ELSEVIER Journal of Pure and Applied Algebra 132 (1998) 179–193

JOURNAL OF
PURE AND
APPLIED ALGEBRA

Semistable reduction of abelian varieties over extensions of small degree

A. Silverberg[a,*,1], Yu. G. Zarhin[b,c,2]

[a] Department of Mathematics, Ohio State University, Columbus, OH 43210-1174, USA
[b] Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA
[c] Institute for Mathematical Problems in Biology, Russian Academy of Sciences, Pushchino, Moscow Region, 142292, Russia

Communicated by E.M. Friedlander; received 20 February 1997

Abstract

We obtain necessary and sufficient conditions for abelian varieties to acquire semistable reduction over fields of low degree. Our criteria are expressed in terms of torsion points of small order defined over unramified extensions. © 1998 Elsevier Science B.V. All rights reserved.

AMS Classification: Primary 11G10; Secondary 14K15

1. Introduction

In this paper we obtain criteria for abelian varieties to acquire semistable reduction over fields of certain given (small) degrees. Our criteria are expressed in terms of unramified torsion points.

Suppose that X is an abelian variety defined over a field F, and n is a positive integer not divisible by the characteristic of F. Let X^* denote the dual abelian variety of X, let X_n denote the kernel of multiplication by n in $X(F^s)$, where F^s denotes a separable closure of F, let X_n^* denote the kernel of multiplication by n in $X^*(F^s)$, and let $\boldsymbol{\mu}_n$ denote the $\mathrm{Gal}(F^s/F)$-module of nth roots of unity in F^s. The Weil pairing $e_n : X_n \times X_n^* \to \boldsymbol{\mu}_n$ is a $\mathrm{Gal}(F^s/F)$-equivariant non-degenerate pairing. If S is a subgroup of X_n, let

$$S^{\perp_n} = \{y \in X_n^* : e_n(x, y) = 1 \text{ for every } x \in S\} \subseteq X_n^*.$$

[*] Correspondence author. E-mail: silver@math.ohio-state.edu
[1] Partially supported by the National Security Agency.
[2] Partially supported by the National Science Foundation.

PII: S0022-4049(97)000121-7

For example, if $n = m^2$ and $S = X_m$, then $S^{\perp_n} = X_m^*$. If X is an elliptic curve and S is a cyclic subgroup of order n, then $S^{\perp_n} = S$. Suppose that v is a discrete valuation on F whose residue characteristic does not divide n.

Previously, we showed that if $n \geq 5$ then X has semistable reduction at v if and only if there exists a subgroup S of X_n such that all the points on S and on $S^{\perp_n}$ are defined over an extension of F unramified over v (see [15, Theorem 4.5]; see also [16, Theorem 6.2]). In the current paper we show that if there exists a subgroup S of X_n, for $n = 2$, 3, or 4 (respectively), such that all the points on S and on $S^{\perp_n}$ are defined over an extension of F unramified over v, then X acquires semistable reduction over every degree 4, 3, or 2 (respectively) extension of F totally ramified above v. We also give necessary and sufficient conditions for semistable reduction over quartic, cubic, and quadratic extensions. Namely, if L is a totally ramified extension of F of degree 4, 3, or 2, respectively, then X has semistable reduction over L if and only if there exist a finite unramified extension K of F, an abelian variety Y over K which is K-isogenous to X, and a subgroup S of Y_n, for $n = 2$, 3, or 4, respectively, such that all the points of S and of $S^{\perp_n}$ are defined over an unramified extension of K. If X is an elliptic curve one may take $Y = X$. This is not true already for abelian surfaces. However, one may take $Y = X$ in the special case where X has purely additive and potentially good reduction, with no restriction on the dimension.

The study of torsion subgroups of abelian varieties with purely additive reduction was initiated in [9] and pursued in [10] (see [4,3] for the case of elliptic curves). See p. 312 of [12] and [8] for information on the smallest extension over which an elliptic curve with additive and potentially good reduction acquires good reduction.

We state and prove Theorem 5.2 in the generality $n \geq 2$ (rather than just $2 \leq n \leq 4$) since doing so requires no extra work and affords us the opportunity to give a slightly different exposition from that in [15] for $n \geq 5$, which highlights the method. See Section 5 for our major results, see Section 6 for applications and refinements, and see Section 7 for examples which demonstrate that our results are sharp.

2. Notation and definitions

Define

$$R(n) = 1 \text{ if } n \geq 5, \quad R(4) = 2, \quad R(3) = 3, \quad R(2) = 4.$$

If X is an abelian variety over a field F, and ℓ is a prime not equal to the characteristic of F, let

$$\rho_{\ell,X} : \mathrm{Gal}(F^s/F) \to \mathrm{Aut}(T_\ell(X))$$

denote the ℓ-adic representation on the Tate module $T_\ell(X)$ of X. We will write ρ_ℓ when there is no ambiguity. Let $V_\ell(X) = T_\ell(X) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$.

If L is a Galois extension of F and w is an extension of v to L, let $\mathscr{I}(w/v)$ denote the inertia subgroup at w of $\mathrm{Gal}(L/F)$. Throughout this paper we will let $\mathscr{I}$ denote

$\mathscr{I}(\bar{v}/v)$, where $\bar{v}$ is a fixed extension of v to F^s, and we will let $\mathscr{J}$ denote the first ramification group (i.e., the wild inertia group). We also write $\mathscr{I}_w$ for $\mathscr{I}(\bar{v}/w)$.

Definition 2.1. Suppose L/F is an extension of fields, w is a discrete valuation on L, and v is the restriction of w to F. Let $e(w/v) = [w(L^\times) : v(F^\times)]$. We say that w/v is *unramified* if $e(w/v) = 1$ and the residue field extension is separable. We say that w/v is *totally ramified* if w is the unique extension of v to L and the residue field extension is purely inseparable. We say that w/v is *tamely ramified* if the residue field extension is separable and $e(w/v)$ is not divisible by the residue characteristic.

3. Preliminaries

Theorem 3.1. *Suppose n is an integer, $n \geq 2$, $\mathcal{O}$ is an integral domain of characteristic zero such that no rational prime which divides n is a unit in $\mathcal{O}$, $\alpha \in \mathcal{O}$, α has finite multiplicative order, and $(\alpha - 1)^2 \in n\mathcal{O}$. Then $\alpha^{R(n)} = 1$.*

Proof. See Corollary 3.3 of [17]. □

Lemma 3.2 (Silverberg and Zarhin [16, Lemma 5.2]). *Suppose that d and n are positive integers, and for each prime ℓ which divides n we have a matrix $A_\ell \in M_{2d}(\mathbf{Z}_\ell)$ such that the characteristic polynomials of the A_ℓ have integral coefficients independent of ℓ, and such that $(A_\ell - 1)^2 \in nM_{2d}(\mathbf{Z}_\ell)$. Then for every eigenvalue α of A_ℓ, $(\alpha - 1)/\sqrt{n}$ satisfies a monic polynomial with integer coefficients.*

Theorem 3.3 (Galois criterion for semistable reduction). *Suppose X is an abelian variety over a field F, v is a discrete valuation on F, and ℓ is a prime not equal to the residue characteristic of v. Then the following are equivalent:*

(i) *X has semistable reduction at v,*

(ii) *$\mathscr{I}$ acts unipotently on $T_\ell(X)$; i.e., all the eigenvalues of $\rho_\ell(\sigma)$ are 1, for every $\sigma \in \mathscr{I}$,*

(iii) *for every $\sigma \in \mathscr{I}$, $(\rho_\ell(\sigma) - 1)^2 = 0$.*

Proof. See Proposition 3.5 and Corollary 3.8 of [6] and Theorem 6 on p. 184 of [1]. □

Lemma 3.4. *Suppose ℓ is a prime number and ζ is a primitive ℓ^sth root of unity. Then*

$$\frac{(\zeta - 1)^{\varphi(\ell^s)}}{\ell}$$

is a unit in $\mathbf{Z}[\zeta]$.

Proof. See, for example, the last two lines on p. 9 of [18]. □

4. Lemmas

Remark 4.1. Suppose w is a discrete valuation on a field L, L is a finite extension of a field F, v is the restriction of w to F, and w/v is totally and tamely ramified. Then the maximal unramified extension L_{nr} of L is the compositum of L with the maximal unramified extension F_{nr} of F. Further, L_{nr}/F_{nr} is a cyclic extension whose degree is $[L:F]$ (see [5, Section 8, especially Corollary 3 on p. 31]). Since passing to the maximal unramified extensions does not change the inertia groups, it follows that $\mathcal{I}_w$ is a normal subgroup of $\mathcal{I}$, and $\mathcal{I}/\mathcal{I}_w$ is cyclic of order $[L:F]$.

Lemma 4.2. *Suppose v is a discrete valuation on a field F with residue characteristic $p \geq 0$, R is a positive integer, ℓ is a prime, p does not divide $R\ell$, and L is a degree R extension of F which is totally ramified above v. Suppose that X is an abelian variety over F, and for every $\sigma \in \mathcal{I}$, all the eigenvalues of $\rho_\ell(\sigma)$ are Rth roots of unity. Then X has semistable reduction at the extension of v to L.*

Proof. This was proved in Lemma 5.5 of [16] in the case where L is Galois over F. However, the same proof also works in general. This follows from the fact that in the proof we replaced F by its maximal unramified extension. For fields which have no non-trivial unramified extensions, every totally and tamely ramified extension is cyclic (and therefore Galois), and for each degree prime to the residue characteristic, there is a unique totally ramified extension of that degree. See Section 8 of [5], especially Corollary 3 on p. 31. □

The following result yields a converse of Theorem 5.1 of [17].

Lemma 4.3. *Suppose $\mathcal{O}$ is an integral domain of characteristic zero, and ℓ is a prime number. Suppose k, r, and m are positive integers such that $k \geq m\varphi(\ell^r)$. Suppose $\alpha \in \mathcal{O}$ and $\alpha^{\ell^r} = 1$. Then $(\alpha - 1)^k \in \ell^m \mathbf{Z}[\alpha]$.*

Proof. Let s be the smallest positive integer such that $\alpha^{\ell^s} = 1$. Then

$$(\alpha - 1)^k \in (\alpha - 1)^{m\varphi(\ell^s)}\mathbf{Z}[\alpha] \subseteq \ell^m \mathbf{Z}[\alpha],$$

by Lemma 3.4. □

Lemma 4.4. *Suppose X is an abelian variety over a field F, v is a discrete valuation on F, n and m are integers, and n is not divisible by the residue characteristic of v. Suppose $\sigma \in \mathcal{I}$. If there exists a subgroup S of X_n such that $(\sigma^m - 1)S = 0$ and $(\sigma^m - 1)S^{\perp_n} = 0$, then $(\sigma^m - 1)^2 X_n = 0$.*

Proof. The map $x \mapsto (y \mapsto e_n(x, y))$ induces a $\mathrm{Gal}(F^s/F)$-equivariant isomorphism from X_n/S onto $\mathrm{Hom}(S^{\perp_n}, \boldsymbol{\mu}_n)$. Since $\sigma = 1$ on $\boldsymbol{\mu}_n$, and $\sigma^m = 1$ on $S^{\perp_n}$, it follows that $\sigma^m = 1$ on X_n/S. Therefore, $(\sigma^m - 1)^2 X_n \subseteq (\sigma^m - 1)S = 0$. □

Lemma 4.5. *Suppose X is an abelian variety over a field F, v is a discrete valuation on F, n is an integer not divisible by the residue characteristic of v, and $S = X_n^{\mathcal{I}}$. Then $\mathcal{I}$ acts as the identity on $S^{\perp_n}$ if and only if $(\sigma - 1)^2 X_n = 0$ for every $\sigma \in \mathcal{I}$.*

Proof. Applying Lemma 4.4 with $m = 1$, we obtain the forward implication.

Conversely, suppose that $(\sigma - 1)^2 X_n = 0$ for every $\sigma \in \mathcal{I}$. Writing $\sigma^n = ((\sigma - 1) + 1)^n$, it is easy to see that $\sigma^n = 1$ on X_n for every $\sigma \in \mathcal{I}$. Since n is not divisible by the residue characteristic of v, X_n and X_n^* are tamely ramified at v. Then the action of $\mathcal{I}$ on X_n and on X_n^* factors through the tame inertia group $\mathcal{I}/\mathcal{J}$. Let τ denote a lift to $\mathcal{I}$ of a topological generator of the pro-cyclic group $\mathcal{I}/\mathcal{J}$. Since

$$e_n((\tau - 1)X_n, (X_n^*)^{\mathcal{I}}) = 1,$$

we have

$$\#((X_n^*)^{\mathcal{I}})\#((\tau - 1)X_n) \leq \#X_n^*.$$

The map from X_n to $(\tau - 1)X_n$ defined by $y \mapsto (\tau - 1)y$ defines a short exact sequence

$$0 \to S \to X_n \to (\tau - 1)X_n \to 0.$$

Therefore,

$$\#S\#((\tau - 1)X_n) = \#X_n = \#S\#S^{\perp_n}.$$

Similarly,

$$\#((X_n^*)^{\mathcal{I}})\#((\tau - 1)X_n^*) = \#X_n^*.$$

Therefore,

$$\#S^{\perp_n} = \#((\tau - 1)X_n) \leq \#((\tau - 1)X_n^*).$$

Since $(\tau - 1)X_n^* \subseteq S^{\perp_n}$, we conclude that

$$S^{\perp_n} = (\tau - 1)X_n^*.$$

From the natural $\mathrm{Gal}(F^s/F)$-equivariant isomorphism $X_n^* \cong \mathrm{Hom}(X_n, \boldsymbol{\mu}_n)$ it follows that $(\tau - 1)^2 X_n^* = 0$. Therefore, $\mathcal{I}$ acts as the identity on $S^{\perp_n}$. □

Lemma 4.6. *Suppose X is an abelian variety over a field F, v is a discrete valuation on F, and n is an integer not divisible by the residue characteristic of v. If X has semistable reduction at v, then*

(i) *$(\sigma - 1)^2 X_n = 0$ for every $\sigma \in \mathcal{I}$,*

(ii) *$\mathcal{I}$ acts as the identity on $(X_n^{\mathcal{I}})^{\perp_n}$,*

(iii) *$(\sigma^n - 1)X_n = 0$ for every $\sigma \in \mathcal{I}$; in particular, X_n is tamely ramified at v.*

Proof. By Theorem 3.3, we have (i). By Lemma 4.5, we have (ii). In the proof of Lemma 4.5, we showed that (i) implies (iii). □

Lemma 4.7. *Suppose X is an abelian variety over a field F, v is a discrete valuation on F of residue characteristic $p \geq 0$, and ℓ is a prime number not equal to p. If X_ℓ is tamely ramified at v, then $T_\ell(X)$ is tamely ramified at v.*

Proof. If $p = 0$ then the wild inertia group $\mathscr{J}$ is trivial and we are done. Suppose $p > 0$ and $\sigma \in \mathscr{J}$. Since $p \neq \ell$, $\rho_\ell(\mathscr{J})$ is a finite p-group. Therefore, $\rho_\ell(\sigma)$ has order a power of p. Since X_ℓ is tamely ramified, $\rho_\ell(\sigma) - 1 \in \ell\mathrm{End}(T_\ell(X))$. It follows that $\rho_\ell(\sigma) = 1$ if $\ell \geq 3$, and $\rho_\ell(\sigma)^2 = 1$ if $\ell = 2$. Since p and ℓ are relatively prime, $\rho_\ell(\sigma) = 1$. □

Lemma 4.8. *Suppose X is an abelian variety over a field F, $n = 2$, 3, or 4, ℓ is the prime divisor of n, v is a discrete valuation on F whose residue characteristic is not ℓ, t is a non-negative integer, L is an extension of F of degree $R(n)^{t+1}$ which is totally ramified above v, and X has semistable reduction over L above v. Let τ denote a lift to $\mathscr{I}$ of a topological generator of the pro-cyclic group $\mathscr{I}/\mathscr{J}$. Let $\gamma = \rho_\ell(\tau)^{R(n)^t}$, let $\lambda = (\gamma - 1)^2/n$, and let*

$$T = T_\ell(X) + \lambda T_\ell(X) + \lambda^2 T_\ell(X) + \cdots + \lambda^{R(n)-1} T_\ell(X).$$

Then:

(a) *T is the smallest λ-stable $\mathbf{Z}_\ell$-lattice in $V_\ell(X)$ which contains $T_\ell(X)$,*
(b) *$(\gamma^{R(n)} - 1)^2 = 0$,*
(c) *$n^{R(n)-1} T \subseteq T_\ell(X) \subseteq T$,*
(d) *$(\gamma - 1)^{2R(n)} \subseteq nT_\ell(X)$,*
(e) *if $n = 2$ or 3, then $nT \subseteq T_\ell(X)$ if and only if $(\gamma - 1)^4 T_\ell(X) \subseteq nT_\ell(X)$,*
(f) *if $n = 2$, then $4T \subseteq T_2(X)$ if and only if $(\gamma - 1)^6 T_2(X) \subseteq 2T_2(X)$,*
(g) *if $n = 4$, then $2T \subseteq T_2(X)$ if and only if $(\gamma - 1)^2 T_2(X) \subseteq 2T_2(X)$.*

Proof. Let w denote the restriction of $\bar{v}$ to L. By Remark 4.1, $\mathscr{I}/\mathscr{I}_w$ is cyclic of order $R(n)^{t+1}$. By Theorem 3.3, we have (b). It follows that $(\lambda + \gamma)^2(\lambda + \gamma - 1)^2 = 0$ if $n = 2$, $\lambda(\lambda + \gamma)^2 = 0$ if $n = 3$, and $\lambda(\lambda + \gamma) = 0$ if $n = 4$. Therefore, λ satisfies a polynomial over $\mathbf{Z}[\gamma]$ of degree $R(n)$, and we have (a) and (c). From the definition of T we easily deduce (e), (f), and (g). Further, (d) follows from (b). □

We will apply the following result only in Corollary 6.2(e).

Theorem 4.9. *Suppose L/F is a finite separable field extension, w is a discrete valuation on L, and v is the restriction of w to F. Suppose X is a d-dimensional abelian variety over F which has semistable reduction at w but not at v. Then $[\mathscr{I}_v : \mathscr{I}_w]$ has a prime divisor q such that $q \leq 2d + 1$.*

Proof. Let ℓ be a prime not equal to the residue characteristic p, and let

$$\mathscr{I}_{v,X} = \{\sigma \in \mathscr{I}_v : \sigma \text{ acts unipotently on } V_\ell(X)\}.$$

We have $\mathscr{I}_w \subseteq \mathscr{I}_{v,X} \subsetneqq \mathscr{I}_v$ by Theorem 3.3, since X has semistable reduction at w but not at v. Let F_v be the completion of F at v and let F_v^{nr} be the maximal unramified extension of F_v. Then $\mathscr{I}_{v,X}$ is an open normal subgroup of $\mathscr{I}_v$, is independent of ℓ, and cuts out the smallest Galois extension F' of F_v^{nr} over which X has semistable reduction (see [6, pp. 354–355]). We have $\mathrm{Gal}(F'/F_v^{nr}) \cong \mathscr{I}_v/\mathscr{I}_{v,X}$. By a theorem of Raynaud (see [6, Proposition 4.7]), X has semistable reduction over $F_v^{nr}(X_n)$, for every integer n not divisible by p and greater than 2. The intersection M of these fields therefore contains F'. As on the top of p. 498 of [13], every prime divisor of $[M:F_v^{nr}]$ is at most $2d+1$ (see [14], Theorem 4.1 and Formula 3.1 for an explicit integer that $[M:F_v^{nr}]$ divides). Thus, if q is a prime divisor of $[\mathscr{I}_v : \mathscr{I}_{v,X}]$ then $q \leq 2d+1$. Since $\mathscr{I}_w \subseteq \mathscr{I}_{v,X} \subsetneqq \mathscr{I}_v$, we obtain the desired result. □

Remark 4.10. With hypotheses and notation as in Theorem 4.9, let k_w and k_v denote the residue fields. Then $[\mathscr{I}_v : \mathscr{I}_w] = e(w/v)[k_w : k_v]_i$, where the subscript i denotes the inseparable degree (see [11], Proposition 21 on p. 32, for the case where L/F is Galois. In the non-Galois case, take a Galois extension L' of F which contains L, and apply the result to L'/L and L'/F, to obtain the result for L/F). Taking completions, then $[L_w : F_v] = e(w/v)[k_w : k_v] = [\mathscr{I}_v : \mathscr{I}_w][k_w : k_v]_s$, where the subscript s denotes the separable degree. Therefore, the prime q from Theorem 4.9 divides $[L_w : F_v]$.

5. Semistable reduction

The results in this section extend the results of [15] to the cases $n = 2,3,4$. Theorem 5.2 is also a generalization of Corollary 7.1 of [16].

Remark 5.1. Suppose X is an abelian variety over a field F, v is a discrete valuation on F, and n is an integer greater than 1 which is not divisible by the residue characteristic of v. By Lemma 4.5, the following two statements are equivalent:

(a) there exists a subgroup S of X_n such that $\mathscr{I}$ acts as the identity on S and on $S^{\perp_n}$,

(b) $(\sigma - 1)^2 X_n = 0$ for every $\sigma \in \mathscr{I}$.

Theorem 5.2. *Suppose X is an abelian variety over a field F, v is a discrete valuation on F, and n is an integer greater than* 1 *which is not divisible by the residue characteristic of v. Suppose there exists a subgroup S of X_n such that $\mathscr{I}$ acts as the identity on S and on $S^{\perp_n}$. Then X has semistable reduction over every degree $R(n)$ extension of F totally ramified above v.*

Proof. Suppose $\sigma \in \mathscr{I}$. By Lemma 4.5, $(\sigma - 1)^2 X_n = 0$. Let $\mathscr{I}' \subseteq \mathscr{I}$ be the inertia group for the prime below $\bar{v}$ in a finite Galois extension of F over which X has semistable reduction. Then $\sigma^r \in \mathscr{I}'$ for some r. Let ℓ be a prime divisor of n. Theorem 3.3 implies that $(\rho_\ell(\sigma)^r - 1)^2 = 0$. Let α be an eigenvalue of $\rho_\ell(\sigma)$. Then $(\alpha^r - 1)^2 = 0$.

Therefore, $\alpha^r = 1$. By our hypothesis,

$$(\rho_\ell(\sigma) - 1)^2 \in n\mathrm{M}_{2\mathrm{d}}(\mathbf{Z}_\ell),$$

where $d = \dim(X)$. By Théorème 4.3 of [6], the characteristic polynomial of $\rho_\ell(\sigma)$ has integer coefficients which are independent of ℓ. By Lemma 3.2, $(\alpha - 1)^2 \in n\bar{\mathbf{Z}}$, where $\bar{\mathbf{Z}}$ denotes the ring of algebraic integers. By Theorem 3.1 we have $\alpha^{R(n)} = 1$. The result now follows from Lemma 4.2. □

Corollary 5.3 (Silverberg and Zarhin [15, Theorem 4.5]). *Suppose X is an abelian variety over a field F, v is a discrete valuation on F, n is an integer not divisible by the residue characteristic of v, and $n \geq 5$. Then X has semistable reduction at v if and only if there exists a subgroup S of X_n such that $\mathscr{I}$ acts as the identity on S and on $S^{\perp_n}$.*

Proof. If X has semistable reduction at v, then by Theorem 3.3, $(\sigma - 1)^2 X_n = 0$ for every $\sigma \in \mathscr{I}$. Apply Lemma 4.5.

For the converse, apply Theorem 5.2 with $n \geq 5$. □

Remark 5.4. It follows immediately from Theorem 3.3 and Lemma 4.5 that if X has semistable reduction above v over a degree m extension of F totally ramified above v, then there exists a subgroup S of X_n such that $\mathscr{I}$ acts via a cyclic quotient of order m on S and on $S^{\perp_n}$. (If L is the extension of F, let w be the restriction of $\bar{v}$ to L and let $S = X_n^{\mathscr{I}_w}$.) Theorem 5.5 below gives a different result in the direction converse to Theorem 5.2, and, further, gives conditions for semistable reduction which are both necessary and sufficient, thereby giving a generalization of Corollary 5.3 to the cases $n = 2, 3, 4$. Note that in the case $n \geq 5$, the equivalence of (i) and (ii) in Theorem 5.5 is just a restatement of Corollary 5.3 (since $R(n) = 1$ if $n \geq 5$). We remark that in that case, one can take (in the notation of Theorem 5.5) $Y = X$ and φ the identity map.

Theorem 5.5. *Suppose $n = 2$, 3, or 4, respectively. Suppose X is an abelian variety over a field F, and v is a discrete valuation on F whose residue characteristic does not divide n. Suppose t is a non-negative integer and L is an extension of F of degree $R(n)^{t+1}$ which is totally ramified above v. Then the following are equivalent:*

(i) *X has semistable reduction over L above v,*

(ii) *there exist an abelian variety Y over a finite extension K of F unramified above v, a separable K-isogeny $\varphi : X \to Y$, and a subgroup S of Y_n such that $\mathscr{I}$ acts via a cyclic quotient of order $R(n)^t$ on S and on $S^{\perp_n}$.*

One can take φ so that its kernel is killed by 8, 9, *or* 4, *respectively. If X has potentially good reduction at v, then one can take φ so that its kernel is killed by* 2, 3, *or* 2, *respectively.*

Proof. Let ℓ denote the prime divisor of n.

Suppose K is a finite extension of F unramified above v, Y is an abelian variety over K, X and Y are K-isogenous, and S is a subgroup of Y_n such that $\mathscr{I}$ acts via a cyclic quotient of order $R(n)^t$ on S and on $S^{\perp_n}$. Suppose $\sigma \in \mathcal{I}$. By Lemma 4.4, $(\sigma^{R(n)^t} - 1)^2 Y_n = 0$, i.e.,

$$(\rho_{\ell,Y}(\sigma^{R(n)^t}) - 1)^2 \in nM_{2d}(\mathbf{Z}_\ell).$$

Let α be an eigenvalue of $\rho_{\ell,Y}(\sigma)$. Since Y has potentially semistable reduction, α is a root of unity. By Theorem 3.1, $(\alpha^{R(n)^t})^{R(n)} = 1$. Therefore, all eigenvalues of $\rho_{\ell,Y}(\sigma)$ are $R(n)^{t+1}$-th roots of unity. By Lemma 4.2, Y has semistable reduction over LK above v. Since X and Y are K-isogenous and K/F is unramified above v, X has semistable reduction over L above v.

Conversely, suppose X has semistable reduction over L above v. By Lemma 4.6(iii), for every $\sigma \in \mathcal{I}$ we have $(\sigma^{nR(n)^{t+1}} - 1)X_n = 0$. Since $nR(n)^{t+1}$ is not divisible by the residue characteristic, X_n is tamely ramified at v. Then the action of $\mathcal{I}$ on X_n factors through $\mathcal{I}/\mathcal{J}$. Let τ denote a lift to $\mathcal{I}$ of a topological generator of the pro-cyclic group $\mathcal{I}/\mathcal{J}$. Let T denote the $\mathbf{Z}_\ell$-lattice obtained from Lemma 4.8. By Lemma 4.7, T is stable under $\mathcal{I}$. Note that $n^{R(n)-1} = 8$, 9, or 4 when $n = 2$, 3, or 4, respectively. Let $C = T/T_\ell(X)$, and view C as a subgroup of X_8, X_9, or X_4, respectively. Let $Y = X/C$. Then the projection map $X \to Y$ is a separable isogeny defined over a finite separable extension K of F which is unramified over v,

$$T_\ell(Y) = T \quad \text{and} \quad (\rho_{\ell,Y}(\tau)^{R(n)^t} - 1)^2 Y_n = 0.$$

Let K' (respectively, L') be the maximal unramified extension of K (respectively, L) in F^s, let M be the degree $R(n)^t$ extension of K' in $K'L'$ cut out by $\tau^{R(n)^t}$, let w be the restriction of $\bar{v}$ to M, and let $S = Y_n^{\mathcal{J}_w}$. Then $\tau^{R(n)^t}$ is a lift to $\mathcal{I}_w$ of a topological generator of the pro-cyclic group $\mathcal{I}_w/\mathcal{J}_w$, where $\mathcal{J}_w$ is the first ramification group of $\mathcal{I}_w$. By Lemma 4.5, $\tau^{R(n)^t}$ acts as the identity on S and on $S^{\perp_n}$. Therefore, $\mathcal{I}$ acts on S and on $S^{\perp_n}$ via the cyclic group $\mathcal{I}/\mathcal{I}_w \cong \mathrm{Gal}(M/K')$.

As in Lemma 4.8, let $\gamma = \rho_{\ell,X}(\tau)^{R(n)^t}$ and let $\lambda = (\gamma - 1)^2/n$. If X has potentially good reduction at v, then $\gamma^{R(n)} = 1$. Let $\mu = \lambda + \gamma$. Then $\mu^2 = \mu$ and $T = T_\ell(X) + \mu T_\ell(X)$. Since $\mu = (\gamma^2 + 1)/2$ if $n = 2$, $\mu = (\gamma^2 + \gamma + 1)/3$ if $n = 3$, and $\mu = (\gamma + 1)/2$ if $n = 4$, it follows that C is a subgroup of X_2, X_3, or X_2, respectively. □

Since the most interesting case of Theorem 5.5 is the case $t = 0$, we explicitly state that case.

Corollary 5.6. *Suppose $n = 2$, 3, or 4, respectively. Suppose X is an abelian variety over a field F, and v is a discrete valuation on F whose residue characteristic does not divide n. Suppose L is an extension of F of degree 4, 3, or 2, respectively, which is totally ramified above v. Then the following are equivalent:*

(i) *X has semistable reduction over L above v,*

(ii) *there exist an abelian variety Y over a finite extension K of F unramified above v, a separable K-isogeny $\varphi : X \to Y$, and a subgroup S of Y_n such that $\mathcal{I}$ acts as the identity on S and on $S^{\perp_n}$.*

Further, φ can be taken so that its kernel is killed by 8, 9, *or* 4, *respectively. If X has potentially good reduction at v, then φ can be taken so that its kernel is killed by* 2, 3, *or* 2, *respectively.*

6. Applications and refinements

In the next result we show that the numbers in Theorem 5.5 and Corollary 5.6 can be improved for abelian varieties of dimension 1, 2 (if $n = 2$ or 3), and 3 (if $n = 2$). In Section 7 we show that the numbers in Theorem 6.1 are sharp. See also [7], which deals with other problems concerned with finding a “good” abelian variety in an isogeny class, with an answer depending on the dimension.

Theorem 6.1. *In Theorem 5.5 and Corollary 5.6, with $d = \dim(X)$, φ can be taken so that its kernel is killed by* 4 *if $d = 3$ and $n = 2$, by* 3 *if $d = 2$ and $n = 3$, and by* 2 *if $d = n = 2$. If $d = 1$, then we can take $Y = X$ and φ the identity map.*

Proof. We use the notation from Lemma 4.8 and from the proof of Theorem 5.5.

Suppose $n = 2$ or 3. By Lemma 4.8(d), γ acts unipotently on the $\mathbf{F}_\ell$-vector space $X_\ell \cong 1/\ell T_\ell(X)/T_\ell(X)$. Therefore, $(\gamma - 1)^{2d} X_\ell = 0$. By Lemma 4.8(e), if $d = 2$ then C is killed by n. By Lemma 4.8(f), if $n = 2$ and $d = 3$, then C is killed by 4. If $d = 1$, then λ is an endomorphism of $T_\ell(X)$, so $T = T_\ell(X)$ and $Y = X$.

Suppose $d = 1$ and $n = 4$. Since $\tau \in \mathscr{I}$, we have $\gamma \in \mathrm{SL}_2(\mathbf{Z}_2)$. Therefore, the eigenvalues of γ are either both 1 or both -1. Therefore, either $(\gamma - 1)^2 = 0$ or $(\gamma + 1)^2 = 0$. In both cases, $(\gamma - 1)^2 X_4 = 0$. Therefore, λ is an endomorphism of $T_2(X)$ and $Y = X$. □

We can therefore take $Y = X$ in Theorem 5.5 and Corollary 5.6 when X is an elliptic curve. This is not the case in general for abelian varieties of higher dimension, as shown by the examples in the next section. However, in Corollary 6.4 below we will show that a result of this sort does hold for abelian varieties with purely additive potentially good reduction.

Next, we will give criteria for an elliptic curve to acquire semistable reduction over extensions of degree 2, 3, 4, or 6.

Corollary 6.2. *Suppose X is an elliptic curve over a field F, and v is a discrete valuation on F of residue characteristic $p \geq 0$.*

(a) *If $p \neq 2$, then X has semistable reduction above v over a totally ramified quartic extension of F if and only if X has an $\mathscr{I}$-invariant point of order* 2.

(b) *If $p \neq 3$, then X has semistable reduction above v over a totally ramified cubic extension of F if and only if X has an $\mathscr{I}$-invariant point of order* 3.

(c) *If $p \neq 2$, then X has semistable reduction above v over a quadratic extension of F if and only if either X has an $\mathscr{I}$-invariant point of order* 4, *or all the points of order* 2 *on X are $\mathscr{I}$-invariant.*

(d) *If $p \neq 2$ and X has bad but potentially good reduction at v, then X has good reduction above v over a quadratic extension of F if and only if X has no $\mathcal{I}$-invariant point of order* 4 *and all its points of order* 2 *are $\mathcal{I}$-invariant.*

(e) *Suppose p is not* 2 *or* 3. *Then the following are equivalent*:

(i) *X has no $\mathcal{I}$-invariant points of order* 2 *or* 3,

(ii) *there does not exist a finite separable extension L of F of degree less than* 6 *such that X has semistable reduction at the restriction of $\bar{v}$ to L.*

(f) *Suppose p is not* 2 *or* 3. *Then the following are equivalent*:

(i) *X has no $\mathcal{I}$-invariant points of order* 4 *or* 3 *and not all the points of order* 2 *are $\mathcal{I}$-invariant,*

(ii) *there does not exist a finite separable extension L of F of degree less than* 4 *such that X has semistable reduction at the restriction of $\bar{v}$ to L.*

Proof. Theorem 6.1 implies that, for $n = 2$, 3, or 4, if L is an extension of F of degree $R(n)$ which is totally ramified above v, then X has semistable reduction over L above v if and only if there exists a subgroup $\mathfrak{S}$ of X_n such that $\mathcal{I}$ acts as the identity on $\mathfrak{S}$ and on $\mathfrak{S}^{\perp_n}$. Parts (a), (b), and (c) are a reformulation of this.

For (d), note that by Theorem 7.4 of [16], if X has an $\mathcal{I}$-invariant point of order 4 then X has good reduction at v.

In case (e), if X has an $\mathcal{I}$-invariant point of order 2 (respectively, 3), then X has semistable reduction above v over a totally ramified extension of degree 4 (respectively, 3), by part (a) (respectively, (b)). Conversely, suppose L/F is a finite separable extension of degree less than 6, and suppose X has semistable reduction at the restriction w of $\bar{v}$ to L. If X has semistable reduction at v, then we are done by Corollary 5.3 with $n = 6$. Otherwise, taking completions we have $[L_w : F_v] = 2$, 3, or 4 by Remark 4.10. There exists an intermediate unramified extension M/F_v such that L_w/M is totally ramified. By parts (a), (b), and (c) applied to M in place of F, then X has an $\mathcal{I}$-invariant point of order 2 or 3. Case (f) proceeds the same way as case (e). □

Remark 6.3. Note that if the elliptic curve X has additive reduction at v, but has multiplicative reduction over an extension L of F which is totally and tamely ramified above v, then X has multiplicative reduction over a quadratic extension of F, but not over any non-trivial totally and tamely ramified extension of F of odd degree (since $(x+1)^2$ is the only possibility for the characteristic polynomial of $\rho_\ell(\tau)$, where τ is as before). Therefore in case (b) of Corollary 6.2, either X already has semistable reduction at v, or else X has good (i.e., does not have multiplicative) reduction above v over a cubic extension of F. In case (e), X has good reduction over an extension of degree 6 (see [12, p. 312]).

Corollary 6.4. *Suppose X is an abelian variety over a field F, v is a discrete valuation on F of residue characteristic $p \geq 0$, and X has purely additive and potentially good reduction at v.*

(a) *If $p \neq 2$, then X has good reduction above v over a quadratic extension of F if and only if there exists a subgroup S of X_4 such that $\mathscr{I}$ acts as the identity on S and on $S^{\perp_4}$.*

(b) *If $p \neq 3$, then X has good reduction above v over a totally ramified cubic extension of F if and only if there exists a subgroup S of X_3 such that $\mathscr{I}$ acts as the identity on S and on $S^{\perp_3}$.*

(c) *Suppose $p \neq 2$, and L/F is a degree 4 extension, totally ramified above v, which has a quadratic subextension over which X has purely additive reduction. Then X has good reduction above v over L if and only if there exists a subgroup S of X_2 such that $\mathscr{I}$ acts as the identity on S and on $S^{\perp_2}$.*

Proof. The backwards implications follow immediately from Corollary 5.6.

Let $n = 4$, 3, and 2 and $\ell = 2$, 3, and 2, in cases (a), (b), and (c), respectively. Let τ be a lift to $\mathscr{I}$ of a topological generator of the pro-cyclic group $\mathscr{I}/\mathscr{J}$, and let $\gamma = \rho_\ell(\tau)$. If X acquires good reduction over a totally ramified degree $R(n)$ extension, then $\gamma^{R(n)} = 1$, by Remark 4.1. Since X has purely additive reduction at v, 1 is not an eigenvalue of γ (see [9]). In case (c), -1 is not an eigenvalue of γ, since X has purely additive reduction over a ramified quadratic extension. It follows that in cases (a), (b), and (c), respectively, we have

$$\gamma + 1 = 0, \quad \gamma^2 + \gamma + 1 = 0 \quad \text{and} \quad \gamma^2 + 1 = 0$$

in $\mathrm{End}(V_\ell(X))$. We deduce that $(\gamma - 1)^2 T_\ell(X) \subseteq nT_\ell(X)$, i.e., $(\tau - 1)^2 X_n = 0$. The result now follows from Lemma 4.5. □

7. Examples

We will show that the numbers in Corollary 5.6 and Theorem 6.1 are sharp.

First, we will show that Corollary 5.6 is sharp in the case of potentially good reduction. This will show that we cannot take $Y = X$ in general. In the next 3 examples, we have $n = 2$, 3, or 4, respectively. Let ℓ denote the prime divisor of n. Suppose that F is a field with a discrete valuation v of residue characteristic not equal to ℓ. Suppose E and E' are elliptic curves over F, E has good reduction at v, and E' has additive reduction at v but acquires good reduction over an extension L of F of degree $R(n)$. Let $Y = E \times E'$. As shown in the proof of Theorem 5.5, the action of $\mathscr{I}$ on Y_n factors through $\mathscr{I}/\mathscr{J}$. Let τ be a lift to $\mathscr{I}$ of a topological generator of the pro-cyclic group $\mathscr{I}/\mathscr{J}$, and let $g = \rho_{\ell,Y}(\tau)$. Note that $g^{R(n)} = 1$. Let G denote the cyclic group generated by g. In each example we will construct a certain $\mathbf{Z}_\ell[G]$-module T such that $T \subset T_\ell(Y) \subset (1/\ell)T$. Let $C' = (1/\ell)T/T_\ell(Y)$, view C' as a subgroup of Y_ℓ, and let $X = Y/C'$. Then $T_\ell(X) \cong T$. Viewing $T_\ell(Y)/T$ as a subgroup C of X_ℓ, we have $Y = X/C$. In our three examples, C is stable under $\mathscr{I}$, $(\tau - 1)^2 X_n \neq 0$, and $(\tau - 1)^2 Y_n = 0$. By Remark 5.1, there is a subgroup $S \subseteq Y_n$ such that $\mathscr{I}$ acts as the identity on S and on $S^{\perp_n}$, but there does not exist a subgroup $\mathfrak{S} \subseteq X_n$ such that $\mathscr{I}$ acts as the identity on $\mathfrak{S}$ and on $\mathfrak{S}^{\perp_n}$. We see that X and Y satisfy (ii) of Corollary 5.6.

Example 7.1. Let $n = 2$. Suppose that E' does not acquire good reduction over a quadratic subextension of L/F. As $\mathbf{Z}_2[G]$-modules, we have

$$T_2(Y) \cong (\mathbf{Z}_2[x]/(x-1))^2 \oplus \mathbf{Z}_2[x]/(x^2+1),$$

where g acts via multiplication by x. Let

$$T = \mathbf{Z}_2[x]/(x-1) \oplus \mathbf{Z}_2[x]/(x-1)(x^2+1),$$

and view T as a submodule of $T_2(Y)$ via the natural injection. For example, one could take $F = \mathbf{Q}$, $v = 3$, and E and E', respectively, the elliptic curves 11A3 and 36A1 from the tables in [2].

Example 7.2. Let $n = 3$. As $\mathbf{Z}_3[G]$-modules, we have

$$T_3(Y) \cong (\mathbf{Z}_3[x]/(x-1))^2 \oplus \mathbf{Z}_3[x]/(x^2+x+1),$$

where g acts via multiplication by x. Let

$$T = \mathbf{Z}_3[x]/(x-1) \oplus \mathbf{Z}_3[x]/(x^3-1),$$

and view T as a submodule of $T_3(Y)$ via the natural injection. For example, one could take $F = \mathbf{Q}$, $v = 2$, and E and E', respectively, the elliptic curves 11A3 and 20A2 from the tables in [2].

Example 7.3. Let $n = 4$. As $\mathbf{Z}_2[G]$-modules, we have

$$T_2(Y) \cong (\mathbf{Z}_2[x]/(x-1))^2 \oplus (\mathbf{Z}_2[x]/(x+1))^2 \cong (\mathbf{Z}_2[G])^2,$$

where g acts via multiplication by x. Let

$$T = \mathbf{Z}_2[x]/(x-1) \oplus \mathbf{Z}_2[x]/(x^2-1) \oplus \mathbf{Z}_2[x]/(x+1),$$

and view T as a submodule of $T_2(Y)$ via the natural injection. One could take $F = \mathbf{Q}$, $v = 3$, and E and E', respectively, the elliptic curves 11A3 and 99D1 from the tables in [2].

Next, we will show that the numbers 8, 9 and 4 (respectively) in Corollary 5.6 are sharp.

Example 7.4. Let $n = 2$, 3, or 4. For ease of notation, let $R = R(n)$. Let ℓ be the prime divisor of n. Let F be a field with a discrete valuation v of residue characteristic not equal to ℓ, and suppose E is an elliptic curve over F with multiplicative reduction at v. Suppose that M is a degree R Galois extension of F which is totally ramified above v. Let χ be the composition

$$\mathrm{Gal}(F^s/F) \to \mathrm{Gal}(M/F) \cong \mathbf{Z}/R\mathbf{Z} \hookrightarrow \mathrm{Aut}_F(E^R),$$

where the image of the last map is generated by a cyclic permutation of the factors of E^R, and E^R is the R-fold product of E with itself. Let A denote the twist of E^R by χ. Let τ denote a lift to $\mathscr{I}$ of a generator of $\mathscr{I}/\mathscr{J}$. As $\mathbf{Q}_\ell[\tau]$-modules, $V_\ell(A) \cong \mathbf{Q}_\ell[\tau]/(\tau^R - 1)^2$. Let $\tilde{T}$ be the inverse image of $\mathbf{Z}_\ell[\tau]/(\tau^R - 1)^2$ in $V_\ell(A)$. Then for some integer k, we have $T_\ell(A) \subseteq \ell^k\tilde{T}$. View $\ell^k\tilde{T}/T_\ell(A)$ as a finite subgroup of A and let X be the quotient of A by this subgroup. Then X is defined over an extension K of F unramified above v, and X acquires semistable reduction over KM above v. We have $\tilde{T} = T_\ell(X)$, and the minimal polynomial of τ on X_ℓ is $(x^R - 1)^2 \equiv (x-1)^{2R} \pmod{\ell}$. Therefore,

$$(\tau - 1)^6 X_2 \neq 0 \text{ if } n = 2, \ (\tau - 1)^4 X_3 \neq 0 \text{ if } n = 3, \text{ and } \ (\tau - 1)^2 X_2 \neq 0 \text{ if } n = 4.$$

From Lemma 4.8 (with $t = 0$, $F = K$, and $L = KM$) we obtain a lattice T such that

$$8T \subseteq T_2(X) \subseteq T \quad \text{if } n = 2,$$

$$9T \subseteq T_3(X) \subseteq T \quad \text{if } n = 3,$$

and

$$4T \subseteq T_2(X) \subseteq T \quad \text{if } n = 4.$$

Let $C = T/T_\ell(X)$, view C as a subgroup of X_ℓ, and let $Y = X/C$. As we saw in the proof of Theorem 5.5, $(\tau - 1)^2 Y_n = 0$, and C is killed by 8, 9, or 4 if $n = 2$, 3, or 4 respectively. By Lemma 4.8(e)–(g), the group C is not killed by 4, 3, or 2, respectively.

Suppose K' is a finite extension of K unramified above v, Y' is an abelian variety over K', $\varphi : X \to Y'$ is a separable K'-isogeny, and $(\tau - 1)^2 Y'_n = 0$. Suppose that the kernel of φ is killed by some positive integer s. Then we can suppose $sT_\ell(Y') \subseteq T_\ell(X) \subseteq T_\ell(Y')$. Let $\lambda = (\tau^2 - 1)/n$. Since $T_\ell(Y')$ is a λ-stable $\mathbf{Z}_\ell$-lattice in $V_\ell(X)$ which contains $T_\ell(X)$, we have $T \subseteq T_\ell(Y')$ by Lemma 4.8a. Therefore, $sT \subseteq T_\ell(X)$. Then C is killed by s, and therefore s cannot be 4, 3, or 2, respectively. This shows that the numbers 8, 9, and 4 are sharp in Corollary 5.6. Note that $\dim(X) = 4$, 3, or 2, respectively. By Theorem 6.1, these are the smallest dimensions for which such examples exist.

Example 7.5. Let F be a field with a discrete valuation v of residue characteristic not equal to 2, and suppose E is an elliptic curve over F with multiplicative reduction at v. Suppose that M is a degree 4 Galois extension of F which is totally ramified above v. Let χ be the composition

$$\mathrm{Gal}(F^s/F) \to \mathrm{Gal}(M/F) \cong \mathbf{Z}/4\mathbf{Z} \hookrightarrow \mathrm{Aut}_F(E^4),$$

where the image of the last map is generated by a cyclic permutation of the factors of E^4. Let

$$B = \{(e_1, e_2, e_3, e_4) \in E^4 : e_1 + e_2 + e_3 + e_4 = 0\} \cong E^3,$$

and let A be the twist of B by χ. Let τ denote a lift to $\mathscr{I}$ of a generator of $\mathscr{I}/\mathscr{J}$, and let $f(x) = (x^3 + x^2 + x + 1)^2$. As $\mathbf{Q}_2[\tau]$-modules, $V_2(A) \cong \mathbf{Q}_2[\tau]/f(\tau)$. Let $\tilde{T}$

be the inverse image of $\mathbf{Z}_2[\tau]/f(\tau)$ in $V_2(A)$. As in the previous example, we obtain an abelian variety X such that $\tilde{T} = T_2(X)$, and such that the minimal polynomial of τ on X_2 is $f(x) \equiv (x-1)^6 \pmod 2$. Therefore, $(\tau - 1)^4 X_2 \neq 0$. As above, we see that X is isogenous over an unramified extension to an abelian variety Y such that $(\tau - 1)^2 Y_2 = 0$ and such that the kernel of the isogeny is killed by 4. Using Lemma 4.8e, we see that there does not exist such a Y where the kernel is killed by 2. This shows that thc result in Theorem 6.1 for $d = 3$ and $n = 2$ is sharp. The sharpness of the other numbers in Theorem 6.1 follows from Examples 7.2 and 7.1.

References

[1] S. Bosch, W. Lütkebohmert, M. Raynaud, Néron Models, Springer, Berlin, 1990.

[2] J.E. Cremona, Algorithms for Modular Elliptic Curves, Cambridge University Press, Cambridge, 1992.

[3] M. Flexor, J. Oesterlé, Sur les points de torsion des courbes elliptiques, Astérisque 183 (1990) 25–36.

[4] G. Frey, Some remarks concerning points of finite order on elliptic curves over global fields, Ark. Mat. 15 (1977) 1–19.

[5] A. Fröhlich, Local fields, in: J. W. S. Cassels, A. Fröhlich (Eds), Algebraic Number Theory, Thompson Book Company, Washington, 1967, pp. 1–41.

[6] A. Grothendieck, Modèles de Néron et monodromie, in: A. Grothendieck (Ed.), Groupes de Monodromie en Géometrie Algébrique, SGA7 I, Lecture Notes in Math., vol. 288, Springer, Berlin, 1972, pp. 313–523.

[7] N.M. Katz, Galois properties of torsion points on abelian varieties, Invent. Math. 62 (1981) 481–502.

[8] A. Kraus, Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive, Manuscripta Math. 69 (1990) 353–385.

[9] H.W. Lenstra, Jr., F. Oort, Abelian varieties having purely additive reduction, J. Pure Appl. Algebra 36 (1985) 281–298.

[10] D. Lorenzini, On the group of components of a Néron model, J. Reine Angew. Math. 445 (1993) 109–160.

[11] J.-P. Serre, Corps Locaux, Hermann, Paris, 1968.

[12] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. 15 (1972) 259–331.

[13] J.-P. Serre, J. Tate, Good reduction of abelian varieties, Ann. Math. 88 (1968) 492–517.

[14] A. Silverberg, Fields of definition for homomorphisms of abelian varieties, J. Pure Appl. Algebra 77 (1992) 253–262.

[15] A. Silverberg, Yu. G. Zarhin, Reduction of abelian varieties, in: Sinnou David (Ed.), Séminaire de Théorie des Nombres, Paris, 1994–95, Cambridge University Press, Cambridge, to appear.

[16] A. Silverberg, Yu. G. Zarhin, Semistable reduction and torsion subgroups of abelian varieties, Ann. Inst. Fourier 45 (2) (1995) 403–420.

[17] A. Silverberg, Yu. G. Zarhin, Variations on a theme of Minkowski and Serre, J. Pure Appl. Algebra 111 (1996) 285–302.

[18] L.C. Washington, Introduction to Cyclotomic Fields, Springer, Berlin, 1982.