PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY, SERIES B
Volume 9, Pages 272–285 (May 27, 2022)
https://doi.org/10.1090/bproc/131

A BOUND FOR THE IMAGE CONDUCTOR OF A PRINCIPALLY POLARIZED ABELIAN VARIETY WITH OPEN GALOIS IMAGE

JACOB MAYLE

(Communicated by Rachel Pries)

Abstract. Let A be a principally polarized abelian variety of dimension g over a number field K. Assume that the image of the adelic Galois representation of A is an open subgroup of $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$. Then there exists a positive integer m so that the Galois image of A is the full preimage of its reduction modulo m. The least m with this property, denoted m_A, is called the *image conductor* of A. Jones [Pacific J. Math. 308 (2020), pp. 307–331] recently established an upper bound for m_A, in terms of standard invariants of A, in the case that A is an elliptic curve without complex multiplication. In this paper, we generalize the aforementioned result to provide an analogous bound in arbitrary dimension.

1. Introduction

Let A be a principally polarized abelian variety of dimension g over a number field K. Let $T(A) := \varprojlim A[m]$ denote the adelic Tate module of A. The *adelic Galois representation* of A is a continuous homomorphism of profinite groups

$$\rho_A : G_K \to \mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$$

that encodes the action of $G_K := \mathrm{Gal}(\overline{K}/K)$ on $T(A)$.

The image of ρ_A is called the *Galois image* of A and, in many cases, is known to be an open subgroup of $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$. For instance, Serre established that this is so for elliptic curves without complex multiplication in his celebrated 1972 open image theorem [11]. Serre later generalized his result to certain higher dimensions.

Theorem 1.1 (Serre, 1986 [13])**.** *Let A be a principally polarized abelian variety of dimension g over a number field K. If $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$ and $g = 2, 6$, or is odd, then $\rho_A(G_K) \subseteq \mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$ is an open subgroup.*

Due to an example of Mumford [8, §4], it is known that the above result does not generalize to arbitrary dimension without further hypotheses. In 2011 [2], Hall gave a *sufficient* condition for a principally polarized abelian variety of arbitrary dimension to have open Galois image. Kowalski proved, as a consequence, that almost all Jacobians of hyperelliptic curves (in a suitable sense) have open Galois image [2, Appendix].

Assume that A has open Galois image. For each positive integer m, we let

$$\bar{\pi}_m : \mathrm{GSp}_{2g}(\hat{\mathbb{Z}}) \twoheadrightarrow \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$$

Received by the editors May 19, 2020, and, in revised form, January 23, 2022.
2020 *Mathematics Subject Classification.* Primary 11G10.

be the natural projection map. The collection $\{\ker \bar{\pi}_m\}_{m=1}^{\infty}$ is a neighborhood basis for the identity of $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$. Since $\rho_A(G_K) \subseteq \mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$ is an open subgroup, there exists an m so that $\ker \bar{\pi}_m \subseteq \rho_A(G_K)$. The least m with this property is the *image conductor* of A, and is denoted by m_A. An important observation is that the Galois image of A is the full preimage of the finite group $\bar{\pi}_{m_A}(\rho_A(G_K))$, as we shall discuss in §2.3.

In a recent paper [3], Jones established an upper bound for m_A, in terms of standard invariants of A, in the case that A is an elliptic curve without complex multiplication. Further, he remarked that his techniques should be able to be extended to prove an analogous result for principally polarized abelian varieties of arbitrary dimension. In this paper, we do precisely that, proving Theorem 1.2.

Theorem 1.2. *Let A be a principally polarized abelian variety of dimension g over a number field K and assume that the image of the adelic Galois representation $\rho_A : G_K \to \mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$ is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$. Then*

$$m_A \leq 2 \cdot \mathcal{B}_A \cdot \Big[\mathrm{GSp}_{2g}(\hat{\mathbb{Z}}) : \rho_A(G_K)\Big],$$

where m_A denotes the image conductor of A and $\mathcal{B}_A$ is the square-free constant, depending on A, that is defined to be the product of each prime number $\ell \in \mathbb{N}$ that satisfies at least one of the following conditions:

1. *$K/\mathbb{Q}$ is ramified at ℓ;*
2. *A has bad reduction at some prime ideal of $\mathcal{O}_K$ that lies over ℓ; or*
3. *$\ell = 2$, in the case that $g = 2$.*

Remark 1.3. We now consider sharpness of the bound in Theorem 1.2 when $g = 2$. Let A be the Jacobian of a genus 2 curve $C/\mathbb{Q}$. Let Δ denote the discriminant of C. Write Δ_{sf} to denote the square-free part of Δ. It follows similarly as in the case of elliptic curves [1, §2.4] that

$$\rho_A(G_{\mathbb{Q}}) \subseteq \Big\{\gamma \in \mathrm{GSp}_4(\hat{\mathbb{Z}}) : \epsilon(\gamma) = \chi_A(\gamma)\Big\} \tag{1.1}$$

where ϵ and χ_A are defined as follows: The character ϵ is the map

$$\epsilon : \mathrm{GSp}_4(\hat{\mathbb{Z}}) \to \mathrm{GSp}_4(\mathbb{Z}/2\mathbb{Z}) \xrightarrow{\sim} S_6 \to \{\pm 1\}$$

given by projection modulo 2, followed by the signature character on the symmetric group S_6. For the character χ_A, first define the constant

$$d_A = \begin{cases} \Delta_{\mathrm{sf}} & \Delta_{\mathrm{sf}} \equiv 1 \pmod 4, \\ 4\Delta_{\mathrm{sf}} & \text{otherwise.} \end{cases}$$

Now χ_A is the map

$$\chi_A : \mathrm{GSp}_4(\hat{\mathbb{Z}}) \to \hat{\mathbb{Z}}^{\times} \to (\mathbb{Z}/\left|d_A\right|\mathbb{Z})^{\times} \to \{\pm 1\}$$

given by the multiplier map, followed by reduction modulo $|d_A|$, followed by the kronecker symbol $\left(\frac{d_A}{\cdot}\right)$.

Assume that A has the property that

$$[\mathrm{GSp}_4(\hat{\mathbb{Z}}) : \rho_A(G_{\mathbb{Q}})] = 2. \tag{1.2}$$

Then the inclusion in (1.1) is an equality. As in the case for Serre curves [1, Proposition 17], it then follows that the image conductor for A is given by

$$m_A = \operatorname{lcm}(2, |d_A|) = \begin{cases} 2\,|\Delta_{\mathrm{sf}}| & \Delta_{\mathrm{sf}} \equiv 1 \pmod 4, \\ 4\,|\Delta_{\mathrm{sf}}| & \text{otherwise.} \end{cases}$$

Thus if A satisfies (1.2), the primes of bad reduction for A and C coincide and include 2, and the discriminant Δ is square-free and congruent to 1 modulo 4, then Theorem 1.2 is sharp for A. The author is not aware of any such abelian surface in the literature, though an example satisfying (1.2) is given in [5, Theorem 1.2].

Remark 1.4. The third condition in Theorem 1.2 is rather unnatural. This assumption on $\mathcal{B}_A$ is used in the proof of Lemma 6.4, and arises from the failure of a relevant lifting result in the case when $\ell = 2$ and $g = 2$. A careful analysis of $\mathrm{GSp}_4(\mathbb{Z}/8\mathbb{Z})$ could perhaps lead to a refined condition (cf. [3, pp. 13-14]).

Remark 1.5. The constant $\mathcal{B}_A$ is constructed in view of Corollary 6.2. Given this, it seems that one should be able write Theorem 1.2 in terms of an arbitrary family of G_K-modules $\{M[n]\}_{n\geq 1}$ of $A(\overline{K})$ that satisfy the conclusion of Corollary 6.2.

2. Notation and preliminaries

2.1. **Symplectic groups.** Let R be a commutative ring with unity and let M be a free R-module of rank $2g$. A map $\langle\cdot,\cdot\rangle : M \oplus M \to R$ is called a *symplectic form* on M if it is bilinear, non-degenerate, and alternating. Given a symplectic form $\langle\cdot,\cdot\rangle$ on M, the *general symplectic group* and *symplectic group* of $(M, \langle\cdot,\cdot\rangle)$ are

$$\begin{aligned} \mathrm{GSp}(M, \langle\cdot,\cdot\rangle) &:= \big\{\gamma \in \mathrm{GL}(M) : \exists m(\gamma) \in R^\times \ \forall v, w \in M \ \langle\gamma v, \gamma w\rangle = m(\gamma)\langle v, w\rangle\big\}, \\ \mathrm{Sp}(M, \langle\cdot,\cdot\rangle) &:= \{\gamma \in \mathrm{GL}(M) : \forall v, w \in M \ \langle\gamma v, \gamma w\rangle = \langle v, w\rangle\}. \end{aligned}$$

We may choose an R-basis for M under which the symplectic form $\langle\cdot,\cdot\rangle$ is represented by the block matrix

$$\Omega_{2g} = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix},$$

where $I_g \in \mathrm{Mat}_{2g\times 2g}(R)$ denotes the $g \times g$ identity matrix. Let $\mu : \mathrm{GL}(M) \xrightarrow{\sim} \mathrm{GL}_{2g}(R)$ be the isomorphism induced by our choice of basis. The images of $\mathrm{GSp}(M, \langle\cdot,\cdot\rangle)$ and $\mathrm{Sp}(M, \langle\cdot,\cdot\rangle)$ under μ are, respectively,

$$\begin{aligned} \mathrm{GSp}_{2g}(R) &:= \big\{\gamma \in \mathrm{GL}_{2g}(R) : \exists m(\gamma) \in R^\times \text{ so that } \gamma^{\intercal}\Omega_{2g}\gamma = m(\gamma)\Omega_{2g}\big\}, \\ \mathrm{Sp}_{2g}(R) &:= \{\gamma \in \mathrm{GL}_{2g}(R) : \gamma^{\intercal}\Omega_{2g}\gamma = \Omega_{2g}\}. \end{aligned}$$

The map $\mathrm{mult} : \mathrm{GSp}_{2g}(R) \twoheadrightarrow R^\times$ defined by $\gamma \mapsto m(\gamma)$ is a surjective homomorphism [9, p. 50] and we see that

$$\mathrm{Sp}_{2g}(R) = \ker\Big(\mathrm{GSp}_{2g}(R) \xrightarrow{\mathrm{mult}} R^\times\Big).$$

The orders of $\mathrm{Sp}_{2g}(R)$ and $\mathrm{GSp}_{2g}(R)$ are, in the important case of $R = \mathbb{F}_\ell$, given [9, Theorem 3.1.2] by

$$\big|\mathrm{Sp}_{2g}(\mathbb{F}_\ell)\big| = \ell^{g^2}\prod_{i=1}^{g}(\ell^{2i} - 1) \quad \text{and} \quad \big|\mathrm{GSp}_{2g}(\mathbb{F}_\ell)\big| = (\ell - 1)\ell^{g^2}\prod_{i=1}^{g}(\ell^{2i} - 1). \tag{2.1}$$

2.2. **Notation.** Throughout this paper, p and ℓ denote prime numbers; m and n denote positive integers.

Let $\hat{\mathbb{Z}}$ denote the ring of profinite integers and $\mathbb{Z}_\ell$ denote the ring of ℓ-adic integers. The Chinese remainder theorem gives an isomorphism $\hat{\mathbb{Z}} \xrightarrow{\sim} \prod_\ell \mathbb{Z}_\ell$. The ring of n-adic integers $\mathbb{Z}_n$ and the ring of (n)-adic integers $\mathbb{Z}_{(n)}$ are, respectively, the quotients of $\hat{\mathbb{Z}}$ that correspond with $\mathbb{Z}_n \cong \prod_{\ell|n} \mathbb{Z}_\ell$ and $\mathbb{Z}_{(n)} \cong \prod_{\ell\nmid n} \mathbb{Z}_\ell$.

We see that $\hat{\mathbb{Z}} \cong \mathbb{Z}_n \times \mathbb{Z}_{(n)}$, and hence

$$\mathrm{GSp}_{2g}(\hat{\mathbb{Z}}) \cong \mathrm{GSp}_{2g}(\mathbb{Z}_n) \times \mathrm{GSp}_{2g}(\mathbb{Z}_{(n)}). \tag{2.2}$$

Let $\mathrm{rad}(m) := \prod_{\ell|m} \ell$ denote the radical of m. With (2.2) in mind, we define the following projection maps

$$\begin{aligned}
\pi_n &: \mathrm{GSp}_{2g}(\hat{\mathbb{Z}}) \to \mathrm{GSp}_{2g}(\mathbb{Z}_n) \\
\pi_{(n)} &: \mathrm{GSp}_{2g}(\hat{\mathbb{Z}}) \to \mathrm{GSp}_{2g}(\mathbb{Z}_{(n)}) \\
\pi_{n^\infty,m} &: \mathrm{GSp}_{2g}(\mathbb{Z}_n) \to \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z}) && \text{(provided } \mathrm{rad}(m) \mid n) \\
\bar{\pi}_n &: \mathrm{GSp}_{2g}(\hat{\mathbb{Z}}) \to \mathrm{GSp}_{2g}(\mathbb{Z}/n\mathbb{Z}) \\
\pi_{n,m} &: \mathrm{GSp}_{2g}(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z}) && \text{(provided } m \mid n).
\end{aligned}$$

For a closed subgroup $G \subseteq \mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$, we employ the following notation

$$G_n := \pi_n(G), \qquad G_{(n)} := \pi_{(n)}(G), \text{ and} \qquad G(n) := \bar{\pi}_n(G).$$

Because Theorem 1.2 is known [3] for $g = 1$, in order to simplify our exposition, g will always denote an integer that is at least two, unless otherwise stated. We shall often use the abbreviation ℓ_g, which denotes

$$\ell_g := \begin{cases} 3 & g = 2 \\ 2 & g \geq 3 \end{cases}. \tag{2.3}$$

2.3. **Conductor.** Let $G \subseteq \mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$ be any open subgroup. Then $\{\ker \bar{\pi}_m\}_{m=1}^\infty$ is a neighborhood basis for the identity of $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$. Hence, there exists an m for which $\ker \bar{\pi}_m \subseteq G$. The *conductor* of G is

$$m_G := \min\{m \in \mathbb{N} : \ker \bar{\pi}_m \subseteq G\}. \tag{2.4}$$

It is sometimes helpful to understand the conductor in the ways described in Lemmas 2.1 and 2.2.

Lemma 2.1. *We have that $G = \bar{\pi}_m^{-1}(G(m))$ if and only if $\ker \bar{\pi}_m \subseteq G$. Consequently,*

$$m_G = \min\left\{m \in \mathbb{N} : G = \bar{\pi}_m^{-1}(G(m))\right\}.$$

Proof. We have $G \subseteq \bar{\pi}_m^{-1}(G(m))$, and both of these groups surject onto $G(m)$ via $\bar{\pi}_m$. Further, we see that

$$\ker\left(\bar{\pi}_m^{-1}(G(m)) \xrightarrow{\bar{\pi}_m} G(m)\right) = \ker \bar{\pi}_m \quad \text{and} \quad \ker\left(G \xrightarrow{\bar{\pi}_m} G(m)\right) = G \cap \ker \bar{\pi}_m.$$

Thus, $G = \bar{\pi}_m^{-1}(G(m))$ if and only if $\ker \bar{\pi}_m = G \cap \ker \bar{\pi}_m$, which happens if and only if $\ker \bar{\pi}_m \subseteq G$. □

For Lemma 2.2, we give some terminology (see, [7, I §1.1]). We say that m *splits* G if

$$(\pi_m \times \pi_{(m)})(G) = G_m \times \mathrm{GSp}_{2g}(\mathbb{Z}_{(m)}).$$

We say that m is *stable* for G if

$$G_m = \pi_{m^\infty,m}^{-1}(G(m)).$$

Lemma 2.2. *We have that $G = \bar{\pi}_m^{-1}(G(m))$ if and only if m splits and is stable for G. Consequently,*

$$m_G = \min\{m \in \mathbb{N} : m \text{ splits and is stable for } G\}.$$

Proof. The map $\pi_m \times \pi_{(m)} : \mathrm{GSp}_{2g}(\hat{\mathbb{Z}}) \to \mathrm{GSp}_{2g}(\mathbb{Z}_m) \times \mathrm{GSp}_{2g}(\mathbb{Z}_{(m)})$ is an isomorphism. We see that

$$(\pi_m \times \pi_{(m)})(\bar{\pi}_m^{-1}(G(m))) = \pi_{m^\infty,m}^{-1}(G(m)) \times \mathrm{GSp}_{2g}(\mathbb{Z}_{(m)}).$$

Thus $G = \bar{\pi}_m^{-1}(G(m))$ if and only if m splits and is stable for G. The conclusion follows from Lemma 2.1. □

2.4. **Galois representations.** Let A be a principally polarized abelian variety of dimension g over a number field K. Let $T(A) := \varprojlim A[m]$ be the adelic Tate module of A. Recall that $T(A)$ is a free $\hat{\mathbb{Z}}$-module of rank $2g$. The Weil pairing and a choice of principal polarization on A yield a symplectic form $\langle \cdot, \cdot \rangle : T(A) \oplus T(A) \to \hat{\mathbb{Z}}^\times$. The continuous action of G_K on $T(A)$ is compatible with this symplectic form and hence induces a representation $G_K \to \mathrm{GSp}(T(A), \langle \cdot, \cdot \rangle)$. With a choice of basis, we obtain the continuous homomorphism of profinite groups

$$\rho_A : G_K \to \mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$$

known as the *adelic Galois representation of A*. The *Galois image* of A is the subgroup $G := \rho_A(G_K)$ of $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$. If G is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$, the *image conductor* of A is defined to be the conductor of G as in (2.4).

Remark 2.3. Below are three key observations relating to the Galois image G of A.

(1) We see that G is a closed subgroup of the profinite group $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$. A consequence is that G is an open subgroup of $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$ if and only if the group index $[\mathrm{GSp}_{2g}(\hat{\mathbb{Z}}) : G]$ is finite.

(2) For a subset $S \subseteq A(\overline{K})$, let $K(S)$ be the extension of K obtained by adjoining to K the coordinates of the points in S. Let $A[n]$ be the n-torsion subgroup of $A(\overline{K})$, $A[n^\infty] := \bigcup_{k=0}^{\infty} A[n^k]$, and $A_{\mathrm{tors}} := \cup_{n=1}^{\infty} A[n]$. We have

$$G \cong \mathrm{Gal}(K(A_{\mathrm{tors}})/K)$$
$$G_n \cong \mathrm{Gal}(K(A[n^\infty])/K)$$
$$G(n) \cong \mathrm{Gal}(K(A[n])/K).$$

Further, let $A_{\mathrm{tors},(n)} := \bigcup_{\gcd(m,n)=1} A[m]$. We have that

$$G_{(n)} \cong \mathrm{Gal}(K(A_{\mathrm{tors},(n)})/K).$$

(3) Let μ_n be the group of nth roots of unity in $\overline{K}$. Let $\mu_{\ell^\infty} := \bigcup_k \mu(\ell^k)$ and $\mu_\infty := \bigcup_n \mu(n)$. The composition $\mathrm{mult} \circ \rho_A : G_K \to \mathrm{GSp}_{2g}(\hat{\mathbb{Z}}) \to \hat{\mathbb{Z}}^\times$ is the cyclotomic character of K. Thus,

$$\mathrm{mult}(G) \cong \mathrm{Gal}(K(\mu_\infty)/K)$$
$$\mathrm{mult}(G_\ell) \cong \mathrm{Gal}(K(\mu_{\ell^\infty})/K)$$
$$\mathrm{mult}(G(n)) \cong \mathrm{Gal}(K(\mu_n)/K).$$

We now give a generalization of a variant of [12, IV-18 Lemma (2)].

Lemma 2.4. *As before, let $G := \rho_A(G_K)$. If ℓ is such that $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell) \subseteq G_\ell$, then $G_\ell = \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ if and only if $K \cap \mathbb{Q}(\mu_{\ell^\infty}) = \mathbb{Q}$. In particular, if $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell) \subseteq G_\ell \neq \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$, then $K/\mathbb{Q}$ is ramified at ℓ.*

Proof. Since $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell) \subseteq G_\ell$, both $\mathrm{mult} : \mathrm{GSp}_{2g}(\mathbb{Z}_\ell) \twoheadrightarrow \mathbb{Z}_\ell^\times$ and the restriction $\mathrm{mult}|_{G_\ell} : G_\ell \to \mathbb{Z}_\ell^\times$ have kernel $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$. Therefore, $G_\ell = \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ if and only if $\mathrm{mult}(G_\ell) = \mathbb{Z}_\ell^\times$. By Remark 2.3(3) and Galois theory,

$$\mathrm{mult}(G_\ell) \cong \mathrm{Gal}(K(\mu_{\ell^\infty})/K) \cong \mathrm{Gal}(\mathbb{Q}(\mu_{\ell^\infty})/(K \cap \mathbb{Q}(\mu_{\ell^\infty}))) \subseteq \mathrm{Gal}(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q}) \cong \mathbb{Z}_\ell^\times.$$

It follows that $\mathrm{mult}(G_\ell) = \mathbb{Z}_\ell^\times$ if and only if the extension $K \cap \mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q}$ is nontrivial.

Now assume $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell) \subseteq G_\ell \neq \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$. By the above, the extension $K \cap \mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q}$ is nontrivial. Thus, this extension is ramified at ℓ as it is a sub-extension of $\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q}$, which is well-known to be totally ramified at ℓ. Thus, $K/\mathbb{Q}$ is ramified at ℓ because it has a ramified sub-extension. □

2.5. **Fiber product.** Let G_1, G_2, and Q be groups. Let $\psi_1 : G_1 \twoheadrightarrow Q$ and $\psi_2 : G_2 \twoheadrightarrow Q$ be surjective homomorphisms. The *fiber product* of G_1 and G_2 over (ψ_1, ψ_2) is the group

$$G_1 \times_{(\psi_1,\psi_2)} G_2 := \{(g_1, g_2) \in G_1 \times G_2 : \psi_1(g_1) = \psi_2(g_2)\}.$$

Observe that $G_1 \times_{(\psi_1,\psi_2)} G_2 \subseteq G_1 \times G_2$ is a subgroup that surjects onto both G_1 and G_2 via the relevant projection maps. Writing $\psi = (\psi_1, \psi_2)$, we say that a fiber product $G_1 \times_\psi G_2$ is *trivial* if $G_1 \times_\psi G_2 = G_1 \times G_2$.

Let L_1/K and L_2/K be Galois extensions, both contained in $\overline{K}$. The *entanglement field* of L_1 and L_2 is the intersection $L_1 \cap L_2$. The *compositum* of L_1 and L_2, denoted L_1L_2, is the smallest (by inclusion) subfield of $\overline{K}$ containing both L_1 and L_2. The Galois group of L_1L_2/K may be described using the fiber product.

Lemma 2.5. *Let L_1/K and L_2/K be Galois extensions, contained in $\overline{K}$. Then L_1L_2/K is Galois and*

$$\mathrm{Gal}(L_1L_2/K) \cong \mathrm{Gal}(L_1/K) \times_{(\psi_1,\psi_2)} \mathrm{Gal}(L_2/K),$$

where each $\psi_i : \mathrm{Gal}(L_i/K) \twoheadrightarrow \mathrm{Gal}(L_1 \cap L_2/K)$ is the canonical restriction homomorphism.

Proof. See [6, Theorem VI 1.14]. □

3. Symplectic groups

In §2.1, we introduced the symplectic groups $\mathrm{GSp}_{2g}(R)$ and $\mathrm{Sp}_{2g}(R)$. In this section, we derive some useful properties of these groups when $R = \mathbb{F}_\ell$ and $R = \mathbb{Z}_\ell$.

3.1. **Normal subgroups.** The objective of this subsection is to understand the normal subgroups of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ for $\ell \geq \ell_g$, where ℓ_g is as in (2.3). We begin by considering the projective symplectic groups.

The center of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ is the scalar subgroup $\Lambda_{2g}(\mathbb{F}_\ell)$ of $\mathrm{GL}_{2g}(\mathbb{F}_\ell)$ [9, 4.2.5(5)]. Let π be the projection

$$\pi : \mathrm{GSp}_{2g}(\mathbb{F}_\ell) \twoheadrightarrow \mathrm{GSp}_{2g}(\mathbb{F}_\ell)/\Lambda_{2g}(\mathbb{F}_\ell).$$

The *projective general symplectic group* $\mathrm{PGSp}_{2g}(\mathbb{F}_\ell)$ and *projective symplectic group* $\mathrm{PSp}_{2g}(\mathbb{F}_\ell)$ are the images of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ and $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ under π, respectively. We give some useful properties of these groups below. Here and later, we let $[\cdot,\cdot]$ denote a commutator and write G' to denote the commutator subgroup of a group G.

Lemma 3.1. *Assume $\ell \geq \ell_g$. Each of the following statements hold.*

(1) *The center of $\mathrm{PGSp}_{2g}(\mathbb{F}_\ell)$ is trivial;*
(2) $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)' = \mathrm{Sp}_{2g}(\mathbb{F}_\ell)' = \mathrm{Sp}_{2g}(\mathbb{F}_\ell)$*;*
(3) $\mathrm{PGSp}_{2g}(\mathbb{F}_\ell)' = \mathrm{PSp}_{2g}(\mathbb{F}_\ell)$*; and*
(4) $\mathrm{PSp}_{2g}(\mathbb{F}_\ell)$ *is simple.*

Proof. Statements (1), (2), and (4) are found in [9, 4.2.5(2), 3.3.6, 3.4.1]. For (3), we apply (2) to see that

$$\mathrm{PGSp}_{2g}(\mathbb{F}_\ell)' = \big(\pi(\mathrm{GSp}_{2g}(\mathbb{F}_\ell))\big)' = \pi(\mathrm{GSp}_{2g}(\mathbb{F}_\ell)') = \pi(\mathrm{Sp}_{2g}(\mathbb{F}_\ell)) = \mathrm{PSp}_{2g}(\mathbb{F}_\ell). \quad \square$$

Using the properties of Lemma 3.1, we now determine the normal subgroups of $\mathrm{PGSp}_{2g}(\mathbb{F}_\ell)$. Our target lemma regarding the normal subgroups of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ then follows. We make the abbreviation $\Lambda_{2g} := \Lambda_{2g}(\mathbb{F}_\ell)$.

Lemma 3.2. *Assume that $\ell \geq \ell_g$. If $N \trianglelefteq \mathrm{PGSp}_{2g}(\mathbb{F}_\ell)$, then either $N = \{\Lambda_{2g}\}$ or $\mathrm{PSp}_{2g}(\mathbb{F}_\ell) \subseteq N$.*

Proof. Assume that $N \trianglelefteq \mathrm{PGSp}_{2g}(\mathbb{F}_\ell)$ is nontrivial. Since the center of $\mathrm{PGSp}_{2g}(\mathbb{F}_\ell)$ is trivial, we have

$$\{\Lambda_{2g}\} \subsetneq [\mathrm{PGSp}_{2g}(\mathbb{F}_\ell), N] \subseteq N \cap \mathrm{PGSp}_{2g}(\mathbb{F}_\ell)' = N \cap \mathrm{PSp}_{2g}(\mathbb{F}_\ell) \trianglelefteq \mathrm{PSp}_{2g}(\mathbb{F}_\ell).$$

By the simplicity of $\mathrm{PSp}_{2g}(\mathbb{F}_\ell)$, this implies that $N \cap \mathrm{PSp}_{2g}(\mathbb{F}_\ell) = \mathrm{PSp}_{2g}(\mathbb{F}_\ell)$. Thus, $\mathrm{PSp}_{2g}(\mathbb{F}_\ell) \subseteq N$. $\square$

Lemma 3.3. *Assume that $\ell \geq \ell_g$. If $N \trianglelefteq \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$, then either $N \subseteq \Lambda_{2g}$ or $\mathrm{Sp}_{2g}(\mathbb{F}_\ell) \subseteq N$.*

Proof. Assume that $N \not\subseteq \Lambda_{2g}$. Then $\pi(N) \trianglelefteq \mathrm{PGSp}_{2g}(\mathbb{F}_\ell)$ is nontrivial. So, by Lemma 3.2, $\mathrm{PSp}_{2g}(\mathbb{F}_\ell) \subseteq \pi(N)$ and hence $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)\Lambda_{2g} \subseteq N\Lambda_{2g}$. By taking commutators, we now see that

$$N \supseteq N' = (N\Lambda_{2g})' \supseteq (\mathrm{Sp}_{2g}(\mathbb{F}_\ell)\Lambda_{2g})' = (\mathrm{Sp}_{2g}(\mathbb{F}_\ell))' = \mathrm{Sp}_{2g}(\mathbb{F}_\ell). \qquad \square$$

3.2. **Index bound.** Here we use Lemma 3.3 and a standard lemma from group theory to obtain a lower bound on the index of each subgroup of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ that does not contain $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$. We write $n!$ to denote the factorial of n.

Lemma 3.4. *Let G be a finite group and $H \subseteq G$ a subgroup. The normal core of H in G, denoted H_G, is the largest (by inclusion) subgroup of H that is normal in G. One has that $[G : H_G]$ divides $[G : H]!$.*

Proof. See [10, 1.6.9]. $\square$

Lemma 3.5. *Let $G \subseteq \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ be a subgroup. If $\mathrm{Sp}_{2g}(\mathbb{F}_\ell) \not\subseteq G$, then*

$$\left[\mathrm{GSp}_{2g}(\mathbb{F}_\ell) : G\right] \geq \ell.$$

Proof. The result is clear for $\ell = 2$, so we assume that $\ell \geq 3$. Let N be the normal core of G in $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$. Then $N \trianglelefteq \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ and $\mathrm{Sp}_{2g}(\mathbb{F}_\ell) \not\subseteq N$, so $N \subseteq \Lambda_{2g}(\mathbb{F}_\ell)$, by Lemma 3.3. Now, by (2.1) and Lemma 3.4,

$$\ell \quad \text{divides} \quad \left|\mathrm{PGSp}_{2g}(\mathbb{F}_\ell)\right| \quad \text{divides} \quad [\mathrm{GSp}_{2g}(\mathbb{F}_\ell) : N] \quad \text{divides} \quad [\mathrm{GSp}_{2g}(\mathbb{F}_\ell) : G]!.$$

□

3.3. **Subgroup lifting.** We state a lifting lemma for $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ that extends [12, IV-23 Lemma 3]. Then, we give two corollaries and state a lifting lemma $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$. As before, we shall assume that $g \geq 2$.

Proposition 3.6. *Let $H_\ell \subseteq \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ be a closed subgroup. If $H(\ell) = \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$, then $H_\ell = \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$.*

Proof. See [4, Theorem 1]. □

For a subgroup $H \subseteq G_\ell$, we let $\overline{H}$ denote the topological closure of H in G_ℓ.

Corollary 3.7. *Assume that $\ell \geq \ell_g$ and let $G_\ell \subseteq \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ be a closed subgroup. If $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) \subseteq G(\ell)$, then $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell) \subseteq G_\ell$.*

Proof. We have that $\overline{(G_\ell)'} \subseteq \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ is a closed subgroup. Further, as G_ℓ surjects onto $G(\ell)$, we have

$$(G_\ell)'(\ell) = (G(\ell))' = \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}),$$

by Lemma 3.1(2). Thus, $\overline{(G_\ell)'}(\ell) = \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$. So, by Proposition 3.6, $G_\ell \supseteq \overline{(G_\ell)'} = \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$. □

Corollary 3.8. *Assume that $\ell \geq 3$ and let $N_\ell \trianglelefteq \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ be a closed normal subgroup. If $\mathrm{mult}(N_\ell) = \mathbb{Z}_\ell^\times$, then $N_\ell = \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$.*

Proof. Since $\mathrm{mult}(N(\ell)) = (\mathbb{Z}/\ell\mathbb{Z})^\times$ and $\mathrm{mult}(\Lambda_{2g}(\mathbb{F}_\ell)) = (\mathbb{Z}/\ell\mathbb{Z})^{\times 2}$, we have $N(\ell) \not\subseteq \Lambda_{2g}(\mathbb{F}_\ell)$. Hence, $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) \subseteq N(\ell)$ by Lemma 3.3. Thus, by Corollary 3.7, we find that $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell) \subseteq N_\ell$. As both $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ and N_ℓ surject onto $\mathbb{Z}_\ell^\times$, via mult, with kernel $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$, we conclude that $N_\ell = \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$. □

We now state a lifting lemma for $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$. Let α_ℓ denote the quantity

$$\alpha_\ell := \begin{cases} 2 & \text{if } \ell = 2 \\ 1 & \text{if } \ell \geq 3 \end{cases}. \tag{3.1}$$

Lemma 3.9. *Let $G_\ell \subseteq \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ be a closed subgroup. We have that if $G(\ell^{\alpha_\ell+1}) = \mathrm{GSp}_{2g}(\mathbb{Z}/\ell^{\alpha_\ell+1}\mathbb{Z})$, then $G_\ell = \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$.*

Proof. See [3, Remark 3.2], the proof of which generalizes directly to arbitrary g, mutatis mutandis. □

4. Proof of Theorem 1.2, assuming two propositions

We begin by stating two propositions, which we shall prove in §5 and §7. The first proposition is purely group-theoretic, whereas the second depends on the arithmetic of the abelian variety A. Due to group-theoretic differences relating to the prime 2 (visible in the statement of Lemma 3.9), we employ a variant of the radical function. This modified radical is denoted rad' and is defined by

$$\mathrm{rad}'(n) := \begin{cases} 2\,\mathrm{rad}(n) & 4 \mid n \\ \mathrm{rad}(n) & \text{otherwise,} \end{cases}$$

where $\mathrm{rad}(n) = \prod_{\ell \mid n} \ell$ is the usual radical of n. Our main propositions are as follows.

Proposition 4.1. *Let g be an integer, $G \subseteq \mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$ be an open subgroup, and m_G be as in* (2.4)*. Then*

$$\frac{m_G}{\mathrm{rad}'(m_G)} \text{ divides } \left[\pi^{-1}_{m_G,\mathrm{rad}'(m_G)}(G(\mathrm{rad}'(m_G))) : G(m_G)\right].$$

Proposition 4.2. *Let $g \geq 2$ be an integer and let A be as in the statement of Theorem* 1.2*. Then*

$$\mathrm{rad}'(m_A) \leq 2 \cdot \mathcal{B}_A \cdot \left[\mathrm{GSp}_{2g}(\mathbb{Z}/\,\mathrm{rad}'(m_A)\mathbb{Z}) : G(\mathrm{rad}'(m_A))\right],$$

where G is the Galois image of A, m_A is the image conductor of A, and $\mathcal{B}_A$ is as in Theorem 1.2*.*

We now prove Theorem 1.2, assuming Proposition 4.1 and Proposition 4.2.

Proof of Theorem 1.2. Write $G := \rho_A(G_K)$ and $r' := \mathrm{rad}'(m_A)$. Using Lemma 2.1 initially, we see

$$\begin{aligned}
[\mathrm{GSp}_{2g}(\hat{\mathbb{Z}}) : G] &= [\mathrm{GSp}_{2g}(\hat{\mathbb{Z}}) : \bar{\pi}^{-1}_{m_A}(G(m_A))] \\
&= [\mathrm{GSp}_{2g}(\mathbb{Z}/m_A\mathbb{Z}) : G(m_A)] \\
&= [\mathrm{GSp}_{2g}(\mathbb{Z}/m_A\mathbb{Z}) : \pi^{-1}_{m_A,r'}(G(r'))][\pi^{-1}_{m_A,r'}(G(r')) : G(m_A)] \\
&= [\mathrm{GSp}_{2g}(\mathbb{Z}/r'\mathbb{Z}) : G(r')][\pi^{-1}_{m_A,r'}(G(r')) : G(m_A)].
\end{aligned}$$

With the above in mind, applying Proposition 4.1 and Proposition 4.2 now yields

$$\begin{aligned}
m_A &= r' \cdot \frac{m_A}{r'} \\
&\leq 2 \cdot \mathcal{B}_A \cdot \left[\mathrm{GSp}_{2g}(\mathbb{Z}/r'\mathbb{Z}) : G(r')\right] \cdot [\pi^{-1}_{m_A,r'}(G(r')) : G(m_A)] \\
&= 2 \cdot \mathcal{B}_A \cdot [\mathrm{GSp}_{2g}(\hat{\mathbb{Z}}) : G].
\end{aligned}$$

□

5. Proof of Proposition 4.1

For the case of $g = 1$, a proof of Proposition 4.1 is given in [3, Proposition 1.6]. This purely group-theoretic proof immediately generalizes, mutatis mutandis, to prove Proposition 4.1 for arbitrary g. For this reason, in this section we shall explain the structure of the proof and refer the reader to [3] for the details.

Let $G \subseteq \mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$ be any open subgroup and write $m_G =: \prod_{\ell \mid m_G} \ell^{\beta_\ell}$ for the prime factorization of its conductor. For each k, write $N_{\ell^k} := \ker(\pi_{\ell^{k+1},\ell^k})$. Using a lifting lemma [3, Lemma 3.1], we may describe [3, Corollary 3.5] each β_ℓ as

$$\beta_\ell = \min\left\{\beta \geq 0 : \forall k \in [\beta, \max\{\beta, \alpha_\ell\}] \cap \mathbb{Z},\ N_{\ell^k} \times \{1_{(\ell)}\} \subseteq (\pi_{\ell^\infty,\ell^{k+1}} \times \pi_{(\ell)})(G)\right\},$$

where α_ℓ is defined in (3.1) and $1_{(\ell)}$ denotes the identity of $\mathrm{GSp}_{2g}(\mathbb{Z}_{(\ell)})$. As a corollary, it follows [3, Lemma 3.8] that if d is a positive integer that satisfies the divisibility condition $\mathrm{rad}'(m_G) \mid d \mid d\ell \mid m_G$, then

$$\ell \quad \text{divides} \quad [\pi^{-1}_{\ell d, d}(G(d)) : G(\ell d)]. \tag{5.1}$$

Write $r' := \mathrm{rad}'(m_G)$. Let ℓ be a prime dividing $\frac{m_G}{r'}$. Let β_ℓ and r_ℓ be such that $\ell^{\beta_\ell} \mid\mid m_G$ and $\ell^{r_\ell} \mid\mid r'$, respectively. Applying (5.1) with $d = \ell^k r'$ for each integer k such that $0 \leq k < \beta_\ell - r_\ell$, we obtain that

$$\begin{aligned} \ell^{\beta_\ell - r_\ell} \quad &\text{divides} \quad \prod_{0 \leq k < \beta_\ell - r_\ell} [\pi^{-1}_{\ell^{k+1} r', \ell^k r'}(G(\ell^k r')) : G(\ell^{k+1} r')] \\ &\text{divides} \quad [\pi^{-1}_{\ell^{\beta_\ell - r_\ell} r', r'}(G(r')) : G(\ell^{\beta_\ell - r_\ell} r')] \\ &\text{divides} \quad [\pi^{-1}_{m_G, r'}(G(r')) : G(m_G)]. \end{aligned}$$

Since the above holds for each prime ℓ dividing $\frac{m_G}{\mathrm{rad}'(m_G)}$, it follows that

$$\frac{m_G}{\mathrm{rad}'(m_G)} = \prod_{\ell \mid \frac{m_G}{r'}} \ell^{\beta_\ell - r_\ell} \quad \text{divides} \quad [\pi^{-1}_{m_G, \mathrm{rad}'(m_G)}(G(\mathrm{rad}'(m_G))) : G(m_G)].$$

6. Constraints on prime divisors of the image conductor

Let A be as in the statement of Theorem 1.2. We give constraints on the primes that divide the image conductor of A. To do so, we employ a variant of the Néron-Ogg-Shafarevich criterion for abelian varieties.

Theorem 6.1 (Serre-Tate, 1968 [14])**.** *Let A be an abelian variety over a number field K. Let $\mathcal{L} \subseteq \mathcal{O}_K$ be a prime ideal of K, lying over a rational prime ℓ. The following are equivalent:*

1. *A has good reduction at $\mathcal{L}$;*
2. *For each positive integer m that is not divisible by ℓ, the prime $\mathcal{L}$ is unramified in $K(A[m])/K$; and*
3. *The prime $\mathcal{L}$ is unramified in $K(A_{\mathrm{tors},(\ell)})/K$, where $A_{\mathrm{tors},(\ell)}$ is defined in Remark* 2.3(2).

Recall that the constant $\mathcal{B}_A$ is defined in the statement of Theorem 1.2.

Corollary 6.2. *Assume that $\ell \geq \ell_g$. Then ℓ divides $\mathcal{B}_A$ if and only if $K(A_{\mathrm{tors},(\ell)})/\mathbb{Q}$ is ramified at ℓ.*

Proof. Since $\ell \geq \ell_g$, we have that ℓ divides $\mathcal{B}_A$ if and only if $K/\mathbb{Q}$ is ramified at ℓ or A has bad reduction at some prime ideal of $\mathcal{O}_K$ that lies over ℓ. By Theorem 6.1, the second condition is equivalent to the condition that $K(A_{\mathrm{tors},(\ell)})/K$ is ramified at some prime ideal of $\mathcal{O}_K$ that lies over ℓ. □

Recall the notation of Remark 2.3(2) and that G denotes the Galois image of A. Lemma 6.3 is key. It uses our understanding of $\mathcal{B}_A$ from Corollary 6.2 to give a constraint on odd primes ℓ that divide m_A for which $G_\ell = \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$.

Lemma 6.3. *Let ℓ be an odd prime that divides m_A. If $G_\ell = \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$, then ℓ divides $\mathcal{B}_A$.*

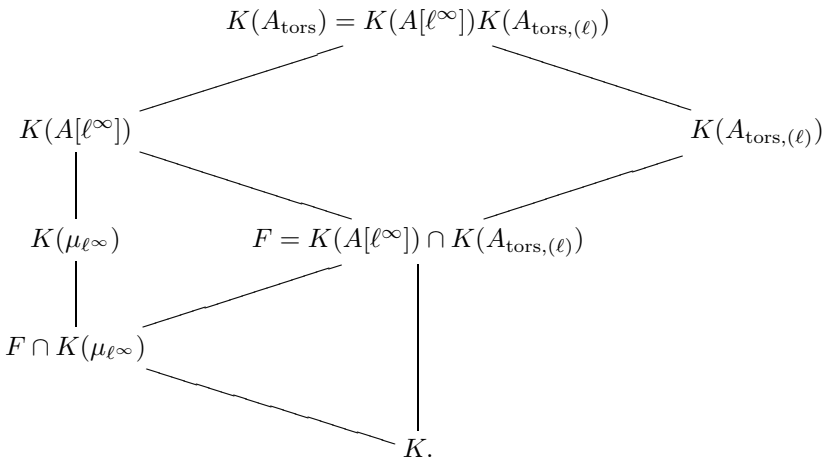
Proof. We see that $m_A \neq \ell$ for otherwise, by Lemma 2.1, we would have that $G = \pi_\ell^{-1}(\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)) = \mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$ and hence $m_A = 1$ is not divisible by ℓ. Thus, as ℓ is stable for G, it follows from Lemma 2.2 that ℓ does not split G. Let F be the entanglement field $F := K(A[\ell^\infty]) \cap K(A_{\mathrm{tors},(\ell)})$. Then, by Lemma 2.5, G may be expressed as the *nontrivial* fiber product

$$G \cong \mathrm{Gal}(K(A[\ell^\infty])K(A_{\mathrm{tors},(\ell)})/K) \cong \mathrm{GSp}_{2g}(\mathbb{Z}_\ell) \times_{(\psi_\ell, \psi_{(\ell)})} \mathrm{Gal}(K(A_{\mathrm{tors},(\ell)})/K),$$

where ψ_ℓ and $\psi_{(\ell)}$ are, upon making the identifications of Remark 2.3(3), the restriction homomorphisms

$$\psi_\ell : \mathrm{GSp}_{2g}(\mathbb{Z}_\ell) \twoheadrightarrow \mathrm{Gal}(F/K) \quad \text{and} \quad \psi_{(\ell)} : \mathrm{Gal}(K(A_{\mathrm{tors},(\ell)})/K) \twoheadrightarrow \mathrm{Gal}(F/K).$$

As the fiber product is nontrivial, in particular $\mathrm{Gal}(F/K)$ is nontrivial. Consider the following field diagram.



If $K/\mathbb{Q}$ is ramified at ℓ, then ℓ divides $\mathcal{B}_A$, so we are done. As such, we assume $K/\mathbb{Q}$ is unramified at ℓ. Note that then $K(\mu_{\ell^\infty})/K$ is totally ramified at each prime ideal of $\mathcal{O}_K$ that lies over ℓ. To show that ℓ divides $\mathcal{B}_A$, it suffices by Corollary 6.2 to show that $K(A_{\mathrm{tors},(\ell)})/K$ is ramified at some prime ideal of $\mathcal{O}_K$ that lies over ℓ. Hence, it suffices merely to show that the extension $F \cap K(\mu_{\ell^\infty})/K$ is nontrivial.

Because ψ_ℓ is a surjective group homomorphism with nontrivial image, its kernel $\ker(\psi_\ell) \triangleleft \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ is proper. Thus, by Corollary 3.8, we have that $\mathrm{mult}(\ker \psi_\ell)$ is a proper subgroup of $\mathbb{Z}_\ell^\times$. So we see,

$$\mathrm{mult}(\langle \ker \psi_\ell, \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)\rangle) = \mathrm{mult}(\ker \psi_\ell) \subsetneq \mathbb{Z}_\ell^\times.$$

Hence $\langle \ker \psi_\ell, \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)\rangle \triangleleft \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ is a proper subgroup. Thus, by Galois theory,

$$\begin{aligned} F \cap K(\mu_{\ell^\infty}) &= K(A[\ell^\infty])^{\ker \psi_\ell} \cap K(A[\ell^\infty])^{\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)} \\ &= K(A[\ell^\infty])^{\langle \ker \psi_\ell, \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)\rangle} \\ &\supsetneq K(A[\ell^\infty])^{\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)} \\ &= K. \end{aligned}$$

We see that the extension $F \cap K(\mu_{\ell^\infty})/K$ is nontrivial, and hence ℓ divides $\mathcal{B}_A$. □

Following Lemma 6.3, which considers a odd prime ℓ, Lemma 6.4 offers a constraint when $\ell = 2$ divides m_A.

Lemma 6.4. *Assume that* 2 *divides* m_A. *Write* $r' := \mathrm{rad}'(m_A)$ *and* $s := \frac{1}{2}r'$. *We have*

$$(\bar{\pi}_2 \times \bar{\pi}_s)(G) \neq \mathrm{GSp}_{2g}(\mathbb{Z}/2\mathbb{Z}) \times G(s) \implies 2 \leq \left[\pi_{r',s}^{-1}(G(s)) : G(r')\right], \tag{6.1}$$

$$(\bar{\pi}_2 \times \bar{\pi}_s)(G) = \mathrm{GSp}_{2g}(\mathbb{Z}/2\mathbb{Z}) \times G(s) \implies 2 \text{ divides } \mathcal{B}_A. \tag{6.2}$$

Proof. Assume first that the hypothesis of (6.1) holds. Then

$$(\pi_{r',2} \times \pi_{r',s})(G(r')) \neq \mathrm{GSp}_{2g}(\mathbb{Z}/2\mathbb{Z}) \times G(s) = (\pi_{r',2} \times \pi_{r',s})(\pi_{r',s}^{-1}(G(s))).$$

Thus $G(r')$ is a proper subgroup of $\pi_{r',s}^{-1}(G(s))$, so the conclusion of (6.1) follows.

Now assume that the hypothesis of (6.2) holds. If $g = 2$, then 2 divides $\mathcal{B}_A$ by definition. As such, we assume $g \geq 3$. By hypothesis, $G(2) = \mathrm{GSp}_{2g}(\mathbb{Z}/2\mathbb{Z})$, so $\mathrm{Sp}_{2g}(\mathbb{Z}_2) \subseteq G_2$ by Corollary 3.7. If $G_2 \neq \mathrm{GSp}_{2g}(\mathbb{Z}_2)$, then by Lemma 2.4, the prime 2 is ramified in $K/\mathbb{Q}$, so 2 divides $\mathcal{B}_A$. Assume, therefore, that $G_2 = \mathrm{GSp}_{2g}(\mathbb{Z}_2)$.

We have that 2 properly divides m_A by Lemma 2.1. Thus, it follows from Lemma 2.2 that

$$G_{r'} \cong (\pi_2 \times \pi_s)(G) = \mathrm{GSp}_{2g}(\mathbb{Z}_2) \times_\psi G_s$$

is a nontrivial fiber product. Observe that each nontrivial finite quotient of $\mathrm{GSp}_{2g}(\mathbb{Z}_2)$ has even order whereas each nontrivial finite quotient of $\ker(\pi_{s^\infty,s})$ has odd order. For this reason, the fiber product

$$(\pi_2 \times \bar{\pi}_s)(G) = \mathrm{GSp}_{2g}(\mathbb{Z}_2) \times_\psi G(s)$$

is nontrivial as well. Making the identifications of Remark 2.3(3), we conclude that the entanglement field $F := K(A[2^\infty]) \cap K(A[s])$ is a nontrivial extension of K.

Consider the Galois group $H := \mathrm{Gal}(K(A_{\mathrm{tors}})/F)$. As F/K is nontrivial, we have that

$$H_2 = \mathrm{Gal}(K(A[2^\infty])/F) \subsetneq \mathrm{Gal}(K(A[2^\infty])/K) = \mathrm{GSp}_{2g}(\mathbb{Z}_2).$$

Further, $H(2) = \mathrm{GSp}_{2g}(\mathbb{Z}/2\mathbb{Z})$ holds by the hypothesis of (6.2). Thus, applying Lemma 2.4 and Corollary 3.7 to A/F, and observing that $H_2 = \mathrm{Gal}(F(A[2^\infty])/F)$, we find that $F/\mathbb{Q}$ is ramified at 2. As F is a subfield of $K(A_{\mathrm{tors},(2)})$, this implies that $K(A_{\mathrm{tors},(2)})/\mathbb{Q}$ is ramified at 2. Thus 2 divides $\mathcal{B}_A$ by Corollary 6.2. □

7. Proof of Proposition 4.2

We apply the constraints of §6 to prove Proposition 4.2. Let A and g be as in the statement of the proposition. Let ℓ be an odd prime that divides m_A. By Lemmas 2.4, 3.5, 6.3 and Corollary 3.7, we know

$$\ell \text{ divides } \mathcal{B}_A \quad \text{or} \quad \ell \leq [\mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) : G(\ell)],$$

depending on whether $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) \subseteq G(\ell)$ or not, respectively. Set $r' := \mathrm{rad}'(m_A)$ and let $r'_{(2)}$ and $\mathcal{B}_{A(2)}$ denote the odd-parts of r' and $\mathcal{B}_A$, respectively (the odd part of an integer n is $\frac{n}{2^k}$ where $2^k \mid\mid n$). Then,

$$\begin{aligned} r'_{(2)} &\leq \prod_{\substack{\text{odd } \ell \mid m_A \\ \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) \subseteq G(\ell)}} \ell \prod_{\substack{\text{odd } \ell \mid m_A \\ \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) \not\subseteq G(\ell)}} [\mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) : G(\ell)] \\ &\leq \mathcal{B}_{A(2)} \cdot \left[\mathrm{GSp}_{2g}(\mathbb{Z}/r'_{(2)}\mathbb{Z}) : G(r'_{(2)})\right]. \end{aligned} \tag{7.1}$$

If $4 \nmid m_A$, then multiplying (7.1) through by 2, we obtain

$$r' \leq 2 \cdot r'_{(2)} \leq 2 \cdot \mathcal{B}_{A(2)} \cdot \Big[\mathrm{GSp}_{2g}(\mathbb{Z}/r'_{(2)}\mathbb{Z}) : G(r'_{(2)}) \Big] \leq 2 \cdot \mathcal{B}_A \cdot \big[\mathrm{GSp}_{2g}(\mathbb{Z}/r'\mathbb{Z}) : G(r') \big].$$

If $4 \mid m_A$, then in particular $2 \mid m_A$, so by Lemma 6.4, we have that

$$2 \cdot [\mathrm{GSp}_{2g}(r'_{(2)}) : G(r'_{(2)})] \leq [\mathrm{GSp}_{2g}(r') : G(r')] \quad \text{or} \quad 2 \cdot \mathcal{B}_{A(2)} = \mathcal{B}_A.$$

With this in mind, multiplying (7.1) through by 4, we find that

$$r' = 4r'_{(2)} \leq 4 \cdot \mathcal{B}_{A(2)} \cdot \Big[\mathrm{GSp}_{2g}(\mathbb{Z}/r'_{(2)}\mathbb{Z}) : G(r'_{(2)}) \Big] \leq 2 \cdot \mathcal{B}_A \cdot \big[\mathrm{GSp}_{2g}(\mathbb{Z}/r'\mathbb{Z}) : G(r') \big].$$

In either case, we see that the bound of Proposition 4.2 holds, completing its proof.

Acknowledgments

The author thanks Nathan Jones for his valuable guidance. The author also thanks the anonymous referees for their comments that served to improve the paper.

References

[1] Renee Bell, Clifford Blakestad, Alina Carmen Cojocaru, Alexander Cowan, Nathan Jones, Vlad Matei, Geoffrey Smith, and Isabel Vogt, *Constants in Titchmarsh divisor problems for elliptic curves*, Res. Number Theory **6** (2020), no. 1, Paper No. 1, 24, DOI 10.1007/s40993-019-0175-9. MR4041152

[2] Chris Hall, *An open-image theorem for a general class of abelian varieties*, Bull. Lond. Math. Soc. **43** (2011), no. 4, 703–711, DOI 10.1112/blms/bdr004. With an appendix by Emmanuel Kowalski. MR2820155

[3] Nathan Jones, *A bound for the conductor of an open subgroup of* GL_2 *associated to an elliptic curve*, Pacific J. Math. **308** (2020), no. 2, 307–331, DOI 10.2140/pjm.2020.308.307. MR4190460

[4] Aaron Landesman, Ashvin A. Swaminathan, James Tao, and Yujie Xu, *Lifting subgroups of symplectic groups over* $\mathbb{Z}/\ell\mathbb{Z}$, Res. Number Theory **3** (2017), Paper No. 14, 12, DOI 10.1007/s40993-017-0078-6. MR3667841

[5] Aaron Landesman, Ashvin A. Swaminathan, James Tao, and Yujie Xu, *Hyperelliptic curves with maximal Galois action on the torsion points of their Jacobians*, Indiana Univ. Math. J. **69** (2020), no. 7, 2461–2492, DOI 10.1512/iumj.2020.69.8178. MR4195609

[6] Serge Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002, DOI 10.1007/978-1-4613-0041-0. MR1878556

[7] Serge Lang and Hale Trotter, *Frobenius distributions in* GL_2*-extensions*, Lecture Notes in Mathematics, Vol. 504, Springer-Verlag, Berlin-New York, 1976. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers. MR0568299

[8] D. Mumford, *A note of Shimura's paper "Discontinuous groups and abelian varieties"*, Math. Ann. **181** (1969), 345–351, DOI 10.1007/BF01350672. MR248146

[9] O. T. O'Meara, *Symplectic groups*, Mathematical Surveys, No. 16, American Mathematical Society, Providence, R.I., 1978. MR502254

[10] Derek J. S. Robinson, *A course in the theory of groups*, 2nd ed., Graduate Texts in Mathematics, vol. 80, Springer-Verlag, New York, 1996, DOI 10.1007/978-1-4419-8594-1. MR1357169

[11] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques* (French), Invent. Math. **15** (1972), no. 4, 259–331, DOI 10.1007/BF01405086. MR387283

[12] Jean-Pierre Serre, *Abelian l-adic representations and elliptic curves*, 2nd ed., Advanced Book Classics, Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989. With the collaboration of Willem Kuyk and John Labute. MR1043865

[13] Thomas Jan Stieltjes, *Œuvres complètes. II/Collected papers. II*, Springer Collected Works in Mathematics, Springer, Berlin, 2017. Edited by Gerrit van Dijk; Reprinted from the 1993 edition [MR1272017]. MR3643001

[14] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517, DOI 10.2307/1970722. MR236190

Department of Mathematics, Statistics, and Computer Science, University of Illinois Chicago, 851 S. Morgan Street, Chicago, Illinois 60607
Email address: jmayle2@uic.edu