

SPLIT REDUCTIONS OF SIMPLE ABELIAN VARIETIES

JEFFREY D. ACHTER

ABSTRACT. Consider an absolutely simple abelian variety X over a number field K . We show that if the absolute endomorphism ring of X is commutative and satisfies certain parity conditions, then $X_{\mathfrak{p}}$ is absolutely simple for almost all primes \mathfrak{p} . Conversely, if the absolute endomorphism ring of X is noncommutative, then $X_{\mathfrak{p}}$ is reducible for \mathfrak{p} in a set of positive density.

An absolutely simple abelian variety over a number field may or may not have absolutely simple reduction almost everywhere. On one hand, let $K = \mathbb{Q}(\zeta_5)$, and let X be the Jacobian of the hyperelliptic curve with affine model

$$t^2 = s(s-1)(s-1-\zeta_5)(s-1-\zeta_5-\zeta_5^2)(s-1-\zeta_5-\zeta_5^2-\zeta_5^3),$$

considered as an abelian surface over K . Then X is absolutely simple [13, p.648] and has ordinary reduction at a set of primes \mathfrak{p} of density one [12, Prop. 1.13]; at such primes $X_{\mathfrak{p}}$ is absolutely simple.

On the other hand, let Y be the Jacobian of the hyperelliptic curve with affine model

$$t^2 = s^6 - 12s^5 + 9s^4 - 32s^3 + 3s^2 + 18s + 3,$$

considered as an abelian surface over $L = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$. Then Y is absolutely simple [3, Thm. 6.1], but $Y_{\mathfrak{q}}$ is reducible for each prime \mathfrak{q} of good reduction. (The conclusions about the simplicity of $X_{\mathfrak{p}}$ and the reducibility of $Y_{\mathfrak{q}}$ follow from Tate's description [25] of the endomorphism rings of abelian varieties over finite fields.)

Note that $\text{End}_K(X) \otimes \mathbb{Q}$ is the cyclotomic field $\mathbb{Q}(\zeta_5)$, while $\text{End}_L(Y) \otimes \mathbb{Q}$ is an indefinite quaternion algebra over \mathbb{Q} . Murty and Patankar study the splitting behavior of abelian varieties over number fields, and advance the following conjecture:

Conjecture. [19, Conj. 5.1] *Let X/K be an absolutely simple abelian variety over a number field. The set of primes of K where X splits has positive density if and only if $\text{End}_{\bar{K}}(X)$ is noncommutative.*

(A similar question has been raised by Kowalski; see [14, Rem. 3.9].) The present paper proves this conjecture under certain parity and signature conditions on $\text{End}(X)$.

The first main result states that a member of a large class of abelian varieties with commutative endomorphism ring has absolutely simple reduction almost everywhere. (Throughout this paper, "almost everywhere" means for a set of primes of density one.)

Theorem A. *Let X/K be an absolutely simple abelian variety over a number field. Suppose that either*

- (i) $\text{End}_{\bar{K}}(X) \otimes \mathbb{Q} \cong F$ a totally real field, and $\dim X/[F : \mathbb{Q}]$ is odd; or
- (ii) $\text{End}_{\bar{K}}(X) \otimes \mathbb{Q} \cong E$ a totally imaginary field, and the action of E on X is not special.

Then for almost every prime \mathfrak{p} , $X_{\mathfrak{p}}$ is absolutely simple.

The author was partially supported by NSA grant H98230-08-1-0051.

(The notion of “not special” is discussed in Section 4; it is satisfied if, for instance, $\dim X$ is prime.) Conversely, the second main result shows that abelian varieties with noncommutative endomorphism ring have split reduction at a set of primes of positive density.

Theorem B. *Suppose X/K is an absolutely simple abelian variety over a number field, and that $\text{End}_{\mathcal{R}}(X)$ is noncommutative.*

- (i) *For \mathfrak{p} in a set of positive density, $X_{\mathfrak{p}}$ is absolutely reducible.*
- (ii) *Suppose $\text{End}_{\bar{K}}(X) \otimes \mathbb{Q}$ is an indefinite quaternion algebra over a totally real field F , and that $\dim X/2[F : \mathbb{Q}]$ is odd. For \mathfrak{p} in a set of positive density, $X_{\mathfrak{p}}$ is geometrically isogenous to the self-product of an absolutely simple abelian variety.*

Moreover, there is a finite extension of K such that the set of primes \mathfrak{p} in Theorem B actually has density one.

Special cases of these results are already known. The case of Theorem A(i) in which $\text{End}(X) \cong \mathbb{Z}$ is due to Chavdarov [5, Cor. 6.10]; see also the related work of Chai and Oort [4]. An abelian surface over a finite field with noncommutative endomorphism ring is absolutely reducible [20, p.261], and the special case of Theorem B(i) in which $F = \mathbb{Q}$ and $\dim X = 2$ is apparently well-known [1, Cor. 2]. More recently, Murty and Patankar have shown that if X is either an abelian variety of CM type [19, Thm. 3.1], or a modular abelian variety with commutative absolute endomorphism ring [19, Thm. 4.1], then X has simple reduction almost everywhere.

Ellenberg et al. [10] have addressed a related problem for families of abelian varieties over a number field. Specifically, they consider the relative Jacobian of a family of hyperelliptic curves $y^2 = f(x)(x - t)$ over $K[t]$, and show that for all but finitely many specializations of t the resulting abelian variety is simple.

The proof of Theorem B uses the fact that, if $\text{End}_{\bar{K}}(X)$ is noncommutative, then the Tate module $T_{\ell}(X)$ is a direct sum of copies of the same representation of $\text{Gal}(K)$. This, in turn, follows from the fact [18] that the first homology of X , as a representation of the Lefschetz group, is isotypic but not irreducible.

The proof of Theorem A is more involved, and uses the Chebotarev theorem and the observation that if the Frobenius at \mathfrak{p} acts irreducibly on the ℓ -torsion for some ℓ , then $X_{\mathfrak{p}}$ is simple. This approach was used by Chavdarov in [5, Cor. 6.10] in the special case where the image of $\text{Gal}(K)$, acting on each X_{ℓ} , is the group of symplectic similitudes $\text{GSp}_{2g}(\mathbb{Z}/\ell)$. We give a more detailed outline of this strategy in the following example, which gives a quick proof of a special (but typical) case of [19, Thm. 3.1]. Let E be a totally imaginary extension of \mathbb{Q} of degree $2g$. Suppose that X/K is an absolutely simple g -dimensional abelian variety with $\text{End}_K(X) = \text{End}_{\bar{K}}(X) \cong \mathcal{O}_E$. Further suppose that the CM type of E is nondegenerate in the sense of [15]. For each rational prime ℓ there are Galois representations $\rho_{X/K, \mathbb{Z}/\ell} : \text{Gal}(K) \rightarrow \text{Aut}(T_{\ell}(X)) \cong \text{GL}_{2g}(\mathbb{Z}/\ell)$ and $\rho_{X/K, \ell} : \text{Gal}(K) \rightarrow \text{Aut}(X_{\ell}) \cong \text{GL}_{2g}(\mathbb{Z}/\ell)$. There is a set of rational primes \mathbb{L} (containing all but finitely many primes) such that if ℓ_1, \dots, ℓ_r are distinct primes in \mathbb{L} , then the image of $\text{Gal}(K)$ under the product representation $\times_{1 \leq i \leq r} \rho_{X/K, \ell_i}$ is $\times_{1 \leq i \leq r} (\mathcal{O}_E \otimes \mathbb{Z}/\ell_i)^{\times}$ (e.g., [21]).

Let ℓ be any prime at which E is inert, so that $(\mathcal{O}_E \otimes \mathbb{Z}/\ell)^{\times} \cong \mathbb{F}_{\ell^{2g}}^{\times}$. Let I_{ℓ} be the set of elements of $\mathbb{F}_{\ell^{2g}}^{\times}$ which are members of some proper subfield of $\mathbb{F}_{\ell^{2g}}$. Note that if $\mathbb{F}_{\ell^{2g}}$ is considered as a vector space over \mathbb{Z}/ℓ , then elements of I_{ℓ} are precisely the elements of $\mathbb{F}_{\ell^{2g}}^{\times}$ which acts reducibly on $\mathbb{F}_{\ell^{2g}}$. There exists a constant $C < 1$ such that for all ℓ inert in E , we have $|I_{\ell}| / |\mathbb{F}_{\ell^{2g}}^{\times}| < C$.

Let $M(X/K)$ be the set of (finite) primes of K where X has good reduction, and let $R(X/K)$ be the set of primes \mathfrak{p} of good reduction for which $X_{\mathfrak{p}}$ is reducible. Suppose $\mathfrak{p} \in M(X/K)$, and let $\sigma_{\mathfrak{p}} \in \text{Gal}(K)$ be a Frobenius element at \mathfrak{p} . Let ℓ be a rational prime relatively prime to \mathfrak{p} . The Frobenius endomorphism of $X_{\mathfrak{p}}$ acts as $\rho_{X/K, \mathbb{Z}_{\ell}}(\sigma_{\mathfrak{p}})$ on $T_{\ell}(X_{\mathfrak{p}}) \cong T_{\ell}(X)$. If $X_{\mathfrak{p}}$ is not simple, then the $\text{Gal}(\kappa(\mathfrak{p}))$ -module $T_{\ell}(X_{\mathfrak{p}})$ is reducible, and in particular $\rho_{X/K, \ell}(\sigma_{\mathfrak{p}})$ acts reducibly on $X_{\mathfrak{p}, \ell} := X_{\mathfrak{p}}[\ell](\overline{\kappa(\mathfrak{p})})$. Therefore, if there exists one prime ℓ such that $\rho_{X/K, \ell}(\sigma_{\mathfrak{p}})$ acts irreducibly on $X_{\mathfrak{p}, \ell}$, then $X_{\mathfrak{p}}$ is simple.

So, let ℓ_1, \dots, ℓ_r be distinct primes in \mathbb{L} at which E is inert. Let $R(X/K; \ell_1, \dots, \ell_r) \subset M(X/K)$ be the set of primes \mathfrak{p} such that for each $1 \leq i \leq r$, $\rho_{X/K, \ell_i}(\sigma_{\mathfrak{p}}) \in I_{\ell_i}$. Then $R(X/K) \subseteq R(X/K; \ell_1, \dots, \ell_r)$.

By the Chebotarev theorem, the density of $R(X/K; \ell_1, \dots, \ell_r)$ is $\prod_{i=1}^r |I_{\ell_i}| / \left| \mathbb{F}_{\ell_i}^{\times} \right| < C^r$. Since $C < 1$ and we may take an arbitrarily large set of rational primes inert in E , the density of $R(X/K)$ is zero, and the density of its complement is therefore one.

Generalizing this argument to other abelian varieties with commutative absolute endomorphism ring requires calculating the image of the Galois representations $\rho_{X/K, \mathbb{Z}_{\ell}}$, which is conjecturally described by the Mumford-Tate conjecture (see Section 3); showing that a positive proportion of elements of $\rho_{X/K, \ell}(\text{Gal}(K))$ act irreducibly on the Tate module (Section 1); and axiomatizing the foregoing argument (Section 2).

Quite recently, Banaszak et al. have extended the methods of [2] to abelian varieties of type III, which allows an extension of Theorem 5.4 to the case of definite quaternion algebras. Also, Zywna points out that sieve methods (e.g., those of [28]) can be used to make the density one statements in Section 4 more explicit. I will explain both of these developments in detail elsewhere.

1. GROUPS OF LIE TYPE

If B is a finite A -algebra, let $\mathbf{R}_{B/A}$ denote Weil's restriction of scalars functor.

Group schemes $G/\mathbb{Z}[1/\Delta]$ of the following forms arise as the images of Galois representations considered here:

- (A) There exist a totally imaginary field E with maximal totally real subfield F ; an $\mathcal{O}_E[1/\Delta]$ -module V which is free of rank $2r$ over $\mathcal{O}_F[1/\Delta]$; and an $\mathcal{O}_E[1/\Delta]$ -Hermitian pairing $\langle \cdot, \cdot \rangle$ on V ; such that G is the Weil restriction $G = \mathbf{R}_{\mathcal{O}_E[1/\Delta]/\mathbb{Z}[1/\Delta]} \text{GU}(V, \langle \cdot, \cdot \rangle)$. Let $Z = E$.
- (C) There exist a totally real field F ; a free $\mathcal{O}_F[1/\Delta]$ -module V of rank $2r$; and an $\mathcal{O}_F[1/\Delta]$ -linear symplectic pairing $\langle \cdot, \cdot \rangle$ on V ; such that $G = \mathbf{R}_{\mathcal{O}_F[1/\Delta]/\mathbb{Z}[1/\Delta]} \text{GSp}(V, \langle \cdot, \cdot \rangle)$. Let $Z = F$.

The center ZG of G satisfies $ZG(\mathbb{Z}[1/\Delta]) \cong \mathcal{O}_Z[1/\Delta]^{\times}$. The adjoint form of G is $G^{\text{ad}} := G/ZG$. For each ℓ inert in Z , let $T_{\ell}^{\text{an}} \subset G(\mathbb{Z}/\ell)$ be a maximally anisotropic maximal torus.

In case (A), the derived group of G is $G^{\text{der}} = \mathbf{R}_{\mathcal{O}_E[1/\Delta]/\mathbb{Z}[1/\Delta]} \text{SU}(V, \langle \cdot, \cdot \rangle)$. Note that $G(\mathbb{Z}/\ell) \cong \text{GU}(V \otimes \mathcal{O}_E/\ell, \langle \cdot, \cdot \rangle)$, and $G^{\text{der}}(\mathbb{Z}/\ell) \cong \text{SU}(V \otimes \mathcal{O}_E/\ell, \langle \cdot, \cdot \rangle)$. In particular, if ℓ is a rational prime inert in E , then $G^{\text{der}}(\mathbb{Z}/\ell) \cong \text{SU}_r(\mathcal{O}_E/\ell)$. Moreover, if r is odd, then T_{ℓ}^{an} acts irreducibly on $V \otimes \mathbb{Z}/\ell$; while if r is even, then T_{ℓ}^{an} stabilizes two subspaces which are in duality with each other.

In case (C), the derived group of G is $G^{\text{der}} = \mathbf{R}_{\mathcal{O}_F[1/\Delta]/\mathbb{Z}[1/\Delta]} \text{Sp}(V, \langle \cdot, \cdot \rangle)$. Note that $G(\mathbb{Z}/\ell) \cong \text{GSp}(V \otimes \mathcal{O}_F/\ell, \langle \cdot, \cdot \rangle)$ and $G^{\text{der}}(\mathbb{Z}/\ell) \cong \text{Sp}(V \otimes \mathcal{O}_F/\ell, \langle \cdot, \cdot \rangle)$. In particular, if ℓ is a rational prime inert in F , then $G^{\text{der}}(\mathbb{Z}/\ell) \cong \text{Sp}_{2r}(\mathcal{O}_F/\ell)$. Moreover, T_ℓ^{an} acts irreducibly on $V \otimes \mathbb{Z}/\ell$.

Let G be a group scheme over $\mathbb{Z}[1/\Delta]$. For a rational prime $\ell \nmid \Delta$, let $J_\ell(G)$ be the set of all $x \in G(\mathbb{Z}/\ell)$ for which the connected component of the centralizer of x is a torus which is maximally anisotropic. Let $I_\ell(G)$ be the complement $G(\mathbb{Z}/\ell) - J_\ell(G)$. Let $J_{\ell,m}(G)$ be the set of x such that $x^m \in J_\ell(G)$, and let $I_{\ell,m}(G)$ be its complement. Each of these sets is stable under conjugation. For G of type (A) or (C), $x \in J_\ell(G)$ if and only if x is $G(\mathbb{Z}/\ell)$ -conjugate to a regular element of T_ℓ^{an} .

Say that an abstract group H_ℓ is of type $G(\mathbb{Z}/\ell)$ if there are inclusions $G^{\text{der}}(\mathbb{Z}/\ell) \subseteq H_\ell \subseteq G(\mathbb{Z}/\ell)$. For such a group H_ℓ , let $I_{\ell,m}(H_\ell) = H_\ell \cap I_{\ell,m}(G)$, and let $J_{\ell,m}(H_\ell) = H_\ell \cap J_{\ell,m}(G)$.

Lemma 1.1. *Suppose $G/\mathbb{Z}[1/\Delta]$ is a group of type (A), or (C), and let m be a natural number. There exists a constant $C = C(m, G)$ such that if ℓ is inert in Z and sufficiently large, and if H_ℓ is of type $G(\mathbb{Z}/\ell)$, then $|I_{\ell,m}(H_\ell)|/|H_\ell| < C$.*

Proof. First, for each $m \in \mathbb{N}$ we show the existence of a positive constant $D_0(m, G)$ such that for all sufficiently large ℓ inert in Z , $|J_{\ell,m}(G)|/|G(\mathbb{Z}/\ell)| > D_0(m, G)$. Subsequently, we show how to deduce a uniform statement for all H_ℓ of type $G(\mathbb{Z}/\ell)$.

Let T_ℓ^* be the set of regular elements of T_ℓ^{an} , and let $T_{\ell,m}^*$ be the set of $x \in T_\ell^{\text{an}}$ such that $x^m \in T_\ell^*$. There are monic polynomials f and f^* of the same degree such that $|T_\ell^{\text{an}}| = f(\ell)$ and $|T_\ell^*| = f^*(\ell)$ [11]. (In fact, [11] works out the analogous polynomials for $|T_\ell^* \cap G'(\mathbb{Z}/\ell)|$, but the result for $G(\mathbb{Z}/\ell)$ itself follows immediately.) Therefore, there exists a constant B such that, if $\ell \gg 0$, then $|T_\ell^*|/|T_\ell^{\text{an}}| > 1 - B/\ell$. By considering the fibers of the m^{th} power map, we see that $|T_{\ell,m}^*|/|T_\ell^{\text{an}}| > 1 - mB/\ell$.

An element of $G(\mathbb{Z}/\ell)$ is in $J_{\ell,m}(G)$ if and only if it is conjugate to an element of $T_{\ell,m}^*$. The normalizer $N_\ell = N_{G(\mathbb{Z}/\ell)}(T_\ell^{\text{an}})$ is an extension of a finite group W by T_ℓ^{an} ; the group W depends on G , but not on ℓ . Moreover, $T_{\ell,m}^*$ is stable under the action of N_ℓ . We obtain the estimate

$$\begin{aligned} \frac{|J_{\ell,m}(G)|}{|G(\mathbb{Z}/\ell)|} &= \frac{1}{|G(\mathbb{Z}/\ell)|} \left(\frac{|G(\mathbb{Z}/\ell)|}{|N_\ell|} |T_{\ell,m}^*| \right) \\ &= \frac{1}{|W|} \frac{|T_{\ell,m}^*|}{|T_\ell^{\text{an}}|} > \frac{1}{|W|} \left(1 - \frac{mB}{\ell} \right). \end{aligned}$$

This shows the existence of $D_0(m, G)$ with the desired properties. Membership in $J_{\ell,m}(G)$ is well-defined on cosets modulo the center of G . Therefore, the proportion of elements of $G^{\text{ad}}(\mathbb{Z}/\ell)$ which are (represented by) elements whose m^{th} power is maximally anisotropic is also at least $D_0(m, G)$.

Now let H_ℓ be any group of type $G(\mathbb{Z}/\ell)$, and let $H_\ell^{\text{ad}} = H_\ell/(ZG(\mathbb{Z}/\ell) \cap H_\ell)$. There is an inclusion of groups $H_\ell^{\text{ad}} \hookrightarrow G^{\text{ad}}(\mathbb{Z}/\ell)$, with cokernel a finite cyclic group whose order n divides the rank of G .

Suppose $x \in J_{\ell,mn}(G)$. The equivalence class of x^n modulo the center is represented by an element h of H_ℓ . Moreover, for such an h , $h^m \equiv x^{mn} \pmod{ZG(\mathbb{Z}/\ell)}$ is maximally anisotropic modulo the center. The elements of $G^{\text{ad}}(\mathbb{Z}/\ell)$ which are maximally anisotropic give rise to at least $\frac{1}{n}D_0(mn, G)|G^{\text{ad}}(\mathbb{Z}/\ell)|$ distinct maximally anisotropic elements of H_ℓ^{ad} . Let $D(m, G) =$

$\min\{\frac{1}{n}D_0(mn, G) : n|\text{rank}(G)\}$. Then one may take $1 - D(m, G)$ for $C(m, G)$ in the statement of Lemma 1.1. \square

Remark 1.2. For groups of type (C), the case $m = 1$ and $H_\ell = G(\mathbb{Z}/\ell)$ of Lemma 1.1 is proved in [5, Cor. 3.6].

Lemma 1.3. *Let $G/\mathbb{Z}[1/\Delta]$ be a group. Suppose that either G is of type (A) with $r \geq 2$ or that G is of type (C). Let ℓ_1, \dots, ℓ_m be distinct rational primes which are inert in \mathbb{Z} . Let H be a subgroup of $G^{\text{der}}(\mathbb{Z}/(\prod \ell_i))$ such that for each i , the composition $H \hookrightarrow G^{\text{der}}(\mathbb{Z}/(\prod \ell_i)) \rightarrow G^{\text{der}}(\mathbb{Z}/\ell_i)$ is surjective. Then $H = G^{\text{der}}(\mathbb{Z}/(\prod \ell_i))$.*

Proof. This is Goursat's lemma [22, p. 793]; see also [5, Prop. 5.1]. The hypothesis guarantees that the adjoint groups $G^{\text{ad}}(\mathbb{Z}/\ell_i)$ are distinct nonabelian simple groups. \square

Lemma 1.4. *Let $r \in \mathbb{N}$ and let \mathbb{F} be a finite field, with $\mathbb{F} \notin \{\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_3, \mathbb{F}_9\}$. Suppose that either G is GU_r/\mathbb{F} and $r \geq 2$ or that G is $\text{GSp}_{2r}/\mathbb{F}$. Let G^{der} be the derived group of G , let G^{ad} be the adjoint form of G , and let $\alpha : G \rightarrow G^{\text{ad}}$ and $\beta : G^{\text{der}} \rightarrow G^{\text{ad}}$ be the canonical projections. Let $H \subset G(\mathbb{F})$ be a subgroup. If $\beta^{-1}(\alpha(H)) = G^{\text{der}}(\mathbb{F})$, then H contains $G^{\text{der}}(\mathbb{F})$.*

Proof. This is standard; the hypothesis on \mathbb{F} rules out exceptional cases. \square

2. ABELIAN VARIETIES

Let X/k be a principally polarized abelian variety over a field k . For each rational prime ℓ invertible in k , let $T_\ell(X)$ be the ℓ -adic Tate module of X , and let $X_\ell := X[\ell](\bar{k}) = T_\ell(X)/\ell T_\ell(X)$. Then $T_\ell X$ and X_ℓ come equipped with an action by $\text{Gal}(k)$. Let $\rho_{X/k, \mathbb{Z}_\ell} : \text{Gal}(k) \rightarrow \text{Aut}(T_\ell(X))$ and $\rho_{X/k, \ell} : \text{Gal}(k) \rightarrow \text{Aut}(X_\ell)$ be the associated representations, with respective images $H_{X/k, \mathbb{Z}_\ell}$ and $H_{X/k, \ell}$. Let $H_{X/k, \mathbb{Q}_\ell}$ be the Zariski closure of $H_{X/k, \mathbb{Z}_\ell}$ in $\text{Aut}(T_\ell(X) \otimes \mathbb{Q})$.

Suppose X is simple. Then the endomorphism algebra $D(X) = \text{End}(X) \otimes \mathbb{Q}$ is a central simple algebra over a number field $E(X)$ with positive involution. Let $F(X) \subseteq E(X)$ be the subfield fixed by the involution. Then $F(X)$ is a totally real field, and either $E(X) = F(X)$ or $E(X)$ is a totally imaginary quadratic extension of $F(X)$. Let $f(X) = [F(X) : \mathbb{Q}]$, let $e(X) = [E(X) : \mathbb{Q}]$, and let $d(X) = \sqrt{[D(X) : E(X)]}$.

If X and Y are isogenous abelian varieties, write $X \sim Y$.

If K is a number field, let M_K be the set of (finite) primes of K ; if $\mathfrak{p} \in M_K$, denote its residue field by $\kappa(\mathfrak{p})$. Suppose X/K is an absolutely simple abelian variety. As in the introduction, let $M(X/K) \subset M_K$ be the set of primes of good reduction of X . It is convenient to distinguish the following subsets of $M(X/K)$:

- $S(X/K) = \{\mathfrak{p} \in M(X/K) : X_{\mathfrak{p}} \text{ is simple}\};$
- $S^*(X/K) = \{\mathfrak{p} \in M(X/K) : X_{\mathfrak{p}} \text{ is absolutely simple}\};$
- $R(X/K) = \{\mathfrak{p} \in M(X/K) : X_{\mathfrak{p}} \text{ is reducible}\};$
- $R^*(X/K) = \{\mathfrak{p} \in M(X/K) : X_{\mathfrak{p}} \text{ is absolutely reducible}\}.$

Then $R(X/K)$ is the complement of $S(X/K)$; $R^*(X/K)$ is the complement of $S^*(X/K)$; $S^*(X/K) \subset S(X/K)$; and $R^*(X/K) \supset R(X/K)$. In this notation, [19, Conj. 5.1] states that $S(X/K)$ has density one if and only if $\text{End}_{\bar{K}}(A)$ is commutative.

Many attributes of $X_{\bar{K}}$, the base change of X to an algebraic closure of K , are already detectable over a finite extension of K . Consider the following condition on an abelian variety X over a number field K and a finite, Galois extension K'/K :

$$(2.1) \quad \begin{aligned} \text{End}_{K'}(X) &= \text{End}_{\bar{K}}(X); \text{ for all but finitely many } \mathfrak{p} \in \\ &M(X/K), \text{ if } \mathfrak{p}' \in M(X/K') \text{ is a prime which divides } \mathfrak{p}, \text{ and} \\ &\text{if } X_{\mathfrak{p}'} \text{ is simple, then } X_{\mathfrak{p}} \text{ is absolutely simple; and } H_{X/K', \mathbb{Q}_\ell} \text{ is} \\ &\text{connected for each rational prime } \ell. \end{aligned}$$

Lemma 2.1. *Let X/K be an abelian variety over a number field. Fix a natural number $n \geq 5$, and let K'/K be a finite, Galois extension which contains the field of definition of all n -torsion points of X . Then $(X/K, K')$ satisfies (2.1).*

Proof. There are three conditions in (2.1). The first follows from Silverberg's criterion [23, Thm. 2.4]. The second follows from this and the fact that, if \mathfrak{p} is relatively prime to n , then $X[n](K') \hookrightarrow X_{\mathfrak{p}'}[n](\kappa(\mathfrak{p}'))$. The final condition is [24, Thm. 4.6]. \square

In Lemma 2.1, if one insists that n be divisible by two distinct primes n_1 and n_2 , each of which is at least five, then the second condition of (2.1) holds for all primes $\mathfrak{p} \in M(X/K)$.

Throughout this paper Lemma 2.1 will be used, often implicitly, to show the existence of an extension K'/K such that $(X/K, K')$ satisfies (2.1).

We will often work with an abelian variety X/K , a group scheme $G/\mathbb{Z}[1/\Delta]$, and an infinite set of rational primes $\mathbb{L} \subset M_{\mathbb{Q}}$ relatively prime to Δ which satisfy the following hypotheses:

$$(2.2) \quad \begin{aligned} &\text{The abelian variety } X \text{ is absolutely simple. For each } \ell \in M_{\mathbb{Q}}, \\ &H_{X/K, \ell} \text{ is isomorphic to a subgroup of } G(\mathbb{Z}/\ell). \text{ For each } \ell \in \\ &\mathbb{L}, H_{X/K, \ell} \text{ is of type } G(\mathbb{Z}/\ell). \text{ For each finite subset } A \subset \mathbb{L}, \\ &\text{the image of } \text{Gal}(K) \text{ under } \times_{\ell \in A} \rho_{X, \ell} \text{ is } \times_{\ell \in A} H_{X/K, \ell}. \end{aligned}$$

If $(X/K, G/\mathbb{Z}[1/\Delta], \mathbb{L})$ satisfies (2.2), and if $A \subset M_{\mathbb{Q}}$ is any set of primes, let $I(X/K; G; A) \subset M(X/K)$ be the set of primes \mathfrak{p} such that for each $\ell \in A$ and each Frobenius element $\sigma_{\mathfrak{p}} \in \text{Gal}(K)$ at \mathfrak{p} , $\rho_{X, \ell}(\sigma_{\mathfrak{p}}) \in I_{\ell}(G)$. Its complement $J(X/K; G; A)$ is the set of primes $\mathfrak{p} \in M(X/K)$ for which there exists some prime $\ell \in A$ such that $\rho_{X, \ell}(\sigma_{\mathfrak{p}}) \in J_{\ell}(G)$.

Let $I(X/K; G) = I(X/K; G; M_{\mathbb{Q}})$ and let $J(X/K; G) = J(X/K; G; M_{\mathbb{Q}})$. Note that for any $A \subset M_{\mathbb{Q}}$, $I(X/K; G) \subseteq I(X/K; G; A)$ and $J(X/K; G; A) \subseteq J(X/K; G)$.

Lemma 2.2. *Suppose $(X/K, G/\mathbb{Z}[1/\Delta], \mathbb{L})$ satisfies (2.2). Suppose that there is a constant $C < 1$ such that for each $\ell \in \mathbb{L}$ and each group H_{ℓ} of type $G(\mathbb{Z}/\ell)$, $|I_{\ell}(H_{\ell})|/|H_{\ell}| < C$. Then $J(X/K; G)$ has density one.*

Proof. Let $A \subset \mathbb{L}$ be a finite subset. The Chebotarev density theorem, applied to the representation $\times_{\ell \in A} \rho_{X/K, \ell}$ of $\text{Gal}(K)$, shows that the density of $I(X/K; G; A)$ is $\prod_{\ell \in A} \left| \frac{I_{\ell}(H_{X/K, \ell})}{|H_{X/K, \ell}|} \right|$, which is less than $C^{|A|}$. By taking A arbitrarily large, we find that $I(X/K; G)$ has density zero and its complement, $J(X/K; G)$, has density one. \square

Recall that if G is of type (C), or of type (A) with r odd, and if ℓ is inert in Z , then the natural representation of $G(\mathbb{Z}/\ell)$ is an irreducible module over T_{ℓ}^{an} . Equivalently, some semisimple element of $G(\mathbb{Z}/\ell)$ acts irreducibly on $V \otimes \mathbb{Z}/\ell$.

Lemma 2.3. *Suppose $(X/K, G/\mathbb{Z}[1/\Delta], \mathbb{L})$ satisfies (2.2). Suppose $\mathfrak{p} \in M(X/K)$, and let $\sigma_{\mathfrak{p}}$ be a Frobenius element at \mathfrak{p} . If $\rho_{X/K, \ell}(\sigma_{\mathfrak{p}}) \in J_{\ell}(G)$, and if some semisimple element of $G(\mathbb{Z}/\ell)$ acts irreducibly on X_{ℓ} , then the reduction $X_{\mathfrak{p}}$ is simple.*

Proof. Let ℓ be a rational prime relatively prime to \mathfrak{p} , and suppose $\rho_{X/K, \ell}(\sigma_{\mathfrak{p}}) \in J_{\ell}(G)$. Then the group $\langle \rho_{X/K, \ell}(\sigma_{\mathfrak{p}}) \rangle$ acts irreducibly on X_{ℓ} , so that $\langle \rho_{X/K, \mathbb{Z}, \ell}(\sigma_{\mathfrak{p}}) \rangle$ acts irreducibly on $T_{\ell}(X)$. The Tate module of X is an irreducible $\text{Gal}(\kappa(\mathfrak{p}))$ -module, thus the abelian variety $X_{\mathfrak{p}}/\kappa(\mathfrak{p})$ is simple [25, Thm. 1(b)]. \square

Lemma 2.4. *Suppose $(X/K, G/\mathbb{Z}[1/\Delta], \mathbb{L})$ satisfies (2.2), and that G is of type (A) with r even. Suppose $\ell \in \mathbb{L}$ is inert in Z , and that $\mathfrak{p} \in M(X/K)$. If $\sigma_{\mathfrak{p}}$ is a Frobenius element at \mathfrak{p} , if $\rho_{X/K, \ell}(\sigma_{\mathfrak{p}}) \in J_{\ell}(G)$, and if X_{ℓ} is the natural representation of $G(\mathbb{Z}/\ell)$, then the reduction $X_{\mathfrak{p}}$ is simple.*

Proof. Possibly after conjugating, assume that $t := \rho_{X/K, \ell}(\sigma_{\mathfrak{p}})$ lies in T_{ℓ}^{an} . Recall that T_{ℓ}^{an} stabilizes two maximal isotropic subspaces W_1 and W_2 of X_{ℓ} which are in duality with each other; the action of T_{ℓ}^{an} on W_2 is the Frobenius twist of its action on W_1 . By Tate's theorem, either $X_{\mathfrak{p}}$ is irreducible, or $X_{\mathfrak{p}} \sim Y_1 \times Y_2$ with each Y_j irreducible. In the latter case, the polarization would place Y_1 and Y_2 in duality, and in particular Y_1 and Y_2 are isogenous. However, since t is a regular element of T_{ℓ}^{an} , its eigenvalues on W_1 are distinct from its eigenvalues on W_2 . Therefore, $X_{\mathfrak{p}}$ is irreducible. \square

Lemma 2.5. *Suppose $(X/K, G/\mathbb{Z}[1/\Delta], \mathbb{L})$ satisfies (2.2). Suppose that there is a constant $C < 1$ such that for each $\ell \in \mathbb{L}$ and each group H_{ℓ} of type $G(\mathbb{Z}/\ell)$, $|I_{\ell}(H_{\ell})|/|H_{\ell}| < C$. Suppose that for each $\ell \in \mathbb{L}$, either*

- (a) *some semisimple element of $G(\mathbb{Z}/\ell)$ acts irreducibly on X_{ℓ} ; or*
- (b) *G is of type (A), r is even, ℓ is inert in Z , and X_{ℓ} is the natural representation.*

Then $S(X/K)$ has density one.

Proof. Part (a) follows immediately from Lemmas 2.2 and 2.3. Part (b) follows from Lemmas 2.2 and 2.4. \square

In the other direction, we have:

Lemma 2.6. *Suppose X/K is an absolutely simple abelian variety over a number field, and suppose $\mathfrak{p} \in M(X/K)$. Suppose that there exist a prime ℓ relatively prime to \mathfrak{p} , an integer $d \geq 2$, and a \mathbb{Q}_{ℓ} -representation $W_{\mathbb{Q}_{\ell}}$ of $\text{Gal}(K)$ with $T_{\ell}(X) \otimes \mathbb{Q} \cong W_{\mathbb{Q}_{\ell}}^{\oplus d}$ as $\text{Gal}(K)$ -module.*

- (a) *There are simple abelian varieties Y_1, \dots, Y_s over $\kappa(\mathfrak{p})$ such that*

$$(2.3) \quad X_{\mathfrak{p}} \sim Y_1^{e_1} \times \dots \times Y_s^{e_s}.$$

For each j with $1 \leq j \leq s$, $d|e_j \cdot d(Y_j)$.

- (b) *If the residue field $\kappa(\mathfrak{p})$ is a field of prime order, then each $e_j \geq d$. In particular, $X_{\mathfrak{p}}$ is not simple.*

Proof. Recall that $f_{\mathfrak{p}}(t)$, the characteristic polynomial of Frobenius of $X_{\mathfrak{p}}$, coincides with the characteristic polynomial of $\rho_{X/K, \mathbb{Z}, \ell}(\sigma_{\mathfrak{p}})$. Since $T_{\ell}(X) \otimes \mathbb{Q} \cong W_{\mathbb{Q}_{\ell}}^{\oplus d}$, there exists a polynomial $g_{\mathfrak{p}, \ell}(t) \in \mathbb{Z}_{\ell}(t)$ with $f_{\mathfrak{p}}(t) = g_{\mathfrak{p}, \ell}(t)^d$. Note that $f_{\mathfrak{p}}$ and $g_{\mathfrak{p}, \ell}$ are both monic. By inductively analyzing the coefficients of $g_{\mathfrak{p}, \ell}(t)$ (in descending order), one sees that $g_{\mathfrak{p}, \ell}(t) \in \mathbb{Q}[t] \cap \mathbb{Z}_{\ell}[t] \subset \mathbb{Q}_{\ell}[t]$; by Gauss's lemma, $g_{\mathfrak{p}, \ell}(t) \in \mathbb{Z}[t]$. Factor $g_{\mathfrak{p}, \ell}(t) = g_1(t)^{a_1} \dots g_s(t)^{a_s}$ as a product of powers of distinct irreducible polynomials, so that $f_{\mathfrak{p}}(t) = g_1(t)^{a_1 d} \dots g_s(t)^{a_s d}$. Consider some j with $1 \leq j \leq s$. By

the theory developed by Tate and Honda [25, Thm. 1(b) and Thm. 2(e)] [26, Thm. 1 and Rem. 2], there is a simple abelian variety Y_j over $\kappa(\mathfrak{p})$ with characteristic polynomial of Frobenius $g_j(t)^{d(Y_j)}$. Moreover, any abelian variety over $\kappa(\mathfrak{p})$ with characteristic polynomial divisible by $g_j(t)$ contains a sub-abelian variety isogenous to Y_j . From this the decomposition (2.3) follows, where $e_j = \frac{a_j d}{d(Y_j)}$. This proves (a).

For (b), a simple abelian variety over a prime field has commutative endomorphism ring. (This follows from [26, Thm. 1(ii)], and was noted in [6, p. 469].) Therefore, each Y_j has commutative endomorphism ring; $d(Y_j) = 1$; and each exponent e_j in (2.3) is a multiple of $d \geq 2$. \square

Lemma 2.7. *Suppose $(X/K, G/\mathbb{Z}[1/\Delta], \mathbb{L})$ satisfies (2.2), where X is an absolutely simple abelian variety. Suppose there is a constant $C < 1$ such that for each $\ell \in \mathbb{L}$ and each group H_ℓ of type $G(\mathbb{Z}/\ell)$, $|I_\ell(H_\ell)|/|H_\ell| < C$. Suppose there is an integer $d \geq 2$ such that for each $\ell \in \mathbb{L}$ there exists an irreducible $\text{Gal}(K)$ -module $W_{\mathbb{Q}_\ell}$ with $T_\ell(X) \otimes \mathbb{Q} \cong W_{\mathbb{Q}_\ell}^{\oplus d}$. Finally, suppose there exists $\sigma \in \text{Gal}(K)$ such that $\rho_{X/K, \mathbb{Z}_\ell}$ acts irreducibly and semisimply on $W_{\mathbb{Q}_\ell}$. Then for \mathfrak{p} in a set of density one there exists a simple abelian variety $Y_{\mathfrak{p}}/\kappa(\mathfrak{p})$ such that $X_{\mathfrak{p}}$ is isogenous to $Y_{\mathfrak{p}}^{\oplus d}$.*

Proof. Suppose $\mathfrak{p} \in M(X/K)$, and choose $\ell \in \mathbb{L}$ prime to \mathfrak{p} . Let $g_{\mathfrak{p}, \ell}(t) \in \mathbb{Z}[t]$ be the characteristic polynomial of $\sigma_{\mathfrak{p}}$ acting on $W_{\mathbb{Q}_\ell}$ via $\rho_{X/K, \mathbb{Z}_\ell}$, and let $f_{\mathfrak{p}}(t)$ be the characteristic polynomial of Frobenius of $X_{\mathfrak{p}}$. We have seen (Lemma 2.6) that $f_{\mathfrak{p}}(t) = g_{\mathfrak{p}, \ell}(t)^d$.

By Lemma 2.2, $J(X/K; G)$ has density one. If $\mathfrak{p} \in J(X/K; G)$, then $\sigma_{\mathfrak{p}}$ acts irreducibly on $W_{\mathbb{Q}_\ell}$, and thus $g_{\mathfrak{p}, \ell}(t)$ is irreducible (over \mathbb{Q}). Therefore, for such \mathfrak{p} , $s = 1$ in (2.3), and $X_{\mathfrak{p}} \sim Y^e$ for some e with $d(Y) \cdot e = d$.

If we further restrict \mathfrak{p} to have residue degree one (which is still a density-one condition), then $d(Y) = 1$ and $e = d$ (Lemma 2.6(b)). \square

In fact, we will need slightly stronger variants of Lemmas 2.5 and 2.6.

Proposition 2.8. *Let X/K be an absolutely simple abelian variety over a number field, and let K'/K be a finite Galois extension of degree m such that $(X/K, K')$ satisfies (2.1). Suppose $(X/K', G/\mathbb{Z}[1/\Delta], \mathbb{L})$ satisfies (2.2). Suppose that there is a constant $C < 1$ such that for all $\ell \in \mathbb{L}$ and each H_ℓ of type $G(\mathbb{Z}/\ell)$, $|I_{\ell, m}(H_\ell)|/|H_\ell| < C$. Suppose that for each $\ell \in \mathbb{L}$, either*

- (a) *some semisimple element of $G(\mathbb{Z}/\ell)$ acts irreducibly on X_ℓ ; or*
- (b) *G is of type (A), r is even, ℓ is inert in \mathbb{Z} , and X_ℓ is the natural representation.*

Then $S^(X/K)$ has density one.*

Proof. We indicate how to prove Lemmas 2.2 and 2.3 in this more general setting. This will prove Proposition 2.8 under hypothesis (a); the result for hypothesis (b) is entirely analogous. Let $B = \text{Gal}(K'/K)$, and for each ℓ let $B_\ell = H_{X/K, \ell}/H_{X/K', \ell}$. Then B_ℓ is a quotient of B .

Let $J_m(X/K; G)$ be the set of primes $\mathfrak{p} \in M(X/K)$ for which there exists some $\ell \in \mathbb{L}$ such that $\rho_{X/K, \ell}(\sigma_{\mathfrak{p}})^m \in J_\ell(G)$, i.e., such that $\rho_{X/K, \ell}(\sigma_{\mathfrak{p}}) \in J_{\ell, m}(H_{X/K, \ell})$. We start by showing that $J_m(X/K; G)$ has density one.

Suppose $A \subset \mathbb{L}$ is a finite set. The hypothesis (2.2), applied to the subgroup $\prod_{\ell \in A} H_{X/K', \ell}$ of $\prod_{\ell \in A} H_{X/K, \ell}$, implies that there is a quotient B_A of B such that the image of $\text{Gal}(K)$ under $\times_{\ell \in A} \rho_{X/K, \ell}$ is an extension of B_A by $\prod_{\ell \in A} H_{X/K', \ell}$.

Suppose $\ell \in \mathbb{L}$. Since $|B_\ell|$ is bounded independently of ℓ , by hypothesis there exists a constant $C' < 1$ such that

$$\frac{|H_{X/K,\ell} - J_{\ell,m}(G)|}{|H_{X/K,\ell}|} < C'.$$

As in Lemma 2.2, this implies that the set $J_m(X/K; G)$ has density one.

Suppose $\mathfrak{p} \in J_m(X/K; G)$ is not one of the finitely many exceptional primes allowed by (2.1), and choose an ℓ such that $\rho_\ell(\sigma_{\mathfrak{p}}) \in J_{\ell,m}(G)$. Not only is $X_{\mathfrak{p}}$ simple, but it is absolutely simple. Indeed, let $\mathfrak{p}' \in M(X/K')$ be a prime lying over \mathfrak{p} ; then $\rho_\ell(\sigma_{\mathfrak{p}'})$ is a power of the mod- ℓ reduction of the Frobenius element of $X_{\mathfrak{p}'} = X_{\mathfrak{p}} \times_{\kappa(\mathfrak{p})} \kappa(\mathfrak{p}')$, and $X_{\mathfrak{p}'}$ is simple. Moreover, $\kappa(\mathfrak{p}')$ contains the field of definition of the n -torsion of $X_{\mathfrak{p}}$. Since $X_{\mathfrak{p}}$ is simple over $\kappa(\mathfrak{p}')$ (Lemma 2.3), it is absolutely simple (by (2.1)).

Since $J_m(X/K; G) \subseteq S^*(X/K)$, the set of primes at which X has absolutely simple reduction has density one. \square

Proposition 2.9. *Suppose X/K is an absolutely simple abelian variety over a number field. Suppose that there exist a finite Galois extension K'/K , an integer $d \geq 2$, and an infinite set of primes \mathbb{L} such that for each $\ell \in \mathbb{L}$ there exists a representation $W_{\mathbb{Q}_\ell}$ of $\text{Gal}(K')$ such that $T_\ell(X) \otimes \mathbb{Q}_\ell \cong W_{\mathbb{Q}_\ell}^{\oplus d}$ as $\text{Gal}(K')$ -module.*

- (a) *For \mathfrak{p} in a set of density at least $1/[K' : K]$, there exists an abelian variety $Y_{\mathfrak{p}}$ over $\kappa(\mathfrak{p})$ such that $X_{\mathfrak{p}} \sim Y_{\mathfrak{p}}^{\oplus d}$.*
- (b) *Suppose $(X/K', G/\mathbb{Z}[1/\Delta], \mathbb{L})$ satisfies (2.2), and that $(X/K, K')$ satisfies (2.1). Suppose there is a constant $C < 1$ such that for each $\ell \in \mathbb{L}$ and each group H_ℓ of type $G(\mathbb{Z}/\ell)$, $|I_\ell(H_\ell)|/|H_\ell| < C$. Suppose there exists $\sigma \in \text{Gal}(K')$ such that $\rho_{X/K', \mathbb{Z}_\ell}(\sigma)$ acts irreducibly and semisimply on $W_{\mathbb{Q}_\ell}$. Then for \mathfrak{p} in a set of density at least $1/[K' : K]$, $X_{\mathfrak{p}} \times \overline{\kappa(\mathfrak{p})} \sim Y_{\overline{\mathfrak{p}}}^{\oplus d}$ for an absolutely simple abelian variety $Y_{\overline{\mathfrak{p}}}$ over $\overline{\kappa(\mathfrak{p})}$.*

Proof. Let $T(X/K, K')$ be the set of primes $\mathfrak{p} \in M(X/K)$ which lie under some $\mathfrak{p}' \in M(X/K')$ with prime residue field. (Note that $T(X/K, K')$ has density at least $1/[K' : K]$.) If $\mathfrak{p} \in T(X/K, K')$, then $X_{\mathfrak{p}'}$ is reducible by Lemma 2.6(b). Since $\kappa(\mathfrak{p}') = \kappa(\mathfrak{p})$, $X_{\mathfrak{p}}$ is reducible, too. This proves (a).

Now suppose the hypotheses of (b) hold. Let $T^*(X/K')$ be the set of primes $\mathfrak{p}' \in M(X/K')$ such that $X_{\mathfrak{p}'}$ is isogenous to $Y_{\mathfrak{p}'}^{\oplus d}$ for some simple abelian variety $Y_{\mathfrak{p}'}/\kappa(\mathfrak{p}')$. By hypothesis (2.1), such a $Y_{\mathfrak{p}'}$ is actually absolutely simple. By Lemma 2.7, $T^*(X/K')$ has density one; the set of primes of K lying under elements of $T^*(X/K')$ has density at least $1/[K' : K]$. \square

3. LEFSCHETZ GROUPS

Suppose X/K is an abelian variety whose endomorphism algebra is a (noncommutative) division algebra. In this section we show that the representation of $\text{Gal}(K)$ on $T_\ell(X)$ is isomorphic to several copies of the same representation. The result follows from an analogous description of Lefschetz groups due to Milne, whose treatment [18] we follow here.

Consider a Weil cohomology theory $X \mapsto H^*(X)$ with coefficients in a field k of characteristic zero. Examples of such a theory include Betti cohomology (for varieties over \mathbb{C}) and ℓ -adic cohomology. If X is an abelian variety, let $V(X)_k$ be the dual of its first cohomology group in this cohomology theory. For example, $V(X)_{\mathbb{Q}_\ell} = T_\ell(X) \otimes_{\mathbb{Z}} \mathbb{Q}$; and if X is a complex abelian variety, then $V(X)_{\mathbb{Q}}$ is its first Betti homology $H_1(X(\mathbb{C}), \mathbb{Q})$.

In this context there is a Lefschetz group $\text{Lef}(X)_k$, an algebraic group over k which is naturally a subgroup of $\text{GL}(V(X)_k)$. It is the largest subgroup which fixes the (suitably Tate twisted) cohomology classes of cycles on powers of X which are linear combinations of intersections of divisor classes.

Suppose X is a simple abelian variety; recall the conventions surrounding the endomorphism algebra $D(X) = \text{End}(X) \otimes \mathbb{Q}$ introduced in Section 2. Say that k totally splits $D(X)$ if $E(X) \otimes_{\mathbb{Q}} k \cong \bigoplus_{\tau: E(X) \hookrightarrow k} k \cong k^{\oplus e(X)}$, and if for each $\tau: E(X) \hookrightarrow k$, one has $D(X) \otimes_{E(X), \tau} k \cong \text{Mat}_{d(X)}(k)$.

Lemma 3.1. *Let X be an absolutely simple abelian variety. Consider a Weil cohomology theory with coefficients in a field k , and suppose that k totally splits $D(X)$. There is a representation W_k of $\text{Lef}(X)_k$ such that $V(X)_k \cong W_k^{\oplus d(X)}$ as $\text{Lef}(X)_k$ -representations.*

Proof. Suppose k is algebraically closed. There exists an algebraic group $\widetilde{\text{Lef}}(X)_k$ and a natural isomorphism $\iota: \text{Lef}(X)_k \cong \bigoplus_{\sigma: F(X) \hookrightarrow k} \widetilde{\text{Lef}}(X)_k$ [18, Sec. 2]. Moreover, there exists a representation \widetilde{V}_k of $\widetilde{\text{Lef}}(X)_k$ such that, under the isomorphism ι , $V(X)_k$ and $\bigoplus_{\sigma: F(X) \hookrightarrow k} \widetilde{V}_k^{\oplus d(X)}$ are isomorphic representations of $\text{Lef}(X)_k$. Then $W_k := \bigoplus_{\sigma: F(X) \hookrightarrow k} \widetilde{V}_k$ is the sought-for decomposition of $V(X)_k$ as $\text{Lef}(X)_k$ representation. The analysis in [18, Sec. 2] relies only on the fact that the field of coefficients totally splits the endomorphism algebra, and thus the result holds under this weaker hypothesis on k . \square

Recall that for an abelian variety X over a number field K , $H_{X/K; \mathbb{Q}_\ell}$ is the Zariski closure of $\rho_{X/K, \mathbb{Z}_\ell}(\text{Gal}(K))$ in $\text{GL}(V(X)_{\mathbb{Q}_\ell})$.

Lemma 3.2. *Let X/K be an absolutely simple abelian variety over a number field. Suppose \mathbb{Q}_ℓ totally splits $D(X)$. Suppose that $H_{X/K; \mathbb{Q}_\ell}$ is connected. There is a representation $W_{\mathbb{Q}_\ell}$ of $\text{Gal}(K)$ such that, as $\text{Gal}(K)$ -modules,*

$$V(X)_{\mathbb{Q}_\ell} \cong W_{\mathbb{Q}_\ell}^{\oplus d(X)}.$$

Proof. Fix an embedding $K \hookrightarrow \mathbb{C}$, so that X has a natural structure of complex abelian variety. Associated to X is its Mumford-Tate group $\text{MT}(X)$. It is an algebraic subgroup of $\text{GL}(V(X)_{\mathbb{Q}})$, and there is a natural inclusion $\text{MT}(X) \subseteq \text{Lef}(X)_{\mathbb{Q}}$. Since comparison isomorphisms in cohomology furnish isomorphisms of Lefschetz groups, there are thus natural inclusions $\text{MT}(X) \times \mathbb{Q}_\ell \subseteq \text{Lef}(X)_{\mathbb{Q}} \times \mathbb{Q}_\ell \cong \text{Lef}(X)_{\mathbb{Q}_\ell}$. Work of Deligne, Piatetskii-Shapiro and Borovoi (see, for example [9, Prop. 2.9 and Thm. 2.11]) shows there is a natural inclusion

$$(3.1) \quad H_{X/K; \mathbb{Q}_\ell} \subseteq \text{MT}(X) \times_{\mathbb{Q}} \mathbb{Q}_\ell.$$

(In general, (3.1) holds only for the connected component $H_{X/K; \mathbb{Q}_\ell}^0$; the Mumford-Tate conjecture asserts that (3.1) is actually an equality.) By Lemma 3.1, there exists a representation $W_{\mathbb{Q}_\ell} \subseteq V(X)_{\mathbb{Q}_\ell}$ such that $V(X)_{\mathbb{Q}_\ell} \cong W_{\mathbb{Q}_\ell}^{\oplus d(X)}$. Therefore, $V(X)_{\mathbb{Q}_\ell} \cong W_{\mathbb{Q}_\ell}^{\oplus d(X)}$ as $H_{X/K; \mathbb{Q}_\ell}$ -modules, and thus as $\text{Gal}(K)$ -modules. \square

4. COMMUTATIVE ENDOMORPHISM RING

Theorem 4.1. *Let X/K be an absolutely simple abelian variety over a number field. Suppose $F = \text{End}_{\bar{k}}(X_{\bar{k}}) \otimes \mathbb{Q}$ is a totally real field. If $r = \dim X/[F : \mathbb{Q}]$ is odd then $S^*(X/K)$, the set of primes where X has good, absolutely simple reduction, has density one.*

Proof. Using Lemma 2.1, choose a finite Galois extension K'/K such that $(X/K, K')$ satisfies (2.1). Let $G = \mathbf{R}_{\mathcal{O}_F/\mathbb{Z}} \mathrm{GSp}_{2r}$, with derived group $G^{\mathrm{der}} = \mathbf{R}_{\mathcal{O}_F/\mathbb{Z}} \mathrm{Sp}_{2r}$. For all $\ell \gg 0$, the derived group of $H_{X/K', \ell}$ is $G^{\mathrm{der}}(\mathbb{Z}/\ell)$ [2, Thm. B] (see also [22] for the case $r = 1$), so that $H_{X/K', \ell}$ is of type $G(\mathbb{Z}/\ell)$. Moreover, X_ℓ is the natural representation of $H_{X/K', \ell}$. By Lemmas 1.1 and 1.3 and Proposition 2.8, $S^*(X/K) = 1$. \square

Theorem 4.2. *Let X/K be an absolutely simple abelian variety over a number field. Suppose there is some prime ℓ_0 such that $H_{X/K, \mathbb{Q}_{\ell_0}} = \mathrm{GSp}_{2g}(\mathbb{Q}_{\ell_0})$. Then $S^*(X/K)$ has density one.*

Proof. There is always an *a priori* inclusion $H_{X/K, \mathbb{Q}_\ell} \subseteq \mathrm{GSp}_{2g}(\mathbb{Q}_\ell)$. Since if the Mumford-Tate conjecture is true for X at one prime ℓ_0 it is true at all primes [16, Thm. 4.3], the hypothesis holds for every rational prime ℓ . A theorem of Larsen [17, Thm. 3.17], combined with Lemma 1.4, implies that for ℓ in a set of primes \mathbb{L} of density one, the derived subgroup $H_{X/K, \ell}^{\mathrm{der}}$ of the image of $\rho_{X/K, \ell}$ is $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell)$. Choose an extension K'/K such that $(X/K, K')$ satisfies (2.1). Then $H_{X/K', \ell}^{\mathrm{der}} \cong \mathrm{Sp}_{2g}(\mathbb{Z}/\ell)$ for ℓ in a set of primes $\mathbb{L}' \subseteq \mathbb{L}$ which still has density one. Again, Lemmas 1.1 and 1.3 and Proposition 2.8 show that $S^*(X/K)$ has density one. \square

Remark 4.3. Under the hypotheses of Theorem 4.2, Chai and Oort show that $S(X/K)$ has positive density [4, Rem. 5.4]. Under the apparently stronger hypothesis that $H_{X/K, \ell} = \mathrm{GSp}_{2g}(\mathbb{Z}/\ell)$ for all $\ell \gg 0$, Chavdarov shows that $S^*(X/K)$ has density one [5, Cor. 6.10].

Let X/K be an absolutely simple abelian variety of dimension g such that $D(X) = \mathrm{End}_{\bar{K}}(X) \otimes \mathbb{Q} \cong E$, a totally imaginary extension of \mathbb{Q} . Let $r = 2g/[E : \mathbb{Q}]$. Fix an embedding $E \hookrightarrow \mathbb{C}$; the tangent space $\mathrm{Lie}(X_{\mathbb{C}})$ of $X_{\mathbb{C}}$ is a g -dimensional vector space over \mathbb{C} , and thus a module over $E \otimes_{\mathbb{Q}} \mathbb{C} \cong \bigoplus_{\tau: E \rightarrow \mathbb{C}} \mathbb{C}$. Let m_τ be the \mathbb{C} -dimension of the subspace of $\mathrm{Lie}(X_{\mathbb{C}})$ on which E acts via τ . For $\tau \in \mathrm{hom}(E, \mathbb{C})$, let $\bar{\tau}$ denote the composition of τ with complex conjugation. Then $m_\tau + m_{\bar{\tau}} = r$ is independent of the choice of τ .

Vasiu has proved the Mumford-Tate conjecture for X , provided that the action of E on X is non-special [27, Thm. 1.3.4]. We defer a full exposition to *loc. cit.*, but note that each of the following is an example of a non-special action [27, 6.2.4]:

- (i) $r = 4$ or r is prime;
- (ii) there exists a $\tau \in \mathrm{hom}(E, \mathbb{C})$ such that $m_\tau = 1$;
- (iii) there exist τ and τ' such that $1 \leq m_\tau < m_{\tau'} \leq r/2$ and either $\mathrm{gcd}(m_\tau, r)$ or $\mathrm{gcd}(m_{\tau'}, r)$ is 1;
- (iv) there exists a τ such that $\mathrm{gcd}(m_\tau, m_{\bar{\tau}}) = 1$, and the natural numbers $(m_\tau, m_{\bar{\tau}})$ are not of the form $((\binom{i}{j-1}, \binom{i}{j}))$ for any natural numbers i and j .

The case of the Mumford-Tate conjecture where $[E : \mathbb{Q}] = 2$ and $r = g$ is prime is due to Chi [8, Cor. 3.2].

Theorem 4.4. *Let X/K be an absolutely simple abelian variety over a number field. Suppose $E := \mathrm{End}_{\bar{K}}(X_{\bar{K}}) \otimes \mathbb{Q}$ is a totally imaginary field, and that X is of non-special type. Then $S^*(X/K)$ has density one.*

Proof. Since Murty and Patankar have proved this result for abelian varieties of CM type [19, Thm. 3.1], we assume that $2 \dim X/[E : \mathbb{Q}] > 1$. Let K'/K be a finite extension such that $(X/K, K')$

satisfies (2.1). By [27, Thm. 1.3.4], the Mumford-Tate conjecture is true for each representation $\rho_{X/K, \mathbb{Q}_\ell} |_{\text{Gal}(K')}$. More precisely, there is a group $G/\mathbb{Z}[1/\Delta]$ of type (A) such that for almost all ℓ , the Zariski closure of $H_{X/K', \mathbb{Q}_\ell}$ is isomorphic to a subgroup of $G(\mathbb{Q}_\ell)$ which contains $G^{\text{der}}(\mathbb{Q}_\ell)$. By [17, Thm. 3.17] and Lemma 1.4, there is a set of primes \mathbb{L} of density one such that for $\ell \in \mathbb{L}$, $H_{X/K', \ell}$ is of type $G(\mathbb{Z}/\ell)$. Moreover, X_ℓ is the natural representation of $H_{X/K', \ell}$. Since the groups $G(\mathbb{Z}/\ell)$ satisfy Goursat's lemma (Lemma 1.3), $S^*(X/K)$ has density one by Lemma 1.1 and Proposition 2.8. \square

Via the Torelli functor, these results yield information about curves. For example, consider the following condition on a curve C over a field k :

(4.1) If $C \rightarrow D$ is finite of degree at least 2, then D has genus zero.

If the Jacobian $\text{Jac}(C)$ is simple, then C satisfies (4.1). The converse is true if the genus of C is at most 6, since almost every principally polarized abelian variety is a Jacobian in dimension at most 3.

Corollary 4.5. *Let C/K be a curve of odd prime genus g over a number field such that C/\bar{K} satisfies (4.1). Suppose that either $g \in \{3, 5\}$ or that $\text{Jac}(C)$ is absolutely simple. For almost all primes \mathfrak{p} , $C_{\mathfrak{p}}/\kappa(\mathfrak{p})$ satisfies (4.1).*

Proof. By hypothesis (and the preceding discussion), $\text{Jac}(C)$ is absolutely simple. A simple abelian variety of odd prime dimension over a number field has commutative endomorphism ring. This endomorphism ring is totally real or totally imaginary; and in the latter case, the action is not special. Now use Theorem 4.1 or 4.4 as appropriate. \square

In general, a curve C which satisfies (4.1) need not have reductions $C_{\mathfrak{p}}$ satisfying (4.1) for a dense, or even infinite, set of primes \mathfrak{p} . Indeed, let C be the second curve considered in the introduction. Then $\text{Jac}(C)$ is simple, thus C satisfies (4.1); but for each prime \mathfrak{p} of good reduction, $\text{Jac}(C_{\mathfrak{p}} \times \overline{\kappa(\mathfrak{p})})$ dominates, and thus $C_{\mathfrak{p}}$ covers, an elliptic curve.

5. NONCOMMUTATIVE ENDOMORPHISM RING

Recall the definitions of $D(X)$ and $d(X)$ from Section 2.

Proposition 5.1. *Let X/K be an absolutely simple abelian variety over a number field. Suppose that $\text{End}_{\bar{K}}(X_{\bar{K}})$ is noncommutative.*

- (a) *Then $R(X/K)$, the set of primes \mathfrak{p} such that $X_{\mathfrak{p}}$ is reducible, has positive density.*
- (b) *If $\text{End}_K(X) = \text{End}_{\bar{K}}(X)$ and $H_{X/K, \mathbb{Q}_\ell}$ is connected, then $R(X/K)$ has density one.*

Proof. Let K'/K be a finite extension such that $(X/K, K')$ satisfies (2.1); such an extension exists by Lemma 2.1. The conclusion of (b) for $X_{K'}$ implies the conclusion of (a) for X . Therefore, it suffices to assume $\text{End}_K(X) = \text{End}_{\bar{K}}(X)$ and that $H_{X/K, \mathbb{Q}_\ell}$ is connected, and then prove that $R(X/K) = M(X/K)$.

Consider the set \mathbb{L} of primes ℓ such that \mathbb{Q}_ℓ totally splits $D(X)$. Note that \mathbb{L} has positive density, and in particular is infinite. Suppose $\ell \in \mathbb{L}$. By Lemma 3.2, there exists a representation $W_{\mathbb{Q}_\ell}$ of $\text{Gal}(K)$ such that $T_\ell(X) \otimes \mathbb{Q} \cong W_{\mathbb{Q}_\ell}^{\oplus d(X)}$ as $\text{Gal}(K)$ -module. Note that $d(X) > 1$ since $D(X)$ is

noncommutative. By Lemma 2.6, for \mathfrak{p} in a subset of $M(X/K)$ of density one, $X_{\mathfrak{p}}$ is isogenous to $Y_{\mathfrak{p}}^{\oplus d(X)}$ for some abelian variety $Y_{\mathfrak{p}}/\kappa(\mathfrak{p})$. \square

Remark 5.2. In the special case of an abelian surface X with action by an indefinite quaternion algebra, X has absolutely split reduction at every prime of good reduction. This is explained in detail in [20, Sec. 2]; see also [4, Rem. 5.(ii)]. It is possible that Lemma 5.3 will yield a generalization of this. In the context of Proposition 5.1, Murty and Patankar show [19, Prop. 5.4] that $X_{\mathfrak{p}}$ is not simple at any prime \mathfrak{p} of *ordinary* reduction.

Lemma 5.3. *Let X/K be an absolutely simple abelian variety over a number field with noncommutative endomorphism algebra $D(X)$. Let Δ be the product of all (finite) primes of $E(X)$ which ramify in $D(X)$. Suppose $\mathfrak{p} \in M(X/K)$ is relatively prime to Δ . Then $E(X_{\mathfrak{p}})$ is ramified at every prime dividing Δ .*

Proof. Suppose $X_{\mathfrak{p}}$ is simple, and let p be the characteristic of $\kappa(\mathfrak{p})$. The inclusion $\text{End}(X) \hookrightarrow \text{End}(X_{\mathfrak{p}})$ forces $D(X_{\mathfrak{p}})$ to be noncommutative. By [25, Thm. 2(e)], $D(X_{\mathfrak{p}})$ is split at all primes not dividing p . In particular, $D(X_{\mathfrak{p}})$ is split at all primes not dividing Δ . Since only a ramified field extension splits a division algebra over a local field, $E(X_{\mathfrak{p}})$ must ramify at all primes dividing Δ . \square

If the endomorphism ring of X is an indefinite quaternion algebra, one knows more about the structure of the reductions $X_{\mathfrak{p}}$:

Theorem 5.4. *Let X/K be an absolutely simple abelian variety over a number field. Suppose that $\text{End}_{\bar{K}}(X_{\bar{K}}) \otimes \mathbb{Q}$ is an indefinite quaternion algebra over a totally real field F . If $\dim X/2[F : \mathbb{Q}]$ is odd, then for \mathfrak{p} in a set of positive density, $X_{\mathfrak{p}}$ is geometrically isogenous to the self-product of an absolutely simple abelian variety $Y_{\bar{\mathfrak{p}}}/\overline{\kappa(\mathfrak{p})}$ of dimension $(\dim X)/2$.*

Proof. Let K'/K be a finite extension of K such that $(X/K, K')$ satisfies (2.1). By [2, Thm. B], Lemma 1.1 and Lemma 1.3, there exists a group $G/\mathbb{Z}[1/\Delta]$ of type (C) and an infinite set of primes \mathbb{L} such that $(X/K', G/\mathbb{Z}[1/\Delta], \mathbb{L})$ satisfies (2.2). Moreover, there is a G -module $W/\mathbb{Z}[1/\Delta]$ such that for all $\ell \in \mathbb{L}$, $W \otimes \mathbb{Z}/\ell$ is an irreducible $G(\mathbb{Z}/\ell)$ -module and $X_{\ell} \cong (W \oplus W) \otimes \mathbb{Z}/\ell$ as $G(\mathbb{Z}/\ell)$ -module. (This is [2, Thm. 5.4]; see also [7] for the analogous statement for \mathbb{Q}_{ℓ} -modules.) The result now follows from Proposition 2.9. \square

ACKNOWLEDGEMENTS

My debt to the work of Murty and Patankar is obvious, and I thank V. Kumar Murty for sharing [19] with me in preprint form. It's also a pleasure to acknowledge helpful discussions with Bob Guralnick, Tim Penttila, Rachel Pries and David Zywinia, as well as comments from the referee.

REFERENCES

- [1] C. Adimoolam, *A note on good reduction of simple Abelian varieties*, Proc. Amer. Math. Soc. **64** (1977), no. 2, 196–198.
- [2] G. Banaszak, W. Gajda, and P. Krasoń, *On the image of l -adic Galois representations for abelian varieties of type I and II*, Doc. Math. (2006), no. Extra Vol., 35–75 (electronic).
- [3] Peter Bending, *Curves of genus 2 with $\sqrt{2}$ multiplication*, August 2006, arXiv:math.NT/991723, arXiv:math.NT/991723.
- [4] Ching-Li Chai and Frans Oort, *A note on the existence of absolutely simple Jacobians*, J. Pure Appl. Algebra **155** (2001), no. 2-3, 115–120.

- [5] Nick Chavdarov, *The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy*, Duke Math. J. **87** (1997), no. 1, 151–180.
- [6] Wên Chên Chi, *On the l -adic representations attached to some absolutely simple abelian varieties of type II*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **37** (1990), no. 2, 467–484.
- [7] ———, *On the Tate modules of absolutely simple abelian varieties of type II*, Bull. Inst. Math. Acad. Sinica **18** (1990), no. 2, 85–95.
- [8] ———, *On the l -adic representations attached to simple abelian varieties of type IV*, Bull. Austral. Math. Soc. **44** (1991), no. 1, 71–78.
- [9] Pierre Deligne, *Hodge cycles on abelian varieties*, Hodge cycles, motives, and Shimura varieties (Berlin), Lecture Notes in Mathematics, vol. 900, Springer-Verlag, 1982, pp. 9–100.
- [10] J. Ellenberg, C. Elsholtz, C. Hall, and E. Kowalski, *Non-simple abelian varieties in a family: geometric and analytic approaches*, J. London Math. Soc. (2008), arXiv:0804.2166, in press.
- [11] Peter Fleischmann and Ingo Janiszczak, *The number of regular semisimple elements for Chevalley groups of classical type*, J. Algebra **155** (1993), no. 2, 482–528.
- [12] Tomoyoshi Ibukiyama, Toshiyuki Katsura, and Frans Oort, *Supersingular curves of genus two and class numbers*, Compositio Math. **57** (1986), no. 2, 127–152.
- [13] Jun-ichi Igusa, *Arithmetic variety of moduli for genus two*, Ann. of Math. (2) **72** (1960), 612–649.
- [14] E. Kowalski, *Weil numbers generated by other Weil numbers and torsion fields of abelian varieties*, J. London Math. Soc. (2) **74** (2006), no. 2, 273–288.
- [15] Tomio Kubota, *On the field extension by complex multiplication*, Trans. Amer. Math. Soc. **118** (1965), 113–122.
- [16] M. J. Larsen and R. Pink, *Abelian varieties, l -adic representations, and l -independence*, Math. Ann. **302** (1995), no. 3, 561–579.
- [17] Michael J. Larsen, *Maximality of Galois actions for compatible systems*, Duke Math. J. **80** (1995), no. 3, 601–630.
- [18] J. S. Milne, *Lefschetz classes on abelian varieties*, Duke Math. J. **96** (1999), no. 3, 639–675.
- [19] V. K. Murty and V. M. Patankar, *Splitting of abelian varieties*, IMRN **2008** (2008), Art. ID rnn033, 27 pages.
- [20] V. Kumar Murty, *Splitting of abelian varieties: a new local-global problem*, Algebra and number theory, Hindustan Book Agency, Delhi, 2005, pp. 258–268.
- [21] K. A. Ribet, *Division fields of abelian varieties with complex multiplication*, Mém. Soc. Math. France (N.S.) (1980/81), no. 2, 75–94, Abelian functions and transcendental numbers (Colloq., École Polytech., Palaiseau, 1979).
- [22] Kenneth A. Ribet, *Galois action on division points of Abelian varieties with real multiplications*, Amer. J. Math. **98** (1976), no. 3, 751–804.
- [23] A. Silverberg, *Fields of definition for homomorphisms of abelian varieties*, J. Pure Appl. Algebra **77** (1992), no. 3, 253–262.
- [24] A. Silverberg and Yu. G. Zarhin, *Connectedness extensions for abelian varieties*, Math. Z. **228** (1998), no. 2, 387–403.
- [25] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144.
- [26] ———, *Classes d’isogénie des variétés abéliennes sur un corps fini (d’après T. Honda)*, Séminaire Bourbaki, no. 352, 1968, pp. 95–110.
- [27] Adrian Vasiu, *Some cases of the Mumford-Tate conjecture and Shimura varieties*, Indiana Univ. Math. J. **57** (2008), 1–76.
- [28] David Zywina, *The large sieve and galois representations*, Ph.D. thesis, University of California, Berkeley, 2008.

E-mail address: j.achter@colostate.edu

DEPARTMENT OF MATHEMATICS, COLORADO STATE UNIVERSITY, FORT COLLINS, CO 80523-1874

URL: <http://www.math.colostate.edu/~achter>