THE WEIL CONJECTURES FOR ABELIAN VARIETIES

HAHN LHEEM, TOMMASO LUCANTONI

Abstract. We prove two of the Weil conjectures for abelian varieties over finite fields. First, we show that the zeta function attached to an abelian variety is a rational function, where we can further factor the numerator and denominator into polynomials with integer coefficients. We then prove the analogue of the Riemann Hypothesis for finite fields, which translates to a statement about the magnitude of the complex roots of each polynomial factor in the zeta function.

Contents

1. The Weil Conjectures

In 1949, André Weil postulated the following conjecture about smooth projective varieties over finite fields.

Conjecture 1.1 (Weil Conjectures)**.** *Let X be a smooth projective variety of dimension d over a finite field $\mathbb{F}_q$. Denote $N_n := \#X(\mathbb{F}_{q^n})$. Define the zeta function of X as the power series $Z(X,T) \in \mathbb{Q}[[T]]$ given by*

$$Z(X,T) := \exp\left(\sum_{n=1}^{\infty} N_n \frac{T^n}{n}\right).$$

The zeta function satisfies the following properties:

(1) (Rationality) There exist polynomials $P_i(T) \in \mathbb{Z}[T]$, for $0 \leq i \leq 2d$, such that

$$Z(X,T) = \frac{P_1(T)P_3(T)\cdots P_{2d-1}(T)}{P_0(T)P_2(T)\cdots P_{2d}(T)}.$$

(2) (Functional Equation) The zeta function satisfies the functional equation

$$Z\left(X, \frac{1}{q^d T}\right) = \pm q^{\chi d/2} T^{\chi} Z(X,T)$$

where $\chi = \sum_{i \geq 0} (-1)^i \deg P_i(T)$.

(3) (Analogue of Riemann Hypothesis) Each $P_i(T)$ splits over $\mathbb{C}$ as $\prod_j (1 - \alpha_{i,j}T)$, where each $\alpha_{i,j}$ satisfies $|\alpha_{i,j}| = q^{i/2}$.

(4) (Betti numbers) If X is the good reduction at $\mathfrak{p}$ of a smooth projective variety $\widetilde{X}$ over some number field $K \hookrightarrow \mathbb{C}$, where $\mathfrak{p} \subset \mathcal{O}_K$ is prime, then $\deg P_i(T)$ is equal to the i^{th} Betti number of $\widetilde{X}(\mathbb{C})$.

All four conjectures have since been proven, thanks to the advent of a new cohomology theory for varieties over finite fields – étale cohomology, first laid out in SGA4 [AGV64] and SGA5 [Gro77] – which is compatible with singular cohomology for the complex analytic topology. The most difficult of these conjectures is the analogue of the Riemann Hypothesis, which was proved by Deligne in both [Del74] and [Del80].

In this report, we will provide a proof of the first and third statements for when X is an abelian variety over a finite field, primarily following [Mum74].[1]

1.1. Cultural Asides.

The proof of the Weil conjectures is known as one of the hallmark achievements of mathematics in the 20th century. The benefits of these statements even just for the abelian variety setting are far-reaching. We illustrate a few examples.

The first, addressed in Professor Cadoret's lecture, is that we can obtain a $\mathbb{Q}$-compatibility result for a system of Galois representations obtained by the ℓ-adic realization of some abelian variety. Let $X_{/\mathbb{F}_p}$ be an abelian variety and ρ_ℓ be the ℓ-adic Galois representation given by its ℓ-adic Tate module (defined just before §2.1). Denote π as the Frobenius morphism at p, which acts on $X(\overline{\mathbb{F}_p})$ and hence on $T_\ell X$ (see Lemma 5.2). Once we identify $T_\ell X \simeq H^1_{\text{ét}}(X_{\overline{\mathbb{F}_p}}, \mathbb{Z}_\ell)^\vee$, we can obtain that $P_1(T)$ is the characteristic polynomial of π on $H^1_{\text{ét}}$.

Given two primes $\ell, \ell' \neq p$, taking the ℓ-adic cohomology of $X_{\overline{\mathbb{F}_p}}$ will produce *two* factorizations of $Z(X,T)$ as in conjecture (1) above. We will write the polynomials corresponding to ℓ, ℓ' as $P_{i,\ell}(T)$, $P_{i,\ell'}(T)$, respectively. Note that the definition of $Z(X,T)$ is independent of any choice of ℓ. But by looking at the roots of each $P_{i,\ell}(T)$ (resp., $P_{i,\ell'}(T)$), the Riemann Hypothesis forces equality $P_{i,\ell}(T) = P_{i,\ell'}(T)$ for each $0 \leq i \leq 2d$. In particular, for $i = 1$ we get that the characteristic polynomial of the Frobenius is *independent of ℓ.*

We list a few more notable consequences below, albeit with minimal detail.

[1] All page number references are for the second edition, not the first.

- We can get a Hasse-like bound for the number of $\mathbb{F}_{q^n}$-rational points of X. In particular, the Riemann Hypothesis will guarantee that
$$\left|\#X(\mathbb{F}_{q^n}) - q^{n\dim X}\right| = O\left(q^{n\left(\dim X - \frac{1}{2}\right)}\right).$$
This follows from the expression for N_m given in the beginning of §5.1.
- The Weil conjectures for curves can be deduced from the Weil conjectures for their Jacobians, which are abelian varieties. This sequence of ideas is summarized in Exercises V.1.10 and C.5.7 of [Har77].
- Deligne proved in [Del71] that for any normalized new eigenform f of weight $k \geq 2$ and level N, the p^{th} Fourier coefficient $a_p(f)$ (for $p \neq N$) satisfies $|a_p(f)| \leq 2p^{(k-1)/2}$. In his proof, he shows that this result (the Ramanujan conjecture) is implied by the Weil conjectures for modular curves.
- One may ask whether all maps between ℓ-adic Tate modules come from morphisms between their corresponding abelian varieties. (In other words, is Theorem 3.5 really an isomorphism?) By results of Tate and Honda, they gave the affirmative in the setting of finite fields if one only considers the Galois-equivariant maps between Tate modules. A neat consequence of this is that there is a bijection between isogeny classes of abelian varieties over $\mathbb{F}_q$ and algebraic numbers with magnitude $\sqrt{q}$, where X corresponds to an eigenvalue of Frobenius on $T_\ell X$. This implies, for instance, that all supersingular elliptic curves over $\mathbb{F}_q$ are isogenous. Some discussions can be found in [Mum74, Appendix I].

2. Abelian Varieties

Throughout, we denote k to be an algebraically closed field. A **variety** over k is an integral separated scheme of finite type over k.

Definition 2.1 (Abelian Variety)**.** An **abelian variety** over k is a complete variety X over k with k-morphisms of varieties $m : X \times X \to X$ (multiplication), $e : \operatorname{Spec} k \to X$ (identity), and $\iota : X \to X$ (inverse) satisfying the usual group axioms.

Remark 2.2. Although the definition does not require the group law to be commutative, one can show that commutativity must follow if X is complete. This is a direct consequence of the Rigidity Lemma, see [Mum74, pp. 40-41]. In this spirit, we denote $0 = 0_X \in X$ as the image of e.

We will denote $x + y \coloneqq m(x, y)$. Let $x \in X$. We denote T_x as the translation-by-x map $T_x : y \mapsto x + y$. It follows from m being a morphism of varieties that T_x is an automorphism of X as a variety.

Remark 2.3. Via translation, one can show an abelian variety X must be everywhere non-singular. Indeed, there must exist a non-singular point $x_0 \in X$, and as T_x is a morphism of varieties, $T_x(x_0) = x_0 + x$ is non-singular for all $x \in X$.

A homomorphism of abelian varieties is a morphism of varieties which is also a group homomorphism on the underlying k-points. We denote the additive group of all homomorphisms between X and Y as $\operatorname{Hom}(X, Y)$ and the ring of endomorphisms of X as $\operatorname{End}(X)$. Later, we will be interested in the $\mathbb{Q}$-algebra $\operatorname{End}^0(X) \coloneqq \operatorname{End}(X) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Definition 2.4 (Isogeny)**.** An **isogeny** is a surjective homomorphism of abelian varieties $X \to Y$ with finite kernel.

We say two abelian varieties are *isogenous* if there exists an isogeny between them. Isogenies are of particular importance, one reason being that they become isomorphisms (hence invertible) in $\operatorname{End}^0(X)$. (See the discussion directly following Theorem 3.1.)

Suppose $f : X \to Y$ is an isogeny. Following general facts of morphisms of varieties, we have that the separable degree of f is $\deg_s f = f^{-1}(y)$ for almost all $y \in Y$. But the group structure on Y allows us to construct an explicit bijection between any two fibers, so we get the following result.

Proposition 2.5. *For an isogeny f between abelian varieties,*

$$\deg_s(f) = \# \ker(f).$$

Example 2.6 (Multiplication-by-n)**.** Let n be an integer such that $\operatorname{char} k \nmid n$. Denote the multiplication-by-n on X by n_X and its kernel as $X[n]$. First, it is separable, as one can show the induced map on the tangent space at 0_X is also multiplication-by-n. Using a collection of results in the next subsection, one can also show that $\deg n_X$, and hence $\#X[n]$, is $n^{2 \dim X}$. But this is true for all n, in particular all divisors $m \mid n$, which is only possible if $X[n] \simeq (\mathbb{Z}/n\mathbb{Z})^{2 \dim X}$ as groups.

Although they will not be used until later, we introduce the ℓ-adic Tate module for $\ell \neq \operatorname{char} k$ prime. The **ℓ-adic Tate module** of X is simply the inverse limit

$$T_\ell X \coloneqq \varprojlim_n X[\ell^n],$$

where the inverse system consists of the multiplication-by-ℓ maps $X[\ell^{n+1}] \xrightarrow{\ell_X} X[\ell^n]$. From above, we have $X[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^{2 \dim X}$ as groups, meaning $T_\ell X \simeq \mathbb{Z}_\ell^{2 \dim X}$ as $\mathbb{Z}_\ell$-modules.

From the Grothendieck perspective using cohomology, the ℓ-adic Tate module is at the heart of this story. Indeed, for an abelian variety X over k, the ℓ-adic Tate module is isomorphic to the dual of $H^1_{\text{ét}}(X_{\overline{k}}, \mathbb{Z}_\ell)$. Furthermore, abelian varieties satisfy the amazing property that for any $1 \leq r \leq 2 \dim X$, we have an isomorphism

$$\bigwedge^r H^1_{\text{ét}}(X_{\overline{k}}, \mathbb{Z}_\ell) \simeq H^r_{\text{ét}}(X_{\overline{k}}, \mathbb{Z}_\ell).$$

Although not done in the language of étale cohomology, this perspective elucidates our proof of the Weil conjectures, such as the factorization of the polynomials $P_r(T)$, which are just the characteristic polynomials of π on $H^r_{\text{ét}}$, in §5.1.

Even better, morphisms of abelian varieties induce $\mathbb{Z}_\ell$-linear maps between their ℓ-adic Tate modules. This comes from the fact that any $f : X \to Y$ restricts to $f^{(n)} : X[\ell^n] \to Y[\ell^n]$ for all $n \geq 1$, and these $f^{(n)}$ morphisms are compatible with multiplication-by-ℓ. We denote the induced map from $f : X \to Y$ on the Tate modules as $T_\ell f$.

2.1. **Dual Abelian Variety.** Associated to an abelian variety X is its *dual variety* $X^\vee$, which is isogenous to X. This construction will be crucial in understanding the structure of $\mathrm{End}^0(X)$.

Our first useful feature of line bundles on complete varieties is the Seesaw Theorem. It is called so roughly because it says that for a line bundle on a product of complete varieties, its restrictions on the first component dictate those on the second. We state it without proof; see [Mum74, p.51] for a proof.

Theorem 2.7 (Seesaw Theorem)**.** *Let X be a complete variety, T a variety, and $\mathcal{L} \in \mathrm{Pic}(X \times T)$. Then, the set $T' \coloneqq \{t \in T : \mathcal{L}_{X\times\{t\}} \simeq \mathcal{O}_{X\times\{t\}}\}$ is closed in T. In addition, there exists some $\mathcal{L}' \in \mathrm{Pic}(T')$ such that $\mathcal{L}|_{X\times T'} \simeq \mathrm{pr}_2^*\mathcal{L}'$ where $\mathrm{pr}_2 : X \times T' \to T'$.*

Corollary 2.8. *Let X, Y be complete varieties, and choose $\mathcal{L}_y \in \mathrm{Pic}(X)$ (more honestly, a line bundle on $X\times\{y\}$) for each $y \in Y$. There exists at most one $\mathcal{L} \in \mathrm{Pic}(X\times Y)$ such that $\mathcal{L}|_{\{x\}\times Y}$ is trivial for some $x \in X$ and $\mathcal{L}|_{X\times\{y\}} \simeq \mathcal{L}_y$ for all $y \in Y$.*

Proof. It suffices to consider the case where $\mathcal{L}_y \simeq \mathcal{O}_X$ for all $y \in Y$. But then the Seesaw Theorem tells us that $\mathcal{L} \simeq \mathrm{pr}_2^*\mathcal{L}'$ for some $\mathcal{L}' \in \mathrm{Pic}(Y)$. The second condition translates to $\mathcal{L}|_{\{x\}\times Y} \simeq (\mathrm{pr}_2^*\mathcal{L}')|_{\{x\}\times Y} \simeq \mathcal{L}'$ being trivial, so $\mathcal{L}$ is trivial. □

This helps yield the Theorem of the Cube, which dictates more generally the behavior of line bundles on (products of) complete varieties. We state this also without proof, but see [Mum74, p.53].

Theorem 2.9 (Theorem of the Cube)**.** *Let X, Y, Z be complete varieties*[2] *with specified base points x_0, y_0, z_0 respectively. Let $\mathcal{L}$ be a line bundle on $X \times Y \times Z$ such that its restrictions to each of $\{x_0\} \times Y \times Z$, $X \times \{y_0\} \times Z$, and $X \times Y \times \{z_0\}$ are trivial. Then $\mathcal{L}$ must be trivial.*

This gives us the important Theorem of the Square.

Theorem 2.10 (Theorem of the Square)**.** *Let X be an abelian variety and $\mathcal{L} \in \mathrm{Pic}(X)$. Then for any $x, y \in X$,*

$$T_{x+y}^*\mathcal{L} \otimes \mathcal{L} \cong T_x^*\mathcal{L} \otimes T_y^*\mathcal{L}.$$

Proof. Let $p_i : X \times X \times X \to X$ the projection on the i-th component, denote by $n_{ij} = p_i + p_j$ and by $n = p_1 + p_2 + p_3$.

We want to apply the theorem of the cube to the line bundle

$$\mathcal{M} = n^*\mathcal{L} \otimes n_{12}^*\mathcal{L}^{-1} \otimes n_{23}^*\mathcal{L}^{-1} \otimes n_{13}^*\mathcal{L}^{-1} \otimes p_1^*\mathcal{L} \otimes p_2^*\mathcal{L} \otimes p_3^*\mathcal{L}$$

on $X \times X \times X$. Consider $q : X \times X \to X \times X \times X$ such that $q(x, x') = (0, x, x')$. Then

$$q^*\mathcal{M} = m^*\mathcal{L} \otimes q_1^*\mathcal{L}^{-1} \otimes q_2^*\mathcal{L}^{-1} \otimes m^*\mathcal{L}^{-1} \otimes 0^*\mathcal{L} \otimes q_1^*\mathcal{L} \otimes q_2^*\mathcal{L}$$

where q_j is the projection on the j-th factor, m is the addition and 0 is the zero map. Hence $q^*\mathcal{M}$ is trivial and by symmetry $\mathcal{M}$ is trivial on $X \times \{0\} \times X$ and on $X \times X \times \{0\}$ too. Therefore, applying the theorem of the cube, $\mathcal{M}$ is trivial.

[2] The result still holds if one of them is not complete. As all of our applications will be when X, Y, Z are abelian, hence complete, this hypothesis suffices.

Finally, the statement follows taking the pullback of $\mathcal{M}$ with respect to $(c_x, c_y, id) : X \to X \times X \times X$, where c_x and c_y denote the constant map at x and y respectively. □

Fix a line bundle $\mathcal{L}$ on X. Define $\phi_{\mathcal{L}}$ to be the natural map (a priori of sets)

$$\begin{aligned}\phi_{\mathcal{L}} : X &\to \operatorname{Pic}(X)\\ x &\mapsto (T_x^*\mathcal{L} \otimes \mathcal{L}^{-1}).\end{aligned}$$

The Theorem of the Square shows that $\phi_{\mathcal{L}}$ is in fact a group homomorphism. We care about $\phi_{\mathcal{L}}$ in the case where $\mathcal{L}$ is ample. The existence of an ample line bundle is guaranteed by the following lemma.

Lemma 2.11. *Every abelian variety is projective.*

Proof. It suffices to find a divisor $D \in \operatorname{Div}(X)$ such that the complete linear system $|D|$ separates points and tangent vectors.

We begin by constructing a divisor $D_0 = \sum Z_i$ which separates $0_X \in X$ from all other points and $0 \in T_0X$ from all other tangent vectors. We can do this using the crucial fact that X, being a variety, is Noetherian, hence satisfies the descending chain condition for closed subsets. In brief, we can implement the following procedure, outlined below:

(1) Suppose we have prime divisors $\{Z_1, \ldots, Z_r\}$ such that $\bigcap Z_i \supsetneq \{0\}$. Let $p \neq 0$ be in the intersection.
(2) We can find some open affine subset which contains both 0 and p: choose an open affine neighborhood $U \ni 0$, choose some $u \in U \cap (U + p)$, and then take $U' := U + p - u$. We may identify U' as a closed subscheme of some $\mathbb{A}^n$.
(3) In this affine space, we can find a hyperplane $H \subset \mathbb{A}^n$ which passes through 0 but not p.
(4) Define $Z_{r+1} := \overline{H \cap U'} \subset X$.

By the Noetherian property, this process must eventually terminate, so we can find a finite set of prime divisors whose collective intersection is just $\{0_X\}$. We can run a similar procedure to isolate just the zero tangent vector.

Denote this finite set of prime divisors from this procedure as $\{Z_1, \ldots, Z_n\}$. We claim that the divisor

$$D := 3D_0 = 3\sum_{i=1}^{n} Z_i$$

produces the desired complete linear system.

We prove that $|D|$ separates points; the proof for separating tangent vectors is similar. Note that for any collection of points $x_1, \ldots, x_n, y_1, \ldots, y_n$, the Theorem of the Square (2.10) guarantees that

$$\sum_{i=1}^{n} T_{x_i}^* Z_i + T_{y_i}^* Z_i + T_{-x_i-y_i}^* Z_i \in |D|.$$

Fix $p \neq q \in X$. Note from our choice of $\{Z_i\}$ that there must exist some i such that $q - p \notin Z_i$. Setting $p = x_i$, note then that $q \notin T_p^* Z_i$, but clearly $p \in T_p^* Z_i$ since

$0 \in Z_i$. We also have that $\{y_i : q \in T^*_{y_i} Z_i\}$ (and likewise $\{y_i : q \in T^*_{-p-y_i} Z_i\}$) is a proper closed subset of X, hence we can find some y_i which lies in the intersection of their complements. Similarly, for all other $j \neq i$, we can always find a pair of points (x_j, y_j) such that q does not lie on any of the divisors $T^*_{x_j} Z_j$, $T^*_{y_j} Z_j$, $T^*_{-x_j-y_j} Z_j$. In conclusion, we have constructed an effective divisor in $|D|$, namely $\sum_{i=1}^n T^*_{x_i} Z_i + T^*_{y_i} Z_i + T^*_{-x_i-y_i} Z_i$, which separates p and q. As this construction works for any $p \neq q \in X$, we are done. □

Fix an ample line bundle $\mathcal{L}$ on X. Restrict the codomain of $\phi_{\mathcal{L}}$ to its image so that $\phi_{\mathcal{L}}$ is surjective. As $\phi_{\mathcal{L}}$ is a group homomorphism, its image is an abelian group. Our aim is to enrich $\phi_{\mathcal{L}}$ to be an isogeny of *abelian varieties*, i.e., construct an abelian variety, which we will call the dual of X, whose underlying group of k-points is isomorphic to $\operatorname{Im} \phi_{\mathcal{L}}$. Implicit in the uniqueness of the dual abelian variety is that our construction should ultimately be *independent* of the choice of ample $\mathcal{L}$. This is a legitimate concern, although we sweep it under the rug for our purposes.

But first, if we hope to upgrade $\phi_{\mathcal{L}}$ to an isogeny, we must verify that its kernel is finite.

Lemma 2.12. *If $\mathcal{L} \in \operatorname{Pic}(X)$ is ample, then $\ker \phi_{\mathcal{L}}$ is finite.*

Proof. Denote $Y = (\ker \phi_{\mathcal{L}})^0$ as the connected component of the identity. We will show $\dim Y = 0$. Note $\mathcal{L}|_Y$ is ample and $T^*_y(\mathcal{L}|_Y) \simeq \mathcal{L}|_Y$ for all $y \in Y$ as $Y \subset \ker \phi_{\mathcal{L}}$. Denoting $\operatorname{pr}_i : Y \times Y \to Y$ as the projections, the translation-invariance of $\mathcal{L}|_Y$ implies $\mathcal{M} := m^*\mathcal{L}|_Y \otimes \operatorname{pr}_1^*\mathcal{L}|_Y^{-1} \otimes \operatorname{pr}_2^*\mathcal{L}|_Y^{-1}$ is trivial on all restrictions $Y \times \{y\}$, $\{y\} \times Y$. The Seesaw Theorem (in the form of Corollary 2.8) then forces $\mathcal{M}$ to be trivial.

Consider the pullback of $\mathcal{M}$ along the morphism $\operatorname{id}_Y \times (-\operatorname{id}_Y) : Y \to Y \times Y$. By definition of $\mathcal{M}$, we have $(\operatorname{id}_Y \times -\operatorname{id}_Y)^*\mathcal{M} = \mathcal{L}|_Y \otimes (-\operatorname{id}_Y)^*\mathcal{L}|_Y$. But $\mathcal{M}$ is trivial, so the pullback must also be trivial. However, both $\mathcal{L}|_Y$ and $(-\operatorname{id}_Y)^*\mathcal{L}|_Y$ are ample, so the trivial bundle on Y must be trivial. This is only possible if $\dim Y = 0$. □

From this alone, we can offer a construction of the dual abelian variety, thanks to the general construction of quotient varieties as provided in [Mum74, §7].

Theorem 2.13. *Let X be an algebraic variety and G a finite subgroup of $\operatorname{Aut}(X)$. Suppose that for any $x \in X$, the orbit Gx of x is contained in an affine open subset of X. Then, there is a unique (up to isomorphism) pair (Y, π), where Y is a variety and $\pi : X \to Y$ a morphism, satisfying the following conditions:*

(1) In the category Top, we have $Y = G\backslash X$ and π is the natural projection map.
(2) If $\pi_*(\mathcal{O}_X)^G$ is the subsheaf of G-invariants of $\pi_*(\mathcal{O}_X)$, then the natural homomorphism $\mathcal{O}_Y \to \pi_*(\mathcal{O}_X)^G$ is an isomorphism.

Furthermore, π is finite, surjective, and separable, and it is étale if G acts freely on X. This construction is also universal in the sense that any G-invariant morphism $f : X \to Z$ must factor uniquely through (Y, π).

Of course, it is unclear that this quotient is independent of the choice of $\mathcal{L}$, both as a group and as a variety. For conciseness, we will not properly address this discrepancy. The important thing for us is that a "dual" abelian variety $X^\vee$ of X exists and is equipped with a morphism $X \to X^\vee$, both of which we have constructed after a choice of ample line bundle.

We give a general impression of how to remove the independence on $\mathcal{L}$. The idea is to define the dual abelian variety via a representable functor. Informally, the functor which takes a k-variety T to a family of line bundles over X parametrized by T (equivalently, a line bundle on $X \times T$ with extra conditions) is representable by a k-variety. The construction in [Mum74, p.74] takes a more direct yet similar approach, where the representability is reflected in the construction of the *Poincaré bundle*. Showing that this construction is independent of any choice of ample line bundle relies on a bijection (in fact, an equivalence of categories) between coherent $\mathcal{O}_Y$-modules and coherent G-sheaves on X, where $Y = G\backslash X$ as in the theorem above. (The precise statement is [Mum74, Prop. 2].)

An important feature of dualizing is that it also applies to isogenies. If $f : X \to Y$ is an isogeny, then there exists a (unique) isogeny $f^\vee : Y^\vee \to X^\vee$, called the **dual isogeny** of f. The construction of the dual isogeny comes from the representability of the dual abelian variety (relatedly, the universal property of the Poincaré bundle). For our purposes, we offer the following fact and guarantee:

(1) An isogeny $f : X \to Y$ induces by pullback a group homomorphism $f^* : \operatorname{Pic} Y \to \operatorname{Pic} X$, which by restriction to the degree 0 part gives us a group homomorphism $f^* : \operatorname{Pic}^0 Y \to \operatorname{Pic}^0 X$.
(2) This map can be enriched to a morphism of abelian varieties $f^\vee : Y^\vee \to X^\vee$.

Remark 2.14. Even more generally, one can construct the *relative Picard scheme*, which is again defined by some moduli problem. In this regard, the pullback map f^* can really be seen as a morphism of group schemes, and restricting to the connected component at the identity gives $f^\vee$.

3. Structure of Endomorphism Algebra

Let X be an abelian variety. The concern of this section is to describe the structure of $\operatorname{End}^0(X) := \operatorname{End}(X) \otimes_{\mathbb{Z}} \mathbb{Q}$, leading up to the handy Theorem 3.10.

Even in the elliptic curve case, where over $\mathbb{Q}$ the most common scenario $\operatorname{End}^0(E) = \mathbb{Q}$ does not supply us with much information about the elliptic curve, the rare cases where $\mathbb{Q} \subsetneq \operatorname{End}^0(E)$ gives rise to the beautiful theory of complex multiplication. Over finite fields, which is the primary interest of this exposition, the Frobenius morphism ensures every elliptic curve has “complex multiplication,” and a close study of the endomorphism ring ultimately gives the Weil conjectures for elliptic curves. See [Sil09, §5] for details.

Before we proceed, we state a fundamental result relating the group structure of X to isogenies out of X. Recall the quotient variety construction from Theorem 2.13.

Theorem 3.1 (Finite Subgroup–Separable Isogeny Correspondence)**.** *For an abelian variety X, there is a bijective correspondence*

$$\{\textit{finite subgroups } K \subset X\} \quad \longleftrightarrow \quad \left\{ \begin{array}{c} \textit{(isomorphism classes of)} \\ \textit{separable isogenies } f : X \to Y \end{array} \right\}$$

where $K \subset X$ corresponds to $f : X \to Y = X/K$. Here, we say two isogenies $f_1 : X \to Y_1$ and $f_2 : X \to Y_2$ are isomorphic if there exists an isomorphism $g : Y_1 \xrightarrow{\simeq} Y_2$ such that $f_2 = g \circ f_1$.

Proof. Let $K \subset X$ be a finite subgroup. Theorem 2.13 immediately offers that the natural projection $f : X \to X/K$ is a surjective, separable morphism of varieties with finite kernel. It remains to check X/K is an abelian variety, but one can check the composite $X \times X \xrightarrow{m} X \xrightarrow{f} X/K$ factors through $(X \times X)/(K \times K) \simeq X/K \times X/K$, so the group law given by m induces a morphism $X/K \times X/K \to X/K$.

Conversely, let $g : X \to Y$ be a separable isogeny. By definition, its kernel is a finite subgroup of X. We check that g is isomorphic to $f : X \to X/K$, which is a separable isogeny from above, or equivalently that $X/K \simeq Y$. The universality of the quotient variety (the last statement of Theorem 2.13) gives us a unique morphism $X/K \xrightarrow{h} Y$. By construction, it is an epimorphism with trivial kernel. At the same time, Zariski's Main Theorem [Vak25, Theorem 28.6.2] says that h is finite as it is proper and quasifinite. We conclude from the fact that a finite morphism with singleton fibers everywhere is an isomorphism. □

We give a useful application of this result. If an isogeny $f : Y \to X$ has kernel of order n, then $\ker f \subseteq \ker n_Y$. But this means $n_Y : Y \to Y$ can factor through $X = Y/\ker f$, hence there exists an isogeny $g : X \to Y$ such that $g \circ f = n_Y$. Note then that $f \circ g = n_X$ as well by the following simple slick computation: for any $x \in X$, we can find some $y \in f^{-1}(x)$, and then $(f \circ g)(x) = (f \circ g)(f(y)) = f(g \circ f(y)) = f(n \cdot y) = n \cdot f(y) = n \cdot x$.

In $\operatorname{End}^0(X)$, the isogeny n_X is clearly invertible. We can interpret the above as follows: consider the category AbVar_k^0 whose objects are abelian varieties over k and whose morphisms are given by $\operatorname{Mor}(X, Y) := \operatorname{Hom}^0(X, Y)$. Then, isogenous abelian varieties are *isomorphic* in AbVar_k^0. In effect, by linearizing homomorphisms over $\mathbb{Q}$, we only care about abelian varieties up to isogeny. This is advantageous to us because of the following theorem.

Theorem 3.2 (Poincare's complete reducibility)**.** *Let X be an abelian variety and $Y \subset X$ be any abelian subvariety. Then, there exists another abelian subvariety $Z \subset X$ such that X is isogenous to $Y \times Z$.*

In other words, AbVar_k^0 is a semisimple abelian category, all of whose objects have finite length.

Proof. Let $i : Y \hookrightarrow X$ the inclusion and $i^\vee : X^\vee \to Y^\vee$ its dual homomorphism. Moreover, let $\mathcal{L}$ be an ample line bundle on X, so $\phi_{\mathcal{L}}$ is an isogeny. We define Z to be the connected component of 0 in $\phi_{\mathcal{L}}^{-1}(\ker i^\vee)$. We have

$$\dim Z = \dim \ker i^\vee \geq \dim X^\vee - \dim Y^\vee = \dim X - \dim Y$$

where the equalities come from the fact that isogenies preserve dimensions. Further, by definition $z \in Z \cap Y$ if and only if $(T_z^* \mathcal{L} \otimes \mathcal{L}^{-1})|_Y$ is trivial that is z is in $\ker \phi_{\mathcal{L}|_Y}$. Since $\mathcal{L}|_Y$ is ample, $\phi_{\mathcal{L}|_Y}$ is an isogeny and has finite kernel. Hence, the sum $Y \times Z \to X$ has finite kernel and it is surjective because

$$\dim(Y \times Z) = \dim Y + \dim Z \geq \dim Y + \dim X - \dim Y = \dim X,$$

so the two are isogenous. □

Call an abelian variety **simple** if it has no nonzero abelian subvariety besides itself. Like with finite-dimensional semisimple representations, we can obtain the following results.

Corollary 3.3 (Unique Decomposition)**.** *An abelian variety X is isogenous to a finite product $\prod_i X_i^{n_i}$, where the X_i's are pairwise non-isogenous simple abelian varieties and $n_i \in \mathbb{Z}_{>0}$. The n_i's are uniquely determined, as are the X_i's up to isogeny.*

Corollary 3.4 (Structure of $\operatorname{End}^0(X)$)**.** *Let X be an abelian variety. If X decomposes (isogenously) as $\prod_i X_i^{n_i}$, then*

$$\operatorname{End}^0(X) = \bigoplus_i M_{n_i}(D_i),$$

where $D_i = \operatorname{End}^0(X_i)$ is a finite-dimensional division algebra over $\mathbb{Q}$ and $M_{n_i}(D_i)$ is the algebra of $n_i \times n_i$ matrices over D_i.

The finite-dimensionality of the $\mathbb{Q}$-division algebras D_i is the only subtle detail, but it is a direct consequence of the following theorem, in conjunction with $\dim_{\mathbb{Z}_\ell} T_\ell X = 2 \dim X$.

Theorem 3.5. *Let X, Y be abelian varieties over k, and fix a prime $\ell \neq \operatorname{char} k$. The map*

$$\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \operatorname{Hom}(X, Y) \to \operatorname{Hom}_{\mathbb{Z}_\ell}(T_\ell X, T_\ell Y)$$

induced from $f \mapsto T_\ell f$ is injective.

We can summarize Corollary 3.4 by Wedderburn's Theorem as "$\operatorname{End}^0(X)$ *is a finite-dimensional semisimple algebra over* $\mathbb{Q}$."

The upshot of this structure is that such algebras come equipped with canonical trace and norm forms, such that all other trace and norm forms arise from the canonical ones.

Definition 3.6 (Trace and Norm Forms)**.** Let A be a finite-dimensional associative algebra over a field k. A **trace form** on A is a k-linear map $S : A \to k$ such that $S(ab) = S(ba)$ for any $a, b \in A$. A **norm form** on A is a non-zero map $N : A \to k$ satisfying $N(ab) = N(ba)$ for any $a, b \in A$ and, upon choosing a k-basis $\{a_1, \ldots, a_n\}$ of A, we have $N\left(\sum_{i=1}^n x_i a_i\right) = P(x_1, \ldots, x_n)$ where P is a polynomial. The last statement can be reformulated as N being a *polynomial function.*

One important example of a norm form on $\operatorname{End}^0(X)$ is the degree. To show it is a polynomial function, one requires this deep lemma relating degrees and Euler characteristics.

Lemma 3.7. *Let $f : X \to Y$ be an isogeny between abelian varieties over k. If $\mathcal{L} \in \operatorname{Pic} Y$ is ample, then*

$$\chi(f^*\mathcal{L}) = \deg(f) \cdot \chi(\mathcal{L}),$$

where χ is the Euler characteristic.

The proof of this requires Grothendieck's *dévissage* theorem [GD61, Théorème 3.1.2]. For a complete treatment which implicitly uses dévissage in its argument, see [Mum74, §12, Theorem 2]. An alternate, more general approach to this is via the Hirzebruch–Riemann–Roch Theorem. In any case, we use this lemma to show that the degree function is polynomial.

Proposition 3.8. *Let X be a simple abelian variety and $d = \dim X$. Then, the degree function on $\operatorname{End}(X)$ extends to a norm form on $\operatorname{End}^0(X)$ which has degree $2d$ as a (homogeneous) polynomial function.*

Proof. The degree function is clearly multiplicative, so we only need to prove the polynomial function statement. By Example 2.6, we know $\deg n = n^{2d}$, hence it only remains to show that the degree map is a polynomial function. Explicitly, we will show $D(n) = \deg(n\phi + \psi)$ is a polynomial function for any $\phi, \psi \in \operatorname{End}(X)$. By the above lemma, noting that any nonzero endomorphism of simple X must be an isogeny, we have that for any ample line bundle $\mathcal{L}$ on X,

$$D(n) = \frac{\chi((n\phi + \psi)^*\mathcal{L})}{\chi(\mathcal{L})}.$$

The denominator is constant, so we reduce the problem to showing $\chi((n\phi + \psi)^*\mathcal{L})$ is polynomial in n.

Denote $\mathcal{L}_n \coloneqq (n\phi + \psi)^*\mathcal{L}$. We will proceed similarly to the proof of the Theorem of the Square (2.10), replacing the projections p_i with the three morphisms $n\phi + \psi$, ϕ, and ϕ. Applying the Theorem of the Cube to the analogous line bundle

$$\mathcal{M} \coloneqq \mathcal{L}_{n+2} \otimes \mathcal{L}_{n+1}^{-1} \otimes \mathcal{L}_{n+1}^{-1} \otimes (2\phi)^*\mathcal{L}^{-1} \otimes \mathcal{L}_n \otimes \phi^*\mathcal{L} \otimes \phi^*\mathcal{L},$$

we can deduce that $\mathcal{M}$ is in fact trivial, and hence $\mathcal{L}_{n+2} \otimes \mathcal{L}_{n+1}^{-2} \otimes \mathcal{L}_n$ is independent of n. It follows that there exist line bundles $\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3 \in \operatorname{Pic} X$ such that

$$\mathcal{L}_n = \mathcal{M}_1^{\frac{n(n-1)}{2}} \otimes \mathcal{M}_2^n \otimes \mathcal{M}_3.$$

By the Hirzebruch–Riemann–Roch theorem [Ful98, Corollary 15.2.1], one can show that $\chi(\mathcal{M}_i^{p(n)})$, for any polynomial $p(n)$, is a polynomial in n. The theorem also implies that the Euler characteristic of the tensor product is a polynomial in n, as it is a polynomial on each component. This completes the proof. □

The next lemma describes the reduced trace and norm forms for finite-dimensional simple algebras. Upon restriction to its simple factors, one can determine all trace and norm forms for semisimple $\mathbb{Q}$-algebras like $\operatorname{End}^0(X)$.

Lemma 3.9 (Canonical Trace/Norm Forms)**.** *Let A be a finite-dimensional associative simple k-algebra for some infinite field k. Let K be the center of A, and suppose it is a separable field extension over k. There exists a* ***canonical trace form*** *Tr^0 of A over K such that any norm form of A over k must be equal to $(N_{K/k} \circ N^0)^r$ for some $r \in \mathbb{Z}_{\geq 0}$. Likewise, there exists a* ***canonical norm form*** *N^0 of A over K such that any trace form of A over k must be equal to $\phi \circ \operatorname{Tr}^0$ for some k-linear map $\phi : K \to k$.*

We now reach the most important result of this section. Attached to the endomorphism algebra $\operatorname{End}^0(X)$ (or, as we will shortly prefer, the $\mathbb{Q}_\ell$-algebra $\mathbb{Q}_\ell \otimes_{\mathbb{Q}} \operatorname{End}^0(X)$) are two natural norm forms: the degree (Proposition 3.8) and the determinant of the induced map on $T_\ell X$. Note that as polynomial functions, both have degree $2 \dim X$, the former via Proposition 3.8 and the latter from $\operatorname{rank}_{\mathbb{Z}_\ell} T_\ell X = 2\dim X$. The next theorem asserts that these two norm forms are in fact the same.

Theorem 3.10. *Let X be an abelian variety and $f \in \operatorname{End}(X)$. Fix a prime $\ell \neq \operatorname{char}(k)$, and denote $T_\ell f$ as the induced endomorphism of $T_\ell X$. Then,*

$$\deg f = \det T_\ell f.$$

Proof. We prove it in the case where X is simple. In the general case, one can decompose $\mathbb{Q}_\ell \otimes_{\mathbb{Z}} \operatorname{End}(X)$ into simple $\mathbb{Q}_\ell$-algebras via Corollary 3.4 and apply the proceeding argument to each simple component. Using notation from Lemma 3.9, denote $N_{\text{red}} = N_{K/k} \circ N^0$, so any other norm form on $\mathbb{Q}_\ell \otimes_{\mathbb{Z}} \operatorname{End}(X)$ must be of the form N_{red}^r.

Denote $d = \dim X$. From the above discussion, we see that both $f \mapsto \deg f$ and $f \mapsto \det T_\ell f$ give rise to norm forms on $\mathbb{Q}_\ell \otimes_{\mathbb{Z}} \operatorname{End}(X)$ which have degree $2d$ as polynomial functions. Denote the respective norm maps as $N_{\deg}$ and $N_{\det}$, respectively. We know then that $N_{\deg} = N_{\text{red}}^{r_1}$ and $N_{\det} = N_{\text{red}}^{r_2}$ for some $r_1, r_2 \in \mathbb{Z}$. To show $r_1 = r_2$, it suffices to show that $|N_{\deg}(\alpha)|_\ell = |N_{\det}(\alpha)|_\ell$ for any $\alpha \in \mathbb{Q}_\ell \otimes_{\mathbb{Z}} \operatorname{End}(X)$. By homogeneity and continuity, it suffices to show the equality just for all $\alpha = f \in \operatorname{End}(X)$. But this follows from the string of equalities

$$|\deg f|_\ell = |\#\ker f|_\ell = \lim_{n\to\infty} (\#(\ker f)[\ell^n])^{-1} = (\#\operatorname{coker} T_\ell f)^{-1} = |\det T_\ell f|_\ell.$$

Thus, $\deg f = \det T_\ell f$ when X is simple. The general case follows by comparing the ℓ-adic valuations of $N_{\deg}$ and $N_{\det}$ on each simple factor of $\mathbb{Q}_\ell \otimes_{\mathbb{Z}} \operatorname{End}(X)$. □

We may state the theorem in a slightly more practical form, which is the version we use in the proof of the Riemann Hypothesis (Proposition 5.5).

Corollary 3.11. *Adopt the same notation as above. Denote $P(T) \coloneqq \det(T \cdot \operatorname{id}_{T_\ell X} - T_\ell f)$ as the characteristic polynomial of $T_\ell f$. Then $P(T)$ is monic of degree $2 \dim X$, has coefficients in $\mathbb{Z}$, and satisfies*

$$\deg(n \cdot \operatorname{id}_X - f) = P(n)$$

for all $n \in \mathbb{Z}$.

Proof. The equality is trivial from the theorem, as well as the fact that $P(T)$ is monic of degree $2 \dim X$. For the integrality of its coefficients, we first note that its coefficients must all be rational as $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$. Additionally, we may deduce from Theorem 3.5 that $\operatorname{End}(X)$ is a finite $\mathbb{Z}$-module, and hence f satisfies some monic polynomial relation with coefficients in $\mathbb{Z}$. Thus, the eigenvalues of $T_\ell f$ are algebraic integers, so all coefficients of $P(T)$ are also algebraic integers. The conclusion follows from $\mathbb{Q} \cap \{\text{algebraic integers}\} = \mathbb{Z}$. □

4. Weil Pairing and Rosati Involution

We want to define a pairing on $T_\ell(X) \times T_\ell(X^\vee)$. To do so, we first define a pairing on $X[\ell^n] \times X^\vee[\ell^n]$.

Let λ be an ℓ-torsion point in $X^\vee$. We denote by $\mathcal{L}$ the line bundle corresponding to λ and by D the divisor such that $L = \mathcal{O}_X(D)$. By definition of λ, $\mathcal{L}^\ell$ is trivial, hence ℓD is the divisor of a rational function f. The same holds for $\ell_X^*\mathcal{L}$ and we denote by g the rational function whose divisor is $\ell_X^* D$. Then, $\operatorname{div} \ell_X^* f = \ell_X^* \ell D = \operatorname{div} g^\ell$, thus $g(x)^\ell = \alpha f(\ell x)$ for a constant $\alpha \in k$. Using this last equality, we have for every $a \in X[\ell]$

$$\left(\frac{g(x)}{g(x+a)}\right)^\ell = 1.$$

So, it make sense to define for $a \in X[\ell]$, $\lambda \in X^\vee[\ell]$,

$$\widetilde{e_\ell}(a, \lambda) = \frac{g(x)}{g(x+a)}.$$

Doing the same construction for ℓ^k, $k \geq 1$ we define $\widetilde{e_{\ell^k}}$. Moreover, we can prove that for any $k \geq 1$ and for any $a \in X[\ell^{k+1}]$, $\lambda \in X^\vee[\ell^{k+1}]$,

$$\widetilde{e_{\ell^k}}(\ell a, \ell\lambda) = \widetilde{e_{\ell^{k+1}}}(a, \lambda),$$

so passing to the inverse limit we define the Weil pairing

$$e_\ell : T_\ell X \times T_\ell X^\vee \to \mathbb{Z}_\ell.$$

This is a $\mathbb{Z}_\ell$-bilinear pairing and it is non-degenerate. Moreover, if $f : X \to Y$ is a homomorphism of abelian varieties and $T_\ell f$ is the induced morphism on the Tate modules, Weil pairing satisfies

$$e_\ell(T_\ell f(x), y) = e_\ell(x, T_\ell f^\vee(y))$$

for every $x \in T_\ell X$, $y \in T_\ell X^\vee$.

Weil pairing is a very useful tool in the theory of abelian varieties because we can also define it as a non-degenerate pairing on $T_\ell X \times T_\ell X$: fix a line bundle $\mathcal{L}$ and define for $x, y \in T_\ell X$,

$$e_\ell^{\mathcal{L}}(x, y) = e_\ell(x, T_\ell \phi_{\mathcal{L}}(y)).$$

This is a skew-symmetric non-degenerate pairing.

4.1. **Rosati Involution.**

Our next aim is to define an involution on $\operatorname{End}^0(X)$. This involution will be crucial in defining a non-degenerate pairing on $\operatorname{End}^0(X)$ that we will use to prove Riemann Hypothesis for the zeta function associated to an abelian variety. We fix an ample line bundle $\mathcal{L}$ on X so that $\phi_{\mathcal{L}}$ is an isogeny.

Definition 4.1. The Rosati involution on the algebra $\operatorname{End}^0(X)$ with respect to $\mathcal{L}$ is

$$\begin{aligned} ' : \operatorname{End}^0(X) &\to \operatorname{End}^0(X) \\ \phi &\mapsto \phi' = \phi_{\mathcal{L}}^{-1} \circ \phi^\vee \circ \phi_{\mathcal{L}}. \end{aligned}$$

Remark 4.2. The Rosati involution is $\mathbb{Q}$-linear and for every ϕ, $\psi \in \operatorname{End}^0(X)$, it satisfies $(\phi\psi)' = \psi'\phi'$ by property of dual isogeny.

Lemma 4.3. *The Rosati involution is an involution.*

Proof. We will use the Weil pairing to prove the lemma. Let $x, y \in T_\ell X$, $\phi \in \mathrm{End}^0(X)$ then

$$\begin{aligned} e_\ell^{\mathcal{L}}(x, \phi' y) &= e_\ell(x, \phi_{\mathcal{L}} \circ \phi_{\mathcal{L}}^{-1} \circ \phi^\vee \circ \phi_{\mathcal{L}} y) \\ &= e_\ell(x, \phi^\vee \circ \phi_{\mathcal{L}}) \\ &= e_\ell(\phi x, \phi_{\mathcal{L}} y) \\ &= e_\ell^{\mathcal{L}}(\phi x, y). \end{aligned}$$

This means that $\phi'' = \phi$ as we wanted to prove. □

The Rosati involution is very useful because it allows to define a quadratic form on $\mathrm{End}^0(X)$.

Theorem 4.4. *Let S be the trace form on $\mathrm{End}^0 X$ induced by the canonical trace forms on its simple factors. For every non zero $\phi \in \mathrm{End}^0(X)$, $S(\phi\phi') > 0$, thus S defines a definite positive quadratic form on $\mathrm{End}^0 X$.*

Proof. See [Mum74, Section 21, Theorem 1]. □

5. Proof of Weil Conjectures (1 and 3)

We now deliver our promise. Here, X will be an abelian variety over a finite field $\mathbb{F}_q$ (for q a power of p), and $\overline{X} = \operatorname{Spec} \overline{\mathbb{F}_q} \times_{\operatorname{Spec} \mathbb{F}_q} X$ is the base change of X to the algebraic closure of $\mathbb{F}$.

The key player in these proofs will be the (absolute) Frobenius morphism $\pi = \pi_{\overline{X}}$ of $\overline{X}$. We define this now.

Definition 5.1 (Frobenius morphism)**.** The **Frobenius morphism** on X is the automorphism $\pi_X : X \to X$ which is the identity as a map of topological spaces and the structure sheaf morphism $\mathcal{O}_X \to \mathcal{O}_X$ given by $s \mapsto s^q$. The Frobenius morphism on $\overline{X}$ is the automorphism $\pi = \pi_{\overline{X}}$ of $\overline{X}$ obtained from π_X by base extension.

We briefly review the necessary properties of π.

Lemma 5.2. *Let X be a variety over $\overline{\mathbb{F}_q}$. The points on $X(\overline{\mathbb{F}_q})$ fixed by π^n are exactly the $\mathbb{F}_{q^n}$-rational points $X(\mathbb{F}_{q^n})$.*

Proof. We can look locally, so assume $X = \operatorname{Spec} \mathbb{F}_q[X_1, \dots, X_r]/I$ is affine. Then π^n induces the morphism $\overline{X_i} \mapsto \overline{X_i}^{q^n}$ on the ring of functions, so the geometric point $(x_1, \dots, x_r)$ maps to $(x_1^{q^n}, \dots, x_r^{q^n})$ under π^n. We have $x_i = x_i^{q^n}$ iff $x_i \in \mathbb{F}_{q^n}$. □

Lemma 5.3. *Suppose X has an $\mathbb{F}_{q^n}$-rational point. The endomorphism $1 - \pi^n$ of X is separable.*

Proof. Let $x \in X(\mathbb{F}_{q^n})$, which exists by assumption. As $1 = \mathrm{id}_X$ induces the identity on the tangent space at x, it suffices to show π^n induces the zero map. We can again work locally, in which case the differential of the map $\overline{X_i} \mapsto \overline{X_i}^{q^n}$ in characteristic p is indeed the zero map. □

Remark 5.4. We can show when X is an abelian variety over $\overline{\mathbb{F}_q}$, then it has an $\mathbb{F}_q$-rational point. Write $\pi(x) = \pi(0_X) + h(x)$ for some $h \in \operatorname{End}(X)$. As π on the tangent space at x_0 is 0, so is h, and hence $1-h$ induces the identity. In particular, this means $1-h$ is étale. But by construction, $1-h$ fixes 0, and it is an easy consequence of the Rigidity Lemma that any morphism between abelian varieties, seen just as varieties, which preserves the identity is automatically a group homomorphism. It follows that $1-h$ is an endomorphism of X as an abelian variety, and étaleness forces it to be surjective. Take $x' \in X(\overline{\mathbb{F}_q})$ such that $(1-h)(x') = \pi(0_X)$. Then, we have $x' = \pi(0) + h(x') = \pi(x')$, and we conclude x' is $\mathbb{F}_q$-rational.

5.1. **Rationality of Zeta Function.** The proof that $Z(X,T)$ is a rational function as specified is a direct consequence of Corollary 3.11 for $f = \pi$ the Frobenius morphism for $\overline{X}$. Denote $\omega_1, \dots, \omega_{2d}$ the roots of the characteristic polynomial of π and $N_n \coloneqq \#X(\mathbb{F}_{q^n})$ as in the statement of the Weil conjectures. Because the fixed points of π^n, equivalently the kernel of $1-\pi^n$ (which is separable by Lemma 5.3), are the $\mathbb{F}_{q^n}$-rational points of X by Lemma 5.2, we have the nice equality

$$N_n = \deg(1-\pi^n) = \prod_{i=1}^{2g}(1-\omega_i^n).$$

Moreover we define

$$P_r(T) = \prod_{1\le i_1<\dots<i_r\le 2d} (T - \omega_{i_1}\dots\omega_{i_r})$$

for every $0 \le r \le 2d$. Then, $P_r(T)$ has integer coefficients because they are obtained inductively from $P_1(T)$ that is the characteristic polynomial of π and has integer coefficients by Corollary 3.11. Finally,

$$Z(X,T) = \exp\left(\sum_{n=1}^{\infty} N_n \frac{T^n}{n}\right) = \sum_{m=0}^{\infty} \frac{1}{m!}\left(\sum_{n=1}^{\infty} N_n \frac{T^n}{n}\right)^m.$$

Taking the log and using the fact that $-\log(1-t) = \sum_{m=1}^{\infty} \frac{t^m}{m}$, we find that

$$\log(Z(X,T)) = \log\left(\frac{P_1(T)\dots P_{2d-1}(T)}{P_0(T)\dots P_{2d}(T)}\right),$$

as we wanted.

5.2. **Riemann Hypothesis.** The proof of the Riemann Hypothesis follows from the following proposition that given an endomorphism α connects the product $\alpha\alpha'$ with the absolute value of the roots of the characteristic polynomial of α.

Proposition 5.5. *Let X be an abelian variety, $'$ be the Rosati involution and α be an endomorphism of X such that $\alpha\alpha' = a \in \mathbb{Z}$. Denote by $\omega_1, \dots, \omega_{2d}$ the roots of the characteristic polynomial P of α. Then $\mathbb{Q}[\alpha] \subset \operatorname{End} X$ is semisimple and $|\omega_i|^2 = a$ for every $i = 1, \dots, 2d$.*

Proof. Let P, respectively Q, be the characteristic, respectively minimal, polynomial of α. Then, $Q \mid P$ by definition. Moreover, by Corollary 3.11, P is also the characteristic polynomial of $T_l\alpha$. But then, $Q(\omega)$ is an eigenvalue of $T_lQ(\alpha)$ that is the zero map because $Q(\alpha) = 0$. Therefore, $Q(\omega) = 0$ and P and Q have the same roots. We restrict the proof to the roots of Q.

If we restrict the trace form on $\operatorname{End}^0 X$ to a trace form on $\mathbb{Q}[\alpha]$, it still defines a definite positive quadratic form as in Theorem 4.4. Moreover, the Rosati involution defines an automorphism of $\mathbb{Q}[\alpha]$ because $\alpha' = \frac{a}{\alpha} \in \mathbb{Q}[\alpha]$.

$\mathbb{Q}[\alpha]$ has finite dimension over $\mathbb{Q}$, hence it is an artinian ring. We want to write it as product of fields and to do so, we have to prove that it does not have any nilpotents. Let $\beta \in \mathbb{Q}[\alpha]$ and denote $b = \beta\beta'$. Since $S(\beta\beta') > 0$, $b \neq 0$. Moreover, $b' = b$, so $b^2 \neq 0$ because $S(bb') > 0$. Inductively, any power of b is non zero, hence any power of a it is. This also proves that $\mathbb{Q}[\alpha]$ is a semisimple algebra because it is product of simple algebras.

Denote $\mathbb{Q}[\alpha] = K_1 \times \cdots \times K_r$. Since for every $\beta \in \mathbb{Q}[\alpha]$, $S(\beta\beta') > 0$, the Rosati involution has to be an automorphism of every K_i. Hence, K_i is totally real with trivial involution or an imaginary quadratic extension of a totally real field. If we extend every embedding $\rho : K_i \hookrightarrow \mathbb{C}$ to homomorphisms $\mathbb{Q}[\alpha] \to \mathbb{C}$, then every ω is equal to $\rho(\alpha)$ for a unique ρ. The fact that it is unique comes from the fact that we are considering ω as a root of Q. This concludes the proof because $\rho(\alpha') = \overline{\rho(\alpha)}$ and

$$a = \rho(a) = \rho(\alpha\alpha') = \rho(\alpha)\overline{\rho(\alpha)} = |\omega|^2$$

as we wanted. □

We would like to apply this proposition to the proof of Riemann Hypothesis. Let $\mathcal{L}_0$ a line bundle on X. We apply a base change so that $\mathcal{L}_0 \times_{\operatorname{Spec}\mathbb{F}_q} \operatorname{Spec}\mathbb{F}_{q^m}$ is an ample line bundle over $X \times_{\operatorname{Spec}\mathbb{F}_q} \operatorname{Spec}\mathbb{F}_{q^m}$. With an abuse of notation, we denote $X \times_{\operatorname{Spec}\mathbb{F}_q} \operatorname{Spec}\mathbb{F}_{q^m}$ by X and q^m by q. It remains to prove that $\pi\pi' = q$. By definition of the Rosati involution, this is equivalent to prove that

$$\pi^\vee(\phi_{\mathcal{L}}(\pi(x))) = q\phi_{\mathcal{L}}(x)$$

for every $x \in X$. Since

$$\pi^\vee(\phi_{\mathcal{L}}(\pi(x))) = \pi^*(T^*_{\pi(x)}\mathcal{L} \otimes \mathcal{L}^{-1}) = T^*_x\pi^*\mathcal{L} \otimes \pi^*\mathcal{L}^{-1}$$

and $\pi^*\mathcal{L} = \mathcal{L}^q$, we find that

$$\pi^\vee(\phi_{\mathcal{L}}(\pi(x))) = (T^*_x\mathcal{L} \otimes \mathcal{L}^{-1})^q$$

as we wanted. Thus, by Proposition 5.5, we have proved the Riemann Hypothesis for abelian varieties.

References

[AGV64] M. Artin, A. Grothendieck, and J. L. Verdier. *SGA 4: Théorie des topos et cohomologie étale des schémas.* Vol. 269–270–305. Lecture Notes in Mathematics. Séminaire de Géométrie Algébrique du Bois Marie 1963–1964. Springer-Verlag, 1963–1964.

[Del71] Pierre Deligne. “Formes modulaires et représentations ℓ-adiques”. In: *Séminaire Bourbaki, 21^e année (1968/69), Exposé 355*. Vol. 179. Lecture Notes in Mathematics. Springer, 1971, pp. 139–172.

[Del74] Pierre Deligne. “La conjecture de Weil: I”. In: *Publications Mathématiques de l’IHÉS* 43 (1974), pp. 273–307.

[Del80] Pierre Deligne. “La conjecture de Weil: II”. In: *Publications Mathématiques de l’IHÉS* 52 (1980), pp. 137–252.

[Ful98] William Fulton. *Intersection Theory*. 2nd. Vol. 2. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. With appendices by the author and Robert MacPherson. Berlin: Springer-Verlag, 1998. ISBN: 978-3-540-62046-9.

[Gro77] A. Grothendieck. *SGA 5: Cohomologie l-adique et fonctions L*. Vol. 589. Lecture Notes in Mathematics. Séminaire de Géométrie Algébrique du Bois Marie 1965–1966. Springer-Verlag, 1977.

[GD61] Alexandre Grothendieck and Jean Dieudonné. “Éléments de géométrie algébrique. III. Étude cohomologique des faisceaux cohérents. I”. In: *Publications Mathématiques de l’IHÉS* 11 (1961), pp. 5–167.

[Har77] Robin Hartshorne. *Algebraic Geometry*. Vol. 52. Graduate Texts in Mathematics. New York: Springer-Verlag, 1977. ISBN: 978-0-387-90244-9.

[Mum74] David Mumford. *Abelian Varieties*. Vol. 5. Tata Institute of Fundamental Research Studies in Mathematics. Bombay: Tata Institute of Fundamental Research, 1974.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. 2nd. Vol. 106. Graduate Texts in Mathematics. Springer, 2009. ISBN: 978-0-387-09493-9. DOI: 10.1007/978-0-387-09494-6.

[Vak25] Ravi Vakil. *The Rising Sea: Foundations of Algebraic Geometry*. Princeton University Press, 2025, p. 704. ISBN: 9780691268668.