curves E over $\mathbb{Q}$ for which "φ_E has image as large as possible modulo this obstruction," i.e. for which

$$\varphi_E(G_{\mathbb{Q}}) = \mathrm{GL}_2(\hat{\mathbb{Z}})_{\chi=\varepsilon}. \tag{3}$$

Following Lang and Trotter, we call an elliptic curve E over $\mathbb{Q}$ a **Serre curve** if (3) holds. One has

$$E \text{ is a Serre curve } \iff [\mathrm{GL}_2(\hat{\mathbb{Z}}) : \varphi_E(G_{\mathbb{Q}})] = 2. \tag{4}$$

It has been shown (see [10], [3]) that "almost all" elliptic curves E over $\mathbb{Q}$ are Serre curves (see also [15], which, building on [6], gives an asymptotic formula for the number of Serre curves of bounded height).

In the present paper, we consider the following generalization of the above. Fix once and for all a level $m \geq 1$ and a subgroup $G(m) \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, and let

$$G = \pi^{-1}(G(m)) \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}}) \tag{5}$$

be the entire pre-image of $G(m)$ under the canonical projection. Suppose that we have found an elliptic curve E over $\mathbb{Q}$ for which the associated Galois representation maps into G:

$$\varphi_E \colon G_{\mathbb{Q}} \longrightarrow G. \tag{6}$$

Our goal is to describe the analogue of (1) in this context, thus making precise the notion that "φ_E has image as large as possible, given that it lands in G" and allowing us to define the relative concept of a G-**Serre curve**; this is Definition 2.9 below. We will then prove a theorem (see Theorem 2.6) which characterizes G-Serre curves in terms of explicit criteria at finite level.

There is a modular curve $X_{G(m)}$ whose non-cuspidal $\mathbb{Q}$-rational points correspond to j-invariants of elliptic curves E over $\mathbb{Q}$ for which (6) holds (up to $\mathrm{GL}_2(\hat{\mathbb{Z}})$-conjugation). When the genus of $X_{G(m)}$ is zero and $X_{G(m)}(\mathbb{Q}) \neq \emptyset$, one may fix a morphism

$$f \colon \mathbb{A}^1 \longrightarrow X_{G(m)},$$

and count the rational points $t_0 \in \mathbb{Q}$ for which $f(t_0)$ corresponds to a G-Serre curve. One may use the same techniques as in [3] to prove that "almost all elliptic curves in a one-parameter family on $X_{G(m)}$ are G-Serre curves" (see Theorem 2.11). As another application, in [11] we use these results to prove that, when ordered by height, almost all k-tuples of elliptic curves over $\mathbb{Q}$ have division fields with composita "as large as possible."

Finally, we remark that the techniques used in the current paper are exclusively group-theoretical. Consequently, our results are applicable in a wider context than we have stated here; see Theorem 2.18 in Section 2.1. For instance, in Corollary 2.20, we apply Theorem 2.18 to the Galois representation on the torsion of a simple principally polarized k-dimensional abelian variety.

2. Statement of results

To motivate our definitions, we begin by re-examining (1) in more detail. Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication and let Δ_E denote the discriminant of any Weierstrass model of E. Recall that, thanks to the Weil pairing (see [20]), for any $d \geq 1$ the d-th cyclotomic field $\mathbb{Q}(\mu_d)$ is contained in $\mathbb{Q}(E[d])$. Furthermore, choosing a $\mathbb{Z}/d\mathbb{Z}$-basis of $E[d]$ (and thus an imbedding $\iota\colon \operatorname{Gal}(\mathbb{Q}(E[d])/\mathbb{Q}) \to \operatorname{GL}_2(\mathbb{Z}/d\mathbb{Z})$), the following diagram is commutative:

$$\begin{tikzcd}
\operatorname{Gal}(\mathbb{Q}(E[d])/\mathbb{Q}) \arrow[r, "\text{res}"] \arrow[d, "\iota"] & \operatorname{Gal}(\mathbb{Q}(\mu_d)/\mathbb{Q}) \arrow[d] \\
\operatorname{GL}_2(\mathbb{Z}/d\mathbb{Z}) \arrow[r, "\det"] & (\mathbb{Z}/d\mathbb{Z})^\times,
\end{tikzcd} \tag{7}$$

where the unlabeled vertical arrow is the usual (canonical) isomorphism. Since

$$[\operatorname{GL}_2(\mathbb{Z}/2\mathbb{Z}), \operatorname{GL}_2(\mathbb{Z}/2\mathbb{Z})] = (\ker \varepsilon \pmod 2) \subsetneq \operatorname{SL}_2(\mathbb{Z}/2\mathbb{Z}),$$

we see (assuming $\varphi_{E,2}(G_{\mathbb{Q}}) = \operatorname{GL}_2(\mathbb{Z}/2\mathbb{Z})$) that

$$\mathbb{Q} = \mathbb{Q}(\mu_2) = \mathbb{Q}(E[2])^{\operatorname{SL}_2(\mathbb{Z}/2\mathbb{Z})} \subsetneq \mathbb{Q}(E[2])^{[\operatorname{GL}_2(\mathbb{Z}/2\mathbb{Z}), \operatorname{GL}_2(\mathbb{Z}/2\mathbb{Z})]} = \mathbb{Q}(\sqrt{\Delta_E}).$$

Since $\mathbb{Q}(\sqrt{\Delta_E})$ is an abelian extension of $\mathbb{Q}$, it is contained in some $\mathbb{Q}(\mu_d)$, by the Kronecker-Weber Theorem. This containment, together with (7), implies (1).

This may be re-cast as follows. We will denote by

$$\mathbb{Q}^{\mathrm{cyc}} := \bigcup_{d \geq 1} \mathbb{Q}(\mu_d)$$

the cyclotomic closure of $\mathbb{Q}$ and by $\mathbb{Q}^{\mathrm{ab}}$ the maximal abelian extension of $\mathbb{Q}$. By the Kronecker-Weber theorem, one has $\mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}^{\mathrm{ab}}$. Let us denote the Galois representation φ_E simply by φ. The commutator subgroup[2] $[\varphi(G_{\mathbb{Q}}), \varphi(G_{\mathbb{Q}})]$ satisfies

$$[\varphi(G_{\mathbb{Q}}), \varphi(G_{\mathbb{Q}})] \subseteq \varphi(G_{\mathbb{Q}}) \cap \mathrm{SL}_2(\hat{\mathbb{Z}}). \tag{8}$$

Furthermore, by Galois theory (and since $\mathbb{Q}^{\mathrm{cyc}} \subseteq \mathbb{Q}(E_{\mathrm{tors}})$) we have

$$\mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(E_{\mathrm{tors}})^{[\varphi(G_{\mathbb{Q}}), \varphi(G_{\mathbb{Q}})]} \supseteq \mathbb{Q}(E_{\mathrm{tors}})^{\varphi(G_{\mathbb{Q}}) \cap \mathrm{SL}_2(\hat{\mathbb{Z}})} = \mathbb{Q}^{\mathrm{cyc}},$$

which implies that we must have equality in (8):

$$[\varphi(G_{\mathbb{Q}}), \varphi(G_{\mathbb{Q}})] = \varphi(G_{\mathbb{Q}}) \cap \mathrm{SL}_2(\hat{\mathbb{Z}}).$$

This motivates the following definitions.

Definition 2.1. A subgroup $H \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ is called **commutator-thick** if

$$[H, H] = H \cap \mathrm{SL}_2(\hat{\mathbb{Z}}).$$

Definition 2.2. A subgroup $H \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ is called **determinant-surjective** if $\det(H) = \hat{\mathbb{Z}}^\times$.

Remark 2.3. The above discussion shows that $\varphi_E(G_{\mathbb{Q}}) \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ is always a commutator-thick, determinant-surjective subgroup.

As in the previous section, assume now that $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ is a fixed subgroup of finite index, and that $\varphi_E(G_{\mathbb{Q}}) \subseteq G$. The following definition captures the notion that $\varphi_E(G_{\mathbb{Q}})$ is as large as possible, given that it's a subset of G.

Definition 2.4. We call a commutator-thick subgroup $H \subseteq G$ a **G-maximal commutator-thick subgroup of G** if $[H, H] = [G, G]$.

[2] For a profinite group H, we are defining the commutator subgroup $[H, H]$ to be the *closure* of the subgroup generated by its set of commutators $\{xyx^{-1}y^{-1} : x, y \in H\}$.

Remark 2.5. Suppose $H \subseteq G$ is determinant-surjective and commutator-thick. Noting the exact sequence

$$1 \longrightarrow H \cap \mathrm{SL}_2(\hat{\mathbb{Z}}) \longrightarrow H \longrightarrow \hat{\mathbb{Z}}^\times \longrightarrow 1, \tag{9}$$

and that the kernel $H \cap \mathrm{SL}_2(\hat{\mathbb{Z}}) = [H, H] \subseteq [G, G]$, it follows that, if H is a G-maximal commutator-thick subgroup of G in the sense of Definition 2.4, then H is also maximal (with respect to subset inclusion) among the determinant-surjective commutator-thick subgroups of G. Furthermore, it follows from (9) and the corresponding sequence with G replacing H that

$$H \cap \mathrm{SL}_2(\hat{\mathbb{Z}}) = [G, G] \iff [G : H] = \left[G \cap \mathrm{SL}_2(\hat{\mathbb{Z}}) : [G, G] \right].$$

Thus, Definition 2.4 is equivalent to H having minimal index in G among the determinant-surjective commutator-thick subgroups of G.

Our main result gives the following theorem, which explicitly characterizes G-maximal commutator-thick subgroups of G. Recall the set-up: $m \geq 1$ is any positive integer, $G(m) \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ is an arbitrary subgroup, and $G := \pi^{-1}(G(m)) \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ is the full pre-image of $G(m)$ under the natural projection. Define the positive integer m_0 by

$$m_0 := \operatorname{lcm}\left(2^3 \cdot 3^3 \cdot 5^3, \prod_{\substack{\ell \text{ prime} \\ \ell \mid m}} \ell^{2\mathrm{ord}_\ell(m)+1} \right). \tag{10}$$

Theorem 2.6. *With $m \geq 1$ and $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ as in* (5)*, let m_0 be defined by* (10)*. Let $H \subseteq G$ be any subgroup. Then $[H, H] = [G, G]$ if and only if*

$$\begin{aligned} &[H \,(\mathrm{mod}\, n), H \,(\mathrm{mod}\, n)] = [G \,(\mathrm{mod}\, n), G \,(\mathrm{mod}\, n)] \\ &(\forall n \in \{m_0\} \cup \{\ell \textit{ prime} : \ell \nmid m_0\}). \end{aligned} \tag{11}$$

In particular, if H is commutator-thick, then H is a G-maximal commutator-thick subgroup if and only if (11) *holds.*

We remark that, since for any prime $\ell \geq 5$, $[\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}), \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})] = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ (this follows because $\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is simple for $\ell \geq 5$), Theorem 2.6 is equivalent to the following theorem.

Theorem 2.7. *With $m \geq 1$ and $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ as in* (5)*, let m_0 be defined by* (10)*. Let $H \subseteq G$ be any subgroup. Then $[H,H] = [G,G]$ if and only if the following two conditions hold.*

1) *For each prime ℓ not dividing m_0, one has $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \subseteq H \pmod{\ell}$.*
2) *One has $[H \pmod{m_0}, H \pmod{m_0}] = [G \pmod{m_0}, G \pmod{m_0}]$.*

In particular, if H is commutator-thick, then H is a G-maximal commutator-thick subgroup if and only if conditions (1) and (2) above hold.

In applications, it is often useful to have the level m_0 given explicitly in terms of m, which is part of the motivation for our theorem.

Remark 2.8. If each prime ℓ which divides m satisfies $\ell \not\equiv \pm 1 \pmod 5$, then Theorems 2.6 and 2.7 hold with

$$m_0 = \mathrm{lcm}\left(2^3 \cdot 3^3, \prod_{\substack{\ell \text{ prime} \\ \ell \mid m}} \ell^{2\mathrm{ord}_\ell(m)+1} \right). \tag{12}$$

Returning to our original example of an elliptic curve, we make the following definition.

Definition 2.9. Let $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ be an open subgroup. An elliptic curve E over $\mathbb{Q}$ which satisfies $\varphi_E(G_{\mathbb{Q}}) \subseteq G$ is called a ***G*-Serre curve** if $\varphi_E(G_{\mathbb{Q}})$ is a G-maximal commutator-thick subgroup. If the group G is understood, one may refer to a G-Serre curve simply as a **relative Serre curve**.

As an immediate corollary of Theorem 2.6, we will give a characterization of G-Serre curves. For any positive integer $n \geq 1$ denote by $G(n)$ the reduction of G modulo n, viewed as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, and define the following set of subgroups of $G(n)$:

$$\mathcal{M}_G(n) := \{H \subseteq G(n) : [H,H] \subsetneq [G(n), G(n)]\}.$$

Note that, for any prime ℓ not dividing m_0,

$$\mathcal{M}_G(\ell) = \{H \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \not\subseteq H\}.$$

Also, let $X(n)$ denote the complete modular curve of level n, which parametrizes elliptic curves together with chosen $\mathbb{Z}/n\mathbb{Z}$-bases of $E[n]$. Let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ satisfying $-I \in H$ and for which the determinant map

$$\det\colon H \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$

is surjective, and consider the quotient curve $X_H := X(n)/H$ together with the j-invariant

$$j\colon X_H \longrightarrow \mathbb{P}^1.$$

Any $x \in \mathbb{P}^1(\mathbb{Q})$ is in the image of j if and only if there exists an elliptic curve E over $\mathbb{Q}$ with j-invariant x for which $\varphi_{E,n}(G_\mathbb{Q})$ is contained in a subgroup conjugate to H in $GL_2(\mathbb{Z}/n\mathbb{Z})$.

We define the following set of modular curves:

$$\mathcal{X}_G := \left(\bigcup_{\substack{\ell \text{ prime} \\ \ell \nmid m_0}} \{X_H : H \in \mathcal{M}_G(\ell)\} \right) \cup \{X_H : H \in \mathcal{M}_G(m_0)\}.$$

Now suppose we choose the group

$$G = \pi^{-1}(G(m)) \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$$

as above so that the corresponding modular curve $X_{G(m)}$ has genus zero and satisfies $X_{G(m)}(\mathbb{Q}) \neq \emptyset$, and suppose that

$$\mathbb{E}\colon y^2 = x^3 + A(t)x + B(t) \qquad (A(t), B(t) \in \mathbb{Q}(t))$$

is an elliptic curve over $\mathbb{Q}(t)$ satisfying

$$\varphi_{\mathbb{E},\mathbb{Q}(t)}(G_{\mathbb{Q}(t)}) = G. \tag{13}$$

(Note in particular that $\mathbb{E}$ then defines a morphism $\mathbb{P}^1 \longrightarrow X_{G(m)}$.) For a real parameter $T \geq 0$, define the sets

$$\begin{aligned}
\mathcal{F}_\mathbb{E}(T) &:= \{t_0 \in \mathbb{Q} : \mathcal{H}(t_0) \leq T,\ E_{t_0}/\mathbb{Q} \text{ is an elliptic curve}\}, \\
\mathcal{E}_{\mathbb{E},\text{non-}G\text{-Serre}}(T) &:= \{t_0 \in \mathcal{F}_\mathbb{E}(T) : E_{t_0} \text{ is not a } G\text{-Serre curve}\}, \\
\mathcal{E}_{\mathbb{E},X_H}(T) &:= \{t_0 \in \mathcal{F}_\mathbb{E}(T) : j_\mathbb{E}(t_0) \in \mathbb{Q} \text{ is the image under } j \text{ of} \\
&\qquad \text{a point in } X_H(\mathbb{Q})_{\text{non-cusp.}}\},
\end{aligned}$$

where E_{t_0} denotes the specialization of $\mathbb{E}$ at t_0, $\mathcal{H}(t_0)$ denotes the height of t_0 (i.e. if we write $t_0 = a/b$ in lowest terms, $\mathcal{H}(a/b) := \max\{|a|, |b|\}$), and $j\colon X_H \longrightarrow \mathbb{P}^1$ denotes the j-map associated to X_H. We have the following corollary of Theorem 2.6.

Corollary 2.10. *Let $m \geq 1$ and $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ be as in* (5)*, and let $\mathbb{E}/\mathbb{Q}(t)$ be an elliptic curve satisfying* (13)*. Then, for any $T \geq 0$,*

$$\mathcal{E}_{\mathbb{E},\textit{non-G-Serre}}(T) = \bigcup_{X_H \in \mathcal{X}_G} \mathcal{E}_{\mathbb{E},X_H}(T).$$

Corollary 2.10 allows us to deduce the following generalization of [3, Main Theorem].

Theorem 2.11. *Let $\varepsilon > 0$ be arbitrary. One has*

$$|\mathcal{E}_{\mathbb{E},\textit{non-G-Serre}}(T)| = O_{\mathbb{E},\varepsilon}(T^{1+\varepsilon}).$$

Since $|\mathcal{F}_{\mathbb{E}}(T)| \asymp T^2$, Theorem 2.11 implies that “almost all specializations of $\mathbb{E}$ are G-Serre curves.” The main theorem of [3] gives Theorem 2.11 when $G = \mathrm{GL}_2(\hat{\mathbb{Z}})$, and also gives much better bounds in some cases. The proof of Theorem 2.11 proceeds along the same lines (with Corollary 2.10 replacing [3, Corollary 19]), and also gives better bounds in the appropriate cases. For the sake of brevity, Theorem 2.11 states only the weakest form of what one can deduce from Corollary 2.10, and (since its proof is exactly the proof of [3, Main Theorem], mutatis mutandis) we will not include it in the present paper.

2.1. The general case

The definitions and theorems we have described apply more generally to the following situation. Let $r \geq 1$ be a positive integer and let $\mathcal{G} \subseteq \mathrm{GL}_r$ be any matrix group, i.e. $\mathcal{G}$ is subgroup scheme of GL_r. Assume further that there is a homomorphism $\delta \colon \mathcal{G} \longrightarrow \mathrm{GL}_1$ for which $\mathcal{G}(\hat{\mathbb{Z}}) \longrightarrow \mathrm{GL}_1(\hat{\mathbb{Z}})$ is surjective, and let $\mathcal{S} := \ker \delta$ denote its kernel, which is also a matrix group. We have an exact sequence

$$1 \longrightarrow \mathcal{S}(\hat{\mathbb{Z}}) \longrightarrow \mathcal{G}(\hat{\mathbb{Z}}) \xrightarrow{\delta} \hat{\mathbb{Z}}^\times \longrightarrow 1.$$

Note that (since they are algebraic groups) the Chinese remainder theorem holds for $\mathcal{G}$ and for $\mathcal{S}$:

$$\mathcal{G}(\hat{\mathbb{Z}}) \simeq \prod_{\ell \text{ prime}} \mathcal{G}(\mathbb{Z}_\ell), \qquad \mathcal{S}(\hat{\mathbb{Z}}) \simeq \prod_{\ell \text{ prime}} \mathcal{S}(\mathbb{Z}_\ell). \tag{14}$$

We will be considering the reductions of $\mathcal{G}(\hat{\mathbb{Z}})$ and $\mathcal{S}(\hat{\mathbb{Z}})$ modulo positive integers, and so we make the definitions

$$\mathcal{G}(m) := \mathcal{G}(\hat{\mathbb{Z}})(\operatorname{mod} m), \qquad \mathcal{S}(m) := \mathcal{S}(\hat{\mathbb{Z}})(\operatorname{mod} m). \tag{15}$$

It follows from (14) that, for any positive integer m, one has

$$\mathcal{G}(m) \simeq \prod_{\ell^{n_\ell} \| m} \mathcal{G}(\ell^{n_\ell}), \qquad \mathcal{S}(m) \simeq \prod_{\ell^{n_\ell} \| m} \mathcal{S}(\ell^{n_\ell}).$$

The subsets $\mathfrak{g}_{\ell^n} \subseteq M_{r\times r}(\mathbb{Z}_\ell)$ and $\mathfrak{s}_{\ell^n} \subseteq M_{r\times r}(\mathbb{Z}_\ell)$ defined by the exact sequences

$$1 \longrightarrow I + \ell^n \mathfrak{g}_{\ell^n} \longrightarrow \mathcal{G}(\mathbb{Z}_\ell) \longrightarrow \mathcal{G}(\ell^n) \longrightarrow 1 \tag{16}$$

and

$$1 \longrightarrow I + \ell^n \mathfrak{s}_{\ell^n} \longrightarrow \mathcal{S}(\mathbb{Z}_\ell) \longrightarrow \mathcal{S}(\ell^n) \longrightarrow 1 \tag{17}$$

will play an important role for us, and in particular, we will consider their reductions modulo ℓ. We define $\mathfrak{g}_{\ell^n}(\ell), \mathfrak{s}_{\ell^n}(\ell) \subseteq M_{r\times r}(\mathbb{Z}/\ell\mathbb{Z})$ to be the reductions modulo ℓ of $\mathfrak{g}_{\ell^n}$ and $\mathfrak{s}_{\ell^n}$ respectively, so that there is an exact sequence

$$1 \longrightarrow I + \ell^n \mathfrak{s}_{\ell^n}(\ell) \longrightarrow \mathcal{S}(\ell^{n+1}) \longrightarrow \mathcal{S}(\ell^n) \longrightarrow 1.$$

It follows from the proof of [17, Lemma 3, IV-23] that we have an increasing sequence of $\mathbb{Z}/\ell\mathbb{Z}$-vector spaces

$$\begin{array}{ll} \mathfrak{s}_\ell(\ell) \subseteq \mathfrak{s}_{\ell^2}(\ell) \subseteq \cdots \subseteq \mathfrak{s}_{\ell^n}(\ell) \subseteq \cdots \subseteq M_{r\times r}(\mathbb{Z}/\ell\mathbb{Z}) & (\ell \text{ odd}) \\ \mathfrak{s}_4(2) \subseteq \mathfrak{s}_8(2) \subseteq \cdots \subseteq \mathfrak{s}_{2^n}(2) \subseteq \cdots \subseteq M_{r\times r}(\mathbb{Z}/2\mathbb{Z}) & (\ell = 2), \end{array}$$

which must stabilize. We will assume that this sequence stabilizes immediately, i.e. we will assume that for any prime ℓ,

$$\mathfrak{s}_\ell(\ell) = \mathfrak{s}_{\ell^2}(\ell) = \cdots = \mathfrak{s}_{\ell^n}(\ell) = \cdots \subseteq M_{r\times r}(\mathbb{Z}/\ell\mathbb{Z}).$$

Fix now a positive integer $m \geq 1$ and an arbitrary subgroup $G(m) \subseteq \mathcal{G}(m)$, and let

$$G := \{g \in \mathcal{G}(\hat{\mathbb{Z}}) : g\,(\operatorname{mod} m) \in G(m)\} \tag{18}$$

denote the corresponding finite index subgroup of $\mathcal{G}(\hat{\mathbb{Z}})$. Furthermore, suppose that

$$\varphi\colon G_{\mathbb{Q}} \longrightarrow G$$

is any Galois representation for which $\delta \circ \varphi\colon G_{\mathbb{Q}} \longrightarrow \hat{\mathbb{Z}}^\times$ agrees with the cyclotomic character. In this context, Definition 2.1 may be phrased as follows.

Definition 2.12. A subgroup $H \subseteq \mathcal{G}(\hat{\mathbb{Z}})$ is called **commutator-thick** if

$$[H, H] = H \cap \mathcal{S}(\hat{\mathbb{Z}}).$$

Definition 2.4 remains the same, and we replace Definition 2.2 with

Definition 2.13. A subgroup $H \subseteq \mathcal{G}(\hat{\mathbb{Z}})$ is called **δ-surjective** if $\delta(H) = \hat{\mathbb{Z}}^\times$.

We remark that (for the same reason as in the GL$_2$ case) the image $\varphi(G_{\mathbb{Q}})$ must be commutator-thick and δ-surjective.

Following [17, IV-25], we make the following definition.

Definition 2.14. Given a topological group G and a finite simple group Σ we say that Σ **occurs in** G if and only if there are closed subgroups $G_1 \subseteq G$ and $G_2 \subseteq G_1$ with G_2 a normal subgroup of G_1 and such that $G_1/G_2 \simeq \Sigma$.

Let us now make the following assumptions about the groups $\mathcal{G}$ and $\mathcal{S}$. Recall that $\mathfrak{g}_{\ell^n}(\ell) := \mathfrak{g}_{\ell^n} \pmod{\ell}$ and $\mathfrak{s}_{\ell^n}(\ell) := \mathfrak{s}_{\ell^n} \pmod{\ell}$, with $\mathfrak{g}_{\ell^n}, \mathfrak{s}_{\ell^n} \subseteq M_{r\times r}(\mathbb{Z}_\ell)$ as in (16) and (17).

A0 For any prime ℓ and any $n \geq 1$, one has $\mathfrak{s}_{\ell^n}(\ell) = \mathfrak{s}_\ell(\ell)$.

A1 There is a finite set $\mathcal{L}$ of primes such that, for any prime $\ell \notin \mathcal{L}$ there is a finite simple non-abelian group $\mathcal{PS}(\ell)$ and a finite set of surjective homomorphisms

$$\varpi_i\colon \mathcal{S}(\ell) \twoheadrightarrow \mathcal{PS}(\ell)$$

satisfying the conditions

$$\begin{gathered}\forall \text{ normal subgroup } N \trianglelefteq \mathcal{S}(\ell),\\ \text{either } N \subseteq \ker \varpi_i \text{ for some } i, \text{ or } N = \mathcal{S}(\ell)\end{gathered} \tag{19}$$

and

$$\forall \text{ prime } \ell',\ \ell' \neq \ell \Longrightarrow \mathcal{PS}(\ell) \text{ does } \textit{not} \text{ occur in } \mathcal{S}(\ell'). \tag{20}$$

We will assume for convenience that $\{2,3\} \subseteq \mathcal{L}$.

A2 For any prime ℓ, one has

$$\langle CD - DC : C, D \in \mathfrak{g}_\ell(\ell) \rangle = \mathfrak{s}_\ell(\ell).$$

A3 For every prime ℓ, $\mathfrak{s}_\ell(\ell)$ may be generated as a $\mathbb{Z}/\ell\mathbb{Z}$-vector space by a set of matrices $\{u_i\}$ which satisfy

$$\begin{aligned} &\forall i,\, u_i^2 = 0 \\ &\forall i,\, I + u_i \in \mathcal{S}(\ell). \end{aligned}$$

Remark 2.15. The discussion in [17, IV-25] shows that assumption A1 implies that in fact, for any prime $\ell \notin \mathcal{L}$ and any positive integer n,

$$\begin{aligned} &\big(\forall \ell' \mid n,\ \mathcal{PS}(\ell) \text{ does not occur in } \mathcal{S}(\ell')\big) \\ &\Longrightarrow \mathcal{PS}(\ell) \text{ does } \textit{not} \text{ occur in } \prod_{\ell' \mid n} \mathcal{S}(\mathbb{Z}_{\ell'}). \end{aligned} \tag{21}$$

Remark 2.16. Taken together with the proof of [17, Lemma 3, IV-23], assumption A0 implies that, for each prime ℓ, there is an exponent $e_\ell \leq 3$ such that, whenever $K \subseteq \mathcal{S}(\mathbb{Z}_\ell)$ is a closed subgroup and $K \pmod{\ell^{e_\ell}} = \mathcal{S}(\ell^{e_\ell})$, one has $K = \mathcal{S}(\mathbb{Z}_\ell)$. If ℓ is an odd prime, one may take $e_\ell \leq 2$. Assumption A3 additionally implies that $e_2, e_3 \leq 2$, and $e_\ell = 1$ for any prime $\ell \geq 5$.

Remark 2.17. For all but finitely many prime powers ℓ^n, we have that $\mathcal{G}(\mathbb{Z}/\ell^n\mathbb{Z})$ (resp. $\mathcal{S}(\mathbb{Z}/\ell^n\mathbb{Z})$) consists entirely of smooth points. For such primes, it follows that $\mathcal{G}(\mathbb{Z}/\ell^n\mathbb{Z}) = \mathcal{G}(\ell^n)$ (resp. $\mathcal{S}(\mathbb{Z}/\ell^n\mathbb{Z}) = \mathcal{S}(\ell^n)$), and also that assumption A0 holds. In particular, assumption A0 need only be verified for a finite set $\mathcal{B}$ of "bad" primes ℓ for which $\mathcal{G}(\mathbb{Z}/\ell\mathbb{Z})$ (resp. $\mathcal{S}(\mathbb{Z}/\ell\mathbb{Z})$) contains singular points. For these primes, it is possible that $\mathcal{S}(\ell^n) \subsetneq \mathcal{S}(\mathbb{Z}/\ell^n\mathbb{Z})$ for some $n \geq 1$. In particular, the sequence

$$1 \longrightarrow \mathcal{S}(m) \longrightarrow \mathcal{G}(m) \xrightarrow{\delta} (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow 1$$

may fail to be exact when m is divisible by a prime $\ell \in \mathcal{B}$.

We now define

$$m_0 := \operatorname{lcm}\left(\prod_{\ell \in \mathcal{L}} \ell^3 \, , \prod_{\substack{\ell \text{ prime} \\ \ell | m}} \ell^{2\operatorname{ord}_\ell(m)+1} \right). \tag{22}$$

We will prove the following general theorem, of which Theorem 2.6 is a special case.

Theorem 2.18. *Let $\mathcal{G} \subseteq \mathrm{GL}_r$ be any matrix group satisfying assumptions A0, A1, A2, and A3 above, and for any $m \in \mathbb{N}$, define $\mathcal{G}(m)$ by* (15)*. Let $G(m) \subseteq \mathcal{G}(m)$ be any subgroup and $G \subseteq \mathcal{G}(\hat{\mathbb{Z}})$ the corresponding finite index subgroup defined by* (18)*. Define m_0 by* (22)*. Let $H \subseteq G$ be any subgroup. Then $[H,H] = [G,G]$ if and only if the following two conditions hold.*

1) *For each prime ℓ not dividing m_0, one has $[H \pmod{\ell}, H \pmod{\ell}] = [G \pmod{\ell}, G \pmod{\ell}]$.*
2) *One has $[H \pmod{m_0}, H \pmod{m_0}] = [G \pmod{m_0}, G \pmod{m_0}]$.*

In particular, if H is commutator-thick, then H is a G-maximal commutator-thick subgroup if and only if conditions (1) and (2) above hold.

Remark 2.19. Remark 2.16 together with assumptions A1 and A3 imply that for any $\ell \notin \mathcal{L}$ and any $n \geq 1$, one has

$$[\mathcal{S}(\ell^n), \mathcal{S}(\ell^n)] = \mathcal{S}(\ell^n)$$

and also

$$N \trianglelefteq \mathcal{S}(\ell^n) \implies \begin{cases} N \pmod{\ell} \subseteq \ker \varpi_i \text{ for some } i, \text{ or} \\ N = \mathcal{S}(\ell^n). \end{cases} \tag{23}$$

In particular, condition (1) in Theorem 2.18 is equivalent to

For each prime ℓ not dividing m_0, one has $\mathcal{S}(\ell) \subseteq H \pmod{\ell}$.

In Section 6, we apply Theorem 2.18 to the Galois representation φ_A on the torsion of a k-dimensional simple principally polarized abelian variety A over $\mathbb{Q}$, which maps into $\mathcal{G}(\hat{\mathbb{Z}})$ for $\mathcal{G} = \mathrm{GSp}_{2k}$, the group of degree k

symplectic similitudes. Fix any subgroup $G(m) \subseteq \mathrm{GSp}_{2k}(\mathbb{Z}/m\mathbb{Z})$ and let

$$G = \pi^{-1}_{\mathrm{GSp}_{2k}(\hat{\mathbb{Z}})}(G(m)) \subseteq \mathrm{GSp}_{2k}(\hat{\mathbb{Z}}) \tag{24}$$

be the corresponding finite index subgroup of $\mathrm{GSp}_{2k}(\hat{\mathbb{Z}})$. In this case m_0 is given by

$$m_0 = \mathrm{lcm}\left(2^3 \cdot 3^3, \prod_{\substack{\ell \text{ prime} \\ \ell | m}} \ell^{2\mathrm{ord}_\ell(m)+1}\right). \tag{25}$$

Corollary 2.20. *Let A be a simple principally polarized abelian variety over $\mathbb{Q}$ of dimension $k \geq 2$ and assume that $\varphi_A(G_\mathbb{Q}) \subseteq G$, where G is as in (24). Define m_0 by (25). The image $\varphi_A(G_\mathbb{Q}) \subseteq G$ is a G-maximal commutator-thick subgroup if and only if the following conditions hold.*

1) *For each prime $\ell \nmid m_0$, one has $\mathrm{Sp}_{2k}(\mathbb{Z}/\ell\mathbb{Z}) \subseteq \varphi_A(G_\mathbb{Q}) \pmod{\ell}$.*
2) *One has*

$$[\varphi_A(G_\mathbb{Q}) \pmod{m_0}, \varphi_A(G_\mathbb{Q}) \pmod{m_0}] = [G \pmod{m_0}, G \pmod{m_0}].$$

Finally, we apply our study to the Galois representation $\varphi_{(E_i)}$ on the torsion of a k-tuple $(E_1, \dots, E_k)$ of elliptic curves E_i over $\mathbb{Q}$, in which case the appropriate group $\mathcal{G}$ is

$$\mathcal{G} = (\mathrm{GL}_2)^k_\Delta := \{(g_1, g_2, \dots, g_k) \in \mathrm{GL}_2^k : \det g_1 = \det g_2 = \cdots = \det g_k\}.$$

Indeed, one has

$$\varphi_{(E_i)} \colon G_\mathbb{Q} \longrightarrow (\mathrm{GL}_2)^k_\Delta(\hat{\mathbb{Z}}).$$

In analogy with (4), we make the following definition.

Definition 2.21. A k-tuple $(E_1, \dots, E_k)$ of elliptic curves over $\mathbb{Q}$ is a **Serre k-tuple** if

$$[(\mathrm{GL}_2)^k_\Delta(\hat{\mathbb{Z}}) : \varphi_{(E_i)}(G_\mathbb{Q})] = 2^k.$$

A Serre k-tuple is a k-tuple for which $\varphi_{(E_i)}(G_\mathbb{Q})$ is as large as possible. In Section 6, we obtain the following corollary.

Corollary 2.22. *The k-tuple $(E_1, E_2, \dots, E_k)$ is a Serre k-tuple if and only if the following conditions hold.*

1) *For each prime* $\ell \geq 5$*, one has* $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})^k \subseteq \big(\varphi_{(E_i)}(G_{\mathbb{Q}}) \pmod{\ell}\big)$.
2) *One has* $[\varphi_{(E_i)}(G_{\mathbb{Q}}) \pmod{36}, \varphi_{(E_i)}(G_{\mathbb{Q}}) \pmod{36}] = (\mathrm{SL}_2(\mathbb{Z}/36\mathbb{Z}) \cap \ker\varepsilon)^k$*, where* ε *is as in* (2).

The special case $k = 1$ gives the following corollary, which improves [10, Lemma 5] to an "if and only-if" statement.

Corollary 2.23. *An elliptic curve* E *over* $\mathbb{Q}$ *is a Serre curve if and only if the following two conditions hold.*

1) *For each prime* $\ell \geq 5$*, one has* $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \subseteq \varphi_{E,\ell}(G_{\mathbb{Q}})$.
2) *One has* $[\varphi_{E,36}(G_{\mathbb{Q}}), \varphi_{E,36}(G_{\mathbb{Q}})] = \mathrm{SL}_2(\mathbb{Z}/36\mathbb{Z}) \cap (\ker\varepsilon \pmod{36})$*, where* ε *is as in* (2).

In [11], Corollary 2.22 is used to prove that, when ordered by height, almost all k-tuples (E_i) are Serre k-tuples.

Remark 2.24. The fact that $\varphi_E(G_{\mathbb{Q}})$ must be commutator-thick is a consequence of the Kronecker-Weber theorem, and so one cannot draw the same conclusion if E is defined over a number field $K \neq \mathbb{Q}$. Indeed, as shown in [7] (see also [21]), there are number fields K and elliptic curves E over K for which $\varphi_{E_K}(G_K) = \mathrm{GL}_2(\hat{\mathbb{Z}})$, and (by (34) below) $\mathrm{GL}_2(\hat{\mathbb{Z}})$ is not commutator-thick.

3. Notation and preliminaries

Throughout the paper, we will use the following notation. For positive integers n and m, we will write

$$n \mid m^\infty$$

to mean that, for every prime number p, if p divides n then p divides m. The symbols p and ℓ will always denote prime numbers. We use the usual notation

$$\hat{\mathbb{Z}} := \lim_{\leftarrow} \mathbb{Z}/m\mathbb{Z}$$

for the inverse limit of the projective system $\{\mathbb{Z}/m_1\mathbb{Z} \to \mathbb{Z}/m_2\mathbb{Z} : m_1, m_2 \geq 1,\ m_2 \mid m_1\}$. The Chinese remainder theorem gives an isomorphism

$$\hat{\mathbb{Z}} \simeq \prod_\ell \mathbb{Z}_\ell,$$

where $\mathbb{Z}_\ell$ denotes the ring of ℓ-adic integers. We will often make implicit use of this isomorphism. For any fixed positive integer m, we will denote by $\mathbb{Z}_m$ (respectively by $\mathbb{Z}_{(m)}$) the quotient of $\hat{\mathbb{Z}}$ which corresponds under this isomorphism to $\prod_{\ell \mid m} \mathbb{Z}_\ell$ (respectively to $\prod_{\ell \nmid m} \mathbb{Z}_\ell$). Given a subgroup $H \subseteq \mathrm{GL}_r(\hat{\mathbb{Z}})$, we will denote by H_m the image of H under the canonical projection $\mathrm{GL}_r(\hat{\mathbb{Z}}) \to \mathrm{GL}_r(\mathbb{Z}_m)$, by $H_{(m)}$ the image of H under $\mathrm{GL}_r(\hat{\mathbb{Z}}) \to \mathrm{GL}_r(\mathbb{Z}_{(m)})$, and by $H(m)$ the image of H under $\mathrm{GL}_r(\hat{\mathbb{Z}}) \to \mathrm{GL}_r(\mathbb{Z}/m\mathbb{Z})$. We will overwork the symbol π, using it to denote any of the following canonical projections:

$$\begin{aligned} \pi \colon \mathcal{G}(\hat{\mathbb{Z}}) &\longrightarrow \mathcal{G}(\mathbb{Z}_m) \\ \pi \colon \mathcal{G}(\hat{\mathbb{Z}}) &\longrightarrow \mathcal{G}(m) \\ \pi \colon \mathcal{G}(m_1) &\longrightarrow \mathcal{G}(m_2) \qquad (m_2 \mid m_1). \end{aligned}$$

As a consequence of the convention mentioned in Section 2.1, $\mathcal{G}(m)$ is always equal to the image modulo m of $\mathcal{G}(\hat{\mathbb{Z}})$, so that each of these maps is *surjective*. In some cases we will use π_H to denote the restriction of any of these projections to a subgroup H; hopefully the meaning will be clear from context.

For a pair of elements h and k in any group, we will use the standard notation for the commutator:

$$[h, k] := hkh^{-1}k^{-1}.$$

For any positive integer M and any prime ℓ dividing M, consider the kernel of the reduction modulo M/ℓ map:

$$I + \frac{M}{\ell}\left(\frac{M_{r\times r}(\mathbb{Z}/M\mathbb{Z})}{\ell M_{r\times r}(\mathbb{Z}/M\mathbb{Z})}\right) \subseteq M_{r\times r}(\mathbb{Z}/M\mathbb{Z}).$$

In light of the isomorphism $\frac{M_{r\times r}(\mathbb{Z}/M\mathbb{Z})}{\ell M_{r\times r}(\mathbb{Z}/M\mathbb{Z})} \simeq M_{r\times r}(\mathbb{Z}/\ell\mathbb{Z})$, we will use the abbreviated notation

$$I + \frac{M}{\ell} M_{r\times r}(\mathbb{Z}/\ell\mathbb{Z}) \subseteq M_{r\times r}(\mathbb{Z}/M\mathbb{Z}),$$

and refer to $I + \frac{M}{\ell}A \in M_{r\times r}(\mathbb{Z}/M\mathbb{Z})$ when $A \in M_{r\times r}(\mathbb{Z}/\ell\mathbb{Z})$, hoping that this will not cause too much confusion. In particular, we will use $\mathfrak{g}_\ell(\ell)$ and

$\mathfrak{s}_\ell(\ell)$ in the exact sequences

$$1 \longrightarrow I + \ell^n \mathfrak{g}_\ell(\ell) \longrightarrow \mathcal{G}(\ell^{n+1}) \longrightarrow \mathcal{G}(\ell^n) \longrightarrow 1$$

and

$$1 \longrightarrow I + \ell^n \mathfrak{s}_\ell(\ell) \longrightarrow \mathcal{S}(\ell^{n+1}) \longrightarrow \mathcal{S}(\ell^n) \longrightarrow 1.$$

4. Proof of Theorem 2.18

In this section, we will prove Theorem 2.18. Note that the "only if" part is trivial, so we will focus on the "if" part. We remark that many of the essential ideas are already present in the proof of the Proposition on page IV-19 of [17], wherein a slightly weaker hypothesis than that of Theorem 2.18 is used to deduce that H is an open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$. We begin with some preparatory lemmas.

4.1. Preparatory lemmas

Our first lemma will be used repeatedly throughout the paper.

Lemma 4.1. *(Goursat's Lemma) Let G_0 and G_1 be groups and $G \subseteq G_0 \times G_1$ a subgroup satisfying*

$$\pi_i(G) = G_i \qquad (i \in \{0, 1\}),$$

where π_i denotes the canonical projection onto the i-th factor. Let $N_i := \pi_i(G \cap \ker \pi_{1-i})$. Then there is an isomorphism of groups $\psi\colon G_0/N_0 \to G_1/N_1$ (whose graph is induced by G) for which

$$G = \{(g_0, g_1) \in G_0 \times G_1 : \psi(g_0 N_0) = g_1 N_1\}.$$

Proof. See [16, Lemma (5.2.1)], which shows that the image of G in $G_0/N_0 \times G_1/N_1$ is the graph of an isomorphism ψ. Thus, $G \subseteq \{(g_0, g_1) \in G_0 \times G_1 : \psi(g_0 N_0) = g_1 N_1\}$. Now note that $N_0 \times N_1 \subseteq G$, from which the equality follows. □

Remark 4.2. When applying Lemma 4.1 in this paper, we will usually formulate the conclusion equivalently as "then there exists a group Q and surjective homomorphisms $\psi_0\colon G_0 \to Q$, $\psi_1\colon G_1 \to Q$ for which $G = \{(g_0, g_1) \in G_0 \times G_1 : \psi_0(g_0) = \psi_1(g_1)\}$."

The following corollary may be viewed as a “fibered version” of Lemma 4.1. Suppose now that G_0 and G_1 are groups, together with surjective homomorphisms

$$\eta_0 \colon G_0 \longrightarrow R, \quad \eta_1 \colon G_1 \longrightarrow R$$

onto a fixed group R. Let

$$G_0 \times_R G_1 := \{(g_0, g_1) \in G_0 \times G_1 : \eta_0(g_0) = \eta_1(g_1)\}$$

denote the fibered product of G_0 and G_1 over R.

Corollary 4.3. *Suppose that $G \subseteq G_0 \times_R G_1$ is any subgroup satisfying $\pi_i(G) = G_i$ for $i \in \{0,1\}$. Then there is a group Q together with surjective homomorphisms $f \colon Q \to R$, $\psi_0 \colon G_0 \to Q$, and $\psi_1 \colon G_1 \to Q$ for which $f \circ \psi_i = \eta_i$ ($i \in \{0,1\}$), and*

$$G = \{(g_0, g_1) \in G_0 \times G_1 : \psi_0(g_0) = \psi_1(g_1)\}.$$

Proof. We apply Lemma 4.1 and note that there is a well-defined surjective group homomorphism

$$\begin{aligned} f \colon Q \simeq G_i/N_i &\to R \qquad (i \in \{0,1\}) \\ g_i N_i &\mapsto \eta_i(g_i). \end{aligned}$$

The corollary follows. □

4.2. Working in $\mathcal{G}(\mathbb{Z}_{m_0})$

Lemma 4.4. *Fix a prime number ℓ, an exponent $n \geq 1$, and a pair of matrices $C, D \in M_{r\times r}(\mathbb{Z}_\ell)$. Then one has*

$$[I + \ell^n C, I + \ell^n D] = I + \ell^{2n}(CD - DC) + \ell^{3n} E,$$

where $E \in M_{r\times r}(\mathbb{Z}_\ell)$.

Proof. A calculation, using the series representation $(I + \ell^n C)^{-1} = I - \ell^n C + \ell^{2n} C^2 - \ell^{3n} C^3 + \cdots$ verifies the statement of the lemma. □

Recall that an integer m_0 is called *square-full* if, for each prime ℓ, one has

$$\ell \mid m_0 \implies \ell^2 \mid m_0.$$

Lemma 4.5. *Let ℓ be any prime number and let $A \in M_{r\times r}(\mathbb{Z}/\ell\mathbb{Z})$. Suppose that m_0 is any positive square-full integer divisible by ℓ^2, and in case $\ell = 2$ assume further either that 8 divides m_0 or that $A^2 \equiv 0 \,(\mathrm{mod}\, 2)$. Let $H \subseteq \mathrm{GL}_r(\mathbb{Z}_{m_0})$ be any subgroup and let M be any multiple of m_0 satisfying $m_0 \mid M \mid m_0^\infty$. We then have*

$$I + \frac{m_0}{\ell} A \in H(m_0) \implies I + \frac{M}{\ell} A \in H(M).$$

Proof. The proof is by induction on M, the base case $M = m_0$ being trivial. If $M > m_0$, then there is a prime p dividing M for which $m_0 \mid M/p$. By induction, we have that

$$I + \frac{m_0}{\ell} A \in H(m_0) \implies I + \frac{M/p}{\ell} A \in H\left(M/p\right),$$

which implies that

$$I + \frac{M/p}{\ell} \cdot pA \in H(M/p), \tag{26}$$

since H is a subgroup.

Case: $p \neq \ell$. We regard $H(M)$ as a subgroup of the fibered product

$$H(M) \subseteq \left\{ (h_0, h_1) \in H\left(\frac{M}{p}\right) \times H\left(\frac{M}{\ell}\right) : \pi_0(h_0) = \pi_1(h_1) \right\} \tag{27}$$

via the embedding $h \mapsto (h \pmod{M/p}, h \pmod{M/\ell})$. Here, $\pi_0 \colon H\left(\frac{M}{p}\right) \to H\left(\frac{M}{\ell p}\right)$ and $\pi_1 \colon H\left(\frac{M}{\ell}\right) \to H\left(\frac{M}{\ell p}\right)$ are the natural projections. By Corollary 4.3, there must be a group Q, a surjective group homomorphism $f \colon Q \to H\left(\frac{M}{\ell p}\right)$ and surjective group homomorphisms

$$\psi_0 \colon H\left(\frac{M}{p}\right) \longrightarrow Q, \qquad \psi_1 \colon H\left(\frac{M}{\ell}\right) \longrightarrow Q$$

for which $f \circ \psi_i = \pi_i$ ($i \in \{0, 1\}$) and, under (27),

$$H(M) = \left\{ (h_0, h_1) \in H\left(\frac{M}{p}\right) \times H\left(\frac{M}{\ell}\right) : \psi_0(h_0) = \psi_1(h_1) \right\}.$$

Furthermore, since the degrees of π_0 and π_1 are relatively prime, we see that Q must be equal to $H\left(\frac{M}{\ell p}\right)$, $\psi_i = \pi_i$, and (27) is in fact an equality:

$$H(M) = \left\{ (h_0, h_1) \in H\left(\frac{M}{p}\right) \times H\left(\frac{M}{\ell}\right) : \pi_0(h_0) = \pi_1(h_1) \right\}.$$

By (26) we have that $(h_0, h_1) = \left(I + \frac{M/p}{\ell} \cdot pA, I\right)$ belongs to the right-hand side above, and this corresponds under $h \mapsto (h \pmod{M/p}, h \pmod{M/\ell})$ to $h = I + (M/\ell)A$, which therefore belongs to $H(M)$.

Case: $p = \ell$. Now we have $I + \frac{M}{\ell^2}A \in H\left(\frac{M}{\ell}\right)$. Let $I + \frac{M}{\ell^2}A + \frac{M}{\ell}B \in H(M)$ be any lift. In case ℓ is odd, note that ℓ divides M/ℓ^2 (since m_0 is square-full), and so $I + \frac{M}{\ell^2}A \equiv I \,(\operatorname{mod} \ell)$. It follows that

$$\begin{aligned}\left(I + \frac{M}{\ell^2}A + \frac{M}{\ell}B\right)^{\ell} &\equiv \left(I + \frac{M}{\ell^2}A\right)^{\ell} (\operatorname{mod} M) \\ &\equiv I + \frac{M}{\ell}A \,(\operatorname{mod} M).\end{aligned}$$

In case $\ell = 2$ and $A^2 \not\equiv 0 \,(\operatorname{mod} 2)$ note that 8 then divides $M/2$, so 16 divides $(M/4)^2$, and so we may use the same reasoning. In case $\ell = 2$ and $A^2 \equiv 0 \,(\operatorname{mod} 2)$, one computes

$$\begin{aligned}\left(I + \frac{M}{4}A + \frac{M}{2}B\right)^2 &\equiv I + \frac{M}{2}A + MB + \frac{M^2}{16}A^2 + \frac{M^2}{8}(AB + BA) \\ &\quad + \frac{M^2}{4}B^2 \,(\operatorname{mod} M) \\ &\equiv I + \frac{M}{2}A \,(\operatorname{mod} M).\end{aligned}$$

This concludes the proof of Lemma 4.5. □

The following key lemma is a corollary of Lemma 4.5.

Lemma 4.6. *Assume that A0 and A3 hold. Let m_0 be any positive square-full integer and $H(m_0) \subseteq \mathcal{S}(m_0)$ any subgroup satisfying*

$$\forall \ell \mid m_0, \quad I + \frac{m_0}{\ell}\mathfrak{s}_{\ell}(\ell) \subseteq H(m_0). \tag{28}$$

Suppose that $K \subseteq \mathcal{S}(\mathbb{Z}_{m_0})$ is any closed subgroup for which $K(m_0) = H(m_0)$. Then we must have

$$K = \pi_{\mathcal{S}(\mathbb{Z}_{m_0})}^{-1}(H(m_0)).$$

Remark 4.7. In case A3 does not hold (in particular if $\mathfrak{s}_2(2)$ cannot be generated as a $\mathbb{Z}/2\mathbb{Z}$-vector space by matrices u_i simultaneously satisfying $u_i^2 \equiv 0 \,(\operatorname{mod} 2)$ and $I + u_i \in \mathcal{S}(2)$), then the same conclusion follows from the additional hypothesis that 8 divides m_0.

Proof. Since K is closed, it suffices to show that $K(M) = \pi^{-1}(H(m_0)) \subseteq \mathcal{S}(M)$, for any positive integer M satisfying $m_0 \mid M \mid m_0^\infty$. This is proved by induction on M, the base case $M = m_0$ being trivial. If $M > m_0$, then there is a prime ℓ for which $m_0 \mid (M/\ell)$. By induction, $K(M/\ell) = \pi^{-1}(H(m_0)) \subseteq \mathcal{S}(M/\ell)$. Considering the exact sequence

$$1 \longrightarrow I + (M/\ell)\mathfrak{s}_\ell(\ell) \longrightarrow \mathcal{S}(M) \longrightarrow \mathcal{S}(M/\ell) \longrightarrow 1,$$

we see that $K(M) = \pi^{-1}(H(m_0))$ if and only if $I + (M/\ell)\mathfrak{s}_\ell(\ell) \subseteq K(M)$. This last containment follows from (28) and Lemma 4.5. □

Proposition 4.8. *Suppose $\mathcal{G}$ satisfies assumptions A0, A2 and A3. Let $m \geq 1$ be any positive integer and define m_0 by (22). Let $G(m) \subseteq \mathcal{G}(m)$ be any subgroup and let $G_{m_0} = \pi^{-1}_{\mathcal{G}(\mathbb{Z}_{m_0})}(G(m))$ be the corresponding finite index subgroup. Suppose $H_{m_0} \subseteq G_{m_0}$ is any subgroup which satisfies*

$$[H(m_0), H(m_0)] = [G(m_0), G(m_0)]. \tag{29}$$

Then

$$[H_{m_0}, H_{m_0}] = [G_{m_0}, G_{m_0}] = \pi^{-1}_{\mathcal{S}(\mathbb{Z}_{m_0})}\left([G(m_0), G(m_0)]\right).$$

Proof. By Lemma 4.6 (and noting (29)), the proposition will follow from the containment

$$\forall \ell \mid m_0, \quad I + \frac{m_0}{\ell}\mathfrak{s}_\ell(\ell) \subseteq [G(m_0), G(m_0)].$$

Define m_0' by $m_0 = m_0' \cdot \ell^{\operatorname{ord}_\ell(m_0)}$, so that $\ell \nmid m_0'$, and view $G(m_0) \subseteq G(m_0') \times G(\ell^{\operatorname{ord}_\ell(m_0)})$ via the Chinese remainder theorem. The above condition then becomes

$$\begin{aligned} \forall \ell \mid m_0, \quad \{I\} \times \left(I + \ell^{\operatorname{ord}_\ell(m_0)-1}\mathfrak{s}_\ell(\ell)\right) &\subseteq [G(m_0), G(m_0)] \\ &\subseteq G(m_0') \times G(\ell^{\operatorname{ord}_\ell(m_0)}). \end{aligned} \tag{30}$$

To prove this, fix a prime ℓ dividing m_0. If ℓ divides m, then since $G_{m_0} = \pi^{-1}_{\mathcal{G}(\mathbb{Z}_{m_0})}(G(m))$, we see that for any $C \in \mathfrak{g}(\mathbb{Z}_\ell)$, one has

$$(I, I + \ell^{\mathrm{ord}_\ell(m)} C) \in G_{m_0} \subseteq G_{m_0'} \times G_\ell.$$

Likewise, pick $(I, I + \ell^{\mathrm{ord}_\ell(m)} D) \in G_{m_0}$ for another arbitrary $D \in \mathfrak{g}(\mathbb{Z}_\ell)$. Applying Lemma 4.4 to the commutator $[(I, I+\ell^{\mathrm{ord}_\ell(m)} C), (I, I+\ell^{\mathrm{ord}_\ell(m)} D)]$, and using assumption A2, we see that (30) is satisfied. If ℓ does not divide m, then similarly one finds that

$$(I, I + \ell C), (I, I + \ell D) \in G_{m_0} \subseteq G_{m_0'} \times G_\ell,$$

for any $C, D \in \mathfrak{g}(\mathbb{Z}_\ell)$, implying (30) again by assumption A2. This completes the proof of the proposition. □

4.3. Working in $\mathcal{G}(\mathbb{Z}_{(m_0)})$

Lemma 4.9. *Assume that A0, A1 and A3 hold. Let m_0 be any integer divisible by $\prod_{\ell \in \mathcal{L}} \ell$ (where $\mathcal{L}$ is as in assumption A1) and suppose that $K \subseteq \mathcal{S}(\mathbb{Z}_{(m_0)})$ is any closed subgroup satisfying*

$$\forall \ell \nmid m_0, \quad K(\ell) = \mathcal{S}(\ell).$$

Then $K = \mathcal{S}(\mathbb{Z}_{(m_0)})$.

Proof. Since K is closed, it suffices to show that, for each integer M with $\gcd(m_0, M) = 1$, $K(M) = \mathcal{S}(M)$. We prove this by induction on the number of prime divisors ℓ of M. The base case where $M = \ell^n$ is a prime power follows immediately from Remark 2.16. For the induction step, suppose that M is divisible by more than one prime and write $M = \ell^n M'$, where $\ell \nmid M'$ and $M' > 1$. By induction, we have that

$$K(M') = \mathcal{S}(M') \quad \text{and} \quad K(\ell^n) = \mathcal{S}(\ell^n).$$

By Lemma 4.1, there is a common quotient group Q, together with surjective homomorphisms

$$\psi_0 \colon K(M') \longrightarrow Q, \qquad \psi_1 \colon K(\ell^n) \longrightarrow Q,$$

such that under the isomorphism of the Chinese remainder theorem, we have

$$K(M) = \{(h_0, h_1) \in K(M') \times K(\ell^n) : \psi_0(h_0) = \psi_1(h_1)\}.$$

Now we apply the observation (23) (with $N = \ker \psi_1$), concluding that either Q has $\mathcal{PS}(\ell)$ as a quotient, or else $Q = 1$. But since M' is not divisible by ℓ, (21) implies that Q cannot have $\mathcal{PS}(\ell)$ as a quotient, and so $Q = 1$ and $K(M) = \mathcal{S}(M)$, finishing the proof of Lemma 4.9. □

Applying Lemma 4.9 with K a commutator subgroup, and using Remark 2.16, we conclude the following corollary.

Corollary 4.10. *Assume that A0, A1 and A3 hold. Suppose that m_0 is any positive integer divisible by $\prod_{\ell \in \mathcal{L}} \ell$ and $H_{(m_0)} \subseteq \mathcal{G}(\mathbb{Z}_{(m_0)})$ is any subgroup satisfying*

$$\forall \ell \nmid m_0, \quad \mathcal{S}(\ell) \subseteq H(\ell).$$

Then, $[H_{(m_0)}, H_{(m_0)}] = [\mathcal{G}(\mathbb{Z}_{(m_0)}), \mathcal{G}(\mathbb{Z}_{(m_0)})] = \mathcal{S}(\mathbb{Z}_{(m_0)})$.

4.4. Finishing the proof of Theorem 2.18

We will now finish the proof of Theorem 2.18. If $H \subseteq G$ is any subgroup satisfying

$$\forall n \in \{m_0\} \cup \{\text{primes } \ell : \ell \nmid m_0\}, \quad [H(n), H(n)] = [G(n), G(n)],$$

then by Proposition 4.8, Corollary 4.10 and Lemma 4.1, we see that there is a group Q and surjective homomorphisms $\psi_0 \colon [G_{m_0}, G_{m_0}] \to Q$ and $\psi_1 : \mathcal{S}(\mathbb{Z}_{(m_0)}) \to Q$ for which (regarding $H \subseteq H_{m_0} \times H_{(m_0)}$)

$$[H, H] = \{(h_0, h_1) \in [G_{m_0}, G_{m_0}] \times \mathcal{S}(\mathbb{Z}_{(m_0)}) : \psi_0(h_0) = \psi_1(h_1)\}.$$

We now only need to show that $Q = \{1\}$. Consider the subgroup $\ker \psi_1 \subseteq \mathcal{S}(\mathbb{Z}_{(m_0)})$, and its projection $\ker \psi_1(\ell) \subseteq \mathcal{S}(\ell)$. By assumption A1, either $\mathcal{S}(\ell)/\ker \psi_1(\ell)$ has $\mathcal{PS}(\ell)$ as a quotient, or $\ker \psi_1(\ell) = \mathcal{S}(\ell)$. If $\mathcal{S}(\ell)/\ker \psi_1(\ell)$ had $\mathcal{PS}(\ell)$ as a quotient, then so would Q, and hence so would $[G_{m_0}, G_{m_0}]$, contradicting (21). Thus we see that, for each prime $\ell \nmid m_0$, $\ker \psi_1(\ell) = \mathcal{S}(\ell)$. By Lemma 4.9, it follows that $\ker \psi_1 = \mathcal{S}(\mathbb{Z}_{(m_0)})$, and so $Q = 1$ and $[H, H] = [G, G]$, finishing the proof of Theorem 2.18.

5. Examples and remarks

Having proved Theorem 2.18, we will give a few examples which illustrate some of the subtlety of this study. The first example highlights the fact that, even though there may exist a determinant-surjective, commutator-thick subgroup H of a given finite index subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$, there may nevertheless be no elliptic curve E over $\mathbb{Q}$ for which $\varphi_E(G_{\mathbb{Q}}) \subseteq G$.

Example 5.1. Let ℓ be a prime,

$$G(\ell) := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : b \in \mathbb{Z}/\ell\mathbb{Z};\ a, d \in (\mathbb{Z}/\ell\mathbb{Z})^\times \right\},$$

and $G = \pi^{-1}(G(\ell)) \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$. Even though there do exist commutator-thick, determinant-surjective subgroups $H \subseteq G$, Mazur has shown (see [13]) that, for $\ell > 163$, there is no elliptic curve E over $\mathbb{Q}$ for which $\varphi_E(G_{\mathbb{Q}}) \subseteq G$. More generally, when the index of G in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ is large enough, one expects that no subgroup of G arises as $\varphi_E(G_{\mathbb{Q}})$ for E over $\mathbb{Q}$ (see [18, § 4.3] and [1]).

The next example shows that there do exist finite index subgroups $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ which have no commutator-thick, determinant-surjective subgroups.

Example 5.2. Let ℓ be an odd prime and fix any element $\varepsilon \in (\mathbb{Z}/\ell\mathbb{Z})^\times$ which is not a square, i.e. for which $\left(\frac{\varepsilon}{\ell}\right) = -1$. Let $\mathcal{C}_{\mathrm{ns}}(\ell)$ denote the non-split Cartan subgroup

$$\mathcal{C}_{\mathrm{ns}}(\ell) := \left\{ \begin{pmatrix} x & \varepsilon y \\ y & x \end{pmatrix} \right\} \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

The group $G := \pi^{-1}(\mathcal{C}_{\mathrm{ns}}(\ell)) \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ has no subgroup H which is simultaneously commutator-thick and determinant-surjective.

Proof. If there were a commutator-thick, determinant-surjective subgroup $H \subseteq \pi^{-1}(\mathcal{C}_{\mathrm{ns}}(\ell))$ then there would necessarily be a group homomorphism $\psi\colon \hat{\mathbb{Z}}^\times \longrightarrow \mathcal{C}_{\mathrm{ns}}(\ell)$ for which the diagram

$$\begin{tikzcd} \hat{\mathbb{Z}}^\times \arrow[r, equal] \arrow[d, "\psi"'] & \hat{\mathbb{Z}}^\times \arrow[d, "\mathrm{red}"] \\ \mathcal{C}_{\mathrm{ns}}(\ell) \arrow[r, "\det"] & (\mathbb{Z}/\ell\mathbb{Z})^\times \end{tikzcd} \tag{31}$$

commutes. We will show that such a homomorphism ψ cannot exist. Suppose for the sake of contradiction that such a ψ does exist. The group $\mathcal{C}_{\mathrm{ns}}(\ell)$ is a cyclic group of order $\ell^2 - 1$, from which it follows that ψ factors as

$$\hat{\mathbb{Z}}^\times \xrightarrow{\text{red}} (\mathbb{Z}/\ell m'\mathbb{Z})^\times \xrightarrow{\psi} \psi((\mathbb{Z}/\ell m'\mathbb{Z})^\times) \subseteq \mathcal{C}_{\text{ns}}(\ell),$$

where ℓ does not divide m'. Let g be a generator of $\mathcal{C}_{\text{ns}}(\ell)$ and consider the image under ψ of $(\mathbb{Z}/\ell\mathbb{Z})^\times \times \{1\} \subseteq (\mathbb{Z}/\ell\mathbb{Z})^\times \times (\mathbb{Z}/m'\mathbb{Z})^\times$. By order considerations, we must have

$$\psi((\mathbb{Z}/\ell\mathbb{Z})^\times \times \{1\}) \subseteq \langle g^{\ell+1} \rangle,$$

from which it follows by (31) (since $g^{\ell+1}$ is a scalar matrix) that the canonical projection $(\mathbb{Z}/\ell m'\mathbb{Z})^\times \to (\mathbb{Z}/\ell\mathbb{Z})^\times$ maps into $[(\mathbb{Z}/\ell\mathbb{Z})^\times]^2$, a contradiction. Thus, there is no ψ making (31) commute, proving the assertion. □

Remark 5.3. By Remark 2.3, the previous example gives another proof (See also [19, Lemme 17, p. 197]) that

$$\nexists E/\mathbb{Q} \ \text{ for which } \ \varphi_{E,\ell}(G_{\mathbb{Q}}) \subseteq \mathcal{C}_{\text{ns}}(\ell).$$

Our third example illustrates, among other things, that the $\mathbb{Z}/\ell\mathbb{Z}$-vector space $\mathcal{V} \subseteq M_{2\times 2}(\mathbb{Z}/\ell\mathbb{Z})$ defined by the exact sequence

$$1 \to I + m\mathcal{V} \to H(\ell m) \to H(m) \to 1$$

may shrink when we replace m by a multiple of m (thus, care must be taken in Lemma 4.6). Let the split-Cartan subgroup $\mathcal{C}_{\text{s}}(\mathbb{Z}/\ell^n\mathbb{Z})$ and the Borel subgroup $B(\mathbb{Z}/\ell^n\mathbb{Z})$ be defined as usual by

$$\mathcal{C}_{\text{s}}(\mathbb{Z}/\ell^n\mathbb{Z}) := \left\{ \begin{pmatrix} x & 0 \\ 0 & z \end{pmatrix} \right\} \subseteq \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \right\} =: B(\mathbb{Z}/\ell^n\mathbb{Z}) \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}).$$

Let $\chi^{(1)}_{\ell^n}, \chi^{(2)}_{\ell^n} : B(\mathbb{Z}/\ell^n\mathbb{Z}) \longrightarrow (\mathbb{Z}/\ell^n\mathbb{Z})^\times$ be the characters defined by

$$\chi^{(1)}_{\ell^n}\left(\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \right) := x, \qquad \chi^{(2)}_{\ell^n}\left(\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \right) := z,$$

and let us use the same symbols to denote their corresponding restrictions to $\mathcal{C}_{\text{s}}(\mathbb{Z}/\ell^n\mathbb{Z})$. Note that, if $\pi^{-1}(\mathcal{C}_{\text{s}}(\mathbb{Z}/\ell\mathbb{Z})) \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell^2\mathbb{Z})$ denotes the full pre-image of $\mathcal{C}_{\mathrm{s}}(\mathbb{Z}/\ell\mathbb{Z})$, then there is a surjective group homomorphism

$$\mu\colon \pi^{-1}(\mathcal{C}_{\mathrm{s}}(\mathbb{Z}/\ell\mathbb{Z})) \longrightarrow \mathcal{C}_{\mathrm{s}}(\mathbb{Z}/\ell^2\mathbb{Z})$$

$$\mu\left(\begin{pmatrix} x+3a & 3b \\ 3c & z+3d \end{pmatrix}\right) := \begin{pmatrix} x+3a & 0 \\ 0 & x+3d \end{pmatrix}.$$

Finally, we use $\mathcal{L}_\ell\colon (\mathbb{Z}/\ell\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/3\mathbb{Z})^\times$ to denote the (unique) surjective homomorphism which sends a generator of $(\mathbb{Z}/\ell\mathbb{Z})^\times$ to -1.

Example 5.4. Suppose that $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ is a subgroup with

$$G(3\cdot 7\cdot 13) = \Big\{(g_3, g_7, g_{13}) \in \mathcal{C}_{\mathrm{s}}(\mathbb{Z}/3\mathbb{Z}) \times B(\mathbb{Z}/7\cdot 13\mathbb{Z}) : \\ \det(g_3) = \mathcal{L}_7(\chi_7^{(1)}(g_7)),\ \chi_3^{(1)}(g_3) = \mathcal{L}_{13}(\chi_{13}^{(1)}(g_{13}))\Big\}.$$

It is possible that $G(9\cdot 7\cdot 13) \subseteq \mathrm{GL}_2(\mathbb{Z}/9\cdot 7\cdot 13)$ is smaller than the full pre-image $\pi^{-1}(G(3\cdot 7\cdot 13)) \subseteq \mathrm{GL}_2(\mathbb{Z}/9\cdot 7\cdot 13\mathbb{Z})$. For example, one could have

$$G(9\cdot 7\cdot 13) = \Big\{(g_9, g_7, g_{13}) \in \pi^{-1}(\mathcal{C}_{\mathrm{s}}(\mathbb{Z}/3\mathbb{Z})) \times B(\mathbb{Z}/7\cdot 13\mathbb{Z})) : \\ \det(g_9) = \theta_7(\chi_7^{(1)}(g_7)),\ \chi_9^{(1)}(\mu(g_9)) = \theta_{13}(\chi_{13}^{(1)}(g_{13}))\Big\},$$

where $\theta_\ell\colon (\mathbb{Z}/\ell\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/9\mathbb{Z})^\times$ denotes any surjective homomorphism.

Suppose that $G = \pi^{-1}(G(9\cdot 7\cdot 13)) \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$, where $G(9\cdot 7\cdot 13)$ is as above. To see that $\pi(G(9\cdot 7\cdot 13)) = G(3\cdot 7\cdot 13)$, note that $\theta_\ell(\chi_\ell^{(1)}(g_\ell)) \pmod 3 = \mathcal{L}_\ell(\chi_\ell^{(1)}(g_\ell))$ and $\chi_9^{(1)}(\mu(g_9)) \pmod 3 = \chi_3^{(1)}(g_9 \pmod 3))$. Also note that the exact sequence

$$1 \to I + 3M_{2\times 2}(\mathbb{Z}/3\mathbb{Z}) \to G(9) \to G(3) \to 1$$

has a larger kernel than

$$1 \to I + 3\cdot 7\left\{\begin{pmatrix} a & b \\ c & -a \end{pmatrix} \pmod 3\right\} \to G(9\cdot 7) \to G(3\cdot 7) \to 1,$$

whose kernel is still larger than

$$1 \to I + 3\cdot 7\cdot 13\left\{\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} \pmod 3\right\} \to G(9\cdot 7\cdot 13) \to G(3\cdot 7\cdot 13) \to 1.$$

Remark 5.5. The **torsion conductor** m_E of an elliptic curve E over $\mathbb{Q}$ is defined in [9] to be the smallest positive integer $m \geq 1$ for which

$$\varphi_E(G_{\mathbb{Q}}) = \pi^{-1}(\varphi_{E,m}(G_{\mathbb{Q}})).$$

Example 5.4 indicates that the determination of m_E can be quite delicate.

6. The special cases $\mathcal{G} = \mathrm{GSp}_{2k}$ and $\mathcal{G} = (\mathrm{GL}_2)^k_\Delta$

For any positive integer $k \geq 1$, our study may be applied to the group $\mathcal{G} = \mathrm{GSp}_{2k}$ of degree k symplectic similitudes. This group arises when one considers the action of Galois on the torsion of a simple principally polarized abelian variety of dimension k. For any commutative ring R, the group $\mathrm{GSp}_{2k}(R)$ of R-valued points is

$$\mathrm{GSp}_{2k}(R) = \{g \in \mathrm{GL}_{2k}(R) : \exists c = c_g \in R^\times \text{ with } g^t\Omega g = c\Omega\},$$

where Ω is the $2k \times 2k$ matrix given in block form by

$$\Omega := \begin{pmatrix} 0 & I_k \\ -I_k & 0 \end{pmatrix}.$$

Note that $\mathrm{GSp}_2 = \mathrm{GL}_2$, and the $k = 1$ case coincides with that of an elliptic curve; this case will be treated below when considering $\mathcal{G} = (\mathrm{GL}_2)^k_\Delta$. Therefore, for the remainder of our consideration of $\mathcal{G} = \mathrm{GSp}_{2k}$, we will assume that $k \geq 2$.

It is well-known that the function

$$\delta\colon\ \mathrm{GSp}_{2k}(R) \longrightarrow R^\times,\ g \mapsto c_g$$

is a group homomorphism, whose kernel defines the symplectic group Sp_{2k}, which is also a subgroup of SL_{2k}:

$$\mathrm{Sp}_{2k}(R) = \{g \in \mathrm{SL}_{2k}(R) : g^t\Omega g = \Omega\}.$$

Furthermore, if

$$\varphi_A\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GSp}_{2k}(\hat{\mathbb{Z}})$$

is the Galois representation defined by letting $G_{\mathbb{Q}}$ operate on the torsion of A, then (by virtue of the Weil pairing) $\delta \circ \varphi_A\colon G_{\mathbb{Q}} \longrightarrow \hat{\mathbb{Z}}^\times$ agrees with the cyclotomic character.

We will now verify assumptions A0, A1, A2 and A3 for $\mathcal{G} = \mathrm{GSp}_{2k}$.

Lemma 6.1. *If $k \geq 2$, then assumption A1 holds for $\mathcal{G} = \mathrm{GSp}_{2k}$, with $\mathcal{PS}(\ell) = \mathrm{PSp}_{2k}(\mathbb{Z}/\ell\mathbb{Z}) := \mathrm{Sp}_{2k}(\mathbb{Z}/\ell\mathbb{Z})/\{\pm I\}$, $\mathcal{L} = \{2, 3\}$ and a single map*

$$\varpi\colon \mathrm{Sp}_{2k}(\mathbb{Z}/\ell\mathbb{Z}) \longrightarrow \mathrm{PSp}_{2k}(\mathbb{Z}/\ell\mathbb{Z})$$

given by the natural projection.

Proof. In [8, Hauptsatz 9.22] one may find the proof that $\mathrm{PSp}_{2k}(\mathbb{Z}/\ell\mathbb{Z})$ is simple in the stated cases. Fix any normal subgroup $N \trianglelefteq \mathrm{Sp}_{2k}(\mathbb{Z}/\ell\mathbb{Z})$. Considering the exact sequence

$$1 \longrightarrow \{\pm I\} \longrightarrow \mathrm{Sp}_{2k}(\mathbb{Z}/\ell\mathbb{Z}) \longrightarrow \mathrm{PSp}_{2k}(\mathbb{Z}/\ell\mathbb{Z}) \longrightarrow 1,$$

one sees that if $N \not\subseteq \ker\omega$, it follows that $N = \mathrm{Sp}_{2k}(\mathbb{Z}/\ell\mathbb{Z})$ since the above sequence doesn't split. Finally, it follows by considering Sylow subgroups that $\mathrm{PSp}_{2k}(\mathbb{Z}/\ell\mathbb{Z})$ does not occur in $\mathrm{Sp}_{2k}(\mathbb{Z}/\ell'\mathbb{Z})$ for $\ell \geq 5$ and $\ell' \neq \ell$, completing the proof of Lemma 6.1. □

Lemma 6.2. *Assumptions A0, A2 and A3 hold for the group $\mathcal{G} = \mathrm{GSp}_{2k}$.*

Proof. Note that, for any $n \geq 1$, one has

$$\mathfrak{s}_{\ell^n}(\ell) = \{A \in M_{2k\times 2k}(\mathbb{Z}/\ell\mathbb{Z}) : A^t\Omega + \Omega A = 0\}.$$

In particular, assumption A0 holds. For indices i and j with $1 \leq i, j \leq k$, let $E_{i,j}$ denote the $k \times k$ block matrix with a 1 in the i-th row and j-th column and with all other entries equal to zero, and set

$$S_{i,j} := \begin{cases} E_{i,j} + E_{j,i} & \text{if } i \neq j \\ E_{i,i} & \text{otherwise.} \end{cases}$$

One verifies that

$$\begin{aligned}\mathcal{U} := &\left\{\begin{pmatrix} E_{i,j} & 0 \\ 0 & -E_{j,i}\end{pmatrix}\right\}_{\substack{1\leq i,j\leq k \\ i\neq j}} \sqcup \left\{\begin{pmatrix} 0 & S_{i,j} \\ 0 & 0\end{pmatrix}\right\}_{\substack{1\leq i,j\leq k \\ i\leq j}} \\ &\sqcup \left\{\begin{pmatrix} 0 & 0 \\ S_{i,j} & 0\end{pmatrix}\right\}_{\substack{1\leq i,j\leq k \\ i\leq j}} \sqcup \left\{\begin{pmatrix} E_{i,i} & E_{i,i} \\ -E_{i,i} & -E_{i,i}\end{pmatrix}\right\}_{1\leq i\leq k}\end{aligned}$$

is a basis of $\mathfrak{s}_\ell(\ell)$ as a $\mathbb{Z}/\ell\mathbb{Z}$-vector space. Furthermore, one verifies that for each $u_i \in \mathcal{U}$, $u_i^2 \equiv 0 \pmod{\ell}$ and also that $I + u_i \in \mathcal{S}(\ell)$. Thus, assumption

A3 holds for $\mathcal{G} = \mathrm{GSp}_{2k}$. Now note that

$$\begin{aligned}\mathfrak{s}_\ell(\ell) &= \{A \in M_{2k\times 2k}(\mathbb{Z}/\ell\mathbb{Z}) : A^t\Omega + \Omega A = 0\}\\ &= \Omega \cdot \mathrm{Sym}_{2k}(\mathbb{Z}/\ell\mathbb{Z}),\end{aligned}$$

where

$$\mathrm{Sym}_{2k}(\mathbb{Z}/\ell\mathbb{Z}) := \{A \in M_{2k\times 2k}(\mathbb{Z}/\ell\mathbb{Z}) : A^t = A\}$$

is the set of symmetric matrices. Consider the Lie bracket

$$\begin{aligned}\Omega\mathrm{Sym}_{2k}(\mathbb{Z}/\ell\mathbb{Z}) \times \Omega\mathrm{Sym}_{2k}(\mathbb{Z}/\ell\mathbb{Z}) &\to \Omega\mathrm{Sym}_{2k}(\mathbb{Z}/\ell\mathbb{Z})\\ [\Omega X, \Omega Y] &= \Omega X \cdot \Omega Y - \Omega Y \cdot \Omega X.\end{aligned}$$

Since $\Omega^{-1}\mathrm{Sym}_{2k}(\mathbb{Z}/\ell\mathbb{Z})\Omega = \mathrm{Sym}_{2k}(\mathbb{Z}/\ell\mathbb{Z})$, we may replace X with $\Omega X\Omega$, so that the Lie bracket becomes

$$[\Omega \cdot \Omega X\Omega, \Omega Y] = XY + \Omega Y X \Omega.$$

Writing X andy Y in block form as

$$X = \begin{pmatrix} A & B \\ B^t & D \end{pmatrix} \quad \text{and} \quad Y = \begin{pmatrix} E & F \\ F^t & J \end{pmatrix},$$

one computes that

$$XY + \Omega Y X \Omega = \begin{pmatrix} AE - JD + BF^t - F^tB & BJ + JB^t + AF + F^tA \\ B^tE + EB + DF^t + FD & -EA + DJ + B^tF - FB^t \end{pmatrix}.$$

Taking $A = D = E = J = 0$ and $F = E_{i,i}$, $B = E_{i,j}$ (with $i \neq j$), we conclude that

$$\begin{pmatrix} -E_{i,j} & 0 \\ 0 & E_{j,i} \end{pmatrix} \in \langle CD - DC : C, D \in \mathfrak{g}_\ell(\ell)\rangle.$$

Similarly, taking $A = E_{i,i}$, $E = I$ and $B = D = F = J = 0$ gives us that

$$\begin{pmatrix} E_{i,i} & 0 \\ 0 & -E_{i,i} \end{pmatrix} \in \langle CD - DC : C, D \in \mathfrak{g}_\ell(\ell)\rangle.$$

Taking $A = E_{i,i}$, $F = E_{i,j}$ $(i \neq j)$ and $B = D = E = J = 0$ and similarly $B = E_{i,j}$, $E = E_{i,i}$ and $A = D = F = J = 0$ gives

$$\begin{pmatrix} 0 & E_{i,j} + E_{j,i} \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ E_{i,j} + E_{j,i} & 0 \end{pmatrix} \in \langle CD - DC : C, D \in \mathfrak{g}_\ell(\ell)\rangle,$$

while taking $A = E_{i,i}$, $F = E_{i,i}$ and $B = D = E = J = 0$ and also $B = E_{i,i}$, $E = E_{i,i}$ and $A = D = F = J = 0$ gives

$$\begin{pmatrix} 0 & 2E_{i,i} \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 2E_{i,i} & 0 \end{pmatrix} \in \langle CD - DC : C, D \in \mathfrak{g}_\ell(\ell) \rangle.$$

This verifies A3 when ℓ is an odd prime. For $\ell = 2$, one uses the fact that

$$\mathfrak{g}_\ell(\ell) = \{A \in M_{2k\times 2k}(\mathbb{Z}/\ell\mathbb{Z}) : A^t\Omega + \Omega A \in \mathbb{Z}/\ell\mathbb{Z} \cdot \Omega\},$$

so that in particular,

$$\begin{pmatrix} 0 & 0 \\ 0 & I \end{pmatrix} \in \mathfrak{g}_\ell(\ell).$$

Thus,

$$\begin{pmatrix} 0 & E_{i,i} \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & I \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 0 & I \end{pmatrix}\begin{pmatrix} 0 & E_{i,i} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & E_{i,i} \\ 0 & 0 \end{pmatrix},$$

and a similar calculation verifies that

$$\begin{pmatrix} 0 & E_{i,i} \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ E_{i,i} & 0 \end{pmatrix} \in \langle CD - DC : C, D \in \mathfrak{g}_\ell(\ell) \rangle,$$

finishing the proof of Lemma 6.2. □

As mentioned in Section 2, we may apply Theorem 2.18 to the Galois representation φ_A on the torsion of a k-dimensional simple abelian variety A over $\mathbb{Q}$. Fix any subgroup $G(m) \subseteq \mathrm{GSp}_{2k}(\mathbb{Z}/m\mathbb{Z})$ and let

$$G = \pi^{-1}_{\mathrm{GSp}_{2k}(\hat{\mathbb{Z}})}(G(m)) \subseteq \mathrm{GSp}_{2k}(\hat{\mathbb{Z}})$$

be the corresponding finite index subgroup of $\mathrm{GSp}_{2k}(\hat{\mathbb{Z}})$. In this case m_0 is given by

$$m_0 = \mathrm{lcm}\left(2^3 \cdot 3^3, \prod_{\ell | m} \ell^{2\mathrm{ord}_\ell(m)+1}\right).$$

The following corollary restates Corollary 2.20 from Section 2, which we may now deduce from Theorem 2.18.

Corollary 6.3. *Let A be a simple principally polarized abelian variety over $\mathbb{Q}$ of dimension $k \geq 2$, and assume that $\varphi_A(G_\mathbb{Q}) \subseteq G$. The image $\varphi_A(G_\mathbb{Q}) \subseteq G$ is a G-maximal commutator-thick subgroup if and only if the following conditions hold.*

1) *For each prime* $\ell \nmid m_0$, *one has* $\mathrm{Sp}_{2k}(\mathbb{Z}/\ell\mathbb{Z}) \subseteq \varphi_A(G_{\mathbb{Q}}) \,(\mathrm{mod}\, \ell)$.

2) *One has* $[\varphi_A(G_{\mathbb{Q}}) \,(\mathrm{mod}\, m_0), \varphi_A(G_{\mathbb{Q}}) \,(\mathrm{mod}\, m_0)] = [G(m_0), G(m_0)]$.

If a k-dimensional abelian variety is a product of elliptic curves, the representation φ_A maps into a different group, which we now consider. Define the group $(\mathrm{GL}_2)^k_\Delta$ by specifying its R-valued points, for any commutative ring R as

$$\begin{aligned}(\mathrm{GL}_2)^k_\Delta(R) := \{(g_1, g_2, \dots, g_k) \in \mathrm{GL}_2(R)^k :\\ \det(g_1) = \det(g_2) = \cdots = \det(g_k)\}.\end{aligned}$$

Note that the diagonal imbedding

$$(g_1, g_2, \dots, g_k) \mapsto \begin{pmatrix} g_1 & 0 & \cdots & 0 \\ 0 & g_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_k \end{pmatrix} \tag{32}$$

realizes $(\mathrm{GL}_2)^k_\Delta$ as an algebraic subgroup of GL_{2k}. Taking $\delta((g_1, g_2, \dots, g_k))$ $:= \det g_i$ to be the common determinant of any of the entries, one has

$$\mathcal{S} = (\mathrm{SL}_2)^k.$$

We will presently verify the assumptions A0 through A3.

Lemma 6.4. *Assumption A1 holds for* $\mathcal{G} = (\mathrm{GL}_2)^k_\Delta$, *with* $\mathcal{L} = \{2, 3, 5\}$, $\mathcal{PS}(\ell) = \mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$, *and*

$$\varpi_i \colon \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})^k \longrightarrow \mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z}), \qquad (i = 1, 2, \dots, k)$$

given by projection onto the i-th factor followed by the projection $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

Proof. The well-known fact that $\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is simple for $\ell \geq 5$ may be found in [8, Hauptsatz 6.13].

To prove that any normal subgroup $N \trianglelefteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})^k$ must satisfy either $N \subseteq \ker \varpi_i$ for some i or $N = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})^k$, we proceed by induction on $k \geq$

1. The $k=1$ case follows immediately from the fact that the exact sequence

$$1 \longrightarrow \{\pm I\} \longrightarrow \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \longrightarrow \mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z}) \longrightarrow 1$$

does not split. By induction we assume that the statement of the lemma holds for some fixed k and now let $N \trianglelefteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})^{k+1}$ be any normal subgroup satisfying $N \not\subseteq \ker \varpi_i$ for each i. Let $\pi_1\colon\ \mathrm{SL}_2^{k+1} \longrightarrow \mathrm{SL}_2^k$ be the projection onto the first k factors and $\pi_2\colon\ \mathrm{SL}_2^{k+1} \longrightarrow \mathrm{SL}_2$ the projection onto the last factor. By induction, we have that $\pi_1(N) = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})^k$ and $\pi_2(N) = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. By Lemma 4.1, we have that

$$N = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})^k \times_Q \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

for some group Q. Either Q has $\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$ as a quotient, or $Q = \{1\}$. Conjugation by $\{I\}^k \times \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$, one sees that the first possibility contradicts $N \trianglelefteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})^k$ being a normal subgroup. Thus $Q = \{1\}$, and the induction step is complete.

Finally, we verify that $\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$ does not occur in $\mathrm{SL}_2(\mathbb{Z}/\ell'\mathbb{Z})^k$ for $\ell \geq 7$ and $\ell' \neq \ell$. Define the notation

$$\mathrm{Occ}(G) := \{ \text{ finite simple non-abelian groups } \Sigma \text{ occurring in } G \ \}.$$

Then for any exact sequence of groups

$$1 \longrightarrow G_1 \longrightarrow G \longrightarrow G_2 \longrightarrow 1,$$

one has

$$\mathrm{Occ}(G) = \mathrm{Occ}(G_1) \cup \mathrm{Occ}(G_2).$$

This observation reduces to the case $k=1$, which in turn follows from the fact that

$$\mathrm{Occ}(\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})) = \mathrm{Occ}(\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})) \subseteq \{\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z}), A_5\},$$

where A_5 is the alternating group on 5 elements (see [8, Hauptsatz 8.27]). This finishes the proof of Lemma 6.4. □

Lemma 6.5. *Assumptions A0, A2 and A3 hold for the group* $\mathcal{G} = (\mathrm{GL}_2)^k_\Delta$.

Proof. To verify assumption A2, first note that the imbedding (32) realizes $\mathfrak{g}_\ell(\ell)$ as

$$\mathfrak{g}_\ell(\ell) = \left\{ \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_k \end{pmatrix} : \begin{array}{l} A_i \in M_{2\times 2}(\mathbb{Z}/\ell\mathbb{Z}), \\ \operatorname{tr} A_1 = \operatorname{tr} A_2 = \cdots = \operatorname{tr} A_k \end{array} \right\}.$$

If ℓ is odd, we observe that

$$\begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & xI & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & xI \end{pmatrix} \in \mathfrak{g}_\ell(\ell),$$

where $2x = \operatorname{tr} A_1$, and similarly with the other main diagonal entries. If $\ell = 2$ then we observe that

$$\begin{pmatrix} A & 0 & \cdots & 0 \\ 0 & I & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & I \end{pmatrix}, \begin{pmatrix} B & 0 & \cdots & 0 \\ 0 & B & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & B \end{pmatrix} \in \mathfrak{g}_2(\mathbb{Z}/2\mathbb{Z})$$

(where $\operatorname{tr} A = 0$ and $\operatorname{tr} B = 1$), and similarly for the other main diagonal entries. These observations reduce us to the case $k = 1$, which is a special case of Lemma 6.2. This verifies assumption A2. For assumptions A0 and A3, one takes the special case $k = 1$ of the basis $\mathcal{U}$ occurring in the proof of Lemma 6.2, applied to each main diagonal entry. This verifies assumptions A0 and A3, finishing the proof of Lemma 6.5. □

As mentioned above, the group $\mathcal{G} = (\mathrm{GL}_2)^k_\Delta$ just considered arises when one considers the Galois representation

$$\varphi_{(E_i)} \colon G_{\mathbb{Q}} \longrightarrow (\mathrm{GL}_2)^k_\Delta(\hat{\mathbb{Z}})$$

attached to a k-tuple $(E_1, E_2, \ldots, E_k)$ of elliptic curves E_i over $\mathbb{Q}$.

Theorem 2.18 gives a criterion for detecting Serre k-tuples (see Definition 2.21) that involves the level $m_0 = 2^3 \cdot 3^3 \cdot 5^3 = 27,000$. With a bit more work, using particular information about GL$_2$, one can improve this to $m_0 = 2^2 \cdot 3^2 = 36$, as follows. First, we observe that Remark 2.8 holds.

Indeed, choosing $\mathcal{L}$ minimally so that A1 is satisfied, we may decompose $\mathcal{L}$ as a disjoint union $\mathcal{L} = \mathcal{L}_0 \sqcup \mathcal{L}_1$, where

$$\mathcal{L}_0 := \left\{ \ell \in \mathcal{L} : \begin{array}{c} \forall \text{ finite simple non-abelian group } \mathcal{PS}(\ell) \text{ and } \forall \text{ set } \{\varpi_i\} \\ \text{of surjective homomorphisms } \varpi_i : \mathcal{S}(\ell) \twoheadrightarrow \mathcal{PS}(\ell), \\ \exists N \trianglelefteq \mathcal{S}(\ell), \text{ with } \forall i \; N \not\subseteq \ker \varpi_i \text{ and } N \neq \mathcal{S}(\ell) \end{array} \right\}$$
$$\cup \{2, 3\}$$

and $\mathcal{L}_1 := \mathcal{L} - \mathcal{L}_0$. Thus, $\mathcal{L}_0$ is the subset of primes in $\mathcal{L}$ for which condition (19) fails (together with the primes 2 and 3), while $\mathcal{L}_1$ is the subset of primes in $\mathcal{L}$ for which condition (20) fails.

For the group $\mathcal{G} = (\mathrm{GL}_2)^k_\Delta$, one has $\mathcal{L}_0 = \{2, 3\}$ and $\mathcal{L}_1 = \{5\}$. We now show that, replacing m_0 with (12), the proof of Theorem 2.18 still holds in this case. Indeed, the proof of Proposition 4.8 remains valid for the new value of m_0. Furthermore, replacing $\mathcal{L} = \{2, 3, 5\}$ with $\{2, 3\}$ in Lemma 4.9, and choosing ℓ in the decomposition $M = \ell^n M'$ occurring in its proof so that $\ell \neq 5$, one sees that Lemma 4.9 also remains valid. Finally, for any prime $\ell \neq 5$ with $\ell \not\equiv \pm 1 \pmod 5$, since 5 doesn't divide $|\,\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})|$, the group $\mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z}) \simeq A_5$ does not occur in $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Thus, under the hypothesis that no prime ℓ dividing m satisfies $\ell \equiv \pm 1 \pmod 5$, it follows from (21) that $\mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z})$ does not occur in $[G_{m_0}, G_{m_0}]$, and so the proof occurring in Section 4.4 also remains valid. Thus, Theorem 2.18 holds with m_0 given by (12) when $\mathcal{G} = (\mathrm{GL}_2)^k_\Delta$. In particular, this justifies Remark 2.8.

In case $m = 1$, we may further reduce m_0 from $2^3 \cdot 3^3 = 216$ to $2^2 \cdot 3^2 = 36$. For this, we will need the following technical lemma. Suppose G_1 and G_2 are groups together with surjective group homomorphisms

$$\varpi_1 \colon G_1 \longrightarrow A$$
$$\varpi_2 \colon G_2 \longrightarrow A$$

onto a common abelian group A. Let $G = G_1 \times_A G_2$ denote the fibered product

$$G = \{(g_1, g_2) \in G_1 \times G_2 : \varpi_1(g_1) = \varpi_2(g_2)\}.$$

Lemma 6.6. *With notation as above, suppose that there exists a subset $B_2 \subseteq G_2$ satisfying $\varpi_2(B_2) = A$ and all of whose elements commute with one another. Then one has*

$$[G, G] = [G_1, G_1] \times [G_2, G_2].$$

Proof. See [12, Lemma 1, p. 174]. □

We will now use Lemmas 6.6, 4.6 to deduce Corollary 2.22 from Section 2:

Corollary 6.7. *The k-tuple $(E_1, E_2, \ldots, E_k)$ is a Serre k-tuple if and only if the following conditions hold.*

1) *For each prime $\ell \geq 5$, one has* $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})^k \subseteq \big(\varphi_{(E_i)}(G_{\mathbb{Q}}) \,(\mathrm{mod}\, \ell)\big)$.
2) *One has* $[\varphi_{(E_i)}(G_{\mathbb{Q}}) \,(\mathrm{mod}\, 36),\ \varphi_{(E_i)}(G_{\mathbb{Q}}) \,(\mathrm{mod}\, 36)] = (\mathrm{SL}_2(\mathbb{Z}/36\mathbb{Z}) \cap \ker \varepsilon)^k$, *where ε is as in* (2).

Proof. In this case one has $\mathcal{G} = (\mathrm{GL}_2)^k_{\Delta}$ and $m = 1$. Put $m_0 = 36$. As in the argument of Section 4.4, Lemma 4.6 and Corollary 4.10 reduce the proof to showing that

$$\Big[(\mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z}))^k_{\Delta}, (\mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z}))^k_{\Delta}\Big] = (\mathrm{SL}_2(\mathbb{Z}/36\mathbb{Z}) \cap \ker \varepsilon)^k. \tag{33}$$

We observe that for any level n, the image of the embedding

$$(\mathbb{Z}/n\mathbb{Z})^{\times} \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}), \qquad x \mapsto \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$$

defines a subgroup $B_2 \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ realizes the conditions of Lemma 6.6 for $G_1 = (\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}))^{k-1}_{\Delta}$ and $G_2 = \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. By induction, we are reduced to verifying (33) in the case $k = 1$. This case follows from [12, Theorem 2.1, p. 166] and the discussion on pages 181–183 of [12]. (In fact, these observations imply that

$$[\mathrm{GL}_2(\hat{\mathbb{Z}}), \mathrm{GL}_2(\hat{\mathbb{Z}})] = \mathrm{SL}_2(\hat{\mathbb{Z}}) \cap \ker \varepsilon, \tag{34}$$

an index 2 subgroup of $\mathrm{SL}_2(\hat{\mathbb{Z}})$.) This finishes the proof of Corollary 2.22. □

7. Acknowledgments

Some of the research leading to this paper was done while visiting the Hausdorff Research Institute for Mathematics and subsequently the Max Planck Institute for Mathematics (both in Bonn, Germany). I would like to thank each of these institutes for providing stimulating work environments. I would also like to thank D. Zywina for comments on a previous version, as well as A.C. Cojocaru, D. Grant and G. Banaszak for useful conversations. Finally, I would like to thank the anonymous referee for carefully reading the manuscript and offering several helpful comments.

References

[1] K. Arai, *On uniform lower bound of the Galois images associated to elliptic curves.* Journal de théorie des nombres de Bordeaux, **20** no. 1 (2008), 23–43.

[2] Y. Bilu and P. E. Parent, *Serre's uniformity problem in the split Cartan case.* Ann. of Math., **173**, no. 1 (2011), 569–584.

[3] A. C. Cojocaru, D. Grant and N. Jones, *One-parameter families of elliptic curves over $\mathbb{Q}$ with maximal Galois representations.* Proc. Lond. Math. Soc., **103**, no. 3 (2011), 654–675.

[4] C. David and F. Papalardi, *Average Frobenius distributions of elliptic curves.* International Math. Research Notices, **4** (1999), 165–183.

[5] É. Fouvry and M. R. Murty, *On the distribution of supersingular primes.* Can. J. Math., **48** (1996), 81–104.

[6] D. Grant, *A Formula for the Number of Elliptic Curves with Exceptional Primes.* Compos. Math., **122** (2000), 151–164.

[7] A. Greicius, *Elliptic curves with surjective global Galois representation.* Experiment. Math., **19**, no. 4 (2010), 495–507.

[8] B. Huppert, *Endliche Gruppen I.* Grundlehren der mathematischen Wissenschaften, **134**, Springer-Verlag, Berlin (1967).

[9] N. Jones, *A bound for the torsion conductor of a non-CM elliptic curve.* Proc. Amer. Math. Soc., **137** (2009), 37–43.

[10] N. Jones, *Almost all elliptic curves are Serre curves.* Trans. Amer. Math. Soc., **362** (2010), 1547–1570.

[11] N. Jones, *Pairs of elliptic curves with maximal Galois representations.* J. Number Theory, **133** (2013), 3381–3393.

[12] S. Lang and H. Trotter, *Frobenius distribution in* GL_2 *extensions.* Lecture Notes in Math., **504**, Springer (1976).

[13] B. Mazur, *Rational isogenies of prime degree.* Invent. Math., **44**, no. 2 (1978), 129–162.

[14] B. Mazur, *Rational points on modular curves.* Lecture Notes in Math., **601**, Springer, NY 1977, 107–148.

[15] V. Radhakrishnan, *An asymptotic formula for the number of non-Serre curves in a two-parameter family of elliptic curves.* Ph.D. dissertation, University of Colorado at Boulder (2008).

[16] K. Ribet, *Galois action on division points of Abelian varieties with real multiplications.* Amer. J. Math., **98**, no. 3 (1976), 751–804.

[17] J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves.* Benjamin, New York-Amsterdam, 1968.

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

[19] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev.* Inst. Hautes Études Sci. Publ. Math., **54** (1981), 123–201.

[20] J. H. Silverman, *The Arithmetic of Elliptic Curves.* Springer-Verlag, New York, 1986.

[21] D. Zywina, *Elliptic curves with maximal Galois action on their torsion points.* Bull. Lond. Math. Soc., **42** (2010), 811–826.

Department of Mathematics, Statistics, and Computer Science
University of Illinois at Chicago
322 Science and Engineering Offices
851 S Morgan Street
Chicago, IL 60607-7045, USA
E-mail address: ncjones@uic.edu

Received October 31, 2012