Landesman et al. *Res. Number Theory*
DOI 10.1007/s40993-017-0078-6

Research in Number Theory

RESEARCH Open Access

Lifting subgroups of symplectic groups over $\mathbb{Z}/\ell\mathbb{Z}$

Aaron Landesman[1], Ashvin A. Swaminathan[2], James Tao[2*] and Yujie Xu[3]

*Correspondence:
jamestao@college.harvard.edu
[2]Department of Mathematics, Harvard College, Cambridge, MA 02138, USA
Full list of author information is available at the end of the article

Abstract

For a positive integer g, let $\mathrm{Sp}_{2g}(R)$ denote the group of $2g \times 2g$ symplectic matrices over a ring R. Assume $g \geq 2$. For a prime number ℓ, we give a self-contained proof that any closed subgroup of $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ which surjects onto $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ must in fact equal all of $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$. The result and the method of proof are both motivated by group-theoretic considerations that arise in the study of Galois representations associated to abelian varieties.

Keywords: Linear algebraic groups, Local fields, Abelian varieties

1 Introduction

Let g be a positive integer, and for a ring R, denote by $\mathrm{Sp}_{2g}(R)$ the group of $2g \times 2g$ symplectic matrices over R. Let $\mathbb{Z}_\ell$ denote the ring of ℓ-adic integers, and consider the natural projection map $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell) \to \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$. In this paper, we show that when $g > 1$, there are no proper closed subgroups of $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ that surject via this projection map onto all of $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$.

The case $g = 1$, in which $\mathrm{Sp}_2 = \mathrm{SL}_2$, is well-understood. Indeed, as proven in [11, Lemma 3, Section IV.3.4], if $\ell \geq 5$ and $H_\ell \subset \mathrm{SL}_2(\mathbb{Z}_\ell)$ is a closed subgroup that surjects onto $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$, then $H_\ell = \mathrm{SL}_2(\mathbb{Z}_\ell)$. The corresponding result for $\ell \in \{2, 3\}$ simply does not hold: in each of these cases, there are nontrivial subgroups of $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell^2\mathbb{Z})$ that surject onto $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. See [11, Section IV.3.4, Exercises 1–3] for exercises outlining a proof, and also see for more comprehensive descriptions [5] for the case $\ell = 2$ and [6] for the case $\ell = 3$.

The objective of the present article is to generalize [11, Lemma 3, Section IV.3.4], to hold for all $g \geq 2$. Our main theorem is stated as follows:

Theorem 1 *Let $g \geq 2$, let ℓ be a prime number, and let $H_\ell \subset \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ be a closed subgroup. If the mod-ℓ reduction of H_ℓ equals all of $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$, then $H_\ell = \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$, and in particular, the mod-ℓ^k reduction of H_ℓ equals all of $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z})$ for each positive integer k.*

Remark 1 A more general version of Theorem 1 is proven for a large class of semisimple Lie groups G in [14, Theorem B] (except for the case that $g = 3$ and $\ell = 2$) and also in [12, Theorem 1.3]. In the present article, we provide an elementary and self-contained proof for the special case $G = \mathrm{Sp}_{2g}$. In particular, our inductive method circumvents

Springer Open

the use of Lie theory, and is therefore suitable for somewhat more general groups (e.g. certain finite-index subgroups of matrix groups over $\mathbb{Z}_\ell$) which arise in the study of Galois representations associated to abelian varieties, cf. [8].

Remark 2 To give a typical application, one can directly use Theorem 1 to reduce the problem of checking that the ℓ-adic Galois representation associated to an abelian variety has maximal image to the simpler problem of checking that the mod-ℓ reduction has maximal image. Indeed, the conclusion of Theorem 1 has been applied many times in the study of Galois representations, such as in [15, Proof of Lemma 2.4], [7, Proof of Theorem 8], [1, Proof of Corollary 3.5], [2, Proof of Lemma 5.1], [13, p. 467], as well in the authors' own papers [8,9].

The rest of this paper is organized as follows. In Sect. 2.1, we introduce the basic definitions and properties of the symplectic group. Next, in Sect. 2.2, we compute the commutator subgroups of $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ and $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z})$ for every prime number ℓ and positive integer k. Finally, in Sect. 3, we prove Theorem 1.

2 Background on symplectic groups

In this section, we first detail the basic definitions and properties of symplectic groups, and then proceed to prove a number of lemmas that are used in our proof of Theorem 1.

2.1 Symplectic groups

Fix a commutative ring R, let $\mathrm{Mat}_{2g\times 2g}(R)$ denote the space of $2g \times 2g$ matrices with entries in R, and define $\Omega_{2g} \in \mathrm{Mat}_{2g\times 2g}(R)$ as

$$\Omega_{2g} := \left[\begin{array}{c|c} 0 & \mathrm{id}_g \\ \hline -\mathrm{id}_g & 0 \end{array}\right],$$

where id_g denotes the $g \times g$ identity matrix. We define the symplectic group $\mathrm{Sp}_{2g}(R)$ as the set of $M \in \mathrm{SL}_{2g}(R)$ so that $M^T\Omega_{2g}M = \Omega_{2g}$.

In the proof of Theorem 1, we will make heavy use of the "Lie algebra" $\mathfrak{sp}_{2g}(R)$, which is defined by

$$\mathfrak{sp}_{2g}(R) := \{M \in \mathrm{Mat}_{2g\times 2g}(R) : M^T\Omega_{2g} + \Omega_{2g}M = 0\}.$$

It is easy to see that $M^T\Omega_{2g} + \Omega_{2g}M = 0$ is equivalent to M being a block matrix with $g \times g$ blocks of the form

$$M = \left[\begin{array}{c|c} A & B \\ \hline C & -A^T \end{array}\right],$$

where B and C are symmetric.

In what follows, we specialize to studying symplectic groups over $R = \mathbb{Z}$, $R = \mathbb{Z}_\ell$, or $R = \mathbb{Z}/\ell^k\mathbb{Z}$ for ℓ a prime number and k a positive integer. We will adhere to the following notational conventions:

- Let $H_\ell \subset \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ be a closed subgroup.
- Let $H(\ell^k) \subset \mathrm{Sp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z})$ be the mod-ℓ^k reduction of H_ℓ.
- Notice that the map $S \mapsto \mathrm{id}_{2g} + \ell^k S$ gives an isomorphism of groups

$$\mathfrak{sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) \simeq \ker(\mathrm{Sp}_{2g}(\mathbb{Z}/\ell^{k+1}\mathbb{Z}) \to \mathrm{Sp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z}))$$

for every $k \geq 1$. We will use $\mathfrak{sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ to denote the above kernel when we want to think of its elements additively, and we will use the kernel notation when we want to view its elements multiplicatively.

- For any group G, let $[G, G]$ be its commutator subgroup, and let $G^{\mathrm{ab}} = G/[G, G]$ be its abelianization.

2.2 Commutators

We shall now compute the abelianizations of $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ and $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z})$ for every integer $g \geq 2$, prime number ℓ, and positive integer k. It will first be convenient for us to compute the abelianization $\mathrm{Sp}_{2g}(\mathbb{Z})^{\mathrm{ab}}$.

Lemma 1 *The abelianization* $\mathrm{Sp}_{2g}(\mathbb{Z})^{\mathrm{ab}}$ *is trivial when* $g \geq 3$ *and is isomorphic to* $\mathbb{Z}/2\mathbb{Z}$ *when* $g = 2$.

Proof The case $g \geq 3$ follows from [3, Remark, p. 123], so it only remains to deal with the case $g = 2$. By [4, Satz], $\mathrm{Sp}_4(\mathbb{Z})$ has two generators K and L that satisfy several relations, three of which are given as follows:

$$\begin{aligned} K^2 &= \mathrm{id}_{2g}, \\ L^{12} &= \mathrm{id}_{2g}, \\ (K \cdot L^5)^5 &= (L^6 \cdot K \cdot L^5 \cdot K \cdot L^7 \cdot K)^2. \end{aligned}$$

By the universal property of the abelianization, we have that $\mathrm{Sp}_4(\mathbb{Z})^{\mathrm{ab}}$ is a quotient of the rank-2 free abelian group $K\mathbb{Z} \oplus L\mathbb{Z}$ generated by K and L. Thus, from the aforementioned multiplicative relations between K and L in $\mathrm{Sp}_4(\mathbb{Z})$, we obtain the following additive relations in the abelianization

$$\begin{aligned} 2K &= 0, \\ 12L &= 0, \\ 5(K + 5L) &= 2 \cdot (6L + K + 5L + K + 7L + K). \end{aligned}$$

Substituting the first two relations above into the third relation, we find $L = K$, which implies that $\mathrm{Sp}_4(\mathbb{Z})^{\mathrm{ab}}$ is a quotient of $(K\mathbb{Z} \oplus L\mathbb{Z})/(2K, K - L) \simeq \mathbb{Z}/2\mathbb{Z}$.

It remains to show that $\mathrm{Sp}_4(\mathbb{Z})$ maps surjectively onto $\mathbb{Z}/2\mathbb{Z}$. Postcomposing the surjection $\mathrm{Sp}_4(\mathbb{Z}) \twoheadrightarrow \mathrm{Sp}_4(\mathbb{Z}/2\mathbb{Z})$ with the isomorphism $\mathrm{Sp}_4(\mathbb{Z}/2\mathbb{Z}) \simeq S_6$ by [10, 3.1.5] and then applying the sign map $S_6 \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$ yields the desired result. □

Remark 3 Let $\widehat{\mathbb{Z}}$ denote the profinite completion of $\mathbb{Z}$. It follows immediately from Lemma 1, together with the fact if G_1 and G_2 are groups with $\widehat{G_1} \simeq \widehat{G_2}$ then $\widehat{G_1^{\mathrm{ab}}} \simeq \widehat{G_2^{\mathrm{ab}}}$, that the group $\mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})^{\mathrm{ab}}$ is trivial for $g \geq 3$ and is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ when $g = 2$.

Using Lemma 1, we can now compute the abelianizations of all aforementioned groups.

Proposition 1 *We have the following results:*

a. The group $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)^{\mathrm{ab}}$ *is trivial except when* $g = \ell = 2$, *in which case it is isomorphic to* $\mathbb{Z}/2\mathbb{Z}$.

b. *Let* $k \geq 1$. *The group* $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z})^{\mathrm{ab}}$ *is trivial except when* $g = \ell = 2$, *in which case it is isomorphic to* $\mathbb{Z}/2\mathbb{Z}$.

Proof We first verify Statement (a). For $g \geq 3$, since $\mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})^{\mathrm{ab}}$ is trivial, and since we have a surjection $\mathrm{Sp}_{2g}(\widehat{\mathbb{Z}}) \twoheadrightarrow \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$, the result follows immediately. Now take $g = 2$. First, we have surjections $\mathrm{Sp}_4(\widehat{\mathbb{Z}}) \twoheadrightarrow \mathrm{Sp}_4(\mathbb{Z}_2) \twoheadrightarrow \mathrm{Sp}_4(\mathbb{Z}/2\mathbb{Z}) \cong S_6$. Since the former and the latter have abelianizations isomorphic to $\mathbb{Z}/2\mathbb{Z}$, using Lemma 1, it follows that $\mathrm{Sp}_4(\mathbb{Z}_2)^{\mathrm{ab}} \cong \mathbb{Z}/2\mathbb{Z}$. Then, since we have

$$\mathbb{Z}/2\mathbb{Z} \cong \mathrm{Sp}_4(\widehat{\mathbb{Z}})^{\mathrm{ab}} \cong \mathrm{Sp}_4(\mathbb{Z}_2)^{\mathrm{ab}} \times \prod_{\ell \neq 2} \mathrm{Sp}_4(\mathbb{Z}_\ell)^{\mathrm{ab}} \cong \mathbb{Z}/2\mathbb{Z} \times \prod_{\ell \neq 2} \mathrm{Sp}_4(\mathbb{Z}_\ell)^{\mathrm{ab}},$$

it follows that $\mathrm{Sp}_4(\mathbb{Z}_\ell)^{\mathrm{ab}}$ is trivial for $\ell \neq 2$.

Now, observe that Statement (b) follows from Statement (a): indeed, notice that the surjection $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell) \to \mathrm{Sp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z})$ induces a surjection $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)^{\mathrm{ab}} \to \mathrm{Sp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z})^{\mathrm{ab}}$ and in the case of $\ell = g = 2$, $\mathrm{Sp}_4(\mathbb{Z}/2^k\mathbb{Z})^{\mathrm{ab}}$ is nontrivial as it surjects onto $\mathrm{Sp}_4(\mathbb{Z}/2\mathbb{Z})^{\mathrm{ab}} \cong \mathbb{Z}/2\mathbb{Z}$. ◻

3 Proof of Theorem 1

In this section, we provide a complete proof of the main theorem of this paper, namely Theorem 1. The basic strategy has two steps: lift from ℓ^2 to ℓ^∞ (see Sect. 3.1), and lift from ℓ to ℓ^2 (see Sect. 3.2). Considerable care must be taken in dealing with the cases where $\ell = 2, 3$, so we treat these situations separately (see Sects. 3.3 and 3.4). We execute this strategy as follows:

3.1 Lifting from ℓ^2 to ℓ^∞ for $\ell \geq 3$, and from 8 to 2^∞

Lemma 2 *If* $\ell \geq 3$, *then* $H(\ell^2) = \mathrm{Sp}_{2g}(\mathbb{Z}/\ell^2\mathbb{Z})$ *implies* $H_\ell = \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$. *If* $\ell = 2$, *then* $H(8) = \mathrm{Sp}_{2g}(\mathbb{Z}/8\mathbb{Z})$ *implies* $H_2 = \mathrm{Sp}_{2g}(\mathbb{Z}_2)$.

Proof This is done in the $g = 1$ case in [11, Lemma 3, Section IV.3.4], which readily generalizes to the case of $g \geq 2$. ◻

3.2 Lifting from ℓ to ℓ^2 for $\ell \geq 5$

Lemma 3 *Fix* $g \geq 2$. *If* $\ell \geq 5$, *then* $H(\ell) = \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ *implies* $H(\ell^2) \subset \mathrm{Sp}_{2g}(\mathbb{Z}/\ell^2\mathbb{Z})$.

Proof It suffices to show that $H(\ell^2)$ contains all of

$$\ker(\mathrm{Sp}_{2g}(\mathbb{Z}/\ell^2\mathbb{Z}) \twoheadrightarrow \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})) = \mathrm{id}_{2g} + \ell \cdot \mathfrak{sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}).$$

We prove this by taking ℓth powers of specific matrices. We want to pick $M \in \mathfrak{sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ such that $\mathrm{id}_{2g} + M$ lies in $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ and such that $M^2 = 0$. As it happens, these two conditions are equivalent: indeed, since $M^T\Omega_{2g} + \Omega_{2g}M = 0$, we have

$$\begin{aligned}(\mathrm{id}_{2g} + M)^T\Omega_{2g}(\mathrm{id}_{2g} + M) &= \Omega_{2g} + M^T\Omega_{2g} + \Omega_{2g}M + M^T\Omega_{2g}M \\ &= \Omega_{2g} + M^T\Omega_{2g}M \\ &= \Omega_{2g} - \Omega_{2g}M^2,\end{aligned}$$

so the condition that $\mathrm{id}_{2g} + M$ is symplectic is equivalent to the condition that $M^2 = 0$. Moreover, by expanding in terms of matrices, we see that $M^2 = 0$ if and only if

$$\left[\begin{array}{c|c} A^2 + BC & AB - BA^T \\ \hline CA - A^T C & CB + (A^T)^2 \end{array}\right] = 0.$$

In particular, this shows that $\mathrm{id}_{2g} + M$ is symplectic whenever $A^2 = 0$ and two of A, B, C are zero.

For $M \in \mathfrak{sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$, choose an arbitrary lift of M in $\mathrm{Mat}_{2g\times 2g}(\mathbb{Z}/\ell^2\mathbb{Z})$, and by abuse of notation, also denote it M. By assumption, $H(\ell^2)$ contains an element of the form $\mathrm{id}_{2g} + M + \ell V$ for some $V \in \mathrm{Mat}_{2g\times 2g}(\mathbb{Z}/\ell\mathbb{Z})$. This means that $H(\ell^2)$ contains

$$\begin{aligned}(\mathrm{id}_{2g} + M + \ell V)^\ell &\equiv \mathrm{id}_{2g} + \ell(M + \ell V) + \binom{\ell}{2}(M + \ell V)^2 + \cdots \\ &\quad + \binom{\ell}{\ell - 1}(M + \ell V)^{\ell-1} + (M + \ell V)^\ell \\ &\equiv \mathrm{id}_{2g} + \ell M \pmod{\ell^2},\end{aligned}$$

where the last step above relies crucially upon the assumption that $\ell \geq 5$.

We conclude that $H(\ell^2)$ contains $\mathrm{id}_{2g} + \ell M$ for every M satisfying the above conditions.

Taking $A = C = 0$, we see that $H(\ell^2)$ contains

$$\mathrm{id}_{2g} + \ell \cdot \left[\begin{array}{c|c} 0 & B \\ \hline 0 & 0 \end{array}\right]$$

for any symmetric matrix B. Similarly, taking $A = B = 0$ gives us any symmetric matrix in the lower-left corner.

Taking $B = C = 0$ shows that $H(\ell^2)$ contains

$$\mathrm{id}_{2g} + \ell \cdot \left[\begin{array}{c|c} A & 0 \\ \hline 0 & -A^T \end{array}\right]$$

for any matrix A with $A^2 = 0$. It is a standard fact that the span of such matrices A is the space of trace zero matrices. Observe that $\mathrm{tr}\, A = 0$ is a single linear condition on $\mathfrak{sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ that singles out a codimension-one linear subspace $W \subset \mathfrak{sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$, so that

$$\mathrm{id}_{2g} + \ell W \subset H(\ell^2) \cap \ker(\mathrm{Sp}_{2g}(\mathbb{Z}/\ell^2\mathbb{Z}) \twoheadrightarrow \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})). \tag{3.1}$$

Observe that if the inclusion in (3.1) were strict, then the right-hand side would be all of $\mathrm{id}_{2g} + \ell \cdot \mathfrak{sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$, and the desired result follows. Therefore, suppose the inclusion in (3.1) is an equality. Since W has index ℓ in $\mathfrak{sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$, it follows that $H(\ell^2)$ has index ℓ in $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell^2\mathbb{Z})$. We obtain a surjection

$$\mathrm{Sp}_{2g}(\mathbb{Z}/\ell^2\mathbb{Z}) \twoheadrightarrow \mathrm{Sp}_{2g}(\mathbb{Z}/\ell^2\mathbb{Z})/H(\ell^2) \cong \mathbb{Z}/\ell\mathbb{Z},$$

which contradicts Proposition 1. □

3.3 Lifting from 4 to 8

Lemma 4 *Fix* $g \geq 2$. *Then* $H(4) = \mathrm{Sp}_{2g}(\mathbb{Z}/4\mathbb{Z})$ *implies* $H(8) = \mathrm{Sp}_{2g}(\mathbb{Z}/8\mathbb{Z})$.

Proof We modify the proof of Lemma 3. As in that proof, we consider a matrix

$$M = \left[\begin{array}{c|c} A & B \\ \hline C & -A^T \end{array}\right] \in \mathfrak{sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$$

with the property that $\mathrm{id}_{2g}+2M$ lies in $\mathrm{Sp}_{2g}(\mathbb{Z}/4\mathbb{Z})$ and $M^2=0$. This time, however, the first condition automatically holds because

$$\begin{aligned}(\mathrm{id}_{2g}+2M)^T\Omega_{2g}(\mathrm{id}_{2g}+2M) &\equiv \Omega_{2g}+2(M^T\Omega_{2g}+\Omega_{2g}M)+4M^T\Omega_{2g}M\\ &\equiv \Omega_{2g} \pmod 4.\end{aligned}$$

Nevertheless, note that the second condition is again satisfied whenever $A^2=0$ and two of A, B, and C are zero.

Choose an arbitrary lift of M in $\mathrm{Mat}_{2g\times 2g}(\mathbb{Z}/4\mathbb{Z})$, and by abuse of notation also refer to it as M. By assumption, $H(8)$ contains an element of the form $\mathrm{id}_{2g}+2M+4V$ for some $V\in\mathrm{Mat}_{2g\times 2g}(\mathbb{Z}/2\mathbb{Z})$, which means that $H(8)$ contains

$$(\mathrm{id}_{2g}+2M+4V)^2\equiv \mathrm{id}_{2g}+4M \pmod 8.$$

Taking $W\subset\mathfrak{sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$ to be the trace-zero subspace as before, this implies

$$\mathrm{id}_{2g}+4\cdot W\subset H(8)\cap\ker(\mathrm{Sp}_{2g}(\mathbb{Z}/8\mathbb{Z})\twoheadrightarrow\mathrm{Sp}_{2g}(\mathbb{Z}/4\mathbb{Z})).$$

If the inclusion were strict, again the right-hand side would contain the kernel of reduction, so the desired result follows. Therefore, suppose the inclusion is an equality, so that $H(8)$ has index 2 in $\mathrm{Sp}_{2g}(\mathbb{Z}/8\mathbb{Z})$. If $g\geq 3$, Proposition 1 tells us that $\mathrm{Sp}_{2g}(\mathbb{Z}/8\mathbb{Z})^{\mathrm{ab}}$ is trivial, which is a contradiction. If $g=2$, the same proposition tells us that $H(8)=[\mathrm{Sp}_4(\mathbb{Z}/8\mathbb{Z}),\mathrm{Sp}_4(\mathbb{Z}/8\mathbb{Z})]$, so since the image of this commutator under the abelianization map

$$\mathrm{Sp}_4(\mathbb{Z}/8\mathbb{Z})\twoheadrightarrow\mathrm{Sp}_4(\mathbb{Z}/2\mathbb{Z})\twoheadrightarrow\mathbb{Z}/2\mathbb{Z}$$

is trivial, $H(8)$ cannot surject onto $\mathrm{Sp}_4(\mathbb{Z}/2\mathbb{Z})$, which is again a contradiction. □

3.4 Lifting from 2 to 4 and from 3 to 9

Proposition 2 *Fix $g\geq 2$. The following statements hold:*

a. *Take $\ell=2$. Then $H(2)=\mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$ implies that $H(4)=\mathrm{Sp}_{2g}(\mathbb{Z}/4\mathbb{Z})$.*
b. *Take $\ell=3$. Then $H(3)=\mathrm{Sp}_{2g}(\mathbb{Z}/3\mathbb{Z})$ implies that $H(9)=\mathrm{Sp}_{2g}(\mathbb{Z}/9\mathbb{Z})$.*

Idea of Proof

The argument will proceed by induction on g. We start by verifying the base case $g=2$ in Lemma 5. We then inductively assume this holds for $g-1$ and prove it for g. We use the inductive hypothesis to construct a particular element lying in $H(\ell^2)$ in Lemma 6. Then, we use Lemma 7 to show that conjugates of this particular element generate $\mathfrak{sp}_4(\mathbb{Z}/\ell^2\mathbb{Z})$, embedded as in (3.8). We finally translate around this copy of $\mathfrak{sp}_4(\mathbb{Z}/\ell^2\mathbb{Z})$ to obtain that $H(\ell^2)=\mathrm{Sp}_{2g}(\mathbb{Z}/\ell^2\mathbb{Z})$.

The following lemma deals with the base case:

Lemma 5 *Proposition 2 holds in the case that $g=2$.*

Proof The following `Magma` code verifies the claim for both $\ell=2$ and $\ell=3$.

```
for l in [2,3] do
Z := Integers();
G := GL(4,quo<Z|l*l>);
A := elt<G | 1,0,0,0, 1,-1,0,0, 0,0,1,1, 0,0,0,-1>;
B := elt<G| 0,0,-1,0, 0,0,0,-1, 1,0,1,0, 0,1,0,0>;
H := sub<G|A,B>;
maximals := SubgroupClasses(H: Al := "Maximal");
S := quo<Z|l>;
grp, f := ChangeRing(G, S);
for H in maximals do
if #f(H`subgroup) eq #Sp(4,l) then
assert false;
end if;
end for;
end for;
```

This concludes the proof of Lemma 5. □

In order to handle the inductive step of Proposition 2, we first introduce some notation. Let $\phi_{\ell,2g}\colon \operatorname{Sp}_{2g}(\mathbb{Z}/\ell^2\mathbb{Z}) \twoheadrightarrow \operatorname{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ denote the usual reduction map. Our aim is to define the maps π, ι_ℓ in the diagram

$$\begin{tikzcd}
& \phi^{-1}_{\ell,2g}(\operatorname{Sp}_{2g-2}(\mathbb{Z}/\ell\mathbb{Z})) \arrow[r, hook] \arrow[dl, two heads, "\pi"'] \arrow[dd, two heads] & \operatorname{Sp}_{2g}(\mathbb{Z}/\ell^2\mathbb{Z}) \arrow[dd, two heads, "\phi_{\ell,2g}"] \\
\operatorname{Sp}_{2g-2}(\mathbb{Z}/\ell^2\mathbb{Z}) \arrow[dr, two heads, "\phi_{\ell,2g-2}"'] & & \\
& \operatorname{Sp}_{2g-2}(\mathbb{Z}/\ell\mathbb{Z}) \arrow[r, hook, "\iota_\ell"'] & \operatorname{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})
\end{tikzcd} \tag{3.2}$$

The map ι_ℓ will be defined in (3.3) and the map π will be defined in (3.4) For the present purpose, it is convenient to use a different Ω-matrix, which we shall denote by J_{2g}, in the definition of symplectic group Sp_{2g} and its Lie algebra $\mathfrak{sp}_{2g}$. Inductively define

$$J_2 := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad \text{and} \quad J_{2g} := \left[\begin{array}{c|c} J_{2g-2} & 0 \\ \hline 0 & J_2 \end{array}\right].$$

The matrix J_{2g} is a block-diagonal matrix with each block being a copy of J_2.

Now let $M \in \operatorname{Sp}_{2g-2}(\mathbb{Z}/\ell^2\mathbb{Z})$. The map

$$M \mapsto \left[\begin{array}{c|c} M & 0 \\ \hline 0 & \mathrm{id}_2 \end{array}\right]$$

gives an inclusion

$$\iota_{\ell^2}\colon \operatorname{Sp}_{2g-2}(\mathbb{Z}/\ell^2\mathbb{Z}) \hookrightarrow \operatorname{Sp}_{2g}(\mathbb{Z}/\ell^2\mathbb{Z})$$

which, when taken modulo ℓ, reduces to an inclusion

$$\iota_\ell\colon \operatorname{Sp}_{2g-2}(\mathbb{Z}/\ell\mathbb{Z}) \hookrightarrow \operatorname{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}). \tag{3.3}$$

Thus, the group $\phi^{-1}_{\ell,2g}(\operatorname{Sp}_{2g-2}(\mathbb{Z}/\ell\mathbb{Z}))$ [see the diagram in (3.2)] consists of matrices satisfying

$$\left[\begin{array}{c|c} A_{(2g-2)\times(2g-2)} & B_{(2g-2)\times 2} \\ \hline C_{2\times(2g-2)} & D_{2\times 2} \end{array}\right] \equiv \left[\begin{array}{c|c} M & 0 \\ \hline 0 & \mathrm{id}_2 \end{array}\right] \pmod{\ell}$$

where $M \in \mathrm{Sp}_{2g-2}(\mathbb{Z}/\ell\mathbb{Z})$ and the blocks A, B, C, D have the indicated sizes. For two such matrices, we have

$$\left[\begin{array}{c|c} A_1 & B_1 \\ \hline C_1 & D_1 \end{array}\right] \cdot \left[\begin{array}{c|c} A_2 & B_2 \\ \hline C_2 & D_2 \end{array}\right] \equiv \left[\begin{array}{c|c} A_1A_2 + B_1C_2 & A_1B_2 + B_1D_2 \\ \hline C_1A_2 + D_1C_2 & C_1B_2 + D_1D_2 \end{array}\right]$$
$$\equiv \left[\begin{array}{c|c} A_1A_2 & A_1B_2 + B_1D_2 \\ \hline C_1A_2 + D_1C_2 & D_1D_2 \end{array}\right] \pmod{\ell^2},$$

where the last step follows because $B_1C_2 \equiv C_1B_2 \equiv 0 \pmod{\ell^2}$. Therefore, the map

$$\pi : \phi_{\ell,2g}^{-1}(\mathrm{Sp}_{2g-2}(\mathbb{Z}/\ell\mathbb{Z})) \twoheadrightarrow \mathrm{Sp}_{2g-2}(\mathbb{Z}/\ell^2\mathbb{Z}) \quad \text{sending} \quad \left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right] \mapsto A \tag{3.4}$$

is a group homomorphism. This completes the definition of the maps ι_ℓ and π, and it is apparent that the diagram in (3.2) commutes.

With this notation set, we continue our proof of Proposition 2. In Lemma 6, we show via explicit matrix multiplication that one of two particular matrices lies in $H(\ell^2)$.

Lemma 6 *Suppose that* $\pi(H(\ell^2) \cap \phi_{\ell,2g}^{-1}(\mathrm{Sp}_{2g-2}(\mathbb{Z}/\ell\mathbb{Z}))) = \mathrm{Sp}_{2g-2}(\mathbb{Z}/\ell^2\mathbb{Z})$ *and* $H(\ell) = \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$*. Then, defining*

$$\Phi := \mathrm{id}_{2g} + \ell \cdot \left[\begin{array}{cccc|c} -1 & -1 & 0 & 0 & \\ 0 & 1 & 0 & 0 & \\ 0 & 0 & 0 & 0 & 0_{4\times(2g-4)} \\ 0 & 0 & 0 & 0 & \\ \hline \multicolumn{4}{c|}{0_{(2g-4)\times 4}} & 0_{(2g-4)\times(2g-4)} \end{array}\right] \quad \text{and} \tag{3.5}$$

$$\Psi := \mathrm{id}_{2g} + \ell \cdot \left[\begin{array}{cccc|c} -1 & -1 & 1 & 0 & \\ 0 & 1 & 0 & 0 & \\ 0 & 0 & 0 & 0 & 0_{4\times(2g-4)} \\ 0 & -1 & 0 & 0 & \\ \hline \multicolumn{4}{c|}{0_{(2g-4)\times 4}} & 0_{(2g-4)\times(2g-4)} \end{array}\right], \tag{3.6}$$

we have that either Φ *or* Ψ *lies in* $H(\ell^2)$*.*

Proof Since we are assuming $\pi(H(\ell^2) \cap \phi_{\ell,2g}^{-1}(\mathrm{Sp}_{2g-2}(\mathbb{Z}/\ell\mathbb{Z}))) = \mathrm{Sp}_{2g-2}(\mathbb{Z}/\ell^2\mathbb{Z})$, it follows that

$$\mathrm{id}_{2g-2} + \ell \cdot \left[\begin{array}{cc|c} 0 & 0 & \\ 1 & 0 & 0_{2\times(2g-4)} \\ \hline \multicolumn{2}{c|}{0_{(2g-4)\times 2}} & 0_{(2g-4)\times(2g-4)} \end{array}\right]$$

lies in $\pi(H(\ell^2) \cap \phi_{\ell,2g}^{-1}(\mathrm{Sp}_{2g-2}(\mathbb{Z}/\ell\mathbb{Z})))$.

It follows that $H(\ell^2)$ contains an element of the form $M = \mathrm{id}_{2g} + \ell U$ for

$$U = \left[\begin{array}{cc|c|c} 0 & 0 & & \\ 1 & 0 & 0_{2\times(2g-4)} & A_{2\times 2} \\ \hline \multicolumn{2}{c|}{0_{(2g-4)\times 2}} & 0_{(2g-4)\times(2g-4)} & B_{(2g-4)\times 2} \\ \hline \multicolumn{2}{c|}{A'_{2\times 2}} & B'_{2\times(2g-4)} & C_{2\times 2} \end{array}\right],$$

where there is a linear relation between $A_{2\times 2}$ and $A'_{2\times 2}$, as well as a linear relation between $B_{(2g-4)\times 2}$ and $B'_{2\times(2g-4)}$, imposed by the symplectic constraint $M^T J_{2g} M = J_{2g}$. For any $M \in H(\ell^2)$, the group $H(\ell^2)$ also contains

$$M^{-1}(\mathrm{id}_{2g} + \ell U)M = \mathrm{id}_{2g} + \ell M^{-1}UM,$$

where the right-hand-side only depends on the reduction of M modulo ℓ. Since $H(\ell^2)$ surjects onto $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$, the matrix $M \pmod{\ell}$ ranges over all elements of $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$. With this in mind, take a matrix M given by

$$M := \left[\begin{array}{c|c|c} \begin{matrix}1 & 1\\ 0 & 1\end{matrix} & 0_{2\times(2g-4)} & 0_{2\times 2} \\ \hline 0_{(2g-4)\times 2} & \mathrm{id}_{2g-4} & 0_{(2g-4)\times 2} \\ \hline 0_{2\times 2} & 0_{2\times(2g-4)} & \mathrm{id}_2 \end{array}\right] \pmod{\ell}$$

so that $H(\ell^2)$ contains $M^{-1}(\mathrm{id}_{2g} + \ell U)M$, which equals

$$\mathrm{id}_{2g} + \ell \cdot \left[\begin{array}{c|c|c} \begin{matrix}-1 & -1\\ 0 & 1\end{matrix} & 0_{2\times(2g-4)} & \begin{bmatrix}0 & -1\\ 0 & 0\end{bmatrix} \cdot A_{2\times 2} \\ \hline 0_{(2g-4)\times 2} & 0_{(2g-4)\times(2g-4)} & 0_{(2g-4)\times 2} \\ \hline A'_{2\times 2} \cdot \begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix} & 0_{2\times(2g-4)} & 0_{2\times 2} \end{array}\right]. \tag{3.7}$$

Multiplying (3.7) on the left by $(\mathrm{id}_{2g} + \ell U)^{-1} \equiv \mathrm{id}_{2g} - \ell U \pmod{\ell^2}$ shows that $H(\ell^2)$ contains

$$\begin{aligned} N &:= (\mathrm{id}_{2g} + \ell U)^{-1} M^{-1} (\mathrm{id}_{2g} + \ell U) M \\ &= \mathrm{id}_{2g} + \ell \cdot \left[\begin{array}{c|c|c} \begin{matrix}-1 & -1\\ 0 & 1\end{matrix} & 0_{2\times(2g-4)} & \begin{bmatrix}0 & -1\\ 0 & 0\end{bmatrix} \cdot A_{2\times 2} \\ \hline 0_{(2g-4)\times 2} & 0_{(2g-4)\times(2g-4)} & 0_{(2g-4)\times 2} \\ \hline A'_{2\times 2} \cdot \begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix} & 0_{2\times(2g-4)} & 0_{2\times 2} \end{array}\right]. \end{aligned}$$

Conjugating N by any matrix of the form

$$P := \left[\begin{array}{c|c|c} \mathrm{id}_2 & 0_{2\times(2g-4)} & 0_{2\times 2} \\ \hline 0_{(2g-4)\times 2} & \mathrm{id}_{2g-4} & 0_{(2g-4)\times 2} \\ \hline 0_{2\times 2} & 0_{2\times(2g-4)} & M_{2\times 2} \end{array}\right] \pmod{\ell},$$

where $M_{2\times 2} \in \mathrm{Sp}_2(\mathbb{Z}/\ell^2\mathbb{Z})$, results in the matrix

$$\begin{aligned} N' &:= P^{-1}NP \\ &= \mathrm{id}_{2g} + \ell \cdot V, \end{aligned}$$

where

$$V := \left[\begin{array}{c|c|c} \begin{matrix}-1 & -1\\ 0 & 1\end{matrix} & 0_{2\times(2g-4)} & \begin{bmatrix}0 & -1\\ 0 & 0\end{bmatrix} \cdot A_{2\times 2} \cdot M_{2\times 2} \\ \hline 0_{(2g-4)\times 2} & 0_{(2g-4)\times(2g-4)} & 0_{(2g-4)\times 2} \\ \hline M_{2\times 2}^{-1} \cdot A'_{2\times 2} \cdot \begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix} & 0_{2\times(2g-4)} & 0_{2\times 2} \end{array}\right].$$

By choosing $M_{2\times 2}$ judiciously, we may arrange that

$$\begin{bmatrix} 0 & -1 \\ 0 & 0 \end{bmatrix} \cdot A_{2\times 2} \cdot M_{2\times 2} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},$$

depending on whether the bottom row of $A_{2\times 2}$ is nonzero or zero, respectively. Upon conjugating by the matrix

$$\left[\begin{array}{c|c} \mathrm{id}_2 & 0_{2\times(2g-2)} \\ \hline 0_{(2g-2)\times 2} & \begin{array}{c|c|c} 0_{2\times 2} & 0_{2\times(2g-6)} & \mathrm{id}_2 \\ \hline 0_{(2g-6)\times 2} & \mathrm{id}_{2g-6} & 0_{(2g-6)\times 2} \\ \hline \mathrm{id}_2 & 0_{2\times(2g-6)} & 0_{2\times 2} \end{array} \end{array}\right] \in \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}),$$

we conclude that $H(\ell^2)$ contains either Φ or Ψ. □

Next, in Lemma 7, we show that we can conjugate the matrices Φ and Ψ from Lemma 6 to obtain all of $\mathrm{Sp}_4(\mathbb{Z}/\ell\mathbb{Z})$.

Lemma 7 *Let $\ell = 2$ or 3. Let $\overline{\Phi}$ and $\overline{\Psi}$ denote the upper-left 4×4 blocks of Φ and Ψ, respectively. Then the sets*

$$\left\{M^{-1}\overline{\Phi}M : M \in \mathrm{Sp}_4(\mathbb{Z}/\ell\mathbb{Z})\right\} \quad \textit{and} \quad \left\{M^{-1}\overline{\Psi}M : M \in \mathrm{Sp}_4(\mathbb{Z}/\ell\mathbb{Z})\right\}$$

are both spanning sets for $1 + \ell \cdot \mathfrak{sp}_4(\mathbb{Z}/\ell\mathbb{Z})$.

Proof The following `Magma` code verifies that each of the sets defined in the lemma statement span $\mathfrak{sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$.

```
for l in [2, 3] do
Z := Integers();
G := GL(4,quo<Z|l*l>);
A := elt<G| 1,0,0,0, 1,1,0,0, 0,0,1,0, 0,0,0,1>;
B := elt<G| 1,1,0,0, 0,1,1,0, 1,1,1,1, 1,1,0,1>;
H := sub<G|A,B>;
grp, f := ChangeRing(G, quo<Z|l>);
Lie := Kernel(f) meet H;
M := elt<G| 1-l,-l,0,0, 0,1+l,0,0, 0,0,1,0, 0,0,0,1>;
N := elt<H| 1-l,-l,l,0, 0,1 + l,0,0, 0,0,1,0, 0,-l,0,1>;
#sub<H|Conjugates(H,M)> eq #Lie;
#sub<H|Conjugates(H,N)> eq #Lie;
end for;
```

This concludes the proof of Lemma 7. □

We now have the tools to prove Proposition 2.

Proof of Proposition 2 The base case $g = 2$ is Lemma 5. Now take $g \geq 3$, and suppose the result holds for $g - 1$. We shall now use the inductive hypothesis to show that $\ker \phi_{\ell,2g} \subset H(\ell^2)$, which would imply that $H(\ell^2) = \mathrm{Sp}_{2g}(\mathbb{Z}/\ell^2\mathbb{Z})$. Since $H(\ell^2)$ surjects onto $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$, we have that the group $H(\ell^2) \cap \phi_{\ell,2g}^{-1}(\mathrm{Sp}_{2g-2}(\mathbb{Z}/\ell\mathbb{Z}))$ surjects onto $\mathrm{Sp}_{2g-2}(\mathbb{Z}/\ell\mathbb{Z})$, and therefore so does $\pi(H(\ell^2) \cap \phi_{\ell,2g}^{-1}(\mathrm{Sp}_{2g-2}(\mathbb{Z}/\ell\mathbb{Z})))$. By the inductive hypothesis, $\pi(H(\ell^2) \cap \phi_{\ell,2g}^{-1}(\mathrm{Sp}_{2g-2}(\mathbb{Z}/\ell\mathbb{Z}))) = \mathrm{Sp}_{2g-2}(\mathbb{Z}/\ell^2\mathbb{Z})$, so upon applying Lemma 6, we deduce that either Φ or Ψ lies in $H(\ell^2)$. Now, conjugating by matrices of the form

$$\left[\begin{array}{c|c} M_{4\times 4} & 0_{4\times(2g-4)} \\ \hline 0_{(2g-4)\times 4} & \mathrm{id}_{2g-4} \end{array}\right] \pmod{\ell}$$

where $M_{4\times 4} \in \mathrm{Sp}_4(\mathbb{Z}/\ell\mathbb{Z})$ serves to conjugate the upper-left 4×4 of Φ and Ψ by $M_{4\times 4}$. By Lemma 7, we have that $\mathfrak{sp}_4(\mathbb{Z}/\ell^2\mathbb{Z}) \subset H(\ell^2)$, embedded as

$$\mathrm{id}_{2g} + \ell \cdot \left[\begin{array}{c|c} \mathfrak{sp}_4(\mathbb{Z}/\ell\mathbb{Z}) & 0_{4\times(2g-4)} \\ \hline 0_{(2g-4)\times 4} & 0_{(2g-4)\times(2g-4)} \end{array}\right]. \tag{3.8}$$

Construct $Q \in \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ by taking any $g \times g$ permutation matrix and replacing each 1 with an id_2-block. Conjugating the subspace in (3.8) by various such Q shows that $H(\ell^2)$ contains $\ker \phi_{\ell,2g}$. This can be seen by a straightforward argument involving choosing a basis for $\mathfrak{sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ whose elements are elementary matrices or sums of two elementary matrices. □

3.5 Finishing the Proof

We can now complete the proof of Theorem 1

Proof of Theorem 1 We split into three cases:

- Suppose $\ell \geq 5$. Then Lemma 3 implies $H(\ell^2) = \mathrm{Sp}_{2g}(\mathbb{Z}/\ell^2\mathbb{Z})$.
- Suppose $\ell = 3$. Then Lemma 2 implies $H(9) = \mathrm{Sp}_{2g}(\mathbb{Z}/9\mathbb{Z})$.
- Suppose $\ell = 2$. Then Lemma 2 implies $H(4) = \mathrm{Sp}_{2g}(\mathbb{Z}/4\mathbb{Z})$. From this, Lemma 4 implies $H(8) = \mathrm{Sp}_{2g}(\mathbb{Z}/8\mathbb{Z})$.

Combining the above results with Lemma 2 gives the desired conclusion. □

Author details

[1]Department of Mathematics, Stanford University, Stanford, CA 94305, USA, [2]Department of Mathematics, Harvard College, Cambridge, MA 02138, USA, [3]Department of Mathematics, Caltech, Pasadena, CA 91126, USA.

Acknowledgements

This research was supervised by Ken Ono and David Zureick-Brown at the Emory University Mathematics REU and was supported by the National Science Foundation (Grant Number DMS-1557960). We would like to thank David Zureick-Brown for suggesting the problem that led to the present article and for offering us his invaluable advice and guidance. We would also like to thank David Zureick-Brown for providing the intuition behind the proof of Lemma 3. We would like to thank Jackson Morrow, Ken Ono, and David Zureick-Brown for making several helpful comments regarding the composition of this article. We would like to acknowledge Michael Aschbacher and Nick Gill for their helpful advice. We used `Magma` and *Mathematica* for explicit calculations.

Competing interests

The authors declare that they have no competing interests.

Received: 21 February 2017 Accepted: 26 February 2017

References

1. Achter, J.D., Pries, R.: The integral monodromy of hyperelliptic and trielliptic curves. Math. Ann. **338**(1), 187–206 (2007). doi:10.1007/s00208-006-0072-0
2. Achter, J.D., Pries, R.: Monodromy of the *p*-rank strata of the moduli space of curves. Int. Math. Res. Not. **25**, rnn053 (2008). doi:10.1093/imrn/rnn053
3. Bass, H., Milnor, J., Serre, J.P.: Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$). Inst. Hautes Études Sci. Publ. Math. **33**, 59–137 (1967)
4. Bender, P.: Eine Präsentation der symplektischen Gruppe Sp(4, $\mathbf{Z}$) mit 2 Erzeugenden und 8 definierenden Relationen. J. Algebra **65**(2), 328–331 (1980). doi:10.1016/0021-8693(80)90221-5
5. Dokchitser, T., Dokchitser, V.: Surjectivity of mod 2^n representations of elliptic curves. Math. Z. **272**(3–4), 961–964 (2012). doi:10.1007/s00209-011-0967-7
6. Elkies, N.D.: Elliptic curves with 3-adic Galois representation surjective mod 3 but not mod 9. ArXiv Mathematics e-prints (2006)
7. Hui, C.Y., Larsen, M.: Type A images of Galois representations and maximality. Mathematische Zeitschrift **284**, 1–15 (2016). doi:10.1007/s00209-016-1683-0
8. Landesman, A., Swaminathan, A.A., Tao, J., Xu, Y.: Hyperelliptic curves with maximal Galois action on the torsion points of their Jacobians (2016). In Preparation
9. Landesman, A., Swaminathan, A.A., Tao, J., Xu, Y.: Surjectivity of Galois representations in rational families of abelian varieties (2016). In Preparation
10. O'Meara, O.T.: Symplectic Groups, Mathematical Surveys, vol. 16. American Mathematical Society, Providence (1978)

11. Serre, J.P.: Abelian ℓ-adic representations and elliptic curves, *Research Notes in Mathematics*, vol. 7. A K Peters, Ltd., Wellesley, MA (1998). With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original
12. Vasiu, A.: Surjectivity criteria for p-adic representations. I. Manuscripta Math. **112**(3), 325–355 (2003). doi:10.1007/s00229-003-0402-4
13. Wallace, E.: Principally polarized abelian surfaces with surjective Galois representations on l-torsion. J. Lond. Math. Soc. **90**(2), 451–471 (2014). doi:10.1112/jlms/jdu033
14. Weigel, T.: On the profinite completion of arithmetic groups of split type. Lois d'algèbres et variétés algébriques (Colmar, 1991), Travaux en Cours, vol. 50, pp. 79–101. Hermann (1996)
15. Zywina, D.: An explicit Jacobian of dimension 3 with maximal Galois action. ArXiv e-prints (2015)