DIOPHANTINE STABILITY

BARRY MAZUR AND KARL RUBIN, WITH AN APPENDIX BY MICHAEL LARSEN

Abstract. If V is an irreducible algebraic variety over a number field K, and L is a field containing K, we say that V is *diophantine-stable* for L/K if $V(L) = V(K)$. We prove that if V is either a simple abelian variety, or a curve of genus at least one, then under mild hypotheses there is a set S of rational primes with positive density such that for every $\ell \in S$ and every $n \geq 1$, there are infinitely many cyclic extensions L/K of degree ℓ^n for which V is diophantine-stable. We use this result to study the collection of finite extensions of K generated by points in $V(\bar{K})$.

Contents

2010 *Mathematics Subject Classification.* Primary: 11G30, Secondary: 11G10, 11R34, 14G25.

This material is based upon work supported by the National Science Foundation under grants DMS-1302409, DMS-1065904, and DMS-1101424. Mazur and Larsen would also like to thank MSRI for support and hospitality.

Part 1. Introduction, conjectures and results

1. Introduction

Throughout Part 1 (§1 through §4) we fix a number field K.

A. Diophantine stability. For any field K, we denote by $\bar{K}$ a fixed separable closure of K, and by G_K the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$.

Definition 1.1. Suppose V is an irreducible algebraic variety over K. If L is a field containing K, we say that V is *diophantine-stable* for L/K if $V(L) = V(K)$.

If ℓ is a rational prime, we say that V is *ℓ-diophantine-stable* over K if for every positive integer n, and every finite set Σ of places of K, there are infinitely many cyclic extensions L/K of degree ℓ^n, completely split at all places $v \in \Sigma$, such that $V(L) = V(K)$.

The main results of this paper are the following two theorems.

Theorem 1.2. *Suppose A is a simple abelian variety over K and all $\bar{K}$-endomorphisms of A are defined over K. Then there is a set S of rational primes with positive density such that A is ℓ-diophantine-stable over K for every $\ell \in S$.*

Theorem 1.3. *Suppose X is an irreducible curve over K, and let $\tilde{X}$ be the normalization and completion of X. If $\tilde{X}$ has genus ≥ 1, and all $\bar{K}$-endomorphisms of the jacobian of $\tilde{X}$ are defined over K, then there is a set S of rational primes with positive density such that X is ℓ-diophantine-stable over K for every $\ell \in S$.*

Remarks 1.4. (1) Note that our assumptions on A imply that A is absolutely simple. It is natural to ask whether the assumption on $\mathrm{End}(A)$ is necessary, and whether the assumption that A is simple is necessary. See Remark 10.4 for more about the latter question.

(2) The condition on the endomorphism algebra in Theorems 1.2 and 1.3 can always be satisfied by enlarging K.

(3) For each $\ell \in S$ in Theorem 1.2 and each $n \geq 1$, Theorem 11.2 below gives a quantitative lower bound for the number of cyclic extensions of degree ℓ^n and bounded conductor for which A is ℓ-diophantine-stable.

We will deduce Theorem 1.3 from Theorem 1.2 in §3 below, and prove the following consequences in §4. Corollary 1.5 is proved by applying Theorem 1.3 repeatedly to the modular curve $X_0(p)$, and Corollary 1.6 by applying Theorem 1.3 repeatedly to an elliptic curve over $\mathbb{Q}$ of positive rank and using results of Shlapentokh.

Corollary 1.5. *Let $p \geq 23$ and $p \neq 37, 43, 67, 163$. There are uncountably many pairwise non-isomorphic subfields L of $\bar{\mathbb{Q}}$ such that no elliptic curve defined over L possesses an L-rational subgroup of order p.*

Corollary 1.6. *For every prime p, there are uncountably many pairwise non-isomorphic totally real fields L of algebraic numbers in $\mathbb{Q}_p$ over which the following two statements both hold:*

(i) *There is a diophantine definition of $\mathbb{Z}$ in the ring of integers $\mathcal{O}_L$ of L. In particular, Hilbert's Tenth Problem has a negative answer for $\mathcal{O}_L$; i.e., there does not exist an algorithm to determine whether a polynomial (in many variables) with coefficients in $\mathcal{O}_L$ has a solution in $\mathcal{O}_L$.*

(ii) *There exists a first-order definition of the ring $\mathbb{Z}$ in L. The first-order theory for such fields L is undecidable.*

B. Fields generated by points on varieties. Our original motivation for Theorem 1.3 was to understand, given a variety V over K, the set of (necessarily finite) extensions of K generated by a single $\bar{K}$-point of V. More precisely, we make the following definition.

Definition 1.7. Suppose V is a variety defined over K. A finite extension L/K is *generated over K by a point of V* if (any of) the following equivalent conditions hold:

- There is a point $x \in V(L)$ such that $x \notin V(L')$ for any proper subextension L'/K.
- There is an $x \in V(\bar{K})$ such that $L = K(x)$.
- There is an open subvariety $W \subset V$, an embedding $W \hookrightarrow \mathbb{A}^N$ defined over K, and a point in the image of W whose coordinates generate L over K.

If V is a variety over K we will say that L/K *belongs to* V if L/K is generated by a point of V over K. Denote by $\mathcal{L}(V;K)$ the set of finite extensions of K belonging to V, that is:

$$\mathcal{L}(V;K) := \{K(x)/K : x \in V(\bar{K})\}.$$

For example, if V contains a curve isomorphic over K to an open subset of $\mathbb{P}^1$, then it follows from the primitive element theorem that every finite extension of K belongs to V. It seems natural to us to conjecture the converse. We prove this conjecture for irreducible curves. Specifically:

Theorem 1.8. *Let X be an irreducible curve over K. Then the following are equivalent:*

(i) *all but finitely many finite extensions L/K belong to X,*
(ii) *X is birationally isomorphic (over K) to the projective line.*

Theorem 1.8 is a special case of Theorem 1.10 below, taking $Y = \mathbb{P}^1$.

More generally, one can ask to what extent $\mathcal{L}(X;K)$ determines the curve X.

Question 1.9. *Let X and Y be irreducible smooth projective curves over a number field K. If $\mathcal{L}(X;K) = \mathcal{L}(Y;K)$, are X and Y necessarily isomorphic over $\bar{K}$?*

With $\bar{K}$ replaced by K in Question 1.9, the answer is "no". A family of counterexamples found by Daniel Goldstein and Zev Klagsbrun is given in Proposition 2.5 below. However, Theorem 1.10 below shows that a stronger version of Question 1.9 has a positive answer if X has genus zero.

We will write $\mathcal{L}(X;K) \approx \mathcal{L}(Y;K)$ to mean that $\mathcal{L}(X;K)$ and $\mathcal{L}(Y;K)$ agree up to a finite number of elements, i.e., the symmetric difference

$$\mathcal{L}(X;K) \cup \mathcal{L}(Y;K) - \mathcal{L}(X;K) \cap \mathcal{L}(Y;K)$$

is finite.

We can also ask Question 1.9 with "=" replaced by "$\approx$". Lemma 2.4 below shows that up to "$\approx$" equivalence, $\mathcal{L}(X;K)$ is a birational invariant of the curve X.

Theorem 1.10. *Suppose X and Y are irreducible curves over K, and Y has genus zero. Then $\mathcal{L}(X;K) \approx \mathcal{L}(Y;K)$ if and only if X and Y are birationally isomorphic over K.*

Theorem 1.10 will be proved in §2.

C. Growth of Mordell-Weil ranks in cyclic extensions. Fix an abelian variety A over K. Theorem 1.2 produces a large number of cyclic extensions L/K such that $\mathrm{rank}(A(L)) = \mathrm{rank}(A(K))$. For fixed $m \geq 2$, it is natural to ask how "large" is the set

$$\mathcal{S}_m(A/K) := \{L/K \text{ cyclic of degree } m : \mathrm{rank}(A(L)) > \mathrm{rank}(A(K))\}.$$

In §11 we use the proof of Theorem 1.2 to give quantitative information about the size of $\mathcal{S}_{\ell^n}(A/K)$ for prime powers ℓ^n.

Conditional on the Birch and Swinnerton-Dyer Conjecture, $\mathcal{S}_m(A/K)$ is closely related to the collection of 1-dimensional characters χ of K of order dividing m such that the L-function $L(A,\chi;s)$ of the abelian variety A twisted by χ has a zero at the central point $s = 1$. There is a good deal of literature on the statistics of such zeroes, particularly in the case where $A = E$ is an elliptic curve over $\mathbb{Q}$. For ℓ prime let

$$N_{E,\ell}(x) := |\{\text{Dirichlet characters } \chi \text{ of order } \ell : \mathrm{cond}(\chi) \leq x \text{ and } L(E,\chi,1) = 0\}|.$$

David, Fearnley and Kisilevsky [**DFK**] conjecture that $\lim_{x\to\infty} N_{E,\ell}(x)$ is infinite for $\ell \leq 5$, and finite for $\ell \geq 7$. More precisely, the Birch and Swinnerton-Dyer Conjecture would imply

$$\log N_{E,2}(x) \sim \log(x),$$

and David, Fearnley and Kisilevsky [**DFK**] conjecture that as $x \to \infty$,

$$\log N_{E,3}(x) \sim \tfrac{1}{2}\log(x), \quad \log N_{E,5}(x) \ll_\epsilon \epsilon \log(x) \text{ for all } \epsilon > 0.$$

Examples with $L(E,\chi,1) = 0$ for χ of large order ℓ seem to be quite rare over $\mathbb{Q}$. Fearnley and Kisilevsky [**FK**] provide examples when $\ell = 7$ and one example with $\ell = 11$ (the curve $E : y^2 + xy = x^3 + x^2 - 32x + 58$ of conductor 5906, with χ of conductor 23).

In contrast, working over more general number fields there can be a large supply of cyclic extensions L/K in which the rank grows. We will say that a cyclic extension L/K is of *dihedral type* if there are subfields $k \subset K_0 \subset K$ and $L_0 \subset L$ such that $[K_0 : k] = 2$, L_0/k is Galois with dihedral Galois group, and $KL_0 = L$. The rank frequently grows in extensions of dihedral type, as can be detected for parity reasons, and sometimes buttressed by Heegner point constructions. See [**MR1**, §2, §3] and [**MR3**, Theorem B]. This raises the following natural question.

Question 1.11. *Suppose V is either an abelian variety or an irreducible curve of genus at least one over K. Is there a bound $M(V)$ such that if L/K is cyclic of degree $\ell > M(V)$ and not of dihedral type, then $V(L) = V(K)$?*

A positive answer to Question 1.11 for abelian varieties implies a positive answer for irreducible curves of positive genus, exactly as Theorem 1.3 follows from Theorem 1.2 (see §3).

D. Outline of the paper. In §2 we prove Theorem 1.10. The rest of Part 1 is devoted to deducing Theorem 1.3 from Theorem 1.2, and deducing Corollary 1.5 from Theorem 1.3. The heart of the paper is Part 2 (sections 6 through 10), where we prove Theorem 1.2. In §11 we give quantitative information about the number of extensions L/K relative to which our given abelian variety is diophantine-stable.

Here is a brief description of the strategy of the proof of Theorem 1.2 in the case when $\mathrm{End}(A) = \mathbb{Z}$ and $n = 1$. (For a more thorough description see §5, the introduction to Part 2.) The strategy in the general case is similar, but must deal with the complexities of the endomorphism ring of A. If L/K is a cyclic extension of degree ℓ, we show (Proposition 8.8) that $\mathrm{rank}(A(L)) = \mathrm{rank}(A(K))$ if and only if a certain Selmer group we call $\mathrm{Sel}(L/K, A[\ell])$ vanishes. The Selmer group $\mathrm{Sel}(L/K, A[\ell])$ is a subgroup of $H^1(K, A[\ell])$ cut out by local conditions $\mathcal{H}_\ell(L_v/K_v) \subset H^1(K_v, A[\ell])$ for every place v, that depend on the local extension L_v/K_v. Thus finding L with $A(L) = A(K)$ is almost the same as finding L with "good local conditions" so that $\mathrm{Sel}(L/K, A[\ell]) = 0$.

If v is a prime of K, not dividing ℓ, where A has good reduction, we call v "critical" if $\dim_{\mathbb{F}_\ell} A[\ell]/(\mathrm{Fr}_v - 1)A[\ell] = 1$, and "silent" if $\dim_{\mathbb{F}_\ell} A[\ell]/(\mathrm{Fr}_v - 1)A[\ell] = 0$. If v is a critical prime, then the local condition $\mathcal{H}_\ell(L_v/K_v)$ only depends on whether L/K is ramified at v or not. If v is a silent prime, then $\mathcal{H}_\ell(L_v/K_v) = 0$ and does not depend on L at all. Given a sufficiently large supply of critical primes, we show (Propositions 9.10 and 9.17) how to choose a finite set Σ_c of critical primes so that if Σ_s is any finite set of silent primes, L/K is completely split at all primes of bad reduction and all primes above ℓ, and the set of primes ramifying in L/K is $\Sigma_c \cup \Sigma_s$, then $\mathrm{Sel}(L/K, A[\ell]) = 0$.

The existence of critical primes and silent primes for a set of rational primes ℓ with positive density is Theorem A.1 of the Appendix by Michael Larsen. We are very grateful to Larsen for providing the Appendix, and to Robert Guralnick, with whom we consulted and who patiently explained much of the theory to us. We also thank Daniel Goldstein and Zev Klagsbrun for Proposition 2.5 below.

2. Fields generated by points on varieties

Recall that for a variety V over K we have defined

$$\mathcal{L}(V; K) := \{K(x)/K : x \in V(\bar{K})\}.$$

A. Brauer-Severi varieties. Suppose that X is a variety defined over K and isomorphic over $\bar{K}$ to $\mathbb{P}^n$, i.e., X is an n-dimensional Brauer-Severi variety. Let $\mathrm{Br}(K) := H^2(G_K, \bar{K}^\times)$ denote the Brauer group of K. As a twist of $\mathbb{P}^n$, X corresponds to a class in $H^1(G_K, \mathrm{Aut}_{\bar{K}}(\mathbb{P}^n))$, so using the map

$$H^1(G_K, \mathrm{Aut}_{\bar{K}}(\mathbb{P}^n)) = H^1(G_K, \mathrm{PSL}_{n+1}(\bar{K})) \hookrightarrow H^2(G_K, \boldsymbol{\mu}_{n+1}) = \mathrm{Br}(K)[n+1]$$

X determines (and is determined up to K-isomorphism by) a class

$$c_X \in \mathrm{Br}(K)[n+1].$$

For every place v of K, let $\mathrm{inv}_v : \mathrm{Br}(K) \to \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}$ denote the local invariant.

Proposition 2.1. *Suppose that X is a Brauer-Severi variety over K, and let $c_X \in \mathrm{Br}(K)$ be the corresponding Brauer class. If L is a finite extension of K then the following are equivalent:*

(i) *$X(L)$ is nonempty,*
(ii) *$L \in \mathcal{L}(X; K)$,*
(iii) *$[L_w : K_v]\mathrm{inv}_v(c_X) = 0$ for every v of K and every w of L above v.*

Proof. Let $n := \dim(X)$, and suppose $X(L)$ is nonempty. Then X is isomorphic over L to $\mathbb{P}^n$. If $K \subset F \subset L$ then the Weil restriction of scalars $\mathrm{Res}_K^F X$ is a variety of dimension $n[F : K]$, and there is a natural embedding

$$\mathrm{Res}_K^F X \longrightarrow \mathrm{Res}_K^L X.$$

If we define $W := \mathrm{Res}_K^L X - \cup_{K\subset F\subsetneq L}\mathrm{Res}_K^F X$ then W is a (nonempty) Zariski open subvariety of the rational variety $\mathrm{Res}_K^L X$, so in particular $W(K)$ is nonempty. But taking K points in the definition of W shows that

$$W(K) = (\mathrm{Res}_K^L X)(K) - \cup_{K\subset F\subsetneq L}(\mathrm{Res}_K^F X)(K) = X(L) - \cup_{K\subset F\subsetneq L} X(F).$$

Thus $X(L)$ properly contains $\cup_{K\subset F\subsetneq L} X(F)$, so $L \in \mathcal{L}(X;K)$ and (i) $\Rightarrow$ (ii).

If v is a place of K and w is a place of L above v, then (see for example [**SCF**, Proposition 2, §1.3])

$$\mathrm{inv}_w(\mathrm{Res}_L(c_X)) = [L_w : K_v]\mathrm{inv}_v(c_X). \tag{2.2}$$

If $L \in \mathcal{L}(X;K)$, then by definition $X(L)$ is nonempty, so X is isomorphic over L to $\mathbb{P}^n$ and $\mathrm{Res}_L(c_X) = 0$. Thus (2.2) shows that (ii) $\Rightarrow$ (iii).

Finally, if (iii) holds then $\mathrm{inv}_w(\mathrm{Res}_L(c_X)) = 0$ for every w of L by (2.2), so $\mathrm{Res}_L(c_X) = 0$ (see for example [**TCF**, Corollary 9.8]). Hence X is isomorphic over L to $\mathbb{P}^n$, so $X(L)$ is nonempty and we have (iii) $\Rightarrow$ (i). □

Corollary 2.3. *If X and Y are Brauer-Severi varieties, then $\mathcal{L}(X;K) = \mathcal{L}(Y;K)$ if and only if $\mathrm{inv}_v(c_X)$ and $\mathrm{inv}_v(c_Y)$ have the same denominator for every v.*

Proof. This follows directly from the equivalence (ii) $\Leftrightarrow$ (iii) of Proposition 2.1. □

B. Curves. For this subsection X will be a curve over K, and we will prove Theorem 1.10.

Lemma 2.4. *Suppose X and Y are curves defined over K and birationally isomorphic over K. Then $\mathcal{L}(X;K) \approx \mathcal{L}(Y;K)$.*

Proof. If X and Y are birationally isomorphic, then there are Zariski open subsets $U_X \subset X$, $U_Y \subset Y$ such that $U_X \cong U_Y$ over K. Let T denote the finite variety $X - U_X$. Then

$$\mathcal{L}(X;K) = \mathcal{L}(U_X;K) \cup \mathcal{L}(T;K),$$

and $\mathcal{L}(T;K)$ is finite. Therefore $\mathcal{L}(X;K) \approx \mathcal{L}(U_X;K)$, and similarly for Y, so

$$\mathcal{L}(X;K) \approx \mathcal{L}(U_X;K) = \mathcal{L}(U_Y;K) \approx \mathcal{L}(Y;K).$$

□

Recall the statement of Theorem 1.10:

Theorem 1.10. *Suppose X and Y are irreducible curves over K, and Y has genus zero. Then $\mathcal{L}(X;K) \approx \mathcal{L}(Y;K)$ if and only if X and Y are birationally isomorphic over K.*

Proof of Theorem 1.10. The 'if' direction is Lemma 2.4. Suppose now that X and Y are not birationally isomorphic over K; we will show that $\mathcal{L}(X;K) \not\approx \mathcal{L}(Y;K)$.

Replacing X and Y by their normalizations and completions (and using Lemma 2.4 again), we may assume without loss of generality that X and Y are both smooth and projective.

Case 1: X has genus zero. In this case X and Y are one-dimensional Brauer-Severi varieties, so we can apply Proposition 2.1. Let $c_X, c_Y \in \mathrm{Br}(K)[2]$ be the corresponding Brauer classes. Since X and Y are not isomorphic, there is a place v such that (switching X and Y if necessary) $\mathrm{inv}_v(c_X) = 0$ and $\mathrm{inv}_v(c_Y) = 1/2$. Let T be the (finite) set of places of K different from v where $\mathrm{inv}_v(c_X)$ and $\mathrm{inv}_v(c_Y)$ are not both zero. If L/K is a quadratic extension in which v splits, but no place in T splits, then by Proposition 2.1 we have $L \in \mathcal{L}(X;K)$ but $L \notin \mathcal{L}(Y;K)$. There are infinitely many such L, so $\mathcal{L}(X;K) \not\approx \mathcal{L}(Y;K)$.

Case 2: X has genus at least one. Let K'/K be a finite extension large enough so that all $\bar{K}$-endomorphisms of the jacobian of X are defined over K', and $Y(K')$ is nonempty. By Theorem 1.3 applied to X/K' we can find infinitely many nontrivial cyclic extensions L/K' such that $X(L) = X(K')$, so in particular $L \notin \mathcal{L}(X;K)$. But $Y(L)$ is nonempty, so $L \in \mathcal{L}(Y;K)$ by Proposition 2.1. Since there are infinitely many such L, we conclude that $\mathcal{L}(X;K) \not\approx \mathcal{L}(Y;K)$. □

C. Principal homogeneous spaces for abelian varieties. The following proposition was suggested by Daniel Goldstein and Zev Klagsbrun. It shows that the answer to Question 1.9 is "no" if $\bar{K}$ is replaced by K. To see this, suppose that A is an elliptic curve, and $\mathbf{a}, \mathbf{a}' \in H^1(K, A)$ generate the same cyclic subgroup, but there is no $\alpha \in \mathrm{Aut}_K(A)$ such that $\mathbf{a}' = \alpha\mathbf{a}$. Then the corresponding principal homogeneous spaces X, X' are not isomorphic over K, but Proposition 2.5 shows that $\mathcal{L}(X;K) = \mathcal{L}(X';K)$.

Proposition 2.5. *Fix an abelian variety A, and suppose X and X' are principal homogeneous spaces over K for A with corresponding classes $\mathbf{a}, \mathbf{a}' \in H^1(K, A)$. If the cyclic subgroups $\mathbb{Z}\mathbf{a}$ and $\mathbb{Z}\mathbf{a}'$ are equal, then $\mathcal{L}(X;K) = \mathcal{L}(X';K)$.*

Proof. Fix n such that $n\mathbf{a} = 0$. The short exact sequence

$$0 \to A[n] \to A(\bar{K}) \to A(\bar{K}) \to 0$$

leads to the descent exact sequence

$$0 \longrightarrow A(K)/nA(K) \longrightarrow H^1(K, A[n]) \longrightarrow H^1(K, A)[n] \longrightarrow 0,$$

and it follows that $\mathbf{a}$ can be represented by a cocycle $\sigma \mapsto a_\sigma$ with $a_\sigma \in A[n]$. Since $\mathbf{a}$ and $\mathbf{a}'$ generate the same subgroup, for some $m \in (\mathbb{Z}/n\mathbb{Z})^\times$ we can represent $\mathbf{a}'$ by $\sigma \mapsto a'_\sigma$ with $a'_\sigma = m a_\sigma$.

There are isomorphisms $\phi : A \to X$, $\phi' : A \to X'$ defined over $\bar{K}$ such that if $P \in A(\bar{K})$ and $\sigma \in G_K$, then

$$\phi(P)^\sigma = \phi(P^\sigma + a_\sigma), \qquad \phi'(P)^\sigma = \phi'(P^\sigma + a'_\sigma)$$

In particular, if $\sigma \in G_K$ then

$$\phi(P)^\sigma = \phi(P) \iff P^\sigma - P = -a_\sigma,$$

so

$$K(\phi(P)) \text{ is the fixed field of the subgroup } \{\sigma \in G_K : P^\sigma - P = -a_\sigma\} \tag{2.6}$$

and similarly with ϕ and $\mathbf{a}$ replaced by ϕ' and $\mathbf{a}'$.

Suppose $L \in \mathcal{L}(X;K)$. Then we can fix $P \in A(\bar{K})$ such that $K(\phi(P)) = L$. In other words, by (2.6) we have

$$G_L = \{\sigma \in G_K : P^\sigma - P = -a_\sigma\}. \tag{2.7}$$

Since the set $\{P^\sigma - P + a_\sigma : \sigma \in G_K\}$ is finite and m is relatively prime to n, we can choose $r \in \mathbb{Z}$ with $r \equiv m \pmod{n}$ such that $\{P^\sigma - P + a_\sigma : \sigma \in G_K\} \cap A[r] = 0$. Then by (2.7)

$$\begin{aligned}\{\sigma \in G_K : (rP)^\sigma - rP = -a'_\sigma\} &= \{\sigma \in G_K : (rP)^\sigma - rP = -ra_\sigma\} \\ &= \{\sigma \in G_K : P^\sigma - P = -a_\sigma\} = G_L,\end{aligned}$$

so (2.6) applied to ϕ' and $\mathbf{a}'$ shows that $K(\phi'(rP)) = L$, i.e., $L \in \mathcal{L}(X';K)$. Thus $\mathcal{L}(X;K) \subset \mathcal{L}(X';K)$, and reversing the roles of X and X' shows that we have equality. $\square$

It seems natural to ask the following question about a possible converse to Proposition 2.5.

Question 2.8. *Suppose that A is an abelian variety, and X, X' are principal homogeneous spaces for A over K with corresponding classes $\mathbf{a}, \mathbf{a}' \in H^1(K, A)$. If $\mathcal{L}(X;K) = \mathcal{L}(X';K)$, does it follow that $\mathbf{a}$ and $\mathbf{a}'$ generate the same* $\mathrm{End}_K(A)$*-submodule of $H^1(K, A)$?*

Example 2.9. Let E be the elliptic curve 571A1 : $y^2 + y = x^3 - x^2 - 929x - 10595$, with $\mathrm{End}_{\mathbb{Q}}(E) = \mathrm{End}_{\bar{\mathbb{Q}}}(E) = \mathbb{Z}$. Then the Shafarevich-Tate group $\text{Ш}(E/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and the three nontrivial elements (which generate distinct cyclic subgroups of $H^1(\mathbb{Q}, E)$) are represented by the principal homogeneous spaces

$$X_1 : y^2 = -19x^4 + 112x^3 - 142x^2 - 68x - 7$$
$$X_2 : y^2 = -16x^4 - 82x^3 - 52x^2 + 136x - 44$$
$$X_3 : y^2 = -x^4 - 26x^3 - 148x^2 + 274x - 111.$$

Let $d_1 = 17$, $d_2 = 41$, and $d_3 = 89$. A computation in Sage [**Sag**] shows that $\mathbb{Q}(\sqrt{d_i}) \in \mathcal{L}(X_j;\mathbb{Q})$ if and only if $i = j$, so the sets $\mathcal{L}(X_j;\mathbb{Q})$ are distinct.

3. Theorem 1.2 implies Theorem 1.3

In this section we deduce Theorem 1.3 from Theorem 1.2.

Lemma 3.1. *The conclusion of Theorem 1.3 depends only on the birational equivalence class of X over K. More precisely, if X, Y are irreducible curves over K, birationally isomorphic over K, and ℓ is sufficiently large (depending on X and Y), then*

$$X \text{ is } \ell\text{-diophantine-stable over } K \iff Y \text{ is } \ell\text{-diophantine-stable over } K.$$

Proof. It suffices to prove the lemma in the case that Y is a dense open subset of X. This is because any two K-birationally equivalent curves contain a common open dense subvariety.

Let $T := X - Y$. Then $T = \coprod_{i \in I} \mathrm{Spec}(K_i)$ for some finite index set I and number fields K_i containing K. Let $\delta = \max\{[K_i : K] : i \in I\}$. Then for every cyclic extension L/K of prime-power degree ℓ^n with $\ell > \delta$, we have $L \cap K_i = K$ for all $i \in I$, so $T(L) = T(K)$ and $X(L) = X(K) \iff Y(L) = Y(K)$. $\square$

It suffices, then, to prove Theorem 1.3 for irreducible projective smooth curves X.

Lemma 3.2. *Suppose $f : X \to Y$ is a nonconstant map (defined over K) of irreducible curves over K. If ℓ is sufficiently large (depending on X, Y, and f), and Y is ℓ-diophantine-stable over K, then X is ℓ-diophantine-stable over K.*

Proof. By Lemma 3.1 we may assume that $f : X \to Y$ is a morphism of finite degree, say d, of smooth projective curves. Let L/K be a cyclic extension of degree ℓ^n with $\ell > d$ such that $Y(L) = Y(K)$. We will show that $X(L) = X(K)$.

Consider a point $x \in X(L)$, and let $y := f(x) \in Y(L) = Y(K)$. Form the fiber, i.e., the zero-dimensional scheme $T := f^{-1}(y)$. Then $x \in T(L)$. As in the proof of

Lemma 3.1, the reduction of the scheme T is a disjoint union of spectra of number fields of degree at most d over K. Since $\ell > d$, we have $T(L) = T(K)$ and hence $x \in X(K)$. □

Lemma 3.3. *Theorem 1.2 $\implies$ Theorem 1.3.*

Proof. Let $\tilde{X}$ be the completion and normalization of X. Let D be a K-rational divisor on $\tilde{X}$ of nonzero degree d, and define a nonconstant map over K from $\tilde{X}$ to its jacobian $J(\tilde{X})$ by $x \mapsto D - d \cdot [x]$. Let A be a simple abelian variety quotient of $J(\tilde{X})$ defined over K, and let $Y \subset A$ be the image of $\tilde{X}$. Theorem 1.2 applied to A shows that there is a set S of primes, with positive density, such that A (and hence Y as well) is ℓ-diophantine-stable over K for every $\ell \in S$. It follows from Lemmas 3.1 and 3.2 that (for ℓ sufficiently large) X is ℓ-diophantine-stable over K for every $\ell \in S$ as well, i.e., the conclusion of Theorem 1.3 holds for X. □

4. Infinite extensions

In this section we will prove Corollaries 1.5 and 1.6.

Theorem 4.1. *Suppose V is either a simple abelian variety over K as in Theorem 1.2 or an irreducible curve over K as in Theorem 1.3. For every finite set Σ of places of K, there are uncountably many pairwise non-isomorphic extensions L of K in $\bar{K}$ such that all places in Σ split completely in L, and $V(L) = V(K)$.*

Proof. Let

$$\mathcal{N} := (n_1, n_2, n_3, \dots)$$

be an arbitrary infinite sequence of positive integers. Using Theorem 1.3, choose a prime ℓ_1 and a Galois extension K_1/K, completely split at all $v \in \Sigma$, that is cyclic of degree $\ell_1^{n_1}$ and such that $V(K_1) = V(K)$. Continue inductively, using Theorem 1.3, to choose an increasing sequence of primes $\ell_1 < \ell_2 < \ell_3 < \cdots$ and a tower of fields $K \subset K_1 \subset K_2 \subset K_3 \subset \cdots$ such that K_i/K_{i-1} is cyclic of degree $\ell_i^{n_i}$, completely split at all places above Σ, and $X(K_i) = X(K)$ for every i. Let $K_{\mathcal{N}} := \cup_{i \geq 1} K_i \subset \bar{K} \cap K_v$.

We have that $X(K_{\mathcal{N}}) = X(K)$ for every $\mathcal{N}$. We claim further that no matter what choices are made for the ℓ_i, the construction

$$\mathcal{N} \mapsto K_{\mathcal{N}}$$

establishes an *injection* of the (uncountable) set of sequences $\mathcal{N}$ of positive integers into the set of subfields of $\bar{K} \cap K_v$. To see this, observe that by writing a subfield $F \subset \bar{K}$ as a union of finite extensions of K, one can define the degree $[F : \mathbb{Q}]$ as a formal product $\prod_p p^{a_p}$ over all primes p, with $a_p \leq \infty$ (i.e., a supernatural number). Then $[K_{\mathcal{N}} : K] = \prod_i \ell_i^{n_i}$, and since the ℓ_i are increasing, this formal product determines the sequence $\mathcal{N}$. Therefore there are uncountably many such fields $K_{\mathcal{N}}$, and they are pairwise non-isomorphic. □

Recall the statement of Corollary 1.5:

Corollary 1.5. *Let $p \geq 23$ and $p \neq 37, 43, 67, 163$. There are uncountably many pairwise non-isomorphic subfields L of $\bar{\mathbb{Q}}$ such that no elliptic curve defined over L possesses an L-rational subgroup of order p.*

Proof of Corollary 1.5. By [**Maz**], if p is a prime satisfying the hypotheses of the corollary, then the modular curve $X := X_0(p)$ defined over $\mathbb{Q}$ only has two rational points, namely the cusps $\{0\}$ and $\{\infty\}$, and the genus of X is greater than zero. Since the jacobian of X is semistable, its endomorphisms are all defined over $\mathbb{Q}$ (see [**Rib**]). Thus the hypotheses of Theorem 1.3 hold with $K := \mathbb{Q}$, and Theorem 4.1 produces uncountably many subfields L of $\bar{\mathbb{Q}}$ such that $X_0(p)$ has no non-cuspidal L-rational points. □

Corollary 4.2. *For every prime p, there are uncountably many pairwise non-isomorphic fields $L \subset \bar{\mathbb{Q}}$ such that*

(i) *L is totally real,*
(ii) *p splits completely in L,*
(iii) *there is an elliptic curve E over $\mathbb{Q}$ such that $E(L)$ is a finitely generated infinite group.*

Proof. Fix any elliptic curve E over $\mathbb{Q}$ with positive rank, and without complex multiplication. Apply Theorem 4.1 to E with $\Sigma = \{\infty, p\}$. □

Recall the statement of Corollary 1.6:

Corollary 1.6. *For every prime p, there are uncountably many pairwise non-isomorphic totally real fields L of algebraic numbers in $\mathbb{Q}_p$ over which the following two statements both hold:*

(i) *There is a diophantine definition of $\mathbb{Z}$ in the ring of integers $\mathcal{O}_L$ of L. In particular, Hilbert's Tenth Problem has a negative answer for $\mathcal{O}_L$; i.e., there does not exist an algorithm to determine whether a polynomial (in many variables) with coefficients in $\mathcal{O}_L$ has a solution in $\mathcal{O}_L$.*
(ii) *There exists a first-order definition of the ring $\mathbb{Z}$ in L. The first-order theory for such fields L is undecidable.*

Proof of Corollary 1.6. The corollary follows directly from Corollary 4.2 and results of Shlapentokh, as follows. Suppose L is an infinite extension of $\mathbb{Q}$ satisfying Corollary 4.2(i,ii,iii). Assertion (i) follows from Corollary 4.2(i,iii) and [**Sh1**, Main Theorem A]. Since p splits completely in L, the prime p is q-bounded (for every rational prime q) in the sense of [**Sh2**, Definition 4.2], so assertion (ii) follows from Corollary 4.2(ii,iii) and [**Sh2**, Theorem 8.5]. □

Part 2. Abelian varieties and diophantine stability

5. Strategy of the proof

Notation. For sections 6 through 10 fix a simple abelian variety A defined over an arbitrary field K (in practice K will be a number field or one of its completions). Let $\mathcal{R}$ denote the center of $\mathrm{End}_K(A)$, and $\mathcal{M} := \mathcal{R} \otimes \mathbb{Q}$. Since A is simple, $\mathcal{M}$ is a number field and $\mathcal{R}$ is an order in $\mathcal{M}$. Fix a rational prime ℓ that does not divide the discriminant of $\mathcal{R}$, and fix a prime λ of $\mathcal{M}$ above ℓ. In particular ℓ is unramified in $\mathcal{M}/\mathbb{Q}$. Denote by $\mathcal{M}_\lambda$ the completion of $\mathcal{M}$ at λ.

In the following sections we develop the machinery that we need to prove Theorem 1.2. Here is a description of the strategy of the proof.

The standard method—perhaps the only fully proved method—of finding upper bounds for Mordell-Weil ranks is the *method of descent* that seems to have been already present in some arguments due to Fermat and has been elaborated and refined ever since. These days "descent" is done via computation of *Selmer groups*. To check for diophantine stability we will be considering the relative theory; that is, how things change when passing from our base field K to L, a cyclic extension of prime power degree ℓ^n over K. The Galois group $\mathrm{Gal}(L/K)$ acts on the finite dimensional $\mathbb{Q}$-vector space $A(L) \otimes \mathbb{Q}$. Diophantine stability here requires that the action be trivial; i.e, it requires that for any Galois character $\chi_i : G_K \to \mathbb{C}^*$ of order ℓ^i $(0 < i \leq n)$ that cuts out a nontrivial sub-extension, L_i/K of L/K, the χ_i-component of the $\mathrm{Gal}(L/K)$-representation $A(L) \otimes \mathbb{C}$ vanishes. Since this representation is defined over $\mathbb{Q}$, if, for $i > 0$, the χ_i-part of $A(L) \otimes \mathbb{C}$ vanishes then

$$A(L_i) \otimes \mathbb{Q} = A(L_{i-1}) \otimes \mathbb{Q}. \tag{5.1}$$

Sections 6 and 7 below prepare for a discussion of a certain relevant relative Selmer group, denoted $\mathrm{Sel}(L_i/K, A[\lambda])$ defined in Section 8 that has the property that its vanishing implies (5.1). More precisely, Proposition 8.8 below gives:

$$\mathrm{rank}_{\mathbb{Z}} A(L) \leq \mathrm{rank}_{\mathbb{Z}} A(K) + \mathrm{rank}_{\mathbb{Z}}(\mathcal{R}) \sum_{i=1}^{n} \phi(\ell^i) \cdot \dim_{\mathcal{R}/\lambda} \mathrm{Sel}(L_i/K, A[\lambda]).$$

The key to the technique we adopt is that for all cyclic ℓ^n-extensions L/K (for fixed ℓ), the corresponding relative Selmer groups $\mathrm{Sel}(L/K, A[\lambda])$ are canonically 'tied together' as finite dimensional subspaces of a single (infinite dimensional) $\mathcal{R}/\lambda$-vector space, namely $H^1(G_K, A[\lambda])$. The subspace $\mathrm{Sel}(L/K, A[\lambda])$ of $H^1(G_K, A[\lambda])$ is determined by specific local conditions at all places v of K, these local conditions in turn being determined by A/K_v and L_v/K_v where L_v is the completion of L at any prime of L above v. Even more specifically, $\mathrm{Sel}(L/K, A[\lambda])$ is determined by A/K and the collection of local extensions L_v/K_v for v primes of K; moreover, an 'artificial Selmer subgroup' of $H^1(G_K, A[\lambda])$ can be defined corresponding to any collection of local extensions L_v/K_v even if this collection doesn't come from a global L/K.

Nevertheless, when passing from one global extension L/K to another L'/K of the same degree, one needs only change the local conditions that determine $\mathrm{Sel}(L/K, A[\lambda])$ at a finite set of primes S to obtain the local conditions that determine $\mathrm{Sel}(L'/K, A[\lambda])$. Our aim, of course, is to find a large quantity of extensions L/K with $\mathrm{Sel}(L/K, A[\lambda]) = 0$. We do this by starting with an arbitrary L/K and then constructing inductively appropriate finite sets Σ, with changes of local conditions at the primes in Σ corresponding to extensions L'/K such that the $\mathrm{Sel}(L'_i/K, A[\lambda]) = 0$ for all i.

For this, it is essential that we are supplied with what we call *critical primes* and *silent primes*.

Enough critical primes: Critical primes are judiciously chosen primes v for which a change of local condition at v lowers the dimension of the corresponding Selmer group by 1. They are primes v of good reduction for A and such that ℓ divides the order of the multiplicative group of the residue field of v (no problem finding primes of this sort) and such that the action of the Frobenius element at v on the vector space $A[\lambda]$ has a one-dimensional fixed space. Here—given some other hypotheses that will obtain when $\ell \gg 0$—we make use of global duality to guarantee that between the strictest local condition at v and the most relaxed local condition at v, the corresponding Selmer groups differ in size by one dimension. Moreover, we engineer our choice of prime v so that the localization map from $\mathrm{Sel}(L/K, A[\lambda])$ onto the one-dimensional Selmer local condition at v is surjective. In this set-up, any change of local condition subgroup at v will define an 'artificial global Selmer group' of dimension $\dim_{\mathcal{R}/\lambda} \mathrm{Sel}(L/K, A[\lambda]) - 1$.

Iterating this process a finite number of times leads us to a modification of the initial local conditions at finitely many critical primes, such that the artificially constructed Selmer group is zero. This proved in Proposition 9.17.

Enough silent primes: For $\ell \gg 0$, silent primes are primes v of good reduction for A such that ℓ divides the order of the multiplicative group of the residue field of v, and such that the Frobenius element at v has *no* nonzero fixed vectors in its action on $A[\lambda]$. For these primes the local cohomology group vanishes, so changing the local extension L'_v/K_v at such primes doesn't change the local condition, hence doesn't change the Selmer group. By making use of silent primes, we can ensure that we have infinitely many collections of local data such that the corresponding (artificial) Selmer group is zero. In addition, Larsen in his appendix requires the existence of silent primes in order to prove the existence of critical primes.

In the description above, we chose a finite collection of local extensions L'_v/K_v with specified properties for the construction of our Selmer group, a single place v at a time, to keep lowering dimension. At the end of this process, we need to have a *global* extension L'/K corresponding to our collection of local extensions $\{L'_v/K_v\}_v$. The existence of such an L' is given by Lemma 9.15.

In the appendix, Michael Larsen proves a general theorem (Theorem A.1) guaranteeing the existence of sufficiently many critical and silent primes in the general context of Galois representations on $A[\lambda]$ for A a simple abelian variety over a number field.

6. Twists of abelian varieties

Keep the notation from from the beginning of §5. In this section we recall results from [**MRS**] about twists of abelian varieties. We will use these twists in §7 and §8 to define the relative Selmer groups $\mathrm{Sel}(L/K, A[\lambda])$ described in §5.

Fix for this section a cyclic extension L/K of degree ℓ^n with $n \geq 0$. Let $G := \mathrm{Gal}(L/K)$. If $n \geq 1$ (i.e., if $L \neq K$), let L' be the (unique) subfield of L of degree ℓ^{n-1} over K and $G' := \mathrm{Gal}(L'/K) = G/G^{\ell^{n-1}}$.

Definition 6.1. Define an ideal $\mathcal{I}_L \subset \mathcal{R}[G]$ by

$$\mathcal{I}_L := \begin{cases} \ker(\mathcal{R}[G] \longrightarrow \mathcal{R}[G']) & \text{if } n \geq 1, \\ \mathcal{R}[G] & \text{if } n = 0. \end{cases}$$

Then $\mathrm{rank}_{\mathcal{R}}(\mathcal{I}_L) = \varphi(\ell^n)$, where φ is the Euler φ-function, and we define the L/K-*twist* A_L of A to be the abelian variety $\mathcal{I}_L \otimes A$ of dimension $\varphi(\ell^n)\dim(A)$ as defined in [**MRS**, Definition 1.1]. Concretely, if $n \geq 1$ then

$$A_L := \ker(\mathrm{Res}^L_K A \longrightarrow \mathrm{Res}^{L'}_K A).$$

Here $\mathrm{Res}^L_K A$ denotes the Weil restriction of scalars of A from L to K, and the map is obtained by identifying $\mathrm{Res}^L_K A = \mathrm{Res}^{L'}_K \mathrm{Res}^L_{L'} A$ and using the canonical map $\mathrm{Res}^L_{L'} A \to A$. If $n = 0$, we simply have $A_K = A$.

See [**MR3**, §3] or [**MRS**] for a discussion of A_L and its properties.

Definition 6.2. With notation as above, let $\mathbf{N}_{L/L'} := \sum_{\sigma\in\mathrm{Gal}(L/L')} \sigma \in \mathcal{R}[G]$ if $n \geq 1$ and $\mathbf{N}_{L/L'} = 0$ if $n = 0$, and define
$$R_L := \mathcal{R}[G]/\mathbf{N}_{L/L'}\mathcal{R}[G]$$
so $\mathrm{rank}_{\mathcal{R}} R_L = \varphi(\ell^n)$.

Fixing an identification $G \xrightarrow{\sim} \boldsymbol{\mu}_{\ell^n}$ of G with the group of ℓ^n-th roots of unity in $\bar{\mathcal{M}}$ induces an inclusion
$$R_L \hookrightarrow \mathcal{M}(\boldsymbol{\mu}_{\ell^n})$$
that identifies R_L with an order in $\mathcal{M}(\boldsymbol{\mu}_{\ell^n})$. Since ℓ is unramified in $\mathcal{M}/\mathbb{Q}$ we have that λ is totally ramified in $\mathcal{M}(\boldsymbol{\mu}_{\ell^n})/\mathcal{M}$, and we let λ_L denote the (unique) prime of R_L above λ.

Note that $\mathcal{I}_L$ is the annihilator of $\mathbf{N}_{L/L'}$ in $\mathcal{R}[G]$, so $\mathcal{I}_L$ is an R_L-module. The following proposition summarizes some of the properties of A_L proved in [**MRS**] that we will need.

Proposition 6.3. (i) *The natural action of G on $\mathrm{Res}_K^L(A)$ induces an inclusion $R_L \subset \mathrm{End}_K(A_L)$.*

(ii) *For every commutative K-algebra D, and every Galois extension F of K containing L, there is a natural $R_L[\mathrm{Gal}(F/K)]$-equivariant isomorphism*
$$A_L(D \otimes_K F) \cong \mathcal{I}_L \otimes_{\mathcal{R}} A(D \otimes_K F),$$
where R_L acts on A_L via the inclusion of (i) and on $\mathcal{I}_L \otimes A(D \otimes_K F)$ by multiplication on $\mathcal{I}_L$, and $\gamma \in \mathrm{Gal}(L/K)$ acts on $\mathcal{I}_L \otimes A(D \otimes_K F)$ as $\gamma^{-1} \otimes (1 \otimes \gamma)$.

(iii) *For every ideal $\mathfrak{b}$ of $\mathcal{R}$, the isomorphism of (ii) induces an isomorphism of $R_L[G_K]$-modules*
$$A_L[\mathfrak{b}] \cong \mathcal{I}_L \otimes_{\mathcal{R}} A[\mathfrak{b}].$$

(iv) *For every commutative K-algebra D, the isomorphism of (ii) induces an isomorphism of $\mathcal{R}$-modules*
$$A_L(D) \cong \mathcal{I}_L \otimes_{\mathcal{R}[G]} A(D \otimes_K L)$$
where $\gamma \in \mathrm{Gal}(L/K)$ acts on $D \otimes_K L$ as $1 \otimes \gamma$.

Proof. The first assertion is [**MRS**, Theorem 5.5], and the second is [**MRS**, Lemma 1.3]. Then (iii) follows from (ii) by taking $D := K$ and $F := \bar{K}$ (see [**MRS**, Theorem 2.2]), and (iv) follows from (ii) by setting $F := L$ and taking $\mathrm{Gal}(L/K)$ invariants of both sides (see [**MRS**, Theorem 1.4]). □

Corollary 6.4. *The isomorphism of Proposition 6.3(iii) induces an isomorphism of $\mathcal{R}[G_K]$-modules*
$$A_L[\lambda_L] \cong A[\lambda].$$

Proof. Fix a generator γ of G, and let $\bar{\gamma}$ denote its projection to R_L. Then λ_L is generated by λ and $\bar{\gamma} - 1$, so Proposition 6.3(iii) shows that
$$A_L[\lambda_L] = A_L[\lambda][\bar{\gamma} - 1] = (\mathcal{I}_L \otimes A[\lambda])[\bar{\gamma} - 1].$$
If $L = K$ there is nothing to prove. If $L \neq K$ then $\mathcal{I}_L$ is defined by the exact sequence
$$0 \longrightarrow \mathcal{I}_L \longrightarrow \mathcal{R}[G] \longrightarrow \mathcal{R}[G'] \longrightarrow 0. \tag{6.5}$$

Tensoring the free $\mathcal{R}$-modules of (6.5) with $A[\lambda]$ and taking the kernel of $\gamma - 1$ gives

$$0 \longrightarrow A_L[\lambda_L] \longrightarrow (\mathcal{R}[G] \otimes A[\lambda])[\gamma - 1] \longrightarrow \mathcal{R}[G'] \otimes A[\lambda]. \tag{6.6}$$

Explicitly,

$$(\mathcal{R}[G] \otimes A[\lambda])[\gamma - 1] = \{\textstyle\sum_{g \in G} g \otimes a : a \in A[\lambda]\} \cong A[\lambda],$$

and this is in the kernel of the right-hand map of (6.6), so the corollary follows. □

7. Local fields and local conditions

In this section we use the twists A_L of §6 to define the local conditions that will be used in §8 to define our relative Selmer groups $\mathrm{Sel}(L/K, A[\lambda])$.

Let A, $\mathcal{R}$, ℓ, and λ be as in §6, and keep the rest of the notation of §5 and §6 as well. For this section we restrict to the case where K is a local field of characteristic zero, i.e., a finite extension of some $\mathbb{Q}_\ell$ or of $\mathbb{R}$. Fix for this section a cyclic extension L/K of ℓ-power degree, and let $G := \mathrm{Gal}(L/K)$.

Definition 7.1. Define $\mathcal{H}_\lambda(L/K) \subset H^1(K, A[\lambda])$ to be the image of the composition

$$A_L(K)/\lambda_L A_L(K) \hookrightarrow H^1(K, A_L[\lambda_L]) \cong H^1(K, A[\lambda])$$

where λ_L is as in Definition 6.2, the first map is the Kummer map, and the second map is the isomorphism of Corollary 6.4. (This Kummer map depends on the choice of a generator of λ_L/λ_L^2, but its image is independent of this choice.) When $L = K$, $\mathcal{H}_\lambda(K/K)$ is just the image of the Kummer map

$$A(K)/\lambda A(K) \hookrightarrow H^1(K, A[\lambda])$$

and we will denote it simply by $\mathcal{H}_\lambda(K)$. We suppress the dependence on A from the notation when possible, since A is fixed throughout this section.

If K is nonarchimedean of characteristic different from ℓ, and A/K has good reduction, we define

$$H^1_{\mathrm{ur}}(K, A[\lambda]) := H^1(K^{\mathrm{ur}}/K, A[\lambda]),$$

the unramified subgroup of $H^1(K, A[\lambda])$.

Lemma 7.2. *Suppose K is nonarchimedean of residue characteristic different from ℓ.*

(i) *We have* $\dim_{\mathbb{F}_\ell}(\mathcal{H}_\lambda(L/K)) = \dim_{\mathbb{F}_\ell} A(K)[\lambda]$.

(ii) *If A has good reduction and $\phi \in G_K$ is an automorphism that restricts to Frobenius in* $\mathrm{Gal}(K^{\mathrm{ur}}/K)$*, then*

$$\dim_{\mathbb{F}_\ell}(\mathcal{H}_\lambda(L/K)) = \dim_{\mathbb{F}_\ell} A[\lambda]/(\phi - 1)A[\lambda].$$

Proof. Suppose K is nonarchimedean of residue characteristic different from ℓ. Then $A_L(K)$ has a subgroup of finite index that is ℓ-divisible, so

$$A_L(K)/\lambda_L A_L(K) \cong A_L(K)_{\mathrm{tors}}/\lambda_L A_L(K)_{\mathrm{tors}} \cong A_L(K)[\lambda_L] \cong A(K)[\lambda]$$

where the second isomorphism is non-canonical and the third is Corollary 6.4. Since $\mathcal{H}_\lambda(L/K) \cong A_L(K)/\lambda_L A_L(K)$ by definition, this proves (i).

If further A has good reduction then $A[\lambda] \subset A(K^{\mathrm{ur}})$. If ϕ is an Frobenius automorphism in $\mathrm{Gal}(K^{\mathrm{ur}}/K)$, then $A(K)[\lambda] = A[\lambda]^{\phi=1}$ so

$$\dim_{\mathbb{F}_\ell} A(K)[\lambda] = \dim_{\mathbb{F}_\ell} A[\lambda]^{\phi=1} = \dim_{\mathbb{F}_\ell}(A[\lambda]/(\phi - 1)A[\lambda].$$

Now (ii) follows from (i). □

Lemma 7.3. *Suppose K is nonarchimedean of residue characteristic different from ℓ, A/K has good reduction, and L/K is unramified.*

(i) *If $\phi \in G_K$ is an automorphism that restricts to Frobenius in* $\mathrm{Gal}(K^{\mathrm{ur}}/K)$, *then evaluation of cocycles at ϕ induces an isomorphism*

$$H^1_{\mathrm{ur}}(K, A[\lambda]) \xrightarrow{\sim} A[\lambda]/(\phi - 1)A[\lambda].$$

(ii) *The twist A_L has good reduction, and $\mathcal{H}_\lambda(L/K) = H^1_{\mathrm{ur}}(K, A[\lambda])$. In particular under these assumptions $\mathcal{H}_\lambda(L/K)$ is independent of L.*

Proof. This is well-known. For (i), see for example [**Ru**, Lemma 1.3.2(i)]. That A_L has good reduction when L/K is unramified follows from the criterion of Néron-Ogg-Shafarevich and Proposition 6.3(iii). Since A_L has good reduction and L/K is unramified, we have $\mathcal{H}_\lambda(L/K) \subset H^1_{\mathrm{ur}}(K, A[\lambda])$, and further

$$\dim_{\mathbb{F}_\ell} \mathcal{H}_\lambda(L/K) = \dim_{\mathbb{F}_\ell}(A[\lambda]/(\phi - 1)A[\lambda]) = \dim_{\mathbb{F}_\ell} H^1_{\mathrm{ur}}(K, A[\lambda])$$

using Lemma 7.2(ii) for the first equality, and (i) for the second. This proves (ii). $\square$

Lemma 7.4. *Suppose K is nonarchimedean of residue characteristic different from ℓ, A/K has good reduction, and L/K is nontrivial and totally ramified. Let L_1 be the unique cyclic extension of K of degree ℓ in L. Then the map*

$$A_L(K)/\lambda_L A_L(K) \to A_L(L_1)/\lambda_L A_L(L_1)$$

induced by the inclusion $A_L(K) \subset A_L(L_1)$ is the zero map.

Proof. Since A/K has good reduction and the residue characteristic is different from ℓ, we have that $K(A[\ell^\infty])/K$ is unramified. Since L/K is totally ramified, $L \cap K(A[\ell^\infty]) = K$. Hence $A(L)[\ell^\infty] = A(K)[\ell^\infty]$, so by Proposition 6.3(iii),

$$\begin{aligned} A_L(K)[\ell^\infty] &= (\mathcal{I}_L \otimes A[\ell^\infty])^{G_K} = ((\mathcal{I}_L \otimes A[\ell^\infty])^{G_L})^G \\ &= (\mathcal{I}_L \otimes (A(L)[\ell^\infty]))^G = (\mathcal{I}_L \otimes (A(K)[\ell^\infty]))^G. \end{aligned} \tag{7.5}$$

As in the proof of Corollary 6.4, tensoring the exact sequence (6.5) with $A(K)[\ell^\infty]$ and taking G invariants gives an exact sequence

$$0 \longrightarrow (\mathcal{I}_L \otimes A(K)[\ell^\infty])^G \longrightarrow (\mathcal{R}[G] \otimes A(K)[\ell^\infty])^G \longrightarrow (\mathcal{R}[G'] \otimes A(K)[\ell^\infty])^G.$$

Since G acts trivially on $A(K)[\ell^\infty]$, we have

$$(\mathcal{R}[G] \otimes A(K)[\ell^\infty])^G = \{\textstyle\sum_{g \in G} g \otimes a : a \in A(K)[\ell^\infty]\}.$$

The map to $\mathcal{R}[G'] \otimes A(K)[\ell^\infty]$ sends $\sum_{g \in G} g \otimes a$ to $\ell \sum_{g \in G'} g \otimes a$, which is zero if and only if $a \in A[\ell]$. Therefore

$$(\mathcal{I}_L \otimes (A(K)[\ell^\infty]))^G = \{\textstyle\sum_{g \in G} g \otimes a : a \in A(K)[\ell]\},$$

and combining this with (7.5) gives

$$A_L(K)[\ell^\infty] = \{\textstyle\sum_{g \in G} g \otimes a : a \in A(K)[\ell]\}. \tag{7.6}$$

An identical calculation shows that

$$A_L(L_1)[\ell] = \{\textstyle\sum_{i=0}^{\ell^n - 1} (\gamma^i \otimes a_i) : a_i \in A(K)[\ell] \text{ and } a_i = a_j \text{ if } i \equiv j \pmod{\ell}\}. \tag{7.7}$$

If $a \in A(K)[\ell]$, then using the identification (7.7) we have $\sum_{i=0}^{\ell^n-1}(\gamma^i \otimes ia) \in A_L(L_1)[\ell]$, and

$$(\gamma - 1)\sum_{i=0}^{\ell^n-1}(\gamma^i \otimes ia) = -\sum_{i=0}^{\ell^n-1}\gamma^i \otimes a.$$

Taken together with (7.6), this proves that

$$A_L(K)[\ell^\infty] \subset (\gamma-1)A_L(L_1) \subset \lambda_L A_L(L_1)$$

Now the lemma follows, because the map

$$A_L(K)[\ell^\infty] \twoheadrightarrow A_L(K)/\lambda_L A_L(K)$$

is surjective (since the residue characteristic of K is different from ℓ). $\square$

Proposition 7.8. *Suppose A/K has good reduction, K is nonarchimedean of residue characteristic different from ℓ, and L/K is nontrivial and totally ramified.*

(i) *If $K \subsetneq L' \subseteq L$ then $\mathcal{H}_\lambda(L'/K) = \mathcal{H}_\lambda(L/K)$.*
(ii) $H^1_{\mathrm{ur}}(K, A[\lambda]) \cap \mathcal{H}_\lambda(L/K) = 0$.

Proof. Let L_1 be the cyclic extension of K of degree ℓ in L. In the commutative diagram

$$\begin{tikzcd}
A_L(L_1)/\lambda_L A_L(L_1) \arrow[r, hook] & H^1(L_1, A_L[\lambda_L]) \arrow[r, "\sim"] & H^1(L_1, A[\lambda]) \\
A_L(K)/\lambda_L A_L(K) \arrow[r, hook] \arrow[u] & H^1(K, A_L[\lambda_L]) \arrow[r, "\sim"] \arrow[u] & H^1(K, A[\lambda]) \arrow[u]
\end{tikzcd}$$

the left-hand vertical map is zero by Lemma 7.4, so by definition of $\mathcal{H}_\lambda(L/K)$ we have

$$\mathcal{H}_\lambda(L/K) \subset \ker(H^1(K, A[\lambda]) \to H^1(L_1, A[\lambda])). \tag{7.9}$$

Since the inertia group acts trivially on $A[\lambda]$, we have $A[\lambda]^{G_L} = A[\lambda]^{G_{L_1}} = A[\lambda]^{G_K}$, so

$$\begin{aligned}\ker(H^1(K, A[\lambda]) \to H^1(L_1, A[\lambda])) &= H^1(L_1/K, A[\lambda]^{G_{L_1}}) \\ &= H^1(L_1/K, A[\lambda]^{G_K}) = \mathrm{Hom}(\mathrm{Gal}(L_1/K), A(K)[\lambda]).\end{aligned} \tag{7.10}$$

We have (using Lemma 7.2(i) for the first equality)

$$\dim_{\mathbb{F}_\ell} \mathcal{H}_\lambda(L/K) = \dim_{\mathbb{F}_\ell} A(K)[\lambda] = \dim_{\mathbb{F}_\ell} \mathrm{Hom}(\mathrm{Gal}(L_1/K), A(K)[\lambda]). \tag{7.11}$$

Combining (7.9), (7.10), and (7.11) shows that the inclusion (7.9) must be an equality. This proves (i), because the kernel in (7.9) depends only on L_1. Assertion (ii) follows from (7.9) and the fact that (since L_1/K is totally ramified) the restriction map

$$H^1_{\mathrm{ur}}(K, A[\lambda]) \hookrightarrow H^1_{\mathrm{ur}}(L_1, A[\lambda]) \subset H^1(L_1, A[\lambda])$$

is injective. $\square$

Remark 7.12. The proof of Proposition 7.8 shows that if A has good reduction, and L/K is a ramified cyclic extension of degree ℓ, then $\mathcal{H}_\lambda(L/K)$ is the "L-transverse" subgroup of $H^1(K, A[\lambda])$, as defined in [**MR2**, Definition 1.1.6].

8. Selmer groups and Selmer structures

In this section we use the definitions of §6 and §7 to define the relative Selmer groups $\mathrm{Sel}(L/K, A[\lambda])$ described in §5.

Keep the notation of the previous sections, except that from now on K is a number field. If v is a place of K we will denote by L_v the completion of L at some fixed place above v. We will write A_L, R_L, $\mathcal{I}_L$, and λ_L for the objects defined in §6 using the extension L/K, and A_{L_v}, R_{L_v}, $\mathcal{I}_{L_v}$, and λ_{L_v} for the ones corresponding to the extension L_v/K_v.

Definition 8.1. If L/K is a cyclic extension of ℓ-power degree, we define the λ-Selmer group $\mathrm{Sel}(L/K, A[\lambda]) \subset H^1(K, A[\lambda])$ by

$$\mathrm{Sel}(L/K, A[\lambda]) := \{c \in H^1(K, A[\lambda]) : \mathrm{loc}_v(c) \in \mathcal{H}_\lambda(L_v/K_v) \text{ for every } v\}.$$

Here $\mathrm{loc}_v : H^1(K, A[\lambda]) \to H^1(K_v, A[\lambda])$ is the localization map, K_v is the completion of K at v, and L_v is the completion of L at any place above v. When $L = K$ this is the standard λ-Selmer group of A/K, and we denote it by $\mathrm{Sel}(K, A[\lambda])$.

Remark 8.2. The Selmer group $\mathrm{Sel}(L/K, A[\lambda])$ defined above consists of all classes $c \in H^1(K, A[\lambda])$ such that for every v, the localization $\mathrm{loc}_v(c)$ lies in the image of the composition of the upper two maps in the diagram

$$\begin{tikzcd} A_{L_v}(K_v)/\lambda_{L_v} A_{L_v}(K_v) \arrow[r, hook] & H^1(K_v, A_{L_v}[\lambda_{L_v}]) \arrow[d, "\cong"'] \\ & H^1(K_v, A[\lambda]) \\ A_L(K_v)/\lambda_L A_L(K_v) \arrow[r, hook] & H^1(K_v, A_L[\lambda_L]) \arrow[u, "\cong"] \end{tikzcd} \tag{8.3}$$

On the other hand, the classical λ_L-Selmer group of A_L is the set of all c in $H^1(K, A[\lambda])$ such that for every v, $\mathrm{loc}_v(c)$ is in the image of the composition of the *lower* two maps. Our methods apply directly to the Selmer groups $\mathrm{Sel}(L/K, A[\lambda])$, but for our applications we are interested in the classical Selmer group. The following lemma shows that these two definitions give the same Selmer groups.

Lemma 8.4. *The isomorphism of Proposition 6.3(iii) identifies* $\mathrm{Sel}(L/K, A[\lambda])$ *with the classical* λ_L*-Selmer group of* A_L.

Proof. We will show that for every place v, the image of the composition of the upper maps in (8.3) coincides with the image of the composition of the lower maps, and then the lemma follows from the definitions of the respective Selmer groups. We will do this by constructing a vertical isomorphism on the left-hand side of (8.3) that makes the diagram commute.

Let $G := \mathrm{Gal}(L/K)$ and $G_v := \mathrm{Gal}(L_v/K_v)$. The choice of place of L above v induces an isomorphism

$$\mathcal{R}[G] \otimes_{\mathcal{R}[G_v]} A(L_v) \xrightarrow{\sim} A(K_v \otimes_K L). \tag{8.5}$$

Using Proposition 6.3(iv) and (8.5) we have

$$\begin{aligned} A_L(K_v) &= \mathcal{I}_L \otimes_{\mathcal{R}[G]} A(K_v \otimes_K L) \\ &= \mathcal{I}_L \otimes_{\mathcal{R}[G]} (\mathcal{R}[G] \otimes_{\mathcal{R}[G_v]} A(L_v)) = \mathcal{I}_L \otimes_{\mathcal{R}[G_v]} A(L_v). \end{aligned} \tag{8.6}$$

Suppose first that $L_v = K_v$, so $A_{L_v} = A$ in (8.3). Tensoring (8.6) with R_L/λ_L gives

$$A_L(K_v)/\lambda_L A_L(K_v) \cong A(K_v) \otimes_{\mathcal{R}} \mathcal{I}_L/\lambda_L \mathcal{I}_L \cong A(K_v)/\lambda A(K_v)$$

and inserting this isomorphism into (8.3) gives a commutative diagram. This proves the lemma in this case.

Now suppose $L_v \neq K_v$. The inclusion $\mathcal{R}[G_v] \hookrightarrow \mathcal{R}[G]$ induces an isomorphism

$$\mathcal{R}[G] \otimes_{\mathcal{R}[G_v]} \mathcal{I}_{L_v} \xrightarrow{\sim} \mathcal{I}_L \tag{8.7}$$

(using here that $L_v \neq K_v$). Using Proposition 6.3(iv) (with K_v in place of K, and $D = K_v$) and (8.7) we have

$$\begin{aligned}\mathcal{I}_L \otimes_{\mathcal{R}[G_v]} A(L_v) &= (\mathcal{R}[G] \otimes_{\mathcal{R}[G_v]} \mathcal{I}_{L_v}) \otimes_{\mathcal{R}[G_v]} A(L_v) \\ &= \mathcal{R}[G] \otimes_{\mathcal{R}[G_v]} A_{L_v}(K_v) = R_L \otimes_{R_{L_v}} A_{L_v}(K_v)\end{aligned}$$

since $\mathcal{R}[G_v]$ acts on A_{L_v} through R_{L_v}. Combining this with (8.6) gives the first equality of

$$\begin{aligned}A_L(K_v)/\lambda_L A_L(K_v) &= A_{L_v}(K_v) \otimes_{R_{L_v}} (R_L/\lambda_L) \\ &= A_{L_v}(K_v) \otimes_{R_{L_v}} (R_{L_v}/\lambda_{L_v}) = A_{L_v}(K_v)/\lambda_{L_v} A_{L_v}(K_v)\end{aligned}$$

and the second follows from the natural isomorphism $R_{L_v}/\lambda_{L_v} \cong R_L/\lambda_L$ (again using that $L_v \neq K_v$). As in the previous case, inserting this isomorphism into (8.3) gives a commutative diagram and completes the proof of the lemma. $\square$

Proposition 8.8. *Suppose L/K is a cyclic extension of degree ℓ^n. Then*

$$\mathrm{rank}_{\mathbb{Z}}(A(L)) \leq \mathrm{rank}_{\mathbb{Z}}(A(K)) + \mathrm{rank}_{\mathbb{Z}}(\mathcal{R}) \sum_{i=1}^{n} \varphi(\ell^i) \dim_{\mathcal{R}/\lambda}(\mathrm{Sel}(L_i/K, A[\lambda]))$$

where L_i is the extension of K of degree ℓ^i in L.

Proof. There is an isogeny

$$\bigoplus_{i=0}^{n} A_{L_i} \longrightarrow \mathrm{Res}_K^L A$$

defined over K (see for example [**MR3**, Theorem 3.5] or [**MRS**, Theorem 5.2]). Since $A_{L_0} = A$, and $(\mathrm{Res}_K^{L_i} A)(K) = A(L_i)$, taking the K-points yields

$$\mathrm{rank}_{\mathbb{Z}} A(L) = \mathrm{rank}_{\mathbb{Z}} A(K) + \sum_{i=1}^{n} \mathrm{rank}_{\mathbb{Z}} A_{L_i}(K). \tag{8.9}$$

For every i, by Lemma 8.4 the Kummer map gives an injection

$$A_{L_i}(K) \otimes (R_{L_i}/\lambda_{L_i}) \hookrightarrow \mathrm{Sel}(L_i/K, A[\lambda]).$$

For every i the natural map $\mathcal{R} \to R_{L_i}$ induces an isomorphism $\mathcal{R}/\lambda \to R_{L_i}/\lambda_{L_i}$, and $\mathrm{rank}_{\mathbb{Z}}(R_{L_i}) = \varphi(\ell^i)\,\mathrm{rank}_{\mathbb{Z}}(\mathcal{R})$, so

$$\begin{aligned}\mathrm{rank}_{\mathbb{Z}} A_{L_i}(K) &= \mathrm{rank}_{\mathbb{Z}}(R_{L_i})\ \mathrm{rank}_{R_{L_i}}(A_{L_i}(K)) \\ &\leq \varphi(\ell^i)\ \mathrm{rank}_{\mathbb{Z}}(\mathcal{R})\ \dim_{\mathcal{R}/\lambda}(A_{L_i}(K) \otimes (R_{L_i}/\lambda_{L_i})) \\ &\leq \varphi(\ell^i)\ \mathrm{rank}_{\mathbb{Z}}(\mathcal{R})\ \dim_{\mathcal{R}/\lambda}(\mathrm{Sel}(L_i/K, A[\lambda])).\end{aligned}$$

Combined with (8.9) this proves the inequality of the proposition. $\square$

9. Twisting to decrease the Selmer rank

In this section we carry out the main argument of the proof of Theorem 1.2. Namely, we show how to choose good local conditions on the fields L so that the corresponding relative Selmer groups $\mathrm{Sel}(L/K, A[\lambda])$ vanish.

Let A/K, ℓ^n, and λ be as in the previous sections. Let $\mathcal{E} := \mathrm{End}_K(A)$, and recall that $\mathcal{R}$ is the center of $\mathcal{E}$. We will abbreviate $\mathbb{F}_\lambda := \mathcal{R}/\lambda$ and $\mathcal{E}/\lambda := \mathcal{E} \otimes_{\mathcal{R}} \mathbb{F}_\lambda$, so in particular $A[\lambda]$ is an $\mathcal{E}/\lambda$-module. Fix a polarization of A, and let $\alpha \mapsto \alpha^\dagger$ denote the Rosati involution of $\mathcal{E}$ corresponding to this polarization.

Definition 9.1. The ring $M_d(\mathbb{F}_\lambda)$ of $d \times d$ matrices with entries in $\mathbb{F}_\lambda$ has a unique (up to isomorphism) simple left module, namely $\mathbb{F}_\lambda^d$ with the natural action. If R is any ring isomorphic to $M_d(\mathbb{F}_\lambda)$, W is a simple left R-module, and V is a finitely generated left $\mathcal{E}/\lambda$-module, then $V \cong W^r$ for some r and we call r the *length* of V, so that

$$\mathrm{length}_{\mathcal{E}/\lambda} V = \frac{1}{d} \dim_{\mathbb{F}_\lambda} V.$$

For this section we assume in addition that:

(H.1) $\ell \geq 3$ and ℓ does not divide the degree of our fixed polarization,

(H.2) there are isomorphisms $\mathcal{E} \otimes_{\mathcal{R}} \mathcal{M}_\lambda \cong M_d(\mathcal{M}_\lambda)$, $\mathcal{E}/\lambda \cong M_d(\mathbb{F}_\lambda)$ for some d,

(H.3) $A[\lambda]$ and $\mathcal{A}[\lambda^\dagger]$ are irreducible $\mathcal{E}[G_K]$-modules,

(H.4) $H^1(K(A[\lambda])/K, A[\lambda]) = 0$ and $H^1(K(A[\lambda^\dagger])/K, A[\lambda^\dagger]) = 0$,

(H.5) there is no abelian extension of degree ℓ of $K(\boldsymbol{\mu}_\ell)$ in $K(\boldsymbol{\mu}_\ell, A[\lambda])$,

(H.6) there is a $\tau_0 \in G_{K(\boldsymbol{\mu}_\ell)}$ such that $A[\lambda]/(\tau_0 - 1)A[\lambda] = 0$,

(H.7) there is a $\tau_1 \in G_{K(\boldsymbol{\mu}_\ell)}$ such that $\mathrm{length}_{\mathcal{E}/\lambda}(A[\lambda]/(\tau_1 - 1)A[\lambda]) = 1$.

We will show in §10 below, using results of Serre, that almost all ℓ satisfy (H.1) through (H.5). If K is sufficiently large, then it follows from results of Larsen in the Appendix that (H.6) and (H.7) hold for a set of primes ℓ of positive density.

Suppose U is a finitely generated subgroup of $K^\times$, and consider the following diagram:

(9.2)
$$\begin{tikzcd}
 & K(\boldsymbol{\mu}_{\ell^n}, U^{1/\ell^n}, A[\lambda]) \arrow[dl, dash] \arrow[ddrr, dash] & & & \\
K(\boldsymbol{\mu}_{\ell^n}, U^{1/\ell^n}) \arrow[ddrr, dash] & & & & \\
 & & & K(\boldsymbol{\mu}_\ell, A[\lambda]) \arrow[dl, dash] \arrow[dr, dash] & \\
 & & K(\boldsymbol{\mu}_\ell) \arrow[dr, dash] & & K(A[\lambda]) \arrow[dl, dash] \\
 & & & K &
\end{tikzcd}$$

Lemma 9.3. *If U is a finitely generated subgroup of $K^\times$, then in the diagram* (9.2) *we have*

$$K(\boldsymbol{\mu}_{\ell^n}, U^{1/\ell^n}) \cap K(\boldsymbol{\mu}_\ell, A[\lambda]) = K(\boldsymbol{\mu}_\ell).$$

Proof. Let $F := K(\boldsymbol{\mu}_{\ell^n}, U^{1/\ell^n}) \cap K(\boldsymbol{\mu}_\ell, A[\lambda])$. Then $F/K(\boldsymbol{\mu}_\ell)$ is a Galois ℓ-extension, so if $F \neq K(\boldsymbol{\mu}_\ell)$ then F contains a cyclic extension $F'/K(\boldsymbol{\mu}_\ell)$ of degree ℓ. But since $F' \subset K(\boldsymbol{\mu}_\ell, A[\ell])$, this is impossible by (H.5). This proves the lemma. □

Lemma 9.4. *If U is a finitely generated subgroup of $K^\times$, then the restriction map*

$$H^1(K, A[\lambda]) \longrightarrow H^1(K(\boldsymbol{\mu}_{\ell^n}, U^{1/\ell^n}, A[\lambda]), A[\lambda])$$

is injective.

Proof. Let $F := K(\boldsymbol{\mu}_{\ell^n}, U^{1/\ell^n})$. Restriction gives a composition

$$\mathrm{Gal}(F(A[\lambda])/F) \xrightarrow{\sim} \mathrm{Gal}(K(\boldsymbol{\mu}_\ell, A[\lambda])/K(\boldsymbol{\mu}_\ell)) \hookrightarrow \mathrm{Gal}(K(A[\lambda])/K) \tag{9.5}$$

where the first map is an isomorphism by Lemma 9.3, and the second map is injective with cokernel of order prime to ℓ. The restriction map in the lemma is the composition of two restriction maps

$$H^1(K, A[\lambda]) \xrightarrow{f_1} H^1(F, A[\lambda]) \xrightarrow{f_2} H^1(F(A[\lambda]), A[\lambda]).$$

By (9.5) and (H.4), we have

$$\ker(f_2) = H^1(F(A[\lambda])/F, A[\lambda]) = H^1(K(A[\lambda])/K, A[\lambda]) = 0.$$

Further,

$$\ker f_1 = H^1(F/K, A(F)[\lambda]).$$

If $\tau_0 \in \mathrm{Gal}(K(\boldsymbol{\mu}_\ell, A[\lambda])/K(\boldsymbol{\mu}_\ell))$ is as in (H.6), then by (9.5) we can find $\tau_0' \in \mathrm{Gal}(F(A[\lambda])/F)$ that restricts to τ_0. But then τ_0' has no nonzero fixed points in $A[\lambda]$. Hence $A(F)[\lambda] = 0$, so $\ker(f_1) = 0$ as well and the proof is complete. □

Lemma 9.6. *Suppose F is a Galois extension of K containing $K(A[\lambda])$, and c is a cocycle representing a class in $H^1(K, A[\lambda])$ whose restriction to F is nonzero. If $\sigma \in G_K$ and $(\sigma - 1)A[\lambda] \neq A[\lambda]$, then the restriction of c to G_F induces a nonzero homomorphism*

$$G_F \longrightarrow A[\lambda]/(\sigma - 1)A[\lambda].$$

Proof. Since G_F acts trivially on $A[\lambda]$, the restriction of c to G_F is a (nonzero, by assumption) homomorphism $f : G_F^{\mathrm{ab}} \to A[\lambda]$. Recall that $\mathcal{E} := \mathrm{End}_K(A)$, and let $D \subset A[\lambda]$ denote the $\mathcal{E}$-module generated by the image of f. Since c is a lift from K, we have that f is G_K-equivariant, and in particular D is a nonzero $\mathcal{E}[G_K]$-submodule of $A[\lambda]$. By (H.3) it follows that $D = A[\lambda]$. But $(\sigma - 1)A[\lambda]$ is a proper $\mathcal{E}$-stable submodule of $A[\lambda]$, so the image of f cannot be contained in $(\sigma - 1)A[\lambda]$. □

Recall we have fixed a polarization of A of degree prime to ℓ (by (H.1)), and $\alpha \mapsto \alpha^\dagger$ is the corresponding Rosati involution of $\mathcal{E}$. The polarization induces a nondegenerate pairing $A[\ell] \times A[\ell] \to \boldsymbol{\mu}_\ell$, which restricts to a nondegenerate pairing

$$A[\lambda] \times A[\lambda^\dagger] \to \boldsymbol{\mu}_\ell$$

and induces an isomorphism

$$A[\lambda^\dagger] \cong \mathrm{Hom}(A[\lambda], \boldsymbol{\mu}_\ell). \tag{9.7}$$

Note that if conditions (H.1) through (H.7) hold for λ, then they also hold for $\lambda^\dagger$ (with the same τ_0 and τ_1).

Definition 9.8. If $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$, define relaxed-at-$\mathfrak{a}$ and strict-at-$\mathfrak{a}$ Selmer groups to be, respectively,

$$\mathrm{Sel}(K, A[\lambda])^{\mathfrak{a}} := \{c \in H^1(K, A[\lambda]) : \mathrm{loc}_v(c) \in \mathcal{H}_\lambda(K_v) \text{ for every } v \nmid \mathfrak{a}\},$$
$$\mathrm{Sel}(K, A[\lambda])_{\mathfrak{a}} := \{c \in \mathrm{Sel}(K, A[\lambda])^{\mathfrak{a}} : \mathrm{loc}_v(c) = 0 \text{ for every } v \mid \mathfrak{a}\},$$

and similarly with λ replaced by $\lambda^\dagger$. Note that

$$\mathrm{Sel}(K, A[\lambda])_{\mathfrak{a}} \subset \mathrm{Sel}(K, A[\lambda]) \subset \mathrm{Sel}(K, A[\lambda])^{\mathfrak{a}}.$$

Definition 9.9. From now on let Σ be a finite set of places of K containing all places where A has bad reduction, all places dividing $\ell\infty$, and large enough so that the primes in Σ generate the ideal class group of K. Define

$$\mathcal{O}_{K,\Sigma} := \{x \in K : x \in \mathcal{O}_{K_v} \text{ for every } v \notin \Sigma\},$$

the ring of Σ-integers of K. Define sets of primes $\mathcal{P} \subset \mathcal{Q}$ by

$$\mathcal{Q} := \{\mathfrak{p} \notin \Sigma : \mathbf{N}\mathfrak{p} \equiv 1 \pmod{\ell^n}\}$$
$$\mathcal{P} := \{\mathfrak{p} \in \mathcal{Q} : \text{the inclusion } K^\times \hookrightarrow K_{\mathfrak{p}}^\times \text{ sends } \mathcal{O}_{K,\Sigma}^\times \text{ into } (\mathcal{O}_{K_{\mathfrak{p}}}^\times)^{\ell^n}\}.$$

Note that the action of $\mathcal{E}$ on $A[\lambda]$ makes $H^1_{\mathrm{ur}}(K_{\mathfrak{p}}, A[\lambda])$ an $\mathcal{E}$-module. Define partitions of $\mathcal{P}, \mathcal{Q}$ into disjoint subsets $\mathcal{P}_i, \mathcal{Q}_i$ for $i \geq 0$ by

$$\mathcal{Q}_i := \{\mathfrak{p} \in \mathcal{Q} : \mathrm{length}_{\mathcal{E}/\lambda} H^1_{\mathrm{ur}}(K_{\mathfrak{p}}, A[\lambda]) = i\}, \quad \mathcal{P}_i := \mathcal{Q}_i \cap \mathcal{P}$$

and if $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$, let $\mathcal{P}_1(\mathfrak{a})$ be the subset of all $\mathfrak{p} \in \mathcal{P}_1$ such that the localization maps

$$\mathrm{Sel}(K, A[\lambda])_{\mathfrak{a}} \xrightarrow{\mathrm{loc}_{\mathfrak{p}}} H^1_{\mathrm{ur}}(K_{\mathfrak{p}}, A[\lambda]), \quad \mathrm{Sel}(K, A[\lambda^\dagger])_{\mathfrak{a}} \xrightarrow{\mathrm{loc}_{\mathfrak{p}}} H^1_{\mathrm{ur}}(K_{\mathfrak{p}}, A[\lambda^\dagger])$$

are both nonzero.

Note that by Lemma 7.3(i) and (9.7), if $\mathfrak{p} \in \mathcal{Q}_i$ then $\mathrm{length}_{\mathcal{E}/\lambda^\dagger} H^1_{\mathrm{ur}}(K_{\mathfrak{p}}, A[\lambda^\dagger]) = i$ as well.

In the language of the Introduction and §5, the *critical primes* are the primes in $\mathcal{Q}_1$ and the *silent primes* are the primes in $\mathcal{Q}_0$.

Proposition 9.10. (i) *The sets $\mathcal{P}_0$ and $\mathcal{P}_1$ have positive density.*

(ii) *Suppose $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$ such that both $\mathrm{Sel}(K, A[\lambda])_{\mathfrak{a}}$ and $\mathrm{Sel}(K, A[\lambda^\dagger])_{\mathfrak{a}}$ are nonzero. Then $\mathcal{P}_1(\mathfrak{a})$ has positive density, and if $\mathfrak{p} \in \mathcal{P}_1(\mathfrak{a})$ then*

$$\mathrm{length}_{\mathcal{E}/\lambda} \mathrm{Sel}(K, A[\lambda])_{\mathfrak{a}\mathfrak{p}} = \mathrm{length}_{\mathcal{E}/\lambda} \mathrm{Sel}(K, A[\lambda])_{\mathfrak{a}} - 1,$$
$$\mathrm{length}_{\mathcal{E}/\lambda^\dagger} \mathrm{Sel}(K, A[\lambda^\dagger])_{\mathfrak{a}\mathfrak{p}} = \mathrm{length}_{\mathcal{E}/\lambda^\dagger} \mathrm{Sel}(K, A[\lambda^\dagger])_{\mathfrak{a}} - 1.$$

Proof. Let τ_0, τ_1 be as in (H.6) and (H.7). By Lemma 9.3,

$$K(\boldsymbol{\mu}_\ell, A[\lambda]) \cap K(\boldsymbol{\mu}_{\ell^n}, (\mathcal{O}_{K,\Sigma}^\times)^{1/\ell^n}) = K(\boldsymbol{\mu}_\ell),$$

so for $i = 0$ or 1 we can choose $\sigma_i \in G_K$ such that

$$\sigma_i = \tau_i \text{ on } A[\lambda], \tag{9.11}$$

$$\sigma_i = 1 \text{ on } K(\boldsymbol{\mu}_{\ell^n}, (\mathcal{O}_{K,\Sigma}^\times)^{1/\ell^n}). \tag{9.12}$$

Fix $i = 0$ or 1, and suppose that $\mathfrak{p}$ is a prime of K whose Frobenius conjugacy class in $\mathrm{Gal}(K(\boldsymbol{\mu}_{\ell^n}, (\mathcal{O}_{K,\Sigma}^\times)^{1/\ell^n}, A[\lambda])/K)$ is the class of σ_i. Since Frobenius fixes $\boldsymbol{\mu}_{\ell^n}$ and $(\mathcal{O}_{K,\Sigma}^\times)^{1/\ell^n}$ by (9.12), we have that $\boldsymbol{\mu}_{\ell^n}$ and $(\mathcal{O}_{K,\Sigma}^\times)^{1/\ell^n}$ are contained in $K_{\mathfrak{p}}^\times$.

Hence $\mathbf{N}\mathfrak{p} \equiv 1 \pmod{\ell^n}$ and the inclusion $K^\times \hookrightarrow K_\mathfrak{p}^\times$ sends $\mathcal{O}_{K,\Sigma}^\times$ into $(\mathcal{O}_{K,\mathfrak{p}}^\times)^{\ell^n}$, so by definition $\mathfrak{p} \in \mathcal{P}$.

By (9.11) and Lemma 7.3, evaluation of cocycles on a Frobenius element for $\mathfrak{p}$ in G_K induces an isomorphism

$$\mathcal{H}_\lambda(K_\mathfrak{p}) = H^1_{\mathrm{ur}}(K_\mathfrak{p}, A[\lambda]) \xrightarrow{\sim} A[\lambda]/(\tau_i - 1)A[\lambda] \tag{9.13}$$

and similarly for $\lambda^\dagger$. Thus $\mathfrak{p} \in \mathcal{P}_i$, so the Cebotarev Theorem shows that $\mathcal{P}_0$ and $\mathcal{P}_1$ have positive density. This is (i).

Fix an ideal $\mathfrak{a}$ of $\mathcal{O}_K$ and suppose that c and d are cocycles representing nonzero elements of $\mathrm{Sel}(K, A[\lambda])_\mathfrak{a}$ and $\mathrm{Sel}(K, A[\lambda^\dagger])_\mathfrak{a}$, respectively. Let

$$F := K(\boldsymbol{\mu}_{\ell^n}, (\mathcal{O}_{K,\Sigma}^\times)^{1/\ell^n}, A[\lambda]),$$

and let σ_1 be as above. By Lemmas 9.4 and 9.6, the restrictions of c and d to G_F induce nonzero homomorphisms

$$\tilde{c} : G_F \longrightarrow A[\lambda]/(\sigma_1 - 1)A[\lambda], \quad \tilde{d} : G_F \longrightarrow A[\lambda^\dagger]/(\sigma_1 - 1)A[\lambda^\dagger].$$

Let Z_c be the subset of all $\gamma \in G_F$ such that $c(\gamma) = -c(\sigma_1)$ in $A[\lambda]/(\sigma_1 - 1)A[\lambda]$, and similarly for Z_d with λ replaced by $\lambda^\dagger$. Since $\tilde{c}$ and $\tilde{d}$ are nonzero, Z_c and Z_d each have Haar measure at most $1/\ell$ in G_F, so $Z_c \cup Z_d \neq G_F$ (this is where we use that $\ell \geq 3$ in assumption (H.1)).

Thus we can find $\gamma \in G_F$ such that $\tilde{c}(\gamma\sigma_1) \neq 0$ and $\tilde{d}(\gamma\sigma_1) \neq 0$. Since γ acts trivially on $A[\lambda]$, this means that

$$c(\gamma\sigma_1) \notin (\sigma_1 - 1)A[\lambda] = (\gamma\sigma_1 - 1)A[\lambda]$$

and similarly for d. Let N be a Galois extension of K containing F and such that the restrictions of c and d to G_F factor through $\mathrm{Gal}(N/F)$. If $\mathfrak{p}$ is a prime whose Frobenius conjugacy class in $\mathrm{Gal}(N/K)$ is the class of $\gamma\sigma_1$, then $\mathrm{loc}_\mathfrak{p}(c) \neq 0$ and $\mathrm{loc}_\mathfrak{p}(d) \neq 0$, so $\mathfrak{p} \in \mathcal{P}_1(\mathfrak{a})$. Now the Cebotarev Theorem shows that $\mathcal{P}_1(\mathfrak{a})$ has positive density.

If $\mathfrak{p} \in \mathcal{P}_1(\mathfrak{a})$ then we have exact sequences of $\mathcal{E}/\lambda$ and $\mathcal{E}/\lambda^\dagger$-modules

$$0 \longrightarrow \mathrm{Sel}(K, A[\lambda])_{\mathfrak{a}\mathfrak{p}} \longrightarrow \mathrm{Sel}(K, A[\lambda])_\mathfrak{a} \xrightarrow{\mathrm{loc}_\mathfrak{p}} H^1_{\mathrm{ur}}(K_\mathfrak{p}, A[\lambda]) \longrightarrow 0$$

$$0 \longrightarrow \mathrm{Sel}(K, A[\lambda^\dagger])_{\mathfrak{a}\mathfrak{p}} \longrightarrow \mathrm{Sel}(K, A[\lambda^\dagger])_\mathfrak{a} \xrightarrow{\mathrm{loc}_\mathfrak{p}} H^1_{\mathrm{ur}}(K_\mathfrak{p}, A[\lambda^\dagger]) \longrightarrow 0$$

where the right-hand maps are surjective because they are nonzero and (by (9.13)) the target modules are simple. This completes the proof of (ii). □

Definition 9.14. Suppose T is a finite set of primes of K, disjoint from Σ. We will say that an extension L/K is *T-ramified and Σ-split* if every $\mathfrak{p} \in T - \mathcal{Q}_0$ is totally ramified in L/K, every $\mathfrak{p} \notin T$ is unramified in L/K, and every $v \in \Sigma$ splits completely in L/K.

The primes in $\mathcal{Q}_0$ are the silent primes referred to in the Introduction and §5. The local Selmer conditions at these primes are zero, so we need no condition on their splitting behavior in Definition 9.14.

Lemma 9.15. *Suppose T is a nonempty finite subset of $\mathcal{P}$, and let $T_0 := T \cap \mathcal{P}_0$. For each $\mathfrak{p} \in T_0$ fix $e_\mathfrak{p}$ with $0 \leq e_\mathfrak{p} \leq n$. If $T = T_0$ assume in addition that some $e_\mathfrak{p} = n$. Then there is a cyclic extension L/K of degree ℓ^n that is T-ramified and Σ-split, and such that if $\mathfrak{p} \in T_0$ then the ramification degree of $\mathfrak{p}$ in L/K is $\ell^{e_\mathfrak{p}}$.*

Proof. Suppose $\mathfrak{p} \in \mathcal{P}$. Let $\mathbb{A}_K^\times$ denote the group of ideles of K, and let $K(\mathfrak{p})$ be the abelian extension of K corresponding by global class field theory to the subgroup

$$Y := K^\times (\mathcal{O}_{K_\mathfrak{p}}^\times)^{\ell^n} \prod_{v \in \Sigma} K_v^\times \prod_{v \notin \Sigma \cup \{\mathfrak{p}\}} \mathcal{O}_{K_v}^\times \subset \mathbb{A}_K^\times.$$

Class field theory tells us that the inertia (resp., decomposition) group of a place v in $\mathrm{Gal}(K(\mathfrak{p})/K)$ is the image of $\mathcal{O}_{K_v}^\times$ (resp., $K_v^\times$) in $\mathbb{A}_K^\times/Y$. If $v \nmid p$ then $\mathcal{O}_{K_v}^\times \subset Y$, so $K(\mathfrak{p})/K$ is unramified outside of $\mathfrak{p}$. If $v \in \Sigma$ then $K_v^\times \subset Y$, so every $v \in \Sigma$ splits completely in $K(\mathfrak{p})/K$. Since Σ was chosen large enough to generate the ideal class group of K, the natural map $\mathcal{O}_{K_\mathfrak{p}}^\times \to \mathbb{A}_K^\times/Y$ is surjective, so $K(\mathfrak{p})/K$ is totally ramified at $\mathfrak{p}$. It follows from the definition of $\mathcal{P}$ that $\mathrm{Gal}(K(\mathfrak{p})/K) \cong \mathbb{A}_K^\times/Y$ is cyclic of order ℓ^n. Now we can find an extension that is T-ramified and Σ-split, with the desired ramification degree at primes in T_0, inside the compositum of the fields $K(\mathfrak{p})$ for $\mathfrak{p} \in T$. $\square$

Lemma 9.16. *Suppose T is a finite subset of $\mathcal{P}$, and L/K is a cyclic extension of degree ℓ^n that is T-ramified and Σ-split. If $K \subsetneq L' \subset L$ then* $\mathrm{Sel}(L'/K, A[\lambda]) = \mathrm{Sel}(L/K, A[\lambda])$.

Proof. We will show that $\mathcal{H}_\lambda(L'_v/K_v) = \mathcal{H}_\lambda(L_v/K_v)$ for every v. If $v \in \Sigma$ this holds because $L'_v = L_v = K_v$. If $v \in T - \mathcal{P}_0$ this holds by Proposition 7.8(i). If $v \notin \Sigma \cup T$ this holds by Lemma 7.3(ii). Finally, if $v \in \mathcal{P}_0$ then $\mathcal{H}_\lambda(L'_v/K_v) = \mathcal{H}_\lambda(L_v/K_v) = 0$ by Lemmas 7.2(ii) and 7.3(i). Thus the two Selmer groups coincide in $H^1(K, A[\lambda])$. $\square$

In the terminology of the Introduction and §5, we next use critical primes (those in $\mathcal{P}_1$) to decrease the rank of the Selmer group, while the silent primes (those in $\mathcal{P}_0$) have no effect on the rank.

Proposition 9.17. *Let* $r := \mathrm{length}_{\mathcal{E}/\lambda}\mathrm{Sel}(K, A[\lambda])$, $r^\dagger := \mathrm{length}_{\mathcal{E}/\lambda^\dagger}\mathrm{Sel}(K, A[\lambda^\dagger])$, *and suppose that* $t \le \min\{r, r^\dagger\}$.

(i) *There is a set of primes $T \subset \mathcal{P}_1$ of cardinality t such that*

$$\mathrm{length}_{\mathcal{E}/\lambda}\mathrm{Sel}(K, A[\lambda])_\mathfrak{a} = r - t, \quad \mathrm{length}_{\mathcal{E}/\lambda^\dagger}\mathrm{Sel}(K, A[\lambda^\dagger])_\mathfrak{a} = r^\dagger - t,$$

where $\mathfrak{a} := \prod_{\mathfrak{p} \in T} \mathfrak{p}$.

(ii) *If T is as in (i), T_0 is a finite subset of $\mathcal{Q}_0$, and L/K is a cyclic extension of K of degree ℓ^n that is $(T_0 \cup T)$-ramified and Σ-split, then*

$$\mathrm{length}_{\mathcal{E}/\lambda}\mathrm{Sel}(L/K, A[\lambda]) = r - t, \quad \mathrm{length}_{\mathcal{E}/\lambda^\dagger}\mathrm{Sel}(L/K, A[\lambda^\dagger]) = r^\dagger - t.$$

Proof. We will prove (i) by induction on t. When $t = 0$ there is nothing to check.

Suppose T satisfies the conclusion of the lemma for t, and $t < \min\{r, r^\dagger\}$. Let $\mathfrak{a} := \prod_{\mathfrak{p} \in T} \mathfrak{p}$. Then we can apply Proposition 9.10(ii), to choose $\mathfrak{p} \in \mathcal{P}_1(\mathfrak{a})$ so that

$$\mathrm{length}_{\mathcal{E}/\lambda}\mathrm{Sel}(K, A[\lambda])_{\mathfrak{a}\mathfrak{p}} = r - t - 1, \quad \mathrm{length}_{\mathcal{E}/\lambda^\dagger}\mathrm{Sel}(K, A[\lambda^\dagger])_{\mathfrak{a}\mathfrak{p}} = r^\dagger - t - 1.$$

Then $T \cup \{\mathfrak{p}\}$ satisfies the conclusion of (i) for $t + 1$.

Now suppose that T is such a set, and $\mathfrak{a} := \prod_{\mathfrak{p}\in T}\mathfrak{p}$. Consider the exact sequences

$$\begin{array}{ll} & 0 \longrightarrow \mathrm{Sel}(K, A[\lambda]) \longrightarrow \mathrm{Sel}(K, A[\lambda])^{\mathfrak{a}} \xrightarrow{\oplus \mathrm{loc}_{\mathfrak{p}}} \bigoplus_{\mathfrak{p}\in T} H^1(K_{\mathfrak{p}}, A[\lambda])/\mathcal{H}_\lambda(K_{\mathfrak{p}}) \\ (9.18) & \\ & 0 \longrightarrow \mathrm{Sel}(K, A[\lambda^\dagger])_{\mathfrak{a}} \longrightarrow \mathrm{Sel}(K, A[\lambda^\dagger]) \xrightarrow{\quad\oplus \mathrm{loc}_{\mathfrak{p}}\quad} \bigoplus_{\mathfrak{p}\in T} \mathcal{H}_{\lambda^\dagger}(K_{\mathfrak{p}}). \end{array}$$

Using (9.7) to identify $A[\lambda^\dagger]$ with the dual of $A[\lambda]$, the local conditions that define the Selmer groups $\mathrm{Sel}(K, A[\lambda])$ and $\mathrm{Sel}(K, A[\lambda^\dagger])$ (resp. $\mathrm{Sel}(K, A[\lambda])^{\mathfrak{a}}$ and $\mathrm{Sel}(K, A[\lambda^\dagger])_{\mathfrak{a}}$) are dual Selmer structures in the sense of [**MR2**, §2.3]. Thus we can use global duality (see for example [**MR2**, Theorem 2.3.4]) to conclude that the images of the two right-hand maps in (9.18) are orthogonal complements of each other under the sum of the local Tate pairings. By our choice of T the lower right-hand map is surjective, so the upper right-hand map is zero, i.e.,

$$(9.19) \qquad (\oplus_{\mathfrak{p}\in T}\mathrm{loc}_{\mathfrak{p}})(\mathrm{Sel}(K, A[\lambda])^{\mathfrak{a}}) \subset \bigoplus_{\mathfrak{p}\in T} \mathcal{H}_\lambda(K_{\mathfrak{p}}).$$

Let T_0 be a finite subset of $\mathcal{Q}_0$, let $\mathfrak{b} := \prod_{\mathfrak{p}\in T_0}\mathfrak{p}$, and suppose L is a cyclic extension that is $(T_0 \cup T)$-ramified and Σ-split. By definition (and Lemma 7.3(ii)), $\mathrm{Sel}(L/K, A[\lambda])$ is the kernel of the map

$$\mathrm{Sel}(K, A[\lambda])^{\mathfrak{ab}} \xrightarrow{\oplus_{\mathfrak{p}\in T_0\cup T}\mathrm{loc}_{\mathfrak{p}}} \bigoplus_{\mathfrak{p}\in T_0\cup T} H^1(K_{\mathfrak{p}}, A[\lambda])/\mathcal{H}_\lambda(L_{\mathfrak{p}}/K_{\mathfrak{p}}).$$

We have $\mathcal{H}_\lambda(K_{\mathfrak{p}}) = \mathcal{H}_\lambda(L_{\mathfrak{p}}/K_{\mathfrak{p}}) = 0$ for every $\mathfrak{p} \in \mathcal{Q}_0$ by Lemmas 7.2(ii) and 7.3(i) and the definition of $\mathcal{Q}_0$, so in fact $\mathrm{Sel}(L/K, A[\lambda])$ is the kernel of the map

$$(9.20) \qquad \mathrm{Sel}(K, A[\lambda])^{\mathfrak{a}} \xrightarrow{\oplus_{\mathfrak{p}\in T}\mathrm{loc}_{\mathfrak{p}}} \bigoplus_{\mathfrak{p}\in T} H^1(K_{\mathfrak{p}}, A[\lambda])/\mathcal{H}_\lambda(L_{\mathfrak{p}}/K_{\mathfrak{p}}).$$

By Proposition 7.8(ii), $\mathcal{H}_\lambda(K_{\mathfrak{p}}) \cap \mathcal{H}_\lambda(L_{\mathfrak{p}}/K_{\mathfrak{p}}) = 0$ for every $\mathfrak{p} \in \mathcal{P}_1$. Combining (9.19) and (9.20) shows that $\mathrm{Sel}(L/K, A[\lambda]) = \mathrm{Sel}(L/K, A[\lambda])_{\mathfrak{a}}$, so by our choice of T we have $\mathrm{length}_{\mathcal{E}/\lambda}\mathrm{Sel}(L/K, A[\lambda]) = r - t$. The proof for $\lambda^\dagger$ is the same. ☐

Theorem 9.21. *Suppose that* (H.1) *through* (H.7) *all hold, and $n \geq 1$. Then for every finite set Σ of primes of K, there are infinitely many cyclic extensions L/K of degree ℓ^n, completely split at all places in Σ, such that $A(L) = A(K)$.*

Proof. Enlarge Σ if necessary so that the conditions of Definition 9.9 are satisfied. We may also assume without loss of generality that

$$\mathrm{length}_{\mathcal{E}/\lambda}\mathrm{Sel}(K, A[\lambda]) \leq \mathrm{length}_{\mathcal{E}/\lambda^\dagger}\mathrm{Sel}(K, A[\lambda^\dagger])$$

(if not, we can simply switch λ and $\lambda^\dagger$; all the properties we require for λ hold equivalently for $\lambda^\dagger$, using the isomorphism (9.7)). Apply Proposition 9.17(i) with $t := \mathrm{length}_{\mathcal{E}/\lambda}\mathrm{Sel}(K, A[\lambda])$ to produce a finite set $T \subset \mathcal{P}_1$.

Now suppose that T_0 is a finite subset of $\mathcal{Q}_0$. If L/K is cyclic of degree ℓ^n, $(T_0 \cup T)$-ramified and Σ-split, then Proposition 9.17 shows $\mathrm{Sel}(L/K, A[\lambda]) = 0$. Further, Lemma 9.16 shows that $\mathrm{Sel}(L'/K, A[\lambda]) = 0$ if $K \subsetneq L' \subset L$, so by Proposition 8.8 we have $\mathrm{rank}(A(L)) = \mathrm{rank}(A(K))$.

Since $\mathcal{P}_0$ has positive density (Proposition 9.10(i)), there are infinitely many finite subsets T_0 of $\mathcal{P}_0 \subset \mathcal{Q}_0$. For each such T_0, Lemma 9.15 shows that there is a cyclic extension L/K of degree ℓ^n that is $(T_0 \cup T)$-ramified and Σ-split, and totally ramified at all primes in T_0 as well. These fields are all distinct, so we have infinitely many different L with $\mathrm{rank}(A(L)) = \mathrm{rank}(A(K))$.

Now suppose that the set T_0 in the construction above contains primes $\mathfrak{p}_1, \mathfrak{p}_2$ with different residue characteristics. In particular L/K is totally ramified at $\mathfrak{p}_1$ and $\mathfrak{p}_2$. If $A(L) \neq A(K)$, then (since $\mathrm{rank}(A(L)) = \mathrm{rank}(A(K))$) there is a prime p and point $x \in A(L)$ such that $x \notin A(K)$ but $px \in A(K)$. It follows that the extension $K(x)/K$ is unramified outside of Σ and primes above p. In particular $K \subset K(x) \subset L$ but $K(x)/K$ cannot ramify at both $\mathfrak{p}_1$ and $\mathfrak{p}_2$, so we must have $K(x) = K$, i.e., $x \in A(K)$. This contradiction shows that $A(L) = A(K)$ for all such T_0, and this proves the theorem. □

10. Proof of Theorem 1.2

Proposition 10.1. *Conditions* (H.1) *through* (H.5) *hold for all sufficiently large* ℓ.

Proof. This is clear for (H.1).

Recall that λ was chosen not to divide the discriminant of $\mathcal{R}$, so $\mathcal{R}_\lambda$ is the ring of integers of $\mathcal{M}_\lambda$. Since A is simple, $\mathcal{E} \otimes \mathbb{Q}$ is a central simple division algebra over $\mathcal{M}$, of some degree d. By the general theory of such algebras (see for example [**Pi**, Proposition in §18.5]), for all but finitely many primes λ of $\mathcal{M}$ we have

$$\mathcal{E} \otimes_{\mathcal{R}} \mathcal{M}_\lambda \cong M_d(\mathcal{M}_\lambda).$$

If in addition λ does not divide the index of $\mathcal{E}$ in a fixed maximal order of $\mathcal{E} \otimes_{\mathcal{R}} \mathcal{M}$, then

$$\mathcal{E} \otimes_{\mathcal{R}} \mathcal{R}_\lambda \text{ is a maximal order in } \mathcal{E} \otimes_{\mathcal{R}} \mathcal{M}_\lambda.$$

By [**AG**, Proposition 3.5], every maximal order in $M_d(\mathcal{M}_\lambda)$ is conjugate to $M_d(\mathcal{R}_\lambda)$, so for such λ we have

$$\mathcal{E}/\lambda := \mathcal{E} \otimes_{\mathcal{R}} \mathbb{F}_\lambda \cong M_d(\mathcal{R}_\lambda) \otimes_{\mathcal{R}} \mathbb{F}_\lambda = M_d(\mathbb{F}_\lambda)$$

which is (H.2).

Condition (H.3) holds for large ℓ by Corollary A.16 of the Appendix.

Let $B \subset \mathrm{Gal}(K(A[\lambda])/K)$ denote the subgroup acting as scalars on $A[\lambda]$. Then B is a normal subgroup and we have the inflation-restriction exact sequence

$$(10.2) \qquad H^1(K(A[\lambda])^B/K, A[\lambda]^B) \longrightarrow H^1(K(A[\lambda])/K, A[\lambda]) \longrightarrow H^1(B, A[\lambda]).$$

Since B has order prime to ℓ, $H^1(B, A[\lambda] = 0$. Serre [**Ser**, Théorème of §5] shows that B is nontrivial for all sufficiently large ℓ. When B is nontrivial, $A[\lambda]^B = 0$ so the left-hand term in (10.2) vanishes and (H.4) holds.

Let Γ denote the image of $\mathrm{Gal}(K(\boldsymbol{\mu}_\ell, A[\lambda])/K(\boldsymbol{\mu}_\ell))$ in $\mathrm{Aut}(A[\lambda])$. Then [**LP2**, Theorem 0.2] shows that there are normal subgroups $\Gamma_3 \subset \Gamma_2 \subset \Gamma_1$ of Γ such that Γ_3 is an ℓ-group, Γ_2/Γ_3 has order prime to ℓ, Γ_1/Γ_2 is a direct product of finite simple groups of Lie type in characteristic ℓ, and $[\Gamma : \Gamma_1]$ is bounded independently of ℓ. By Faltings' theorem (see for example the proof of (H.3) referenced above) Γ acts semisimply on $A[\lambda]$ for sufficiently large ℓ, and then Γ_3 must be trivial. It follows that if ℓ is sufficiently large then Γ has no cyclic quotient of order ℓ, i.e., (H.5) holds. □

Theorem 10.3 (Larsen)**.** *Suppose that all $\bar{K}$-endomorphisms of A are defined over K. Then the conditions* (H.6) *and* (H.7) *hold simultaneously for a set of primes ℓ of positive density.*

Proof. This is Theorem A.1 of the Appendix. □

Proof of Theorem 1.2. If all $\bar{K}$-endomorphisms of A are defined over K, then by Proposition 10.1 and Theorem 10.3 there is a set S of rational primes with positive density such that our hypotheses (H.1) through (H.7) hold simultaneously for all $\ell \in S$. Thus Theorem 1.2 follows from Theorem 9.21. □

Proof of Theorem 1.3. Lemma 3.3 showed that Theorem 1.3 follows from Theorem 1.2. □

Remark 10.4. It is natural to try to strengthen Theorem 1.2 by removing the assumption that A is simple. This generalization can be reduced to the problem, given a finite collection of abelian varieties, of finding many cyclic extensions for which they are all simultaneously diophantine-stable.

Precisely, suppose that $A_1, \ldots, A_m$ are pairwise non-isogenous absolutely simple abelian varieties, ℓ is a rational prime, and λ_i is a prime ideal of the center of $\mathrm{End}(A_i)$ above ℓ for each i. Suppose ℓ is large enough so that (H.1) through (H.5) hold for every A_i.

If the results of the Appendix could be extended to show that for every j there is an element $\tau_j \in G_{K(\boldsymbol{\mu}_\ell)}$ such that

$$A_i[\lambda_i]/(\tau_j - 1)A_i[\lambda_i] \;\text{ is }\; \begin{cases} \text{zero if } i \neq j, \\ \text{a nonzero simple } \mathrm{End}(A_j)/\lambda_j\text{-module if } i = j, \end{cases}$$

then the methods of §9 above would show that there is a set S of rational primes with positive density such that for every $\ell \in S$ and every $n \geq 1$ there are infinitely many cyclic extensions L/K of degree ℓ^n such that every A_i is diophantine-stable for L/K. Using the argument at the end of the proof of Theorem 9.21 it would follow that S can be chosen so that the same result holds for every abelian variety isogenous over K to $\prod_i A_i^{d_i}$.

11. Quantitative results

Fix a simple abelian variety A/K such that $\mathrm{End}_K(A) = \mathrm{End}_{\bar{K}}(A)$, and an ℓ such that our hypotheses (H.1) through (H.7) all hold. The proof of Theorem 1.2, and more precisely Theorem 9.21, makes it possible to quantify how many cyclic ℓ^n-extensions L/K are being found with $A(L) = A(K)$. For simplicity we will take $n = 1$, and count cyclic ℓ-extensions. Keep the notation of the previous sections.

For real numbers $X > 0$, define

$$\mathcal{F}_K(X) := \{\text{cyclic extensions } L/K \text{ of degree } \ell : \mathbf{N}\mathfrak{d}_{L/K} < X\},$$
$$\mathcal{F}_K^0(X) := \{L \in \mathcal{F}_K(X) : A(L) = A(K)\},$$

where $\mathbf{N}\mathfrak{d}_{L/K}$ denotes the absolute norm of the relative discriminant of L/K. For $\mathfrak{p} \notin \Sigma$ let $\mathrm{Fr}_\mathfrak{p} \in G_K$ denote a Frobenius automorphism for $\mathfrak{p}$. It follows from Definition 9.9 and Lemma 7.3(i) that

$$\mathcal{Q}_0 := \{\mathfrak{p} \notin \Sigma : \mathrm{Fr}_\mathfrak{p} = 1 \text{ on } \boldsymbol{\mu}_\ell \text{ and } \mathrm{Fr}_\mathfrak{p} \text{ has no nonzero fixed points in } A[\lambda]\},$$

and let

$$\delta := \frac{|\{\sigma \in \mathrm{Gal}(K(\boldsymbol{\mu}_\ell, A[\lambda])/K(\boldsymbol{\mu}_\ell)) : \sigma \text{ has no nonzero fixed points in } A[\lambda]\}|}{[K(\boldsymbol{\mu}_\ell, A[\lambda]) : K(\boldsymbol{\mu}_\ell)]}$$

The proof of Proposition 9.10(i) shows that $\mathcal{Q}_0$ has density $\delta/[K(\boldsymbol{\mu}_\ell) : K]$, and (H.6) and (H.7) show that $0 < \delta < 1$.

Theorem 11.1 (Wright [**Wri**]). *There is a positive constant C such that*

$$|\mathcal{F}_K(X)| \sim CX^{1/(\ell-1)} \log(X)^{(\ell-1)/[K(\boldsymbol{\mu}_\ell):K]-1}$$

as $X \to \infty$.

The main result of this section is the following.

Theorem 11.2. *As $X \to \infty$ we have*

$$|\mathcal{F}_K^0(X)| \gg X^{1/(\ell-1)} \log(X)^{(\ell-1)\delta/[K(\boldsymbol{\mu}_\ell):K]-1}.$$

Example 11.3. Suppose E is a non-CM elliptic curve, and ℓ is large enough so that the Galois representation $G_K \to \mathrm{Aut}(E[\ell]) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is surjective. Then $[K(\boldsymbol{\mu}_\ell) : K] = \ell - 1$, and an elementary calculation shows that the number of elements of $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ with nonzero fixed points is ℓ^2. Thus $\delta = 1 - \ell/(\ell^2 - 1)$ so in this case

$$|\mathcal{F}_K(X)| \sim CX^{1/(\ell-1)}, \quad |\mathcal{F}_K^0(X)| \gg X^{1/(\ell-1)}/\log(X)^{\ell/(\ell^2-1)}.$$

The rest of this section is devoted to a proof of Theorem 11.2.

Lemma 11.4. *There is a finite subset $T_1 \subset \mathcal{Q}_0$ such that the natural map*

$$\mathcal{O}_{K,\Sigma}^\times/(\mathcal{O}_{K,\Sigma}^\times)^\ell \longrightarrow \prod_{v \in T_1} \mathcal{O}_{K_v}^\times/(\mathcal{O}_{K_v}^\times)^\ell$$

is injective.

Proof. Suppose $u \in \mathcal{O}_{K,\Sigma}^\times$ and $u \notin (K^\times)^\ell$. Then $u \notin (K(\boldsymbol{\mu}_\ell)^\times)^\ell$, so by Lemma 9.3 and (H.6) we can choose $\sigma \in G_K$ such that $\sigma = 1$ on $\boldsymbol{\mu}_\ell$, σ has no nonzero fixed points in $A[\lambda]$, and σ does not fix $u^{1/\ell}$. If $v \notin \Sigma$ and the Frobenius of v on $K(\boldsymbol{\mu}_\ell, A[\lambda], (\mathcal{O}_{K,\Sigma}^\times)^{1/\ell})$ is in the conjugacy class of σ, then $v \in \mathcal{Q}_0$ and $u \notin (\mathcal{O}_{K_v}^\times)^\ell$. Taking a collection of such v as u varies gives a suitable set T_1. ☐

Recall that $\mathbb{A}_K^\times$ denote the ideles of K. Fix a set T_1 as in Lemma 11.4.

Lemma 11.5. *The natural composition*

$$\mathrm{Hom}(G_K, \boldsymbol{\mu}_\ell) \longrightarrow \mathrm{Hom}(\mathbb{A}_K^\times, \boldsymbol{\mu}_\ell) \longrightarrow \prod_{v \in \Sigma} \mathrm{Hom}(K_v^\times, \boldsymbol{\mu}_\ell) \prod_{v \notin \Sigma \cup T_1} \mathrm{Hom}(\mathcal{O}_{K_v}^\times, \boldsymbol{\mu}_\ell)$$

is surjective.

Proof. By class field theory and our assumption that the primes in Σ generate the ideal class group of K, we have an isomorphism

$$\mathrm{Hom}(G_K, \boldsymbol{\mu}_\ell) \cong \mathrm{Hom}\Big((\prod_{v \in \Sigma} K_v^\times \prod_{v \in T_1} \mathcal{O}_{K_v}^\times \prod_{v \notin \Sigma \cup T_1} \mathcal{O}_{K_v}^\times)/\mathcal{O}_{K,\Sigma}^\times, \boldsymbol{\mu}_\ell \Big)$$

Now the lemma follows by a simple argument using Lemma 11.4; see for example [**KMR**, Lemma 6.6(ii)]. ☐

As in the proof of Theorem 9.21, we can use Proposition 9.17 to fix a finite set $T \subset \mathcal{P}_1$ such that for every finite set $T_0 \subset \mathcal{Q}_0$, and every cyclic ℓ-extension L/K that is

- $(T_0 \cup T)$-ramified and Σ-split,

- ramified at two primes in T_0 of different residue characteristics,

we have $A(L) = A(K)$.

Definition 11.6. Fix two primes $\mathfrak{p}_1, \mathfrak{p}_2 \in \mathcal{P}_0 - T_1$ of different residue characteristics, and let $T' := T \cup \{\mathfrak{p}_1, \mathfrak{p}_2\}$. For every finite subset T_0 of $\mathcal{Q}_0 - T_1$, let $\mathcal{C}(T_0) \subset \mathrm{Hom}(G_K, \boldsymbol{\mu}_\ell)$ be the subset of characters χ satisfying, under the class field theory surjection of Lemma 11.5,

- $\chi|_{K_v^\times} = 1$ if $v \in \Sigma$,
- $\chi|_{\mathcal{O}_{K_v}^\times} \neq 1$ if $v \in T' \cup T_0$,
- $\chi|_{\mathcal{O}_{K_v}^\times} = 1$ if $v \notin \Sigma \cup T' \cup T_0 \cup T_1$.

Lemma 11.7. *Let α be the (surjective) composition of maps in Lemma 11.5. Then for every finite subset $T_0 \subset \mathcal{Q}_0 - T_1$ we have $|\mathcal{C}(T_0)| = |\ker(\alpha)|(\ell-1)^{|T'|}(\ell-1)^{|T_0|}$.*

Proof. This is clear from the surjectivity of α. $\square$

Lemma 11.8. *Suppose T_0 is a finite subset of $\mathcal{Q}_0 - T_1$, and $\chi \in \mathcal{C}(T_0)$. Let L be the fixed field of the kernel of χ. Then:*

(i) *$A(L) = A(K)$,*
(ii) *the discriminant of L/K is $\prod_{\mathfrak{p} \in T' \cup T_0} \mathfrak{p}^{\ell-1}$.*

Proof. The first assertion follows from the definition of T above. For the second, by definition of $\mathcal{C}(T_0)$ we have that L/K is cyclic of degree ℓ, totally tamely ramified at $\mathfrak{p} \in T' \cup T_0$ and unramified elsewhere. $\square$

Proof of Theorem 11.2. Define a function f on ideals of K by

$$f(\mathfrak{a}) := \begin{cases} (\ell-1)^{|T_0|} & \text{if } T_0 \text{ is a finite subset of } \mathcal{Q}_0 - T_1 \text{ and } \mathfrak{a} = \prod_{\mathfrak{p} \in T_0} \mathfrak{p}, \\ 0 & \text{if } \mathfrak{a} \text{ is not a squarefree product of primes in } \mathcal{Q}_0 - T_1. \end{cases}$$

Then $\sum_{\mathfrak{a}} f(\mathfrak{a}) \mathbf{N}\mathfrak{a}^{-s} = \prod_{\mathfrak{p} \in \mathcal{Q}_0 - T_1} (1 + (\ell-1)\mathbf{N}\mathfrak{p}^{-s})$, so

$$\log\Bigl(\sum_{\mathfrak{a}} f(\mathfrak{a}) \mathbf{N}\mathfrak{a}^{-s}\Bigr) \approx (\ell-1) \sum_{\mathfrak{p} \in \mathcal{Q}_0 - T_1} \mathbf{N}\mathfrak{p}^{-s} \approx \frac{(\ell-1)\delta}{[K(\boldsymbol{\mu}_\ell):K]} \frac{1}{\log(s-1)}$$

where "$\approx$" means that the two sides are holomorphic on $\Re(s) > 1$ and their difference approaches a finite limit as $\Re(s) \to 1^+$. Therefore by a variant of the Ikehara Tauberian Theorem (see for example [**Win**, p. 322]) we conclude that there is a constant D such that

$$\sum_{\mathbf{N}\mathfrak{a} < X} f(\mathfrak{a}) \sim DX \log(X)^{(\ell-1)\delta/[K(\boldsymbol{\mu}_\ell):K]-1}.$$

By Lemmas 11.7 and 11.8, for every $\mathfrak{a}$ the number of cyclic ℓ-extensions L/K of discriminant $(\mathfrak{a} \prod_{\mathfrak{p} \in T'} \mathfrak{p})^{\ell-1}$ with $A(L) = A(K)$ is at least $f(\mathfrak{a})$, and the theorem follows. $\square$

References

[**AG**] M. Auslander, O. Goldman, Maximal orders. *Trans. Amer. Math. Soc.* **97** (1960) 1–24.

[**DFK**] C. David, J. Fearnley, H. Kisilevsky, Vanishing of L-functions of elliptic curves over number fields. In: Ranks of elliptic curves and random matrix theory, *London Math. Soc. Lecture Notes* **341**, Cambridge Univ. Press, Cambridge (2007) 247–259.

[**FK**] J. Fearnley, H. Kisilevsky, Critical values of derivatives of twisted elliptic L-functions. *Experiment. Math.* **19** (2010) 149–160.

[**KMR**] Z. Klagsbrun, B. Mazur, K. Rubin, Disparity in Selmer ranks of quadratic twists of elliptic curves. *Annals of Math.* **178** (2013) 287–320.

[**LP2**] M. Larsen, R. Pink, Finite subgroups of algebraic groups. *J. Amer. Math. Soc.* **24** (2011) 1105–1158.

[**Maz**] B. Mazur, Rational isogenies of prime degree. Inventiones math. **44** (1978) 129–162.

[**MR1**] B. Mazur, K. Rubin, Studying the growth of Mordell-Weil. *Documenta Math.* Extra volume Kato (2003) 585–607.

[**MR2**] B. Mazur, K. Rubin, Kolyvagin systems. *Memoirs of the Amer. Math. Soc.* **799** (2004).

[**MR3**] B. Mazur, K. Rubin, Finding large Selmer rank via an arithmetic theory of local constants. *Annals of Math.* **166** (2007) 569–612.

[**MRS**] B. Mazur, K. Rubin, A. Silverberg, Twisting commutative algebraic groups. *Journal of Algebra* **314** (2007) 419–438.

[**Pi**] R. Pierce, Linear Associative Algebras. *Graduate Texts in Math.* **88**, Springer-Verlag, Berlin (1982).

[**Rib**] K. Ribet, Endomorphisms of semi-stable abelian varieties over number fields. *Annals of Math.* **101** (1975) 555–562.

[**Ru**] K. Rubin, Euler Systems. *Annals of Math. Studies* **147**, Princeton: Princeton University Press (2000).

[**SCF**] J-P. Serre, Local Class Field Theory. In: Algebraic Number Theory, Cassels and Fröhlich, eds. Thompson Book Co., Washington DC (1967) 128–161.

[**Ser**] J-P. Serre, Lettre à Marie-France Vignéras du 10/2/1986. Œuvres. Collected papers. IV. 1985–1998. Springer-Verlag, Berlin, 2000.

[**Sag**] W. A. Stein et al, Sage Mathematics Software (Version 6.3), The Sage Development Team, `http://www.sagemath.org` (2015).

[**Sh1**] A. Shlapentokh, Rings of algebraic numbers in infinite extensions of $\mathbb{Q}$ and elliptic curves retaining their rank. *Archive for Mathematical Logic* **48** (2009) 77–114.

[**Sh2**] A. Shlapentokh, First order decidability and definability of integers in infinite algebraic extensions of rational numbers. Preprint `http://arxiv.org/abs/1307.0743`

[**TCF**] J. Tate, Global Class Field Theory. In: Algebraic Number Theory, Cassels and Fröhlich, eds. Thompson Book Co., Washington DC (1967) 162–203.

[**Win**] A. Wintner, On the prime number theorem. *Amer. J. Math.* **64** (1942) 320–326.

[**Wri**] D. Wright, Distribution of discriminants of abelian extensions. *Proc. London Math. Soc* **58** (1989) 17–50.

Department of Mathematics, Harvard University, Cambridge, MA 02138, USA
E-mail address: `mazur@math.harvard.edu`

Department of Mathematics, UC Irvine, Irvine, CA 92697, USA
E-mail address: `krubin@math.uci.edu`

Part 3. Appendix by Michael Larsen: Galois elements acting on ℓ-torsion points of abelian varieties

The goal of this appendix is the following theorem:

Theorem A.1. *Let A be a simple abelian variety defined over K, and suppose that $\mathcal{E} := \mathrm{End}_K(A) = \mathrm{End}_{\bar{K}}(A)$. There is a positive density set S of rational primes such that for every prime λ of $\mathcal{M}$ lying above S we have:*

(i) *there is a $\tau_0 \in G_{K^{\mathrm{ab}}}$ such that $A[\lambda]^{\langle\tau_0\rangle} = 0$,*
(ii) *there is a $\tau_1 \in G_{K^{\mathrm{ab}}}$ such that $A[\lambda]/(\tau_1 - 1)A[\lambda]$ is a simple $\mathcal{E}/\lambda$-module.*

The idea of the proof is as follows. For simplicity, let us assume $\mathrm{End}_{\bar{K}}(A) = \mathbb{Z}$ and further that K is "large enough". Let Γ_ℓ denote the image of $\mathrm{Gal}(\bar{K}/K)$ in $\mathrm{GL}_n(\mathbb{F}_\ell) = \mathrm{Aut}(A[\ell])$, where $n = 2\dim A$. Using results of Nori, Serre, and Faltings (see Proposition A.9 below), we can show that there exists an absolutely irreducible, closed, connected, reductive subgroup $G_\ell \subset \mathrm{GL}_n$ such that Γ_ℓ is a subgroup of $G_\ell(\mathbb{F}_\ell)$ of index $\leq C$, where C depends only on n.

Using Serre's theory of Frobenius tori, we can find a finite extension L over K such that if ℓ splits completely in L, then G_ℓ is a split group. The elements τ_0 and τ_1 which we seek lie in the derived group of G_K, so their images $\bar{\tau}_0$ and $\bar{\tau}_1$ in $\Gamma_\ell \subset \mathrm{Aut}(A[\ell])$ lie in $[\Gamma_\ell, \Gamma_\ell]$, i.e., in the group of $\mathbb{F}_\ell$-points of the derived group H_ℓ of G_ℓ, which is connected, split, and semisimple. Roughly, we want to show that $H_\ell(\mathbb{F}_\ell) \subset \mathrm{GL}_n(\mathbb{F}_\ell)$ has two elements which have 0 and 1 Jordan blocks of eigenvalue 1 respectively. Such elements need not exist in general. There exist split semisimple groups H_ℓ with absolutely irreducible representation V such that every element of $H_\ell(\mathbb{F}_\ell)$ has an invariant space of dimension ≥ 2 in V. For instance, H_ℓ can be a split semisimple group of rank ≥ 2 and V can be the adjoint representation.

We use a theorem of Pink [6] to rule out examples of this kind; from his result it is fairly easy to find elements for which 1 is not an eigenvalue. To get a 1-dimensional 1-eigenspace is still delicate, however, since V is self-dual and of even dimension, so the *multiplicity* of 1 as an eigenvalue is always even. In particular, a semisimple element cannot have a 1-dimensional 1-eigenspace. This makes it necessary to consider elements with non-trivial Jordan decomposition. The construction of such an element is given in Proposition A.6.

We begin with some estimates useful for guaranteeing the existence of sufficiently generic elements in maximal tori over large finite fields (i.e., elements whose eigenvalues do not satisfy specified multiplicative conditions).

Definition A.2. If k is a positive integer, a subset S of a free abelian group X is *k-bounded* if there exists a basis e_i of X such that each element of S is a linear combination of the e_i with coefficients in $[-k, k]$

Lemma A.3. *Suppose X is a finitely generated free abelian group, and S is a k-bounded linearly independent subset of X. Let Y be the span of S, and suppose Z is a subgroup of X containing Y with Z/Y finite. Then*

$$[Z : Y] \leq r!k^r$$

where $r := |S|$.

Proof. Without loss of generality we may suppose that $X = \mathbb{Z}^n$ (viewed as row vectors), and the basis with respect to which the coefficients of S are bounded by k is the standard one. Let $S = \{s_1, \ldots, s_r\}$, and let $\{z_1, \ldots, z_r\}$ be a basis of Z. Let

M_Y (resp., M_Z) be the matrix whose i-th row is s_i (resp., z_i). Let N be the $r \times r$ matrix representing the s_i in terms of the z_i, i.e., such that $NM_Z = M_Y$. Then $[Z : Y] = \det(N)$, and $\det(N)$ divides every $r \times r$ minor of M_Y. Since the entries of M_Y are bounded by k, these minors are bounded by $r!k^r$. At least one of them is nonzero, so the lemma follows. □

If T is an algebraic torus then $X^*(T)$ will denote the character group $\mathrm{Hom}(T, \mathbb{G}_m)$.

Lemma A.4. *If T is an r-dimensional split torus over $\mathbb{F}_\ell$ and $\{\chi_1, \chi_2\}$ is a k-bounded subset of $X^*(T)$ that generates a rank-2 subgroup, then for all $a_1, a_2 \in \mathbb{F}_\ell^\times$, we have*

$$|\{t \in T(\mathbb{F}_\ell) \mid \chi_1(t) = a_1,\ \chi_2(t) = a_2\}| \le 2k^2(\ell - 1)^{r-2}.$$

Proof. In the natural bijection between closed subgroups of T and subgroups of $X^*(T)$, we have that $\mathcal{T} := \ker \chi_1 \cap \ker \chi_2 \subset T$ corresponds to $\mathcal{X} := \langle \chi_1, \chi_2 \rangle \subset X^*(T)$, and the identity component $\mathcal{T}^\circ$ corresponds to $\mathcal{X}^\circ := (\mathcal{X} \otimes \mathbb{Q}) \cap X^*(T)$. As $\mathcal{X}$ has rank 2, we have $\dim \mathcal{T} = \dim \mathcal{T}^\circ = r - 2$, and

$$[\mathcal{T} : \mathcal{T}^\circ] = |\mathcal{X}^\circ / \mathcal{X}|.$$

As χ_1 and χ_2 are k-bounded, Lemma A.3 shows that this index is bounded above by $2k^2$, so $\{t \in T(\mathbb{F}_\ell) \mid \chi_1(t) = a_1,\ \chi_2(t) = a_2\}$ (which is either empty or a coset of $\mathcal{T}(\mathbb{F}_\ell)$) satisfies

$$|\{t \in T(\mathbb{F}_\ell) \mid \chi_1(t) = a_1,\ \chi_2(t) = a_2\}| \le |\mathcal{T}(\mathbb{F}_\ell)| \le 2k^2(\ell - 1)^{r-2}.$$

□

Lemma A.5. *If G is a semisimple group over a field K, (ρ, V) is a representation of G, and there exists $g \in G(K)$ such that $V^{\langle \rho(g) \rangle} = (0)$, then 0 does not appear as a weight of ρ.*

Proof. Without loss of generality we may assume K is algebraically closed. Let T be a maximal torus. If 0 appears as a weight of ρ, then $\rho(t)$ has eigenvalue 1 for all $t \in T(K)$. The condition of having eigenvalue 1 is conjugation-invariant on G, and the union of all conjugates of T includes all regular semisimple elements of G and is therefore Zariski-dense. Thus, $\rho(g)$ has eigenvalue 1 for all $g \in G(K)$, and it follows that $V^{\langle \rho(g) \rangle}$ is non-trivial. □

The following proposition gives the key construction of this appendix. Given a semisimple group $G/\mathbb{F}_\ell$ and an absolutely irreducible n-dimensional representation V of G defined over $\mathbb{F}_\ell$, in favorable situations we prove that there exists an element of $G(\mathbb{F}_\ell)$ that fixes a subspace of V of dimension 1. If the representation is not self-dual, we can use a semisimple element which fixes the highest weight space W_η and acts non-trivially on all other weight spaces. In the self-dual case, we find an element whose unique Jordan block with eigenvalue 1 has size 2, acting on $W_\eta \oplus W_{-\eta}$.

Proposition A.6. *For every positive integer n, there exists a positive integer N such that if ℓ is a prime congruent to 1 (mod N), G is a simply connected, split semisimple algebraic group over $\mathbb{F}_\ell$, and $\rho\colon G \to \mathrm{GL}_n$ is an absolutely irreducible representation such that $(\mathbb{F}_\ell^n)^{\langle \rho(g_0) \rangle} = 0$ for some $g_0 \in G(\mathbb{F}_\ell)$, then there exists $g_1 \in G(\mathbb{F}_\ell)$ such that*

$$\dim(\mathbb{F}_\ell^n)^{\langle \rho(g_1) \rangle} = 1.$$

Proof. By replacing N by a suitable multiple, the condition $\ell \equiv 1 \pmod N$ can be made to imply ℓ sufficiently large, so henceforth we assume ℓ is as large as needed.

We fix a Borel subgroup B of G and a maximal split torus T of B, both defined over $\mathbb{F}_\ell$. Every dominant weight η of T defines an irreducible representation of $G_{\bar{\mathbb{F}}_\ell}$, and all irreducible representations of $G_{\bar{\mathbb{F}}_\ell}$ arise in this way. By a theorem of Steinberg [11, 13.1], every irreducible $\bar{\mathbb{F}}_\ell$-representation of $G(\mathbb{F}_\ell)$ is obtained from a unique irreducible representation $\tilde{\rho}$ of the algebraic group $G_{\bar{\mathbb{F}}_\ell}$ whose highest weight $\eta = a_1\varpi_1 + \cdots + a_r\varpi_r$ can be expressed as a linear combination of fundamental weights with coefficients $0 \le a_i < \ell$. By [13, 1.30], this implies $\max a_i \le n$. Thus, the set Σ of weights of $\tilde{\rho}$ (with respect to T) is k-bounded for some constant k depending only on n and the root system of G (and hence, in fact, on n alone). By Lemma A.5, $0 \notin \Sigma$, so if $|m| > k$ and $\chi \in X^*(T)$, then $m\chi \notin \Sigma$. We assume that N is divisible by $k!$. We also assume that for all $\chi_1, \chi_2 \in \Sigma$ distinct, N does not divide $\chi_1 - \chi_2$. This guarantees that for $\chi \in \Sigma$

$$\{v \in \mathbb{F}_\ell^n \mid \rho(t)(v) = \chi(t)v \ \forall t \in T(\mathbb{F}_\ell)\}$$

is the χ-weight space of the algebraic group T.

For each $\chi \in X^*(T)$, we denote by T_χ the kernel of χ. Let d be the largest integer such that $\eta \in dX^*(T)$, and let $\mu := \eta/d$. Thus, μ induces a surjective map $T(\mathbb{F}_\ell) \to \mathbb{F}_\ell^\times$. As $d \le k$, we have $\ell \equiv 1 \pmod d$, so we can fix an element $e \in \mathbb{F}_\ell^\times$ of order d. Let $T_{\mu,e}$ denote the translate of T_μ consisting of elements $t \in T$ such that $\mu(t) = e$. The number of $\mathbb{F}_\ell$-points of $T_{\mu,e}$ is $(\ell-1)^{r-1}$. For $\chi \in \Sigma$ not a multiple of μ, the intersection $T_{\mu,e}(\mathbb{F}_\ell) \cap T_\chi(\mathbb{F}_\ell)$ has at most $2k^2(\ell-1)^{r-2}$ elements by Lemma A.4. For $\chi \in \Sigma$ a non-trivial multiple of μ other than $\pm\eta$, $T_{\mu,e}(\mathbb{F}_\ell) \cap T_\chi(\mathbb{F}_\ell)$ is empty. For ℓ sufficiently large, therefore,

$$T_{\mu,e}(\mathbb{F}_\ell) \setminus \bigcup_{\chi \in \Sigma \setminus \{\pm\eta\}} T_\chi(\mathbb{F}_\ell)$$

has an element t. Thus $\chi(t) \ne 1$ for all $\chi \in \Sigma$ except for $\pm\eta$, and $\eta(t) = 1$.

If $-\eta \notin \Sigma$, then setting $g_1 = t$, we are done. We assume, therefore that $-\eta \in \Sigma$, so in particular ρ is self-dual. If $W_\eta \subset \mathbb{F}_\ell^n$ denotes the η-weight space of T (or equivalently $T(\mathbb{F}_\ell)$), there exists a unique projection $\pi_\eta \colon \mathbb{F}_\ell^n \to W_\eta$ which respects the $T(\mathbb{F}_\ell)$-action and fixes W_η pointwise. Let U be the unipotent radical of B. If there exists $u \in U(\mathbb{F}_\ell)$ such that $\pi_\eta(\rho(u)w) \ne 0$ for some $w \in W_{-\eta}$ then setting $g_1 = tu$, we are done.

We assume henceforth that $N \ge 3(h-1)$ where h denotes the Coxeter number of G. An upper bound for h is determined by n. By the Jacobson-Morozov theorem in positive characteristic (cf. [7]), $\ell > N$ implies that there exists a *principal* homomorphism $\phi \colon \mathrm{SL}_2 \to G$. Conjugating, we may assume that the Borel subgroup B_{SL_2} lies in B and the maximal torus $T_{\mathrm{SL}_2} \subset \mathrm{SL}_2$ lies in T. We identify $X^*(T_{\mathrm{SL}_2})$ with $\mathbb{Z}$ so that positive weights of T restrict to positive weights of T_{SL_2}. By definition of principal homomorphism, the restriction of every simple root of G with respect to T to T_{SL_2} equals 2. Thus, the restriction j of η to T_{SL_2} is strictly larger than the restriction of any other element of Σ to T_{SL_2}, and $-j$ is the smallest value obtained by restricting elements of S to T_{SL_2}. The restriction of V to SL_2 is semisimple when ℓ is large by [4] (see also [3]), and by definition of j, $V|_{\mathrm{SL}_2}$ is a direct sum of one representation V_1 of SL_2 of degree $j+1$ and other representations of strictly smaller degrees. The weight spaces W_η and $W_{-\eta}$ are contained in V_1. It suffices to find u in $B_{\mathrm{SL}_2}(\mathbb{F}_\ell) \cap U(\mathbb{F}_\ell)$ and $w \in W_{-\eta} \subset V_1$ such that $\pi_\eta(\rho(u)w) \ne 0$.

As

$$\mathrm{Sym}^{j-1}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & j-1 & \binom{j-1}{2} & \cdots & 1\\ 0 & 1 & j-2 & \cdots & 1\\ 0 & 0 & 1 & \cdots & 1\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \cdots & 1\end{pmatrix},$$

any non-trivial u and w will do. □

Lemma A.7. *Fix a positive integer B. Suppose H is a connected reductive algebraic group over $\mathbb{F}_\ell$, and Γ is a subgroup of $H(\mathbb{F}_\ell)$ of index $\le B$. Let $\tilde{H}$ denote the universal covering group of the derived group of H, and $\pi_\ell : \tilde{H}(\mathbb{F}_\ell) \to H(\mathbb{F}_\ell)$ the covering map. If ℓ is sufficiently large in terms of B, then the derived group of Γ contains the image of π_ℓ.*

Proof. Let $\tilde{\Gamma} = \pi_\ell^{-1}(\Gamma) \subset \tilde{H}(\mathbb{F}_\ell)$, so $[\tilde{H}(\mathbb{F}_\ell) : \tilde{\Gamma}] \le B$. If ℓ is sufficiently large, then the quotient of $\tilde{H}(\mathbb{F}_\ell)$ by its center is a product Π of finite simple groups ([12, Theorems 5 and 34]), and $\tilde{H}(\mathbb{F}_\ell)$ is a universal central extension of this quotient ([12, Theorems 10 and 34]). Moreover, each factor of Π is a quotient group of $\tilde{H}(\mathbb{F}_\ell)$, is therefore generated by elements of ℓ-power order ([11, Theorem 12.4]), and therefore has order at least ℓ. If $\tilde{\Gamma}$ is a proper subgroup of $\tilde{H}(\mathbb{F}_\ell)$, then its image in Π is a proper subgroup of index $\le B$, which is impossible if $\ell > B!$. Thus if ℓ is sufficiently large, we conclude that $\tilde{\Gamma} = \tilde{H}(\mathbb{F}_\ell)$, and so $\pi_\ell(\tilde{H}(\mathbb{F}_\ell)) \subset \Gamma$ and (since $\tilde{H}(\mathbb{F}_\ell)$ is perfect),

$$\pi_\ell(\tilde{H}(\mathbb{F}_\ell)) = [\pi_\ell(\tilde{H}(\mathbb{F}_\ell)), \pi_\ell(\tilde{H}(\mathbb{F}_\ell))] \subset [\Gamma, \Gamma].$$

□

Fix a simple abelian variety A defined over a number field K. Let $\mathcal{E} := \mathrm{End}_K(A)$, let $\mathcal{R}$ denote the center of $\mathcal{E}$, and $\mathcal{M} = \mathcal{R} \otimes \mathbb{Q}$. Since A is simple, $\mathcal{M}$ is a number field and $\mathcal{R}$ is an order in $\mathcal{M}$. Suppose ℓ is a rational prime not dividing the discriminant of $\mathcal{R}$, such that ℓ splits completely in $\mathcal{M}/\mathbb{Q}$, and λ is a prime of $\mathcal{M}$ above ℓ. We will abbreviate

$$\mathcal{M}_\lambda\mathcal{E} := \mathcal{E} \otimes_{\mathcal{R}} \mathcal{M}_\lambda, \quad \mathcal{E}/\lambda := \mathcal{E} \otimes_{\mathcal{R}} \mathcal{R}/\lambda.$$

We assume from now on that K is large enough so that

$$\mathcal{E} := \mathrm{End}_K(A) = \mathrm{End}_{\bar{K}}(A)$$

and ℓ is large enough (Proposition 9.1) so that

$$\mathcal{M}_\lambda\mathcal{E} \cong M_d(\mathbb{Q}_\ell) \quad \text{and} \quad \mathcal{E}/\lambda \cong M_d(\mathbb{F}_\ell)$$

where for a field F, $M_d(F)$ denote the simple F-algebra of $d \times d$ matrices with entries in F. Let $V_\lambda(A)$ denote the λ-adic Tate module

$$V_\lambda(A) := (\varprojlim A[\lambda^k]) \otimes_{\mathcal{R}_\lambda} \mathcal{M}_\lambda,$$

let W_λ (resp., $\bar{W}_\lambda$) denote the unique (up to isomorphism) simple $\mathcal{M}_\lambda\mathcal{E}$-module (resp., $\mathcal{E}/\lambda$-module), and define

$$X_\lambda = \mathrm{Hom}_{\mathcal{M}_\lambda\mathcal{E}}(W_\lambda, V_\lambda(A)), \quad \bar{X}_\lambda = \mathrm{Hom}_{\mathcal{E}/\lambda}(\bar{W}_\lambda, A[\lambda]).$$

Then X_λ is a $\mathbb{Q}_\ell$-vector space of dimension n, and $\bar{X}_\lambda$ is an $\mathbb{F}_\ell$-vector space of dimension n, where

$$n := \mathrm{length}_{\mathcal{M}_\lambda \mathcal{E}} V_\lambda(A) = \mathrm{length}_{\mathcal{E}/\lambda} A[\lambda] = \frac{2\dim(A)}{d}.$$

There is a natural Galois action on X_λ and $\bar{X}_\lambda$, where we let G_K act trivially on W_λ and $\bar{W}_\lambda$. Denote by

$$\rho_\lambda : G_K \to \mathrm{Aut}(X_\lambda) \cong \mathrm{GL}_n(\mathbb{Q}_\ell), \quad \bar{\rho}_\lambda : G_K \to \mathrm{Aut}(\bar{X}_\lambda) \cong \mathrm{GL}_n(\mathbb{F}_\ell),$$

the corresponding representations.

Lemma A.8. *There are natural G_K-equivariant isomorphisms*

$$\mathrm{End}_{\mathbb{Q}_\ell}(X_\lambda) \cong \mathrm{End}_{\mathcal{M}_\lambda \mathcal{E}}(V_\lambda(A)), \quad \mathrm{End}_{\mathbb{F}_\ell}(\bar{X}_\lambda) \cong \mathrm{End}_{\mathcal{E}/\lambda}(A[\lambda]).$$

Proof. The map $\mathrm{End}_{\mathcal{M}_\lambda \mathcal{E}}(V_\lambda(A)) \times X_\lambda \to X_\lambda$ given by $(f, \varphi) \mapsto f \circ \varphi$ induces an injective homomorphism $\mathrm{End}_{\mathcal{M}_\lambda \mathcal{E}}(V_\lambda(A)) \to \mathrm{End}_{\mathbb{Q}_\ell}(X_\lambda)$. Since both spaces have $\mathbb{Q}_\ell$-dimension n^2, this map is an isomorphism. The proof of the second isomorphism is the same. $\square$

Let $G_\lambda \subset \mathrm{Aut}(X_\lambda)$ be the Zariski closure of the image $\rho_\lambda(G_K)$.

Proposition A.9. *Replacing K by a finite extension if necessary, for all ℓ sufficiently large we have:*

- (i) *G_λ is a connected, reductive, absolutely irreducible subgroup of $\mathrm{Aut}(X_\lambda)$, with center equal to the group of scalars $\mathbb{G}_m$,*
- (ii) *there is a connected, reductive, absolutely irreducible subgroup H_λ of $\mathrm{Aut}(\bar{X}_\lambda)$, with center equal to the group of scalars $\mathbb{G}_m$, such that*
  - (a) *the image $\bar{\rho}_\lambda(G_K)$ is contained in $H_\lambda(\mathbb{F}_\ell)$ with index bounded independently of λ and ℓ,*
  - (b) *the rank of H_λ is equal to the rank of G_λ (and is independent of λ and ℓ).*

Proof. Using Lemma A.8, we can identify G_λ with the Zariski closure of the image of G_K in $\mathrm{Aut}_{\mathcal{M}_\lambda \mathcal{E}}(V_\lambda(A)) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\lambda(A))$. The fact that G_λ is reductive and connected (after possibly increasing K) now follows from a combination of Faltings' theorem and a theorem of Serre [9, §2.2].

It also follows from Faltings' theorem that the commutant of G_λ in $\mathrm{Aut}_{\mathbb{Q}_\ell}(V_\lambda(A))$ is $\mathcal{M}_\lambda \mathcal{E}$, and hence the commutant of G_λ in $\mathrm{End}_{\mathcal{M}_\lambda \mathcal{E}}(V_\lambda(A)) = \mathrm{End}(X_\lambda)$ is the center of $\mathcal{M}_\lambda \mathcal{E}$, which is $\mathbb{Q}_\ell$. This shows that G_λ is absolutely irreducible, and since G_λ contains the scalar matrices [1] this completes the proof of (i).

The proof of (ii) is similar. The definition of the connected reductive group $H_\lambda \subset \mathrm{Aut}_{\mathcal{E}/\lambda}(A[\lambda]) \subset \mathrm{Aut}_{\mathbb{F}_\ell}(A[\lambda])$ is given by Serre in [10, §3]. The fact that H_λ is absolutely irreducible, and that the center of H_λ is $\mathbb{G}_m$, follows as for (i): Remark 4 at the end of [10, §3] shows that the commutant of H_λ in $\mathrm{Aut}_{\mathbb{F}_\ell}(A[\lambda])$ is $\mathcal{E}/\lambda$, so the commutant of H_λ in $\mathrm{Aut}_{\mathcal{E}/\lambda}(A[\lambda]) = \mathrm{Aut}(\bar{X}_\lambda)$ is the center of $\mathcal{E}/\lambda$, which is $\mathbb{F}_\ell$. That H_λ containes the homotheties is [10, §5].

Théorèmes 1 and 2 of [10] give (a) and (b) of (ii). $\square$

From now on suppose that K and ℓ are large enough to satisfy Proposition A.9, and let H_λ be as in Proposition A.9(ii). Let $\tilde{G}_\lambda$ and $\tilde{H}_\lambda$ denote the simply connected cover of the derived group of G_λ and H_λ, respectively.

Lemma A.10. *There is a positive integer r, independent of λ and ℓ, such that for every $h \in H_\lambda(\mathbb{F}_\ell)$, we have $h^{nr}/\det(h)^r \in \operatorname{image}(\tilde{H}_\lambda(\mathbb{F}_\ell) \to H_\lambda(\mathbb{F}_\ell))$.*

Proof. By Proposition A.9(i), we have $H_\lambda = \mathbb{G}_m \cdot \mathrm{S}H_\lambda$ where $\mathrm{S}H_\lambda$, the derived group of H_λ, is $H_\lambda \cap \mathrm{SL}_n(\tilde{X}_\lambda)$. We have $h^{nr}/\det(h)^r \in \mathrm{S}H_\lambda(\mathbb{F}_\ell)$ for every r, so to prove the lemma we need only show that the cokernel of $\pi : \tilde{H}_\lambda(\mathbb{F}_\ell) \to \mathrm{S}H_\lambda(\mathbb{F}_\ell)$ is bounded by a constant depending only on n.

It follows from Lang's theorem (cf. [2, Proposition 16.8]) that the kernel and cokernel of π have the same order. The kernel of π is a subgroup of the center of $\tilde{H}_\lambda$, and the order of the center of a semisimple group can be bounded only in terms of its root datum. (Indeed, this can be checked over an algebraically closed field; the center lies in the centralizer T of every maximal torus T and in the point stabilizer $\ker \alpha \subset T$ of every root space U_α of T.)

□

Lemma A.11. *The representation of $\tilde{G}_\lambda$ on X_λ does not have 0 as a weight.*

Proof. By [6, Corollary 5.11], the highest weight of G_λ acting on X_λ is minuscule; i.e., the weights form an orbit under the Weyl group. Any weight which is trivial on the derived group of G_λ is fixed by the Weyl group of G_λ; as the representation X_λ is faithful, no such weight can occur. Regarding X_λ as a representation of $\tilde{G}_\lambda$, it factors through G_λ, so again, there can be no zero weight. □

Proposition A.12. *Suppose r is a positive integer. If ℓ is sufficiently large then there is a prime $v \nmid \ell$ of K such that (writing Fr_v for a Frobenius automorphism at v)*

(i) *A has good reduction at v and at all primes above ℓ,*
(ii) *$\rho_\lambda(\mathrm{Fr}_v) \in G_\lambda(\mathbb{Q}_\ell)$ generates a Zariski dense subgroup of the unique maximal torus to which it belongs,*
(iii) $\det(\rho_\lambda(\mathrm{Fr}_v^{nr})/\det(\rho_\lambda(\mathrm{Fr}_v^{r})) - 1) \neq 0$.

Proof. By Proposition A.9(i), G_λ contains all scalar matrices. It follows from Lemma A.11 (as in the proof of Lemma A.10) that the condition that $\det(g)^r$ is an eigenvalue of g^{rn} does not hold on all of $\tilde{G}_\lambda$, so it does not hold on all of G_λ, so it holds on a proper closed subset of G_λ.

By [8], there is a dense open subset U of G_λ such that $\rho_\lambda(\mathrm{Fr}_v) \in U(\mathbb{Q}_\ell)$ implies that $\rho_\lambda(\mathrm{Fr}_v)$ generates a Zariski-dense subgroup of the unique maximal torus to which it belongs. By Chebotarev density, there exists v such that $g := \rho_\lambda(\mathrm{Fr}_v)$ satisfies this condition together with the condition that $\det(g)^r$ is not an eigenvalue of g^{rn}. □

Fix $\lambda_0 \mid \ell_0$ and v satisfying Proposition A.12, and define

$$g_0 := \rho_{\lambda_0}(\mathrm{Fr}_v) \in \mathrm{Aut}(X_{\lambda_0}).$$

Let $P_v(x) \in \mathbb{Z}[x]$ be the characteristic polynomial of g_0, which is independent of the choice of ℓ_0 and λ_0, and let L denote the splitting field of $P_v(x)$ over $\mathbb{Q}$. Let Σ denote the set of distinct weights of G_{λ_0} with respect to the (unique, maximal) torus containing g_0.

Fix r as in Proposition A.10. Without loss of generality we may assume that r is divisible by $(n-1)!$. Let $\gamma_0 := g_0^{nr}/\det(g_0^r)$, and define

$$\mu := \prod_{\chi\in\Sigma}(\chi(\gamma_0)-1)\prod_{\chi,\chi'\in\Sigma,\chi\neq\chi'}(\chi(\gamma_0)-\chi'(\gamma_0))$$

Lemma A.13. *We have $\mu \neq 0$.*

Proof. By Proposition A.12(iii), 1 is not an eigenvalue of γ_0, so $\chi(\gamma_0)\neq 1$ for every weight χ. Since $\rho_{\lambda_0}(\mathrm{Fr}_v)$ generates a Zariski dense subgroup of the maximal torus that contains it, so does Fr_v^{nr}. Hence if $\chi\neq\chi'\in\Sigma$, then $\chi(\rho_{\lambda_0}(\mathrm{Fr}_v^{nr}))\neq\chi'(\rho_{\lambda_0}(\mathrm{Fr}_v^{nr}))$ and $\chi(\gamma_0)\neq\chi'(\gamma_0)$. □

Proposition A.14. *Suppose ℓ splits completely in $L/\mathbb{Q}$ and ℓ does not divide $\mathbf{N}_{L/\mathbb{Q}}\mu$. Then $\tilde{H}_\lambda$ is split, and there is an η_0 in the image of the map $\tilde{H}_\lambda(\mathbb{F}_\ell)\to H_\lambda(\mathbb{F}_\ell)$ such that $(\bar{X}_\lambda)^{\langle\eta_0\rangle}=0$.*

Proof. Let $h_0=\bar{\rho}_\lambda(\mathrm{Fr}_v)\in H_\lambda(\mathbb{F}_\ell)$, and let $\bar{P}_v(x)\in\mathbb{F}_\ell[x]$ be the characteristic polynomial of h_0. Then $\bar{P}_v(x)$ is the reduction of $P_v(x)$ modulo λ.

Let $h_0=su$ be the Jordan decomposition of h_0, with s semisimple and u unipotent, and Z a maximal torus of H_λ such that $s\in Z(\mathbb{F}_\ell)$. Since ℓ splits completely in L/K, all roots of $\bar{P}(x)$ lie in $\mathbb{F}_\ell$, and distinct weights correspond to distinct eigenvalues. If $\bar{\chi}$, $\bar{\chi}'$ are weights of H_λ with respect to Z, and $\mathrm{Fr}_\lambda(\bar{\chi})=\bar{\chi}'\neq\bar{\chi}$, then $\bar{\chi}(s)\in\mathbb{F}_\ell$ implies that $\bar{\chi}(s)=\bar{\chi}'(s)$, contrary to assumption. Thus Fr_λ acts trivially on the weights of H_λ. It follows that Fr_λ acts trivially on Z, which means H_λ is split, and therefore $\tilde{H}_\lambda$ is split.

Let $\eta_0=h_0^{nr}/\det(h_0^r)$, so η_0 is in the image of $\tilde{H}_\lambda(\mathbb{F}_\ell)\to H_\lambda(\mathbb{F}_\ell)$ by Lemma A.10(ii). The eigenvalues of γ_0 are the values $\chi(\gamma_0)$ for $\chi\in\Sigma$, and the eigenvalues of η_0 are the reductions of those values modulo λ. By assumption none of those values reduce to 1, so 1 is not an eigenvalue of η_0 and $(\bar{X}_\lambda)^{\langle\eta_0\rangle}=0$. □

Proposition A.15. *The representation $\pi_\ell:\tilde{H}(\mathbb{F}_\ell)\to H(\mathbb{F}_\ell)\subset\mathrm{GL}_n(\mathbb{F}_\ell)$ is absolutely irreducible.*

Proof. By Proposition A.9(ii), the subgroup $H_\lambda(\mathbb{F}_\ell)\subset\mathrm{GL}_n(\mathbb{F}_\ell)$ is absolutely irreducible. By functoriality, the image $\pi_\ell(\tilde{H}_\lambda(\mathbb{F}_\ell))$ is a normal subgroup of $H_\lambda(\mathbb{F}_\ell)$. If π_ℓ is not absolutely irreducible, then there is a decomposition

$$\bar{\mathbb{F}}_\ell^n=\bigoplus Z_i$$

where each Z_i is an irreducible $\pi_\ell(\tilde{H}_\lambda(\mathbb{F}_\ell))$-module and the Z_i are permuted transitively by the action of $H_\lambda(\mathbb{F}_\ell)/\pi_\ell(\tilde{H}_\lambda(\mathbb{F}_\ell))$. The number of irreducible summands is bounded by the dimension n, so for every $g\in H_\lambda(\mathbb{F}_\ell)$, every eigenvalue of $g^{n!}$ occurs with multiplicity greater than 1.

Since g_0 generates a Zariski dense subgroup of the unique maximal torus in G_{λ_0} that contains it, so does $g_0^{n!}$. It follows that the eigenvalue of $g_0^{n!}$ corresponding to the highest weight has multiplicity 1. Since $\ell\nmid\mu$, the eigenvalues of $g_0^{n!}$ are distinct modulo λ, so one of the eigenvalues of $\bar{\rho}_\lambda(\mathrm{Fr}_v^{n!})$ has multiplicity 1. This contradiction shows that π_ℓ is absolutely irreducible. □

Corollary A.16. *If ℓ is sufficiently large then $A[\lambda]$ is an irreducible $\mathcal{E}[G_K]$-module.*

Proof. By Lemma A.7 applied with $H := H_\lambda$ and $\Gamma := \bar{\rho}_\lambda(G_K)$, and Proposition A.9(ii)(a), the image of G_K in $H_\lambda(\mathbb{F}_\ell)$ contains the image of $\tilde{H}_\lambda(\mathbb{F}_\ell)$. By Proposition A.15 and Lemma A.8 the latter is an irreducible subgroup of $\mathrm{Aut}(\bar{X}_\lambda) = \mathrm{Aut}_{\mathcal{E}/\lambda}(A[\lambda])$. □

We can now prove Theorem A.1.

Proof. Since $\mathrm{End}_K(A) = \mathrm{End}_{\bar{K}}(A)$, we have that A is absolutely simple and increasing K does not change $\mathcal{E}$. Thus it suffices to prove the theorem with K replaced by a finite extension, if necessary, so we may assume that K and ℓ satisfy Proposition A.9.

Suppose now that ℓ splits completely in $\mathcal{M}$ and in the number field L defined before Lemma A.13, and that $\ell \equiv 1 \pmod{N}$ where N is as in Proposition A.6. We will apply Proposition A.6 with $G = \tilde{H}_\lambda$, and the representation $\rho = \pi_\ell : \tilde{H}_\lambda \to H_\lambda \subset \mathrm{GL}_n$. By Proposition A.14, $\tilde{H}_\lambda$ is split and there is an $\eta_0 \in \tilde{H}_\lambda(\mathbb{F}_\ell)$ such that $(\bar{X}_\lambda)^{\langle \pi_\ell(\eta_0)\rangle} = 0$. By Proposition A.15, π_ℓ is absolutely irreducible. Thus we can apply Proposition A.6 to conclude that there is an $\eta_1 \in \tilde{H}_\lambda(\mathbb{F}_\ell)$ such that $\dim_{\mathbb{F}_\ell}(\bar{X}_\lambda)^{\langle \pi_\ell(\eta_1)\rangle} = 1$.

By Lemma A.7 (applied with $H := H_\lambda$ and $\Gamma := \bar{\rho}_\lambda(G_K)$) and Proposition A.9(ii)(a), for all sufficiently large ℓ we have $\pi_\ell(\tilde{H}_\lambda) \subset \bar{\rho}_\lambda(G_{K^{\mathrm{ab}}})$. In particular we can choose $\tau_i \in G_{K^{\mathrm{ab}}}$ so that $\bar{\rho}_\lambda(\tau_i) = \pi_\ell(\eta_i)$ for $i = 0, 1$. We have

$$(\bar{X}_\lambda)^{\langle \tau_i \rangle} = \mathrm{Hom}_{\mathcal{E}/\lambda}(\bar{W}_\lambda, A[\lambda])^{\langle \tau_i \rangle} = \mathrm{Hom}_{\mathcal{E}/\lambda}(\bar{W}_\lambda, A[\lambda]^{\langle \tau_i \rangle})$$

so

$$\mathrm{length}(A[\lambda]^{\langle \tau_i \rangle}) = \dim(\bar{X}_\lambda)^{\langle \tau_i \rangle} = i$$

for $i = 0, 1$. This proves the theorem. □

References

[1] Bogomolov, Fedor: Sur l'algébricité des représentations ℓ-adiques. *C. R. Acad. Sci. Paris Sér. A-B* **290** (1980) A701-?A703.

[2] Borel, Armand: Linear Algebraic Groups. *Graduate Texts in Math.* **126**, Springer-Verlag, Berlin (1991).

[3] Jantzen, Jens Carsten: Low-dimensional representations of reductive groups are semisimple. In: Algebraic groups and Lie groups, Austral. Math. Soc. Lect. Ser. **9**, Cambridge Univ. Press, Cambridge (1997) 255–266.

[4] Larsen, Michael: On the semisimplicity of low-dimensional representations of semisimple groups in characteristic p. *J. Algebra* **173** (1995), no. 2, 219–236.

[5] Larsen, M.; Pink, R.: On l-independence of algebraic monodromy groups in compatible systems of representations. *Invent. Math.* **107** (1992), no. 3, 603–636.

[6] Pink, Richard: l-adic algebraic monodromy groups, cocharacters, and the Mumford-Tate conjecture. *J. Reine Angew. Math.* **495** (1998), 187–237.

[7] Premet, Alexander: An analogue of the Jacobson-Morozov theorem for Lie algebras of reductive groups of good characteristics. *Trans. Amer. Math. Soc.* **347** (1995) 2961–2988.

[8] Serre, Jean-Pierre: Lettre à Ken Ribet du 1/1/1981. Œuvres. Collected papers. IV. 1985–1998. Springer-Verlag, Berlin, 2000.

[9] Serre, Jean-Pierre: Résumé des cours de 1984–1985. Œuvres. Collected papers. IV. 1985–1998. Springer-Verlag, Berlin, 2000.

[10] Serre, Jean-Pierre: Lettre à Marie-France Vignéras du 10/2/1986. Œuvres. Collected papers. IV. 1985–1998. Springer-Verlag, Berlin, 2000.

[11] Steinberg, Robert: Endomorphisms of linear algebraic groups. Memoirs of the American Mathematical Society, No. 80 American Mathematical Society, Providence, R.I. 1968 108 pp.

[12] Steinberg, Robert: Lectures on Chevalley Groups. Notes prepared by John Faulkner and Robert Wilson. Yale University, New Haven, Conn., 1968.

[13] Testerman, Donna M.: Irreducible subgroups of exceptional algebraic groups. *Mem. Amer. Math. Soc.* **75** (1988), no. 390.

Department of Mathematics, Indiana University, Bloomington, IN 47405, USA
E-mail address: larsen@math.indiana.edu