Abelian varieties over finitely generated fields and the conjecture of Geyer and Jarden on torsion

Sara Arias-de-Reyna
Institut für Experimentelle Mathematik,
45326 Essen, Germany
sara.arias-de-reyna@uni-due.de

Wojciech Gajda
Department of Mathematics,
Adam Mickiewicz University,
61614 Poznań, Poland
gajda@amu.edu.pl

Sebastian Petersen*
Universität Kassel,
Fachbereich Mathematik,
34132 Kassel, Germany
sebastian.petersen@unibw.de

October 28, 2013

Abstract

In this paper we prove the Geyer-Jarden conjecture on the torsion part of the Mordell-Weil group for a large class of abelian varieties defined over finitely generated fields of arbitrary characteristic. The class consists of all abelian varieties with *big monodromy*, i.e., such that the image of Galois representation on ℓ-torsion points, for almost all primes ℓ, contains the full symplectic group.

*the corresponding author
2000 MSC: 11E30, 11G10, 14K15.
Key words and phrases: Abelian variety, Galois representation, Haar measure.

Introduction

Let A be a polarized abelian variety defined over a finitely generated field K. Denote by $\widetilde{K}$ (respectively, $K_{\rm sep}$) the algebraic (resp., separable) closure of K. It is well known that the Mordell-Weil group $A(K)$ is a finitely generated $\mathbb{Z}$-module. On the other hand $A(\widetilde{K})$ is a divisible group with an infinite torsion part $A(\widetilde{K})_{\rm tor}$ and $A(\widetilde{K})$ has infinite rank, unless K is algebraic over a finite field. Hence, it is of fundamental interest to study the structure of the groups $A(\Omega)$ for infinite algebraic extensions Ω/K smaller than $\widetilde{K}$. For example, Ribet in [26] and Zarhin in [37] considered the question of finiteness of $A(K_{\rm ab})_{\rm tor}$, where $K_{\rm ab}$ is the maximal abelian extension of K.

We denote by $G_K := G(K_{\rm sep}/K)$ the absolute Galois group of K. For a positive integer e and for $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_e)$ in the group $G_K^e = G_K \times G_K \times \ldots \times G_K$, we denote by $K_{\rm sep}(\sigma)$ the subfield in $K_{\rm sep}$ fixed by $\sigma_1, \sigma_2, \ldots, \sigma_e$. There exists a substantial literature on arithmetic properties of the fields $K_{\rm sep}(\sigma)$. In particular, the Mordell-Weil groups $A(K_{\rm sep}(\sigma))$ have been already studied, e.g., Larsen formulated a conjecture in [22] on the rank of $A(K_{\rm sep}(\sigma))$ (cf. [2], [12] for results supporting the conjecture of Larsen).

In this paper we consider the torsion part of the groups $A(K_{\rm sep}(\sigma))$. In order to recall the conjecture which is mentioned in the title, we agree to say that a property $\mathcal{A}(\sigma)$ *holds for almost all* $\sigma \in G_K^e$, if $\mathcal{A}(\sigma)$ holds for all $\sigma \in G_K^e$, except for a set of measure zero with respect to the (unique) normalized Haar measure on the compact group G_K^e. In [10] Geyer and Jarden proposed the following conjecture on the torsion part of $A(K_{\rm sep}(\sigma))$.

Conjecture of Geyer and Jarden. *Let K be a finitely generated field. Let A be an abelian variety defined over K.*

a) For almost all $\sigma \in G_K$ there are infinitely many prime numbers ℓ such that the group $A(K_{\rm sep}(\sigma))[\ell]$ of $\ell-$division points is nonzero.

b) Let $e \geq 2$. For almost all $\sigma \in G_K^e$ there are only finitely many prime numbers ℓ such that the group $A(K_{\rm sep}(\sigma))[\ell]$ of $\ell-$division points is nonzero.

It is known due to the work of Jacobson and Jarden [18] that for all $e \geq 1$, almost all $\sigma \in G_K^e$ and all primes ℓ the group $A(K_{\rm sep}(\sigma))[\ell^\infty]$ is finite. This was formerly part (c) of the conjecture. Moreover the Conjecture is known for elliptic curves [10]. Part (b) holds true provided $\mathrm{char}(K) = 0$ (see [18]). In a very recent preprint Zywina proves part (a) in the special case where K is a number field (cf. [**?**]), stengthening results of Geyer and Jarden [11].

As for today, for an abelian variety A of dimension ≥ 2 defined over a finitely generated field of positive characteristic, parts (a) and (b) of the Conjecture of Geyer and Jarden are open and part (a) is open over a finitely generated transcendental extension of $\mathbb{Q}$.

In this paper we prove the Conjecture of Geyer and Jarden for abelian varieties with big monodromy. To formulate our main result we need some notation. Let $\ell \neq \mathrm{char}(K)$ be a prime number. We denote by $\rho_{A[\ell]} : G_K \longrightarrow \mathrm{Aut}(A[\ell])$ the Galois representation attached to the action of G_K on the ℓ-torsion points of A. We define $\mathcal{M}_K(A[\ell]) := \rho_{A[\ell]}(G_K)$ and call this group *the mod-ℓ monodromy group of A/K*. We fix a polarization and denote by $e_\ell{:}A[\ell] \times A[\ell] \to \mu_\ell$ the corresponding Weil pairing. Then $\mathcal{M}_K(A[\ell])$ is a subgroup of the group of symplectic similitudes $\mathrm{GSp}(A[\ell], e_\ell)$ of the Weil pairing. We will say that A/K *has big monodromy* if there exists a constant ℓ_0 such that $\mathcal{M}_K(A[\ell])$ contains the symplectic group $\mathrm{Sp}(A[\ell], e_\ell)$, for every prime number $\ell \geq \ell_0$. Note that the property of having big monodromy does not depend on the choice of the polarization.

The main result of our paper is the following

Main Theorem. *[cf. Thm. 3.1, Thm. 5.1] Let K be a finitely generated field and A/K an abelian variety with big monodromy. Then the Conjecture of Geyer and Jarden holds true for A/K.*

Surprisingly enough, the most difficult to prove is the case (a) of the Conjecture for abelian varieties with big monodromy, when $\mathrm{char}(K) > 0$. The method of our proof relies in this case on the Borel-Cantelli Lemma of measure theory and on a delicate counting argument in the group $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ which was modeled after a construction of subsets $S'(\ell)$ in $\mathrm{SL}_2(\mathbb{F}_\ell)$ in Section 3 of the classical paper [10] of Geyer and Jarden.

It is interesting to combine the main Theorem with existing computations of monodromy groups for certain families of abelian varieties. Certainly, the most prominent result of this type is the classical theorem of Serre (cf. [28], [29] for the number field case; the generalization to finitely generated fields of characteristic zero is well-known): *If A is an abelian variety over a finitely generated field K of characteristic zero with $\mathrm{End}(A) = \mathbb{Z}$ and $\dim(A) = 2, 6$ or odd, then A/K has big monodromy.* Here $\mathrm{End}(A) = \mathrm{End}_{\tilde{K}}(A_{\tilde{K}})$ stands for the absolute endomorphism ring of A.

In this paper we focus our attention at abelian varieties with $\mathrm{End}(A) = \mathbb{Z}$, which have been recently considered by Chris Hall in his open image theorem [16]. To simplify notation, we will say that an abelian variety A over a finitely generated field K *is of Hall type*, if $\mathrm{End}(A) = \mathbb{Z}$ and K has a discrete valuation at which A has semistable reduction of toric dimension one. The following result, proven in our paper [1], gives examples of abelian varieties with big monodromy in all dimensions (and including the case $\mathrm{char}(K) > 0$): *If A is an abelian variety of Hall type over a finitely generated infinite field K, then A/K has big monodromy.* In the special case where K is a global field this has recently been shown by Hall (cf. [15], [16]). The generalization to an arbitrary finitely generated ground field K is carried out in [1] using methods of group theory, finiteness properties of the fundamental group of schemes and Galois theory of large field extensions. In combination with the main Theorem we obtain the following

Corollary. *Let A be an abelian variety over a finitely generated infinite field K. Assume that either condition i) or ii) is satisfied.*

i) A is of Hall type.

ii) $\mathrm{char}(K) = 0$, $\mathrm{End}(A) = \mathbb{Z}$ *and* $\dim(A) = 2, 6$ *or odd.*

Then the Conjecture of Geyer and Jarden holds true for A/K.

We thus obtain over every finitely generated infinite field and for every dimension families of abelian varieties for which the Conjecture of Geyer and Jarden holds true. In the case when $\mathrm{char}(K) > 0$ the Corollary offers the first evidence for the conjecture of Geyer and Jarden on torsion going beyond the case of elliptic curves.

We warmly thank Gerhard Frey, Dieter Geyer, Cornelius Greither and Moshe Jarden for conversations and useful comments on the topic of this paper.

1 Notation and background material

In this section we fix notation and gather some background material on Galois representations that is important for the rest of this paper.

If K is a field, then we denote by K_{sep} (resp. $\widetilde{K}$) the separable (resp. algebraic) closure of K and by $G_K = G(K_{\mathrm{sep}}/K)$ its absolute Galois group. If G is a profinite (hence compact) group, then it has a unique normalized Haar measure μ_G. The expression "assertion $\mathcal{A}(\sigma)$ holds for almost all $\sigma \in G$" means "assertion $\mathcal{A}(\sigma)$ holds true for all σ outside a zero set with respect to μ_G". A finitely generated field is by definition a field which is finitely generated over its prime field. Let X be a scheme of finite type over a field K. For a geometric point $P \in X(\tilde{K})$ we denote by $K(P) \subset \tilde{K}$ the residue field at P.

For $n \in \mathbb{N}$ coprime to $\mathrm{char}(K)$, we let $A[n]$ be the group of n-torsion points in $A(\tilde{K})$ and define $A[n^\infty] = \bigcup_{i=1}^{\infty} A[n^i]$. For a prime $\ell \neq \mathrm{char}(K)$ we denote by $T_\ell(A) = \varprojlim_{i \in \mathbb{N}} A[\ell^i]$ the ℓ-adic Tate module of A. Then $A[n]$, $A[n^\infty]$ and $T_\ell(A)$ are G_K-modules in a natural way.

If M is a G_K-module (for example $M = \mu_n$ or $M = A[n]$ where A/K is an abelian variety), then we shall denote the corresponding representation of the Galois group G_K by

$$\rho_M : G_K \to \mathrm{Aut}(M)$$

and define $\mathcal{M}_K(M) := \rho_M(G_K)$. We define $K(M) := K_{\mathrm{sep}}^{\ker(\rho_M)}$ to be the fixed field in K_{sep} of the kernel of ρ_M. Then $K(M)/K$ is a Galois extension and $G(K(M)/K) \cong \mathcal{M}_K(M)$.

If R is a commutative ring with 1 (usually $R = \mathbb{F}_\ell$ or $R = \mathbb{Z}_\ell$) and M is a finitely generated free R-module equipped with a non-degenerate alternating bilinear pairing $e : M \times M \to R'$ into a free R'-module of rank 1 (which is a multiplicatively written R-module in our setting below), then we denote by

$$\mathrm{Sp}(M, e) = \{f \in \mathrm{Aut}_R(M) \quad | \quad \forall x, y \in M : e(f(x), f(y)) = e(x, y)\}$$

the corresponding symplectic group and by

$$\mathrm{GSp}(M, e) = \{f \in \mathrm{Aut}_R(M) \quad | \quad \exists \varepsilon \in R^\times : \forall x, y \in M : e(f(x), f(y)) = \varepsilon e(x, y)\}$$

the corresponding group of symplectic similitudes.

Let n be an integer coprime to $\mathrm{char}(K)$ and ℓ be a prime different from $\mathrm{char}(K)$. Let A/K be an abelian variety. We denote by $A^\vee$ the dual abelian variety and let $e_n : A[n] \times A^\vee[n] \to \mu_n$ and $e_{\ell^\infty} : T_\ell A \times T_\ell A^\vee \to \mathbb{Z}_\ell(1)$ be the corresponding Weil pairings. If $\lambda : A \to A^\vee$ is a polarization, then we deduce Weil pairings $e_n^\lambda : A[n] \times A[n] \to \mu_n$ and $e_{\ell^\infty}^\lambda : T_\ell A \times T_\ell A \to \mathbb{Z}_\ell(1)$ in the obvious way. If ℓ does not divide $\deg(\lambda)$ and if n is coprime to $\deg(\lambda)$, then e_n^λ and $e_{\ell^\infty}^\lambda$ are non-degenerate, alternating, G_K-equivariant pairings. Hence we have representations

$$\rho_{A[n]} : G_K \to \mathrm{GSp}(A[n], e_n^\lambda),$$

$$\rho_{T_\ell A} : G_K \to \mathrm{GSp}(T_\ell A, e_{\ell^\infty}^\lambda)$$

with images $\mathcal{M}_K(A[n]) \subset \mathrm{GSp}(A[n], e_n^\lambda)$ and $\mathcal{M}_K(T_\ell A) \subset \mathrm{GSp}(T_\ell A, e_{\ell^\infty}^\lambda)$. We shall say that an abelian variety (A, λ) over a field K has *big monodromy*, if there is a constant $\ell_0 > \max(\mathrm{char}(K), \deg(\lambda))$ such that $\mathcal{M}_K(A[\ell]) \supset \mathrm{Sp}(A[\ell], e_\ell^\lambda)$ for every prime number $\ell \geq \ell_0$.

2 Properties of abelian varieties with big monodromy

Let (A, λ) be a polarized abelian variety with big monodromy over a finitely generated field K. Then $\mathrm{Sp}(A[\ell], e_\ell^\lambda) \subset \mathcal{M}_K(A[\ell])$ for sufficiently large primes ℓ. In this section we determine $\mathcal{M}_K(A[n])$ completely for every "sufficiently large" integer n. The main result (cf. Proposition 2.4 below) is due to Serre in the number field case, and the general case requires only a slight adaption of Serre's line of reasoning. However, as the final outcome is somewhat different in positive characteristic, we do include the details. Proposition 2.4 will be crucial for our results on the Conjecture of Geyer and Jarden.

Now let K be an arbitrary field and A/K an abelian variety. Recall that for every algebraic extension L/K we defined $\mathcal{M}_L(A[n]) = \rho_{A[n]}(G_L)$ (n coprime to $\mathrm{char}(K)$) and $\mathcal{M}_L(T_\ell A) = \rho_{T_\ell A}(G_L)$ ($\ell > \mathrm{char}(K)$ a prime number). Furthermore the representations induce isomorphisms $G(L(A[n])/L) \cong \mathcal{M}_L(A[n])$ and $G(L(A[\ell^\infty]/L) \cong \mathcal{M}_L(T_\ell A)$. Note that $\mathcal{M}_L(T_\ell A) \to \mathcal{M}_L(A[\ell^i])$ is surjective (because $G(L(A[\ell^\infty])/L) \to G(L(A[\ell^i])/L)$ is surjective) for every integer i. Clearly $\mathcal{M}_L(A[n])$ is a subgroup of $\mathcal{M}_K(A[n])$.

Remark 2.1. *If L/K is a* Galois *extension, then $\mathcal{M}_L(A[n])$ is a* normal *subgroup of $\mathcal{M}_K(A[n])$ and the quotient group $\mathcal{M}_K(A[n])/\mathcal{M}_L(A[n])$ is isomorphic to $G(L \cap K(A[n])/K)$.*

Proposition 2.2. *Let K be a field and (A, λ) a polarized abelian variety over K with big monodromy. Let L/K be an abelian Galois extension with $L \supset \mu_\infty$. Then there is a constant $\ell_0 > \max(\mathrm{char}(K), \deg(\lambda))$ with the following properties.*

a) $\mathcal{M}_L(T_\ell A) = \mathrm{Sp}(T_\ell A, e^\lambda_{\ell^\infty})$ for all primes $\ell \geq \ell_0$.

b) Let c be the product of all prime numbers $\leq \ell_0$. Then $\mathcal{M}_L(A[n]) = \mathrm{Sp}(A[n], e^\lambda_n)$ for every integer n which is coprime to c.

Proof. Part a). There is a constant $\ell_0 > \max(\mathrm{char}(K), \deg(\lambda), 5)$ such that $\mathcal{M}_K(A[\ell]) \supset \mathrm{Sp}(A[\ell], e^\lambda_\ell)$ for all primes $\ell \geq \ell_0$, because A has big monodromy. Let $\ell \geq \ell_0$ be a prime and define $K_\ell := K(\mu_\ell)$. Then basic properties of the Weil pairing imply that $G(K_\ell(A[\ell])/K_\ell) \cong \mathcal{M}_{K_\ell}(A[\ell]) = \mathrm{Sp}(A[\ell], e^\lambda_\ell)$. This group is perfect, because $\ell \geq 5$ (cf. [33, Theorem 8.7]). As L/K_ℓ is an abelian Galois extension, $\mathcal{M}_L(A[\ell])$ is a normal subgroup of the perfect group $\mathcal{M}_{K_\ell}(A[\ell])$ and the quotient $\mathcal{M}_{K_\ell}(A[\ell])/\mathcal{M}_L(A[\ell])$ is isomorphic to a subquotient of $G(L/K)$ (cf. Remark 2.1), hence abelian. This implies that

$$\mathcal{M}_L(A[\ell]) = \mathcal{M}_{K_\ell}(A[\ell]) = \mathrm{Sp}(A[\ell], e^\lambda_\ell).$$

Denote by $p : \mathrm{Sp}(T_\ell A, e^\lambda_{\ell^\infty}) \to \mathrm{Sp}(A[\ell], e^\lambda_\ell)$ the canonical projection. Then $\mathcal{M}_L(T_\ell A)$ is a closed subgroup of $\mathrm{Sp}(T_\ell A, e^\lambda_{\ell^\infty})$ with

$$p(\mathcal{M}_L(T_\ell A)) = \mathcal{M}_L(A[\ell]) = \mathrm{Sp}(A[\ell], e^\lambda_\ell).$$

Hence $\mathcal{M}_L(T_\ell A) = \mathrm{Sp}(T_\ell A, e^\lambda_{\ell^\infty})$ by [21, Proposition 2.6].

Part b). Consider the map

$$\rho : G_L \to \prod_{\ell \geq \ell_0} \mathcal{M}_L(T_\ell A) = \prod_{\ell \geq \ell_0} \mathrm{Sp}(T_\ell A, e^\lambda_{\ell^\infty})$$

induced by the representations $\rho_{T_\ell A}$ and denote by $X := \rho(G_L)$ its image. Then X is a closed subgroup of $\prod_{\ell \geq \ell_0} \mathrm{Sp}(T_\ell A, e^\lambda_{\ell^\infty})$. If pr_ℓ denotes the ℓ-th projection of the product, then $\mathrm{pr}_\ell(X) = \mathrm{Sp}(T_\ell A, e^\lambda_{\ell^\infty})$. Hence [31, Section 7, Lemme 2] implies that $X = \prod_{\ell \geq \ell_0} \mathrm{Sp}(T_\ell A, e^\lambda_{\ell^\infty})$, i.e. that ρ is *surjective*.

Let c be the product of all prime numbers $\leq \ell_0$. Let n be an integer coprime to c. Then $n = \prod_{\ell | n \text{ prime}} \ell^{v_\ell}$ for certain integers $v_\ell \geq 1$. The canonical map $r : \mathcal{M}_L(A[n]) \to \prod_{\ell | n \text{ prime}} \mathcal{M}_L(A[\ell^{v_\ell}])$ is injective. Consider the diagram

$$\begin{array}{ccccc} G_L & \xrightarrow{\rho'} & \prod_{\ell|n} \mathcal{M}_L(T_\ell A) & = & \prod_{\ell|n} \mathrm{Sp}(T_\ell A, e^\lambda_{\ell^\infty}) \\ \downarrow & & \downarrow & & \downarrow \\ \mathcal{M}_L(A[n]) & \xhookrightarrow{r} & \prod_{\ell|n} \mathcal{M}_L(A[\ell^{v_\ell}]) & \hookrightarrow & \prod_{\ell|n} \mathrm{Sp}(A[\ell^{v_\ell}], e^\lambda_{\ell^{v_\ell}}). \end{array}$$

The vertical maps are surjective. The horizontal map ρ' is surjective as well, because ρ is surjective. This implies, that the lower horizontal map

$$\mathcal{M}_L(A[n]) \to \prod_{\ell|n} \mathrm{Sp}(A[\ell^{v_\ell}], e^\lambda_{\ell^{v_\ell}})$$

is in fact bijective. It follows from the Chinese Remainder Theorem that the canonical map

$$\prod_{\ell|n} \mathrm{Sp}(A[\ell^{v_\ell}], e^\lambda_{\ell^{v_\ell}}) \to \mathrm{Sp}(A[n], e^\lambda_n)$$

is bijective as well. Assertion b) follows from that. □

Corollary 2.3. *Let K be a field and (A, λ) a polarized abelian variety over K with big monodromy. Then there is a constant c coprime to $\deg(\lambda)$ and to $\mathrm{char}(K)$, if $\mathrm{char}(K)$ is positive, with the following property: $\mathcal{M}_K(A[n]) \supset \mathrm{Sp}(A[n], e^\lambda_n)$ for every integer n coprime to c.*

Proof. Let $L = K_{\mathrm{ab}}$ be the maximal abelian extension. Then there is a constant c as above, such that $\mathcal{M}_L(A[n]) = \mathrm{Sp}(A[n], e^\lambda_n)$ for every n coprime to c by Proposition 2.2. Furthermore $\mathcal{M}_L(A[n]) \subset \mathcal{M}_K(A[n])$ by the discussion before Remark 2.1. □

Let K be a field and (A, λ) a polarized abelian variety over K with big monodromy. There is a constant c (divisible by $\deg(\lambda)$ and by $\mathrm{char}(K)$, if $\mathrm{char}(K) \neq 0$) such that

$$\mathrm{Sp}(A[n], e^\lambda_n) \subset \mathcal{M}_K(A[n]) \subset \mathrm{GSp}(A[n], e^\lambda_n)$$

for all $n \in \mathbb{N}$ coprime to c (cf. Corollary 2.3). One can easily determine $\mathcal{M}_K(A[n])$ completely, if K is finitely generated. Let $K_n := K(A[n])$. There is a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & G(K_n/K(\mu_n)) & \longrightarrow & G(K_n/K) & \longrightarrow & G(K(\mu_n)/K) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \rho_{A[n]}} & & \downarrow{\scriptstyle \rho_{\mu_n}} & & \\
0 & \longrightarrow & \mathrm{Sp}(A[n], e^\lambda_n) & \longrightarrow & \mathrm{GSp}(A[n], e^\lambda_n) & \xrightarrow{\varepsilon} & (\mathbb{Z}/n)^\times & \longrightarrow & 0
\end{array}$$

with exact rows and injective vertical maps, where ρ_{μ_n} is the cyclotomic character and ε is the multiplicator map. The left hand vertical map is an isomorphism for every $n \in \mathbb{N}$ coprime to c. Hence

$$\mathcal{M}_K(A[n]) = \{f \in \mathrm{GSp}(A[n], e^\lambda_n) \mid \varepsilon(f) \in \mathrm{im}(\rho_{\mu_n})\}.$$

Assume from now on that K is finitely generated. Then the image of the cyclotomic character involved above has a well known explicit description. Denote by F the algebraic closure of the prime field of K in K and define $q := q(K) := |F| \in \mathbb{N} \cup \{\infty\}$. Then, after possibly replacing c by a larger constant, we have

$$\mathrm{im}(\rho_{\mu_n}) = \begin{cases} \langle \overline{q} \rangle & \mathrm{char}(K) \neq 0, \\ (\mathbb{Z}/n)^\times & \mathrm{char}(K) = 0. \end{cases}$$

for all $n \in \mathbb{N}$ coprime to c. Here $\langle \overline{q} \rangle$ is the subgroup of $(\mathbb{Z}/n)^\times$ generated by the residue class $\overline{q}$ of q modulo n, provided q is finite. If q is finite, then we define

$$\mathrm{GSp}^{(q)}(A[n], e_n^\lambda) = \{f \in \mathrm{GSp}(A[n], e_n^\lambda) \mid \varepsilon(f) \in \langle \overline{q} \rangle\}.$$

Finally we put $\mathrm{GSp}^{(\infty)}(A[n], e_n^\lambda) = \mathrm{GSp}(A[n], e_n^\lambda)$. We have shown:

Proposition 2.4. *Let K be a finitely generated field and (A, λ) a polarized abelian variety over K with big monodromy. Let $q = q(K)$. Then there is a constant c (divisible by $\deg(\lambda)$ and by $\mathrm{char}(K)$, if $\mathrm{char}(K) \neq 0$) such that $\mathcal{M}_K(A[n]) = \mathrm{GSp}^{(q)}(A[n], e_n^\lambda)$ for all $n \in \mathbb{N}$ coprime to c.*

3 Proof of the Conjecture of Geyer and Jarden, part b)

Let (A, λ) be a polarized abelian variety of dimension g over a field K. In this section we will use the notation $K_\ell := K(A[\ell])$ and $G_\ell := G(K_\ell/K)$ for every prime $\ell \neq \mathrm{char}(K)$. Our main result in this section is the following theorem.

Theorem 3.1. *If (A, λ) has big monodromy, then for all $e \geq 2$ and almost all $\sigma \in G_K^e$ (in the sense of the Haar measure) there are only finitely many primes ℓ such that $A(K_{\mathrm{sep}}(\sigma))[\ell] \neq 0$.*

The following Lemma 3.2 is due to Oskar Villareal (private communication). We thank him for his kind permission to include it into our manuscript.

Lemma 3.2. *Assume that A has big monodromy. Then there is a constant ℓ_0 such that $[K(P) : K]^{-1} \leq [K_\ell : K]^{-\frac{1}{2g}}$ for all primes $\ell \geq \ell_0$ and all $P \in A[\ell]$, where $K(P)$ denotes the residue field of the point P.*

Proof. By assumption on A, there is a constant ℓ_0 such that $\mathrm{Sp}(A[\ell], e_\ell^\lambda) \subset \mathcal{M}_K(A[\ell])$ for all primes $\ell \geq \ell_0$. Let $\ell \geq \ell_0$ be a prime and $P \in A[\ell]$. Then the $\mathbb{F}_\ell$-vector space generated inside $A[\ell]$ by the orbit $X := \{f(P) : f \in \mathcal{M}_K(A[\ell])\}$ is the whole of $A[\ell]$, because $A[\ell]$ is a simple $\mathbb{F}_\ell[\mathrm{Sp}(A[\ell], e_\ell^\lambda)]$-module. Thus we can choose an $\mathbb{F}_\ell$-basis $(P_1, \cdots, P_{2g})$ of $A[\ell]$ with $P_1 = P$ in such a way that each $P_i \in X$. Then each P_i is conjugate to P under the action of G_K and $[K(P) : K] = [K(P_i) : K]$ for all i. The field K_ℓ is the composite field $K_\ell = K(P_1) \cdots K(P_{2g})$. It follows that

$$[K_\ell : K] \leq [K(P_1) : K] \cdots [K(P_{2g}) : K] = [K(P) : K]^{2g}.$$

The desired inequality follows from that. □

The following notation will be used in the sequel: For sequences $(x_n)_n$ and $(y_n)_n$ of positive real numbers we shall write $x_n \sim y_n$, provided the sequence $(\frac{x_n}{y_n})$ converges to a positive real number. If $x_n \sim y_n$ and $\sum x_n < \infty$, then $\sum y_n < \infty$.

The proof of Theorem 3.1 will make heavy use of the following classical fact.

Lemma 3.3. (Borel-Cantelli, [9, 18.3.5]) *Let $(A_1, A_2, \cdots)$ be a sequence of measurable subsets of a profinite group G. Let*

$$A := \bigcap_{n=1}^{\infty} \bigcup_{i=n}^{\infty} A_i = \{x \in G : x \text{ belongs to infinitely many } A_i\}.$$

a) If $\sum_{i=1}^{\infty} \mu_G(A_i) < \infty$, then $\mu_G(A) = 0$.

b) If $\sum_{i=1}^{\infty} \mu_G(A_i) = \infty$ and $(A_i)_{i\in\mathbb{N}}$ is a μ_G-independent sequence (i.e. for every finite set $I \subset \mathbb{N}$ we have $\mu_G(\bigcap_{i\in I} A_i) = \prod_{i\in I} \mu_G(A_i)$), then $\mu_G(A) = 1$.

Proof of Theorem 3.1. Assume that A/K has big monodromy and let ℓ_0 be a constant as in the definition of the term "big monodromy". We may assume that $\ell_0 \geq \mathrm{char}(K)$. Let $e \geq 2$ and define

$$X_\ell := \{\sigma \in G_K^e : A(K_{\mathrm{sep}}(\sigma))[\ell] \neq 0\}$$

for every prime ℓ. Let μ be the normalized Haar measure on G_K^e. Theorem 3.1 follows from Claim 1 below, because Claim 1 together with the Borel-Cantelli Lemma 3.3 implies that

$$\bigcap_{n\in\mathbb{N}} \bigcup_{\ell\geq n \text{ prime}} X_\ell$$

has measure zero.

Claim 1. The series $\sum_{\ell \text{ prime}} \mu(X_\ell)$ converges.

Let $\ell \geq \ell_0$ be a prime number. Note that

$$X_\ell = \bigcup_{P\in A[\ell]\setminus\{0\}} \{\sigma \in G_K^e \mid \sigma_i(P) = P \text{ for all } i\} = \bigcup_{P\in A[\ell]\setminus\{0\}} G^e_{K(P)}.$$

Let $\mathbb{P}(A[\ell]) = (A[\ell] \setminus \{0\})/\mathbb{F}_\ell^\times$ be the projective space of lines in the $\mathbb{F}_\ell$-vector space $A[\ell]$. It is a projective space of dimension $2g-1$. For $P \in A[\ell] \setminus \{0\}$ we denote by $\overline{P} := \mathbb{F}_\ell^\times P$ the equivalence class of P in $\mathbb{P}(A[\ell])$. For $\overline{P} \in \mathbb{P}(A[\ell])$ and $P_1, P_2 \in \overline{P}$ there is an $a \in \mathbb{F}_\ell^\times$ such that $P_1 = aP_2$ and $P_2 = a^{-1}P_1$, and this implies $K(P_1) = K(P_2)$. It follows that we can write

$$X_\ell = \bigcup_{\overline{P}\in\mathbb{P}(A[\ell])} G^e_{K(P)}.$$

Hence

$$\mu(X_\ell) \leq \sum_{\overline{P}\in\mathbb{P}(A[\ell])} \mu(G^e_{K(P)}) = \sum_{\overline{P}\in\mathbb{P}(A[\ell])} [K(P) : K]^{-e},$$

and Lemma 3.2 implies

$$\mu(X_\ell) \leq \sum_{\overline{P}\in\mathbb{P}(A[\ell])} [K_\ell : K]^{-e/2g} = \frac{\ell^{2g}-1}{\ell-1}[K_\ell : K]^{-e/2g} = \frac{\ell^{2g}-1}{\ell-1}|G_\ell|^{-e/2g}.$$

But G_ℓ contains $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ and

$$s_\ell := |\mathrm{Sp}_{2g}(\mathbb{F}_\ell)| = \ell^{g^2} \prod_{i=1}^{g} (\ell^{2i} - 1)$$

(cf. [33]). It is thus enough to prove the following

Claim 2. The series $\sum_{\ell \geq \ell_0 \text{ prime}} \frac{\ell^{2g}-1}{\ell-1} s_\ell^{-e/2g}$ converges.

But $s_\ell \sim \ell^{g^2+2+4+\cdots+2g} = \ell^{2g^2+g}$ and $\frac{\ell^{2g}-1}{\ell-1} \sim \ell^{2g-1}$, hence

$$\frac{\ell^{2g}-1}{\ell-1} s_\ell^{-e/2g} \sim \ell^{2g-1} \ell^{-e(g+\frac{1}{2})} = \ell^{(2-e)g-(1+\frac{e}{2})} \leq \ell^{-2},$$

because $e \geq 2$. Claim 2 follows from that. □

4 Special sets of symplectic matrices

This section contains a construction of certain special sets of symplectic matrices (cf. Theorem 4.6 below) that will play a crucial role in the proof of part a) of the Conjecture of Geyer and Jarden.

Let $g \geq 2$, and let V be a vector space of dimension $2g$ over a prime finite field $\mathbb{F}_\ell$, endowed with a symplectic form $e : V \times V \to \mathbb{F}_\ell$. Fix a symplectic basis $E = \{e_1, \ldots, e_{2g}\}$ of V such that the symplectic form is given by the matrix

$$J_g = \begin{pmatrix} J_1 & & & \\ & J_1 & & \\ & & \ddots & \\ & & & J_1 \end{pmatrix} \text{ where } J_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

For each $A \in \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ there is an element $\lambda \in \mathbb{F}_\ell^\times$ such that $e(Av, Aw) = \lambda e(v, w)$ for all $v, w \in V$. We will say that the value $\lambda = \varepsilon(A)$ of the multiplicator map ε is the *multiplier* of A, and we will denote by $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)[\lambda]$ the set of matrices in $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ with multiplier λ.

Remark 4.1. *Here we collect some notation. Let p be a prime, q a power of p and $n \in \mathbb{N}$.*

- *For n not divisible by p, we will denote by $\mathrm{ord}_n q$ the order of q modulo n.*
- *Denote by $\mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}/n\mathbb{Z})$ the set of matrices in $\mathrm{GSp}_{2g}(\mathbb{Z}/n\mathbb{Z})$ with multiplier equal to a power of q modulo n.*
- *Denote by $\mathrm{GSp}_{2g}^{(\infty)}(\mathbb{Z}/n\mathbb{Z}) := \mathrm{GSp}_{2g}(\mathbb{Z}/n\mathbb{Z})$.*
- *Let $\alpha_3, \alpha_4, \ldots, \alpha_{2g}, \beta \in \mathbb{F}_\ell$. Call $u_\alpha = e_2 + \alpha_3 e_3 + \cdots + \alpha_{2g} e_{2g}$. We denote by $T_{u_\alpha}[\beta]$ the morphism $v \mapsto v + \beta e(v, u_\alpha) u_\alpha$ (which is a transvection if $\beta \neq 0$).*

We begin with two easy lemmas that will be essential for Definition 4.4.

Lemma 4.2. *Let ℓ be a prime number. For each $\lambda \in \mathbb{F}_\ell^\times$, the matrices of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)[\lambda]$ that fix the vector e_1 are of the form*

$$\left(\begin{array}{c|c|ccc} 1 & d & b_1 & b_2 & \dots \\ \hline 0 & \lambda & 0 & 0 & \dots \\ \hline 0 & d_1 & & & \\ \vdots & \vdots & & B & \\ \vdots & \vdots & & & \end{array}\right) \tag{1}$$

with $B = (b_{ij})_{i,j=1,\dots,2g-2} \in \mathrm{GSp}_{2g-2}(\mathbb{F}_\ell)[\lambda]$, $d, d_1, \dots, d_{2g-2} \in \mathbb{F}_\ell$ and

$$b_k = \frac{1}{\lambda}\left(\sum_{j=1}^{g-1}(d_{2j-1}b_{2j,k} - d_{2j}b_{2j-1,k})\right) \text{ for each } k = 1, \dots, 2g-2. \tag{2}$$

Proof. Let $A \in \mathrm{GSp}_{2g}(\mathbb{F}_\ell)[\lambda]$ be such that $Ae_1 = e_1$. Let us write the matrix of A with respect to the symplectic basis $\{e_1, e_2, \dots, e_{2g-1}, e_{2g}\}$. Since $e(e_1, e_k) = 0$ for all $k = 3, \dots, 2g$, we obtain that $e(e_1, Ae_k) = 0$. Therefore we can write the matrix A as

$$\left(\begin{array}{c|c|ccc} 1 & d & b_1 & b_2 & \dots \\ \hline 0 & d' & 0 & 0 & \dots \\ \hline 0 & d_1 & & & \\ \vdots & \vdots & & B & \\ \vdots & \vdots & & & \end{array}\right)$$

where in the second row we get all entries zero save the $(2,2)$-th. Moreover, since $e(e_1, e_2) = 1$, we get that $e(e_1, Ae_2) = e(Ae_1, Ae_2) = \lambda e(e_1, e_2) = \lambda$, that is to say, $d' = \lambda$.

Furthermore, we have that $e(e_2, e_k) = 0$ for all $k = 3, \dots, 2g$, hence $e(Ae_2, Ae_k) = 0$. These conditions give rise to the equations (2). The rest of the conditions one has to impose imply that $B \in \mathrm{GSp}_{2g-2}(\mathbb{F}_\ell)[\lambda]$. This proves that the conditions in the lemma are necessary. On the other hand, one can check that the product

$$A^t J_g A = \lambda J_g,$$

so they are also sufficient. □

Lemma 4.3. *The set of matrices in $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)[\lambda]$ that do not have the eigenvalue 1 has cardinality greater than $\beta(\ell, g)|\mathrm{Sp}_{2g-2}(\mathbb{F}_\ell)|$, where*

$$\beta(\ell, g) = \ell^{2g-1}(\ell^{2g} - 1)\frac{\ell - 2}{\ell - 1}.$$

Proof. The set of matrices $A \in \mathrm{GSp}_{2g}(\mathbb{F}_\ell)[\lambda]$ that fix the vector e_1 consists of matrices of the form (1), where B belongs to $\mathrm{GSp}_{2g-2}(\mathbb{F}_\ell)[\lambda]$ and $b_1, \dots, b_{2g-2}$

are given by the formula (2) of Lemma 4.2. Therefore the cardinality of the set of such matrices is exactly

$$\ell^{2g-1}|\mathrm{GSp}_{2g-2}(\mathbb{F}_\ell)[\lambda]| = \ell^{2g-1}|\mathrm{Sp}_{2g-2}(\mathbb{F}_\ell)|.$$

On the other hand, the symplectic group acts transitively on the set of cyclic subgroups of V (cf. [17, Thm. 9.9, Ch. 2]). Therefore if a matrix fixes any nonzero vector, it can be conjugated to one of the above. Hence, to obtain an upper bound for the number of matrices with eigenvalue 1 one has to multiply the previous number by the number of cyclic groups of V, namely $\frac{\ell^{2g}-1}{\ell-1}$.

Therefore the set of matrices in $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)[\lambda]$ that have the eigenvalue 1 has cardinality less than $\ell^{2g-1}\frac{\ell^{2g}-1}{\ell-1}|\mathrm{Sp}_{2g-2}(\mathbb{F}_\ell)|$. Hence the number of matrices in $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)[\lambda]$ that do not have the eigenvalue 1 is greater than $|\mathrm{Sp}_{2g}(\mathbb{F}_\ell)| - \ell^{2g-1}\frac{\ell^{2g}-1}{\ell-1}|\mathrm{Sp}_{2g-2}(\mathbb{F}_\ell)|$.

Now apply the well known identity (see for instance the proof of [17, Theorem 9.3. b)])

$$|\mathrm{Sp}_{2g}(\mathbb{F}_\ell)| = (\ell^{2g}-1)\ell^{2g-1}|\mathrm{Sp}_{2g-2}(\mathbb{F}_\ell)|. \tag{3}$$

We thus see that the set of matrices in $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)[\lambda]$ that do not have the eigenvalue 1 has cardinality greater than $\beta(\ell,g)|\mathrm{Sp}_{2g-2}(\mathbb{F}_\ell)|$. □

Definition 4.4. *For each $\lambda \in \mathbb{F}_\ell^\times$ choose once and for all a subset $\mathcal{B}_\lambda$ of matrices $B \in \mathrm{GSp}_{2g-2}(\mathbb{F}_\ell)[\lambda]$ which do not have the eigenvalue 1, with*

$$|\mathcal{B}_\lambda| = \beta(\ell, g-1)|\mathrm{Sp}_{2g-4}(\mathbb{F}_\ell)|$$

(which can be done by Lemma 4.3). Define

$$\begin{aligned} S_\lambda(\ell)_0 := \{&A \text{ of the shape } (1) \text{in Lemma 4.2 such that:} \\ &B \in \mathcal{B}_\lambda \\ &d_1, \dots, d_{2g-2} \in \mathbb{F}_\ell \\ &d \in \mathbb{F}_\ell \setminus \{-(b_1, \dots, b_{2g-2})(\mathrm{Id} - B)^{-1}\left(d_1, \quad \dots, \quad d_{2g-2}\right)^t\}, \\ S_\lambda(\ell) := \{&T_{u_\alpha}[\beta]^{-1} \cdot A \cdot T_{u_\alpha}[\beta] : \alpha_3, \dots, \alpha_{2g}, \beta \in \mathbb{F}_\ell, A \in S_i(\ell)_0\}, \end{aligned}$$

Let q be a power of a prime $p \neq \ell$. Define

$$S^{(q)}(\ell) := \bigcup_{i=1}^{\mathrm{ord}_\ell q} S_{q^i}(\ell).$$

Define also

$$S^{(\infty)}(\ell) = \bigcup_{\lambda \in \mathbb{F}_\ell^\times} S_\lambda(\ell).$$

Remark 4.5. *Clearly $S^{(q)}(\ell) \neq \emptyset$ and $S^{(\infty)}(\ell) \neq \emptyset$. Note moreover that all matrices in $S^{(q)}(\ell)$ and $S^{(\infty)}(\ell)$ fix an element of V.*

This section is devoted to prove the following result.

Theorem 4.6. *The following properties hold:*

(1) Let q be a power of a prime number or $q = \infty$. Then

$$\sum_{\ell} \frac{|S^{(q)}(\ell)|}{|\mathrm{GSp}_{2g}^{(q)}(\mathbb{F}_\ell)|} = \infty.$$

In the first case ℓ runs through all prime numbers coprime to q and in the second case through all prime numbers.

(2) Let q be a power of a prime number p or $q = \infty$. Let $\ell_1, \ldots, \ell_r$ be different prime numbers. If $q \neq \infty$ assume that the ℓ_i are different from p. Let $n = \ell_1 \cdot \cdots \cdot \ell_r$. Then

$$\frac{|S^{(q)}(n)|}{|\mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}/n\mathbb{Z})|} = \prod_{j=1}^{r} \frac{|S^{(q)}(\ell_j)|}{|\mathrm{GSp}_{2g}^{(q)}(\mathbb{F}_{\ell_j})|}$$

where $S^{(q)}(n) \subset \mathrm{GSp}_{2g}(\mathbb{Z}/n\mathbb{Z})$ is the set of matrices that belong to $S^{(q)}(\ell_j)$ modulo ℓ_j, for all $j = 1, \ldots, r$.

First we will prove part (1) of Theorem 4.6. We will need four lemmata.

On the one hand, the cardinality of $S_\lambda(\ell)_0$ is very easy to compute.

Lemma 4.7. *It holds that*

$$|S_\lambda(\ell)_0| = \ell^{2g-2}(\ell-1)\beta(\ell, g-1)|\mathrm{Sp}_{2g-4}(\mathbb{F}_\ell)|.$$

Moreover we can compute the cardinality of $S_\lambda(\ell)$ in terms of $|S_\lambda(\ell)_0|$.

Lemma 4.8. $|S_\lambda(\ell)| = (\ell^{2g-2}(\ell-1)+1)|S_\lambda(\ell)_0|$.

Proof. Let $A \in S_\lambda(\ell)_0$. First of all we will see that the vectors fixed by A are those in the cyclic subgroup generated by e_1. Since the matrix A clearly fixes the vectors in the cyclic subgroup generated by e_1, it suffices to show that any vector fixed by A must belong to this subgroup.

Consider the system of equations $A(x_1, \ldots, x_{2g})^t = (x_1, \ldots, x_{2g})^t$. Assume first that we have a solution with $x_2 = 0$. Then the last $2g-2$ equations boil down to

$$B(x_3, \ldots, x_{2g})^t = (x_3, \ldots, x_{2g})^t.$$

But since B does not have the eigenvalue 1, this equations are not simultaneously satisfied by a nonzero tuple, hence $(x_1, \ldots, x_{2g})^t$ belongs to the cyclic group generated by e_1.

Assume now that we have a solution $(x_1, \ldots, x_g)^t$ with $x_2 \neq 0$. Since 1 is not an eigenvalue of B, the matrix $\mathrm{Id} - B$ is invertible, and we can write the last $2g-2$ equations as

$$(x_3/x_2, \dots, x_{2g}/x_2)^t = (\mathrm{Id} - B)^{-1}(d_1, \dots, d_{2g-2})^t.$$

On the other hand, the first equation reads

$$d = -(b_1, \dots, b_{2g-2})(x_3/x_2, \dots, x_{2g}/x_2)^t.$$

Hence

$$d = -(b_1, \dots, b_{2g-2})(\mathrm{Id} - B)^{-1}(d_3, \dots, d_{2g})^t.$$

But we have precisely asked that d does not satisfy such an equation, cf. Definition 4.4.

Now one can check that, if we have $A, \widetilde{A} \in S_\lambda(\ell)_0$ and elements $\alpha_3, \dots, \alpha_{2g}$, $\beta, \widetilde{\alpha}_3, \dots, \widetilde{\alpha}_{2g}$, $\widetilde{\beta}$ in $\mathbb{F}_\ell$ such that $T_{u_\alpha}[\beta]^{-1} \cdot A \cdot T_{u_\alpha}[\beta] = T_{u_{\widetilde{\alpha}}}[\widetilde{\beta}]^{-1} \cdot \widetilde{A} \cdot T_{u_{\widetilde{\alpha}}}[\widetilde{\beta}]$, then either $\beta = \widetilde{\beta} = 0$ and $A = \widetilde{A}$ or else $\alpha_k = \widetilde{\alpha}_k$ for $k = 3, \dots, 2g$, $\beta = \widetilde{\beta}$ and $A = \widetilde{A}$. Namely, one notices that since $\widetilde{A} = T_{u_{\widetilde{\alpha}}}[\beta]T_{u_\alpha}[\beta]^{-1} \cdot A \cdot T_{u_\alpha}[\beta]T_{u_{\widetilde{\alpha}}}[\widetilde{\beta}]^{-1}$ fixes e_1, then A fixes $T_{u_\alpha}[\beta]T_{u_{\widetilde{\alpha}}}[\widetilde{\beta}]^{-1}e_1$. But A only fixes the elements of the cyclic group generated by e_1; hence, $T_{u_\alpha}[\beta]T_{u_{\widetilde{\alpha}}}[\widetilde{\beta}]^{-1}e_1$ must be in the cyclic group generated by e_1. Now computing $T_{u_\alpha}[\beta]T_{u_{\widetilde{\alpha}}}[\widetilde{\beta}]^{-1}e_1$ one can conclude easily.

Therefore each element of $S_\lambda(\ell)_0$ gives rise to a subset of $S_\lambda(\ell)$ by conjugation by the matrices $T_{u_\alpha}[\beta]$, where α runs through the tuples $(\alpha_3, \dots, \alpha_{2g}) \in \mathbb{F}_\ell^{2g-2}$ and $\beta \in \mathbb{F}_\ell$, and $S_\lambda(\ell)$ is the disjoint union of these subsets. Furthermore, each of these sets has cardinality $\ell^{2g-2}(\ell - 1) + 1$.

□

To prove the first part of Theorem 4.6, we only need one more lemma, which is an easy consequence of the Chinese Remainder Theorem.

Lemma 4.9. *(1) Let q be a power of a prime number p, and let n be a squarefree natural number such that $p \nmid n$. The cardinality of $\mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}/n\mathbb{Z})$ equals $\mathrm{ord}_n(q) \cdot \prod_{\ell|n} |\mathrm{Sp}_{2g}(\mathbb{F}_\ell)|$.*

(2) Let $q = \infty$, and let n be a squarefree natural number. The cardinality of $\mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}/n\mathbb{Z})$ equals $\prod_{\ell|n}(\ell - 1)|\mathrm{Sp}_{2g}(\mathbb{F}_\ell)|$.

Proof of Theorem 4.6(1)

Let q be a power of a prime p or $q = \infty$, and let ℓ be a prime. In the first case, let us also assume $\ell \neq p$. Applying the identity (3) in the proof of Lemma 4.3 twice to the cardinality of $\mathrm{GSp}_{2g}^{(q)}(\mathbb{F}_\ell)$ and Lemmas 4.8, 4.7 and 4.9, we obtain

$$\frac{|S^{(q)}(\ell)|}{|\mathrm{GSp}_{2g}^{(q)}(\mathbb{F}_\ell)|} = \frac{(\ell^{2g-2}(\ell-1)+1)\ell^{2g-2}(\ell-1)\beta(\ell, g-1)|\mathrm{Sp}_{2g-4}(\mathbb{F}_\ell)|}{(\ell^{2g}-1)\ell^{2g-1}(\ell^{2g-2}-1)\ell^{2g-3}|\mathrm{Sp}_{2g-4}(\mathbb{F}_\ell)|} \sim \frac{1}{\ell},$$

and the sum $\sum_{\ell \neq p \text{ prime}} \frac{1}{\ell}$ diverges. □

To prove the second part of Theorem 4.6 we need one auxiliary lemma. For the rest of the section, q will be a power of a prime p.

For each squarefree n not divisible by p and each $i = 1, \dots, \mathrm{ord}_n(q)$, define $S_{q^i}(n) := \{A \in S^{(q)}(n) : \varepsilon(A) = q^i \text{ modulo } n\}$.

Lemma 4.10. *Let q be a power of a prime number p. Let $\ell_1, \dots, \ell_r$ be distinct primes which are different from p, and consider $n = \ell_1 \cdot \dots \cdot \ell_r$. Let $i \in \{1, \dots, \mathrm{ord}_n(q)\}$. Then there is a bijection*

$$S_{q^i}(n) \simeq S_{q^i}(\ell_1) \times \dots \times S_{q^i}(\ell_r).$$

Proof. Consider the canonical projection

$$\begin{aligned} \pi : S_{q^i}(n) &\to S_{q^i}(\ell_1) \times \dots \times S_{q^i}(\ell_r) \\ A &\mapsto (A \mod \ell_1, \dots, A \mod \ell_r). \end{aligned}$$

This is clearly an injective map. Now we want to prove surjectivity. For each j, take some matrix $B_j \in S_{q^i}(\ell_j)$.

By the Chinese Remainder Theorem, there exists $A \in \mathrm{GSp}_{2g}(\mathbb{Z}/n\mathbb{Z})$ such that A projects onto B_j for each j. Note that in particular $A \in S^{(q)}(n)$. Since $\varepsilon(A)$ is congruent to $\varepsilon(B_j) = q^i$ modulo ℓ_j for all j, we get that $\varepsilon(A) = q^i$ modulo n. Therefore $A \in S_{q^i}(n)$. □

Proof of Theorem 4.6(2)
Case $q \neq \infty$: On the one hand, since the cardinality of $|S_{q^i}(\ell)|$ does not depend on i, we obtain

$$\prod_{\ell | n} \frac{|S^{(q)}(\ell)|}{|\mathrm{GSp}_{2g}^{(q)}(\mathbb{F}_\ell)|} = \prod_{\ell | n} \frac{\mathrm{ord}_\ell(q)|S_q(\ell)|}{\mathrm{ord}_\ell(q)|\mathrm{Sp}_{2g}(\mathbb{F}_\ell)|} = \prod_{\ell | n} \frac{|S_q(\ell)|}{|\mathrm{Sp}_{2g}(\mathbb{F}_\ell)|}.$$

On the other hand, taking into account again that $|S_{q^i}(\ell)|$ is independent of i, Lemma 4.9, and that $|S_{q^i}(n)| = \prod_{\ell | n} |S_{q^i}(\ell)|$ by Lemma 4.10, we get

$$\frac{|S^{(q)}(n)|}{|\mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}/n\mathbb{Z})|} = \frac{\sum_{i=1}^{\mathrm{ord}_n(q)} |S_{q^i}(n)|}{\mathrm{ord}_n(q) \prod_{\ell | n} |\mathrm{Sp}_{2g}(\mathbb{F}_\ell)|} = \frac{\sum_{i=1}^{\mathrm{ord}_n(q)} \left(\prod_{\ell | n} |S_{q^i}(\ell)| \right)}{\mathrm{ord}_n(q) \prod_{\ell | n} |\mathrm{Sp}_{2g}(\mathbb{F}_\ell)|} =$$

$$= \frac{\sum_{i=1}^{\mathrm{ord}_n(q)} \left(\prod_{\ell | n} |S_q(\ell)| \right)}{\mathrm{ord}_n(q) \prod_{\ell | n} |\mathrm{Sp}_{2g}(\mathbb{F}_\ell)|} = \frac{\mathrm{ord}_n(q) \left(\prod_{\ell | n} |S_q(\ell)| \right)}{\mathrm{ord}_n(q) \prod_{\ell | n} |\mathrm{Sp}_{2g}(\mathbb{F}_\ell)|} =$$

$$= \prod_{\ell | n} \frac{|S_q(\ell)|}{|\mathrm{Sp}_{2g}(\mathbb{F}_\ell)|}.$$

Case $q = \infty$: By the Chinese Remainder Theorem, there is a canonical isomorphism

$$c : \mathrm{GSp}_{2g}^{(\infty)}(\mathbb{Z}/n) \cong \prod_{i=1}^{r} \mathrm{GSp}_{2g}^{(\infty)}(\mathbb{Z}/\ell_i)$$

and

$$S^{(\infty)}(n) = c^{-1}(S^{(\infty)}(\ell_1) \times \cdots \times S^{(\infty)}(\ell_r))$$

by the definition of $S^{(\infty)}(n)$. It follows that

$$\frac{|S^{(\infty)}(n)|}{|\mathrm{GSp}_{2g}^{(\infty)}(\mathbb{Z}/n)|} = \prod_{i=1}^{r} \frac{|S^{(\infty)}(\ell_i)|}{|\mathrm{GSp}_{2g}^{(\infty)}(\mathbb{Z}/\ell_i)|}$$

as desired. □

Remark 4.11. *In the definition of the set $S_{q^i}(\ell)_0$ (cf. Definition 4.4), we choose a subset $\mathcal{B}_{q^i}$ of matrices in $\mathrm{GSp}_{2g-2}(\mathbb{F}_\ell)[q^i]$ without the eigenvalue 1, which is large enough to ensure that part (1) of Theorem 4.6 holds. For a concrete value of g, one can choose such set more explicitly. For instance, when $g = 2$, instead of $\mathcal{B}_{q^i}$ one can consider the set*

$$\mathcal{B}'_{q^i} := \{\begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix} : b_{1,1} \in \mathbb{F}_\ell,\ b_{2,2} \in \mathbb{F}_\ell \setminus \{1 - b_{1,1} + q^i\},$$
$$b_{1,2} \in \mathbb{F}_\ell^\times,\ b_{2,1} = b_{1,2}^{-1}(b_{1,1}b_{2,2} - q^i)\}$$

of $\ell(\ell-1)^2$ matrices, which can also be used to prove the second part of Theorem 4.6 in the case of the group $\mathrm{GSp}_4(\mathbb{F}_\ell)$.

5 Proof of the Conjecture of Geyer and Jarden, part a)

Theorem 5.1. *Let (A, λ) be a polarized abelian variety over a finitely generated field K. Assume that A/K has big monodromy. Then for almost all $\sigma \in G_K$ there are infinitely many prime numbers ℓ such that $A(K_{\mathrm{sep}}(\sigma))[\ell] \neq 0$.*

Proof. Let $p := \mathrm{char}(K)$. Let $G = G_K$ and $g := \dim(A)$. We fix once and for all for every prime number $\ell \neq p$ a symplectic basis of $T_\ell A$. This defines an isometry of symplectic spaces $(A[n], e_n^\lambda) \cong ((\mathbb{Z}/n)^{2g}, e_n^{\mathrm{can}})$, where e_n^{can} denotes the standard symplectic pairing on $(\mathbb{Z}/n)^{2g}$, for every $n \in \mathbb{N}$ which is not divisible by p. We get an isomorphism $\mathrm{GSp}(A[n], e_n^\lambda) \cong \mathrm{GSp}_{2g}(\mathbb{Z}/n)$ for every such n, and we consider the representations

$$\rho_n : G_K \to \mathrm{GSp}_{2g}(\mathbb{Z}/n)$$

attached to A/K after these choices. If m is a divisor of n, then we denote by $r_{n,m} : \mathrm{GSp}_{2g}(\mathbb{Z}/n) \to \mathrm{GSp}_{2g}(\mathbb{Z}/m)$ the corresponding canonical map, such that $r_{n,m} \circ \rho_n = \rho_m$.

Let $q := q(K)$ be the cardinality of the algebraic closure of the prime field of K in K. Thus $q = \infty$ if $p = 0$ and q is a power of p otherwise. As A has big monodromy, we find by Proposition 2.4 an integer c (divisible by p, if $p \neq 0$) such that $\mathrm{im}(\rho_n) = \mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}/n)$, for every n coprime to c.

For every prime number $\ell > c$, we define

$$X_\ell := \{\sigma \in G_K \mid A(K_{\mathrm{sep}}(\sigma))[\ell] \neq 0\}.$$

It is enough to prove that $\bigcap_{n>c} \bigcup_{\ell \geq n \text{ prime}} X_\ell$ has measure 1. Let $S^{(q)}(n) \subset \mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}/n)$ be the special sets of symplectic matrices defined in Section 4. By remark 4.5 $\rho_\ell^{-1}(S^{(q)}(\ell)) \subset X_\ell$ for every prime number $\ell > c$. It is thus enough to prove that $\bigcap_{n>c} \bigcup_{\ell \geq n \text{ prime}} \rho_\ell^{-1}(S^{(q)}(\ell))$ has measure 1. Clearly $\mu_G(\rho_n^{-1}(S^{(q)}(n))) = \frac{|S^{(q)}(n)|}{|\mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}/n)|}$ for all integers n coprime to c. Hence part (1) of Theorem 4.6 implies that $\sum_{\ell>c \text{ prime}} \mu_G(\rho_\ell^{-1}(S^{(q)}(\ell))) = \infty$.

Furthermore, if $\ell_1, \cdots, \ell_r > c$ are different prime numbers and $n = \ell_1 \cdots \ell_r$, then

$$\bigcap_{i=1}^{r} \rho_{\ell_i}^{-1}(S^{(q)}(\ell_i)) = \rho_n^{-1}(S^{(q)}(n))$$

and part (2) of Theorem 4.6 implies

$$\mu_G(\bigcap_{i=1}^{r} \rho_{\ell_i}^{-1}(S^{(q)}(\ell_i))) = \prod_{i=1}^{r} \mu_G(\rho_{\ell_i}^{-1}(S^{(q)}(\ell_i))).$$

Hence $(\rho_\ell^{-1}(S^{(q)}(\ell)))_{\ell>c}$ is a μ_G-independent sequence of subsets of G. Now Lemma 3.3 implies that $\bigcap_{n>c} \bigcup_{\ell \geq n \text{ prime}} \rho_\ell^{-1}(S^{(q)}(\ell))$ has measure 1, as desired. □

Acknowledgements. S. A. is a research fellow of the Alexander von Humboldt Foundation. S. A. was partially supported by the Ministerio de Educación y Ciencia grant MTM2009-07024. S. A. wants to thank the Hausdorff Research Institute for Mathematics in Bonn, the Centre de Recerca Matemàtica in Bellaterra and the Mathematics Department of Adam Mickiewicz University in Poznań for their support and hospitality while she worked on this project. W.G. and S.P. were partially supported by the Deutsche Forschungsgemeinschaft research grant GR 998/5-1. W.G. was partially supported by the Alexander von Humboldt Research Fellowship and an MNiSzW grant. W.G. thanks Centre Recerca Matemàtica in Bellaterra and the Max Planck Institut für Mathematik in Bonn for support and hospitality during visits in 2010, when he worked on this project. S.P. gratefully acknowledges the hospitality of Mathematics Department of Adam Mickiewicz University in Poznań and of the Minkowski center at Tel Aviv University during several research visits.

References

[1] Sara Arias-de-Reyna Sara, Wojciech Gajda and Sebastian Petersen *Big monodromy theorem for abelian varieties over finitely generated fields.* Preprint 2011

[2] Im Bo-Hae and Michael Larsen. Abelian varieties over cyclic fields. *American Journal of Mathematics*, 130(5):1195–1210, 2008.

[3] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron Models.* Springer-Verlag, 1990.

[4] Brian Conrad. Chow's $K|k$-image and $K|k$-trace, and the Lang-Neron theorem. *Enseign. Math.*, 52(1-2):37–108, 2006.

[5] Leonard E. Dickson. *Linear groups: With an exposition of the Galois field theory.* Dover Publications, Inc., New York, 1958.

[6] Jordan Ellenberg, Christian Elsholtz, Chris Hall, and Emmanuel Kowalski. Non-simple jacobians in a family: geometric and analytic approaches. *J. London Math. Soc.*, 80:135–154, 2009.

[7] Gerd Faltings and Gisbert Wüstholz. *Rational points.* Braunschweig: Vieweg, 1984.

[8] Arno Fehm, Moshe Jarden, and Sebastian Petersen. Kuykian Fields. Preprint, 2010.

[9] Michael D. Fried and Moshe Jarden. *Field arithmetic. 2nd revised and enlarged ed.* Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge 11. Berlin: Springer. xxii, 780 p., 2005.

[10] Wulf-Dieter Geyer and Moshe Jarden. Torsion points of elliptic curves over large algebraic extensions of finitely generated fields. *Israel Journal of Mathematics*, 31:157–197, 1978.

[11] Wulf-Dieter Geyer and Moshe Jarden. Torsion of Abelian varieties over large algebraic fields. *Finite Fields Appl.*, 11(1):123–150, 2005.

[12] Wulf-Dieter Geyer and Moshe Jarden. The rank of abelian varieties over large algebraic fields. *Arch. Math.*, 86(3):211–216, 2006.

[13] Alexander Grothendieck. *Séminaire de Géométrie Algébrique 1 - Rêvetements étales et groupe fondamental.* Springer **LNM 224**, 1971.

[14] Alexander Grothendieck. *Séminaire de Géométrie Algébrique 7 - Groupes de monodromy en géométrie algébrique.* Springer **LNM 288**, 1972.

[15] Chris Hall. Big symplectic or orthogonal monodromy modulo l. *Duke Mathematical Journal*, 141(1):179–203, 2008.

[16] Chris Hall. An open image theorem for a general class of abelian varieties. Preprint. Available at HTTP://WWW.ARXIV.ORG, 2010.

[17] Bertram Huppert. *Endliche Gruppen.* Springer-Verlag, 1976.

[18] Marcel Jacobson and Moshe Jarden. Finiteness theorems for torsion of abelian varieties over large algebraic fields. *Acta Arithmetica*, 98:15–31, 2001.

[19] Emmanuel Kowalski. Big Symplectic Monodromy: A theorem of C. Hall. Preprint.

[20] Serge Lang. *Algebraic Number Theory*. Springer Verlag, 1994.

[21] Michael Larsen. Maximality of Galois actions for compatible systems. *Duke Math. J.*, 80(3):601–630, 1995.

[22] Michael Larsen. Rank of elliptic curves over almost separably closed fields. *Bull. London Math. Soc.*, 35(6):817–820, 2003.

[23] Laurent Moret-Bailly. Pinceaux de variétés abéliennes. *Astérisque*, 129, 1985.

[24] Rutger Noot. Abelian varieties - Galois representations and properties of ordinary reduction. *Compositio Mathematica*, 97:161–171, 1995.

[25] Michel Raynaud. Schémas en groupes de type $(p, \cdots, p)$. *Bulletin de la S.M.F.*, 102:241–280, 1974.

[26] Ken Ribet. Torsion points of abelian varieties in cyclotomic extensions (appendix to an article of Nicholas Katz and Serge Lang). *Enseign. Math.*, 27(3-4):285–319, 1981.

[27] Jean-Pierre Serre. Propriété galoisiennes des points d'ordre fini des courbes elliptique. *Invent. Math.*, 15:259–331, 1972.

[28] Jean-Pierre Serre. Résumé des cours de 1984-1985. *Annuaire du Collège de France*, 1985.

[29] Jean-Pierre Serre. Résumé des cours de 1985-1986. *Annuaire du Collège de France*, 1986.

[30] Jean-Pierre Serre. Lettre á Ken Ribet du 1/1/1981. *Collected Papers IV, Springer*, 2000.

[31] Jean-Pierre Serre. Lettre á Marie-France Vignéras du 10/2/1986. *Collected Papers IV, Springer-Verlag*, 2000.

[32] Jean-Pierre Serre and J. Tate. Good reduction of abelian varieties. *Annals of Mathematics*, 88, No. 3:492–517, 1968.

[33] Donald Taylor. *The geometry of the classical groups*. Heldermann Verlag, 1992.

[34] Alexander E. Zalesskiĭ and Vladimir N. Serežkin. Linear groups generated by transvections (Russian). *Izv. Akad. Nauk SSSR*, 40(1):26–49, 1976.

[35] Yuri Zarhin. Endomorphisms of abelian varieties and points of finite order in characteristic p (Russian). *Mat. Zametki*, 21(6):737–744, 1977.

[36] Yuri Zarhin. A finiteness theorem for unpolarized abelian varieties over number fields with prescribed places of bad reduction. *Invent. Math.*, 79:309–321, 1985.

[37] Yuri Zarhin. Endomorphisms and Torsion of abelian varieties. *Duke Math. Jour.*, 54(1):131–145, 1987.