A RADICAL CHARACTERIZATION OF ABELIAN VARIETIES

A Dissertation

Presented to the Faculty of the Graduate School

of Cornell University

in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

by

Heung Shan Theodore Hui

August 2017

A RADICAL CHARACTERIZATION OF ABELIAN VARIETIES

Heung Shan Theodore Hui, Ph.D.

Cornell University 2017

Let A be a square-free abelian variety defined over a number field K. Let S be a density one set of prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$. A famous theorem of Faltings says that the Frobenius polynomials $P_{A,\mathfrak{p}}(x)$ for $\mathfrak{p} \in S$ determine A up to isogeny. We show that the prime factors of $|A(\mathbb{F}_\mathfrak{p})| = P_{A,\mathfrak{p}}(1)$ for $\mathfrak{p} \in S$ also determine A up to isogeny over an explicit finite extension of K. The proof relies on understanding the ℓ-adic monodromy groups which come from the ℓ-adic Galois representations of A, and the absolute Weyl group action on their weights. We also show that there exists an explicit integer $e \geq 1$ such that after replacing K by a suitable finite extension, the Frobenius polynomials of A at $\mathfrak{p}$ must equal to the e-th power of a separable polynomial for a density one set of prime ideals $\mathfrak{p} \subseteq \mathcal{O}_K$.

BIOGRAPHICAL SKETCH

Theodore Hui was born in Hong Kong. He completed his Bachelor of Science at the Chinese University of Hong Kong and his Masters at the University of Waterloo. Beside mathematics, Theodore also loves composing music and playing snooker. He owns a cute Ithacan bunny named Bubbles.

This thesis is dedicated to my parents, Alice and Nathan, who raised me, guided me, and supported my decision of choosing a career in mathematics.

ACKNOWLEDGEMENTS

I could not have completed this thesis without the guidance, support and patience from my advisor David Zywina. He suggested this project to me in February 2014, gave me detailed ideas every time when I was facing a seemingly impossible obstacle in my research. I learnt a lot not only by doing research with David, but also by observing how he fixed mistakes and polished up my thesis, especially on how to present very abstract ideas cleanly without leading to confusion. Most importantly, David kept me focused when I needed to be.

I would also like to thank my fellow graduate students Pok Wai Fong, Wai Kit Yeung and Pak Hin Li, for sharing my love of mathematics and spending time with me in Ithaca.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

Let A be a non-zero abelian variety defined over a number field K. Let Σ_K be the set of non-zero prime ideals of the ring of integers $\mathcal{O}_K$ of K. For each prime $\mathfrak{p} \in \Sigma_K$, let $\mathbb{F}_\mathfrak{p} := \mathcal{O}_K/\mathfrak{p}$ be the corresponding residue field. For all but finitely many primes $\mathfrak{p} \in \Sigma_K$, A has good reduction modulo $\mathfrak{p}$ and such a reduction gives an abelian variety $A_\mathfrak{p}$ defined over $\mathbb{F}_\mathfrak{p}$. Let $P_{A,\mathfrak{p}}(x)$ be the Frobenius polynomial of A at $\mathfrak{p}$ which we will define in §2.1. If A is isogenous to another abelian variety A' also defined over K, then one can show that $P_{A,\mathfrak{p}}(x) = P_{A',\mathfrak{p}}(x)$ for all $\mathfrak{p} \in \Sigma_K$ for which A and A' have good reduction.

Let S be a density one subset of Σ_K for which A has good reduction. A theorem of Faltings says that the function $\mathfrak{p} \in S \mapsto P_{A,\mathfrak{p}}(x)$ determines A up to isogeny [Fal86, §5, Corollary 2], i.e., if A and A' are abelian varieties defined over a number field K such that $P_{A,\mathfrak{p}}(x) = P_{A',\mathfrak{p}}(x)$ for a density 1 set of prime ideals $\mathfrak{p} \in \Sigma_K$, then A is isogenous to A' (over K). In fact, one can further show that the function $\mathfrak{p} \in S \mapsto |A(\mathbb{F}_\mathfrak{p})|$ determines A up to isogeny; note that this is a weaker condition than in Faltings' theorem since $|A(\mathbb{F}_\mathfrak{p})| = P_{A,\mathfrak{p}}(1)$. This result seems to be unknown and we will give a quick proof in §8.

Let Λ be a set of rational primes. For any integer $n \geq 1$, we define the **radical of n with respect to Λ** by

$$\mathrm{rad}_\Lambda(n) := \prod_{\ell \in \Lambda,\ \ell | n} \ell.$$

Note that when Λ is the set of all rational primes, $\mathrm{rad}(n) := \mathrm{rad}_\Lambda(n)$ is the usual definition of radical of n, i.e., the product of the distinct prime divisors of n.

Now, let Λ be a density one subset of rational primes. The main goal of this paper is to study if and when the function $\mathfrak{p} \in S \mapsto \mathrm{rad}_\Lambda |A(\mathbb{F}_\mathfrak{p})|$ determines A up to isogeny; note that this is an even weaker condition. This problem has already been studied for special classes of A, see §1.1.

The abelian variety A is isogenous to $\prod_i B_i^{e_i}$ with B_i pairwise non-isogenous simple abelian varieties defined over K and $e_i \geq 1$. It is easy to see that

$$\mathrm{rad}_\Lambda |A(\mathbb{F}_\mathfrak{p})| = \mathrm{rad}_\Lambda \left| (\prod\nolimits_i B_i)(\mathbb{F}_\mathfrak{p}) \right|$$

for all $\mathfrak{p} \in \Sigma_K$ for which A has good reduction; it does not depend on the $e_i \geq 1$. So in general, we will not be able to recover the isogeny class of A by studying $\mathrm{rad}_\Lambda |A(\mathbb{F}_\mathfrak{p})|$ for $\mathfrak{p} \in \Sigma_K$. This motivates the following definition: we say that A is **square-free** if it is non-zero and $e_i = 1$ for all i.

Let $\overline{K}$ be a fixed algebraic closure of K. Let K_A^{conn} be the minimal extension of K in $\overline{K}$ for which the ℓ-adic monodromy groups of A are connected, see §2.1. We can also characterize K_A^{conn} as the minimal extension of K in $\overline{K}$ for which K_A^{conn} is contained in the torsion field $K(A[\ell])$ for all sufficiently large primes ℓ, see [LP97, Theorem 0.1].

Our main theorem says that if A is square-free and if we replace K with K_A^{conn}, then the function $\mathfrak{p} \in S \mapsto \mathrm{rad}_\Lambda |A(\mathbb{F}_\mathfrak{p})|$ determines A up to isogeny. We will give a proof in §5.

Theorem 1.0.1. *Let A be a square-free abelian variety defined over a number field K satisfying $K_A^{\mathrm{conn}} = K$. Let Λ be a density 1 set of rational primes. Suppose A' is a square-free abelian variety defined over K for which*

$$\mathrm{rad}_\Lambda |A(\mathbb{F}_\mathfrak{p})| = \mathrm{rad}_\Lambda |A'(\mathbb{F}_\mathfrak{p})|$$

holds for all $\mathfrak{p} \in \Sigma_K$ *away from a set of density* 0. *Then* A *is isogenous to* A' *(over* K*).*

One can slightly weaken the assumption and study what happens when $\mathrm{rad}_\Lambda |A'(\mathbb{F}_\mathfrak{p})|$ divides $\mathrm{rad}_\Lambda |A(\mathbb{F}_\mathfrak{p})|$ for all $\mathfrak{p} \in S$. Although it seems stronger, we will deduce the following theorem from Theorem 1.0.1 in §6.

Theorem 1.0.2. *Let* A *be a square-free abelian variety defined over a number field* K *satisfying* $K_A^{\mathrm{conn}} = K$*; it is isogenous to* $\prod_{i=1}^r B_i$*, where* B_i *are pairwise non-isogenous simple abelian varieties defined over* K*. Let* Λ *be a density* 1 *set of rational primes. Suppose that* A' *is any abelian variety defined over* K *for which*

$$\mathrm{rad}_\Lambda |A'(\mathbb{F}_\mathfrak{p})| \text{ divides } \mathrm{rad}_\Lambda |A(\mathbb{F}_\mathfrak{p})|$$

for all $\mathfrak{p} \in \Sigma_K$ *away from a set of density* 0. *Then* A' *is isogenous to* $\prod_{i \in I} B_i^{e_i}$ *for some subset* $I \subseteq \{1, \ldots, r\}$ *and integers* $e_i \geq 1$.

Remarks 1.0.3. We do not know whether Theorems 1.0.1 and 1.0.2 hold without the assumption $K_A^{\mathrm{conn}} = K$. If A' is an abelian variety defined over K such that $\mathrm{rad}_\Lambda |A(\mathbb{F}_\mathfrak{p})| = \mathrm{rad}_\Lambda |A'(\mathbb{F}_\mathfrak{p})|$ for a density 1 set of $\mathfrak{p} \in \Sigma_K$, then one can show that we also have $\mathrm{rad}_\Lambda |A(\mathbb{F}_\mathfrak{P})| = \mathrm{rad}_\Lambda |A'(\mathbb{F}_\mathfrak{P})|$ for a density 1 set of $\mathfrak{P} \in \Sigma_{K_A^{\mathrm{conn}}}$ (see Lemma 5.1.1). Theorem 1.0.1 then implies that A and A' are isogenous over K_A^{conn}.

The methods we used in proving Theorem 1.0.1 also enable us to prove the following theorem in §7.

Theorem 1.0.4. *Let* A *be a simple abelian variety defined over* K *satisfying* $K_A^{\mathrm{conn}} = K$. *There is an integer* $e \geq 1$ *such that* $P_{A,\mathfrak{p}}(x)$ *is equal to the* e*-th power of a separable polynomial for all* $\mathfrak{p} \in \Sigma_K$ *away from a set of density* 0.

Remarks 1.0.5. We can make the integer e of Theorem 1.0.4 explicit. Define $D := \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$; it is a division algebra since A is simple. We then have $e = [D : E]^{1/2}$, where E is the center of D.

1.1 Some previous results

First, we recall some earlier known cases which are related to Theorem 1.0.1. An abelian variety A of dimension $g \geq 1$ defined over a number field K is said to be **fully of type** GSp if the image $\overline{\rho}_{A,\ell}(\mathrm{Gal}_K)$ of the mod-ℓ Galois representation of A, which we will define in §2.1, is isomorphic to $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ for sufficiently large primes ℓ. Perucca [Per15, Theorems 1.1, 1.3] proved the following theorem which extends earlier results of Hall-Perucca [HP13] and Ratazzi [Rat15, Theorem 1.3]; we state it in terms of our radical function rad_Λ.

Theorem 1.1.1. *Let A and A' be abelian varieties defined over a number field K. Let S be a set of prime ideals of $\mathcal{O}_K$ of density 1 for which A and A' have good reduction. Let Λ be an infinite set of rational primes. Suppose that $\mathrm{rad}_\Lambda |A'(\mathbb{F}_\mathfrak{p})|$ divides $\mathrm{rad}_\Lambda |A(\mathbb{F}_\mathfrak{p})|$ for all $\mathfrak{p} \in S$.*

(a) Suppose that each of A and A' is an elliptic curve or an abelian variety fully of type GSp. *Then A is isogenous to A'.*

(b) Suppose that the simple factors of both $A_{\overline{K}}$ and $A'_{\overline{K}}$ are an elliptic curve or an abelian variety fully of type GSp. *Then every simple quotient of $A'_{\overline{K}}$ is also a quotient of $A_{\overline{K}}$.*

When Λ has density 1, Theorem 1.1.1 can be deduced from Theorem 1.0.2. For example, if A is fully of type GSp (and hence $\mathrm{End}(A) = \mathrm{End}(A_{\overline{K}}) = \mathbb{Z}$), then one

can check that A is squarefree and $K_A^{\mathrm{conn}} = K$, so Theorem 1.0.2 applies. Note that it is important to assume Λ is a density 1 set of rational primes in Theorem 1.0.1 since number fields F will arise in our general proof for which we will need infinitely many $\ell \in \Lambda$ that splits completely in F.

When A and A' are products of fully of type GSp or CM elliptic curves, the Galois images $\overline{\rho}_{A\times A',\ell}(\mathrm{Gal}_K)$ (see §2.1) can be explicitly computed for all sufficiently large ℓ; in general, these images are mysterious and we will study them by using the ℓ-adic monodromy groups $G_{A\times A',\ell}$ in §3.

We also recall the following result which is related to Theorem 1.0.4. Let A be an absolutely simple abelian variety defined over a number field K. Zywina showed that if the Mumford-Tate conjecture holds for A, then for a density-one set of primes $\mathfrak{p} \in \Sigma_K$, $A_{\mathfrak{p}}$ is isogenous to some power of B where B is an absolutely simple abelian vareity defined over $\mathbb{F}_{\mathfrak{p}}$ [Zyw14]. Using Honda-Tate theory, one then shows that $P_{A,\mathfrak{p}}(x)$ is an e-th power of an irreducible polynomial for all $\mathfrak{p} \in \Sigma_K$ away from a set of density 0.

1.2 Notation

We will always denote by ℓ a rational prime. The phrase "almost all" refers to elements from a density one subset of the set of interest. For a non-zero polynomial $f(x) \in \mathbb{Q}[x]$ with factorization $f(x) = c\prod_i p_i(x)^{e_i}$ where $c \in \mathbb{Q}^\times$ and $p_i(x)$ are monic and irreducible, we define $\mathrm{rad}\, f(x) := \prod_i p_i(x)$.

Let $\overline{K}$ be a fixed algebraic closure of K. We denote by Gal_K the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ of K. For an algebraic group G defined over a field,

we will denote by G° the connected component of G which contains the identity element; it is an algebraic subgroup of G.

For a free R-module M, where R is a ring, we denote by GL_M the group scheme over R for which $\mathrm{GL}_M(B) = \mathrm{Aut}_B(B \otimes_R M)$ for each R-algebra B.

1.3 Overview

Let A and A' be non-zero abelian varieties defined over a number field K that satisfies $K_A^{\mathrm{conn}} = K$. The idea is to first study the case where A and A' are base extended to $K_{A\times A'}^{\mathrm{conn}}$ (see Proposition 5.0.1) and then show that $K_{A\times A'}^{\mathrm{conn}} = K$ (see Proposition 5.0.2).

In §2.1, we review some basics on the ℓ-adic representations $\rho_{A,\ell}$ arising from the action of Gal_K on the ℓ-power torsion points of an abelian variety A over K. To each prime ℓ, we will associate an algebraic group $G_{A,\ell}$ over $\mathbb{Q}_\ell$ which is called the ℓ-adic monodromy group. The Frobenius polynomials $P_{A,\mathfrak{p}}(x)$ arise from the images of $\rho_{A,\ell}$ and we can study them using $G_{A,\ell}$. In §2.2, we will give background on reductive groups and their weights. In §2.3, we will study a result related to Pink's work on minuscule representations.

In general, these monodromy groups $G_{A,\ell}$ are mysterious. However, after assuming that they are connected, i.e., $K_A^{\mathrm{conn}} = K$, then we know just enough properties about these groups that allow us to prove Theorem 1.0.1.

In §3, after extending K to $K_{A\times A'}^{\mathrm{conn}}$, we study the mod ℓ representations $\overline{\rho}_{A\times A',\ell}$ associated to the abelian variety $A \times A'$ for $\ell \in \Lambda$ and show that $\mathrm{rad}\, P_{A,\mathfrak{p}}(x) = \mathrm{rad}\, P_{A',\mathfrak{p}}(x)$ for all $\mathfrak{p} \in S$. In §4, we show that the Frobenius polynomials of non-

isogenous simple abelian varieties are relatively prime for almost all $\mathfrak{p} \in \Sigma_K$; the proof relies heavily on the results from §2.3. In §5.1, we will then show how to combine §3 and §4 to show that A' is isogenous to a product of simple factors of A over $K^{\mathrm{conn}}_{A\times A'}$. In §5.2, we will further show that $K^{\mathrm{conn}}_{A\times A'} = K$. This gives the proof of Theorem 1.0.1.

In §6, we will show how to use Theorem 1.0.1 to prove Theorem 1.0.2.

In §7, we will use the tools developed in §4 to give the proof of Theorem 1.0.4.

In §8, we will give a quick proof of why the function $\mathfrak{p} \in S \mapsto |A(\mathbb{F}_{\mathfrak{p}})|$ determines A up to isogeny, also as promised in the introduction.

CHAPTER 2

BACKGROUND

2.1 Galois representations

In this section, we let A be an abelian variety of dimension $g \geq 1$ defined over a number field K. For each positive integer m, let $A[m]$ be the m-torsion subgroup of $A(\overline{K})$; it is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank $2g$. Fix a prime ℓ. The **ℓ-adic Tate module** of A is the inverse limit

$$T_\ell(A) := \varprojlim_e A[\ell^e]$$

with respect to the multiplication-by-ℓ transition maps $A[\ell^{e+1}] \xrightarrow{\times \ell} A[\ell^e]$; it is a free $\mathbb{Z}_\ell$-module of rank $2g$. The absolute Galois group Gal_K naturally acts on $A[m]$ and hence also on $T_\ell(A)$. We thus have a Galois representation

$$\rho_{A,\ell} : \mathrm{Gal}_K \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A)).$$

Define $V_\ell(A) := T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$; it is a $\mathbb{Q}_\ell$-vector space of dimension $2g$. By tensoring up with $\mathbb{Q}_\ell$ and $\mathbb{F}_\ell$ respectively, $\rho_{A,\ell}$ induces Galois representations

$$\rho_{A,\ell} : \mathrm{Gal}_K \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A))$$

and

$$\overline{\rho}_{A,\ell} : \mathrm{Gal}_K \to \mathrm{Aut}_{\mathbb{F}_\ell}(A[\ell]),$$

respectively. For a prime $\mathfrak{p} \in \Sigma_K$ such that $\mathfrak{p} \nmid \ell$ and A has good reduction, $\rho_{A,\ell}$ is unramified at $\mathfrak{p}$, and the **Frobenius polynomial** of $\mathfrak{p}$ is defined by

$$P_{A,\mathfrak{p}}(x) := \det(xI - \rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p}));$$

it is a monic polynomial of degree $2g$ with integer coefficients and is independent of ℓ. Note that $P_{A,\mathfrak{p}}(x)$ also agrees with the characteristic polynomial of the Frobenius endomorphism $\pi_{A_\mathfrak{p}}$ of $A_\mathfrak{p}$, where $A_\mathfrak{p}$ is the reduction of A modulo $\mathfrak{p}$, i.e., the unique polynomial $P(x) \in \mathbb{Z}[x]$ such that the isogeny $n - \pi_{A_\mathfrak{p}}$ of A has degree $P(n)$ for all integers n. We have $P_{A,\mathfrak{p}}(1) = \deg(1 - \pi_{A_\mathfrak{p}}) = |A(\mathbb{F}_\mathfrak{p})|$. Note that we also have

$$P_{A,\mathfrak{p}}(x) \equiv \det(xI - \overline{\rho}_{A,\ell}(\mathrm{Frob}_\mathfrak{p})) \pmod{\ell}$$

for all $\mathfrak{p} \nmid \ell$ for which A has good reduction.

Let $\mathcal{G}_{A,\ell}$ be the Zariski closure of $\rho_{A,\ell}(\mathrm{Gal}_K)$ in $\mathrm{GL}_{T_\ell(A)}$; it is a group scheme over $\mathbb{Z}_\ell$. The generic fibre $G_{A,\ell} := (\mathcal{G}_{A,\ell})_{\mathbb{Q}_\ell}$ agrees with the Zariski closure of $\rho_{A,\ell}(\mathrm{Gal}_K)$ in $\mathrm{GL}_{V_\ell(A)}$; it is an algebraic subgroup of $\mathrm{GL}_{V_\ell(A)}$ called the **ℓ-adic algebraic monodromy group** of A. The special fibre $H_{A,\ell} := (\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$ is an algebraic subgroup of $\mathrm{GL}_{A[\ell]}$ and we have $\overline{\rho}_{A,\ell}(\mathrm{Gal}_K) \subseteq H_{A,\ell}(\mathbb{F}_\ell)$.

Let K_A^{conn} be the fixed field in $\overline{K}$ of the subgroup $(\rho_{A,\ell})^{-1}(G^\circ_{A,\ell}(\mathbb{Q}_\ell))$ of Gal_K; it is the minimal Galois extension L of K for which $G_{A_L,\ell}$ is connected (it will equal $G^\circ_{A,\ell}$).

Proposition 2.1.1. *The number field K_A^{conn} is independent of the choice of ℓ. In particular, $K_A^{\mathrm{conn}} = K$ if and only if all the ℓ-adic monodromy groups $G_{A,\ell}$ are connected.*

Proof. See Serre [Ser00, #133 p.17] and [LP97]. □

Note that if A and A' are abelian varieties defined over the number field K, then $K_{A\times A'}^{\mathrm{conn}} \supseteq K_A^{\mathrm{conn}} \cdot K_{A'}^{\mathrm{conn}}$.

Proposition 2.1.2. *Assume that $K_A^{conn} = K$. Then the $\mathbb{Z}_\ell$-group scheme $\mathcal{G}_{A,\ell}$ is*

reductive for all sufficiently large ℓ. The algebraic group $H_{A,\ell}$ is connected and reductive for all sufficiently large ℓ.

Proof. Reductiveness of $\mathcal{G}_{A,\ell}$ was proved in [LP97]; see also [Win02, §1.3] for a minor correction of the proof. Connectedness of $H_{A,\ell}$ follows from the reductiveness of $\mathcal{G}_{A,\ell}$ and the connectedness of $G_{A,\ell}$. □

For a reductive algebraic group G over a field, we say that G is **split** if it contains a split maximal torus. One can find a more precise definition in the next section. Here are some properties concerning $H_{A,\ell}$ related to Serre's work which will be useful in §3; in particular, part (a) shows that $\overline{\rho}_{A,\ell}(\mathrm{Gal}_K)$ "almost equals" $H_{A,\ell}(\mathbb{F}_\ell)$.

Theorem 2.1.3. *Assume that $K_A^{conn} = K$.*

(a) There exists a constant M_A, depending only on A, such that $[H_{A,\ell}(\mathbb{F}_\ell) : \overline{\rho}_{A,\ell}(\mathrm{Gal}_K)] \leq M_A$ for all ℓ.

(b) For ℓ sufficiently large, $H_{A,\ell}$ is connected, reductive and contains the group $\mathbb{G}_m$ of homotheties.

(c) There is a finite Galois extension F of $\mathbb{Q}$ such that $H_{A,\ell}$ is split for all sufficiently large ℓ that splits completely in F.

Proof. In Serre's 1985–1986 course at the Collège de France [Ser00, #136], he constructed for each prime ℓ a connected, reductive algebraic subgroup of $\mathrm{GL}_{A[\ell]} = \mathrm{GL}_{T_\ell(A),\mathbb{F}_\ell}$ that satisfies all the properties as stated in (a) and (b). Wintenberger [Win02, §3.4] showed that this subgroup is isomorphic to the connected component of $H_{A,\ell}$ when ℓ is sufficiently large. For more details, one can refer to [Ser00, #137], [Ser00, #138], [Win02] and [Zyw14, Proposition 2.10].

For (c), see [Zyw16, Lemma 3.2]. □

The following results concerning $\rho_{A,\ell}$ will be useful in §4.

Theorem 2.1.4 (Faltings)**.**

(a) The Galois representation $\rho_{A,\ell} : \mathrm{Gal}_K \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A))$ *is semisimple.*

(b) For abelian varieties A *and* A' *defined over* K*, the natural homomorphism*

$$\mathrm{Hom}(A, A') \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \to \mathrm{Hom}_{\mathbb{Q}_\ell[\mathrm{Gal}_K]}(V_\ell(A), V_\ell(A'))$$

is an isomorphism. In particular, $\mathrm{End}_{\mathbb{Q}_\ell[\mathrm{Gal}_K]}(V_\ell(A))$ *is isomorphic to* $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$*.*

(c) The group $G^\circ_{A,\ell}$ *is reductive.*

Proof. See [Fal86, Theorems 3–4]. □

Lemma 2.1.5. *Assume that* $K_A^{conn} = K$*.*

(a) Then we have $\mathrm{End}(A_{\overline{K}}) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$*.*

(b) For any simple abelian subvariety B *of* A*, the abelian variety* $B_{\overline{K}}$ *is also simple.*

Proof. For (a), see [Zyw14, Proposition 2.2 (iii)]. For (b), let B/K be a simple abelian subvariety of A. Suppose $B_{\overline{K}}$ is not simple. Then there exists $\phi \in \mathrm{End}(A_{\overline{K}})$ such that $\phi(A_{\overline{K}})$ is a non-zero proper abelian subvariety of $B_{\overline{K}}$. By (a), ϕ is defined over K and so $\phi(A)$ is a non-zero proper abelian subvariety of B. This contradicts our assumption that B is simple. □

2.2 Reductive groups and weights

Let G be a connected reductive group defined over a perfect field k and fix an algebraic closure $\overline{k}$ of k. A **torus** of G is an algebraic subgroup $T \subseteq G$ such that $T_{\overline{k}}$ is isomorphic to $(\mathbb{G}_m)^r_{\overline{k}}$ for some integer $r \geq 0$. We say that T is **split** if it is isomorphic to $(\mathbb{G}_m)^r_k$. A **maximal torus** of G is a torus T of G that is not contained in any larger torus of G; the torus $T_{\overline{k}}$ is a maximal torus of $G_{\overline{k}}$. Since G is a reductive group, any two maximal tori of $G_{\overline{k}}$ are conjugate to each other by some element of $G(\overline{k})$. The **rank** r of G is the dimension of any maximal torus. We say that G is **split** if it contains a split maximal torus.

Fix a maximal torus T of G. Denote by $X(T)$ the group of characters $T_{\overline{k}} \to (\mathbb{G}_m)_{\overline{k}}$; it is a free abelian group of rank r. The **(absolute) Weyl group** of G with respect to T is defined as

$$W(G,T) := N_G(T)(\overline{k})/T(\overline{k})$$

where $N_G(T)$ is the normalizer of T in G. For $n \in N_G(T)(\overline{k})$, the homomorphism $\iota_n : T_{\overline{k}} \to T_{\overline{k}}$ defined by $t \mapsto ntn^{-1}$ gives an automorphism $\alpha \mapsto \alpha \circ (\iota_n)^{-1}$ of $X(T)$. This gives a faithful left action of $W(G,T)$ on $X(T)$.

Suppose we have a representation $\rho : G \to \mathrm{GL}_V$ where V is a finite dimensional vector space over k. For each character $\alpha \in X(T)$, let $V(\alpha)$ be the subspace of $V \otimes_k \overline{k}$ consisting of those vectors v for which $\rho(t) \cdot v = \alpha(t)v$ for all $t \in T(\overline{k})$. We say that $\alpha \in X(T)$ is a **weight** of ρ if $V(\alpha) \neq 0$, and we denote the (finite) set of such weights by $\Omega(\rho)$ or $\Omega(V)$. Note that $W(G,T)$ acts on $\Omega(V)$. We have a decomposition $V \otimes_k \overline{k} = \bigoplus_{\alpha \in \Omega(V)} V(\alpha)$ and hence for each $t \in T(\overline{k})$, the

characteristic polynomial of $\rho(t)$ is given by

$$\det(xI - \rho(t)) = \prod_{\alpha \in \Omega(V)} (x - \alpha(t))^{m_\alpha}$$

where $m_\alpha := \dim_{\overline{k}} V(\alpha)$ is the **multiplicity** of α. Note that $m_\alpha = m_\beta$ if α and β are in the same $W(G,T)$-orbit.

2.3 Weak Mumford-Tate pairs and minuscule representations

Let F be a field of characteristic zero. Suppose G is a connected reductive algebraic group over F with a faithful representation $\rho : G \hookrightarrow \mathrm{GL}_U$ where U is a finite dimensional F-vector space. We have an isomorphism $X(\mathbb{G}_m) = \mathbb{Z}$, where an integer $n \in \mathbb{Z}$ corresponds to the character $t \mapsto t^n$.

Definition 2.3.1. The pair (G, ρ) is called a **weak Mumford-Tate pair with weights** $\{0, 1\}$ if there exists a set of cocharacters $\{\mu : (\mathbb{G}_m)_{\overline{F}} \to G_{\overline{F}}\}$ such that

(i) $G_{\overline{F}}$ is generated by the images of the $G(\overline{F})$-conjugates of all μ, and

(ii) the weights of each $\rho \circ \mu$ are in $\{0, 1\}$.

Fix a maximal torus T of G. Let $W(G,T)$ be the (absolute) Weyl group of G with respect to T. Recall that $W(G,T)$ acts on $\Omega(\rho) \subseteq X(T)$. In order to study how $W(G,T)$ acts on $\Omega(\rho)$ when (G, ρ) is a weak Mumford-Tate pair, we will also need the following definition.

Definition 2.3.2. We say that an irreducible representation $\rho : G \to \mathrm{GL}_U$ is **minuscule** if the Weyl group $W(G,T)$ acts transitively on the weights of ρ, i.e., the weights of ρ form a single orbit under the action of the Weyl group $W(G,T)$.

See [Bou05, Ch.VIII §3] for an equivalent definition of minuscule using $\Omega(U)$-saturations.

If F is algebraically closed, then (G, ρ) being minuscule implies that all the weights of ρ must have multiplicity 1 since there exists a highest weight of multiplicity 1 for ρ (see for example [Hum75, §31.3]). We obtained the proof of the following theorem by collecting ideas from Serre [Ser79, §3] and Pink [Pin98, §4].

Theorem 2.3.3. *Suppose G is a connected reductive group over F with a faithful representation $\rho : G \hookrightarrow \mathrm{GL}_U$ where U is a finite dimensional F-vector space. If (G, ρ) is a weak Mumford-Tate pair of weights $\{0, 1\}$, then each irreducible representation $V \subseteq U \otimes_F \overline{F}$ of $G_{\overline{F}}$ is minuscule.*

Proof. First of all, (G, ρ) remains a weak Mumford-Tate pair if we base extend F to $\overline{F}$, so without loss of generality we may assume that $F = \overline{F}$.

Consider an irreducible subrepresentation $\rho_V : G \to \mathrm{GL}_V$ of ρ. Let $G_0 := Z$ denote the identity component of the center of G. If $G \neq Z$, let $G_1, \ldots, G_s$ denote the minimal closed connected normal subgroups of the derived group G^{der} with positive dimension. Each G_i is almost simple. We then have an almost direct product $G = G_0 \cdot G_1 \cdots G_s$ (see for example [Hum75, §27.5]). So multiplication gives a homomorphism

$$\phi : G_0 \times G_1 \times \cdots \times G_s \to G = G_0 \cdot G_1 \cdots G_s$$

with finite kernel (contained in the center of G since $\mathrm{char}(F) = 0$). Moreover, since ρ_V is irreducible, there exists irreducible representations $\rho_i : G_i \to \mathrm{GL}_{V_i}$ for some finite dimensional F-vector spaces V_i, such that $\rho_V \simeq \rho_0 \otimes \cdots \otimes \rho_s$. We can assume that $V = V_0 \otimes \cdots \otimes V_s$.

For each i, choose a maximal torus $T_i \subseteq G_i$. Then $\prod_i T_i$ is a maximal torus of $\prod_i G_i$. Let $T = T_0 \cdots T_s$ (i.e., the image of $\prod T_i$ under ϕ); it is a maximal torus of G. Let $\Omega(V_i)$ be the set of weights with respect to ρ_i.

The homomorphism ϕ induces an isomorphism between $W(\prod G_i, \prod T_i) = \prod W(G_i, T_i)$ and $W(G, T)$; this uses that the kernel of ϕ is finite and contained inside the center of $\prod G_i$. Note that the restriction $\prod T_i \to T$ of ϕ induces an isomorphism $X(T) \otimes_{\mathbb{Z}} \mathbb{Q} \xrightarrow{\sim} \prod X(T_i) \otimes_{\mathbb{Z}} \mathbb{Q}$ and gives a bijection $\Omega(V) \simeq \prod \Omega_i(V_i)$, for which the actions of $W(G, T)$ and $\prod W(G_i, T_i)$ are compatible. Hence, to show that the representation $\rho_V : G \to \mathrm{GL}_V$ is minuscule, i.e., $W(G, T)$ acts transitively on $\Omega(V)$, it suffices to show that $W(G_i, T_i)$ acts transitively on each $\Omega(V_i)$.

When $i = 0$, V_0 is one-dimensional since G_0 is a torus. So $W(G_0, T_0)$ acts transitively on the one element set $\Omega(V_0)$. In particular, when $G = Z$, the theorem is true.

Assume that $G \neq Z$ and consider $i > 0$; note that the kernel of ρ_i is either finite or G_i, since G_i is almost simple. If $\ker(\rho_i)$ is G_i, then $W(G_i, T_i)$ acts transitively on the one element set $\Omega(V_i)$. For each i, let $\tilde{G}_i$ be the image of $G_i \hookrightarrow \prod G_i \xrightarrow{\rho_V \circ \phi} \mathrm{GL}_V$. Let I be the set of $i > 0$ for which $\ker(\rho_i)$ is finite. Fix $i \in I$, we have an isogeny $\phi_i : G_i \to \tilde{G}_i$. The image $\tilde{T}_i$ of T_i under ϕ_i is a maximal torus of $\tilde{G}_i$. The isogeny ϕ_i induces isomorphisms $X(\tilde{T}_i) \otimes_{\mathbb{Z}} \mathbb{Q} \xrightarrow{\sim} X(T_i) \otimes_{\mathbb{Z}} \mathbb{Q}$ and hence an isomorphism $W(G_i, T_i) \xrightarrow{\sim} W(\tilde{G}_i, \tilde{T}_i)$.

The image of ρ_V is a reductive group with almost direct product decomposition $\tilde{G}_0 \cdot \prod_{i \in I} \tilde{G}_i$. Moreover, the $W(G_i, T_i)$ and $W(\tilde{G}_i, \tilde{T}_i)$ actions on $\Omega(V_i)$ are compatible with respect to these isomorphisms. Hence, to show that the representation $\rho_V : G \to \mathrm{GL}_V$ is minuscule, it suffices to show that $W(\tilde{G}_i, \tilde{T}_i)$ acts transitively on

$\Omega(V_i)$ for each $i \in I$.

By [Pin98, §4], since $(G/\ker\rho_V \simeq \tilde{G}_0 \cdot \prod_{i\in I}\tilde{G}_i, \rho_V)$ is a weak Mumford-Tate pair, we have $\tilde{G}_0 = \mathbb{G}_m$ (i.e., the homotheties) and $(\tilde{G}_0 \cdot \tilde{G}_i, \tilde{G}_0 \cdot \tilde{G}_i \hookrightarrow \mathrm{GL}_{V_0\otimes V_i})$ is a weak Mumford-Tate pair for each $i \in I$. In [Pin98, Table 4.2], Pink listed all the possibilities for $(\tilde{G}_i, \tilde{G}_i \hookrightarrow \mathrm{GL}_{V_i})$ and in each case $\tilde{G}_i \hookrightarrow \mathrm{GL}_{V_i}$ is a minuscule representation. This proves the theorem. □

Remark 2.3.4. A **strong Mumford-Tate pair** is a weak Mumford-Tate pair together with the extra condition that all the given cocharacters are contained in a single $\mathrm{Aut}(\overline{F}/F)$-orbit. In [Ser79, §3], Serre focused on the proof of Theorem 2.3.3 for strong Mumford-Tate pairs. However, in [Orr15], Orr pointed out that this extra condition was not being used in the proof. This is also clear from our discussion above. (Note that Orr considered Mumford-Tate triples instead of Mumford-Tate pairs by making the cocharacter set explicit in his paper.)

Let A be any abelian variety defined over a number field K. For every prime ℓ, let $\iota_{A,\ell} : G_{A,\ell} \hookrightarrow \mathrm{GL}_{V_\ell(A)}$ be the tautological representation of the ℓ-adic monodromy group. On the other hand, the first ℓ-adic étale cohomology group $H := H^1_{\text{ét}}(A_{\overline{K}}, \mathbb{Q}_\ell)$ of A is isomorphic to the dual of $V_\ell(A)$. The Gal_K-action on H gives a continuous representation

$$\rho' : \mathrm{Gal}_K \to \mathrm{GL}_H$$

which is dual to the representation $\rho_{A,\ell}$. Let $\iota^\vee_{A,\ell} : G_{A,\ell} \hookrightarrow \mathrm{GL}_H$ be the faithful representation induced by ρ' and the duality. Note that $\rho'(\mathrm{Gal}_K)$ is Zariski dense in $\iota^\vee_{A,\ell}(G_{A,\ell})$. Pink proved the following result in [Pin98, Theorem (5.10)], which will be a main ingredient in the proofs of Theorem 1.0.1 and Theorem 1.0.4.

Theorem 2.3.5 (Pink)**.** *Let A be an abelian variety defined over a number field K.*

Suppose $K_A^{\mathrm{conn}} = K$. Then for every prime ℓ, $(G_{A,\ell}, \iota_{A,\ell}^{\vee})$ is a weak Mumford-Tate pair of weights $\{0,1\}$.

Proposition 2.3.6. *Let A be an abelian variety defined over a number field K. Suppose that $K_A^{\mathrm{conn}} = K$. Then each irreducible representation $V \subseteq V_\ell(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell$ of $(G_{A,\ell})_{\overline{\mathbb{Q}}_\ell}$ is minuscule.*

Proof. By Theorem 2.3.5, $(G_{A,\ell}, \iota_{A,\ell}^{\vee})$ is a weak Mumford-Tate pair of weights $\{0,1\}$ over $\mathbb{Q}_\ell$. By Theorem 2.3.3, each irreducible component of the dual representation $\iota_{A,\ell}^{\vee} : (G_{A,\ell})_{\overline{\mathbb{Q}}_\ell} \hookrightarrow \mathrm{GL}_{H \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell}$ is minuscule and therefore the same also holds for $\iota_{A,\ell}$. □

CHAPTER 3

RADICALS OF FROBENIUS POLYNOMIALS

Let A and A' be non-zero abelian varieties defined over a number field K of dimensions g and g' respectively. We assume throughout the section that the ℓ-adic monodromy groups $G_{A\times A',\ell}$ are connected, i.e., $K^{\mathrm{conn}}_{A\times A'} = K$.

Let S be a set of prime ideals of $\mathcal{O}_K$ of density 1 for which A and A' have good reduction. Suppose there is a density 1 set Λ of rational primes such that $\mathrm{rad}_\Lambda |A(\mathbb{F}_\mathfrak{p})|$ divides $\mathrm{rad}_\Lambda |A'(\mathbb{F}_\mathfrak{p})|$ for all $\mathfrak{p} \in S$. The goal of this section is to build up tools for proving the following result, which will be proved in §3.5.

Proposition 3.0.1. *The polynomial* $\mathrm{rad}\, P_{A,\mathfrak{p}}(x)$ *divides* $\mathrm{rad}\, P_{A',\mathfrak{p}}(x)$ *for all prime* $\mathfrak{p} \in S$.

3.1 Setup

For each prime ℓ, we define $H_\ell := (\mathcal{G}_{A\times A',\ell})_{\mathbb{F}_\ell}$ as in §2. By Proposition 2.1.2 and the assumption $K^{\mathrm{conn}}_{A\times A'} = K$, the group H_ℓ is connected when ℓ is sufficiently large. Recall that we have Galois representations $\overline{\rho}_{A\times A',\ell} : \mathrm{Gal}_K \to H_\ell(\mathbb{F}_\ell)$. We can identify H_ℓ with a closed algebraic subgroup of $(\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell} \times (\mathcal{G}_{A',\ell})_{\mathbb{F}_\ell}$.

Lemma 3.1.1. *For every* $\ell \in \Lambda$ *and* $(B, B') \in \overline{\rho}_{A\times A',\ell}(\mathrm{Gal}_K)$, *if* $\det(I - B) = 0$, *then* $\det(I - B') = 0$.

Proof. Take any $(B, B') \in \overline{\rho}_{A\times A',\ell}(\mathrm{Gal}_K)$. By the Chebotarev density theorem, there exists a prime $\mathfrak{p} \in S$ with $\mathfrak{p} \nmid \ell$ such that $\overline{\rho}_{A\times A',\ell}(\mathrm{Frob}_\mathfrak{p}) =$

$(\overline{\rho}_{A,\ell}(\mathrm{Frob}_{\mathfrak{p}}), \overline{\rho}_{A',\ell}(\mathrm{Frob}_{\mathfrak{p}}))$ is conjugate to (B, B') in $H_\ell(\mathbb{F}_\ell)$. Therefore, $\det(I-B) = 0$ if and only if $\det(I - \overline{\rho}_{A,\ell}(\mathrm{Frob}_{\mathfrak{p}})) = 0$. Since

$$\det(I - \overline{\rho}_{A,\ell}(\mathrm{Frob}_{\mathfrak{p}})) \equiv P_{A,\mathfrak{p}}(1) \equiv |A(\mathbb{F}_{\mathfrak{p}})| \pmod{\ell},$$

we find that $\det(I-B) = 0$ if and only if ℓ divides $|A(\mathbb{F}_{\mathfrak{p}})|$. Similarly, $\det(I-B') = 0$ if and only if ℓ divides $|A'(\mathbb{F}_{\mathfrak{p}})|$. The lemma follows from the assumption that $\mathrm{rad}_\Lambda |A(\mathbb{F}_{\mathfrak{p}})|$ divides $\mathrm{rad}_\Lambda |A'(\mathbb{F}_{\mathfrak{p}})|$ for all $\mathfrak{p} \in S$, i.e., for all $\ell \in \Lambda$ and $\mathfrak{p} \in S$, if $|A(\mathbb{F}_{\mathfrak{p}})|$ is divisible by ℓ, then so is $|A'(\mathbb{F}_{\mathfrak{p}})|$. □

Define

$$\mathcal{V}_\ell := \{(B, B') \in H_\ell : \ \det(I - B) = 0\}$$

and

$$\mathcal{V}'_\ell := \{(B, B') \in H_\ell : \ \det(I - B') = 0\};$$

they are closed subvarieties of H_ℓ defined over $\mathbb{F}_\ell$. The above definitions were motivated by Lemma 3.1.1, which says that

$$\mathcal{V}_\ell(\mathbb{F}_\ell) \cap \overline{\rho}_{A\times A',\ell}(\mathrm{Gal}_K) \subseteq \mathcal{V}'_\ell(\mathbb{F}_\ell) \cap \overline{\rho}_{A\times A',\ell}(\mathrm{Gal}_K). \tag{3.1.1}$$

We will first prove the following proposition in §3.4; it will be a key ingredient in our proof of Proposition 3.0.1 in §3.5.

Proposition 3.1.2. *We have $\mathcal{V}_\ell \subseteq \mathcal{V}'_\ell$ for infinitely many $\ell \in \Lambda$.*

The following lemma says the varieties $\mathcal{V}_\ell \cap \mathcal{T}_\ell$ and $\mathcal{V}'_\ell \cap \mathcal{T}_\ell$, with $\mathcal{T}_\ell$ a maximal torus of H_ℓ, carry enough information to prove Proposition 3.1.2.

Lemma 3.1.3. *Take any $\ell \in \Lambda$ such that H_ℓ is reductive. Let $\mathcal{T}_\ell$ be a maximal torus of H_ℓ. If $\mathcal{V}_\ell \cap \mathcal{T}_\ell \subseteq \mathcal{V}'_\ell \cap \mathcal{T}_\ell$, then $\mathcal{V}_\ell \subseteq \mathcal{V}'_\ell$.*

Proof. Take any $(B, B') \in \mathcal{V}_\ell(\overline{\mathbb{F}}_\ell)$; we have $\det(I - B) = 0$. By the multiplicative Jordan decomposition, $(B, B') \in H_\ell(\overline{\mathbb{F}}_\ell)$ can be expressed uniquely in the form $(B_s, B'_s)(B_u, B'_u)$ with commuting (B_s, B'_s) and $(B_u, B'_u) \in H_\ell(\overline{\mathbb{F}}_\ell)$ such that (B_s, B'_s) is semisimple and (B_u, B'_u) is unipotent. In $H_\ell(\overline{\mathbb{F}}_\ell)$, (B_s, B'_s) is conjugate to some element (C_s, C'_s) of $\mathcal{T}_\ell(\overline{\mathbb{F}}_\ell)$. Note that we have

$$\det(I - C_s) = \det(I - B_s) = \det(I - B) = 0$$

and so $(C_s, C'_s) \in \mathcal{V}_\ell \cap \mathcal{T}_\ell$. By our assumption that $\mathcal{V}_\ell \cap \mathcal{T}_\ell \subseteq \mathcal{V}'_\ell \cap \mathcal{T}_\ell$, we have $(C_s, C'_s) \in \mathcal{V}'_\ell \cap \mathcal{T}_\ell$ and so

$$\det(I - B') = \det(I - B'_s) = \det(I - C'_s) = 0.$$

Hence, $(B, B') \in \mathcal{V}'_\ell(\overline{\mathbb{F}}_\ell)$. Since (B, B') is arbitrary, we have $\mathcal{V}_\ell(\overline{\mathbb{F}}_\ell) \subseteq \mathcal{V}'_\ell(\overline{\mathbb{F}}_\ell)$ and hence $\mathcal{V}_\ell \subseteq \mathcal{V}'_\ell$. □

3.2 Strategy

We will briefly give some ideas behind the proof of Proposition 3.1.2. We will not use this section later.

For $\ell \in \Lambda$, let $\mathcal{T}_\ell$ be a maximal torus of H_ℓ. By Lemma 3.1.3, it suffices to prove that $\mathcal{V}_\ell \cap \mathcal{T}_\ell \subseteq \mathcal{V}'_\ell \cap \mathcal{T}_\ell$.

Take any irreducible component C of $\mathcal{V}_\ell \cap \mathcal{T}_\ell$. We want to show that $C \subseteq \mathcal{V}'_\ell \cap \mathcal{T}_\ell$, this will imply $\mathcal{V}_\ell \cap \mathcal{T}_\ell \subseteq \mathcal{V}'_\ell \cap \mathcal{T}_\ell$ since C is arbitrary. Suppose on the contrary that $C \not\subseteq \mathcal{V}'_\ell \cap C$, since C is irreducible, $\dim(\mathcal{V}'_\ell \cap C) < \dim(C)$. The main idea is to study the set

$$\Gamma_\ell := C(\mathbb{F}_\ell) \cap \overline{\rho}_{A \times A', \ell}(\mathrm{Gal}_K).$$

and try to bound the cardinality $\gamma_\ell := |\Gamma_\ell|$ from below and above and to hope for a contradiction for well-chosen primes $\ell \in \Lambda$ and tori $\mathcal{T}_\ell$.

1. Theorem 2.1.3(a) says that the index of $\overline{\rho}_{A\times A',\ell}(\mathrm{Gal}_K)$ in $H_\ell(\mathbb{F}_\ell)$ is bounded independent of ℓ. So one might expect γ_ℓ to be roughly of size $|C(\mathbb{F}_\ell)|$. Then by an application of the Weil conjectures, one would expect that $|C(\mathbb{F}_\ell)|$ is roughly equal to $\ell^{\dim(C)}$, assuming C is absolutely irreducible. Hence, $\gamma_\ell \gg \ell^{\dim(C)}$ and this gives a lower bound of γ_ℓ with a constant yet to be controlled.

2. By equation (3.1.1), we have

$$\Gamma_\ell \subseteq (C \cap \mathcal{V}'_\ell)(\mathbb{F}_\ell) \cap \overline{\rho}_{A\times A',\ell}(\mathrm{Gal}_K) \subseteq (C \cap \mathcal{V}'_\ell)(\mathbb{F}_\ell).$$

   Then again from the Weil conjectures one would expect that $|(C \cap \mathcal{V}'_\ell)(\mathbb{F}_\ell)|$ is $O(\ell^{\dim(C\cap\mathcal{V}'_\ell)})$. Hence, $\gamma_\ell \ll \ell^{\dim(C\cap\mathcal{V}'_\ell)} \leq \ell^{\dim(C)-1}$ and this gives a upper bound of γ_ℓ with a constant yet to be controlled.

We need to ensure that the implicit constants of (1) and (2) do not depend on ℓ; we then have $\ell^{\dim C} \ll \ell^{\dim C-1}$ where the error term is independent of ℓ. This would then give a contradiction for ℓ large enough. We will restrict our attention to ℓ in an infinite subset $\Lambda_0 \subseteq \Lambda$ constructed in §3.3.

3.3 The set Λ_0

Suppose ℓ is a prime for which H_ℓ is reductive and split. Choose a split maximal torus $\mathcal{T}_\ell \subseteq H_\ell$.

By choosing a basis for $(A \times A')[\ell]$, we can identify H_ℓ with an algebraic subgroup of $\mathrm{GL}_{2g+2g',\mathbb{F}_\ell}$ and we may assume that $\mathcal{T}_\ell$ lies in the diagonal. We have identified $\mathcal{T}_\ell$ with a closed subgroup of the diagonal which we identify with $\mathbb{G}_m^{2g+2g'}$; the diagonal of $\mathrm{GL}_{2g+2g'}$.

For each $1 \leq i \leq 2g$, we define $Z_{\ell,i}$ to be the algebraic subgroup $\mathcal{T}_\ell \cap \{x_i = 1\}$ of $\mathcal{T}_\ell$. Note that

$$\mathcal{V}_\ell \cap \mathcal{T}_\ell = \bigcup_{i=1}^{2g} Z_{\ell,i}.$$

Let C be any irreducible component (defined over $\mathbb{F}_\ell$) of $Z_{\ell,i}$. Theorem 2.1.3(a) says that the index $[H_\ell(\mathbb{F}_\ell) : \overline{\rho}_{A\times A',\ell}(\mathrm{Gal}_K)]$ is bounded by a number $M_{A\times A'}$ which does not depend on ℓ. For each positive integer $m \leq M_{A\times A'}$, define the subvariety $C_m := \{x \in \mathcal{T}_\ell : \ x^m \in C\}$ of $\mathcal{T}_\ell$; note that $\dim C_m = \dim C$.

Definition 3.3.1. Let $\{V_i\}_{i\in I}$ be a collection of affine varieties with V_i defined over a finite field $\mathbb{F}_{\ell_i}$. We say that $\{V_i\}_{i\in I}$ has **bounded complexity** if V_i is isomorphic to a closed subvariety of $\mathbb{A}^n_{\mathbb{F}_{\ell_i}}$ defined by the simultaneous vanishing of r polynomials in $\mathbb{F}_{\ell_i}[x_1, \cdots, x_n]$ each of degree at most D, where the integers n, r and D can be bounded independent of $i \in I$.

Lemma 3.3.2. *There is a positive density subset $\Lambda_0 \subseteq \Lambda$ such that the following hold:*

- *H_ℓ is reductive and split for all $\ell \in \Lambda_0$.*
- *For each prime $\ell \in \Lambda_0$, irreducible component C of $Z_{\ell,i}$ $(1 \leq i \leq 2g)$ and positive integer $m \leq M_{A\times A'}$, the irreducible components of C_m are absolutely irreducible.*
- *The set of varieties $\{C \cap \mathcal{V}'_\ell\}_{\ell,C}$ has bounded complexity with $\ell \in \Lambda_0$ and C ranging over the irreducible components of $Z_{\ell,i}$ $(1 \leq i \leq 2g)$.*

- *The set of varieties* $\{C_m\}_{\ell,C,m}$ *has bounded complexity with* $\ell \in \Lambda_0$, C *ranging over the irreducible components of* $Z_{\ell,i}$ $(1 \leq i \leq 2g)$ *and* $m \leq M_{A\times A'}$.

Proof. Fix a number field F and let Λ_0 be a set consisting of all but finitely many primes $\ell \in \Lambda$ that splits completely in F. In our proof, we will allow ourselves to increase F and remove finitely many ℓ from Λ_0. The set Λ_0 has positive density by the Chebotarev density theorem and our assumption that Λ has density 1.

By Theorem 2.1.3(c), we can increase F so that H_ℓ is reductive and split for all sufficiently large ℓ that split completely in F. So we may assume that H_ℓ is reductive and split for all $\ell \in \Lambda_0$.

Set $M = M_{A\times A'}$. Fix $\ell \in \Lambda_0$. The torus $\mathcal{T}_\ell$ is the locus in $\mathbb{G}_m^{2g+2g'}$ of a finite set of equations

$$\left\{ \prod_{i=1}^{2g+2g'} x_i^{n_i} - 1 : \ (n_1, \cdots, n_{2g+2g'}) \in \mathcal{A}_\ell \right\} \tag{3.3.1}$$

where $\mathcal{A}_\ell$ is a subset of $\mathbb{Z}^{2g+2g'}$. As shown in the proof of [Zyw16, Lemma 3.2], we may further assume that $\mathcal{A}_\ell$ is chosen such that $|n_i| \leq B_{A\times A'}$ for all $(n_1, \cdots, n_{2g+2g'}) \in \mathcal{A}_\ell$, where $B_{A\times A'}$ is a constant that does not depend on ℓ.

Let $\mathfrak{T}_{\mathcal{A}_\ell} \subseteq \mathbb{G}_m^{2g+2g'}$ be the subvariety defined over F given by the locus of the set of equations (3.3.1).

For $1 \leq i \leq 2g$, let $\mathfrak{Z}_{\ell,i} := \mathfrak{T}_{\mathcal{A}_\ell} \cap \{x_i = 1\}$. We extend F such that every irreducible component $\mathfrak{C} \subseteq \mathfrak{Z}_{\ell,i}$ is absolutely irreducible. For each irreducible component $\mathfrak{C} \subseteq \mathfrak{Z}_{\ell,i}$ and $m \leq M$, we define $\mathfrak{C}_m := \{x \in \mathfrak{T}_{\mathcal{A}_\ell} : \ x^m \in \mathfrak{C}\}$. We extend F such that every irreducible component of $\mathfrak{C}_m$ is absolutely irreducible. We can take our number field F independent of $\ell \in \Lambda_0$ since there are only finitely many possibilities for $\mathcal{A}_\ell \subseteq \mathbb{Z}^{2g+2g'}$.

Suppose X/F is a variety such that all irreducible components are absolutely irreducible. Then [Gro66, Lemma (9.7.5)] says that for any model $\mathcal{X}/\mathcal{O}_F$, the irreducible components of $\mathcal{X}_{\mathbb{F}_\lambda}$ are also absolutely irreducible for all but finitely many prime ideals $\lambda \subseteq \mathcal{O}_F$. Hence, by our choice of F above, for all but finitely many prime ideals $\lambda \subseteq \mathcal{O}_F$, every irreducible component of $(\mathfrak{Z}_{\ell,i})_{\mathbb{F}_\lambda}$ $(1 \leq i \leq 2g)$ is absolutely irreducible. Moreover, by further excluding finitely many λ, for each irreducible component $\mathfrak{C}$ of $\mathfrak{Z}_{\ell,i}$ and $m \leq M$, the irreducible components of $(\mathfrak{C}_m)_{\mathbb{F}_\lambda}$ are absolutely irreducible.

Choose a prime ideal $\lambda|\ell$ of $\mathcal{O}_F$. Since ℓ splits completely in F, we have $\mathbb{F}_\lambda = \mathbb{F}_\ell$. By our choice of $\mathcal{A}_\ell$, the torus $(\mathfrak{T}_{\mathcal{A}_\ell})_{\mathbb{F}_\lambda}$ is equal to $\mathcal{T}_\ell$ over $\mathbb{F}_\lambda = \mathbb{F}_\ell$. Similarly, for each $1 \leq i \leq 2g$, we have an equality $(\mathfrak{Z}_{\ell,i})_{\mathbb{F}_\lambda} = Z_{\ell,i}$ of varieties over $\mathbb{F}_\ell$.

Take any irreducible component $\mathfrak{C}$ of $\mathfrak{Z}_{\ell,i}$. After removing a finite number of primes from Λ_0, we may assume that $C := (\mathfrak{C})_{\mathbb{F}_\lambda}$ is an absolutely irreducible variety defined over $\mathbb{F}_\ell$. In fact, every irreducible component of $Z_{\ell,i}$ arises from such a $\mathfrak{C}$. For any $m \leq M$, we have $C_m = (\mathfrak{C}_m)_{\mathbb{F}_\lambda}$. By removing a finite number of primes from Λ_0, we may assume that the irreducible components of C_m are absolutely irreducible.

Note that there are only finitely many $\mathfrak{C}$ and $\mathfrak{C}_m$ as we vary $\ell \in \Lambda_0$ and $m \leq M$ since there are only finitely many $\mathcal{A}_\ell$. So the complexity of all C and C_m is bounded. Moreover, since $C \cap \mathcal{V}'_\ell = \bigcup_{i=2g+1}^{2g'} C \cap \{x_i = 1\}$, the complexity of all $C \cap \mathcal{V}'_\ell$ is also bounded. $\square$

3.4 Proof of Proposition 3.1.2

Let Λ_0 be a set of positive density as in Lemma 3.3.2. Fix $\ell \in \Lambda_0$. By Lemma 3.3.2, H_ℓ is split. Let $\mathcal{T}_\ell \subseteq H_\ell$ be a split maximal torus and we use the same setup as in §3.3. By Lemma 3.1.3, it suffices to prove that $\mathcal{V}_\ell \cap \mathcal{T}_\ell \subseteq \mathcal{V}'_\ell \cap \mathcal{T}_\ell$.

Suppose that $\mathcal{V}_\ell \cap \mathcal{T}_\ell \not\subseteq \mathcal{V}'_\ell \cap \mathcal{T}_\ell$; we want to get a contradiction when $\ell \in \Lambda_0$ is large enough. There exists an irreducible component C of $\mathcal{V}_\ell \cap \mathcal{T}_\ell$ such that $C \neq \mathcal{V}'_\ell \cap C$. Let d be the dimension of C. Since C is irreducible, the dimension d' of $\mathcal{V}'_\ell \cap C$ is strictly less than d. Define

$$\Gamma_\ell := C(\mathbb{F}_\ell) \cap \overline{\rho}_{A\times A',\ell}(\mathrm{Gal}_K)$$

and $\gamma_\ell := |\Gamma_\ell|$.

The following lemma is an application of the Weil conjectures, which approximates the cardinality of $\mathbb{F}_\ell$-points of an affine variety V defined over $\mathbb{F}_\ell$.

Lemma 3.4.1. *Let $\{V_i\}_{i\in I}$ be a collection of affine varieties with V_i defined over a finite field $\mathbb{F}_{\ell_i}$ for each $i \in I$. Suppose $\{V_i\}_{i\in I}$ has bounded complexity.*

(a) For all $i \in I$, we have

$$|V_i(\mathbb{F}_{\ell_i})| = O(\ell_i^{\dim V_i})$$

where the implicit constant is independent of $i \in I$.

(b) Fix an $i \in I$. Suppose that the top dimensional irreducible components of V_i are absolutely irreducible. Then

$$|V_i(\mathbb{F}_{\ell_i})| \geq \ell_i^{\dim V_i} + O(\ell_i^{\dim V_i - 1/2})$$

where the implicit constant is independent of i.

Proof. Let $V \subseteq \mathbb{A}^n_{\mathbb{F}_\ell}$ with $n > 1$ be a closed subvariety defined by the simultaneous vanishing of r polynomials in $\mathbb{F}_\ell[x_1, \cdots, x_n]$ each of degree at most D. Let b be the number of top dimensional irreducible components of $V_{\overline{\mathbb{F}}_\ell}$. In [Zyw16, Theorem 2.1], Zywina gave the following inequalities:

$$|V(\mathbb{F}_\ell)| \leq b\ell^{\dim V} + 6(3 + rD)^{n+1}2^r\ell^{\dim V - 1/2}. \tag{3.4.1}$$

Suppose further that these components are all defined over $\mathbb{F}_\ell$. Then

$$\big||V(\mathbb{F}_\ell)| - b\ell^{\dim V}\big| \leq 6(3 + rD)^{n+1}2^r\ell^{\dim V - 1/2}. \tag{3.4.2}$$

We claim that b is bounded in terms of n, r and D only. The number b of top dimensional irreducible components of $V_{\overline{\mathbb{F}}_\ell}$ is equal to the dimension of the ℓ'-adic étale cohomology group $H^{2n}_c(V_{\overline{\mathbb{F}}_\ell}, \mathbb{Q}_{\ell'})$ with compact support for a prime $\ell' \neq \ell$. Katz [Kat01, Theorem 1] showed that $\dim_{\mathbb{Q}_{\ell'}} H^{2n}_c(V_{\overline{\mathbb{F}}_\ell}, \mathbb{Q}_{\ell'})$ can be bounded in terms of n, r and D only. The claim is now clear.

Recall that we assumed $\{V_i\}_{i\in I}$ has bounded complexity, i.e., the numbers n_i, r_i, D_i as described above for each V_i are bounded independent of i and hence so is b_i in inequalities 3.4.1 and 3.4.2 above. Now (a) follows by applying inequality 3.4.1 to each V_i and (b) follows by applying inequality 3.4.2 to our chosen V_i and using that $b_i \geq 1$. □

We will now give a lower bound for γ_ℓ. Set $m_\ell := [H_\ell(\mathbb{F}_\ell) : \overline{\rho}_{A\times A',\ell}(\mathrm{Gal}_K)]$. By Theorem 2.1.3(a), there exists a constant $M := M_{A\times A'}$ not depending on ℓ such that $m_\ell \leq M$. Consider the function

$$\varphi : C_{m_\ell}(\mathbb{F}_\ell) \to \Gamma_\ell, \quad g \mapsto g^{m_\ell};$$

it is well defined since for all $h \in H_\ell(\mathbb{F}_\ell)$ we have $h^{m_\ell} \in \overline{\rho}_{A\times A',\ell}(\mathrm{Gal}_K)$. Since $\mathcal{T}_\ell$ is a split torus of dimension at most $2g + 2g'$, the kernel of φ has cardinality

bounded by $m_\ell^{2g+2g'} \leq M^{2g+2g'}$. Since $\ell \in \Lambda_0$, the (top dimensional) irreducible components of each C_{m_ℓ} are all absolutely irreducible by Lemma 3.3.2. Hence, by Lemma 3.4.1(b), we have

$$\gamma_\ell = |\Gamma_\ell| \geq \frac{|C_{m_\ell}(\mathbb{F}_\ell)|}{M^{2g+2g'}} \geq \frac{\ell^d}{M^{2g+2g'}} + \frac{O(\ell^{d-1/2})}{M^{2g+2g'}} \tag{3.4.3}$$

where the error term is independent of ℓ since the collection of varieties $\{C_{m_\ell}\}_{\ell \in \Lambda_0, C}$ has bounded complexity by Lemma 3.3.2. Inequality (3.4.3) gives our lower bound of γ_ℓ.

We will now give a upper bound for γ_ℓ. Recall from equation (3.1.1) that we have

$$\mathcal{V}_\ell(\mathbb{F}_\ell) \cap \overline{\rho}_{A\times A',\ell}(\mathrm{Gal}_K) \subseteq \mathcal{V}'_\ell(\mathbb{F}_\ell) \cap \overline{\rho}_{A\times A',\ell}(\mathrm{Gal}_K)$$

and so

$$\Gamma_\ell = C(\mathbb{F}_\ell) \cap \overline{\rho}_{A\times A',\ell}(\mathrm{Gal}_K) \subseteq (C \cap \mathcal{V}'_\ell)(\mathbb{F}_\ell) \cap \overline{\rho}_{A\times A',\ell}(\mathrm{Gal}_K) \subseteq (C \cap \mathcal{V}'_\ell)(\mathbb{F}_\ell)$$

Recall that $C \cap \mathcal{V}'_\ell$ has dimension $d' \leq d-1$. Hence, by Lemma 3.4.1(a), we have

$$\gamma_\ell = O(\ell^{d'}) \tag{3.4.4}$$

where the error term is independent of ℓ since the collection of varieties $\{C \cap \mathcal{V}'_\ell\}_{\ell \in \Lambda_0, C}$ has bounded complexity by Lemma 3.3.2. Inequality (3.4.4) gives our upper bound of γ_ℓ.

By combining inequalities (3.4.3) and (3.4.4), we obtain

$$\frac{\ell^d}{M^{2g+2g'}} + \frac{O(\ell^{d-1/2})}{M^{2g+2g'}} = \gamma_\ell = O(\ell^{d'}) \tag{3.4.5}$$

where the error terms are independent of ℓ. In particular, $\ell^d = O(\ell^{d'})$. By removing a finite number of primes from Λ_0, this will contradict $d' < d$. Therefore, $\mathcal{V}_\ell \cap \mathcal{T}_\ell \subseteq \mathcal{V}'_\ell \cap \mathcal{T}_\ell$. This completes the proof of Proposition 3.1.2.

3.5 Proof of Proposition 3.0.1

Take any prime ideal $\mathfrak{p} \in S$. We need to show that $\operatorname{rad} P_{A,\mathfrak{p}}(x)$ divides $\operatorname{rad} P_{A',\mathfrak{p}}(x)$.

Lemma 3.5.1. *Suppose $f(x)$ and $g(x) \in \mathbb{Z}[x]$ are both monic such that the roots in $\overline{\mathbb{F}}_\ell$ of $f(x)$ are also roots of $g(x)$ for infinitely many ℓ. Then $\operatorname{rad}(f)$ divides $rad(g)$.*

Proof. Suppose that $\operatorname{rad}(f)$ does not divide $\operatorname{rad}(g)$ and hence there exists an $\alpha \in \overline{\mathbb{Q}}$ such that $f(\alpha) = 0$ and $g(\alpha) \neq 0$. Let $F/\mathbb{Q}$ be a finite Galois extension containing α and all the roots of $g(x)$. Define

$$d := N_{F/\mathbb{Q}} \left(\prod_{\beta \in F,\ g(\beta)=0} (\alpha - \beta) \right).$$

Since $f, g \in \mathbb{Z}[x]$ are monic and $g(\alpha) \neq 0$, d is a non-zero integer. From the assumption of the lemma, there is a prime $\ell \nmid d$ for which the roots in $\overline{\mathbb{F}}_\ell$ of $f(x)$ are also roots of $g(x)$. Take any prime ideal $\mathcal{L} \subseteq \mathcal{O}_F$ dividing ℓ. For $a \in \mathcal{O}_F$, let $\overline{a}$ be its image in $\mathcal{O}_F/\mathcal{L}$. Since every root in $\overline{\mathbb{F}}_\ell$ of $f(x)$ is also a root of $g(x)$, we have $\prod_{\beta \in F,\ g(\beta)=0} (\overline{\alpha} - \overline{\beta}) = 0$ and hence

$$\prod_{\beta \in F,\ g(\beta)=0} (\alpha - \beta) \in \mathcal{L}.$$

Therefore, $d \in N_{F/\mathbb{Q}}(\mathcal{L}) \subseteq \ell\mathbb{Z}$ which contradicts $\ell \nmid d$. We conclude that $\operatorname{rad}(f)$ divides $\operatorname{rad}(g)$. □

Take $\ell \in \Lambda$ to be any of the infinitely many primes from Proposition 3.1.2 such that $\mathcal{V}_\ell \subseteq \mathcal{V}'_\ell$ and $\mathfrak{p} \nmid \ell$. By Theorem 2.1.3(b), we may further assume that H_ℓ contains the group $\mathbb{G}_m$ of homotheties.

We claim that the roots in $\overline{\mathbb{F}}_\ell$ of $P_{A,\mathfrak{p}}(x)$ are also roots of $P_{A',\mathfrak{p}}(x)$. Set $(B, B') := \overline{\rho}_{A \times A',\ell}(\operatorname{Frob}_\mathfrak{p}) \in H_\ell(\mathbb{F}_\ell)$. Suppose that $\lambda \in \overline{\mathbb{F}}_\ell^\times$ is any root of $\det(xI - B) \equiv P_{A,\mathfrak{p}}(x)$

(mod ℓ). Since $\mathbb{G}_m \subseteq H_\ell$, we have $(\lambda^{-1}B, \lambda^{-1}B') \in H_\ell(\overline{\mathbb{F}}_\ell)$. Since $\det(I - \lambda^{-1}B) = 0$, we have $(\lambda^{-1}B, \lambda^{-1}B') \in \mathcal{V}_\ell(\overline{\mathbb{F}}_\ell)$. By our choice of ℓ, we have $\mathcal{V}_\ell \subseteq \mathcal{V}'_\ell$ and thus $(\lambda^{-1}B, \lambda^{-1}B') \in \mathcal{V}'_\ell(\overline{\mathbb{F}}_\ell)$. We deduce that λ is also a root of $\det(xI - B') \equiv P_{A',\mathfrak{p}}(x)$ (mod ℓ). This proves our claim.

Since $P_{A,\mathfrak{p}}(x)$ and $P_{A',\mathfrak{p}}(x)$ are monic and the roots in $\overline{\mathbb{F}}_\ell$ of $P_{A,\mathfrak{p}}(x)$ are also roots of $P_{A',\mathfrak{p}}(x)$ for infinitely many ℓ, Lemma 3.5.1 implies that $\operatorname{rad} P_{A,\mathfrak{p}}(x)$ divides $\operatorname{rad} P_{A',\mathfrak{p}}(x)$. This proves Proposition 3.0.1.

CHAPTER 4

FROBENIUS POLYNOMIALS AND WEIGHTS

Let A and A' be simple and non-isogenous abelian varieties defined over a number field K of dimensions g and g' respectively. Assume that $K^{\mathrm{conn}}_{A\times A'} = K$, equivalently, the ℓ-adic monodromy groups $G_{A\times A',\ell}$ are connected. Note that in particular, the ℓ-adic monodromy groups $G_{A,\ell}$ and $G_{A',\ell}$ are connected. We will prove the following theorem in §4.2.

Theorem 4.0.1. *The polynomials $P_{A,\mathfrak{p}}(x)$ and $P_{A',\mathfrak{p}}(x)$ are relatively prime for almost all $\mathfrak{p} \in \Sigma_K$.*

Remark 4.0.2. Theorem 4.0.1 is false without the connectedness assumption. For example, if A and A' are two non-isogenous CM elliptic curves over $\mathbb{Q}$, then $P_{A,p}(x) = x^2 + p = P_{A',p}(x)$ for a set of primes p of positive density.

4.1 Weights for non-isogenous abelian varieties

Set $G = G_{A\times A',\ell}$; it is connected and reductive. Fix a maximal torus $T \subseteq G$. Let $\Omega_{A,\ell} \subseteq X(T)$ and $\Omega_{A',\ell} \subseteq X(T)$ be the weights of G acting on $V_\ell(A)$ and $V_\ell(A')$ respectively. Note that

$$V_\ell(A \times A') = V_\ell(A) \oplus V_\ell(A').$$

Let $W = W(G,T) = N_G(T)(\overline{\mathbb{Q}}_\ell)/T(\overline{\mathbb{Q}}_\ell)$ be the absolute Weyl group of G with respect to T; it acts on $\Omega_{A,\ell}$ and $\Omega_{A',\ell}$.

Lemma 4.1.1. *The sets $\Omega_{A,\ell}$ and $\Omega_{A',\ell}$ are disjoint.*

Proof. Suppose $\Omega_{A,\ell} \cap \Omega_{A',\ell} \neq \emptyset$. Let $\widetilde{\Omega}$ be the W-orbit of an element in $\Omega_{A,\ell} \cap \Omega_{A',\ell}$. Let

$$U \subseteq V_\ell(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell \subseteq V_\ell(A \times A') \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell$$

be an irreducible representation of $G_{\overline{\mathbb{Q}}_\ell}$ for which $\Omega(U)$ contains an element of $\widetilde{\Omega}$. We have $\widetilde{\Omega} \subseteq \Omega(U)$ since $\Omega(U)$ is stable under the action of W. The representation U is minuscule by Proposition 2.3.6, so $\Omega(U) = \widetilde{\Omega}$ and each weight of U has multiplicity 1. Denote by σ the representation of $G_{\overline{\mathbb{Q}}_\ell}$ on U. Similarly, we can construct an irreducible subrepresentation σ' of $V_\ell(A') \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell$ with weights $\widetilde{\Omega}$ that each have multiplicity 1. Therefore, for every $t \in T$, we have

$$\operatorname{tr} \circ \sigma(t) = \sum_{\alpha \in \tilde{\Omega}} \alpha(t) = \operatorname{tr} \circ \sigma'(t)$$

for all $t \in T$. Since G is reductive, this implies that $\operatorname{tr} \circ \sigma = \operatorname{tr} \circ \sigma'$ and hence σ and σ' are isomorphic. So $V_\ell(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell$ and $V_\ell(A') \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell$ have an irreducible representation of $G_{\overline{\mathbb{Q}}_\ell}$ in common. Therefore,

$$\operatorname{Hom}_{\mathbb{Q}_\ell[\mathrm{Gal}_K]}(V_\ell(A), V_\ell(A')) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell = \operatorname{Hom}_{\overline{\mathbb{Q}}_\ell[\mathrm{Gal}_K]}(V_\ell(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell, V_\ell(A') \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell) \neq 0.$$

Since $\operatorname{Hom}_{\mathbb{Q}_\ell[\mathrm{Gal}_K]}(V_\ell(A), V_\ell(A')) \neq 0$, we deduce by Theorem 2.1.4(b) that $\operatorname{Hom}(A, A') \neq 0$. However, this is impossible since A and A' are simple and non-isogenous. Therefore, $\Omega_{A,\ell}$ and $\Omega_{A',\ell}$ are disjoint. □

4.2 Proof of Theorem 4.0.1

Fix notation as in §4.1. By Lemma 4.1.1, we have $\Omega_{A,\ell} \cap \Omega_{A',\ell} = \emptyset$. Define

$$\mathcal{Z} := \left\{ t \in T : \prod_{\substack{\alpha,\beta \in \Omega_{A,\ell} \cup \Omega_{A',\ell} \\ \alpha \neq \beta}} (\alpha(t) - \beta(t)) = 0 \right\};$$

it is a subvariety of T defined over $\mathbb{Q}_\ell$ since $\mathrm{Gal}_{\mathbb{Q}_\ell}$ acts on $\Omega_{A,\ell} \cup \Omega_{A',\ell}$. Moreover, $\dim \mathcal{Z} < \dim T$ since T is irreducible and $\mathcal{Z} \neq T$ ($\Omega_{A,\ell}$ and $\Omega_{A',\ell}$ are non-empty and disjoint, so $\#(\Omega_{A,\ell} \cup \Omega_{A',\ell}) \geq 2$).

For each $\mathfrak{p} \in \Sigma_K$ for which A and A' have good reduction and $\mathfrak{p} \nmid \ell$, choose $t_\mathfrak{p} \in T(\overline{\mathbb{Q}}_\ell)$ such that $t_\mathfrak{p}$ is conjugate to $\rho_{A\times A',\ell}(\mathrm{Frob}_\mathfrak{p})$ in $G(\overline{\mathbb{Q}}_\ell)$.

Lemma 4.2.1. *For almost all $\mathfrak{p} \in \Sigma_K$, we have $\alpha(t_\mathfrak{p}) \neq \beta(t_\mathfrak{p})$ for all $\alpha, \beta \in \Omega_{A,\ell} \cup \Omega_{A',\ell}$ with $\alpha \neq \beta$.*

Proof. Note that G acts on the coordinate algebra $\mathcal{A} = \mathbb{Q}_\ell[G]$ by composing with conjugation, and $\mathcal{A}^G$ is the set of central functions of G. Define $G^\# := \mathrm{Spec}(\mathcal{A}^G)$; it is the variety of semisimple conjugacy classes of G. Denote the natural projection by $\mathrm{cl} : G \to G^\#$; it satisfies the property that for $g_1, g_2 \in G(\overline{\mathbb{Q}}_\ell)$, $\mathrm{cl}(g_1) = \mathrm{cl}(g_2)$ if and only if $(g_1)_s$ and $(g_2)_s$ are conjugate in $G(\overline{\mathbb{Q}}_\ell)$ (recall that g_s is the semisimple component in the multiplicative Jordan decomposition of $g \in G$). Furthermore, for $t_1, t_2 \in T(\overline{\mathbb{Q}}_\ell)$, $\mathrm{cl}(t_1) = \mathrm{cl}(t_2)$ if and only if $w(t_1) = t_2$ for some $w \in W$. The map $\mathrm{cl}|_T : T \to G^\#$ is dominant and $G^\#$ can be identified as a quotient of T (often denoted by $T//W$). The subvariety $\mathcal{Z}_{\overline{\mathbb{Q}}_\ell}$ of $T_{\overline{\mathbb{Q}}_\ell}$ is stable under the action of W and thus $\mathfrak{Z} = \mathrm{cl}(\mathcal{Z})$ is a subvariety of $G^\#$ which is defined over $\mathbb{Q}_\ell$. Define $\mathfrak{V} := \{B \in G : \ \mathrm{cl}(B) \in \mathfrak{Z}\}$; it is a subvariety of G with dimension strictly less than $\dim G$ and stable under conjugation by G.

Recall that $\rho_{A\times A',\ell}(\mathrm{Gal}_K)$ is open in $G(\mathbb{Q}_\ell)$. Chebotarev's density theorem [Ser98, §2.2, Corollary 2(b)] then implies that for almost all $\mathfrak{p} \in \Sigma_K$, we have $\rho_{A\times A',\ell}(\mathrm{Frob}_\mathfrak{p}) \notin \mathfrak{V}(\mathbb{Q}_\ell)$ and hence $t_\mathfrak{p} \notin \mathcal{Z}(\overline{\mathbb{Q}}_\ell)$. Therefore, for almost all $\mathfrak{p} \in \Sigma_K$, we have $\alpha(t_\mathfrak{p}) - \beta(t_\mathfrak{p}) \neq 0$ for all distinct $\alpha, \beta \in \Omega_{A,\ell} \cup \Omega_{A',\ell}$. □

Lemma 4.1.1 says that the sets $\Omega_{A,\ell}$ and $\Omega_{A',\ell}$ are disjoint. So by Lemma 4.2.1,

$\{\alpha(t_{\mathfrak{p}}) : \alpha \in \Omega_{A,\ell}\} \cap \{\beta(t_{\mathfrak{p}}) : \beta \in \Omega_{A',\ell}\} = \emptyset$ for almost all $\mathfrak{p} \in \Sigma_K$. So, the set of roots of $P_{A,\mathfrak{p}}(x)$ and $P_{A',\mathfrak{p}}(x)$ in $\overline{\mathbb{Q}}_\ell$ are disjoint for almost all $\mathfrak{p} \in \Sigma_K$. Therefore, the polynomials $P_{A,\mathfrak{p}}(x)$ and $P_{A',\mathfrak{p}}(x)$ are relatively prime for almost all $\mathfrak{p} \in \Sigma_K$.

CHAPTER 5

PROOF OF THEOREM 1.0.1

Suppose A is a square-free abelian variety defined over a number field K with $K_A^{\mathrm{conn}} = K$. Since A is square-free, it is isogenous to a product $\prod_{i\in I} B_i$, where the B_i are pairwise non-isogenous simple abelian varieties defined over K. Let A' be an abelian variety over K for which there exists a density 1 set S of prime ideals of Σ_K and a density 1 set Λ of rational primes such that

$$\mathrm{rad}_\Lambda\, |A(\mathbb{F}_\mathfrak{p})| = \mathrm{rad}_\Lambda\, |A'(\mathbb{F}_\mathfrak{p})|$$

for all $\mathfrak{p} \in S$. In particular, note that we are not yet assuming that A' is square-free.

The following proposition which we will prove in §5.1, says that A' is isogenous to a product of simple factors of A over an explicit extension of K.

Proposition 5.0.1. *The abelian variety A' isogenous to $\prod_{i\in I} B_i^{e_i}$ over $K_{A\times A'}^{\mathrm{conn}}$ for some $e_i \geq 1$.*

The following proposition says that $K_{A\times A'}^{\mathrm{conn}}$ is in fact K; we will give a proof in §5.2.

Proposition 5.0.2. *We have $K_{A\times A'}^{\mathrm{conn}} = K$.*

Propositions 5.0.1 and 5.0.2 imply that A' is isogenous to $\prod_{i\in I} B_i^{e_i}$ over $K_{A\times A'}^{\mathrm{conn}} = K$ with $e_i \geq 1$. Finally, if we further assume that A' is square-free, we deduce that all the $e_i = 1$ and hence A' is isogenous to A over K. This completes the proof of Theorem 1.0.1.

5.1 Proof of Proposition 5.0.1

Lemma 5.1.1. *To prove Proposition 5.0.1, it suffices to prove it in the case where* $K^{\mathrm{conn}}_{A\times A'} = K$.

Proof. Set $L = K^{\mathrm{conn}}_{A\times A'}$. Note that A_L is square-free since the B_i are simple over $\overline{K}$ (and hence also over L) by Lemma 2.1.5(b). The ℓ-adic monodromy groups of $A_L \times A'_L$ are connected. We need only show that

$$\mathrm{rad}_\Lambda\, |A(\mathbb{F}_\mathfrak{P})| = \mathrm{rad}_\Lambda\, |A'(\mathbb{F}_\mathfrak{P})|$$

for a density 1 set S' of $\mathfrak{P} \in \Sigma_L$, since then Proposition 5.0.1 (with the assumption $K^{\mathrm{conn}}_{A\times A'} = K$) would imply that A'_L is isogenous to $\prod_{i\in I}(B_i)^{e_i}_L$ for some $e_i \geq 1$.

For a density one set of $\mathfrak{P} \in \Sigma_L$, the inertia degree $f(\mathfrak{P}/\mathfrak{p})$ of $\mathfrak{P}$ over $\mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_K \in \Sigma_K$ is 1. Indeed, we have

$$\sum_{\mathfrak{P}\in\Sigma_L, N(\mathfrak{P})\leq x, f(\mathfrak{P}/\mathfrak{P}\cap\mathcal{O}_K)\geq 2} 1 \leq [L:K] \sum_{\mathfrak{p}\in\Sigma_K, N(\mathfrak{p})\leq\sqrt{x}} 1 \leq 2[L:K][K:\mathbb{Q}]\pi(\sqrt{x}) \leq [L:\mathbb{Q}]\sqrt{x}$$

where N is the norm. Note that when $f(\mathfrak{P}/\mathfrak{p}) = 1$, we have $\mathbb{F}_\mathfrak{P} = \mathbb{F}_\mathfrak{p}$ and hence $|A(\mathbb{F}_\mathfrak{P})| = |A(\mathbb{F}_\mathfrak{p})|$. Similarly, $|A'(\mathbb{F}_\mathfrak{P})| = |A'(\mathbb{F}_\mathfrak{p})|$. Hence, by our assumption that $\mathrm{rad}_\Lambda\, |A(\mathbb{F}_\mathfrak{p})| = \mathrm{rad}_\Lambda\, |A'(\mathbb{F}_\mathfrak{p})|$ for all $\mathfrak{p} \in S$, we have

$$\mathrm{rad}_\Lambda\, |A(\mathbb{F}_\mathfrak{P})| = \mathrm{rad}_\Lambda\, |A(\mathbb{F}_\mathfrak{p})| = \mathrm{rad}_\Lambda\, |A'(\mathbb{F}_\mathfrak{p})| = \mathrm{rad}_\Lambda\, |A(\mathbb{F}_\mathfrak{P})|$$

for almost all $\mathfrak{P} \in \Sigma_L$. □

By Lemma 5.1.1, we may assume that $K^{\mathrm{conn}}_{A\times A'} = K$. By assumption, we have $\mathrm{rad}_\Lambda\, |A(\mathbb{F}_\mathfrak{p})| = \mathrm{rad}_\Lambda\, |A'(\mathbb{F}_\mathfrak{p})|$ for all $\mathfrak{p} \in S$. By applying Proposition 3.0.1 twice, we deduce that $\mathrm{rad}\, P_{A,\mathfrak{p}}(x) = \mathrm{rad}\, P_{A',\mathfrak{p}}(x)$ for all $\mathfrak{p} \in S$.

The abelian variety A' is isogenous to $\prod_{j\in J} {B'_j}^{e_j}$, where the B'_j are pairwise non-isogenous simple abelian varieties defined over K and $e_j \geq 1$.

Suppose there exists $i \in I$ such that B_i is not isogenous to any B'_j. Theorem 4.0.1 implies there is a prime $\mathfrak{p} \in S$ such that $\operatorname{rad} P_{B_i,\mathfrak{p}}(x)$ is relatively prime to $\operatorname{rad} P_{B'_j,\mathfrak{p}}(x)$ for all $j \in J$. Since

$$\operatorname{rad} P_{A',\mathfrak{p}}(x) = \operatorname{rad}(\prod_{j\in J} P_{B'_j}(x)^{e_j}) = \operatorname{rad}(\prod_{j\in J} P_{B'_j}(x)),$$

we deduce that $\operatorname{rad} P_{B_i,\mathfrak{p}}(x)$ is relatively prime to $\operatorname{rad} P_{A',\mathfrak{p}}(x)$. This contradicts that $\operatorname{rad} P_{B_i,\mathfrak{p}}(x)$ divides $\operatorname{rad} P_{A,\mathfrak{p}}(x) = \operatorname{rad} P_{A',\mathfrak{p}}(x)$. Hence, we conclude that for each $i \in I$, there exists $j \in J$ such that B_i is isogenous to B'_j; such a $j \in J$ is unique since the B'_j are pairwise non-isogenous. By a similar argument, for each $j \in J$, there exists a unique $i \in I$ such that B_i is isogenous to B'_j. So there is a bijection $f : I \to J$ such that B_i is isogenous to $B'_{f(i)}$ for all $i \in I$. Therefore, A' is isogenous to $\prod_{i\in I} B_i^{e_{f(i)}}$. The proof of Proposition 5.0.1 is now complete.

5.2 Proof of Proposition 5.0.2

Set $L := K_{A\times A'}^{\mathrm{conn}}$. Suppose $L \neq K$; we want a contradiction.

By Proposition 5.0.1, there exists an isogeny

$$\phi : A'_L \to C_L$$

defined over L, where $C := \prod_{i\in I}(B_i)^{e_i}$ is an abelian variety over K for some $e_i \geq 1$. Since A and C have the same simple factors, up to isogeny, we find that the algebraic groups $G_{A,\ell}$ and $G_{C,\ell}$ are isomorphic. Therefore, $G_{C,\ell}$ is connected by the assumption $K_A^{\mathrm{conn}} = K$.

Lemma 5.2.1. *There exists a prime ideal $\mathfrak{q} \in S$ and an algebraic number $\pi \in \overline{\mathbb{Q}}$ such that $P_{A',\mathfrak{q}}(\pi) = 0$ and $P_{C,\mathfrak{q}}(\pi) \neq 0$.*

Proof. Fix a prime ℓ. Set $G = G_{C\times A',\ell}$. We can view G as a closed algebraic subgroup of $G_{C,\ell} \times G_{A',\ell}$. The isogeny ϕ induces an isomorphism $V_\ell(A'_L) \xrightarrow{\sim} V_\ell(C_L)$ of $\mathbb{Q}_\ell[\mathrm{Gal}_L]$-modules. Using this isomorphism as an identification, we can assume that

$$\rho_{C\times A',\ell}(\sigma) = (\rho_{C,\ell}(\sigma), \rho_{A',\ell}(\sigma)) = (\rho_{C,\ell}(\sigma), \rho_{C,\ell}(\sigma))$$

for all $\sigma \in \mathrm{Gal}_L$. Since $G_{(C\times A')_L,\ell}$ is the Zariski closure of $\rho_{C\times A',\ell}(\mathrm{Gal}_L)$, we have $G_{(C\times A')_L,\ell} = \{(B,B) : B \in G_{C,\ell}\}$; note that $G^\circ = G_{(C\times A')_L,\ell}$ since $G_{C,\ell}$ is connected. Therefore,

$$G^\circ = \{(B,B) :\ B \in G_{A,\ell}\}.$$

By our assumption $L \neq K$, we have $G^\circ \subsetneq G$. So there exists a pair $(g,g') \in G(\mathbb{Q}_\ell)\backslash G^\circ(\mathbb{Q}_\ell)$ with $g \neq g'$. Since $(g^{-1},g^{-1}) \in G^\circ(\mathbb{Q}_\ell)$, we have $(I,z) \in G(\mathbb{Q}_\ell)\backslash G^\circ(\mathbb{Q}_\ell)$ with $z := g^{-1}g' \neq I$. Since $G(\mathbb{Q}_\ell)/G^\circ(\mathbb{Q}_\ell)$ is finite, there exists an integer m such that $(I,z^m) = (I,z)^m \in G^\circ(\mathbb{Q}_\ell)$ and so $I = z^m$, i.e., z has finite order. Moreover, since G° is a normal subgroup of G, for any pair $(g_0,g_0) \in G^\circ$, $(g_0, z^{-1}g_0z) = (I,z)^{-1}(g_0,g_0)(I,z) \in G^\circ$ and so $zg_0 = g_0z$. Hence, z commutes with $G_{C,\ell}$. The coset $(I,z)\cdot G^\circ$ of G° in G is given by

$$(I,z)\cdot G^\circ = \{(B, z\cdot B) :\ B \in G_{C,\ell}\};$$

it is not G° since $z \neq I$.

Since $\rho_{C\times A',\ell}(\mathrm{Gal}_K)$ is Zariski dense in G and open in $G(\mathbb{Q}_\ell)$, the set

$$\{\sigma \in \mathrm{Gal}_K :\ \rho_{C,\ell}(\sigma) = z\cdot\rho_{A',\ell}(\sigma)\} \supseteq \rho^{-1}_{C\times A',\ell}(((I,z)\cdot G^\circ)(\mathbb{Q}_\ell))$$

is open in Gal_K. By the Chebotarev density theorem, there exists a prime $\mathfrak{q} \in \Sigma_K$ such that $\rho_{C,\ell}(\mathrm{Frob}_\mathfrak{q}) = z \cdot \rho_{A',\ell}(\mathrm{Frob}_\mathfrak{q})$. Recall that $z \neq I$ has finite order and commutes with $\rho_{A',\ell}(\mathrm{Frob}_\mathfrak{q})$, so z and $\rho_{C,\ell}(\mathrm{Frob}_\mathfrak{q})$ are simultaneously diagonalizable over $\overline{\mathbb{Q}}_\ell$ and hence there exist a root $\pi \in \overline{\mathbb{Q}}$ of $P_{A',\mathfrak{q}}(x)$ such that $\zeta\pi \in \overline{\mathbb{Q}}$ is a root of $P_{C,\mathfrak{q}}(x)$ for some root of unity $\zeta \neq 1$ in $\overline{\mathbb{Q}}$. By Larsen and Pink [LP97, Corollary 1.4], we can further assume that $\mathfrak{q}$ is chosen so that the roots of $P_{C,\mathfrak{q}}(x)$ in $\overline{\mathbb{Q}}^\times$ generates a torsion-free group (such $\mathfrak{q}$ have density 1 since the group $G_{C,\ell}$ is connected). So, in particular π is not a root of $P_{C,\mathfrak{q}}(x)$ (if it was, then the subgroup of $\overline{\mathbb{Q}}^\times$ generated by the roots of $P_{C,\mathfrak{q}}(x)$ contains $\zeta = (\zeta\pi) \cdot \pi^{-1}$ and hence has torsion).

Therefore, there exists $\mathfrak{q} \in \Sigma_K$ and $\pi \in \overline{\mathbb{Q}}$ such that $P_{A',\mathfrak{q}}(\pi) = 0$ and $P_{C,\mathfrak{q}}(\pi) \neq 0$. □

We now try to find a prime ideal $\mathfrak{p} \in S$ and a prime $\ell \in \Lambda$ such that

$$P_{A',\mathfrak{p}}(1) \equiv 0 \pmod{\ell} \quad \text{and} \quad P_{C,\mathfrak{p}}(1) \not\equiv 0 \pmod{\ell};$$

this would then imply that $\mathrm{rad}_\Lambda |C(\mathbb{F}_\mathfrak{p})| \neq \mathrm{rad}_\Lambda |A'(\mathbb{F}_\mathfrak{p})|$. Since $\mathrm{rad}_\Lambda |A(\mathbb{F}_\mathfrak{p})| = \mathrm{rad}_\Lambda |C(\mathbb{F}_\mathfrak{p})|$, this would contradict our assumption that $\mathrm{rad}_\Lambda |A(\mathbb{F}_\mathfrak{p})| = \mathrm{rad}_\Lambda |A'(\mathbb{F}_\mathfrak{p})|$.

Theorem 2.1.3(b) says that $\mathbb{G}_m \subseteq H_\ell$ when ℓ is large enough. Moreover, Theorem 2.1.3(a) says that there exists a number $M_{C\times A'}$ not depending on ℓ such that $[H_\ell(\mathbb{F}_\ell) : \overline{\rho}_{C\times A',\ell}(\mathrm{Gal}_K)] \leq M_{C\times A'}$ for all ℓ. So it follows that there is an integer $m \geq 1$ such that

$$(\mathbb{F}_\ell^\times)^m \cdot I \subseteq \overline{\rho}_{C\times A',\ell}(\mathrm{Gal}_K).$$

for all ℓ. Let F be number field containing an m-th root $\pi^{1/m}$ of π. Let $\ell \in \Lambda$ be a prime that splits completely in F; such a prime exists since we assumed Λ has

density 1. Take any $\lambda \in \Sigma_F$ such that $\lambda|\ell$; we have $\mathbb{F}_\lambda = \mathbb{F}_\ell$. Define c to be the image of $\pi^{1/m} \in \mathcal{O}_F$ in $\mathbb{F}_\lambda = \mathbb{F}_\ell$. Without loss of generality, we assume $\ell \in \Lambda$ is chosen large enough so that $c \neq 0$ and $\mathfrak{q} \nmid \ell$; note that the image of π in $\mathbb{F}_\lambda = \mathbb{F}_\ell$ is c^m.

Define

$$Y := (c^m)^{-1} \cdot \overline{\rho}_{C\times A',\ell}(\mathrm{Frob}_\mathfrak{q}) = ((c^m)^{-1} \cdot \overline{\rho}_{C,\ell}(\mathrm{Frob}_\mathfrak{q}), (c^m)^{-1} \cdot \overline{\rho}_{A',\ell}(\mathrm{Frob}_\mathfrak{q})).$$

We have $Y \in \overline{\rho}_{C\times A',\ell}(\mathrm{Gal}_K)$ since $c^m \in \overline{\rho}_{C\times A',\ell}(\mathrm{Gal}_K)$ by our choice of m. Recall that we have $P_{A',\mathfrak{q}}(\pi) = 0$. So $P_{A',\mathfrak{q}}(c^m) \equiv P_{A',\mathfrak{q}}(\pi) \equiv 0 \pmod{\lambda}$, i.e., c^m is an eigenvalue of $\overline{\rho}_{A',\ell}(\mathrm{Frob}_\mathfrak{q})$. Hence, $(c^m)^{-1} \cdot \overline{\rho}_{A',\ell}(\mathrm{Frob}_\mathfrak{q})$ has 1 as an eigenvalue and we have $\det(I - (c^m)^{-1} \cdot \overline{\rho}_{A',\ell}(\mathrm{Frob}_\mathfrak{q})) = 0$.

Suppose that $\det(I-(c^m)^{-1}\cdot\overline{\rho}_{C,\ell}(\mathrm{Frob}_\mathfrak{q})) = 0$. Then 1 is an eigenvalue of $(c^m)^{-1}\cdot \overline{\rho}_{C,\ell}(\mathrm{Frob}_\mathfrak{q})$ and c^m would then be an eigenvalue of $\overline{\rho}_{C,\ell}(\mathrm{Frob}_\mathfrak{q})$. So, $P_{C,\mathfrak{q}}(\pi) \equiv P_{A,\mathfrak{q}}(c^m) \equiv 0 \pmod{\lambda}$, i.e., λ divides $P_{C,\mathfrak{q}}(\pi) \in \mathcal{O}_F$. Since $P_{C,\mathfrak{q}}(\pi) \neq 0$, this can only happen for finitely many $\ell \in \Lambda$. So we may assume that $\ell \in \Lambda$ is chosen large enough so that $\det(I - (c^m)^{-1} \cdot \overline{\rho}_{C,\ell}(\mathrm{Frob}_\mathfrak{q})) \neq 0$.

Recall that $Y \in \overline{\rho}_{C\times A',\ell}(\mathrm{Gal}_K)$, so by the Chebotarev density theorem, there exists a prime $\mathfrak{p} \in S$ such that $Y = \overline{\rho}_{C\times A',\ell}(\mathrm{Frob}_\mathfrak{p})$. By our arguments above, we have chosen $\ell \in \Lambda$ and $\mathfrak{p} \in S$ such that

$$P_{A',\mathfrak{p}}(1) \equiv 0 \pmod{\ell} \quad \text{and} \quad P_{C,\mathfrak{p}}(1) \not\equiv 0 \pmod{\ell}.$$

That is, $\ell \in \Lambda$ does not divide $|C(\mathbb{F}_\mathfrak{p})|$ but divides $|A'(\mathbb{F}_\mathfrak{p})|$. In particular, $\mathrm{rad}_\Lambda |C(\mathbb{F}_\mathfrak{p})| \neq \mathrm{rad}_\Lambda |A'(\mathbb{F}_\mathfrak{p})|$. Since $\mathrm{rad}_\Lambda |A(\mathbb{F}_\mathfrak{p})| = \mathrm{rad}_\Lambda |C(\mathbb{F}_\mathfrak{p})|$, this contradicts our assumption that $\mathrm{rad}_\Lambda |A(\mathbb{F}_\mathfrak{p})| = \mathrm{rad}_\Lambda |A'(\mathbb{F}_\mathfrak{p})|$. We deduce that $L = K^{\mathrm{conn}}_{A\times A'}$ equals K. The proof of Proposition 5.0.2 is now complete.

CHAPTER 6

PROOF OF THEOREM 1.0.2

The abelian variety A' is isogenous to $\prod_{i=1}^{s} C_i^{e_i}$ with C_i pairwise non-isogenous simple abelian varieties defined over K and $e_i \geq 1$. By removing a finite number of prime ideals of S, we may assume that $A', B_1, \cdots, B_r, C_1, \cdots, C_s$ have good reductions for all $\mathfrak{p} \in S$. Let J be the set of $j \in \{1, \ldots, s\}$ for which C_j is not isogenous to any B_i. We need to show that $J = \emptyset$.

Define

$$A'' := \prod_{i=1}^{r} B_i \times \prod_{j \in J} C_j$$

which is square-free by our choice of J. Since, A is isogenous to the abelian subvariety $\prod_{i=1}^{r} B_i$ of A'', we deduce that $|A(\mathbb{F}_\mathfrak{p})|$ divides $|A''(\mathbb{F}_\mathfrak{p})|$ for all $\mathfrak{p} \in S$. On the other hand, since $|(\prod_{i=1}^{r} B_i)(\mathbb{F}_\mathfrak{p})| = |A(\mathbb{F}_\mathfrak{p})|$ and $|(\prod_{j \in J} C_j)(\mathbb{F}_\mathfrak{p})|$ divides $|A'(\mathbb{F}_\mathfrak{p})|$ for all $\mathfrak{p} \in S$, we find that

$$|A''(\mathbb{F}_\mathfrak{p})| = |(\prod_{i=1}^{r} B_i)(\mathbb{F}_\mathfrak{p})| \cdot |(\prod_{j \in J} C_j)(\mathbb{F}_\mathfrak{p})| \quad \text{divides} \quad |A(\mathbb{F}_\mathfrak{p})| \cdot |A'(\mathbb{F}_\mathfrak{p})|.$$

In particular, $\mathrm{rad}_\Lambda |A''(\mathbb{F}_\mathfrak{p})|$ divides $\mathrm{rad}_\Lambda(|A(\mathbb{F}_\mathfrak{p})| \cdot |A'(\mathbb{F}_\mathfrak{p})|)$. By our assumption that $\mathrm{rad}_\Lambda |A'(\mathbb{F}_\mathfrak{p})|$ divides $\mathrm{rad}_\Lambda |A(\mathbb{F}_\mathfrak{p})|$, we have $\mathrm{rad}_\Lambda(|A(\mathbb{F}_\mathfrak{p})| \cdot |A'(\mathbb{F}_\mathfrak{p})|) = \mathrm{rad}_\Lambda |A(\mathbb{F}_\mathfrak{p})|$ for all $\mathfrak{p} \in S$. Hence, $\mathrm{rad}_\Lambda |A''(\mathbb{F}_\mathfrak{p})|$ divides $\mathrm{rad}_\Lambda |A(\mathbb{F}_\mathfrak{p})|$ and so

$$\mathrm{rad}_\Lambda |A''(\mathbb{F}_\mathfrak{p})| = \mathrm{rad}_\Lambda |A(\mathbb{F}_\mathfrak{p})|$$

holds for all $\mathfrak{p} \in S$. Since both A'' and A are squarefree, by Theorem 1.0.1, A'' is isogenous to A and hence $J = \emptyset$.

CHAPTER 7

THE SPLITTING OF REDUCTIONS OF AN ABELIAN VARIETY

Let A be a simple abelian variety defined over a number K such that $K = K_A^{\mathrm{conn}}$. Since A is simple, $D := \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a division algebra; note that $A_{\overline{K}}$ is simple and $D = \mathrm{End}(A_{\overline{K}}) \otimes_{\mathbb{Z}} \mathbb{Q}$ by Lemma 2.1.5. Let E be the center of D; it is a number field. In particular, D is a central simple algebra over E. Define the integers $e := [D : E]^{1/2}$ and $r = [E : \mathbb{Q}]$.

Choose a prime ℓ that splits completely in E; it exists by the Chebotarev density theorem. Let λ_i $(1 \leq i \leq r)$ be the prime ideals of $\mathcal{O}_E$ that divides ℓ. For each λ_i, let E_{λ_i} be the λ_i-adic completion of E. Then we have $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \bigoplus_{i=1}^{r} E_{\lambda_i}$. Note that the ring $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ acts on $V_\ell(A)$ and commutes with the Gal_K action. If we let $V_{\lambda_i}(A) := V_\ell(A) \otimes_{E \otimes \mathbb{Q}_\ell} E_{\lambda_i}$, then we have a decomposition

$$V_\ell(A) = \bigoplus_{i=1}^{r} V_{\lambda_i}(A)$$

of $\mathbb{Q}_\ell[\mathrm{Gal}_K]$-modules. Each $V_{\lambda_i}(A)$ is also an $E_{\lambda_i}[\mathrm{Gal}_K]$-module which can be expressed as a Galois representation

$$\rho_{A,\lambda_i} : \mathrm{Gal}_K \to \mathrm{Aut}_{E_{\lambda_i}}(V_{\lambda_i}(A)) = \mathrm{Aut}_{\mathbb{Q}_\ell}(V_{\lambda_i}(A))$$

where the equality uses that $E_{\lambda_i} = \mathbb{Q}_\ell$ since ℓ splits completely in E.

Our assumption $K_A^{\mathrm{conn}} = K$ and Theorem 2.1.4(c) imply that the ℓ-adic monodromy group $G_{A,\ell}$ is connected and reductive. Choose a maximal torus $T \subseteq G_{A,\ell}$ and consider the set $\Omega(V_\ell(A)) \subseteq X(T)$ of weights of $G_{A,\ell}$ acting on $V_\ell(A)$. We will denote by $\Omega(V_{\lambda_i}(A))$ $(1 \leq i \leq r)$ the set of weights of $G_{A,\ell}$ acting on $V_{\lambda_i}(A)$. We have $\Omega(V_\ell(A)) = \cup_{i=1}^{r} \Omega(V_{\lambda_i}(A))$.

By Theorem 2.1.4(a), we know that $\rho_{A,\ell} : \mathrm{Gal}_K \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A))$ is semisimple. In the next lemma, we will see that $\rho_{A,\ell}$ decomposes into absolutely irreducible representations in a very special way.

Lemma 7.0.1.

(a) For each λ_i, we have an isomorphism

$$V_{\lambda_i}(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell \simeq e \cdot W_{\lambda_i}$$

of $(G_{A,\ell})_{\overline{\mathbb{Q}}_\ell}$ representations (equivalently, $\overline{\mathbb{Q}}_\ell[\mathrm{Gal}_K]$-modules), where the W_{λ_i} are irreducible. Moreover, $W_{\lambda_i} \not\simeq W_{\lambda_j}$ for $i \neq j$.

(b) The weights of the $(G_{A,\ell})_{\overline{\mathbb{Q}}_\ell}$ representation W_{λ_i} form a single orbit under the absolute Weyl group action and each weight has multiplicity one.

(c) For $i \neq j$, the representations W_{λ_i} and W_{λ_j} of $(G_{A,\ell})_{\overline{\mathbb{Q}}_\ell}$ have no common weights; equivalently, $\Omega(V_{\lambda_i}(A)) \cap \Omega(V_{\lambda_j}(A)) = \emptyset$.

Proof.

(a) First, we have natural isomorphisms

$$\begin{aligned} \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell &= D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \\ &= (D \otimes_E E) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \\ &= D \otimes_E (E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell) \\ &= \textstyle\prod_{i=1}^r D \otimes_E E_{\lambda_i} \end{aligned}.$$

By tensoring $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$ with $\overline{\mathbb{Q}}_\ell$ over $\mathbb{Q}_\ell$, we have

$$\mathrm{End}(A) \otimes_{\mathbb{Z}} \overline{\mathbb{Q}}_\ell = \prod_{i=1}^r (D \otimes_E E_{\lambda_i}) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell.$$

Note that $D \otimes_E E_{\lambda_i}$ naturally acts on each $V_{\lambda_i}(A) = V_\ell(A) \otimes_{(E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)} E_{\lambda_i}$ and commutes with the Galois action, so, we have an inclusion

$$(D \otimes_E E_{\lambda_i}) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell \hookrightarrow \mathrm{End}_{\overline{\mathbb{Q}}_\ell[\mathrm{Gal}_K]}(V_{\lambda_i}(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell).$$

Moreover, since $V_\ell(A) = \bigoplus_{i=1}^r V_{\lambda_i}(A)$, we have the inclusion

$$\prod_{i=1}^r \mathrm{End}_{\overline{\mathbb{Q}}_\ell[\mathrm{Gal}_K]}(V_{\lambda_i}(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell) \hookrightarrow \mathrm{End}_{\overline{\mathbb{Q}}_\ell[\mathrm{Gal}_K]}(V_\ell(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell).$$

By combining the above, we thus have the following inclusions:

$$\prod_{i=1}^r (D \otimes_E E_{\lambda_i}) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell \hookrightarrow \prod_{i=1}^r \mathrm{End}_{\overline{\mathbb{Q}}_\ell[\mathrm{Gal}_K]}(V_{\lambda_i}(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell) \hookrightarrow \mathrm{End}_{\overline{\mathbb{Q}}_\ell[\mathrm{Gal}_K]}(V_\ell(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell). \tag{7.0.1}$$

By Theorem 2.1.4(b), we have $\mathrm{End}(A) \otimes_{\mathbb{Z}} \overline{\mathbb{Q}}_\ell \simeq \mathrm{End}_{\overline{\mathbb{Q}}_\ell[\mathrm{Gal}_K]}(V_\ell(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell)$. So, the homomorphisms in (7.0.1) are isomorphisms. The isomorphism

$$\prod_{i=1}^r \mathrm{End}_{\overline{\mathbb{Q}}_\ell[\mathrm{Gal}_K]}(V_{\lambda_i}(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell) \simeq \mathrm{End}_{\overline{\mathbb{Q}}_\ell[\mathrm{Gal}_K]}(V_\ell(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell)$$

shows that $V_{\lambda_i}(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell$ and $V_{\lambda_j}(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell$ have no isomorphic irreducible representations in common for $i \neq j$. On the other hand, since ℓ splits completely in E, we have $E_{\lambda_i} = \mathbb{Q}_\ell$ and $(D \otimes_E E_{\lambda_i}) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell \simeq D \otimes_E \overline{\mathbb{Q}}_\ell$ is a central simple algebra over $\overline{\mathbb{Q}}_\ell$ (it is a general fact that if D is a central simple algebra with center E, then $D \otimes_E L$ is a central simple algebra over L for any field extension L of E). Hence the algebra $(D \otimes_E E_{\lambda_i}) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell$ is isomorphic to $M_e(\overline{\mathbb{Q}}_\ell)$ since $\overline{\mathbb{Q}}_\ell$ is algebraically closed. The isomorphism $\mathrm{End}_{\overline{\mathbb{Q}}_\ell[\mathrm{Gal}_K]}(V_{\lambda_i}(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell) \simeq M_e(\overline{\mathbb{Q}}_\ell)$ and the semisimplicity of the representation $\rho_{A,\ell}$ implies that $V_{\lambda_i}(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell$ is isotypic and moreover it is isomorphic to a direct summand of e copies of an irreducible representation W_{λ_i} of $\overline{\mathbb{Q}}_\ell[\mathrm{Gal}_K]$. The irreducible representations W_{λ_i} and W_{λ_j}, with $i \neq j$, are not isomorphic since $V_{\lambda_i}(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell$ and $V_{\lambda_j}(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell$ are not isomorphic.

(b) The follows from Proposition 2.3.6 and part (a).

(c) Recall that $\rho_{A,\ell} : \mathrm{Gal}_K \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A))$ induces a representation $\iota_{A,\ell} : G_{A,\ell} \hookrightarrow \mathrm{GL}_{V_\ell(A)}$. For each i, the $G_{A,\ell}$-action preserves $V_{\lambda_i}(A)$ and induces a representation $\iota_{A,\lambda_i} : G_{A,\ell} \to \mathrm{GL}_{V_{\lambda_i}(A)}$.

By (a), $\Omega(V_{\lambda_i}(A))$ is equal to the weights of W_{λ_i}. So by (b), the Weyl group of $(G_{A,\ell})_{\overline{\mathbb{Q}}_\ell}$ acts transitively on $\Omega(V_{\lambda_i}(A))$. So for $i \neq j$, $\Omega(V_{\lambda_i}(A))$ and $\Omega(V_{\lambda_j}(A))$ are either equal or disjoint.

Suppose $\Omega(V_{\lambda_i}(A)) = \Omega(V_{\lambda_j}(A))$ with $i \neq j$. We have

$$\mathrm{tr} \circ \iota_{A,\lambda_i}(t) = e \cdot \sum_{\alpha \in \Omega(V_{\lambda_i}(A))} \alpha(t) = e \cdot \sum_{\alpha \in \Omega(V_{\lambda_j}(A))} \alpha(t) = \mathrm{tr} \circ \iota_{A,\lambda_j}(t)$$

for all $t \in T$. Since $G_{A,\ell}$ is reductive, this implies that $\mathrm{tr} \circ \iota_{A,\lambda_i} = \mathrm{tr} \circ \iota_{A,\lambda_j}$ and hence ι_{A,λ_i} and ι_{A,λ_j} are isomorphic. Therefore, the representations $V_{\lambda_i}(A)$ and $V_{\lambda_j}(A)$ of $G_{A,\ell}$ are isomorphic. This contradicts (a) and hence $\Omega(V_{\lambda_i}(A))$ and $\Omega(V_{\lambda_j}(A))$ are disjoint. □

Lemma 7.0.2. *Each weight of the representation $V_\ell(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell$ of $(G_{A,\ell})_{\overline{\mathbb{Q}}_\ell}$ has multiplicity e.*

Proof. By Lemma 7.0.1(c), the sets $\Omega(V_{\lambda_i}(A))$ and $\Omega(V_{\lambda_j}(A))$ are disjoint for $i \neq j$. By Lemma 7.0.1(b), for each i, each weight in the representation W_{λ_i} of $(G_{A,\ell})_{\overline{\mathbb{Q}}_\ell}$ has multiplicity 1. So by Lemma 7.0.1(a), each weight of $V_\ell(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell$ has multiplicity e. □

7.1 Proof of Theorem 1.0.4

By Lemma 7.0.2, each weight of the representation $V_\ell(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell$ of $(G_{A,\ell})_{\overline{\mathbb{Q}}_\ell}$ has multiplicity e. So we have

$$P_{A,\mathfrak{p}}(x) = \prod_{\alpha \in \Omega(V_\ell(A))} (x - \alpha(t_\mathfrak{p}))^e$$

for all $\mathfrak{p}$ for which A has good reduction and $\mathfrak{p} \nmid \ell$, where $t_\mathfrak{p} \in T(\overline{\mathbb{Q}}_\ell)$ is any element conjugate to $\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p})$ in $G_{A,\ell}(\overline{\mathbb{Q}}_\ell)$.

By taking $A' = 0$ in Lemma 4.2.1, if we consider all distinct pairs of $\alpha, \beta \in \Omega(V_\ell(A))$, then for almost all $\mathfrak{p}$, $\alpha(t_\mathfrak{p}) \neq \beta(t_\mathfrak{p})$ for $\alpha \neq \beta$. Therefore, for almost all $\mathfrak{p}$, the Frobenius polynomial $P_{A,\mathfrak{p}}(x)$ is the e-th power of a separable polynomial.

CHAPTER 8

NUMBER OF POINTS ON ABELIAN VARIETIES

We will now prove the following theorem, as promised in §1, which says that the function $\mathfrak{p} \in S \mapsto |A(\mathbb{F}_\mathfrak{p})|$ determines A up to isogeny.

Theorem 8.0.1. *Let A and A' be abelian varieties defined over a number field K. Let S be any density 1 set of prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ for which A and A' have good reduction. Suppose*

$$|A(\mathbb{F}_\mathfrak{p})| = |A'(\mathbb{F}_\mathfrak{p})|$$

for all $\mathfrak{p} \in S$, then A is isogenous to A' (over K).

When A and A' are elliptic curves, Theorem 8.0.1 is an immediate consequence of Faltings' theorem since $P_{A,\mathfrak{p}}(x) = x^2 - (N(\mathfrak{p}) + 1 - |A(\mathbb{F}_\mathfrak{p})|)x + N(\mathfrak{p}) = P_{A',\mathfrak{p}}(x)$ for all $\mathfrak{p} \in S$, where $N(\mathfrak{p}) = |\mathbb{F}_\mathfrak{p}|$. In higher dimensions, the theorem does not seem to occur in the literature (and in fact is stated as a conjecture in [Per15]). The proof below was supplied by David Zywina.

Proof of Theorem 8.0.1. Fix a prime ℓ. Let $G := G_{A\times A',\ell}$; we can identify G with a closed algebraic subgroup of $G_{A,\ell} \times G_{A',\ell}$.

We claim that $\det(I - B) = \det(I - B')$ holds for every $(B, B') \in G(\mathbb{Q}_\ell)$. Define

$$Y := \{(B, B') \in G : \ \det(I - B) = \det(I - B')\};$$

it is a subvariety of G stable under conjugation. To prove the claim it suffices to show that $Y = G$. Take any $\mathfrak{p} \in S$ such that $\mathfrak{p} \nmid \ell$. By assumption we have $|A(\mathbb{F}_\mathfrak{p})| = |A'(\mathbb{F}_\mathfrak{p})|$ and so

$$\det(I - \rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p})) = |A(\mathbb{F}_\mathfrak{p})| = |A'(\mathbb{F}_\mathfrak{p})| = \det(I - \rho_{A',\ell}(\mathrm{Frob}_\mathfrak{p})).$$

Therefore, $\rho_{A\times A',\ell}(\mathrm{Frob}_{\mathfrak{p}}) \in Y(\mathbb{Q}_\ell)$ for all $\mathfrak{p} \in S$ with $\mathfrak{p} \nmid \ell$. By the Chebotarev density theorem, the Zariski closure G of $\rho_{A\times A',\ell}(\mathrm{Gal}_K)$ is contained in Y. Therefore, $Y = G$ and the claim is now clear.

Fix any $(B, B') \in G(\mathbb{Q}_\ell)$ and $\lambda \in \mathbb{Q}_\ell^\times$. It is known that G contains the group $\mathbb{G}_m$ of homotheties [Bog80]. So $(\lambda^{-1}B, \lambda^{-1}B') \in G(\mathbb{Q}_\ell)$ and by our claim above, we have

$$\det(I - \lambda^{-1}B) = \det(I - \lambda^{-1}B')$$

for all $\lambda \in \mathbb{Q}_\ell^\times$ and so

$$\lambda^{g'} \det(\lambda I - B) = \lambda^{g} \det(\lambda I - B').$$

Hence, we have $x^{g'} \det(xI - B) = x^g \det(xI - B') \in \mathbb{Q}_\ell[x]$ since their difference is a polynomial with infinitely many roots in $\mathbb{Q}_\ell$. Since $\mathbb{Q}_\ell[x]$ is a UFD and $\det(B)\det(B') \neq 0$, it follows that $g = g'$ and $\det(xI - B) = \det(xI - B')$.

So for all $\mathfrak{p} \in S$, we have $\rho_{A\times A',\ell}(\mathrm{Frob}_{\mathfrak{p}}) = (\rho_{A,\ell}(\mathrm{Frob}_{\mathfrak{p}}), \rho_{A',\ell}(\mathrm{Frob}_{\mathfrak{p}})) \in G(\mathbb{Q}_\ell)$ and hence

$$P_{A,\mathfrak{p}}(x) = \det(xI - \rho_{A,\ell}(\mathrm{Frob}_{\mathfrak{p}})) = \det(xI - \rho_{A',\ell}(\mathrm{Frob}_{\mathfrak{p}})) = P_{A',\mathfrak{p}}(x).$$

By Faltings' theorem, we deduce that A is isogenous to A'. □

BIBLIOGRAPHY

[Bog80] Fedor Alekseivich Bogomolov, *Sur l'algébricité des représentations l-adiques*, C. R. Acad. Sci. Paris Sér. A-B **290** (1980), no. 15, A701–A703. MR574307 ↑8

[Bou05] Nicolas Bourbaki, *Lie groups and Lie algebras. Chapters 7–9*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 2005. Translated from the 1975 and 1982 French originals by Andrew Pressley. MR2109105 ↑2.3

[Fal86] Gerd Faltings, *Finiteness theorems for abelian varieties over number fields*, Arithmetic geometry (Storrs, Conn., 1984), 1986, pp. 9–27. Translated from the German original [Invent. Math. **7**3 (1983), no. 3, 349–366; ibid. **7**5 (1984), no. 2, 381; MR 85g:11026ab] by Edward Shipz. MR861971 ↑1, 2.1

[Gro66] A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III*, Inst. Hautes Études Sci. Publ. Math. **28** (1966), 255. MR0217086 ↑3.3

[HP13] Chris Hall and Antonella Perucca, *On the prime divisors of the number of points on an elliptic curve*, C. R. Math. Acad. Sci. Paris **351** (2013), no. 1-2, 1–3. MR3019751 ↑1.1

[Hum75] James E. Humphreys, *Linear algebraic groups*, Springer-Verlag, New York-Heidelberg, 1975. Graduate Texts in Mathematics, No. 21. MR0396773 ↑2.3, 2.3

[Kat01] Nicholas M. Katz, *Sums of Betti numbers in arbitrary characteristic*, Finite Fields Appl. **7** (2001), no. 1, 29–44. Dedicated to Professor Chao Ko on the occasion of his 90th birthday. MR1803934 ↑3.4

[LP97] Michael Larsen and Richard Pink, *A connectedness criterion for l-adic Galois representations*, Israel J. Math. **97** (1997), 1–10. MR1441234 ↑1, 2.1, 2.1, 5.2

[Orr15] Martin Orr, *Lower bounds for ranks of Mumford-Tate groups*, Bull. Soc. Math. France **143** (2015), no. 2, 229–246. MR3351177 ↑2.3.4

[Per15] Antonella Perucca, *The prime divisors of the number of points on abelian varieties*, J. Théor. Nombres Bordeaux **27** (2015), no. 3, 805–814. MR3429320 ↑1.1, 8

[Pin98] Richard Pink, *l-adic algebraic monodromy groups, cocharacters, and the Mumford-Tate conjecture*, J. Reine Angew. Math. **495** (1998), 187–237. MR1603865 ↑2.3, 2.3, 2.3

[Rat15] Nicolas Ratazzi, *Classe d'isogénie de variétés abéliennes pleinement de type GSp*, J. Number Theory **147** (2015), 156–171. MR3276321 ↑1.1

[Ser00] Jean-Pierre Serre, *Œuvres. Collected papers. IV*, Springer-Verlag, Berlin, 2000. 1985–1998. MR1730973 ↑2.1, 2.1

[Ser79] ———, *Groupes algébriques associés aux modules de Hodge-Tate*, Journées de Géométrie Algébrique de Rennes. (Rennes, 1978), Vol. III, 1979, pp. 155–188. MR563476 ↑2.3, 2.3.4

[Ser98] ———, *Abelian l-adic representations and elliptic curves*, Research Notes in Mathematics, vol. 7, A K Peters, Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original. MR1484415 ↑4.2

[Win02] J.-P. Wintenberger, *Démonstration d'une conjecture de Lang dans des cas particuliers*, J. Reine Angew. Math. **553** (2002), 1–16. MR1944805 ↑2.1, 2.1

[Zyw14] David Zywina, *The splitting of reductions of an abelian variety*, Int. Math. Res. Not. IMRN **18** (2014), 5042–5083. MR3264675 ↑1.1, 2.1, 2.1

[Zyw16] ———, *Abelian varieties over large algebraic fields with infinite torsion*, Israel J. Math. **211** (2016), no. 1, 493–508. MR3474973 ↑2.1, 3.3, 3.4