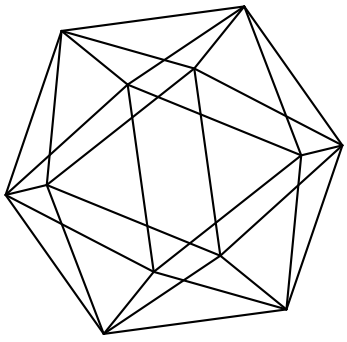
Max-Planck-Institut für Mathematik
Bonn

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

by

Sara Arias-de-Reyna
Wojciech Gajda
Sebastian Petersen



Max-Planck-Institut für Mathematik
Preprint Series 2010 (89)

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

Sara Arias-de-Reyna
Wojciech Gajda
Sebastian Petersen

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

Institut für Experimentelle Mathematik
45326 Essen
Germany

Department of Mathematics
Adam Mickiewicz University
61614 Poznań
Poland

Universität der Bundeswehr
85577 Neubiberg
Germany

MPIM 10-89

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
and
Max Planck Institut
für Mathematik
53072 Bonn, Germany

Sebastian Petersen
Universität der Bundeswehr
85577 Neubiberg,
Germany
sebastian.petersen@unibw.de

October 12, 2010

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. We prove that all abelian varieties over finitely generated fields with the endomorphism ring $\mathbb{Z}$ and semistable reduction of toric dimension one at a place of the base field have big monodromy. In addition, we prove part (a) of the Geyer-Jarden conjecture for abelian varieties over finitely generated transcedental extensions of $\mathbb{Q}$ with endomorphism ring $\mathbb{Z}$ and of dimension 2, 6 or odd.

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

Contents

Introduction

Let A be a polarized abelian variety defined over a finitely generated field K. Denote by $\tilde{K}$ (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 $A(\tilde{K})$ is a divisible group with an infinite torsion part $A(\tilde{K})_{\rm tor}$ and $A(\tilde{K})$ 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 $\tilde{K}$. For example, Ribet in [25] and Zarhin in [36] 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 $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_e)$ in the group $G_K^e = G_K \times G_K \times \dots \times G_K$, we denote by $K_{\rm sep}(\sigma)$ the subfield in $K_{\rm sep}$ fixed by $\sigma_1, \sigma_2, \dots, \sigma_e$. 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 [21] on the rank of $A(K_{\rm sep}(\sigma))$ (cf. [1], [11] 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 [9] Geyer and Jarden proposed the following conjecture on the torsion part of $A(K_{\rm sep}(\sigma))$.

Conjecture A *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 [17] 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 Conjecture A is known for elliptic curves [9]. Part (b) holds true provided $\mathrm{char}(K) = 0$ (see [17]). Geyer and Jarden [10] recently proved the following result towards part (a): *If K is a number field, then there is a finite extension E/K such that part (a) holds true for all σ inside a subset of G_E of full measure.* The field E can be taken to be equal to K provided $\mathrm{End}(A) = \mathbb{Z}$ and $\dim(A) = 2, 6$ or odd and also in some other special cases. 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 Conjecture A are open and part (a) is open over a finitely generated transcendental extension of $\mathbb{Q}$.

In this paper we prove Conjecture A for abelian varieties with big monodromy. To formulate our first 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_ℓ:$A[\ell] \times A[\ell] \to \mu_\ell$ 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 first main result of our paper is the following

Theorem B *[cf. Thm. 6.1, Thm. 7.1] Let K be a finitely generated field and A/K an abelian variety with big monodromy. Then the Conjecture A of Geyer and Jarden holds true for A/K.*

Surprisingly enough, the most difficult to prove is the case (a) of the Conjecture A 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 $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ (cf. Appendix A) which was modeled after a construction of subsets $S'(\ell)$ in $\mathrm{Sl}_2(\mathbb{F}_\ell)$ in Section 3 of the classical paper [9] of Geyer and Jarden.

In the light of Theorem B we are interested in computing monodromy groups for families of abelian varieties. Certainly, the most prominent result of this type is the classical theorem of Serre (cf. Theorem 3.9 below): *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.* In this paper, in addition to varieties such as in the theorem of Serre, we consider monodromies for abelian varieties over finitely generated fields which have been recently investigated by Chris Hall [14], [15]. 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.

In the special case, when $K = F(t)$ is a rational function field over another finitely generated field, it has been shown by Hall that certain hyperelliptic Jacobians have big monodromy; namely the Jacobians J_C of hyperelliptic curves C/K with affine equation $C : Y^2 = (X - t)f(X)$, where $f \in F[X]$ is a monic squarefree polynomial of even degree ≥ 4 (cf. [14, Theorem 5.1]). Furthermore, Hall has proved recently [15] the following theorem which in our notation reads: *If K is a* global *field, then every abelian variety A/K of Hall type has big monodromy.* We strengthen these results as follows.

Theorem C *[cf. Thm. 3.6] If K is a finitely generated field (of arbitrary characteristic) and A/K is an abelian variety of Hall type, then A/K has big monodromy.*

Our proof of Theorem C follows Hall's proof of [15] to some extent, e.g., we have borrowed a group theory result from [15] (cf. Theorem 3.4). In addition to that we apply results on finite generation of Galois groups of certain division fields of abelian varieties, which are gathered in Section 3 of the paper. Furthermore, at a technical point in the case $\mathrm{char}(K) = 0$, we perform a tricky reduction argument (described in detail in Section 4) at a "place" of K whose residue field is a number field.

Combination of Theorem B, Theorem C and Serre's theorem mentioned above leads to the following

Theorem D *[cf. Cor. 6.4, Cor. 7.2] Let A be an abelian variety over a finitely generated 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 Conjecture A holds true for A/K.

As yet another application of our monodromy computations, we obtain the following result on endomorphism rings and simplicity of fibres in certain families of abelian varieties. If K is a finitely generated transcendental extension of another field F and A/K is an abelian variety, then we call A *weakly isotrivial with respect to* F, if there is an abelian variety $B/\tilde{F}$ and an $\tilde{K}$-isogeny $B_{\tilde{K}} \to A_{\tilde{K}}$.

Theorem E *[cf. Thm. 5.2] Let F be a finitely generated field and $K = F(t)$ the function field of $\mathbb{P}_1/F$. Let A/K be an abelian variety. Let $U \subset \mathbb{P}_1$ be an open subscheme such that A extends to an abelian scheme $\mathcal{A}/U$. For $u \in U(F)$ denote by A_u/F the corresponding special fiber of $\mathcal{A}$. Assume that A is not weakly isotrivial with respect to F and that either of the conditions i) or ii) listed below 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 sets:

$$X_1 := \{u \in U(F) \mid \quad \mathrm{End}(A_u) \neq \mathbb{Z}\}$$

and

$$X_2 := \{u \in U(F) \mid \quad A_u/F \text{ is not geometrically simple}\}$$

are finite.

Note that Ellenberg, Elsholtz, Hall and Kowalski proved Theorem E in the special case when A is the Jacobian variety of the hyperelliptic curve given by the affine equation $Y^2 = (X - t)f(X)$, with $f \in F[X]$ squarefree and monic of even degree ≥ 4 (cf. [5, Theorem 8]). It is the case, where the monodromy of A is known by [14, Theorem 5.1]. We obtain part (i) of Theorem E as a consequence of our monodromy Theorem C, our Proposition 5.1 below and also Propositions 4 and 7 of [5]. In order to prove (ii) we use Serre's Theorem 3.9 instead of Theorem C.

We warmly thank Gerhard Frey, Dieter Geyer, Cornelius Greither and Moshe Jarden for conversations and useful comments on the topic of this paper. The mathematical content of the present work has been much influenced by seminal results of J.-P. Serre contained in [27], [28], [29], [30] and by the inspiring paper [15] of C.Hall. We acknowledge this with pleasure.

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.

Let X be a scheme. For $x \in X$ we denote by $k(x)$ the residue field at x. If X is integral, then $R(X)$ stands for the function field of X, that is, for the residue field at the generic point of X. If X happens to be a scheme of finite type over a base field F, then we often write $F(x)$ instead of $k(x)$ and $F(X)$ instead of $R(X)$. We say that a scheme X is a Dedekind scheme, if it is noetherian, connected and covered by spectra of Dedekind rings. In this case $\mathcal{O}_{X,x}^h$ denotes the henselization of the local ring $\mathcal{O}_{X,x}$ at a closed point $x \in X$.

If K is a field, then we denote by K_{sep} (resp. $\tilde{K}$) the separable (resp. algebraic) closure of K and by G_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. For an abelian variety A/K we let $\mathrm{End}_K(A)$ be the ring of all K-endomorphisms of A. We denote by $\mathrm{End}(A) := \mathrm{End}_{\tilde{K}}(A_{\tilde{K}})$ the *absolute* endomorphism ring.

If Γ is an object in an abelian category and $n \in \mathbb{Z}$, then $n_\Gamma : \Gamma \to \Gamma$ is the morphism "multiplication by n" and $\Gamma[n]$ is the kernel of n_Γ. Recall that there is an equivalence of categories between the category of finite étale group schemes over K and the category of finite (discrete) G_K-modules, where we attach $\Gamma(K_{\mathrm{sep}})$ to a finite étale group scheme Γ/K. For such a finite étale group scheme Γ/K we sometimes write just Γ instead of $\Gamma(K_{\mathrm{sep}})$, at least in situations where we are sure that this does not cause any confusion. For non-étale Γ/K we distinguish carefully between the scheme Γ and its geometric points. For example, if A/K is an abelian variety and n an integer coprime to $\mathrm{char}(K)$, then we often write $A[n]$ rather than $A(K_{\mathrm{sep}})[n]$. Furthermore we put $A[n^\infty] := \bigcup_{i \in \mathbb{N}} A[n^i]$.

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 $\ell \geq \ell_0$.

Now let S be a Dedekind scheme with function field $K = R(S)$ and A/K an abelian variety. Denote by $\mathcal{A} \to S$ the Néron model (cf. [2]) of A. For $s \in S$ let $A_s := \mathcal{A} \times_S \mathrm{Spec}(k(s))$ be the corresponding fiber. Recall that we say that A has *good reduction at* s provided A_s is an abelian variety. In general, we denote by A_s° the connected component of A_s. If T is a maximal torus in A_s°, then $\dim(T)$ does not depend on the choice of T [13, IX.2.1] and we call $\dim(T)$ the *toric dimension* of the reduction A_s of A at s. Finally recall that one says that A has *semi-stable reduction at* s, if A_s° is an extension of an abelian variety by a torus.

We shall also need the following connections between the reduction type of A and properties of the Galois representations attached to A. Let s be a closed point of S. The valuation v attached to s admits an extension to the separable closure K_{sep}; we choose such an extension $\overline{v}$ and denote by $D(\overline{v})$ the corresponding decomposition group. This is the absolute Galois group of the quotient field $K_s = Q(\mathcal{O}_{S,s}^h)$ of the henselization of the valuation ring $\mathcal{O}_{S,s}$ of v. Hence the results mentioned in [13, I.0.3] for the henselian case carry over to give the following description of $D(\overline{v})$: If $I(\overline{v})$ is the kernel of the canonical map $D(\overline{v}) \to G_{k(s)}$ defined by $\overline{v}$, then $D(\overline{v})/I(\overline{v}) \cong G_{k(s)}$. Let p be the characteristic of the residue field $k(s)$ (p is zero or a prime number). $I(\overline{v})$ has a maximal pro-p subgroup $P(\overline{v})$ ($P(\overline{v}) = 0$ if $p = 0$) and

$$I(\overline{v})/P(\overline{v}) \cong \varprojlim_{n \notin p\mathbb{Z}} \mu_n(k(s)_{\mathrm{sep}}) \cong \prod_{\ell \neq p \text{ prime}} \mathbb{Z}_\ell(1).$$

Hence the maximal pro-ℓ-quotient $I_\ell(\overline{v})$ of $I(\overline{v})$ is isomorphic to $\mathbb{Z}_\ell(1)$, if $\ell \neq p$ is a prime.

Theorem 1.1 (Grothendieck, [13, IX.3.5, IX.3.6]) *Let $\ell \neq p$ be a prime number.*

a) The following two conditions are equivalent:

i) A has semistable reduction at s.

ii) The restriction $\rho_{T_\ell A}|I(\overline{v})$ factors through the maximal pro-ℓ quotient $I_\ell(\overline{v})$ of $I(\overline{v})$ (in particular $\rho_{T_\ell A}(P(\overline{v})) = \{Id\}$), and if g is a generator of $I_\ell(\overline{v})$, then $(\rho_{T_\ell A}(g) - Id)^2 = 0$.

b) There is a finite separable extension K'/K such that $A_{K'}$ has semistable reduction in all points of the normalization S' of S in K'.

Proposition 1.2 *Let $\ell \neq p$ be a prime number. Assume that A has semi-stable reduction at s.*

a) The image $\rho_{A[\ell]}(P(\overline{v})) = \{Id\}$ and $\rho_{A[\ell]}(I(\overline{v}))$ is a cyclic ℓ-group.

b) Let g be a generator of $\rho_{A[\ell]}(I(\overline{v}))$. Then $(g - Id)^2 = 0$.

c) Assume that ℓ does not divide the order of the component group of A_s. The toric dimension of A at s is equal to $2\dim(A) - \dim_{\mathbb{F}_\ell}(\mathrm{Eig}(g,1))$ if $\mathrm{Eig}(g,1) = \ker(g - Id)$ is the eigenspace of g at 1.

Proof. Part a) and b) are immediate consequences of Theorem 1.1.

Assume from now on that ℓ does not divide the order of the component group of A_s. This assumption implies $A_s^\circ[\ell] \cong A_s[\ell]$.

As we assumed A to be semi-stable at s, there is an exact sequence

$$0 \to T \to A_s^\circ \to B \to 0$$

where T is a torus and B is an abelian variety and $\dim(T)+\dim(B) = \dim(A_s) = \dim(A)$. Now $\dim_{\mathbb{F}_\ell}(T[\ell]) = \dim(T)$ and $\dim_{\mathbb{F}_\ell}(B[\ell]) = 2\dim(B) = 2\dim(A) - 2\dim(T)$. Taking into account that we have an exact sequence

$$0 \to T[\ell] \to A_s^\circ[\ell] \to B[\ell] \to 0$$

(note that $T(\tilde{k}) \cong (\tilde{k}^\times)^{\dim(T)}$ is divisible by ℓ), we find the relation $\dim_{\mathbb{F}_\ell}(A_s[\ell]) = \dim_{\mathbb{F}_\ell}(A_s^\circ[\ell]) = 2\dim(A) - \dim(T)$. This implies c), because $A_s[\ell] = A[\ell]^{I(\overline{v})}$ ([31, p. 495]) and obviously $A[\ell]^{I(\overline{v})} = \mathrm{Eig}(g,1)$. □

In general, if V is a finite dimensional vector space over $\mathbb{F}_\ell$, and $g \in \mathrm{End}_{\mathbb{F}_\ell}(V)$, then one defines $\mathrm{drop}(g) = \dim(V) - \dim(\mathrm{Eig}(g,1))$. One calls g a *transvection*, if it is unipotent of drop 1. We shall say that an abelian variety A over a field K is *of Hall type*, provided $\mathrm{End}(A) = \mathbb{Z}$ and there is a discrete valuation v on K such that A has semistable reduction of toric dimension 1 at v (i.e. at the maximal ideal of the discrete valuation ring of v). We have thus proved the following

Proposition 1.3 *If A is an abelian variety of Hall type over a finitely generated field K, then there is a constant ℓ_0 such that $\mathcal{M}_K(A[\ell])$ contains a transvection for every prime number $\ell \geq \ell_0$.*

2 Finiteness properties of division fields

If A is an abelian variety over a field K (of arbitrary characteristic) and $p = \mathrm{char}(K)$, then we denote by $A_{\neq p}$ the group of points in $A(K_{\mathrm{sep}})$ of order prime

to p. Then

$$K(A_{\neq p}) = \prod_{\ell \neq p \ prime} K(A[\ell^\infty]) = \bigcup_{n \notin p\mathbb{Z}} K(A[n]).$$

If $p = 0$, then $K(A_{\neq p}) = K(A_{\rm tor})$. In this section we prove among other things: If K is finitely generated of positive characteristic, then $G(K(A_{\neq p})/K)$ is a finitely generated profinite group. We follow preprint [7] as far as Lemmas 2.1 and 2.2 are concerned, providing details of proofs for the reader's convenience.

In this section, a *function field of n variables* over a field F will be a finitely generated field extension E/F of transcendence degree n. As usual we call such a function field E/F of n variables *separable* if it has a separating transcendency base.

Lemma 2.1 *Let F be a separably closed field and K/F a function field of one variable. Assume that K/F is separable. Put $p = \mathrm{char}(F)$. Let A/K be an abelian variety. Then $G(K(A_{\neq p})/K)$ is a finitely generated profinite group.*

Proof. There is a smooth projective curve C/F with function field K. By Grothendieck's Theorem 1.1 there is a finite separable extension K'/K such that $A_{K'}$ has semistable reduction at all points of the normalization C' of C in K'. We may assume that K'/K is Galois.

Let $S' \subset C'$ be the finite set of closed points where $A_{K'}$ has bad reduction. Then for every $\ell \neq p$ the extension $K'(A[\ell^\infty])/K'$ is tamely ramified at all points of C' by Theorem 1.1 and unramified outside S' by the criterion of Néron-Ogg-Shafarevich [31, Thm. 1]. Hence $K'(A_{\neq p})$ is contained in the maximal tamely ramified extension $K'_{S',tr}$ of K' which is unramified outside S'. The Galois group $G(K'_{S',tr}/K')$ is finitely generated by [12, Corollaire XIII.2.12]. Hence $G(K'(A_{\neq p})/K')$ is finitely generated as a quotient of $G(K'_{S',tr}/K')$. Furthermore there is an exact sequence

$$1 \to G(K'(A_{\neq p})/K') \to G(K(A_{\neq p})/K) \to G(K'/K)$$

and $G(K'/K)$ is finite. Hence $G(K(A_{\neq p})/K)$ is finitely generated as desired.□

Lemma 2.2 *Let F be a field and K/F a function field of one variable. Assume that K/F is separable. Let $p = \mathrm{char}(F)$. Let A/K be an abelian variety. Let F' be the algebraic closure of F in $K(A_{\neq p})$. Then $G(K(A_{\neq p})/F'K)$ is a finitely generated profinite group.*

Proof. $F_{\rm sep}$ is F'-linearly disjoint from $K(A_{\neq p})$. Hence $F_{\rm sep}K$ is $F'K$-linearly disjoint from $K(A_{\neq p})$. This implies

$$G(K(A_{\neq p})/F'K) \cong G(F_{\rm sep}K(A_{\neq p})/F_{\rm sep}K),$$

and the latter group is finitely generated by Lemma 2.1 above. □

Lemma 2.3 *Let (K, v) be a discrete valued field, A/K an abelian variety with good reduction at v, n an integer coprime to the residue characteristic of v, $L = K(A[n])$ and w an extension of v to L. Denote the residue field of v (resp. w) by $k(v)$ (resp. $k(w)$). Let $A_v/k(v)$ be the reduction of A at v. Then $k(w) = k(v)(A_v[n])$.*

Proof. Let R be the valuation ring of v and $S = \mathrm{Spec}(R)$. Let $\mathcal{A} \to S$ be an abelian scheme with generic fibre A. Then $\mathcal{A}[n]$ is a finite étale group scheme over S. Let T be the normalization of S in L. The restriction map $r : A[n](L) \cong \mathcal{A}[n](T) \to A_v[n](k(w))$ is injective [31] and $|A[n](L)| = n^{2\dim(A)}$. Hence r is an isomorphism and we may identify $A[n]$ with $A_v[n]$. The fact that the whole n-torsion of A_v is defined over $k(w)$ implies that $k(v)(A_v[n]) \subset k(w)$. We have to prove the other inclusion: Let $D(w)$ be the decomposition group of the prime w over v, i.e. the stabilizer of w under the action of $G(L/K)$. Then $D(w) \to G(k(w)/k(v))$ is an isomorphism by the criterion of Néron-Ogg-Shafarevich. As $D(w) \to Aut(A[n])$ is injective, it follows that $G(k(w)/k(v)) \to Aut(A_v[n])$ is injective as well. This implies that $k(v)(A_v[n]) = k(w)$. □

Definition 2.4 *We shall say in the sequel that a field K has property $\mathcal{F}$, if $G(K'(A_{\neq p})/K')$ is a* finitely generated *profinite group for every finite separable extension K'/K and every abelian variety A/K'.*

Lemma 2.5 *Let F be a field that has property $\mathcal{F}$. Let $p = \mathrm{char}(F)$. Let K/F be a function field of one variable. Assume that K/F is separable. Then K has property $\mathcal{F}$.*

Proof. We have to show that $G(K'(A_{\neq p})/K')$ is finitely generated for every finite separable extension K'/K and every abelian variety A/K'. But if K'/K is a finite separable extension, then K'/F is a separable function field of one variable again. Hence it is enough to prove that $G(K(A_{\neq p})/K)$ is finitely generated for every abelian variety A/K.

Let A/K be an abelian variety. Let F_0 be the algebraic closure of F in K. Then K/F_0 is a regular extension. Let C/F_0 be a smooth curve with function field K and such that A has good reduction at all points of C. There is a finite Galois extension F_1/F_0 such that $C(F_1) \neq \emptyset$. If we put $K_1 := F_1K$, then K_1/F_1 is regular. Furthermore there is an exact sequence

$$1 \to G(K_1(A_{\neq p})/K_1) \to G(K(A_{\neq p})/K) \to G(K_1/K)$$

and $G(K_1/K)$ is finite. If we prove that $G(K_1(A_{\neq p})/K_1)$ is finitely generated, then it follows that $G(K(A_{\neq p})/K)$ is finitely generated as well. Hence we may assume that $K_1 = K$, i.e. that K/F is regular and that $C(F) \neq \emptyset$.

Choose a point $c \in C(F)$ and denote by A_c/F the (good) reduction of A at c. As in Lemma 2.2 denote by F' the algebraic closure of F in $K(A_{\neq p})$.

Claim. $F' \subset F(A_{c,\neq p})$.

Let $x \in F'$. Then x is algebraic over F and $x \in K(A[n])$ for some n which is coprime to p. If F_n denotes the algebraic closure of F in $K(A[n])$, then $x \in F_n$. Let w be the extension to $K(A[n])$ of the valuation attached to c. Then $k(w) = F(A_c[n])$ by Lemma 2.3. Obviously $F_n \subset k(w)$. Hence $x \in F(A_c[n]) \subset F(A_{c,\neq p})$. This finishes the proof of the Claim.

The profinite group $G(F(A_{c,\neq p})/F)$ is finitely generated, because F has property $\mathcal{F}$ by assumption. Hence its quotient $G(F'/F)$ is finitely generated as well. Note that $G(F'K/K) = G(F'/F)$. On the other hand $G(K(A_{\neq p})/F'K)$ is finitely generated by Lemma 2.2. From the exact sequence

$$1 \to G(K(A_{\neq p})/F'K) \to G(K(A_{\neq p})/K) \to G(F'K/K) \to 1$$

we see that $G(K(A_{\neq p})/K)$ is finitely generated as desired. □

Proposition 2.6 *Let F be a perfect field which has property $\mathcal{F}$. Then every finitely generated extension K of F has property $\mathcal{F}$.*

Proof. We prove this by induction on $\mathrm{trdeg}(K/F)$. If $\mathrm{trdeg}(K/F) = 0$ there is nothing to prove. Assume $\mathrm{trdeg}(K/F) = d \geq 1$. We may assume that every finitely generated extension F' of F with $\mathrm{trdeg}(F'/F) < d$ has property $\mathcal{F}$.

Choose a separating transcendency base $(x_1, \cdots, x_d)$ for K/F. Put $F' := K(x_1, \cdots, x_{d-1})$. Then F' has property $\mathcal{F}$ by the induction hypothesis. Furthermore K/F' is a function field of one variable and K/F' is separable. Hence Lemma 2.5 implies that K has property $\mathcal{F}$. □

Corollary 2.7 *Let K be a finitely generated field* of positive characteristic *or K be a function field over an algebraically closed field of arbitrary characteristic. Then K has property $\mathcal{F}$. In particular $G(K(A_{\neq p})/K)$ is finitely generated for every abelian variety A/K.*

Proof. A finite field $\mathbb{F}$ is perfect. It has property $\mathcal{F}$, because its absolute Galois group is procyclic. An algebraically closed field is perfect and has property $\mathcal{F}$, because its absolute Galois group is the trivial group. Now in both cases K is a function field over a perfect field which has property $\mathcal{F}$. □

Remark 2.8 *A finitely generated field K of characteristic zero does* not *have property $\mathcal{F}$. In fact, if A/K is principally polarized abelian variety, then by the existence of the Weil pairing $K(A_{\mathrm{tor}}) \supset K(\mu_\infty)$, and plainly $G(K(\mu_\infty)/K)$ is* not *finitely generated, when K is a finitely generated extension of $\mathbb{Q}$.*

3 Monodromy Computations

Let K be a field and A/K an abelian variety. We begin with the question whether $A[\ell]$ is a simple G_K-module for sufficiently large ℓ. In the cases we

need to consider, this question has an affirmative answer due to the following classical fact (cf. [6, p. 118, p. 204], [34], [35],[22]).

Theorem 3.1 (Faltings, Zarhin) *Let K be a finitely generated field and A/K an abelian variety. Then there is a constant $\ell_0 > \mathrm{char}(K)$ such that the $\mathbb{F}_\ell[G_K]$-module $A[\ell]$ is semisimple and the canonical map $\mathrm{End}_K(A) \otimes \mathbb{F}_\ell \to \mathrm{End}_{\mathbb{F}_\ell}(A[\ell])$ is injective with image $\mathrm{End}_{\mathbb{F}_\ell[G_K]}(A[\ell])$ for all primes $\ell \geq \ell_0$.*

Proposition 3.2 *Let A be an abelian variety over a finitely generated field K. Assume that $\mathrm{End}_K(A) = \mathbb{Z}$. Then there is a constant ℓ_0 such that $A[\ell]$ is a simple $\mathbb{F}_\ell[G_K]$-module for all primes $\ell \geq \ell_0$.*

Proof. By Theorem 3.1 there is a constant ℓ_0 such that $A[\ell]$ is a semisimple $\mathbb{F}_\ell[G_K]$-module with $\mathrm{End}_{\mathbb{F}_\ell[G_K]}(A[\ell]) = \mathbb{F}_\ell Id$ for every prime $\ell \geq \ell_0$. This is only possible if $A[\ell]$ is a simple $\mathbb{F}_\ell[G_K]$-module for all primes $\ell \geq \ell_0$. □

We need some notation in order to explain a theorem of Raynaud that will be of importance later. Let $E/\mathbb{F}_p$ be a finite field extension with $|E| = p^d$ and $F/\mathbb{F}_p$ an algebraic extension. Denote by $\mathrm{Emb}(E, \tilde{F})$ the set of all embeddings $E \to \tilde{F}$. If $i \in \mathrm{Emb}(E, \tilde{F})$ is one such embedding, then $\mathrm{Emb}(E, \tilde{F}) = \{i^{p^a} : a \in \{0, \cdots, d-1\}\}$. Furthermore the restriction $i|E^\times$ lies in $\mathrm{Hom}(E^\times, \tilde{F}^\times)$. For every character $\chi \in \mathrm{Hom}(E^\times, F^\times)$ there is a unique $m \in \{0, \cdots, p^d - 2\}$ such that $\chi = (i|E^\times)^m$. Expanding m p-adically, we see that there is a unique function $e : \mathrm{Emb}(E, \tilde{F}) \to \{0, \cdots, p-1\}$ such that

$$\chi = \prod_{j \in \mathrm{Emb}(E, \tilde{F})} (j|E^\times)^{e(j)},$$

and such that $e(j) < p - 1$ for some $j \in \mathrm{Emb}(E, \tilde{F})$. We define $\mathrm{amp}(\chi) := \max(e(j) : j \in \mathrm{Emb}(E, \tilde{F}))$ to be the *amplitude of the character* χ. Let $\rho : E^\times \to \mathrm{Aut}_{\mathbb{F}_p}(V)$ be a representation of $E^\times$ on a finite dimensional $\mathbb{F}_p$-vector space V. If V is a *simple* $\mathbb{F}_p[E^\times]$-module, then there is a finite field F_V with $|F_V| = |V|$ and a structure of 1-dimensional F_V-vector space on V such that ρ factors through a character $\chi_\rho : E^\times \to F_V^\times$. We then define $\mathrm{amp}(V) := \mathrm{amp}(\rho) := \mathrm{amp}(\chi_\rho)$. In general V is a semisimple $\mathbb{F}_p[E^\times]$-module by Maschke's theorem, and we can write $V = V_1 \oplus \cdots \oplus V_t$ as a direct sum of simple $\mathbb{F}_p[E^\times]$-modules and define $\mathrm{amp}(V) := \mathrm{amp}(\rho) := \max(\mathrm{amp}(V_i) : i = 1, \cdots, t)$ to be the *amplitude of the representation* ρ. With this terminology in mind, we can state Raynaud's theorem in the following way.

Theorem 3.3 (Raynaud [24], [26, p. 277]) *Let A be an abelian variety over a number field K. Let v be a place of K with residue characteristic p. Let e be the ramification index of $v|\mathbb{Q}$. Let w be an extension of v to $K(A[p])$. Let I be the inertia group of $w|v$ and P the p-Sylow subgroup of I. Let $C \subset I$ be a subgroup that maps isomorphically onto I/P. Then there is a finite extension $E/\mathbb{F}_p$ and a surjective homomorphism $E^\times \to C$ such that the resulting representation*

$$\rho : E^\times \to C \to \mathrm{Aut}_{\mathbb{F}_p}(A[p])$$

has amplitude $\mathrm{amp}(\rho) \leq e$.

The technical heart of our monodromy computations is the following group theoretical result, which can be extracted from the work of C. Hall [14], [15].

Theorem 3.4 *Let $\ell > 2$ be a prime, let (V, e_V) be a finite-dimensional symplectic space over $\mathbb{F}_\ell$ and M a subgroup of $\Gamma := \mathrm{GSp}(V, e_V)$. Assume that M contains a transvection and that V is a simple $\mathbb{F}_\ell[M]$-module. Denote by R the subgroup of M generated by the transvections in M.*

a) Then there is a non-zero symplectic subspace $W \subset V$, which is a simple $\mathbb{F}_\ell[R]$-module, such that the following properties hold true:

i) Let $H = \mathrm{Stab}_M(W)$. There is a orthogonal direct sum decomposition $V = \bigoplus_{g \in M/H} gW$. In particular $|M/H| \leq \dim(V)$.

ii) $R \cong \prod_{g \in M/H} \mathrm{Sp}(W)$ and $N_\Gamma(R) \cong \prod_{g \in M/H} \mathrm{GSp}(W) \rtimes \mathrm{Sym}(M/H)$.

iii) $R \subset M \subset N_\Gamma(R)$.

Denote by $\varphi : N_\Gamma(R) \to \mathrm{Sym}(M/H)$ the projection.

b) Let $e \in \mathbb{N}$. Let $E/\mathbb{F}_\ell$ be a finite extension and $\rho : E^\times \to M \subset \mathrm{GSp}(V, e_V)$ a homomorphism such that the corresponding representation of $E^\times$ on V has amplitude $\mathrm{amp}(\rho) \leq e$. If $\ell > \dim(V)e + 1$, then $\varphi(\rho(E^\times)) = \{1\}$.

Hall's proof in [14], [15] adresses a slightly less general situation. We will present a self-contained proof of Theorem 3.4 in Appendix B.

Remark 3.5 *Assume that in the situation of Theorem 3.4 the module V is a simple $\mathbb{F}_\ell[\ker(\varphi) \cap M]$-module. Then V is in particular a simple $\mathbb{F}_\ell[\ker(\varphi)]$-module and $\ker(\varphi) = \prod_{g \in M/H} \mathrm{GSp}(W)$. This is only possible if $M = H$, $V = W$ and $R = \mathrm{Sp}(V, e) \subset M$.*

We now state the main result of this section.

Theorem 3.6 *Let K be a finitely generated field. Let (A, λ) be a polarized abelian variety over K of Hall type. Then (A, λ) has big monodromy.*

The case where K is a global field is due to Hall (cf. [15]) and we follow his line of proof to some extent, but we need additional arguments in order to make things work in the more general situation. The proof will occupy almost the rest of this section.

There is a constant $\ell_0 > \max(\deg(\lambda), \mathrm{char}(K))$ such that the following holds true for all primes $\ell \geq \ell_0$:

1. The subgroup $\mathcal{M}_K(A[\ell])$ of $\mathrm{GSp}(A[\ell], e_\ell^\lambda)$ contains a transvection. Denote by R_ℓ the subgroup of $\mathcal{M}_K(A[\ell])$ generated by the transvections in $\mathcal{M}_K(A[\ell])$ (cf. Proposition 1.3).

2. $A[\ell]$ is a simple $\mathbb{F}_\ell[G_K]$-module (cf. Proposition 3.2).

Now Hall's group theory result (cf. Theorem 3.4) gives - for every prime $\ell \geq \ell_0$ - a non-zero symplectic subspace $W_\ell \subset A[\ell]$, which is simple as a $\mathbb{F}_\ell[R_\ell]$-module such that the properties i), ii) and iii) of Theorem 3.4 are satisfied. Let H_ℓ be the stabilizer of W_ℓ under the action of $\mathcal{M}_K(A[\ell])$. Define $M_\ell := \mathcal{M}_K(A[\ell])$ and $\Gamma_\ell := \mathrm{GSp}(A[\ell], e_\ell^\lambda)$. Then

$$\prod_{M_\ell/H_\ell} \mathrm{Sp}(W_\ell, e_\ell^\lambda) \cong R_\ell \subset M_\ell \subset N_{\Gamma_\ell}(R_\ell) = \prod_{M_\ell/H_\ell} \mathrm{Sp}(W_\ell, e_\ell^\lambda) \rtimes \mathrm{Sym}(M_\ell/H_\ell),$$

and we denote by $\varphi_\ell : N_{\Gamma_\ell}(R_\ell) \to \mathrm{Sym}(M_\ell/H_\ell)$ the projection. We have the following property (cf. Remark 3.5):

If $A[\ell]$ is a simple $\mathbb{F}_\ell[\ker(\varphi_\ell) \cap M_\ell]$-module for some prime $\ell \geq \ell_0$, then $M_\ell = H_\ell$, $W_\ell = A[\ell]$ and $M_\ell \supset \mathrm{Sp}(A[\ell], e_\ell^\lambda)$ for this prime ℓ.

We denote by N_ℓ the fixed field inside K_{sep} of the preimage $\rho_{A[\ell]}^{-1}(M_\ell \cap \ker(\varphi_\ell))$, where $\rho_{A[\ell]} : G_K \to \Gamma_\ell$ is the mod-ℓ representation attached to A. Then N_ℓ is an intermediate field of $K(A[\ell])/K$ which is Galois over K, and $G(N_\ell/K)$ is isomorphic to the subgroup $\varphi_\ell(M_\ell)$ of $\mathrm{Sym}(M_\ell/H_\ell)$. In particular $[N_\ell : K] \leq (2\dim(A))!$ is bounded independently of ℓ. If we denote by $N := \prod_{\ell \geq \ell_0 \text{ prime}} N_\ell$ the corresponding composite field, then $G_N = \bigcap_{\ell \geq \ell_0 \text{ prime}} G_{N_\ell}$. Hence the following property holds true.

If $A[\ell]$ is simple as the $\mathbb{F}_\ell[G_N]$-module for some prime $\ell \geq \ell_0$, then $M_\ell \supset \mathrm{Sp}(A[\ell], e_\ell^\lambda)$ for this prime ℓ. $(*)$

Proof of Theorem 3.6 in the special case $\mathrm{char}(K) > 0$. If $\mathrm{char}(K) > 0$, then the Galois group $G(K(A_{\neq p})/K)$ ($p := \mathrm{char}(K)$) is finitely generated, because K then has property $\mathcal{F}$ by Corollary 2.7. Furthermore N_ℓ is an intermediate field of $K(A_{\neq p})/K$ which is Galois over K and with $[N_\ell : K]$ bounded independently of ℓ. Hence N/K must be finite. In particular N is finitely generated. A second application of the result of Faltings and Zarhin (cf. Proposition 3.2) yields a constant $\ell_1 \geq \ell_0$ such that $A[\ell]$ is a simple $\mathbb{F}_\ell[G_N]$-module for all primes $\ell \geq \ell_0$. Hence A has big monodromy by $(*)$. □

To finish the proof of Theorem 3.6 we assume for the rest of the proof that $\mathrm{char}(K) = 0$. We shall prove that N/K is finite also in that case, but the proof of this fact is more complicated, because now K is *not* $\mathcal{F}$-finite (cf. Remark 2.8). We briefly sketch the main steps in the proof, before we go into the details: The first and hardest step is to show that the algebraic closure L of $\mathbb{Q}$ in N is a *finite* extension of $\mathbb{Q}$. In order to achieve this we will construct a finite extension $L'/\mathbb{Q}$ such that some L'-rational "place" of KL' splits up completely into L'-rational "places" of $N_\ell L'$ for every sufficiently large prime ℓ. We use this to show that $G(NL/KL) \cong G(NL_{\mathrm{sep}}/KL_{\mathrm{sep}})$ and the fact that the latter group can be proved to be finite, because KE_{sep} is $\mathcal{F}$-finite (unlike K itself). This suffices to prove that N/K is finite. Once we know this, we shall proceed as in the positive characteristic case above.

We now go into the details. Let F be the algebraic closure of $\mathbb{Q}$ in K. Then F is a number field. Let S be a smooth affine F-variety with function field K such that A extends to an abelian scheme $\mathcal{A}$ over S with generic fibre A (i.e. such that A has good reduction along S). Let S_ℓ be the normalization of S in N_ℓ and let S'_ℓ be the normalization of S_ℓ in $K(A[\ell])$. Then $S'_\ell \to S_\ell \to S$ are finite étale covers. (Note that $\mathrm{char}(F(s)) = 0$ for every point $s \in S$.) In particular S'_ℓ and S_ℓ are smooth F-schemes. (Compare the diagram below.)

Fix a geometric point $P \in S(F_{\mathrm{sep}})$ and denote by $A_P := \mathcal{A} \times_S \mathrm{Spec}(F(P))$ the corresponding special fibre of $\mathcal{A}$. Then A_P is an abelian variety over the number field $F(P)$. Fix for every $\ell \geq \ell_0$ a geometric point $Q_\ell \in S_\ell(F_{\mathrm{sep}})$ over P and a geometric point $Q'_\ell \in S'_\ell(F_{\mathrm{sep}})$ over Q_ℓ. Then $F(Q'_\ell)/F(Q_\ell)$ and $F(Q_\ell)/F(P)$ are finite extensions of number fields. Note that $F(Q'_\ell) = F(P)(A_P[\ell])$ by Lemma 2.3. Denote by $\mathcal{O}$ (resp. $\mathcal{O}_\ell$, resp. $\mathcal{O}'_\ell$) the integral closure of $\mathbb{Z}$ in $F(P)$ (resp. in $F(Q_\ell)$, resp. in $F(Q'_\ell)$). For every prime $\ell \geq \ell_0$ we have the following diagram on the level of schemes

$$\begin{array}{ccccccc}
 & & \mathrm{Spec}(K(A[\ell])) & \longrightarrow & \mathrm{Spec}(N_\ell) & \longrightarrow & \mathrm{Spec}(K) \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & S'_\ell & \longrightarrow & S_\ell & \longrightarrow & S \\
 & & \uparrow & & \uparrow & & \uparrow \\
\mathrm{Spec}(F(P)(A_P[\ell])) & = & \mathrm{Spec}(F(Q'_\ell)) & \longrightarrow & \mathrm{Spec}(F(Q_\ell)) & \longrightarrow & \mathrm{Spec}(F(P)) \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & \mathrm{Spec}(\mathcal{O}'_\ell) & \longrightarrow & \mathrm{Spec}(\mathcal{O}_\ell) & \xrightarrow{f_\ell} & \mathrm{Spec}(\mathcal{O})
\end{array}$$

We now study the ramification of prime ideals $\mathfrak{m} \in \mathrm{Spec}(\mathcal{O})$ in the extension $F(Q_\ell)/F(P)$. Let $\mathbb{P}_{\mathrm{bad}}$ be the (finite) set of primes $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O})$ where $A_P/F(P)$ has bad reduction.

Lemma 3.7 *There is a constant $\ell_2 \geq \ell_0$ with the following property: For every prime number $\ell \geq \ell_2$ the map $f_\ell : \mathrm{Spec}(\mathcal{O}_\ell) \to \mathrm{Spec}(\mathcal{O})$ is étale at every point $\mathfrak{m} \in \mathrm{Spec}(\mathcal{O})$ outside of $\mathbb{P}_{\mathrm{bad}}$.*

Proof. Let $\ell_2 := \max(\ell_0, (2\dim(A))![F(P) : \mathbb{Q}] + 2)$.

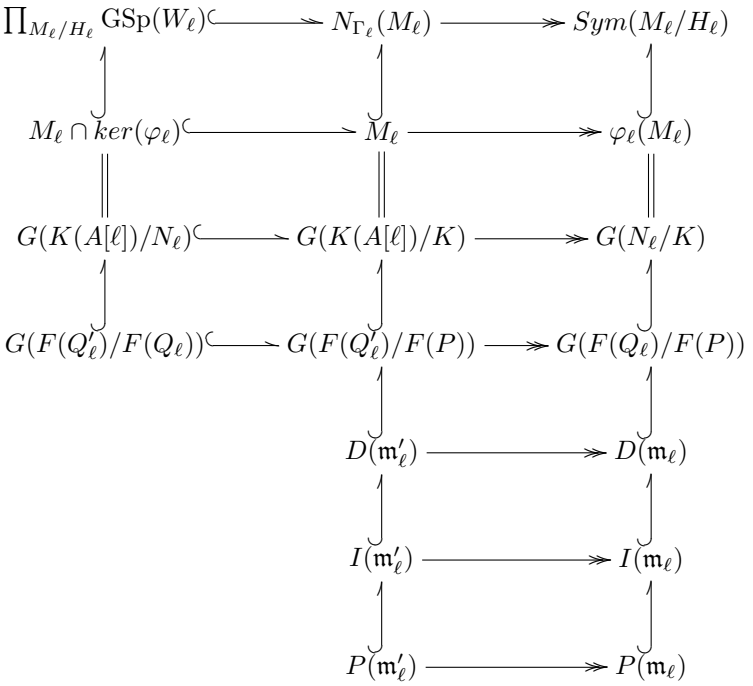
Now let $\ell \geq \ell_2$ be a prime number. Let $\mathfrak{m} \in \mathrm{Spec}(\mathcal{O})$ be an arbitrary prime ideal with $\mathfrak{m} \notin \mathbb{P}_{\mathrm{bad}}$. We have to show that $\mathfrak{m}$ is unramified in $F(Q_\ell)$. Let $p = \mathrm{char}(\mathcal{O}/\mathfrak{m})$ be the residue characteristic of $\mathfrak{m}$.

If $p \neq \ell$, then $\mathfrak{m}$ is unramified even in $F(Q'_\ell) = F(P)(A_P[\ell])$.

We can hence assume that $\boxed{p = \ell}$. Let $\mathfrak{m}_\ell \in \mathrm{Spec}(\mathcal{O}_\ell)$ be a point over $\mathfrak{m}$ and $\mathfrak{m}'_\ell \in \mathrm{Spec}(\mathcal{O}'_\ell)$ a point over $\mathfrak{m}_\ell$. Let $D(\mathfrak{m}'_\ell)$ (resp. $D(\mathfrak{m}_\ell)$) be the decomposition

group of $\mathfrak{m}'_\ell/F(P)$ (resp. of $\mathfrak{m}_\ell/F(P)$) and $I(\mathfrak{m}'_\ell)$ (resp. $I(\mathfrak{m}_\ell)$) the corresponding inertia group. Let $P(\mathfrak{m}'_\ell)$ (resp. $P(\mathfrak{m}_\ell)$) be the (unique) p-Sylow subgroup of $I(\mathfrak{m}'_\ell)$ (resp. $I(\mathfrak{m}_\ell)$).

We have the following commutative diagram on the level of groups:



We have to prove that the image of $I(\mathfrak{m}'_\ell)$ in $\mathrm{Sym}(M_\ell/H_\ell)$ by the maps in the diagram is $\{1\}$. Now $p = \ell > (2\dim(A))!$ due to our choice of ℓ_2 and $|\mathrm{Sym}(M_\ell/H_\ell)| \leq (2\dim(A))!$, hence $P(\mathfrak{m}'_\ell)$ maps to $\{1\}$ in $\mathrm{Sym}(M_\ell/H_\ell)$. In particular, $P(\mathfrak{m}_\ell) = \{1\}$. Consider the tame ramification group $I_t = I(\mathfrak{m}'_\ell)/P(\mathfrak{m}'_\ell)$. It is a cyclic group of order prime to p. Choose a subgroup $C \subset I(\mathfrak{m}'_\ell)$ that maps isomorphically onto I_t under the projection. It is enough to show that C maps to $\{1\}$ in $\mathrm{Sym}(M_\ell/H_\ell)$.

By Raynaud's theorem (cf. Theorem 3.3) there is a finite extension $E/\mathbb{F}_p$ and an epimorphism $E^\times \to C$ such that the resulting representation

$$E^\times \to C \to \mathrm{Aut}(A_P[\ell]) = \mathrm{Aut}(A[\ell])$$

has amplitude $\leq e$, where e is the ramification index of $\mathfrak{m}$ over $\mathbb{Q}$. Clearly $e \leq [F(P) : \mathbb{Q}]$. By part b) of Theorem 3.4, the image of $E^\times$ in $\mathrm{Sym}(M_\ell/H_\ell)$ is $\{1\}$. Hence the image of C in $\mathrm{Sym}(M_\ell/H_\ell)$ is $\{1\}$ as desired. □

Lemma 3.8 *Let L be the algebraic closure of F in N. Then L/F is a finite extension.*

Proof. Let $L' := \prod_{\ell \geq \ell_0 \text{ prime}} F(Q_\ell)$. For every prime $\ell \geq \ell_2$ the Galois extension of number fields $F(Q_\ell)/F(P)$ is unramfied outside $\mathbb{P}_{\text{bad}}$ by Lemma 3.7. Furthermore $[F(Q_\ell) : F(P)] \leq (2\dim(A))!$ for every prime $\ell \geq \ell_2$. The Theorem of Hermite-Minkowski (cf. [19], p. 122) implies that $\prod_{\ell \geq \ell_2 \text{ prime}} F(Q_\ell)$ is a *finite* extension of $F(P)$. This in turn implies that L'/F is a finite extension. It is thus enough to show that $L \subset L'$.

Recall that $K = F(S)$ is the function field of the F-variety S and S_ℓ is the normalization of S in the finite Galois extension N_ℓ/K. Denote by $\hat{S}$ the normalization of S in N and by $h_\ell : \hat{S} \to S_\ell$ the canonical projection. The canonical morphism $\hat{S} \to S$ is surjective, hence there is a point $\hat{P} \in \hat{S}(F_{\text{sep}})$ over P. The point $h_\ell(\hat{P}) \in S_\ell(F_{\text{sep}})$ lies over P. Hence $h_\ell(\hat{P})$ is conjugate to Q_ℓ under the action of $G(N_\ell/K)$. This implies that $F(h_\ell(\hat{P})) = F(Q_\ell)$. For every $\ell \geq \ell_0$ there is a diagram

$$\begin{array}{ccccc}
\text{Spec}(N) & \longrightarrow & \text{Spec}(N_\ell) & \longrightarrow & \text{Spec}(K) \\
\uparrow & & \uparrow & & \uparrow \\
\hat{S} & \xrightarrow{h_\ell} & S_\ell & \longrightarrow & S \\
\downarrow & & \downarrow & & \downarrow \\
\text{Spec}(F(\hat{P})) & \longrightarrow & \text{Spec}(F(Q_\ell)) & \longrightarrow & \text{Spec}(F(P))
\end{array}$$

where the morphisms $S_\ell \to S$ are étale covers and $N = \prod_{\ell \geq \ell_0} N_\ell$. It follows that $F(\hat{P}) = \prod_{\ell \geq \ell_0} F(Q_\ell) = L'$. On the other hand L is the algebraic closure of F in N, hence $\hat{S}$ is a scheme over L. This implies that L is a subfield of $F(\hat{P})$. Hence in fact $L \subset L'$ as desired. □

End of the proof of Theorem 3.6 in the case $\text{char}(K) = 0$. We have an isomorphism $G(NL_{\text{sep}}/KL_{\text{sep}}) \cong G(N/KL)$, because N/L and KL/L are regular extensions. The field KL_{sep} is $\mathcal{F}$-finite by Corollary 2.7. Hence the profinite group $G(KL_{\text{sep}}(A_{\text{tor}})/KL_{\text{sep}})$ is finitely generated. As $NL_{\text{sep}} \subset KL_{\text{sep}}(A_{\text{tor}})$, $G(NL_{\text{sep}}/KL_{\text{sep}})$ must be finitely generated as well. Furthermore $NL_{\text{sep}} = \prod_{\ell \geq \ell_0} N_\ell L_{\text{sep}}$ where $[N_\ell L_{\text{sep}} : KL_{\text{sep}}]$ is bounded independently from ℓ. Hence $G(NL_{\text{sep}}/KL_{\text{sep}})$ is finite and this implies that N/KL is a finite extension. On the other hand it follows from Lemma 3.8 that KL/K is finite. Hence N/K is a *finite* extension. Consequently N is finitely generated, because K is finitely generated. Proposition 3.2 yields a constant $\ell_3 > \ell_0$ such that $A[\ell]$ is a simple $\mathbb{F}_\ell(G_N)$-module for every prime $\ell \geq \ell_3$. Hence A/K has big monodromy by $(*)$, as desired. □

Let K be a finitely generated field of characteristic zero. Let (A, λ) be a polarized abelian variety over K, with $\text{End}(A) = \mathbb{Z}$ and $\dim(A) = 2, 6$ or odd. We finish this section with a comment on this type of abelian varieties for which Serre proved [27], [28] that A/K has big monodromy, provided K is a number field. Serre sketched in [29] a specialization argument that allows to generalize this to the case of an arbitrary finitely generated ground field K of characteristic zero. We recall the specialization argument of Serre for the sake of completeness.

Theorem 3.9 (Serre) *Let K be a finitely generated field of characteristic zero and (A, λ) a polarized abelian variety over K. Assume that* $\mathrm{End}(A) = \mathbb{Z}$ *and* $\dim(A) = 2, 6$ *or odd. Then there is a constant ℓ_0 such that $\mathcal{M}_K(A[\ell]) = \mathrm{GSp}(A[\ell], e_\ell^\lambda)$ for every prime $\ell \geq \ell_0$.*

Proof. We proceed by induction on $\mathrm{trdeg}(K/\mathbb{Q})$. The case $\mathrm{trdeg}(K/\mathbb{Q}) = 0$ is classical, see [27], [28]. Suppose $\mathrm{trdeg}(K/\mathbb{Q}) = d > 0$. Then there is a finitely generated extension $F/\mathbb{Q}$ of transcendence degree $d-1$ and a smooth curve C/F with function field $F(C) = K$. After removing finitely many points from C, we may assume that A extends to an abelian scheme $\mathcal{A} \to C$. By [23, 1.7] there is a closed point $c \in C$ such that $A_c := \mathcal{A} \times_C F(c)$ is an abelian variety *with* $\mathrm{End}(A_c) = \mathbb{Z}$. We have $|G(F(c)(A_c[\ell])/F(c))| \cong |\mathrm{GSp}(2\dim(A), \mathbb{F}_\ell)|$ for all sufficiently large primes ℓ by induction. For every prime ℓ denote by v the discrete valuation of K corresponding to c and by w_ℓ an extension of v to $K(A[\ell])$. Then Lemma 2.3 implies

$$G(F(c)(A_c[\ell])/F(c)) \cong G(F(w_\ell)/F(v)) \cong D(w_\ell) \subset G(K(A[\ell])/K)$$

and the assertion follows from that. □

4 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 use group theoretical methods of Serre in order to determine $\mathcal{M}_K(A[n])$ completely (the result depends on the characteristic of K) for every "sufficiently large" integer n. This will be important 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 4.1 *If L/K is a* Galois *extension, then $\mathcal{M}_L(A[n])$ is* normal *in $\mathcal{M}_K(A[n])$ 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 4.2 *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. [32, 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 4.1), 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 [20, 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 [30, 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 4.3 *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: $\mathcal{M}_K(A[n]) \supset \mathrm{Sp}(A[n], e_n^\lambda)$ 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 $\mathcal{M}_L(A[n]) = \mathrm{Sp}(A[n], e_n^\lambda)$ for every n coprime to c by Proposition 4.2. Furthermore $\mathcal{M}_L(A[n]) \subset \mathcal{M}_K(A[n])$ by the discussion before Remark 4.1. □

Proposition 4.4 *Let K be a field and (A, λ) a polarized abelian variety over K with big monodromy. Let L/K be a finite extension. Then the following properties hold.*

a) There is a constant c (coprime to $\deg(\lambda)$ and to $\mathrm{char}(K)$, if $\mathrm{char}(K)$ is positive) such that $\mathcal{M}_L(A[n]) \supset \mathrm{Sp}(A[n], e_n^\lambda)$ for every integer n which is coprime to c.

b) A is geometrically simple.

Proof. Part a). Let E_0 be the maximal separable extension of K in L and E/K a finite Galois extension containing E_0. By our assumption and Proposition 4.2 there is a constant $\ell_0 > \max(\deg(\lambda), \mathrm{char}(K), 5)$ such that $\mathcal{M}_{K(\mu_\infty)}(A[\ell]) = \mathrm{Sp}(A[\ell], e_\ell^\lambda)$ for every prime $\ell \geq \ell_0$. Furthermore $\mathcal{M}_{E(\mu_\infty)}(A[\ell])$ is a normal subgroup of $\mathcal{M}_{K(\mu_\infty)}(A[\ell])$ (cf. Remark 4.1) of index $\leq [E : K]$. Put $\ell_1 := \max(\ell_0, [E : K] + 1)$. Then

$$|\mathcal{M}_{E(\mu_\infty)}(A[\ell])| \geq \frac{1}{[E : K]} |\mathrm{Sp}(A[\ell], e_\ell^\lambda)| > 2$$

for all primes $\ell \geq \ell_1$. On the other hand the only normal subgroups of $\mathrm{Sp}(A[\ell], e_\ell^\lambda)$ are $\{\pm 1\}$ and the trivial group (cf. [30, p. 53]). Hence

$$\mathcal{M}_{E_0}(A[\ell]) \supset \mathcal{M}_E(A[\ell]) \supset \mathcal{M}_{E(\mu_\infty)}(A[\ell]) = \mathrm{Sp}(A[\ell], e_\ell^\lambda)$$

for all primes $\ell \geq \ell_1$. As L/E_0 is purely inseparable, we find

$$\mathcal{M}_L(A_L[\ell]) = \mathcal{M}_{E_0}(A[\ell]) \supset \mathrm{Sp}(A[\ell], e_\ell^\lambda)$$

for all primes $\ell \geq \ell_1$. Hence A_L/L has big monodromy and Corollary 4.3 implies a).

Part b). Let $A_1, A_2/\tilde{K}$ be abelian varieties and $f : A_{\tilde{K}} \to A_1 \times A_2$ an isogeny. Then A_1, A_2 and f are defined over some finite extension L/K. Hence there is an $\mathbb{F}_\ell[G_L]$-module isomorphism $A[\ell] \cong A_1[\ell] \times A_2[\ell]$ for every prime $\ell > \deg(f)$. By part a) $\mathcal{M}_L(A[\ell]) \supset \mathrm{Sp}(A[\ell]), e_\ell^\lambda)$ for all sufficiently large primes ℓ. Hence

$A[\ell]$ is a simple $\mathbb{F}_\ell[\mathcal{M}_L(A[\ell])]$-module and in particular a simple $\mathbb{F}_\ell(G_L)$-module for all sufficiently large primes ℓ. This is only possible if $A_1 = 0$ or $A_2 = 0$. $\square$

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

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

for all $n \in \mathbb{N}$ coprime to c (cf. Proposition 4.4). 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

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

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

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

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

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

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 4.5 *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.*

5 Simplicity and End's of fibres

In this section we apply our methods to prove a generalization of a result of Ellenberg, Elsholz, Hall and Kowalski on endomorphism rings and simplicity of fibres in certain families of abelian varieties (cf. [5, Theorem 8]).

Let F be a finitely generated field and K/F a finitely generated transcendental field extension and A/K an abelian variety. We say that A/K is *weakly isotrivial with respect to* F, if there is an abelian variety $B/\tilde{F}$ and a $\tilde{K}$-isogeny $B_{\tilde{K}} \to A_{\tilde{K}}$.

Proposition 5.1 *Let F be a finitely generated field, K/F a finitely generated separable transcendental field extension and (A, λ) a polarized abelian variety over K. Assume that A/K has big monodromy and that A/K is* not *weakly isotrivial with respect to F. Define $K' := F_{\mathrm{sep}}K$. There is a constant c (divisible by* $\mathrm{char}(K)$*, if* $\mathrm{char}(K) > 0$*) such that $\mathcal{M}_{K'}(A[n]) = \mathrm{Sp}(A[n], e_n^\lambda)$ for every integer n which is coprime to c.*

Proof. Let $\ell_0 \geq \max(\deg(\lambda), \mathrm{char}(K), 5)$ be a constant such that $\mathcal{M}_K(A[\ell]) \supset \mathrm{Sp}(A[\ell], e_\ell^\lambda)$ for every prime $\ell \geq \ell_0$. Let $\ell \geq \ell_0$ be a prime number. Then

$$\mathcal{M}_{K'}(A[\ell]) \subset \mathrm{Sp}(A[\ell], e_\ell^\lambda) \subset \mathcal{M}_K(A[\ell]),$$

and $\mathcal{M}_{K'}(A[\ell])$ a normal subgroup of $\mathcal{M}_K(A[\ell])$ by Remark 4.1. It follows that $\mathcal{M}_{K'}(A[\ell])$ is *normal* in $\mathrm{Sp}(A[\ell], e_\ell^\lambda)$.

The only proper normal subgroups in $\mathrm{Sp}(A[\ell], e_\ell^\lambda)$ are $\{1\}$ and $\{\pm 1\}$ (cf. [30, p. 53]), because $\ell \geq 5$. Hence either $\mathcal{M}_{K'}(A[\ell]) = \mathrm{Sp}(A[\ell], e_\ell^\lambda)$ or $|\mathcal{M}_{K'}(A[\ell])| \leq 2$. Let Λ be the set of prime numbers $\ell \geq \ell_0$ where $|\mathcal{M}_{K'}(A[\ell])| \leq 2$. We claim that Λ is *finite*.

For every $\ell \in \Lambda$ we have $[K'(A[\ell]) : K'] \leq 2$. Furthermore $G(K'(A_{\neq p})/K')$ is profinitely generated, where $p = \mathrm{char}(K)$. To see this note that

$$G(K'(A_{\neq p})/K') = G(\tilde{F}K'(A_{\neq p})/\tilde{F}K')$$

because $\tilde{F}/F_{\mathrm{sep}}$ is purely inseparable and use Corollary 2.7. Hence $N := \prod_{\ell \in \Lambda} K'(A[\ell])$ is a *finite* extension of K'. In particular N/F_{sep} is a finitely generated regular extension. A/K must be geometrically simple by our assumption that A/K has big monodromy (cf. Proposition 4.4). In particular A_N is simple. Hence assumption that A is not weakly isotrivial with respect to F implies that the Chow trace $\mathrm{Tr}_{N/F_{\mathrm{sep}}}(A_N)$ is zero. It follows by the Mordell-Lang-Néron theorem (cf. [3, Theorem 2.1]) that $A(N)$ is a finitely generated $\mathbb{Z}$-module. In particular the torsion group $A(N)_{\mathrm{tor}}$ is finite. On the other hand, $A(N)$ contains a non-trivial ℓ-torsion point for every $\ell \in \Lambda$. It follows that Λ is in fact finite.

Thus there is a constant $\ell_1 > \ell_0$ such that $\mathcal{M}_{K'}(A[\ell]) = \mathrm{Sp}(A[\ell], e_\ell^\lambda)$ for all primes $\ell \geq \ell_1$. Corollary 4.3 now implies the assertion. □

Theorem 5.2 *Let F be a finitely generated field and $K = F(t)$ the function field of $\mathbb{P}_1/F$. Let A/K be a polarized abelian variety. Let $U \subset \mathbb{P}_1$ be an open subscheme such that A extends to an abelian scheme $\mathcal{A}/U$. For $u \in U(F)$ denote by A_u/F the corresponding special fiber of $\mathcal{A}$. Assume that A is not weakly isotrivial with respect to F and 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 sets:

$$X_1 := \{u \in U(F) \mid \quad \mathrm{End}(A_u) \neq \mathbb{Z}\}$$

and

$$X_2 := \{u \in U(F) \mid \quad A_u/F \text{ is not geometrically simple}\}$$

are finite.

Proof. By Theorem 3.6 and Theorem 3.9 the abelian variety A/K has big monodromy. Define $K' := F_{\mathrm{sep}}K$. As A/K is not weakly isotrivial with respect to F by assumption, Proposition 5.1 implies that there is a constant $\ell_0 > \mathrm{char}(K)$ such that $\mathcal{M}_{K'}(A[\ell]) = \mathrm{Sp}(A[\ell], e_\ell^\lambda)$ for all primes $\ell \geq \ell_0$. Hence $A_{K'}/K'$ has big monodromy. Now Propositions 4 and 7 of [5] imply the assertion. Note that the notion of "big monodromy" in the paper [5] is slightly different from ours.□

6 Proof of Conjecture A, 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 6.1 *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 was communicated to us by Moshe Jarden. It seems to go back to Oskar Villareal.

Lemma 6.2 *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 6.1 will make heavy use of the following classical fact.

Lemma 6.3 (Borel-Cantelli, [8, 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 6.1. 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 6.1 follows from Claim 1 below, because Claim 1 together with the Borel-Cantelli Lemma 6.3 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 6.2 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. [32]). 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. □

Theorem 3.6, Theorem 3.9 and Theorem 6.1 imply the following

Corollary 6.4 *Let K be a finitely generated field and A/K a polarized abelian variety. Assume either that A is of Hall type, or that* $\mathrm{char}(K) = 0$, $\mathrm{End}(A) = \mathbb{Z}$ *and* $\dim(A) = 2, 6$ *or odd. Then part (b) of Conjecture A holds true.*

7 Proof of Conjecture A, part a)

Theorem 7.1 *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 $p := \mathrm{char}(K)$. If $p = 0$ the theorem follows by [10, Proposition 2.8] of Geyer and Jarden. We assume from now on that $p > 0$. Let $G = G_K$ and $g := \dim(A)$. We fix once and for all for every prime number $\ell > p$ 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. As A has big monodromy, we find by Proposition 4.5 an integer c divisible by p such that $\mathrm{im}(\rho_n) = \mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}/n)$ for every n coprime to c. Here we have put $\mathrm{GSp}_{2g}^{(\infty)} = \mathrm{GSp}_{2g}$.

For every prime number $\ell \geq c$ we define

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

If we denote by

$$X'_\ell := \{A \in \mathrm{GSp}_{2g}^{(q)}(\mathbb{F}_\ell) \mid A \text{ has eigenvalue } 1\},$$

then $X_\ell = \rho_\ell^{-1}(X'_\ell)$ and

$$\mu_G(X_\ell) = \frac{|X'_\ell|}{|\mathrm{GSp}_{2g}^{(q)}(\mathbb{F}_\ell)|}.$$

Theorem 8.6 in Appendix A implies that for every prime number ℓ there is a subset $S'(\ell) \subset X'_\ell$ with the following properties:

i) The sum $\sum_{\ell \geq c \text{ prime}} \frac{|S'(\ell)|}{|\mathrm{GSp}_{2g}^{(q)}(\mathbb{F}_\ell)|}$ diverges.

ii) For every set $\ell_1, \cdots, \ell_r$ of pairwise different prime numbers, if we put $n = \ell_1 \cdots \ell_r$, then

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

Here by definition

$$S'(n) = \{A \in \mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}/n) \mid r_{n,\ell_i}(A) \in S'(\ell_i) \text{ for all } i \in \{1, \cdots, r\}\}.$$

If we put $S(\ell) := \rho_\ell^{-1}(S'(\ell))$ for every prime number $\ell \geq c$, then $S(\ell) \subset X_\ell$, $\mu(S(\ell)) = \frac{|S'(\ell)|}{|\mathrm{GSp}_{2g}^{(q)}(\mathbb{F}_\ell)|}$ and the series $\sum_{\ell \geq c \text{ prime}} \mu(S(\ell))$ diverges by i).

We claim that $(S(\ell))_{\ell \geq c \text{ prime}}$ is μ-independent. Let $\ell_1, \cdots, \ell_r \geq c$ be pairwise distinct prime numbers and put $n = \ell_1 \cdots \ell_r$. Then

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

and consequently ii) implies that

$$\mu(\bigcap_{i=1}^{r} S(\ell_i)) = \prod_{i=1}^{r} \mu(S(\ell_i)).$$

Now Lemma 6.3 implies that $\bigcap_{n\geq c}\bigcup_{\ell\geq n \text{ prime}} S(\ell)$ has measure 1, and this implies the assertion. □

Theorem 3.6, Theorem 3.9 and Theorem 7.1 imply the following

Corollary 7.2 *Let K be a finitely generated field and A/K a polarized abelian variety. Assume either that A is of Hall type, or that* $\mathrm{char}(K) = 0$, $\mathrm{End}(A) = \mathbb{Z}$ *and* $\dim(A) = 2, 6$ *or odd. Then part (a) of Conjecture A holds true.*

8 Appendix A. Special sets of symplectic matrices

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 8.1 *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.*
- *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 8.4.

Lemma 8.2 *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 8.3 *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). 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. [16, 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 [16, 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 8.4 *Let p be a prime and q a power of p. 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 8.3).*

For each $i \in \{1, \dots, \mathrm{ord}_\ell(q)\}$, we define

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

Remark 8.5 *Note that all matrices in $S(\ell)$ fix an element of V.*

The Appendix is devoted to prove the following result.

Theorem 8.6 *Let $p \neq \ell$ be two primes, q a power of p. The set $S(\ell)$ is non-empty and the following properties hold:*

(1)

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

(2) For each set of distinct primes $\ell_1, \ldots, \ell_r$ which are different from p, let $n = \ell_1 \cdot \cdots \cdot \ell_r$. Then

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

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

First we will prove part (1) of Theorem 8.6. We will need some lemmas.

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

Lemma 8.7 *It holds that*

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

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

Lemma 8.8 $|S_i(\ell)| = (\ell^{2g-2}(\ell-1)+1)|S_i(\ell)_0|$.

Proof. Let $A \in S_i(\ell)_0$. 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

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

On the other hand, the first equation reads

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

Hence

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

But we have precisely asked that d does not satisfy such an equation, cf. Definition 8.4.

Now one can check that, if we have $A, \widetilde{A} \in S_i(\ell)_0$ and elements $\alpha_3, \ldots, \alpha_{2g}$, $\beta, \widetilde{\alpha}_3, \ldots, \widetilde{\alpha}_{2g}$, $\widetilde{\beta}$ 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 $k = 3, \ldots, 2g$, $\beta = \widetilde{\beta}$ and $A = \widetilde{A}$. Namely, one notices that since $\widetilde{A} = T_{u_{\widetilde{\alpha}}}[\widetilde{\beta}]T_{u_\alpha}[\beta]^{-1} \cdot A \cdot T_{u_\alpha}[\beta]T_{u_{\widetilde{\alpha}}}[\widetilde{\beta}]^{-1}$ 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 $S_i(\ell)_0$ gives rise to a subset of $S_i(\ell)$ by conjugation by the matrices $T_{u_\alpha}[\beta]$, where α runs through the tuples $(\alpha_3, \ldots, \alpha_{2g}) \in \mathbb{F}_\ell^{2g-2}$ and $\beta \in \mathbb{F}_\ell$, and $S_i(\ell)$ 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 8.6, we only need one more lemma, which is an easy consequence of the Chinese Remainder Theorem.

Lemma 8.9 *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 $\mathrm{ord}_n(q) \cdot \prod_{\ell|n} |\mathrm{Sp}_{2g}(\mathbb{F}_\ell)|$.*

Proof of Theorem 8.6(1)

Let $\ell \neq p$ be a prime. Applying Equation (3) twice to the cardinality of $\mathrm{GSp}_{2g}^{(q)}(\mathbb{F}_\ell)$ and Lemmas 8.8, 8.7 and 8.9, we obtain

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

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

To prove the second part of Theorem 8.6 we need one auxiliary lemma.

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

Lemma 8.10 *Let $\ell_1, \ldots, \ell_r$ be distinct primes which are different from p, and consider $n = \ell_1 \cdot \cdots \cdot \ell_r$. Let $i \in \{1, \ldots, \mathrm{ord}_n(q)\}$. Then there is a bijection*

$$S_i(n) \simeq S_i(\ell_1) \times \cdots \times S_i(\ell_r).$$

Proof. Consider the canonical projection

$$\begin{aligned}\pi : S_i(n) &\to S_i(\ell_1) \times \cdots \times S_i(\ell_r) \\ A &\mapsto (A \mod \ell_1, \ldots, A \mod \ell_r).\end{aligned}$$

This is clearly an injective map. Now we want to prove surjectivity. For each j, take some matrix $B_j \in S_i(\ell_j)$.

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 $A \in S(n)$. 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 $A \in S_i(n)$. □

Proof of Theorem 8.6(2)

On the one hand, since the cardinality of $|S_i(\ell)|$ does not depend on i, we obtain

$$\prod_{\ell|n} \frac{|S(\ell)|}{|\mathrm{GSp}_{2g}^{(q)}(\mathbb{F}_\ell)|} = \prod_{\ell|n} \frac{\mathrm{ord}_\ell(q)|S_1(\ell)|}{\mathrm{ord}_\ell(q)|\mathrm{Sp}_{2g}(\mathbb{F}_\ell)|} = \prod_{\ell|n} \frac{|S_1(\ell)|}{|\mathrm{Sp}_{2g}(\mathbb{F}_\ell)|}.$$

On the other hand, taking into account again that $|S_i(\ell)|$ is independent of i, Lemma 8.9 and also that, $|S_i(n)| = \prod_{\ell|n} |S_i(\ell)|$ by the previous Lemma, we get

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

$$= \frac{\sum_{i=1}^{\mathrm{ord}_n(q)} \left(\prod_{\ell|n} |S_1(\ell)|\right)}{\mathrm{ord}_n(q) \prod_{\ell|n} |\mathrm{Sp}_{2g}(\mathbb{F}_\ell)|} = \frac{\mathrm{ord}_n(q) \left(\prod_{\ell|n} |S_1(\ell)|\right)}{\mathrm{ord}_n(q) \prod_{\ell|n} |\mathrm{Sp}_{2g}(\mathbb{F}_\ell)|} =$$

$$= \prod_{\ell|n} \frac{|S_1(\ell)|}{|\mathrm{Sp}_{2g}(\mathbb{F}_\ell)|}.$$

Remark 8.11 *In the definition of the set $S_i(\ell)_0$ (cf. Definition 8.4), 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 8.6 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 8.6 in the case of the group $\mathrm{GSp}_4(\mathbb{F}_\ell)$.

9 Appendix B. Proof of Theorem 3.4

The aim of this Appendix is to provide a selfcontained proof of Theorem 3.4, which was first proven in the papers [14] and [15]. We have also taken advantage of the exposition in [18].

Let $\ell > 2$ be a prime number, let (V, e) be a finite-dimensional symplectic space over $\mathbb{F}_\ell$ and $\Gamma = \mathrm{GSp}(V, e)$. In what follows M will be a subgroup of Γ which contains a transvection, such that V is a simple $\mathbb{F}_\ell[M]$-module.

Remark 9.1

- *For a set $U \subset V$, we will denote by $\langle U \rangle$ the vector space generated by U in V.*
- *For a vector $u \in V$ and a scalar $\lambda \in \mathbb{F}_\ell$, we denote by $T_u[\lambda] \in \Gamma$ the morphism $v \mapsto v + \lambda e(v, u)u$. For each transvection $\tau \in \Gamma$ there exist $u \neq 0$, $\lambda \neq 0$ such that $\tau = T_u[\lambda]$, and $u = \ker(\tau - \mathrm{Id})$. If this is the case we will say that $\langle u \rangle$ is the direction of τ. Each nonzero vector in $\langle u \rangle$ shall be called a* direction vector *of τ.*
- *Given a group $G \subset \Gamma$, we will denote by $L(G)$ the set of vectors $u \in V$ such that there exists a transvection in G with direction vector u.*
- *We will say that a group $G \subset \Gamma$ fixes a vector space W if $\{g(w) : g \in G, w \in W\} \subset W$.*

Part iii) of Theorem 3.4 is quite simple and follows from the following observation.

Lemma 9.2 *Let $G \subseteq \mathrm{GSp}(V)$ be a subgroup and R the subgroup of G generated by the transvections in G. Then for all $g \in G$, $r \in R$, $grg^{-1} \in R$.*

Proof. Note that if $T = T_v[\lambda] \in G$ is a transvection, then $gT_v[\lambda]g^{-1} = T_{gv}[\lambda]$ is also a transvection, which belongs to G, therefore also to R. Now if we have an element of R, say $T_1 \circ \cdots \circ T_k$ for certain transvections $T_1, \ldots, T_k$, then $g(T_1 \circ \cdots \circ T_k)g^{-1} = (gT_1g^{-1}) \circ \cdots \circ (gT_kg^{-1})$ is the composition of transvections of G, therefore an element of R. □

Part i) of Theorem 3.4 is essentially Lemma 3.2 of [14]. Before proceeding to prove it, note the following elementary facts.

Lemma 9.3 *Let G be a group that acts irreducibly on V, and let $W \subset V$ a nonzero vector space. Then $V = \sum_{g \in G} gW$.*

Proof. Let S be the set $S = \{g(w) : g \in G, w \in W\}$. Consider the vector space $\langle S \rangle$. This vector space is fixed by G, hence since G acts irreducibly on V it must coincide with V. □

Lemma 9.4 *Let W be a vector subspace of V, and assume that it is fixed by a transvection $T = T_u[\lambda]$. Then either $u \in W$ or $u \in W^\perp$.*

Proof. Recall that, for all $v \in V$, $T(v) = v + \lambda e(v,u)u$. If $u \notin W$, the only way for T to fix W is that $e(w,u) = 0$ for all $w \in W$. □

Proof of Theorem 3.4, i)

Consider the action of R on V. The first step is to fix one simple nonzero R-submodule W contained in V (This always exists because V is finite-dimensional as an $\mathbb{F}_\ell$-vector space).

By Lemma 9.3, we know that $V = \sum_{g \in M} gW$. Moreover, for $g_1, g_2 \in M$ it holds that $g_1 W = g_2 W$ if and only if $g_1 H = g_2 H$. Therefore we can write $V = \sum_{g \in M/H} gW$, where H is the stabilizer of W in M. The proof of i) boils down to prove that the sum is direct and orthogonal, that is, if $g_1 H \neq g_2 H$, then $g_1 W \cap g_2 W = 0$ and $g_1 W \subset (g_2 W)^\perp$. Equivalently, we will prove that for any $g \in M$, if $gW \neq W$, then $gW \cap W = 0$ and $gW \perp W$.

The first claim, namely $gW \neq W$ implies $gW \cap W = 0$ is easy. The key point is to note that for each $g \in M$, gW is also fixed by R. Take $r \in R$, $gw \in gW$. Then $rgw = g(g^{-1}rg)w \in gW$ since $g^{-1}rg \in R$ by Lemma 9.2 and hence fixes W. Now it follows that $W \cap gW$ is fixed by R, and thus is an R-subrepresentation of W. But W is an simple R-module, hence since $W \cap gW \neq W$, it must follow that $gW \cap W = 0$.

To prove that $gW \neq W$ implies $gW \perp W$, we need to make first the following very important observation.

Claim 9.5 *The set $L(M) \cap W$ generates W.*

Proof of Claim 9.5. First let us see that $L(M) \cap W$ is nontrivial. Since any transvection in M fixes W by definition of W, it follows by Lemma 9.4 that either its direction vector belongs to W, or else it is orthogonal to W, in which case the transvection acts trivially on W. But it cannot happen that all transvections in M act trivially on W. For, if a transvection T acts trivially on W, then for all $g \in M$, gTg^{-1} acts trivially on gW. But since $R = gRg^{-1}$ (because of Lemma 9.2), then if all R acts trivially on W, it also acts trivially on gW. Now recall that $V = \sum_{g \in M} gW$. Then R would act trivially on V. But R contains at least a transvection, and this does not act trivially on V. We have a contradiction.

Hence $L(M) \cap W$ is non zero. But now observe that this set is fixed by the action of R, since the elements of M bring direction vectors into direction vectors. Therefore the vector space $\langle L(M) \cap W \rangle \subset W$ is fixed by the action of R. Since we are assuming W is an simple R-module, it follows that $\langle L(M) \cap W \rangle = W$ □

Now we are able to prove that if $gW \neq W$, then $gW \subset W^\perp$. Because of the previous claim, it suffices to show that, for any nonzero vector $w \in W$ which is the direction vector of a transvection in M, say T, $w \in (gW)^\perp$. Now recall

that, since T fixes gW, by Lemma 9.4 either $w \in gW$ or $w \in (gW)^\perp$. But $gW \cap W = 0$, so $w \in (gW)^\perp$. □

Before proving Part ii) of Theorem 3.4, we will introduce some notation.

Definition 9.6 *Let $g \in M$. We will denote by R_g the subgroup of R generated by the transvections that act non-trivially on gW.*

The following lemma is Lemma 7 of [15].

Lemma 9.7 *Let $g_1, g_2 \in M$ with $g_1 H \neq g_2 H$. Then the commutator $[R_{g_1}, R_{g_2}]$ is trivial.*

Proof. For $i = 1, 2$, let $T_i \in R_{g_i}$ be a transvection. We will see that they commute. By Lemma 9.4 applied to $g_i W$, either T_i acts trivially on $g_i W$ or its direction vector, say u_i, belongs to $g_i W$. By definition of R_{g_i} we have the second possibility. But because of Part i) of Theorem 3.4, for each $g \in M$ such that $g_i W \neq gW$, $g_i W \cap gW = 0$, hence $u_i \notin gW$. Therefore again by Lemma 9.4 applied now to gW, it follows that T_i acts trivially on gW. Therefore T_1 and T_2 commute on each gW, since at least one of them acts trivially on it. Since $V = \bigoplus_{g \in M/H} gW$, it follows that they commute on all V. □

Proof of Theorem 3.4, ii).

Let $M/H = \{g_1 H, \ldots, g_s H\}$, with $g_1 = \mathrm{Id}$. Define the map

$$P : \prod_{i=1}^{s} R_{g_i} \to R$$
$$(r_1, r_2, \ldots, r_s) \mapsto r_1 \cdot r_2 \cdot \cdots \cdot r_s.$$

Since by Lemma 9.7 elements from the different R_{g_i} commute, this map is a group homomorphism. Let us see that it is also an isomorphism.

Assume that $r_1 \cdot r_2 \cdot \cdots r_s = \mathrm{Id}$, and that there is a certain r_j which is not the identity matrix. Then r_j must act nontrivially on a certain vector $v \in V$. Since the elements of R_{g_j} act trivially on the elements of $g_i W$ for $i \neq j$ and $V = \bigoplus_{i=1}^{s} g_i W$, we can assume that $v \in g_j W$. But then the remaining r_i with $i \neq j$ act trivially on v and on $r_j(v)$. Therefore $\mathrm{Id}(v) = r_1 \cdot \cdots \cdot r_s(v) = r_j(v) \neq v$, which is a contradiction. To prove surjectivity, it suffices to note that each transvection T of M belongs to one of the R_{g_i}, (hence each element of R can be generated by elements of $\cup_i R_{g_i}$). And this holds because, since T fixes all the $g_i W$, the direction vector of T must either belong to $g_i W$ or be orthogonal to it because of Lemma 9.4, and since $V = \oplus_{i=1}^{s} g_i W$ it cannot be orthogonal to all the $g_i W$. Therefore we get that $R \simeq \prod_{i=1}^{s} R_{g_i}$.

Now we are going to apply the following result [33, Main Theorem]:

Theorem 9.8 *Suppose $G \subset \mathrm{GL}(n,k)$ is an irreducible group generated by transvections. Suppose also that k is a finite field of characteristic $\ell > 2$, and that $n > 2$. Then G is conjugate in $\mathrm{GL}(n,k)$ to one of the groups $\mathrm{SL}(n,k_0)$, $\mathrm{Sp}(n,k_0)$ or $\mathrm{SU}(n,k_0)$, where k_0 is a subfield of k.*

Note that, if $n = 2$, the result is also true and well known (cf. [4, Section 252]).

Now R_{g_1} is generated by transvections, and acts irreducibly on W (because R acts irreducibly on W, and R_{g_1} is the group generated by all those transvections in M that act nontrivially on W). Therefore R_{g_1} is conjugated to $\mathrm{Sp}(W)$. Since all R_{g_i} are conjugated to R_{g_1}, the same holds for them. Therefore we have the isomorphism $R \simeq \prod_{i=1}^{s} \mathrm{Sp}(W)$.

Finally, we can view $H_1 = \prod_{i=1}^{s} \mathrm{GSp}(W) \simeq \prod_{i=1}^{s} \mathrm{GSp}(g_i W)$ as the subgroup of Γ fixing each $g_i W$ and, fixing a symplectic basis on each $g_i W$, we can view $H_2 = \mathrm{Sym}(M/H)$ as the subgroup of Γ that permutes the $g_i W$ by bringing the fixed symplectic basis of each $g_i W$ into the fixed symplectic basis of another $g_j W$. The group generated by H_1 and H_2 inside Γ, which is the group of elements of Γ that permute the $g_i W$, is the semidirect product $H_1 \rtimes H_2$.

Recall that $N_\Gamma(R) = \{g \in \Gamma : gRg^{-1} = R\}$. Note that $g \in N_\Gamma(R)$ if and only if for all transvections $T \in M$, $gTg^{-1} \in R$. Now, if $T = T_v[\lambda]$, it holds that $gTg^{-1} = T_{g(v)}[\lambda]$, and this transvection belongs to R if and only if it is a transvection of M, that is to say, if and only if $g(v) \in L(M)$. Therefore $g \in N_\Gamma(R)$ if and only if $g(L(M)) = L(M)$. Now since R is isomorphic to $\prod_{i=1}^{s} \mathrm{Sp}(g_i W)$, $L(M)$ is the disjoint union of the $g_i W$. And moreover, if W is an R-module and $g \in N_\Gamma(R)$, then R fixes gW. Therefore, if W is an simple R-module, then $gW \neq W$ implies that $gW \cap W = 0$. Thus if $g \in N_\Gamma(R)$, then g permutes the $g_i W$. In other words, $N_\Gamma(R) \subset \prod_{i=1}^{s} \mathrm{GSp}(W) \rtimes \mathrm{Sym}(M/H)$. Reciprocally, each element of $\prod_{i=1}^{s} \mathrm{GSp}(W) \rtimes \mathrm{Sym}(G/H)$ carries elements of $\bigcup_i g_i W$ in elements of $\bigcup_i g_i W$, that is to say, carries $L(M)$ into $L(M)$, and therefore belongs to $N_\Gamma(R)$. □

This completes the proof of Part a) of Theorem 3.4.

Proof of Part b) of Theorem 3.4. Recall that (V, e) is a symplectic space over $\mathbb{F}_\ell$ and M a subgroup of $\Gamma := \mathrm{GSp}(V, e)$. M contains a transvection and V is a simple $\mathbb{F}_\ell[M]$-module by assumption. Furthermore R is the subgroup of M generated by the transvections in M, $0 \neq W \subset V$ is a simple $\mathbb{F}_\ell[R]$-module and $H = \mathrm{Stab}_M(W)$. We already proved that there is a orthogonal direct sum decomposition $V = \bigoplus_{g \in M/H} gW$. Furthermore $R \cong \prod_{g \in M/H} \mathrm{Sp}(W)$, $N_\Gamma(R) \cong \prod_{g \in M/H} \mathrm{GSp}(W) \rtimes \mathrm{Sym}(M/H)$ and $R \subset M \subset N_\Gamma(R)$. Denote by $\varphi : N_\Gamma(R) \to \mathrm{Sym}(M/H)$ the projection.

Let $E/\mathbb{F}_\ell$ be a finite extension and $\rho : E^\times \to M \subset \mathrm{GL}(V)$ a representation of amplitude $\mathrm{amp}(\rho) \leq e$. Assume that $\ell > e \dim(V) + 1$. We have to prove that $\varphi(\rho(E^\times)) = \{1\}$.

Define $S := \ker(\varphi \circ \rho) \subset E^\times$. Then $[E^\times : S] \leq |M/H| \leq \dim(V)$, and this

implies $e[E^\times : S] < \ell - 1$. Furthermore

$$\rho(S) \subset \ker(\varphi) \cong \prod_{g \in M/H} \mathrm{GSp}(gW).$$

Obviously $\rho(S)$ commutes with the center

$$Z(\ker(\rho)) \cong \prod_{g \in M/H} \mathbb{F}_\ell^\times Id_{gW}$$

of $\ker(\rho)$. Now by [15, Lemma 3] $\rho(E^\times)$ commutes with $Z(\ker(\rho))$, because $e[E^\times : S] < \ell - 1$. The centralizer of $Z(\ker(\rho))$ in $N_\Gamma(R)$ can be seen easily that $\ker(\varphi) \cong \prod_{g \in M/H} \mathrm{GSp}(gW)$. Hence $\rho(E^\times) \subset \ker(\varphi)$ and this implies $\varphi \circ \rho(E^\times) = \{1\}$. □

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

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

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

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

[5] 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.

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

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

[8] 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.

[9] 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[25] 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.

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

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

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

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

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

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

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

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

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

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

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