The Section Conjecture over Large Algebraic Extensions of Finitely Generated Fields

Moshe Jarden, Tel Aviv University
jarden@tauex.tau.ac.il
and
Sebastian Petersen, Universität Kassel
petersen@mathematik.uni-kassel.de

25 December 2020

Abstract

Let K be a finitely generated extension of its prime field and let $e \geq 2$ an integer. We prove the injectivity part of the section conjecture of Grothendieck for almost all $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(K)^e$ and for all smooth geometrically integral projective curves of genus ≥ 1 over the field $\tilde{K}(\boldsymbol{\sigma})$.

MR Classification: 12E30

1 Introduction

Algebraic number theory and Diophantine Geometry prove finiteness theorems for arithmetic and diophantine objects over global fields and, more generally, over **infinite finitely generated fields** K (over their prime fields). For example, the Mordell-Weil-Lang-Néron theorem says that for every abelian variety A over K, the abelian group $A(K)$ has finite rank. Another prominent example due to Faltings (formerly the "Mordell Conjecture") says in the case where $\mathrm{char}(K) = 0$ that $C(K)$ is finite for every geometrically integral curve C over K of genus ≥ 2. An analog of that result is due to Grauert-Manin in positive characteristic.

Of decisive importance from our point of view is Hilbert irreducibility theorem saying that if $f \in K[T, X]$ is irreducible, then there exist infinitely many $a \in K$ such that $f(a, X)$ is irreducible in $K[X]$.

For these reasons, we consider the finitely generated fields as "small". On the other end of the scale stand the algebraic closure $\tilde{K}$ of K. For this field, we have $\mathrm{rank}(A(\tilde{K})) = \infty$ for every non-zero abelian variety A over K, and $V(\tilde{K})$ is infinite for every integral variety V of positive dimension over $\tilde{K}$. Moreover, every non-constant polynomial in $\tilde{K}[X]$ has a zero, so $\tilde{K}$ is not Hilbertian. Similar statements hold for the maximal separable extension K_{sep} of K in $\tilde{K}$. Thus, one may say that $\tilde{K}$ and K_{sep} are "large fields".

"Just below" $\tilde{K}$ and $K_{\rm sep}$ there lie a big family of fields that are also large for a variety of reasons. To introduce these families we recall that the absolute Galois group $\mathrm{Gal}(K) = \mathrm{Gal}(K_{\rm sep}/K)$ of K is profinite. Hence, for each positive integer e, the group $\mathrm{Gal}(K)^e$ has a unique Haar measure μ such that $\mu(\mathrm{Gal}(K)^e) = 1$. For every $\boldsymbol{\sigma} := (\sigma_1, \ldots, \sigma_e)$, we write $K_{\rm sep}(\boldsymbol{\sigma})$ for the fixed field of $\sigma_1, \ldots, \sigma_e$ in $K_{\rm sep}$ and let $\tilde{K}(\boldsymbol{\sigma}) := K_{\rm sep}(\boldsymbol{\sigma})_{\rm ins}$ be the maximal purely inseparable extension of $K_{\rm sep}(\boldsymbol{\sigma})$ in $\tilde{K}$.

By [FrJ08, p. 380, Thm. 18.6.1], for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ (in the sense of the Haar measure μ) every geometrically integral variety over $K_{\rm sep}(\boldsymbol{\sigma})$ has a $K_{\rm sep}(\boldsymbol{\sigma})$-rational point. This means that $K_{\rm sep}(\boldsymbol{\sigma})$ is a **PAC-field** for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$. The same holds for $\tilde{K}(\boldsymbol{\sigma})$. By [FrJ08, p. 379, Thm. 18.5.6], for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, the group $\mathrm{Gal}(K_{\rm sep}(\boldsymbol{\sigma}))$ is isomorphic to the free profinite group $\hat{F}_e$ of e generators. In particular $K_{\rm sep}(\boldsymbol{\sigma})$ has only finitely many extensions of each degree d, so $K_{\rm sep}(\boldsymbol{\sigma})$ is definitely not Hilbertian.

For these reasons, Field Arithmetic considers almost all of the fields $K_{\rm sep}(\boldsymbol{\sigma})$ and $\tilde{K}(\boldsymbol{\sigma})$ as "large". It turns out, that concerning abelian varieties, there is a distinction between the cases $e = 1$ and $e \geq 2$. This is reflected by the following conjecture, where for an abelian variety A over a field M and for a prime number l, we set $A_l(M) = \{\mathbf{a} \in A(M) \mid l\mathbf{a} = \mathbf{o}\}$ and let $A_{\rm tor}(M) = \{\mathbf{a} \in A(M) \mid n\mathbf{a} = \mathbf{o}$ for some $n \in \mathbb{N}\}$.

Conjecture A [GeJ78, p. 260, Conjecture] Let K be a finitely generated field. Then, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ and for every non-zero abelian variety A over $\tilde{K}(\boldsymbol{\sigma})$, the following holds:
(a) If $e = 1$, then there are infinitely many prime numbers l with $A_l(\tilde{K}(\boldsymbol{\sigma})) \neq \mathbf{0}$. Thus, $A_{\rm tor}(\tilde{K}(\boldsymbol{\sigma}))$ is infinite.
(b) If $e \geq 2$, then $A_{\rm tor}(\tilde{K}(\boldsymbol{\sigma}))$ is finite.
(c) If $e \geq 1$, then for every prime number l, the group $A(\tilde{K}(\boldsymbol{\sigma}))$ contains only finitely many points of an l-power order.

Conjecture A is completely proved for elliptic curves in [GeJ78, Thm. 1.1]. Part C is proved in [JaJ01, Thm. 2.7]. Part B in the case where $\mathrm{char}(K) = 0$ is also proved in [JaJ01, Thm. 3.7]. Finally, Part A is proved for $\mathrm{char}(K) = 0$ in [JaP19, Thm. C]. Thus, in this respect, almost all of the fields $\tilde{K}(\boldsymbol{\sigma})$ with $e \geq 2$ are "not so large" as almost all of the fields $\tilde{K}(\boldsymbol{\sigma})$ with $e = 1$.

Goal of the present article. We enhance the above given information about almost all the fields $\tilde{K}(\boldsymbol{\sigma})$ with an injectivity result concerning the "section conjecture" for abelian varieties over those fields in the case when $e \geq 2$.

To this end let X be a smooth geometrically integral variety over a field M with geometric generic point $\bar{\mathbf{x}}$. We choose a geometric generic point $\bar{\mathbf{x}}_{\rm sep}$ of $X_{M_{\rm sep}}$ that lies over $\bar{\mathbf{x}}$. Then, we consider the short exact sequence

$$\mathbf{1} \longrightarrow \pi_1(X_{M_{\rm sep}}, \bar{\mathbf{x}}_{\rm sep}) \longrightarrow \pi_1(X, \bar{\mathbf{x}}) \xrightarrow{\rho} \mathrm{Gal}(M) \longrightarrow \mathbf{1}, \qquad (1) \quad \{\texttt{STIx}\}$$

where $\mathrm{Gal}(M) = \mathrm{Gal}(M_{\rm sep}/M)$ is the absolute Galois group of M, $\pi_1(X, \bar{\mathbf{x}})$ (resp. $\pi_1(X_{M_{\rm sep}}, \bar{\mathbf{x}}_{\rm sep})$) is the fundamental group of X (resp. of $X_{M_{\rm sep}}$) with base point $\bar{\mathbf{x}}$ (resp. $\bar{\mathbf{x}}_{\mathrm{sep}}$), and ρ is the corresponding restriction map (Remark 6.2). Every point $\mathbf{x} \in X(M)$ gives rise to a group theoretic section of ρ which is unique up to $\pi_1(X_{M_{\mathrm{sep}}}, \bar{\mathbf{x}}_{\mathrm{sep}})$-conjugacy (Remark 6.3). We denote the $\pi_1(X_{M_{\mathrm{sep}}}, \bar{\mathbf{x}}_{\mathrm{sep}})$-conjugacy class of that section by $\kappa_{X/M}(\mathbf{x})$ and let $\mathcal{S}_{X/M}$ be the set of all group theoretic sections of ρ up to $\pi_1(X_{M_{\mathrm{sep}}}, \bar{\mathbf{x}}_{\mathrm{sep}})$-conjugacy.

Grothendieck's renowned **section conjecture** says that the **profinite Kummer map**

$$\kappa_{X/M}\colon X(M) \to \mathcal{S}_{X/M} \tag{2}$$ {GRTk}

is bijective if M is a finitely generated extension of $\mathbb{Q}$ and X is a smooth geometrically integral projective curve over M of genus at least 2.

Grothendieck stated his conjecture in a letter to Faltings sent in 1983 [Sti13, p. xiv, 2nd paragraph]. In that letter he mentions that the map $\kappa_{X/M}$ is injective but leaves open the question of its surjectivity.

One may find a proof of the injectivity of $\kappa_{X/M}$ in [Sti13, p. 73, Prop. 73]. To this end we may assume that $X(M)$ is non-empty, otherwise $\kappa_{X/M}$ is trivially injective. Thus, X can be embedded into its Jacobian J. Then, one uses the Mordell-Weil theorem saying that for every finite extension M' of M, the abelian group $J(M')$ is finitely generated [Lan59, p. 71, Thm. 1] to conclude that

$$\bigcap_{n\in\mathbb{N}} nJ(M') = \mathbf{0}, \tag{3}$$ {morD}

and this implies the injectivity of $\kappa_{X/M}$.

Our main result concerns the large fields mentioned above:

Theorem B [Corollary 7.2 and Corollary 7.3]: Let K be an infinite finitely generated field and let $e \geq 2$ be an integer. Then, the following statements hold for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ and every finite extension M of $\tilde{K}(\boldsymbol{\sigma})$:

(a) For every non-zero abelian variety A over M and every non-empty smooth geometrically integral subvariety X of A, the profinite Kummer map $\kappa_{X/M}$ is injective, its image is dense (in an appropriate topology) but the map is not surjective.

(b) For all smooth geometrically integral projective curves C/M of genus ≥ 1 the profinite Kummer map $\kappa_{C/M}$ is injective with a dense image but the map is not surjective.

As mentioned above, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ the field $\tilde{K}(\boldsymbol{\sigma})$ is PAC, hence, by Ax-Roquette, so is every algebraic, in particular finite, extension M of $\tilde{K}(\boldsymbol{\sigma})$ [FrJ08, p. 196, Cor. 11.2.5]. By Koenigsmann-Stix, $\mathcal{S}_{X/M}$ is uncountable for every smooth geometrically integral variety X over M (Proposition 6.7). On the other hand, $X(M)$ is countable, because M is. Hence, a fortiori, we can not expect $\kappa_{X/M}$ in (2) to be bijective. That is, we can not expect the full section conjecture to hold over M.

In a letter to the authors [Sti20], Stix wrote that [Sti13, p. 73, Prop. 73] should have been stated only for varieties over perfect fields. In addition, Stix added that if A is an abelian variety over a perfect field M, then $\kappa_{A/M}\colon A(M) \to \mathcal{S}_{A/M}$ is injective if and only if $\mathrm{div}(A(M)) := \bigcap_{n\in\mathbb{N}} nA(M) = \mathbf{0}$ (Lemma 7.1).

The truth of the latter condition in our case along with additional vital information is stored in the following result.

Theorem C (Theorem 5.2): *Let K be an infinite finitely generated field and let $e \geq 2$. Then, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, all finite extensions M of $\tilde{K}(\boldsymbol{\sigma})$, and every abelian variety A over M we have:*

(a) *M is PAC,*

(b) $\mathrm{div}(A(M)) := \bigcap_{n\in\mathbb{N}} nA(M) = \mathbf{0}$,

(c) *$|A_{l^\infty}(M)| < \infty$ for every prime number l, and*

(d) *if $\mathrm{char}(K) = 0$, also $|A_{\mathrm{tor}}(M)| < \infty$.*

Here, for each prime number l and a positive integer i, we put $A_{l^i}(M) = \{\mathbf{a} \in A(M) \mid l^i\mathbf{a} = \mathbf{o}\}$ and $A_{l^\infty}(M) = \bigcup_{i=1}^{\infty} A_{l^i}(M)$.

By (a) of Theorem C, every smooth geometrically integral curve C over M has an M-rational point, so if its genus is ≥ 1, it can be embedded into its Jacobian. Thus, Statement (b) of Theorem B is a special case of Statement (a) of that theorem.

Using Weil's restriction of scalars for abelian varieties (Section 5), it suffices to prove Theorem C only in the case where $M = \tilde{K}(\boldsymbol{\sigma})$ and $\boldsymbol{\sigma}$ is chosen at random in $\mathrm{Gal}(K)^e$. In this case (c) and (d) are already proved in [JaJ01]. However, Statement (d) is not needed in the proof of Theorem B and we mentioned it only for completeness.

The proof of (b) of Theorem C depends on the following result:

Lemma D (Corollary 3.4): *Let A be a simple abelian variety of dimension g over an infinite finitely generated field K and let $\mathbf{p}$ be a point of $A(K)$ of infinite order. Then, $[K(\mathbf{p}_l) : K] = l^{2g}$ for each point $\mathbf{p}_l \in A(K_{\mathrm{sep}})$ with $l\mathbf{p}_l = \mathbf{p}$ and for all sufficiently large prime numbers l.*

In addition to Lemma D, the proof of (b) of Theorem C uses the obvious observation that $\lim_{l\to\infty}(1/l^{2g(e-1)}) = 0$ if $e \geq 2$. The failure of this observation for $e = 1$ forces us to prove Theorem C only for $e \geq 2$. See also Remark 4.5.

The proof of Corollary 3.4 depends on a result that Ribet proves in [Rib79] when $\mathrm{char}(K) = 0$ and that we generalize to the general case in Section 3. In addition, the proof of Corollary 3.4 uses the following heavy result:

Proposition E (Proposition 2.2): *The following statements hold for every non-zero abelian variety A over a finitely generated field K.*

(a) *$A(K)$ is a finitely generated abelian group.*

(b) *For almost all $l \in \mathbb{L}'$, the $\mathrm{Gal}(K)$-module A_l is semi-simple.*

(c) *For almost all $l \in \mathbb{L}'$, the natural homomorphism $\mathrm{End}_K(A) \otimes \mathbb{Z}/l\mathbb{Z} \to \mathrm{End}_{\mathbb{F}_l[\mathrm{Gal}(K)]}(A_l)$ is an isomorphism.*

(d) *$H^1(\mathrm{Gal}(K(A_l)/K), A_l) = 0$ for almost all $l \in \mathbb{L}'$.*

In this result, $\mathbb{L}' = \mathbb{L} \smallsetminus \{\mathrm{char}(K)\}$ with $\mathbb{L}$ being the set of all prime numbers. Then, "for almost all $l \in \mathbb{L}'$" means "for all but finitely many elements l in $\mathbb{L}'$".

Statement (a) of Proposition E is the Mordell-Weil-Lang-Néron Theorem. Statement (d) relies on Statement (b) and is due to Nori [Nor87]. Statements

(b) and (c) are part of the mod-l version of the l-adic Tate conjecture proved by Faltings. They were proved by Zarhin in the case where K is either a number field or finitely generated of positive characteristic. However, we have not been able to find a proof of that statement in the literature in the case where K is a finitely generated transcendental extension of $\mathbb{Q}$. We therefore supply full proofs of (b) and (c) in that case in Sections 1 and 2. Among others, we use the theorem of Faltings that assures a generalized Conjecture of Shafarevich for K (Proposition 2.3).

Additional results. Finally we mention two additional results. The first one deals with non-perfect fields M. If A is an abelian variety over a non-perfect field M, then the proof of Lemma 7.1 breaks down. It does not prove that the injectivity of $\kappa_{A/M}\colon A(M) \to \mathcal{S}_{A/M}$ follows from $\mathrm{div}(A(M)) = \mathbf{0}$. Instead, the injectivity of $\kappa_{A/M}$ follows from the injectivity of the map $\kappa_{A_{M_{\mathrm{ins}}}/M_{\mathrm{ins}}}\colon A(M_{\mathrm{ins}}) \to \mathcal{S}_{A_{\mathrm{ins}}/M_{\mathrm{ins}}}$ (Lemma 8.2). Therefore, Theorem B holds also when the fields $K_{\mathrm{sep}}(\boldsymbol{\sigma})$ replace the fields $\tilde{K}(\boldsymbol{\sigma})$ (Theorem 8.3).

The second one is concerned with a finite base field K. It turns out that if $e \geq 2$, then for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ the field $\tilde{K}(\boldsymbol{\sigma})$ is finite, hence so is every finite extension M of $\tilde{K}(\boldsymbol{\sigma})$. Following a hint of the referee, we find that the full section conjecture is true in this case, that is the Kummer map is bijective (Theorem 9.1(b)).

In addition to the case $e \geq 2$, we are able to prove the analog of Theorem B for K finite and $e = 1$ (Theorem 9.1(a)). Here, $\tilde{K}(\sigma)$ is infinite for almost all $\sigma \in \mathrm{Gal}(K)$. Hence, so is every finite extension M of $\tilde{K}(\sigma)$. Thus, M is PAC. In addition, we use that $A(\tilde{K}) = A_{\mathrm{tor}}(\tilde{K})$ for every abelian variety A over K.

Theorem B for an infinite finitely generated base field K and $e = 1$ remains open.

The authors are indebted to the anonymous referees for their helpful comments, to Jakob Stix for his enlightened letter [Sti20], and to Aharon Razon for careful reading of the manuscript.

2 Semi-simple Algebras

{SSMa}

Yuri Zarhin proves in [Zar77] that the mod-l reduction of a semi-simple $\mathbb{Q}$-algebra that satisfies a few natural finiteness conditions is again semi-simple if l is a sufficiently large prime number. Based on a theorem of Faltings, we generalize Zarhin's result to finitely generated extensions of $\mathbb{Q}$. This is done in this and the next section.

We denote the algebraic closure of a field K by $\tilde{K}$ and the maximal separable extension of K in $\tilde{K}$ by K_{sep}. Recall that an **abelian variety** over K is, by definition, a group scheme over K which is proper and geometrically integral [Mil86, p. 103, Conventions and Sec. 1]. It is known that abelian varieties are projective [Mil86, p. 113, Thm. 7.1], smooth [Mil86, p. 104, Sec. 1], and commutative [Mil86, p. 105, Cor. 2.4].

{abel}

Remark 2.1. We denote the zero point of an abelian variety A by $\mathbf{o}$ and set $\mathbf{0} = \{\mathbf{o}\}$. For every positive integer n, we let $n_A\colon A \to A$ be the isogeny of A defined by multiplication with n and let $A_n = \mathrm{Ker}(n_A)$. We abuse our notation and write A_n also for $A_n(\tilde{K}) = \{\mathbf{a} \in A(\tilde{K}) \mid n\mathbf{a} = \mathbf{o}\}$, if $\mathrm{char}(K) \nmid n$. In this case, n_A is étale, [Mil86, p. 115, Thm. 8.2]. In particular each $\mathbf{a} \in A_n(\tilde{K})$ already lies in $A_n(K_{\mathrm{sep}})$ [Mum88, p. 245, Cor.(1)]. ∎

As usual, we let $M_n(K)$ be the ring of all $n \times n$ matrices with entries in K.

{MATr}

Lemma 2.2. *The following statements about a perfect field K and a finite-dimensional K-algebra D are equivalent.*

(a) *D is a semi-simple K-algebra.*

(b) *$D \otimes_K \tilde{K}$ is a semi-simple $\tilde{K}$-algebra.*

(c) *There exist positive integers $n_1, \ldots, n_r$ such that $D \otimes_K \tilde{K} \cong \prod_{i=1}^r M_{n_i}(\tilde{K})$.*

(d) *There exist a finite extension L of K and positive integers $n_1, \ldots, n_r$ such that $D \otimes_K L \cong \prod_{i=1}^r M_{n_i}(L)$*

Proof. The implication (a) $\Longrightarrow$ (b) is a special case of [Lan93, p. 658, Thm. 6.2]. See also the second paragraph of [Lan93, p. 659].

(b) $\Longrightarrow$ (c): By assumption, $D \otimes_K \tilde{K}$ is a direct sum of finitely many simple finite dimensional $\tilde{K}$-algebras. By a consequence of Wedderburn theorem, each of them is isomorphic to $M_n(\tilde{K})$ for some positive integer n [Lor08, p. 158, Thm. 6]. Hence, (c) is true.

(c) $\Longrightarrow$ (d): The isomorphism $D \otimes \tilde{K} \cong \prod_{i=1}^r M_{n_i}(\tilde{K})$ is already defined over a finite extension L of K. Hence, $D \otimes_K L \cong \prod_{i=1}^r M_{n_i}(L)$.

(d) $\Longrightarrow$ (a): Let $J = \mathrm{Rad}(D)$ be the Jacobson radical of D, that is the intersection of all maximal right ideals of D. By [Lor08, p. 148, Thm. 4], there exists a positive integer k such that $J^k = \mathbf{0}$. Thus, the product of k elements of J is always 0. Hence, each element of $J \otimes_K L$ is nilpotent. Therefore, by [Lor08, p. 148, F38],

$$J \otimes_K L \subseteq \mathrm{Rad}(D \otimes_K L). \qquad (4)$$ {Jcbs}

By [Lor08, p. 152, F3], each L-algebra $M_{n_i}(L)$ is simple. Hence, $D \otimes_K L$ is semi-simple. Therefore, by [Lan93, p. 658, Thm. 6.1(d)], $\mathrm{Rad}(D \otimes_K L) = \mathbf{0}$, so by (4), $J \otimes_K L = \mathbf{0}$. Finally, the field extension L/K is faithfully flat, so $J = \mathbf{0}$. Therefore, by [Lan93, p. 658, Thm. 6.1(c)], D is semi-simple, as claimed. □

{ZARg}

Lemma 2.3 ([Zar77], Lemma 3.2)**.** *Let D be a $\mathbb{Z}$-algebra which is finitely generated and free as a $\mathbb{Z}$-module. Suppose that the $\mathbb{Q}$-algebra $D \otimes \mathbb{Q}$ is semi-simple. Then, for all large $l \in \mathbb{L}$, the $\mathbb{F}_l$-algebra $D \otimes \mathbb{F}_l$ is semi-simple.*

Proof. By Lemma 1.2, there exist a finite extension L of $\mathbb{Q}$, positive integers $n_1, \ldots, n_r$, and an isomorphism $f\colon D \otimes_{\mathbb{Q}} L \to \prod_{i=1}^r M_{n_i}(L)$ of L-algebras. Then, there exists a positive integer m such that for the integral closure R of $\mathbb{Z}[\frac{1}{m}]$ in L, both f and f^{-1} are defined over R. Hence, the restriction f_0 of f to $D \otimes R$ is an isomorphism onto $\prod_{i=1}^r M_{n_i}(R)$.

For each prime number l that does not divide m, and every maximal ideal $\mathfrak{p}$ of R that lies over $l\mathbb{Z}[\frac{1}{m}]$ we consider the residue field $\bar{L}_\mathfrak{p} = R/\mathfrak{p}$. Then,

$$f_0 \otimes_R \bar{L}_\mathfrak{p} \colon D \otimes \bar{L}_\mathfrak{p} \to \prod_{i=1}^{r} M_{n_i}(\bar{L}_\mathfrak{p})$$

is an isomorphism. It follows from Lemma 1.2, that $D \otimes \mathbb{F}_l$ is semi-simple, as claimed. □

The following lemma appears in a remark on page 169 of [Mum74].

{ISOg}

Lemma 2.4. *Let $f\colon A \to B$ be an isogeny of abelian varieties over a field K. Let n be a positive integer such that $\mathrm{Ker}(f) \le \mathrm{Ker}(n_A)$. Then:*

(a) *There exists an isogeny $g\colon B \to A$ such that $g \circ f = n_A$ and $f \circ g = n_B$.*

(b) $g(B_n) = \mathrm{Ker}(f)$.

Proof. For Statement (a), see [EGM19, p. 75, Prop. 5.12].

For statement (b) we note that since g is surjective, it restricts to a surjective homomorphism $g\colon B_n = \mathrm{Ker}(f \circ g) \to \mathrm{Ker}(f)$. □

As usual, we denote the ring of endomorphisms of A by $\mathrm{End}(A)$ and let $\mathrm{End}_K(A)$ be the ring of endomorphisms of A that are defined over K.

{SEMs}

Lemma 2.5. *Let A be an abelian variety over a field K. Then, $\mathrm{End}_K(A) \otimes \mathbb{F}_l$ is a finite dimensional semi-simple $\mathbb{F}_l$-algebra for almost all $l \in \mathbb{L}$.*

Proof. By [Mil86, p. 123, Thm. 12.5], $\mathrm{End}(A)$ is a free $\mathbb{Z}$-module of rank $\le 4\mathrm{dim}(A)^2$. Hence, $\dim_{\mathbb{F}_l}(\mathrm{End}_K(A) \otimes \mathbb{F}_l) \le 4\mathrm{dim}(A)^2$ for all $l \in \mathbb{L}$.

In general, if abelian varieties B and B' are isogeneous, then $\mathrm{End}(B) \otimes \mathbb{Q} \cong \mathrm{End}(B') \otimes \mathbb{Q}$ [Mil08, Second paragraph after Remark 10.2]. Hence, by Poincaré complete reducibility theorem [Mum74, p. 173, Thm. 1], we may assume that $A = A_1^{n_1} \times \cdots \times A_r^{n_r}$, where $A_1, \ldots, A_r$ are non-isogenous simple abelian varieties. It follows from [Mum74, p. 174, Cor. 2] that $\mathrm{End}_K(A) \otimes \mathbb{Q} \cong \prod_{i=1}^r M_{n_i}(D_i)$, where each D_i is a division ring. Hence, by [Lor08, p. 157, Thm. 4], $\mathrm{End}_K(A) \otimes \mathbb{Q}$ is a semi-simple $\mathbb{Q}$-algebra. Therefore, by Lemma 1.3, $\mathrm{End}_K(A) \otimes \mathbb{F}_l$ is semi-simple for all sufficiently large $l \in \mathbb{L}$, as claimed. □

3 Endomorphism Rings of Abelian Varieties

{ERAv}

Let K be a finitely generated field of characteristic $p \ge 0$ and A a non-zero abelian variety over K. By [Mum74, p. 64, Prop.(3)], we have for each positive integer n with $\mathrm{char}(K) \nmid n$ that

$$A_n \cong (\mathbb{Z}/n\mathbb{Z})^{2\mathrm{dim}(A)} \qquad (5)$$ {torl}

as abelian groups. Moreover, for $l \in \mathbb{L}'$, the group $\mathrm{Gal}(K)$ acts on A_l, so we may consider A_l as an $\mathbb{F}_l[\mathrm{Gal}(K)]$-module.

{MODu}

Notation 3.1 (Rings of endomorphisms)**.** For a module M over an associative ring R with 1, one usually denotes the ring of endomorphisms of M by $\mathrm{End}(M)$ or by $\mathrm{End}_R(M)$, if one wishes to stress the underlying ring R. For example, one writes $\mathrm{End}_{\mathbb{Z}}(M)$ for the ring of endomorphisms of M as an abelian group. ∎

The following result includes some well known results about abelian varieties. However, Statements (b) and (c) for function fields over $\mathbb{Q}$ seem to be missing in the literature.

{galbasics}

Proposition 3.2.

(a) *$A(K)$ is a finitely generated abelian group.*

(b) *For almost all $l \in \mathbb{L}'$, the $\mathrm{Gal}(K)$-module A_l is semi-simple.*

(c) *For almost all $l \in \mathbb{L}'$, the natural homomorphism $\mathrm{End}_K(A) \otimes \mathbb{Z}/l\mathbb{Z} \to \mathrm{End}_{\mathbb{F}_l[\mathrm{Gal}(K)]}(A_l)$ is an isomorphism.*

(d) *$H^1(\mathrm{Gal}(K(A_l)/K), A_l) = 0$ for almost all $l \in \mathbb{L}'$.*

Statement (a) of Proposition 2.2 is the well known Mordell-Weil and Lang-Néron theorem. See [Lan62, Chap. V] for a classical proof and [Con06, Cor. 7.2] for a scheme theoretic proof.

For Part (b) in the case where K is a number field, see [Zar85, Cor. 5.4.3(b)]. Part (b) in the case $p > 0$ can be found at [Zar14, Cor. 2.3.(iii)].

Part (c) for number fields can be found in [Zar85, Cor. 5.4.5]. The case where $p > 0$ is covered by [Zar14, Cor. 2.7].

By (b), A_l is a semi-simple $\mathrm{Gal}(K)$-module for almost all $l \in \mathbb{L}'$. By (5), $\dim_{\mathbb{F}_l}(A_l) = 2\dim(A)$ is independent of l. Hence, Part (d) follows from [Nor87, §4, Thm. E].

The rest of this section is devoted to the proof of Parts (b) and (c) in the remaining case, where K is a function field of several variables over a number field.

Thus, for the remaining of this section, we assume that K is a finitely generated extension of $\mathbb{Q}$. We start by citing a finiteness theorem for K due to Faltings. To this end we choose a finitely generated regular extension R of $\mathbb{Z}$ with quotient field K and cite two major results.

{FaWu}

Proposition 3.3 ([FaW84], p. 205, Thm. 2)**.** *Up to isomorphism, there exist only finitely many abelian varieties of a given dimension g over K which have good reduction at all primes $\mathfrak{p}$ of R of height one.*

{SRTa}

Proposition 3.4 ([SeT68], Cor. 2)**.** *Let v be a discrete valuation of a field F and let A and A' be isogenous abelian varieties over F such that A has good reduction at v. Then, also A' has good reduction at v.*

The following result generalizes [Zar85, Prop. 3.1]. That result relies on Faltings' finiteness theorem for number fields [Fal83, Satz 6]. Our proof applies Proposition 2.3.

{ZRHa}

Lemma 3.5. *Let A be an abelian variety over K. Then, up to an isomorphism, there exist only finitely many abelian varieties over K that are isogenous to A.*

Proof. Since R is finitely generated over $\mathbb{Z}$, it is Noetherian. By assumption, R is regular, hence also integrally closed [Mat94, p. 157, Thm. 19.4]. If the height of a prime ideal $\mathfrak{p}$ of R is 1, then $\mathfrak{p}R_\mathfrak{p}$ is the unique non-zero prime ideal of $R_\mathfrak{p}$. Hence, by [CaF67, p. 4, Prop. 3], $R_\mathfrak{p}$ is a discrete valuation domain.

Using that conclusion, we infer from [Shi98, p. 95, Prop. 25] that there exists a nonzero element $a \in R$ such that if $\mathfrak{p}$ is a prime ideal of R of height 1 and $a \notin \mathfrak{p}$, then A has a good reduction at $\mathfrak{p}$. Replacing R by $R[a^{-1}]$, we may assume without loss that A has good reduction at each $\mathfrak{p} \in \mathrm{Spec}(R)$ of height 1.

Let $\mathcal{A}$ be the set of all abelian varieties A' over K (up to isomorphism) with $\dim(A') = \dim(A)$ and with good reduction at each $\mathfrak{p} \in \mathrm{Spec}(R)$ of height 1. By Proposition 2.3, $\mathcal{A}$ is finite.

Next let $\mathcal{A}'$ be the set of all abelian varieties (up to isomorphism) over K that are isogenous to A and consider $A' \in \mathcal{A}'$. Then, A' is isogenous to A, in particular $\dim(A') = \dim(A)$. If $\mathfrak{p} \in \mathrm{Spec}(R)$ has height 1, then by the first paragraph of the proof and by Proposition 2.4, A' has good reduction at $\mathfrak{p}$. Hence, $A' \in \mathcal{A}$. It follows that $\mathcal{A}' \subseteq \mathcal{A}$, so by the preceding paragraph, $\mathcal{A}'$ is finite, as claimed. □

The following result generalizes [Zar85, Cor. 5.4.1]

{ENDo}

Lemma 3.6. *Let A be an abelian variety over K. Then, for almost all $l \in \mathbb{L}$ and every $\mathrm{Gal}(K)$-submodule W of A_l there exists an endomorphism $u \in \mathrm{End}_K(A)$ such that $u(A_l) = W$.*

Proof. Let $A^{(1)}, \ldots, A^{(s)}$ be all of the abelian varieties over K (up to isomorphism) that are isogenous to A (Lemma 2.5). For each j between 1 and s we choose an isogeny $h_j\colon A \to A^{(j)}$. We set $r = \max(|\mathrm{Ker}(h_1)|, \ldots, |\mathrm{Ker}(h_s)|)$.

Let $l > r$ be a prime number, let W be a $\mathrm{Gal}(K)$-submodule of A_l, and consider the abelian variety $B = A/W$. By Lemma 1.4, there exists an isogeny $g\colon B \to A$ such that

$$g(B_l) = W. \quad (6)$$ {Blwu}

By the first paragraph of the proof, there exists an isomorphism $v\colon A^{(j)} \to B$ for some $j \in \{1, \ldots, s\}$. Then, $f = v \circ h_j\colon A \to B$ is an isogeny and $|\mathrm{Ker}(f)| = |\mathrm{Ker}(h_j)| \le r$. By the choice of l, we have $l > r$, so $l \nmid |\mathrm{Ker}(f)|$. Hence, f maps A_l injectively into B_l. Since f is an isogeny, $\dim(B) = \dim(A)$, Hence,

$$|A_l| \overset{(5)}{=} l^{2\dim(A)} = l^{2\dim(B)} \overset{(5)}{=} |B_l|.$$

Therefore, f maps A_l bijectively onto B_l.

It follows that $u = g \circ f$ is a K-endomorphism of A that satisfies

$$u(A_l) = g(f(A_l)) = g(B_l) \overset{(6)}{=} W,$$

as desired. □

The following Lemma is part of [Hup67, p. 467, Hilfssatz 3.5].

{IDMp}

Lemma 3.7. *Let D be a finite dimensional semi-simple algebra over a field F. Then, for every right ideal $\mathfrak{r}$ of D, there exists an idempotent e of D such that $\mathfrak{r} = eD$.*

{LAMl}

Remark 3.8 (The ring $E_l(A)$)**.** For every abelian variety A over K and every $l \in \mathbb{L}$, we consider the ring homomorphism $\lambda_l \colon \mathrm{End}_K(A) \to \mathrm{End}_{\mathbb{F}_l}(A_l) = \mathrm{End}_{\mathbb{Z}}(A_l)$ defined by $\lambda_l(f) = f|_{A_l}$ for each $f \in \mathrm{End}_K(A)$. Let $E_l(A) = \{f|_{A_l} \mid f \in \mathrm{End}_K(A)\}$ be the image of $\mathrm{End}_K(A)$ in $\mathrm{End}_{\mathbb{F}_l}(A_l)$ under λ_l. For each $f \in \mathrm{End}_K(A)$, every $\sigma \in \mathrm{Gal}(K)$, and all $\mathbf{a} \in A(\tilde{K})$, we have $f(\sigma(\mathbf{a})) = \sigma(f(\mathbf{a}))$, hence,

$$E_l(A) \subseteq \mathrm{End}_{\mathbb{F}_l[\mathrm{Gal}(K)]}(A_l). \qquad (7)$$

{elen}

By definition, $l \cdot \mathrm{End}_K(A) \subseteq \mathrm{Ker}(\lambda_l)$. Conversely, if $f \in \mathrm{Ker}(\lambda_l)$, then f vanishes on $A_l = \mathrm{Ker}(l_A)$. Hence, since l_A is surjective, there exists a homomorphism $g \colon A \to A$ such that $g \circ l_A = f$. Therefore, $f = l_A \circ g \in l \cdot \mathrm{End}(A)$. Moreover, for each $\sigma \in \mathrm{Gal}(K)$, we have $\sigma(g) \circ l_A = \sigma(f) = f = g \circ l_A$. Since $l_A \colon A(\tilde{K}) \to A(\tilde{K})$ is surjective, we have $\sigma(g) = g$, so $g \in \mathrm{End}_K(A)$. We conclude that $\mathrm{Ker}(\lambda_l) = l \cdot \mathrm{End}_K(A)$. It follows that

$$E_l(A) \cong \mathrm{End}_K(A)/l \cdot \mathrm{End}_K(A) \cong \mathrm{End}_K(A) \otimes \mathbb{F}_l. \qquad (8)$$

{kerl}

Thus, by Lemma 1.5, $E_l(A)$ is a finite dimensional semi-simple $\mathbb{F}_l$-algebra for almost all $l \in \mathbb{L}$. ∎

We are now in a position to prove Part (b) of Proposition 2.2 in the remaining case that we restate for the convenience of the reader.

{SEMi}

Lemma 3.9. *Let A be a non-zero abelian variety over a finitely generated extension K of $\mathbb{Q}$. Then, for almost all $l \in \mathbb{L}$ the $\mathrm{Gal}(K)$-module A_l is semi-simple.*

Proof. Let l be a sufficiently large prime number and let W be a $\mathrm{Gal}(K)$-submodule of A_l. We have to prove that there exists a $\mathrm{Gal}(K)$-submodule W' of A_l such that $A_l = W \oplus W'$.

Lemma 2.6 yields an element $u \in E_l(A)$ such that

$$u(A_l) = W. \qquad (9)$$

{Uual}

We consider the right ideal

$$\mathfrak{a} = \{f \in E_l(A) \mid f(A_l) \subseteq W\}$$

of $E_l(A)$. In particular $u \in \mathfrak{a}$. Taking l larger, we may assume by Remark 2.8 that $E_l(A)$ is a semi-simple $\mathbb{F}_l$-algebra. Hence, by Lemma 2.7, there exists an idempotent element v of $E_l(A)$ such that $\mathfrak{a} = vE_l(A)$. In particular, there exists $v' \in E_l(A)$ such that $u = vv'$. It follows from (9) that

$$v(A_l) = W. \qquad (10)$$

{Vval}

Since v is an idempotent, so is $w := \mathrm{id}_{A_l} - v$. By (7), $w \in \mathrm{End}_{\mathbb{F}_l[\mathrm{Gal}(K)]}(A_l)$, so $w \circ \sigma = \sigma \circ w$ for all $\sigma \in \mathrm{Gal}(K)$. Hence,

$$W' := w(A_l) \tag{11}$$ {Wwal}

is a $\mathrm{Gal}(K)$-module that satisfies $A_l = W + W'$.

Now note that $vw = v - v^2 = v - v = 0$ and similarly $wv = 0$. Hence, by (10) and (11), a simple classical argument shows that $A_l = W \oplus W'$ [Coh89, p. 172, Prop. 2.3], as desired. □

Our final goal in this section is the proof of Proposition 2.2(c) for function fields over $\mathbb{Q}$.

{DUBc}

Remark 3.10 (The bi-commutant)**.** Let R be an associative ring with 1 and let M be an R-module. We consider M also as a $\mathbb{Z}$-module, let $\lambda_M\colon R \to \mathrm{End}_{\mathbb{Z}}(M)$ be the homomorphism defined by $\lambda_M(r)(m) = rm$ for all $r \in R$ and $m \in M$, and set $R_M = \lambda_M(R)$ to be the ring of homotheties of M.

We also consider the centralizer (also known as the **commutant**) of R_M in $\mathrm{End}_{\mathbb{Z}}(M)$:

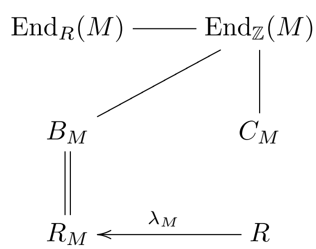
$$C_M = \{\gamma \in \mathrm{End}_{\mathbb{Z}}(M) \mid \ r\gamma(m) = \gamma(rm) \text{ for all } r \in R \text{ and } m \in M\}.$$

The centralizer

$$B_M = \{\beta \in \mathrm{End}_{\mathbb{Z}}(M) \mid \ \beta\gamma = \gamma\beta \text{ for all } \gamma \in C_M\}$$

of C_M in $\mathrm{End}_{\mathbb{Z}}(M)$ is the **double centralizer** (also known as the **bi-commutant**) of R_M. Following the definitions, one finds that $R_M \subseteq B_M$.

Claim: *When M is a semi-simple R-module which is finitely generated as an $\mathrm{End}_R(M)$-module (in particular if M is finite), the* **double centralizer theorem** *asserts that $R_M = B_M$.*



Indeed, Theorem 2 on page 78 of [Bou12] says "Un module génerateur est équilibré". By Définition 1 on page 73 of [Bou12], being équilibré for an R-module M means that $R_M = B_M$. Définition 2 on page 75 of [Bou12] defines the notion of "being génerateur" for M. We do not repeat that definition here. Instead we note that Exemple 3 on page 77 of [Bou12] says that M is genérateur if M satisfies the assumptions of our claim. Thus, by the above quoted Theorem 2, $R_M = B_M$, as claimed. ∎

{ENDl}

Lemma 3.11 (Part (c) of Proposition 2.2 for function fields over $\mathbb{Q}$)**.** *Let A be an abelian variety over a finitely generated extension K of $\mathbb{Q}$. Then, the restriction map $\mathrm{End}_K(A) \to \mathrm{End}_{\mathbb{F}_l[\mathrm{Gal}(K)]}(A_l)$ is surjective for almost all $l \in \mathbb{L}$. In other words, $\mathrm{End}_{\mathbb{F}_l[\mathrm{Gal}(K)]}(A_l) = E_l(A)$ for almost all $l \in \mathbb{L}$.*

Proof. In the notation of Remark 2.8 and Remark 2.10 we consider the associative ring $R = E_l(A)$ and the R-module $M = A_l$. Fixing a sufficiently large $l \in \mathbb{L}$, we have, by Remark 2.8, that $E_l(A)$ is a finitely generated semi-simple $\mathbb{F}_l$-algebra. Hence, by [Lan93, p. 651, Prop. 4.1], M is a semi-simple $E_l(A)$-module. We let λ_M be the identity map of $E_l(A)$ into $\mathrm{End}_{\mathbb{Z}}(M) = \mathrm{End}_{\mathbb{Z}}(A_l)$. Thus, in the notation of Remark 2.10, $R_M = E_l(A)$. Finally let

$$C_l(A) = C_M = \{g \in \mathrm{End}_{\mathbb{Z}}(A_l) \mid \ g \circ f = f \circ g \text{ for all } f \in E_l(A)\}$$

and

$$B_l(A) = B_M = \{h \in \mathrm{End}_{\mathbb{Z}}(A_l) \mid \ h \circ g = g \circ h \text{ for all } g \in C_l(A)\}.$$

By Remark 2.10, $R_M = B_M$. This means that

$$E_l(A) = \{h \in \mathrm{End}_{\mathbb{Z}}(A_l) \mid \ h \circ g = g \circ h \text{ for all } g \in C_l(A)\}. \qquad (12)$$ {dblc}

Hence, in view of (7), it suffices to prove the following statement:

Claim: *for every sufficiently large $l \in \mathbb{L}$, for each $h \in \mathrm{End}_{\mathbb{F}_l[\mathrm{Gal}(K)]}(A_l)$, and all $g \in C_l(A)$, we have that $h \circ g = g \circ h$.*

To this end we consider the abelian variety $A^2 = A \times A$ over K and observe that the graph $\Gamma = \{(\mathbf{a}, h(\mathbf{a})) \mid \mathbf{a} \in A_l\}$ of h is an $\mathbb{F}_l[\mathrm{Gal}(K)]$-submodule of A_l^2 and that $h \circ g = g \circ h$ if and only if $(g,g)(\Gamma) \subseteq \Gamma$.

Now, we consider a sufficiently large l, for which Lemma 2.6 applied to A^2 rather than to A, yields an element $u \in E_l(A^2)$ such that $u(A_l^2) = \Gamma$. By the definition of $C_l(A)$, g centralizes $E_l(A)$. Since $\mathrm{End}_K(A^2)$ naturally agrees with $M_2(\mathrm{End}_K(A))$, the map (g,g) centralizes $E_l(A^2)$. Thus, we have $(g,g) \circ u|_{A_l^2} = u|_{A_l^2} \circ (g,g)$. Therefore, $(g,g)(\Gamma) = (g,g)(u(\mathbb{A}_l^2)) = u((g,g)(A_l^2)) \subseteq u(A_l^2) = \Gamma$, as claimed. $\square$

4 Kummer Theory for Abelian Varieties

{sec:heins}

Let K be a finitely generated field and let A/K be a non-zero abelian variety. For each $l \in \mathbb{L}'$ we set $K_l = K(A_l)$ and consider the following commutative diagram. Both of its rows are exact cohomology sequences associated with the short exact sequence $0 \to A_l \to A(K_{\mathrm{sep}}) \xrightarrow{l} A(K_{\mathrm{sep}}) \to 0$ of $\mathrm{Gal}(K)$ discrete modules:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_l(K_l) & \longrightarrow & A(K_l) & \xrightarrow{l} & A(K_l) & \xrightarrow{\delta_l'} & H^1(\mathrm{Gal}(K_l), A_l) \\ & & \uparrow & & \uparrow & & \uparrow & & \uparrow{\scriptstyle \mathrm{res}_l} \\ 0 & \longrightarrow & A_l(K) & \longrightarrow & A(K) & \xrightarrow{l} & A(K) & \xrightarrow{\delta_l} & H^1(\mathrm{Gal}(K), A_l), \end{array} \qquad (13)$$ {eq:longexact}

where δ_l and δ'_l are the appropriate **connecting homomorphisms** [NSW15, p. 15]. Note that $H^1(\mathrm{Gal}(K_l), A_l) = \mathrm{Hom}(\mathrm{Gal}(K_l), A_l)$, because the action of $\mathrm{Gal}(K_l)$ on A_l is trivial. For each $\mathbf{p} \in A(K_l)$ we set

$$\xi_{l,\mathbf{p}} = \delta'_l(\mathbf{p}). \tag{14}$$ {xi}

By [NSW15, p. 15, The group $H^1(G, A)$], the map $\xi_{l,\mathbf{p}} \in \mathrm{Hom}(\mathrm{Gal}(K_l), A_l)$ has an explicit description: We choose $\mathbf{p}_l \in A(K_{\mathrm{sep}})$ with $l\mathbf{p}_l = \mathbf{p}$, then

$$\xi_{l,\mathbf{p}}(\sigma) = \sigma(\mathbf{p}_l) - \mathbf{p}_l \tag{15}$$ {eq:xiexplizit}

for all $\sigma \in \mathrm{Gal}(K_l)$. In particular, the right hand side of (15) does not depend on the choice of $\mathbf{p}_l$.

The function $\xi_{l,\mathbf{p}}\colon \mathrm{Gal}(K_l) \to A(K_{\mathrm{sep}})$ satisfies a few useful rules:

{xi-rechenregeln}

Lemma 4.1. *Let $\mathbf{p}$ be a point in $A(K)$. Then:*

(a) $\xi_{l,f(\mathbf{p})}(\sigma) = f(\xi_{l,\mathbf{p}}(\sigma))$ *for all* $f \in \mathrm{End}_K(A)$ *and all* $\sigma \in \mathrm{Gal}(K_l)$.
(b) *For all* $l \gg 0$ *in* $\mathbb{L}'$, *we have* $\xi_{l,\mathbf{p}} = 0 \Leftrightarrow \mathbf{p} \in lA(K)$.
(c) $\xi_{l,\mathbf{p}}(\tau\sigma\tau^{-1}) = \tau(\xi_{l,\mathbf{p}}(\sigma))$ *for all* $\sigma \in \mathrm{Gal}(K_l)$ *and all* $\tau \in \mathrm{Gal}(K)$.

Proof. (a) We choose $\mathbf{p}_l \in A(K_{\mathrm{sep}})$ with $l\mathbf{p}_l = \mathbf{p}$ (Remark 1.1). Then, $lf(\mathbf{p}_l) = f(l\mathbf{p}_l) = f(\mathbf{p})$, hence

$$f(\xi_{l,\mathbf{p}}(\sigma)) \overset{(15)}{=} f(\sigma(\mathbf{p}_l) - \mathbf{p}_l) = \sigma(f(\mathbf{p}_l)) - f(\mathbf{p}_l) \overset{(15)}{=} \xi_{l,f(\mathbf{p})}(\sigma),$$

as stated in (a).

(b) We note that $\mathrm{Gal}(K)/\mathrm{Gal}(K_l) = \mathrm{Gal}(K(A_l)/K)$ and $A_l^{\mathrm{Gal}(K_l)} = A_l$. Thus, for all $l \in \mathbb{L}'$ we have the exact inflation-restriction sequence

$$0 \to H^1(\mathrm{Gal}(K(A_l)/K), A_l) \xrightarrow{\mathrm{inf}} H^1(\mathrm{Gal}(K), A_l) \xrightarrow{\mathrm{res}_l} H^1(\mathrm{Gal}(K_l), A_l)^{\mathrm{Gal}(K)}$$

[NSW15, p. 67, Prop. 1.6.7]. By Proposition 2.2(d), $H^1(\mathrm{Gal}(K(A_l)/K), A_l) = 0$ for almost all $l \in \mathbb{L}'$. Hence,

$$\mathrm{Ker}(\mathrm{res}_l) = 0 \quad \text{for almost all } l \in \mathbb{L}'. \tag{16}$$ {eq:kerres}

By Diagram (13) and by (14), $\mathrm{res}_l(\delta_l(\mathbf{p})) = \delta'_l(\mathbf{p}) = \xi_{l,\mathbf{p}}$. Thus, for almost all $l \in \mathbb{L}'$, we have that

$$\xi_{l,\mathbf{p}} = 0 \Leftrightarrow \mathrm{res}_l(\delta_l(\mathbf{p})) = 0 \overset{(16)}{\Leftrightarrow} \delta_l(\mathbf{p}) = 0 \overset{(13)}{\Leftrightarrow} \mathbf{p} \in lA(K),$$

as desired.

(c) We set $\mathbf{x}_l = \tau^{-1}(\mathbf{p}_l) - \mathbf{p}_l$ and note that $l\mathbf{x}_l = \tau^{-1}(\mathbf{p}) - \mathbf{p} = 0$, so $\mathbf{x}_l \in A_l$, hence $\sigma\mathbf{x}_l = \mathbf{x}_l$. Therefore,

$$\begin{aligned}\xi_{l,\mathbf{p}}(\tau\sigma\tau^{-1}) &\overset{(15)}{=} \tau\sigma\tau^{-1}(\mathbf{p}_l) - \mathbf{p}_l = \tau(\sigma(\tau^{-1}(\mathbf{p}_l)) - \tau^{-1}(\mathbf{p}_l)) \\ &= \tau(\sigma(\mathbf{p}_l + \mathbf{x}_l) - (\mathbf{p}_l + \mathbf{x}_l)) = \tau(\sigma(\mathbf{p}_l) - \mathbf{p}_l) \overset{(15)}{=} \tau(\xi_{l,\mathbf{p}}(\sigma)),\end{aligned}$$

as claimed. $\square$

Lemma 3.3 below is proven by Ribet in the case where $\mathrm{char}(K) = 0$ [Rib79, Thm. 1.2]. However, the proof remains intact in the general case. We represent it here for the convenience of the reader. The proof uses Lemma 3.1 and the following one.

{ribet-lemm}

Lemma 4.2. *Let* $\mathbf{p}$ *be a point of* $A(K)$. *Suppose that the homomorphism* $\Phi_{\mathbf{p}}\colon \mathrm{End}_K(A) \to A(K)$ *defined by* $\Phi_{\mathbf{p}}(f) = f(\mathbf{p})$ *is injective. Then, for almost all* $l \in \mathbb{L}'$, *the homomorphism* $\Phi_{\mathbf{p},l}\colon \mathrm{End}_K(A)/l\,\mathrm{End}_K(A) \to A(K)/lA(K)$ *defined by*

$$\Phi_{\mathbf{p},l}(f + l\,\mathrm{End}_K(A)) = f(\mathbf{p}) + lA(K)$$

is also injective.

Proof. Let $Q = A(K)/\Phi_{\mathbf{p}}(\mathrm{End}_K(A))$ and consider the commutative diagram with exact rows,

$$\begin{array}{ccccccccc} \mathbf{0} & \longrightarrow & \mathrm{End}_K(A) & \xrightarrow{\Phi_{\mathbf{p}}} & A(K) & \longrightarrow & Q & \longrightarrow & \mathbf{0} \\ & & \downarrow{\scriptstyle l} & & \downarrow{\scriptstyle l} & & \downarrow{\scriptstyle l} & & \\ \mathbf{0} & \longrightarrow & \mathrm{End}_K(A) & \xrightarrow{\Phi_{\mathbf{p}}} & A(K) & \longrightarrow & Q & \longrightarrow & \mathbf{0}, \end{array}$$

where $A(K) \to Q$ is the quotient map. The snake lemma yields an exact sequence

$$Q_l \to \mathrm{End}_K(A)/l\,\mathrm{End}_K(A) \xrightarrow{\Phi_{\mathbf{p},l}} A(K)/lA(K) \to Q/lQ \to \mathbf{0}, \qquad (17)$$ {eq:tensoredseq}

where $Q_l = \{x \in Q \mid lx = 0\}$ [NSW15, p. 25, Lemma 1.3.1]. By the Mordell-Weil theorem (Proposition 2.2(a)), Q is a finitely generated abelian group. Let $n_0 = |Q_{\mathrm{tor}}|$ be the order of the torsion part of Q. Then, $Q_l = 0$ for all $l > n_0$ in $\mathbb{L}'$. Hence, by (17), $\Phi_{\mathbf{p},l}$ is injective for all $l > n_0$ in $\mathbb{L}'$, as claimed. □

{ribet}

Lemma 4.3. *Let* $\mathbf{p}$ *be a point in* $A(K)$ *with the following property:*

The map $\mathrm{End}_K(A) \to A(K)$ *defined by* $f \mapsto f(\mathbf{p})$ *is injective* . (18) {indep}

Then, for almost all $l \in \mathbb{L}'$, *the homomorphism* $\xi_{l,\mathbf{p}}\colon \mathrm{Gal}(K_l) \to A_l$ *is surjective.*

Proof. For each $l \in \mathbb{L}'$ we set $I_l = \mathrm{Im}(\xi_{l,\mathbf{p}})$. Each element of I_l has the form $\xi_{l,\mathbf{p}}(\sigma)$ for some $\sigma \in \mathrm{Gal}(K_l)$. Hence, for each $\tau \in \mathrm{Gal}(K)$ we have by 3.1(c) that $\tau(\xi_{l,\mathbf{p}}(\sigma)) = \xi_{l,\mathbf{p}}(\tau\sigma\tau^{-1}) \in I_l$. Since $\mathrm{Gal}(K_l)$ acts trivially on A_l, this implies that I_l is an $\mathbb{F}_l[\mathrm{Gal}(K_l/K)]$-submodule of A_l.

By Proposition 2.2(b), for almost all $l \in \mathbb{L}'$ there exists an $\mathbb{F}_l[\mathrm{Gal}(K_l/K)]$-submodule J_l of A_l such that $A_l = I_l \oplus J_l$. Thus, it suffices to prove that $J_l = \mathbf{0}$ for almost all $l \in \mathbb{L}'$. Let $\pi_l\colon A_l \to J_l$ be the projection on J_l. Then, $\pi_l \in \mathrm{End}_{\mathbb{F}_l[\mathrm{Gal}(K)]}(A_l)$.

By Proposition 2.2(c) there exists for almost all $l \in \mathbb{L}'$ an endomorphism $f_l \in \mathrm{End}_K(A)$ whose restriction to A_l coincides with π_l. Now, for almost all $l \in \mathbb{L}'$ and for each $\sigma \in \mathrm{Gal}(K_l)$, we have

$$\xi_{l,f_l(\mathbf{p})}(\sigma) \overset{(*)}{=} f_l(\xi_{l,\mathbf{p}}(\sigma)) = \pi_l(\xi_{l,\mathbf{p}}(\sigma)) \overset{(**)}{=} 0,$$

where (*) follows from Lemma 3.1(a) and (**) holds because $\xi_{l,\mathbf{p}}(\sigma) \in I_l$. From Lemma 3.1(b), we conclude that $f_l(\mathbf{p}) \in lA(K)$ for almost all $l \in \mathbb{L}'$. Then, Lemma 3.2 implies that $f_l \in l \cdot \mathrm{End}_K(A)$ for almost all $l \in \mathbb{L}'$. Thus, there exists $g \in \mathrm{End}_K(A)$ with $lg = f_l$. It follows that $J_l = \pi_l(A_l) = f_l(A_l) = lg(A_l) = g(lA_l) = g(\mathbf{0}) = \mathbf{0}$ for almost all $l \in \mathbb{L}'$, as desired. □

Lemma 3.3 enters our proofs via the following corollary.

{ribetcor}

Corollary 4.4. *Let A be a simple abelian variety over K of dimension g and let $\mathbf{p} \in A(K)$ be a point of infinite order. Then, for almost all $l \in \mathbb{L}'$ and for every $\mathbf{q} \in A(K_{\mathrm{sep}})$ with $l\mathbf{q} = \mathbf{p}$, we have* $\mathrm{Gal}(K_l(\mathbf{q})/K_l) \cong A_l$ *and*

$$[K(\mathbf{q}) : K] = l^{2g}. \qquad (19)$$ {eq:basicestimates}

Proof. We prove that $\mathbf{p}$ satisfies Condition (18). Indeed, if $f \in \mathrm{End}_K(A)$ and $f(\mathbf{p}) = \mathbf{o}$, then $\mathrm{Ker}(f)$ is an infinite Zariski-closed subgroup of A. The connected component $\mathrm{Ker}(f)^0$ of that subgroup has a finite index in $\mathrm{Ker}(f)$ [Bor91, p. 46, Prop.(b)]. Hence $\mathrm{Ker}(f)^0$ is a non-zero abelian subvariety of A. Since A is simple, $\mathrm{Ker}(f)^0 = A$, so also $\mathrm{Ker}(f) = A$, hence $f = 0$, so (18) holds.

It follows from Lemma 3.3 that $\xi_{l,\mathbf{p}}\colon \mathrm{Gal}(K_l) \to A_l$ is surjective for almost all $l \in \mathbb{L}'$. By (15), $\mathrm{Ker}(\xi_{l,\mathbf{p}}) = \mathrm{Gal}(K_l(\mathbf{q}))$ for each $\mathbf{q} \in A(K_{\mathrm{sep}})$ with $l\mathbf{q} = \mathbf{p}$. This implies that $\mathrm{Gal}(K_l(\mathbf{q})/K_l) \cong A_l$ for almost all $l \in \mathbb{L}'$. Since $l \neq \mathrm{char}(K)$, we have by (5) that $|A_l| = l^{2g}$. Hence, $[K(\mathbf{q}) : K] \geq [K_l(\mathbf{q}) : K_l] = |A_l| = l^{2g}$.

On the other hand, $\mathbf{q}$ lies in the fiber of multiplication by l and the degree of this morphism is l^{2g} [Mum74, p. 64, Prop. (1)]. Hence, $[K(\mathbf{q}) : K] \leq l^{2g}$. It follows from the preceding paragraph that $[K(\mathbf{q}) : K] = l^{2g}$. □

5 Divisibility Properties

Let A, K, $\mathrm{End}_K(A)$, K_l, $\mathrm{Gal}(K_l)$ be as in Section 3 and set $g = \dim(A)$.

{JCBs}

Lemma 5.1. *Let A be an abelian variety over a field L and let M be an extension of L. Suppose that*
(a) $A(L) \cap \bigcap_{n\in\mathbb{N}} nA(M) \subseteq A_{\mathrm{tor}}(L)$ *and*
(b) $A_{l^\infty}(M)$ *is finite for every* $l \in \mathbb{L}$.
Then, $A(L) \cap \bigcap_{n\in\mathbb{N}} nA(M) = \mathbf{0}$.

Proof. Assume toward contradiction that there exists a non-zero point $\mathbf{p} \in A(L) \cap \bigcap_{n\in\mathbb{N}} nA(M)$. By (a), $m := \mathrm{ord}(\mathbf{p})$ has a prime divisor l. Set $m' = m/l$ and $\mathbf{p}' = m'\mathbf{p}$. Then, $\mathbf{p}' \in A(L) \cap \bigcap_{n\in\mathbb{N}} nA(M)$ and $\mathrm{ord}(\mathbf{p}') = l$. In particular, for every $j \in \mathbb{N}$ there exists $\mathbf{p}_j \in A(M)$ with $l^j \mathbf{p}_j = \mathbf{p}'$, so $\mathbf{p}_j$ is a point of order l^{j+1} in $A(M)$. This implies that $A_{l^\infty}(M)$ is infinite and contradicts (b). ☐

For each $e \geq 1$, we equip the compact group $\mathrm{Gal}(K)^e$ with its unique normalized Haar measure μ_K. As usual, we say that **almost all** $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ **have a certain property** if the measure of the set of all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ having that property is 1. Also, we say that a subset S of $\mathrm{Gal}(K)^e$ is a **zero set** if $\mu_K(S) = 0$.

{lemm:sec}

Lemma 5.2. *Let $e \geq 2$. Then, $A(K) \cap \bigcap_{l \in \mathbb{L}'} lA(\tilde{K}(\boldsymbol{\sigma})) \subseteq A_{\mathrm{tor}}(K)$ for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$.*

Proof. By definition, the field $\tilde{K}(\boldsymbol{\sigma}) \cap K_{\mathrm{sep}}$ is a separable as well as purely inseparable extension of $K_{\mathrm{sep}}(\boldsymbol{\sigma})$. Hence, $\tilde{K}(\boldsymbol{\sigma}) \cap K_{\mathrm{sep}} = K_{\mathrm{sep}}(\boldsymbol{\sigma})$ for each $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$. By Remark 1.1,

$$A(K) \cap \bigcap_{l \in \mathbb{L}'} lA(K_{\mathrm{sep}}(\boldsymbol{\sigma})) = A(K) \cap \bigcap_{l \in \mathbb{L}'} lA(\tilde{K}(\boldsymbol{\sigma})).$$

Therefore, it suffices to prove that

$$A(K) \cap \bigcap_{l \in \mathbb{L}'} lA(K_{\mathrm{sep}}(\boldsymbol{\sigma})) \subseteq A_{\mathrm{tor}}(K) \text{ for almost all } \boldsymbol{\sigma} \in \mathrm{Gal}(K)^e. \tag{20}$$ {LSEp}

The proof of (20) splits into two cases.

Case A: *A is a simple abelian variety.* Let $\mathbf{p} \in A(K)$ be a non-torsion point. We consider $l \in \mathbb{L}'$ and let $X_l(\mathbf{p}) = \{\mathbf{q} \in A(K_{\mathrm{sep}}) \mid l\mathbf{q} = \mathbf{p}\}$. By (5) and Remark 1.1,

$$|X_l(\mathbf{p})| = l^{2g}. \tag{21}$$ {eq:betragxell}

Next consider $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(K)^e$. Then,

$$\begin{aligned} \mathbf{p} \in \bigcap_{l \in \mathbb{L}'} lA(K_{\mathrm{sep}}(\boldsymbol{\sigma})) \;&\Leftrightarrow\; (\forall l \in \mathbb{L}')(\exists \mathbf{q} \in X_l(\mathbf{p})) : \bigwedge_{i=1}^{e} \sigma_i(\mathbf{q}) = \mathbf{q} \\ &\Leftrightarrow\; (\forall l \in \mathbb{L}')(\exists \mathbf{q} \in X_l(\mathbf{p})) \colon \boldsymbol{\sigma} \in \mathrm{Gal}(K(\mathbf{q}))^e \\ &\Leftrightarrow\; \boldsymbol{\sigma} \in \bigcap_{l \in \mathbb{L}'} \underbrace{\bigcup_{\mathbf{q} \in X_l(\mathbf{p})} \mathrm{Gal}(K(\mathbf{q}))^e}_{=:S_l(\mathbf{p})}. \end{aligned} \tag{22}$$ {eq:equivalencessigma}

By (21) and by Corollary 3.4,

$$\mu(S_l(\mathbf{p})) \leq \sum_{\mathbf{q} \in X_l(\mathbf{p})} \mu(\mathrm{Gal}(K(\mathbf{q}))^e) = \sum_{\mathbf{q} \in X_l(\mathbf{p})} [K(\mathbf{q}) : K]^{-e} = \frac{l^{2g}}{l^{2ge}}.$$

It follows that $\lim_{l \to \infty} \mu(S_l(\mathbf{p})) = 0$, because $e \geq 2$. Thus, $N(\mathbf{p}) := \bigcap_{l \in \mathbb{L}'} S_l(\mathbf{p})$ is a zero set. By (22), for all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e \smallsetminus N(\mathbf{p})$, we have $\mathbf{p} \notin \bigcap_{l \in \mathbb{L}'} lA(K_{\mathrm{sep}}(\boldsymbol{\sigma}))$.

Since K is countable,

$$N := \bigcup_{\mathbf{p}\in A(K)\smallsetminus A_{\mathrm{tor}}(K)} N(\mathbf{p}) \tag{23}$$

is also a zero set. Moreover, for all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e \smallsetminus N$, we have that $A(K) \cap \bigcap_{l\in\mathbb{L}'} lA(K_{\mathrm{sep}}(\boldsymbol{\sigma}))$ does not contain any non-torsion point, so it consists of torsion points, as desired.

Case B: *The general case.* By the Poincaré reducibility theorem, there exist simple abelian varieties $A_1, \ldots, A_r$ and an isogeny

$$f\colon A \to A_1 \times \cdots \times A_r$$

[Mil86, p. 122, Prop. 12.1]. By Case A, for each $i \in \{1, \cdots, r\}$ there exists a zero set Z_i of $\mathrm{Gal}(K)^e$ such that

$$A_i(K) \cap \bigcap_{l\in\mathbb{L}'} lA_i(K_{\mathrm{sep}}(\boldsymbol{\sigma})) \subseteq A_i(K)_{\mathrm{tor}} \text{ for all } \boldsymbol{\sigma} \in \mathrm{Gal}(K)^e \smallsetminus Z_i. \tag{24}$$ {tors}

We consider the zero set $Z = \bigcup_{i=1}^r Z_i$. Let $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e \smallsetminus Z$ and $\mathbf{p} \in A(K) \cap \bigcap_{l\in\mathbb{L}'} lA(K_{\mathrm{sep}}(\boldsymbol{\sigma}))$. We prove that $\mathbf{p}$ is torsion.

To this end let $\mathbf{q}_i$ be the projection of $f(\mathbf{p})$ on $A_i(K)$. Then, $\mathbf{q}_i \in A_i(K) \cap \bigcap_{l\in\mathbb{L}'} lA_i(K_{\mathrm{sep}}(\boldsymbol{\sigma}))$, so by (24), $\mathbf{q}_i \in A_i(K)_{\mathrm{tor}}$. Hence, there exists a positive integer m such that $mf(\mathbf{p}) = 0$. But then, $m\mathbf{p} \in \mathrm{Ker}(f)(K)$. Since f is an isogeny, $\mathrm{Ker}(f)(K)$ is a finite group. Hence, $|\mathrm{Ker}(f)(K)| \cdot m\mathbf{p} = 0$, so $\mathbf{p}$ is torsion, as desired. □

{lemm:sec2}

Lemma 5.3. *Let $e \geq 2$. Then, $A(K) \cap \bigcap_{n\in\mathbb{N}} nA(\tilde{K}(\boldsymbol{\sigma})) = \mathbf{0}$ for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$.*

Proof. Consider the sets

$$S_1 = \{\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e \mid\ A(K) \cap \bigcap_{n\in\mathbb{N}} nA(\tilde{K}(\boldsymbol{\sigma})) \subseteq A_{\mathrm{tor}}(K)\}, \text{ and}$$

$$S_2 = \{\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e \mid \text{ for all } l \in \mathbb{L}, \text{ the set } A_{l^\infty}(\tilde{K}(\boldsymbol{\sigma})) \text{ is finite } \}.$$

By Lemma 4.2, $\mu(S_1) = 1$. By [JaJ01, Main Theorem], $\mu(S_2) = 1$. Hence, $\mu(S_1 \cap S_2) = 1$.

If $\boldsymbol{\sigma} \in S_1 \cap S_2$, then Conditions (a) and (b) of Lemma 4.1 hold for K and $\tilde{K}(\boldsymbol{\sigma})$ rather than for L and M, respectively. Hence, by that lemma, $A(K) \cap \bigcap_{n\in\mathbb{N}} nA(\tilde{K}(\boldsymbol{\sigma})) = \mathbf{0}$, as desired. □

{mtdiv1}

Proposition 5.4. *For $e \geq 2$, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, and for all abelian varieties B over $\tilde{K}(\boldsymbol{\sigma})$ we have* $\mathrm{div}(B(\tilde{K}(\boldsymbol{\sigma}))) = \mathbf{0}$.

Proof. Let $\mathcal{L}$ be the set of all finite extensions of K in $\tilde{K}$. For each $L \in \mathcal{L}$, let L_0 be the maximal separable extension of K in L. Then, $K_{\mathrm{sep}} \cap L$ is a separable extension as well as a purely inseparable extension of L_0. Hence, $K_{\mathrm{sep}} \cap L = L_0$. Since K_{sep}/L_0 is a Galois extension, K_{sep} and L are linearly disjoint over L_0. Also, L_{sep} is a separable as well as a purely inseparable extension of $K_{\mathrm{sep}}L$. Therefore, $K_{\mathrm{sep}}L = L_{\mathrm{sep}}$. It follows that restriction to K_{sep} yields an isomorphism $\mathrm{Gal}(L) \cong \mathrm{Gal}(L_0)$. The uniqueness of the normalized Haar measure implies that this isomorphism respects the Haar measure.

The rest of the proof breaks up into two parts.

Part A: *Proving that* $\tilde{K}(\boldsymbol{\sigma}) = \tilde{L}(\boldsymbol{\sigma})$. Consider $\boldsymbol{\sigma} := (\sigma_1, \dots, \sigma_e) \in \mathrm{Gal}(L)^e$ and denote its restriction to K_{sep} also by $\boldsymbol{\sigma}$. If $\mathrm{char}(K) = 0$, then $K_{\mathrm{sep}} = \tilde{K} = \tilde{L} = L_{\mathrm{sep}}$, so $\tilde{K}(\boldsymbol{\sigma}) = \tilde{L}(\boldsymbol{\sigma})$. Otherwise, we assume for the rest of Part A that $\mathrm{char}(K) > 0$.

Then, $L_{\mathrm{sep}}(\boldsymbol{\sigma})$ is a purely inseparable extension of $K_{\mathrm{sep}}(\boldsymbol{\sigma})$, so $K_{\mathrm{sep}}(\boldsymbol{\sigma}) \subseteq L_{\mathrm{sep}}(\boldsymbol{\sigma}) \subseteq \tilde{K}(\boldsymbol{\sigma})$. This implies that $\tilde{K}(\boldsymbol{\sigma}) = \tilde{L}(\boldsymbol{\sigma})$.

Part B: *Conclusion of the proof.* Let $\mathcal{A}$ be the set of all abelian varieties over $\tilde{K}$. For each $L \in \mathcal{L}$, let $\mathcal{A}_L$ be the set of all $A \in \mathcal{A}$ defined over L. We set

$$S = \{\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e \mid \mathrm{div}(A(\tilde{K}(\boldsymbol{\sigma}))) = \mathbf{0} \text{ for all } A \in \mathcal{A} \text{ defined over } \tilde{K}(\boldsymbol{\sigma})\}.$$

Using Part A, for each $A \in \mathcal{A}_L$, we let

$$\begin{aligned} S_{L,A} &= \{\boldsymbol{\sigma} \in \mathrm{Gal}(L)^e \mid A(L) \cap \mathrm{div}(A(\tilde{L}(\boldsymbol{\sigma}))) = \mathbf{0}\} \\ &= \{\boldsymbol{\sigma} \in \mathrm{Gal}(L)^e \mid A(L) \cap \mathrm{div}(A(\tilde{K}(\boldsymbol{\sigma}))) = \mathbf{0}\}. \end{aligned}$$

Since K is countable, so is the set $\mathcal{B} = \{(L, A) \in \mathcal{L} \times \mathcal{A} \mid A \in \mathcal{A}_L\}$. Since every $A \in \mathcal{A}$ is already defined over some $L \in \mathcal{L}$, we have $S = \bigcap_{(L,A)\in\mathcal{B}} S_{L,A}$. Since $\mathrm{Gal}(K)^e = \bigcup_{L\in\mathcal{L}} \mathrm{Gal}(L_0)^e = \bigcup_{L\in\mathcal{L}} \mathrm{Gal}(L)^e$, we have

$$\mathrm{Gal}(K)^e \smallsetminus S \subseteq \bigcup_{(L,A)\in\mathcal{B}} (\mathrm{Gal}(L)^e \smallsetminus S_{L,A}). \tag{25}$$ {twtf}

For each $(L, A) \in \mathcal{B}$ we have, by Lemma 4.3 applied to L rather than to K, that $\mu_K(\mathrm{Gal}(L)^e \smallsetminus S_{L,A}) = \mu_L(\mathrm{Gal}(L)^e \smallsetminus S_{L,A})/[L : K]^e = 0$. Since $\mathcal{B}$ is countable, it follows from (25) that $\mathrm{Gal}(K)^e \smallsetminus S$ is a zero set, so the Haar measure of S is 1, as claimed. □

{CASe1}

Remark 5.5. Starting from the observation that $\bigcap_{n=1}^\infty n\mathbb{Z} = \mathbf{0}$ and $\bigcap_{n=1}^\infty nA = \mathbf{0}$ if A is a finite abelian group, we find that $\mathrm{div}(A) = \mathbf{0}$ for every finitely generated abelian group. By the Mordell-Weil-Lang-Néron theorem [Lan59, p. 71, Thm. 1], for every finitely generated field K and every abelian variety over K, the group $A(K)$ is a finitely generated abelian group. It follows that $\mathrm{div}(A(K)) = \mathbf{0}$.

On the other hand, multiplication of $A(\tilde{K})$ by every positive integer n is surjective (Remark 1.1). Hence, $\mathrm{div}(A(\tilde{K})) = A(\tilde{K}) \neq \mathbf{0}$ if $\dim(A) \geq 1$.

Proposition 4.4 states that if $e \geq 2$, then for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ and for all abelian varieties A over $\tilde{K}(\boldsymbol{\sigma})$, we have $\mathrm{div}(A(\tilde{K}(\boldsymbol{\sigma}))) = \mathbf{0}$. Thus, in this respect, almost all of the fields $\tilde{K}(\boldsymbol{\sigma})$ behave like finitely generated fields. The proof of that proposition is based among others on the observation used in the proof of Lemma 4.2 that $\lim_{l\to\infty} \frac{1}{l^{2g(e-1)}} = 0$.

This is of course wrong if $e = 1$, so the proof breaks down in that case. Thus, it may be the case that $\mathrm{div}(A(\tilde{K}(\sigma))) \neq \mathbf{0}$ if $e = 1$. But, we do not know that. ∎

6 Weil's Restriction

{WLRs}

Let K'/K be a finite extension of fields and let T be a K-scheme. The Weil restriction attaches to each quasi-projective K'-scheme X' a K-scheme $X = \mathrm{Res}_{K'/K}(X')$ and a natural bijection

$$\eta_T \colon \mathrm{Mor}_K(T, X) \to \mathrm{Mor}_{K'}(T_{K'}, X'). \quad (26)$$ {weil}

See [BLR90, p. 194, Thm. 4] or [Poo17, p. 110, Def. 4.61 and p. 111, Prop. 4.6.3]. When $T = \mathrm{Spec}(K)$, (26) becomes a natural bijection

$$\eta_K \colon X(K) \to X'(K').$$

If X' is a quasi-projective group scheme over K', then $X = \mathrm{Res}_{K'/K}(X')$ acquires a structure of a group scheme over K such that $X(K) \cong X'(K')$ as groups [BLR90, p. 192, lines 11,12].

{RESa}

Lemma 6.1. *If E/K is a finite separable extension of fields and A is an abelian variety over E, then $B = \mathrm{Res}_{E/K}(A)$ is an abelian variety over K. Moreover, $B(K) \cong A(E)$.*

Proof. As an abelian variety, A is projective (paragraph preceding Remark 1.1). Hence, by the paragraph preceding our Lemma, B is a group scheme over K. Since E/K is a separable extension, it is étale. Hence, by [BLR90, p. 195, Sec. 7.6, Prop. 5], B/K is proper.

It remains to check that B is geometrically integral, i.e. that $B_{\tilde{K}}$ is integral. It is known that $B_{\widetilde{K}} = \prod_\sigma A^\sigma_{\widetilde{K}}$ where σ ranges over the K-embeddings $E \to \widetilde{K}$. See [Poo17, p. 113, Exercise 4.7] or [FrJ08, p. 183, Prop. 10.6.2]. Now the A^σ are geometrically integral, because A is geometrically integral. Hence, $B_{\widetilde{K}}$ is integral, as desired.

Finally, the isomorphism $B(K) \cong A(E)$ of abelian groups follows from the paragraph preceding our lemma. □

Recall that a field M is **PAC** (resp. **ample**) if the set of M-rational points of every geometrically integral variety V over M (resp. with a simple M-rational point) is Zariski-dense in V [FrJ08, p. 192, Prop. 11.1.1] (resp. [Jar11, p. 68, Def. 5.3.2]). In particular, every PAC field is ample.

{mtdiv}

Theorem 6.2. *Let K be an infinite finitely generated field and let $e \geq 2$. Then, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, all finite extensions $M/\tilde{K}(\boldsymbol{\sigma})$, and all abelian varieties A/M we have*

(a) *M is PAC,*
(b) *$\mathrm{div}(A(M)) = 0$,*
(c) *$|A_{l^\infty}(M)| < \infty$ for all $l \in \mathbb{L}$, and*
(d) *if $\mathrm{char}(K) = 0$, also $|A_{\mathrm{tor}}(M)| < \infty$.*

Proof. By [FrJ08, p. 242, Thm. 13.4.2], K is a Hilbertian field. By [FrJ08, p. 380, Thm. 18.6.1], Proposition 4.4, and [JaJ01, Thm. 2.7 and Thm. 3.7], for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ and all abelian varieties $B/\tilde{K}(\boldsymbol{\sigma})$ we have: {mpac}

(27a) $K_{\mathrm{sep}}(\boldsymbol{\sigma})$ is PAC, {mtda}
(27b) $\mathrm{div}(B(\tilde{K}(\boldsymbol{\sigma}))) = \mathbf{0}$, {mtdb}
(27c) $|B_{l^\infty}(\tilde{K}(\boldsymbol{\sigma}))| < \infty$ for all $l \in \mathbb{L}$, and {mtdc}
(27d) if $\mathrm{char}(K) = 0$, also $|B_{\mathrm{tor}}(\tilde{K}(\boldsymbol{\sigma}))| < \infty$.

Let $\boldsymbol{\sigma}$ be an element of $\mathrm{Gal}(K)^e$ that satisfies (27a), (27b), (27c), and (27d), let $M/\tilde{K}(\boldsymbol{\sigma})$ be a finite extension, and let A/M be an abelian variety.

As an algebraic extension of $K_{\mathrm{sep}}(\boldsymbol{\sigma})$, the field M is PAC by (27a) and [FrJ08, p. 196, Cor. 11.2.5]. By Lemma 5.1, $B := \mathrm{Res}_{M/\tilde{K}(\boldsymbol{\sigma})}(A)$ is an abelian variety over $\tilde{K}(\boldsymbol{\sigma})$ with $B(\tilde{K}(\boldsymbol{\sigma})) \cong A(M)$. Hence, by (27b), (27c), and (27d), we respectively get (b), (c), and (d). ☐

7 The Profinite Kummer Map

{sec:Application}

In addition to Theorem 5.2 we need results of Stix and Koenigsmann about ample fields and PAC fields.

{SPCs}

Remark 7.1 (The space of sections)**.** We consider a short exact sequence of profinite groups:

$$\mathbf{1} \longrightarrow \tilde{\Pi} \longrightarrow \Pi \xrightarrow{\ \rho\ } G \longrightarrow \mathbf{1}.$$

A **section** of ρ is a homomorphism $s\colon G \to \Pi$ that satisfies $\rho \circ s = \mathrm{id}_G$. In particular, s is injective.

Another section $s'\colon G \to \Pi$ is said to be **$\tilde{\Pi}$-conjugate** to s if there exists $\tilde{\pi} \in \tilde{\Pi}$ such that for all $g \in G$ we have $s'(g) = \tilde{\pi}^{-1}s(g)\tilde{\pi}$. We denote the conjugacy $\tilde{\Pi}$-class of s by $[s]$ and let $\mathcal{S}_{\Pi\to G}$ be the set of all $\tilde{\Pi}$-conjugacy classes of sections of ρ.

For every open subgroup H of Π we set

$$U_H = \{S \in \mathcal{S}_{\Pi\to G} \mid \text{there exists } s \in S \text{ such that } s(G) \subseteq H\}.$$

If H' is an open subgroup of Π and $H' \leq H$, then $U_{H'} \subseteq U_H$. Hence, the collection of all sets U_H forms a basis to a topology on $\mathcal{S}_{\Pi\to G}$ that we call the **pro-discrete topology**. ∎

{PRKm}

Remark 7.2 (The fundamental group)**.** By a **variety over a field** M we mean a separated scheme X of finite type over M.

We consider a geometrically integral normal variety X over M with a geometric generic point $\bar{\mathbf{x}}$ and let $F = M(X) = M(\bar{\mathbf{x}})$ be the function field of X. Let $\mathcal{F}$ be the set of all finite Galois extensions F' of F in $F_{\rm sep}$ such that the normalization X' of X in F' is étale. Thus, $F_{\rm et} = \bigcup_{F' \in \mathcal{F}} F'$ is a Galois extension of F and $\pi_1(X, \bar{\mathbf{x}}) \cong {\rm Gal}(F_{\rm et}/F)$ is the **fundamental group of** X **with base point** $\bar{\mathbf{x}}$. For each finite Galois extension M' of M, the variety $X_{M'} := X \times_M {\rm Spec}(M')$ is the normalization of X in FM' and it is étale. Hence, $M_{\rm sep} \subseteq F_{\rm et}$ and we obtain the following short exact sequence

$$\mathbf{1} \longrightarrow \pi_1(X_{M_{\rm sep}}, \bar{\mathbf{x}}_{\rm sep}) \longrightarrow \pi_1(X, \bar{\mathbf{x}}) \xrightarrow{\rho_X} {\rm Gal}(M) \longrightarrow \mathbf{1}\ ,$$

where $\bar{\mathbf{x}}_{\rm sep}$ is a geometric generic point of $X_{M_{\rm sep}}$ that lies over $\bar{\mathbf{x}}$ and ρ_X is the restriction map ${\rm Gal}(F_{\rm et}/F) \to {\rm Gal}(M)$.

Let $\mathcal{S}_{X/M} = \mathcal{S}_{\pi_1(X,\bar{\mathbf{x}}) \to {\rm Gal}(M)}$ be the **space of sections** of ρ_X up to $\pi_1(X_{M_{\rm sep}}, \bar{\mathbf{x}}_{\rm sep})$-conjugacy equipped with the pro-discrete topology. ∎

{PFKm}

Remark 7.3 (Profinite Kummer map)**.** Let $\mathbf{x}$ be a point in $X(M)$, let $X_{\rm et}$ be the normalization of X in $F_{\rm et}$, let $\mathbf{x}_{\rm et}$ be a point of $X_{\rm et}$ lying over $\mathbf{x}$, and let $D_{\mathbf{x}_{\rm et}/\mathbf{x}}$ be the decomposition group of $\mathbf{x}_{\rm et}$ over F. Since $\mathbf{x}$ is M-rational and is unramified in $F_{\rm et}$ (because the extensions X'/X used in Remark 6.2 to define $\pi_1(X, \bar{\mathbf{x}})$ are étale), there is an isomorphism of $D_{\mathbf{x}_{\rm et}/\mathbf{x}}$ onto ${\rm Gal}(M)$. The inverse of that isomorphism is a section s of ρ_X. As $\mathbf{x}_{\rm et}$ varies on all points of $X_{\rm et}$ that lie over $\mathbf{x}$, s ranges over a $\pi_1(X_{M_{\rm sep}}, \bar{\mathbf{x}}_{\rm sep})$-class $[s]$ of sections of ρ_X that we denote by $\kappa_{X/M}(\mathbf{x})$. Following [Sti13, p. xiv, Def. 1], we call the map

$$\kappa_{X/M}\colon X(M) \to \mathcal{S}_{X/M}$$

the **profinite Kummer map**. ∎

We provide a proof to a result communicated to us by one of the anonymous referees.

{SUBv}

Lemma 7.4. *Let X and A be geometrically integral normal varieties over a field M such that X is Zariski-closed in A. Suppose that the profinite Kummer map $\kappa_{A/M}\colon A(M) \to \mathcal{S}_{A/M}$ is injective. Then, so is $\kappa_{X/M}\colon X(M) \to \mathcal{S}_{X/M}$.*

Proof. We choose geometric generic points $\bar{\mathbf{a}}$ and $\bar{\mathbf{x}}$ for A and X, respectively. Then, the specialization $\bar{\mathbf{a}} \to \bar{\mathbf{x}}$ extends to a place $\psi_{\rm et}$ of $M(\bar{\mathbf{a}})_{\rm et}$ with residue field N that contains $M(\bar{\mathbf{x}})$ and is contained in $M(\bar{\mathbf{x}})_{\rm et}$. Since $\psi_{\rm et}$ is unramified over $M(\bar{\mathbf{a}})$, there is an isomorphism of the decomposition group of $\psi_{\rm et}$ over $M(\bar{\mathbf{a}})$ onto ${\rm Gal}(N/M(\bar{\mathbf{x}}))$. The restriction map ${\rm Gal}(M(\bar{\mathbf{x}})_{\rm et}/M(\bar{\mathbf{x}})) \to {\rm Gal}(N/M(\bar{\mathbf{x}}))$ followed by the inverse of that isomorphism is a homomorphism $\psi\colon \pi_1(X, \bar{\mathbf{x}}) \to$

$\pi_1(A, \bar{\mathbf{a}})$ such that the following diagram is commutative:

$$\begin{array}{ccc} \pi_1(A,\bar{\mathbf{a}}) & \xrightarrow{\rho_A} & \mathrm{Gal}(M) \\ {\scriptstyle\psi}\uparrow & & \| \\ \pi_1(X,\bar{\mathbf{x}}) & \xrightarrow{\rho_X} & \mathrm{Gal}(M). \end{array}$$

If s: $\mathrm{Gal}(M) \to \pi_1(X, \bar{\mathbf{x}})$ is a section of ρ_X, then $\psi \circ s$ is a section of ρ_A and $\psi(\kappa_{A/M}(\mathbf{x})) = \kappa_{A/M}(\mathbf{x})$ for each $\mathbf{x} \in X(M)$. Hence, with ψ_*: $\mathcal{S}_{X/M} \to \mathcal{S}_{A/M}$ being the map that maps the $\pi_1(X_{M_{\mathrm{sep}}}, \bar{\mathbf{x}}_{\mathrm{sep}})$-conjugacy class of s onto the $\pi_1(A_{M_{\mathrm{sep}}}, \bar{\mathbf{a}}_{\mathrm{sep}})$-conjugacy class of $\psi \circ s$, the diagram

$$\begin{array}{ccc} A(M) & \xrightarrow{\kappa_{A/M}} & \mathcal{S}_{A/M} \\ \uparrow & & \uparrow{\scriptstyle\psi_*} \\ X(M) & \xrightarrow{\kappa_{X/M}} & \mathcal{S}_{X/M} \end{array}$$

is commutative.

Consider $\mathbf{x}, \mathbf{x}'$ with $\kappa_{X/M}(\mathbf{x}) = \kappa_{X/M}(\mathbf{x}')$. Then,

$$\kappa_{A/M}(\mathbf{x}) = \psi_*(\kappa_{X/M}(\mathbf{x})) = \psi_*(\kappa_{X/M}(\mathbf{x}')) = \kappa_{A/M}(\mathbf{x}').$$

Since $\kappa_{A/M}$ is injective, we have $\mathbf{x} = \mathbf{x}'$. Hence, $\kappa_{X/M}$ is injective, as claimed. □

{SEPr}

Remark 7.5 (Linearly disjoint extensions)**.** Observe that $F_{\mathrm{et}}/FM_{\mathrm{sep}}$ is Galois, because F_{et}/F is Galois. Since F/M is regular, $FM_{\mathrm{sep}}/M_{\mathrm{sep}}$ is separable. It follows that $F_{\mathrm{et}}/M_{\mathrm{sep}}$ is a separable extension. Since $\tilde{M}/M_{\mathrm{sep}}$ is a purely inseparable extension, we conclude that F_{et} is linearly disjoint from $\tilde{M}$ over M_{sep}. ∎

The following result is due to Stix [Sti13, p. 214, Prop. 239]. We provide a proof for the convenience of the reader.

{DNSe}

Proposition 7.6. *Let M be a PAC field and let X be a geometrically integral normal variety over M. Then, the image of the profinite Kummer map $\kappa_{X/M}$ in $\mathcal{S}_{X/M}$ is dense with respect to the pro-discrete topology.*

Proof. Let H be an open subgroup of $\pi_1(X, \bar{\mathbf{x}})$ such that U_H (Remark 6.1) is non-empty. We have to prove that there exists a point $\mathbf{x} \in X(M)$ such that $\kappa_{X/M}(\mathbf{x}) \in U_H$.

Indeed, there exists a section s: $\mathrm{Gal}(M) \to \pi_1(X, \bar{\mathbf{x}})$ of the restriction map ρ_X: $\pi_1(X, \bar{\mathbf{x}}) \to \mathrm{Gal}(M)$ such that $s(\mathrm{Gal}(M)) \leq H$. In particular, $\rho_X(H) = \mathrm{Gal}(M)$. Since $s(\mathrm{Gal}(M))\pi_1(X_{M_{\mathrm{sep}}}, \bar{\mathbf{x}}_{\mathrm{sep}}) = \pi_1(X, \bar{\mathbf{x}})$, this implies that $H \cdot \pi_1(X_{M_{\mathrm{sep}}}, \bar{\mathbf{x}}_{\mathrm{sep}}) = \pi_1(X, \bar{\mathbf{x}})$.

Let F' be the fixed field of H in $F_{\rm et}$. Then, F' is a finite extension of F in $F_{\rm et}$. By the preceding paragraph, $F'M_{\rm sep} = F_{\rm et}$ and $\rho_X(\mathrm{Gal}(F_{\rm et}/F')) = \rho_X(H) = \mathrm{Gal}(M)$. Hence, F' is linearly disjoint from $M_{\rm sep}$ over M. By Remark 6.5, $F_{\rm et}$ is linearly disjoint from $\tilde{M}$ over $M_{\rm sep}$. Hence, F' is linearly disjoint from $\tilde{M}$ over M. In other words, F'/M is a regular extension.

It follows that the normalization X' of X in F' is geometrically integral [FrJ08, p. 175, Cor. 10.2.2(a)]. Since M is PAC, this implies that $X'(M) \neq \emptyset$.

We choose a point $\mathbf{x}' \in X'(M)$ and let $\mathbf{x}$ be the point of $X(M)$ below $\mathbf{x}$. Then, M is the residue field of both $\mathbf{x}$ and $\mathbf{x}'$. Hence, the decomposition group of each point of $X_{M_{\rm sep}}$ lying over $\mathbf{x}$ in $\mathrm{Gal}(F_{\rm et}/F)$ is the same as the decomposition group of each point of $X'_{M_{\rm sep}}$ lying over $\mathbf{x}'$ and the latter is contained in $\mathrm{Gal}(F_{\rm et}/F')$ which is H. It follows that $\kappa_{X/M}(\mathbf{x}) \in U_H$, as desired. □

We also cite a result of Stix [Sti13, p. 214, Prop. 241 and p. 215, Cor. 242] that generalizes a result of Koenigsmann. See [Sti13, p. 215, Cor. 242] or [Koe05, Prop. 3.1].

Proposition 7.7. *Let M be a countable ample field. Let X/M be a smooth geometrically integral variety. If $X(M) \neq \emptyset$, $\dim(X) > 0$, and $\kappa_{X/M}$ is injective, then the closure of $\mathrm{Im}(\kappa_{X/M})$ in $\mathcal{S}_{X/M}$ under the pro-discrete topology is uncountable, hence so is $\mathcal{S}_{X/M}$. In particular, $\kappa_{X/M}$ is not surjective.* {KOEn}

8 Injectiveness of the Kummer Map

{IKM}

This section contains our main result. It depends on the following lemma from [Sti20].

Lemma 8.1. *For an abelian variety A over a perfect field M the sequence* {IKMa}

$$\mathbf{0} \longrightarrow \bigcap_{n\in\mathbb{N}} nA(M) \longrightarrow A(M) \xrightarrow{\kappa_{A/M}} \mathcal{S}_{A/M}$$

is exact. Thus, $\kappa_{A/M}$ is injective if and only if $\mathrm{div}(A(M)) = \bigcap_{n\in\mathbb{N}} nA(M) = \mathbf{0}$.

Proof. By [Mil86, p. 115, Thm. 8.2], for each positive integer n, the short sequence

$$\mathbf{0} \longrightarrow A_n(\tilde{M}) \longrightarrow A(\tilde{M}) \xrightarrow{n_A} A(\tilde{M}) \longrightarrow \mathbf{0} \qquad (28)$$ {ikma}

is exact. Each term in this series is a discrete $\mathrm{Gal}(M)$-module. Since M is perfect, the fixed modules of $A_n(\tilde{M})$ and $A(\tilde{M})$ under $\mathrm{Gal}(M)$ are $A_n(M)$ and $A(M)$, respectively. Hence, (28) yields a longer exact sequence,

$$\mathbf{0} \longrightarrow A_n(M) \longrightarrow A(M) \xrightarrow{n_A} A(M) \xrightarrow{\delta_n} H^1(\mathrm{Gal}(M), A_n(\tilde{M})), \qquad (29)$$ {ikmb}

where δ_n is the first connecting homomorphism of the long exact cohomology sequence [NSW15, p. 27, Thm. 1.3.2]. The sequence (29) yields a somewhat shorter exact sequence:

$$\mathbf{0} \longrightarrow nA(M) \longrightarrow A(M) \xrightarrow{\delta_n} H^1(\mathrm{Gal}(M), A_n(\tilde{M})). \qquad (30) \quad \{\texttt{ikmc}\}$$

If $m|n$, then multiplication by $\frac{n}{m}$ gives a homomorphism

$$A_n(\tilde{M}) \overset{(n/m)_A}{\longrightarrow} A_m(\tilde{M}).$$

Taking the inverse limit on the exact sequences (30), we get a map

$$A(M) \xrightarrow{\delta} \varprojlim_{n\in\mathbb{N}} H^1(\mathrm{Gal}(M), A_n(\tilde{M})). \qquad (31) \quad \{\texttt{ikmd}\}$$

with

$$\mathrm{Ker}(\delta) = \bigcap_{n\in\mathbb{N}} \mathrm{Ker}(\delta_n) \overset{(30)}{=} \bigcap_{n\in\mathbb{N}} nA(M).$$

Indeed, for each $n \in \mathbb{N}$ let ν_n be the projection of the right hand side of (31) on its nth coordinate. If $\mathbf{a} \in \mathrm{Ker}(\delta)$, then $\delta_n(\mathbf{a}) = \nu_n(\delta(\mathbf{a})) = \nu_n(0) = 0$. Conversely, if $\delta_n(\mathbf{a}) = 0$ for each $n \in \mathbb{N}$, then $\delta(\mathbf{a}) = \varprojlim \delta_n(\mathbf{a}) = 0$.

Since $A_n(\tilde{M})$ are finite discrete $\mathrm{Gal}(M)$ modules, [NSW15, p. 142, Cor. 2.7.6] makes an identification,

$$\varprojlim_{n\in\mathbb{N}} H^1(\mathrm{Gal}(M), A_n(\tilde{M})) = H^1_{\mathrm{cts}}(\mathrm{Gal}(M), \varprojlim_{n\in\mathbb{N}} A_n(\tilde{M})), \qquad (32) \quad \{\texttt{ikmf}\}$$

where the right hand side of (32) is the first continuous cochain cohomology group of $\mathrm{Gal}(M)$ with coefficients in $\varprojlim_{n\in\mathbb{N}} A_n(\tilde{M})$ [NSW15, p. 137, Def. 2.7.1]. By [EGM19, p. 156, Cor. 10.37], there exists a canonical isomorphism

$$\varprojlim_{n\in\mathbb{N}} A_n(\tilde{M}) \cong \pi_1(A_{\tilde{M}}, \tilde{\mathbf{a}}), \qquad (33) \quad \{\texttt{ikmg}\}$$

where $\tilde{\mathbf{a}}$ is a geometrically generic point of $A_{\tilde{M}}$. Hence, (31), (32), and (33) yield the following exact sequence:

$$\mathbf{0} \longrightarrow \bigcap_{n\in\mathbb{N}} nA(M) \longrightarrow A(M) \xrightarrow{\delta} H^1_{\mathrm{cts}}(\mathrm{Gal}(M), \pi_1(A_{\tilde{M}}, \tilde{\mathbf{a}})). \qquad (34) \quad \{\texttt{ikmh}\}$$

Finally, by [Sti13, p. 72, Cor. 71], there exists an isomorphism

$$\varphi\colon \mathcal{S}_{A/M} \to H^1_{\mathrm{cts}}(\mathrm{Gal}(M), \pi_1(A_{\tilde{M}}, \tilde{\mathbf{a}}))$$

such that $\varphi \circ \kappa_{A/M} = \delta$. Hence, by the exactness of (34) the sequence

$$\mathbf{0} \longrightarrow \mathrm{div}(A(M)) \longrightarrow A(M) \overset{\kappa_{A/M}}{\longrightarrow} \mathcal{S}_{A/M}$$

is exact, as claimed. $\square$

{IKMb}

Theorem 8.2. *Let K be an infinite finitely generated field and let $e \geq 2$ be an integer. Then, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, for all finite extensions M of $\tilde{K}(\boldsymbol{\sigma})$, for all abelian varieties A over M, and for every non-empty smooth geometrically integral subvariety X of A over M, the Kummer map $\kappa_{X/M}\colon X(M) \to \mathcal{S}_{X/M}$ is injective with a pro-discrete dense image but it is not surjective.*

Proof. By Theorem 5.2(b), for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, for every finite extension M of $\tilde{K}(\boldsymbol{\sigma})$ and all abelian varieties A over M, we have $\mathrm{div}(A(M)) = \mathbf{0}$. Since by definition, $\tilde{K}(\boldsymbol{\sigma})$ is perfect, so is M. Hence, Lemma 7.1 implies that the profinite Kummer map $\kappa_{A/M}$ is injective,

It follows from Lemma 6.4 that $\kappa_{X/M}$ is injective for every smooth geometrically integral subvariety X of A. Moreover, by Theorem 5.2(a), M is PAC. In particular, $X(M) \neq \emptyset$. Therefore, by Propositions 6.6 and 6.7, $\kappa_{X/M}(X(M))$ is dense in $\mathcal{S}_{X/M}$ in the pro-discrete topology but $\kappa_{X/M}$ is not surjective. □

{IKMc}

Corollary 8.3. *Let K be an infinite finitely generated field and let $e \geq 2$. Then, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, every finite extension M of $\tilde{K}(\boldsymbol{\sigma})$, and all smooth geometrically integral projective curves C/M of genus ≥ 1, the profinite Kummer map $\kappa_{C/M}$ is injective with a dense image but it is not surjective.*

Proof. Again, by Theorem 5.2, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ every finite extension M of $\tilde{K}(\boldsymbol{\sigma})$ is PAC. Now assume that C/M is a smooth geometrically integral projective curve of genus ≥ 1. In particular $C(M) \neq \emptyset$. Hence, C embeds into its Jacobian J [Lan59, p. 40, Prop. 4]. Now apply Theorem 7.2 for C rather than for X. □

9 Injectiveness over Non-perfect Fields

{KSE}

The criterion for the injectivity of the profinite Kummer map for abelian varieties given in Lemma 7.1 depends on the assumption that the base field is perfect. Following [Sti20], we reduce the injectivity over non-perfect fields to the injectivity over perfect fields.

{KSEa}

Lemma 9.1. *Let X be a geometrically integral normal projective variety over a field M with geometric generic point $\mathbf{x}$. Let M' be a purely inseparable extension of M and consider $\mathbf{x}$ also as a generic point of $X' := X_{M'}$. Then, the canonical homomorphism $\pi_1(X', \mathbf{x}) \to \pi_1(X, \mathbf{x})$ is an isomorphism.*

Proof. By Remark 6.2,

$$\mathrm{Gal}(M(\mathbf{x})_{\mathrm{et}}/M(\mathbf{x})) \cong \pi_1(X, \mathbf{x}), \qquad \mathrm{Gal}(M'(\mathbf{x})_{\mathrm{et}}/M'(\mathbf{x})) \cong \pi_1(X', \mathbf{x}).$$

Since $M(\mathbf{x})_{\mathrm{et}}/M(\mathbf{x})$ is Galois and M'/M is purely inseparable, the restriction map

$$\rho := \mathrm{Gal}(M'(\mathbf{x})_{\mathrm{et}}/M'(\mathbf{x})) \to \mathrm{Gal}(M(\mathbf{x})_{\mathrm{et}}/M(\mathbf{x})) \tag{35}$$ {kseb}

is an epimorphism.

It remains to prove that ρ is injective. For this it suffices to prove that $M(\mathbf{x})_{\mathrm{et}} \cdot M'(\mathbf{x}) = M'(\mathbf{x})_{\mathrm{et}}$. Thus, we have to consider a finite extension N of $M'(\mathbf{x})$ in $M'(\mathbf{x})_{\mathrm{et}}$ and to find an extension L of $M(\mathbf{x})$ in $M(\mathbf{x})_{\mathrm{et}}$ such that $L \cdot M'(\mathbf{x}) = N$.

To this end we note that since $M'(\mathbf{x})_{\mathrm{sep}}$ is both separable and purely inseparable extension of $M(\mathbf{x})_{\mathrm{sep}}M'(\mathbf{x})$, we have $M'(\mathbf{x})_{\mathrm{sep}} = M(\mathbf{x})_{\mathrm{sep}}M'(\mathbf{x})$. Since $N \subseteq M'(\mathbf{x})_{\mathrm{sep}}$ we conclude that there exists a finite extension L of $M(\mathbf{x})$ in $M(\mathbf{x})_{\mathrm{sep}}$ such that $L \cdot M'(\mathbf{x}) = N$. Let $\pi\colon Y \to X$ be the normalization of X in L. Let $Y' = Y \times_X X'$ and let $\pi'\colon Y' \to X'$ be the corresponding projection. Then, π' is étale (because $N \subseteq M'(\mathbf{x})_{\mathrm{et}}$). Since $\mathrm{Spec}(M') \to \mathrm{Spec}(M)$ is flat, so is $X' \to X$. Hence, by [EGA67, p. 72, Prop. 17.7.1], π is étale. Therefore, $L \subseteq M(\mathbf{x})_{\mathrm{et}}$, as needed. □

Lemma 8.1 allows now to prove the following reduction step of [Sti20].

{KSEb}

Lemma 9.2. *Let M be a field and X a geometrically integral normal projective variety over a field M. Suppose that the profinite Kummer map $\kappa_{\mathrm{ins}} := \kappa_{X_{\mathrm{ins}}/M_{\mathrm{ins}}}\colon X_{\mathrm{ins}}(M_{\mathrm{ins}}) \to \mathcal{S}_{X_{\mathrm{ins}}/M_{\mathrm{ins}}}$ is injective. Then, the profinite Kummer map $\kappa_{X/M}\colon X(M) \to \mathcal{S}_{X/M}$ is also injective.*

Proof. We consider the following commutative square:

$$\begin{array}{ccc} X_{\mathrm{ins}}(M_{\mathrm{ins}}) & \xrightarrow{\kappa_{\mathrm{ins}}} & \mathcal{S}_{X_{\mathrm{ins}}/M_{\mathrm{ins}}} \\ {\scriptstyle\iota}\uparrow & & \downarrow{\scriptstyle\rho^*} \\ X(M) & \xrightarrow{\kappa_{X/M}} & \mathcal{S}_{X/M}, \end{array}$$

where ι is the inclusion map (taking into account that $X_{\mathrm{ins}}(M_{\mathrm{ins}}) = X(M_{\mathrm{ins}})$) and $\rho^*(s) = \rho \circ s \circ \rho_0^{-1}$ where $\rho_0\colon \mathrm{Gal}(M_{\mathrm{ins}}) \to \mathrm{Gal}(M)$ is the isomorphism defined by restriction from $\tilde{M}$ to M_{sep} and with ρ being the isomorphism appearing in (35). Since by Lemma 8.1, for $M' = M_{\mathrm{ins}}$, ρ is an isomorphism, so is ρ^*. Since by assumption, κ_{ins} is injective, this implies that $\kappa_{X/M}$ is also injective, as claimed. □

As an application we prove the variant of Theorem 7.2 where the fields $K_{\mathrm{sep}}(\boldsymbol{\sigma})$ replace the fields $\tilde{K}(\boldsymbol{\sigma})$.

{ESEc}

Theorem 9.3. *Let K be an infinite finitely generated field and let $e \geq 2$ be an integer. Then, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, for every finite extension M of $K_{\mathrm{sep}}(\boldsymbol{\sigma})$, for every abelian variety A over M, and for every non-empty smooth geometrically integral subvariety X of A over M, the profinite Kummer map $\kappa_{X/M}\colon X(M) \to \mathcal{S}_{X/M}$ is injective with a pro-discrete dense image but it is not surjective.*

Proof. We prove the theorem only for $X = A$.

Let $\boldsymbol{\sigma}$ be one of the elements of the subset of measure 1 of $\mathrm{Gal}(K)^e$ that satisfy the conclusion of Theorem 7.2. Let M be a finite extension of $K_{\mathrm{sep}}(\boldsymbol{\sigma})$

and let A be an abelian variety over M. Then, the perfect field $M_{\rm ins}$ is both separable and purely inseparable extension of $\tilde{K}(\boldsymbol{\sigma})M$. Hence, $\tilde{K}(\boldsymbol{\sigma})M = M_{\rm ins}$. In particular, $M_{\rm ins}$ is a finite extension of $\tilde{K}(\boldsymbol{\sigma})$. By our choice, the map $\kappa_{A_{\rm ins}/M_{\rm ins}}$ is injective. Therefore, by Lemma 8.2, so is the map $\kappa_{A/M}$.

In addition, we may assume by (27a) that $K_{\rm sep}(\boldsymbol{\sigma})$ is PAC and therefore so is M. Hence, by Proposition 6.6, the image of $\kappa_{A/M}$ is pro-discrete dense but according to Proposition 6.7, it is not surjective, as claimed. □

10 Finite Base Fields

{FBF}

Finite fields are not Hilbertian. Still, a variant of Theorem 7.2 does hold. That variant gives, in addition to the case $e \geq 2$, also precise information about the missing case $e = 1$.

{FBFa}

Theorem 10.1. *Let K be a finite field and let e be a positive integer. Then, the following statements hold for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, every finite extension M of $\tilde{K}(\boldsymbol{\sigma})$, and every non-zero abelian variety A over M:*

(a) *If $e = 1$, then for every smooth geometrically integral subvariety X of A over M the profinite Kummer map $\kappa_{X/M}\colon X(M) \to \mathcal{S}_{X/M}$ is injective but not surjective. Moreover, $\kappa_{X/M}$ has a pro-discrete dense image.*

(b) *If $e \geq 2$, then the Kummer map $\kappa_{A/M}\colon A(M) \to \mathcal{S}_{A/M}$ is bijective.*

Proof of (a). In order to avoid repetitions, we only prove that for every finite extension L of K, for every abelian variety A over L, and for almost all $\sigma \in \mathrm{Gal}(L)$ the Kummer map $\kappa_{A/\tilde{K}(\sigma)}\colon A(\tilde{K}(\sigma)) \to \mathcal{S}_{A/\tilde{K}(\sigma)}$ is injective but not surjective and the image of $\kappa_{A/\tilde{K}(\sigma)}$ is pro-discrete dense in $\mathcal{S}_{A/\tilde{K}(\sigma)}$.

First we observe that $A(L)$ is a finite abelian group, so every point of $A(L)$ has a finite order. In particular, for each $\sigma \in \mathrm{Gal}(L)$, we have $A(L) \cap \bigcap_{n\in\mathbb{N}} nA(\tilde{K}(\sigma)) \subseteq A_{\rm tor}(\tilde{K}(\sigma))$. By [JaJ01, Main theorem], for almost all $\sigma \in \mathrm{Gal}(L)$ and for every $l \in \mathbb{L}$, the group $A_{l^\infty}(\tilde{K}(\sigma))$ is finite. Hence, by Lemma 4.1, $A(L) \cap \mathrm{div}(A(\tilde{K}(\sigma))) = \mathbf{0}$.

Arguing as in Part B of the proof of Proposition 4.4, we find that $\mathrm{div}(A(\tilde{K}(\sigma))) = \mathbf{0}$, again for almost all $\sigma \in \mathrm{Gal}(L)$. Since $\tilde{K}(\sigma)$ is perfect, Lemma 7.1 implies that $\kappa_{A/\tilde{K}(\sigma)}\colon A(\tilde{K}(\sigma)) \to \mathcal{S}_{A/\tilde{K}(\sigma)}$ is injective.

By [FrJ08, p. 380, Cor. 18.5.9], for almost all $\sigma \in \mathrm{Gal}(K)$, the field $\tilde{K}(\sigma)$ is an infinite extension of K. As such, $\tilde{K}(\sigma)$ is PAC [FrJ08, p. 196, Cor. 11.2.4]. Hence, by Propositions 6.6 and 6.7, the map $\kappa_{A/\tilde{K}(\sigma)}$ has a dense image with respect to the pro-discrete topology, but it is not surjective.

Proof of (b). In this case $e \geq 2$. Then, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, the field $\tilde{K}(\boldsymbol{\sigma})$ is finite [FrJ08, p. 380, Cor. 18.5.9]. Hence, so is every finite extension M of $\tilde{K}(\boldsymbol{\sigma})$. Hence, by [Sti13, p. 198, Thm. 222], $\kappa_{A/M}$ is bijective, as claimed. □

References

[Bor91] A. Borel, *Linear Algebraic Groups (second enlarged edition)*, Graduate Texts in Mathematics **126**, Springer-Verlag, New York, 1991.

[BLR90] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Band 21, Springer 1990.

[Bou12] N. Bourbaki, *Algèbre, Chapitre 8, Modules et anneaux semi-simples*, N. Bourbaki et Springer-Verlag, Heidelberg 2012.

[CaF67] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press, London, 1967.

[Coh89] P. M. Cohn, *Algebra, Volume 2, second edition*, John Willy & Sons, Chichester, 1989.

[Con06] B. Conrad, *Chow's K/k-image and K/k-trace and the Lang-Néron theorem*, L'Enseignement Mathématique, **52** (2006) 37–108.

[EGA67] A. Grothendieck, *Éléments de Géométrie Algébrique IV, quateriéme partie*, Publications Mathématiques, IHES **32** (1967), 5–255.

[EGM19] B. Edixhoven, G. v. d. Geer, and B. Moonen, *Abelian varieties*, Preliminary version of the first chapters, 2019.

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Inventiones mathmaticae **73** (1983), 349–366.

[FaW84] G. Faltings and G. Wüstholz et al., *Rational Points*, Seminar Bonn/Wuppertal 1983/84, Vieweg, Braunschweig 1984.

[FrJ08] M. D. Fried and M. Jarden, *Field Arithmetic, third edition, revised by Moshe Jarden*, Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 2008.

[GeJ78] W.-D. Geyer and M. Jarden, *Torsion points of elliptic curves over large algebraic extensions of finitely generated fields*, Israel Journal of Mathematics **31** (1978), 157–197.

[Hup67] B. Huppert, *Endliche Gruppen I*, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen **134**, Springer, Berlin, 1967.

[JaJ01] M. Jacobson and M. Jarden, *Finiteness theorems for torsion of abelian varieties over large algebraic fields*, Acta Arithmetica **98** (2001), 15–31.

[Jar11] M. Jarden, *Algebraic Patching*, Springer Monographs in Mathematics, Springer, Heidelberg, 2011.

[JaP19] M. Jarden and S. Petersen, *Torsion on abelian varieties over large algebraic extensions of finitely generated extensions of* $\mathbb{Q}$, Nagoya Mathematical Journal **234** (2019), 1–41.

[Koe05] J. Koenigsmann, *On the section conjecture in anabelian geometry*, Journal für die Reine und Angewandte Mathematik **588** (2005), 221-235.

[Lan59] S. Lang, *Abelian Varieties,* Interscience Tracts in Pure and Applied Mathematics **7**, Interscience Publishers, New York, 1959.

[Lan62] S. Lang, *Diophantine Geometry,* Interscience Tracts in Pure and applied Mathematics **11**, Interscience Publishers, New York, 1962.

[Lan93] S. Lang, *Algebra (third edition),* Addison-Wesley, Reading, 1993.

[Lor08] F. Lorenz, *Algebra II, Fields with Structure, Algebras and Advanced Topics,* Springer 2008.

[Mat94] H. Matsumura, *Commutative ring theory,* Cambridge studies in advanced mathematics **8**, Cambridge University Press, Cambridge 1994.

[Mil86] J. S. Milne, *Abelian Varieties,* Chapter V in "Arithmetic Geometry", edited by G. Cornell and J. H. Silverman, Springer-Verlag, New York, 1986.

[Mil08] J. S. Milne, *Abelian Varieties,* Lecture Notes, Version 2.0, 2008 https://www.jmilne.org/math/CourseNotes/AV.pdf

[Mum74] D. Mumford, *Abelian Varieties,* Oxford University Press, London, 1974.

[Mum88] D. Mumford, *The Red Book of Varieties and Schemes,* Lecture Notes in Mathematics **1358**, Springer, Berlin, 1988.

[NSW15] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of Number Fields,* Grundlehren der mathematischen Wissenschaften **323**, Springer-Verlag, Heidelberg, Second Edition, corrected version 2.2, July 2015. Electronic Edition, https://www.mathi.uni-heidelberg.de/∼schmidt/NSW2e/NSW2.2.pdf

[Nor87] M. V. Nori, *On subgroups of* $\mathrm{GL}_n(\mathbf{F}_p)$, Inventiones mathematicae **88** (1987), 257-275.

[Poo17] B. Poonen, *Rational points on varieties,* Graduate Studies in Mathematics **186**, AMS 2017,
https://math.mit.edu/∼poonen/papers/Qpoints.pdf

[Rib79] K. Ribet, *Kummer theory on extensions of abelian varieties by tori,* Duke Mathematical Journal **46** (1979), 745–761.

[SeT68] J.-P. Serre and J. Tate, *Good reduction of abelian varieties,* Annals of Mathematics **88** (1968), 492-571.

[Shi98] G. Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions,* Princeton University Press, Princeton, 1998.

[Sti13] Jakob Stix, *Rational points and arithmetic of fundamental groups, Evidence for the section conjecture,* Lecture Notes in Mathematics **2054**, Springer, Berlin, Heidelberg, 2013.

[Sti20] Jakob Stix, *e-mail dated 20 April 2020.*

[Zar77] Y. G. Zarhin, *Endomorphisms of abelian varieties and points of finite order in characteristic p,* Mathematical Notes **21** (1977), 415–419.

[Zar85] Y. Zarhin, *A finiteness theorem for unpolarized abelian varieties over number fields with prescribed places of bad reduction,* Inventiones Mathematicae **79** (1985), 309–321.

[Zar14] Y. Zarhin, *Abelian varieties over fields of finite characteristic,* Central European Journal of Mathematics, **12** (2014), 659–675.