Abelian Varieties

Yifeng Huang

February 25, 2018

Abstract

The first three chapters are written as a course project for MATH 632: Algebraic Geometry II, taught by Dr. Tyler Foster in Winter 2016 in University of Michigan. The fourth chapter is a course project for MATH 731: Abelian Varieties, taught by Prof. Bhargav Bhatt in Fall 2017 in Michigan.

Contents

1 Abelian Varieties

1.1 Basics

Throughout this article, k is an algebraic closed field. A **variety** over k means a separable, finite-type and reduced scheme over k. In particular, irreducibility is not assumed. A **group variety** over k is a k-variety equipped with a structure of a group scheme over k. When understood from the context, the ground field k is often omitted in the notation. **Points** will always mean closed points unless specified otherwise.

Definition 1.1. An **abelian variety** is a irreducible projective group variety, i.e. a irreducible projective variety A equipped with a group structure such that the multiplication map $\mu : A \times A \to A$, $(x, y) \mapsto xy$ and the inverse map $\iota : A \to A$, $x \mapsto x^{-1}$ are regular.

Remark. Note that we do not assume A is an abelian group here, but we will show in Corollary 1.5 that the projectivity forces A to be abelian, which justifies the terminology. Also, note that it suffices to assume that A is connected, because A is always smooth (as a group variety) and a smooth and connected variety must be irreducible. (Otherwise the intersection of components must be singular.)

Remark. A more common and historically correct definition is to assume that A is complete (i.e. proper) rather than projective - the first important abelian varieties, namely the Jacobian varieties constructed over $\mathbb{C}$, is not known to be projective a priori. However, it can be proved that a complete algebraic group must be projective. In most of the arguments in this article, the properties of projective varieties I use also hold for complete varieties, except the existence of very ample line bundles.

Lemma 1.2 (Rigidity Lemma)**.** *Let X, Y, Z be varieties with X being projective. Let $x_0 \in X, y_0 \in Y$ and $z_0 \in Z$. Suppose $f : X \times Y \to Z$ is a regular map such that*

$$f((X \times y_0) \cup (x_0 \times Y)) = \{z_0\}.$$

Then f is the constant map z_0.

Proof. Choose an affine open neighborhood U of z_0 in Z. Since X is projective, X is proper over k, so the map $\pi_Y : X \times Y \to Y$ is closed. Consider the open subset

$$V = Y - \pi_Y(f^{-1}(Z - U)) = \{y \in Y : f(X \times y) \subseteq U\}.$$

We have $y_0 \in Y$. Note that $X \times y \cong X$ is projective, and U is affine, so maps from $X \times y$ into U must be constant. Thus for $y \in V$ and $x \in X$, we have $f(x, y) = f(x_0, y) = z_0$. In other words $f(X \times V) = \{z_0\}$. Since $X \times V$ is open dense in $X \times Y$ and Z is separable, we have $f(X \times Y) = \{z_0\}$. □

Theorem 1.3. *Let A, B be abelian varieties, and $f : A \to B$ a regular map sending identity 1_A to identity 1_B. Then f is a group homomorphism, and we call f a **homomorphism** of abelian varieties.*

Proof. Consider $\phi : A \times A \to B$ defined by

$$\phi(a, a') = f(aa')f(a')^{-1}f(a)^{-1}.$$

Observe that if $a = 1_A$ or $a' = 1_A$, since $f(1_A) = 1_B$, we have $\phi(a, a') = 1_B$.

Hence $\phi((1_A \times A) \cup (A \times 1_A)) = \{1_B\}$. By Lemma 1.2, $\phi(a, a') = 1_H$ for all a, a'. This precisely says $f(aa') = f(a)f(a')$, or f is a group homomorphism. □

Corollary 1.4. *The algebraic group structure on an abelian variety is uniquely determined by its identity element.*

Proof. Let $(A, 1, \cdot)$ and $(A, 1, *)$ be two algebraic group structure on A. Consider the identity map $id : (A, 1, \cdot) \to (A, 1, *)$. By Theorem 1.3, it is a group homomorphism, thus an isomorphism. □

Corollary 1.5. *An abelian variety A is necessarily an abelian group.*

Proof. Note that a group is abelian if and only if the inverse map is a group homomorphism. Consider the inverse map $\iota : A \to A$. Since $\iota(1_A) = 1_A$, ι is a group homomorphism. □

Remark. From now on, we shall use additive notation $(A, 0, +)$ for an abelian variety.

1.2 Rational Maps to Abelian Varieties

Let V, W be varieties where V is irreducible, and α be a rational map from V to W. Then there is a largest open set $U \subseteq V$ where α is a morphism. We call U the **domain of definition** of α, and its complement $V - U$ the **locus of indeterminacy** of α.

Theorem 1.6. *A rational map $\alpha : V \dashrightarrow A$ from a smooth variety V to an abelian variety A is defined on the whole of V.*

We need the following lemma,

Lemma 1.7. *Let $\phi : V \dashrightarrow G$ be a rational map from a smooth variety V to a group variety G. Then its indeterminacy locus is either empty or has pure codimension 1.*

Proof. Look at the rational map $\Phi : V \times V \dashrightarrow G$ sending (x, y) to $\phi(x)\phi(y)^{-1}$. Let U be the domain of definition of ϕ. Consider the diagonal $\Delta \subseteq V \times V$. Note that Φ is already defined on $\Delta_U := \{(x, x) : x \in U\}$ with $\Phi(x, x) = e$, the identity element of G, so if Φ is defined at (x, x) after extension, we must have $\Phi(x, x) = e$ as well (since Δ_U is dense in Δ).

Consider the induced map on function field: $\Phi^* : k(G) \to k(V \times V)$. By the previous discussion, Φ is defined at (x, x) (after extension) iff the pullback of any local function near $e \in G$ is defined at (x, x), that is, $\Phi^*(\mathcal{O}_{G,e}) \subseteq \mathcal{O}_{V\times V,(x,x)}$. Hence the set of (x, x) such that Φ is not defined at (x, x) is the union of $P_f := \{Q \in V : \Phi^*(f) \notin \mathcal{O}_{V\times V,Q}\}$ intersecting Δ, where f ranges over all $\mathcal{O}_{G,e}$.

Claim that P_f is the union of poles of $g := \Phi^*(f)$. In other words, if we write $\operatorname{div}(g) = Z - P$ where Z, P are the sums of prime divisors with positive (negative, resp.) coefficients in $\operatorname{div}(g)$, then P_f is the support of P. Indeed, g is defined at $Q \in V \times V$, then g is regular on some neighborhood W of Q, so $\operatorname{div}(g)|_W \geq 0$, so the support of P is outside W. In particular P_f avoids Q. On the other hand, if $Q \notin P_f$, let W be the complement of P_f, which is closed, then $\operatorname{div}(g)|_W \geq 0$, so g is regular on W because $V \times V$ is smooth (thus normal).

In particular, P_f has pure codimension 1 (if not empty) in $V \times V$, so its intersection with Δ has pure codimension 1 in Δ. Taking union of $P_f \cap \Delta$ for all (infinitely many) $f \in \mathcal{O}_{G,e}$, we still get pure codimension 1, because the intersection of Δ and the indeterminacy locus E of Φ is a priori a proper closed subset of Δ. To be specific, if $E \cap \Delta$ has a component with codimension at least 2, choose a point Q lying in this component only and a P_f passing through Q, then P_f must lie inside this component, which is absurd for dimension reason.

Claim that Φ is defined at (x, x) (after extension) if and only if ϕ is defined at x. It suffices to prove the forward implication. Let $W \times W' \subseteq V \times V$ be a neighborhood of (x, x) where Φ is

defined. Define $Y = W' \cap U$, which is nonempty because V is irreducible, but may not contain x a priori. Then for $w \in W$,

$$\phi(w) = \Phi(w, y)\phi(y)$$

defines ϕ on W, a neighborhood of x.

Hence $X - U = \{x \in V : \Phi \text{ is not defined on } (x, x)\} \cong E \cap \Delta$ has pure codimension 1, if not empty (here the isomorphism $X \cong \Delta$ is used).

□

Proof of Theorem 1.6. By Lemma 1.7, the indeterminacy locus of $\alpha : V \dashrightarrow A$ has codimension 1 if nonempty. But V is smooth and A is projective, by a classical theorem, the indeterminacy locus of α has codimension at least 2. The only possibility is that it is empty. In other words, α is defined on the whole of V. □

Corollary 1.8. *If abelian varieties A, B are birational via maps $f : A \dashrightarrow B$ and $g : B \to A$, then they are isomorphic as varieties with mutually inverse isomorphisms $f : A \to B$ and $g : B \to A$.*

Proof. By Theorem 1.6, f,g are regular. The compositions $f \circ g$ and $g \circ f$ are identities on an open dense subset, so that they are both identities. □

1.3 The Theorem of the Cube

The theorem of the cube is a fundamental theorem in the study of abelian varieties that can give a lot of identities in Picard group (i.e. isomorphisms of line bundles). The statement basically says that a invertible sheaf on a "cube" is trivial if and only if its restriction on three faces are all trivial.

Theorem 1.9 (Theorem of the Cube)**.** *Let U, V, W be irreducible projective varieties over k, and u_0, v_0, w_0 be closed points of U, V, W respectively, then an invertible sheaf $\mathcal{L} \in \mathrm{Pic}(U \times V \times W)$ is trivial iff its restrictions to*

$$U \times V \times w_0, U \times v_0 \times W, u_0 \times V \times W$$

are all trivial.

Proof. See [1, I.§5]. □

Notation 1.10. Given an abelian variety A, we use m, p, q to denote the maps $A \times A \to A$ with $m(a, b) = a + b, p(a, b) = a, q(a, b) = b$.

Corollary 1.11. *Let A be an abelian variety, define $p_i : A \times A \times A \to A$ be the projection to i-th factor (i=1,2,3), $p_{ij} = p_i + p_j$, $p_{123} = p_1 + p_2 + p_3$. Then for $\mathcal{L} \in \mathrm{Pic}(A)$, the invertible sheaf on $A \times A \times A$ is trivial:*

$$\mathcal{M} := p_{123}^* L \otimes p_{12}^* \mathcal{L}^\vee \otimes p_{23}^* \mathcal{L}^\vee \otimes p_{31}^* \mathcal{L}^\vee \otimes p_1^* L \otimes p_2^* L \otimes p_2^* L$$

Proof. Apply the theorem of the cube with $U = V = W = A$, $u_0 = v_0 = w_0 = 0$. Then it suffices to show that $\mathcal{M}|_{A \times A \times 0}$ is trivial (by symmetry).

Note that $\mathcal{M}|_{A \times A \times 0}$ is the pullback of M via $i : A \times A \to A \times A \times A$ sending (x, y) to $(x, y, 0)$.

We have

$$p_{123} \circ i = m$$

$$p_{12} \circ i = m$$

$$p_{23} \circ i = q$$

$$p_{31} \circ i = p$$

$$p_1 \circ i = p$$

$$p_2 \circ i = q$$

$$p_3 \circ i = 0$$

Hence $\mathcal{M}|_{A\times A\times 0} = m^*L \otimes m^*L^\vee \otimes q^*L^\vee \otimes p^*L^\vee \otimes p^*L \otimes q^*L$ is trivial. (Note that pullback of a line bundle under a constant map is trivial.) □

As an immediate corollary, we get the following identity that is the starting point of many formulae.

Theorem 1.12. *For any variety V and three maps $f, g, h : V \to A$ from V to an abelian variety A, then the following is trivial on V for all $\mathcal{L} \in \mathrm{Pic}(A)$:*

$$\mathcal{N} := (f+g+h)^*L \otimes (f+g)^*\mathcal{L}^\vee \otimes (g+h)^*L^\vee \otimes (h+f)^*L^\vee \otimes f^*L \otimes g^*L \otimes h^*L$$

Proof. This is the pullback of $\mathcal{M}$ in Corollary 1.11 by the map

$$(f, g, h) : V \to A \times A \times A$$

□

Notation 1.13. Let A be an abelian variety. For $n \in \mathbb{Z}$, denote by n_A the endomorphism of A given by multiplication by n (using the $\mathbb{Z}$-module structure on A). For $a \in A$, denote by t_a the translation map $A \to A$ sending x to $x + a$.

Proposition 1.14. *Let $\mathcal{L}$ be an invertible sheaf on an abelian variety A, then we have*

$$n_A^*\mathcal{L} \cong \mathcal{L}^{\binom{n+1}{2}} \otimes (-1)_A^*\mathcal{L}^{\binom{n}{2}}$$

Proof. For any $n \in Z$, apply Theorem 1.12 with endomorphisms $f = n_A, g = 1_A, h = (-1)_A$, then we get

$$n^*\mathcal{L} \otimes (n+1)^*\mathcal{L}^\vee \otimes 0^*\mathcal{L}^\vee \otimes (n-1)^*\mathcal{L}^\vee \otimes n^*\mathcal{L} \otimes \mathcal{L} \otimes (-1)^*\mathcal{L} \cong \mathcal{O}_A$$

is trivial.

Hence

$$(n+1)^*\mathcal{L} \cong n^*\mathcal{L}^2 \otimes (n-1)^*\mathcal{L}^\vee \otimes \mathcal{L} \otimes (-1)^*\mathcal{L} \qquad (*)$$

Guess $n^*\mathcal{L} \cong \mathcal{L}^{a_n} \otimes (-1)^*\mathcal{L}^{b_n}$. Then $a_0 = b_0 = b_1 = 0$, $a_1 = 1$, and plugging in the guess to (*) justisfies the guess and gives $a_{n+1} = 2a_n - a_{n-1} + 1$ and $b_{n+1} = 2b_n - b_{n-1} + 1$.

Solving the recurrence relations with initial conditions, we get

$$a_n = \binom{n+1}{2}, b_n = \binom{n}{2}$$

□

Corollary 1.15. *If $\mathcal{L}$ is **symmetric**, i.e. $(-1)^*\mathcal{L} \cong \mathcal{L}$, then $n_A^*\mathcal{L} = \mathcal{L}^{n^2}$.*

*If $\mathcal{L}$ is **anti-symmetric**, i.e. $(-1)^*\mathcal{L} \cong \mathcal{L}^\vee$, then $n_A^*\mathcal{L} = \mathcal{L}^n$*

Theorem 1.16 (Theorem of the Square)**.** *Let $\mathcal{L} \in \mathrm{Pic}(A), a, b \in A$, where A is an abelian variety. Then $t_{a+b}^*\mathcal{L} \otimes \mathcal{L} \cong t_a^*\mathcal{L} \otimes t_b^*\mathcal{L}$*

Proof. For $x \in A$, denote by x the constant map $A \to A$ sending everything to x. Let $f = 1_A, g = a, h = b$ in Theorem 1.12. We get

$$\begin{aligned}\mathcal{O}_A &= t_{a+b}^*\mathcal{L} \otimes t_a^*\mathcal{L}^\vee \otimes t_b^*\mathcal{L}^\vee \otimes (a+b)^*\mathcal{L}^\vee \otimes \mathcal{L} \otimes a^*\mathcal{L} \otimes b^*\mathcal{L} \\ &= t_{a+b}^*\mathcal{L} \otimes t_a^*\mathcal{L}^\vee \otimes t_b^*\mathcal{L}^\vee \otimes \mathcal{L}\end{aligned}$$

because pullback of a line bundle by a constant map is trivial. □

Corollary 1.17. *Given a line bundle $\mathcal{L}$ on an abelian variety A. Then the following map*

$$\lambda_{\mathcal{L}} : A \to \mathrm{Pic}(A), a \mapsto t_a^*\mathcal{L} \otimes \mathcal{L}^\vee$$

is a group homomorphism

Proof. For $a, b \in A$, we have

$$\begin{aligned}\lambda_{\mathcal{L}}(a+b) &= t_{a+b}^*\mathcal{L} \otimes \mathcal{L}^\vee \\ &= t_{a+b}^*\mathcal{L} \otimes \mathcal{L} \otimes \mathcal{L}^{-2} \\ &= t_a^*\mathcal{L} \otimes t_b^*\mathcal{L} \otimes \mathcal{L}^{-2} \text{ by Theorem 1.16} \\ &= \lambda_{\mathcal{L}}(a) \otimes \lambda_{\mathcal{L}}(b)\end{aligned}$$

□

Remark (A glance forward). Under certain condition (namely, $\mathcal{L}$ is ample), $\lambda_{\mathcal{L}}$ gives an isogeny from A to its dual abelian variety $A^\vee$, called the **polarization** determined by $\mathcal{L}$.

1.4 Families of Invertible Sheaves and the Seesaw Principle

Definition 1.18. Given a projective k-varieties V and a k-variety T, a **family of invertible sheaves** on V parametrized by T is an invertible sheaf $\mathcal{L}$ on $V \times T$, modulo the equivalence relation that $\mathcal{L} \sim \mathcal{M}$ if $\mathcal{L}|_t \cong \mathcal{M}|_t \in \mathrm{Pic}(V)$ for all $t \in T$. Here $\mathcal{L}|_t$ denotes the restriction of $\mathcal{L}$ at $V \times t$, or equivalently, the pullback of $\mathcal{L}$ via $V \to V \times T, v \mapsto (v, t)$.

Remark. To see the namesake more intuitively, a family of invertible sheaves on V parametrized by T is just an assignment $T \to \mathrm{Pic}(V)$ to each $t \in T$ an invertible sheaf $\mathcal{L}_t$ on V, that "varies smoothly" in the sense that we can find an invertible sheaf on $V \times T$ such that $\mathcal{L}|_t \cong \mathcal{L}_t$.

Proposition 1.19 (Triviality locus is closed)**.** *Let $\mathcal{L}$ be an invertible sheaf of $V \times T$, where V is projective. Then $\{t \in T : \mathcal{L}|_t \cong \mathcal{O}_V\}$ is closed in T.*

Proof. By [2, 13.3], a line bundle on a projective variety is trivial if and only if both itself and its dual have nonzero global sections. Thus, $\mathcal{L}|_t$ is trivial $\Leftrightarrow \Gamma(V, \mathcal{L}|_t) \neq 0$ and $\Gamma(V, \mathcal{L}|_t^\vee) \neq 0$.

Note that $q : V \times T \to T$ is flat and proper because it is a base change of $V \to \operatorname{Spec} k$. Also, L is flat over $V \times T$ because it is locally free. By [4, 24.2.H], L is flat over T. Now apply the semicontinuity theorem [4, 28.1.1], $h^0(V, \mathcal{L}|_t)$ is upper semicontinuous in $t \in T$. In particular $\{t \in T : h^0(V, \mathcal{L}|_t) > 0\}$ is closed. Similarly $\{t \in T : h^0(V, \mathcal{L}^\vee|_t) > 0\}$ is closed. Take the intersection, and we are done. □

Fix a point $v \in V$. The following theorem says that the invertible sheaf $\mathcal{L}$ on $V \times T$ representing a family of sheaves on V indexed by T is uniquely determined if $L|_{v\times T} \in \mathrm{Pic}(T)$ is known.

Theorem 1.20 (Seesaw Principle)**.** *Let $v \in V$, $\mathcal{L}$ be an invertible sheaf on $V \times T$. If $\mathcal{L}|_t$ is trivial for all $t \in T$ and $\mathcal{L}|_v$ is trivial on T, then L is trivial.*

Proof. [1, I.5.18] □

Thus we have the following equivalent definition of a family of invertible sheaves, and we will use it in the rest of this article. However, we shall always use Definition 1.18 to check if two families of sheaves are equal.

Definition 1.21. Given a projective k-varieties V and fix a closed point $v \in V$. A k-variety T, a **family of invertible sheaves** on V parametrized by T is an invertible sheaf $\mathcal{L}$ on $V \times T$ such that $\mathcal{L}|_{v\times T}$ is trivial.

1.5 Isogenies

For a homomorphism $\alpha : A \to B$ of abelian varieties, the **kernel** of α is defined as $\ker(\alpha) := \alpha^{-1}(0)$, the scheme theoretic fiber over $0 \in B$. As 0 is a closed point of B, $\ker(\alpha)$ is a closed subscheme of A. (Base change preserves closed embeddings.)

Definition 1.22. A homomorphism of abelian varieties $\alpha : A \to B$ is called an **isogeny** if (a) $\dim A = \dim B$, (b) $\dim \ker(\alpha) = 0$ and (c) α is surjective.

Observe that it is enough to check two conditions out of three: the image $\alpha(A)$ is an irreducible closed subvariety of B (because A is projective), thus an abelian subvariety of B. The fibers of the surjection $A \to \alpha(A)$ over closed points are translates of $\ker(\alpha)$, so they are isomorphic. Recall from [2, 10.9(b)] that for b in an open dense subset of $\alpha(A)$, $\dim \alpha^{-1}(b) = \dim A - \dim \alpha(A)$. Hence

$$\dim A = \dim \ker(\alpha) + \dim \alpha(A)$$

and the observation follows. (Note that since B is irreducible, $\dim \alpha(A) = \dim B$ implies $\alpha(A) = B$.)

For a zero-dimensional finite-type k-scheme X, we can write $X = \operatorname{Spec} R$ where R is an Artin algebra over k. Define the **degree** of X to be the dimension of R as a k-vector space. When X is reduced, the degree of X is the same as its cardinality. Define the **degree** of an isogeny α to be the degree of $\ker(\alpha)$.

Proposition 1.23. *Let $\alpha : A \to B$ be an isogeny, then*

(a) *α finite and flat.*

(b) *$\deg(\alpha) = [k(A) : \alpha^* k(B)]$, and $\alpha_* \mathcal{O}_A$ is locally free of rank $\deg(\alpha)$.*

Proof. Recall that a morphism from a proper k-scheme to a separated k-scheme is proper [4, 10.3.4(e)]. Thus α is proper. Moreover, all fibers have the same size as $\ker(\alpha)$, which is finite. So α is quasi-finite. By [4, 29.6.2], α is finite.

In particular α is affine, so to show it is flat, it suffices to show that $\alpha_* \mathcal{O}_A$ is flat over $\mathcal{O}_B$. Let $n = \deg(\alpha)$. Choose an open affine $U = \operatorname{Spec} R$ in B, and $\alpha^{-1}(U) = \operatorname{Spec} S$. We know S is a finitely generated R-module, and for all maximal ideals p of R, the fiber $S \otimes_R R/p$ has dimension n over k. This says $\alpha_* \mathcal{O}_A$ has constant rank n on closed points. By [2, 13.1], $\alpha_* \mathcal{O}_A$ is locally free of rank n. In particular, it is flat.

Finally, we may choose U such that $\alpha_*\mathcal{O}_A(U)$ is free. Then S is a free R-module of rank n. As $R \subseteq S$ is an integral extension of domains, every nonzero element in S divides some nonzero element in R. Thus

$$k(A) = \mathrm{Frac}(S) = S \otimes_R \mathrm{Frac}(R) \cong R^n \otimes_R \mathrm{Frac}(R) = \mathrm{Frac}(R)^n = k(B)^n$$

as $k(B)$-vector spaces. Hence $[k(A) : \alpha^* k(B)] = n$. □

Proposition 1.24. *The followings are equivalent for an isogeny $\alpha : A \to B$:*

(a) *α is étale, i.e. flat and unramified* (see [4, 21.6, 25]).

(b) *α is separable, i.e. the field extension $\alpha^* : k(B) \to k(A)$ is separable.*

(c) $\#\ker(\alpha) = \deg(\alpha)$.

Proof. (a) ⇔ (b): (b) means α is unramified at the generic point of B([4, 21.6.D(a)]), so (a) implies (b). Conversely, since the unramification locus is open [4, 21.6.H], and any open subset containing the generic point is open dense, α is unramified on an open dense subset of B. Due to homogeneity, if one closed point is unramified, so is every closed point. Hence α is unramified.

(b) ⇔ (c): Recall the formula that the cardinality of fiber (over a point in an open dense subset of B) is the separable degree of the field extension $\alpha^* : k(B) \to k(A)$. As every fiber is isomorphic, $\#\ker(\alpha) = [k(A) : \alpha^* k(B)]_{\mathrm{sep}}$. Hence (c) ⇔ $[k(A) : \alpha^* k(B)]_{\mathrm{sep}} = [k(A) : \alpha^* k(B)]$ ⇔ $k(A)$ is separable over $\alpha^* k(B)$. □

In particular, when $\mathrm{char}\, k = 0$, the condition (b) of the proposition always holds. More generally, in characteristic $p > 0$, the inseparable degree of a finite field extension is always a power of p, so if $\deg(\alpha)$ is not divisible by p, the only possible inseparable degree of α is 1, in which case α is separable and étale.

Next, we will analyze the degree of isogenies $n_A : A \to A, a \mapsto na$, as a tool to study the n-torsion subgroup of A. The main ingredient here is intersection theory, a tool that can be used to study the degrees of finite maps between projective varieties. We will list the results we are going to use without proof.

Proposition 1.25. *Given a smooth projective variety V of dimension n. There is a symmetric n-multilinear product $\mathrm{Pic}(V) \times ... \times \mathrm{Pic}(V) \to \mathbb{Z}, (D_1, ..., D_n) \mapsto (D_1 \cdot D_2 \cdot ... \cdot D_n)$, called the* ***intersection product****, satisfying the followings:*

(a) *If $\alpha : V \to W$ is a finite map between smooth projective varieties of dimension n, and $D_1, ..., D_n$ are divisors in W, then*

$$(\alpha^* D_1 \cdot ... \cdot \alpha^* D_n) = \deg(\alpha)(D_1 \cdot ... \cdot D_n)$$

(the degree of a nonsurjective finite map is said to be zero.)

(b) *If D is a (very) ample divisor on V, a smooth projective variety of dimension n, then*

$$(D^n) := (D \cdot ... \cdot D) > 0$$

Proof. [2, Chapter 12] □

Lemma 1.26. *Any abelian variety A has a symmetric very ample line bundle (terminology see Corollary 1.15).*

Proof. Since A is projective, there exists a very ample line bundle $\mathcal{L} \in \mathrm{Pic}(A)$. As $(-1)_A$ is an automorphism of A, $(-1)^*\mathcal{L}$ is very ample as well. Recall that the product of very ample line bundles are still very ample, so $\mathcal{L} \otimes (-1)^*\mathcal{L}$ is as required. □

Theorem 1.27. *Let A be an abelian variety of dimension g, and $n \neq 0$. Then $n_A : A \to A$ is an isogeny of degree n^{2g}. In particular, the set of closed points $A(k)$ is a divisible abelian group, and when n is not divided by* $\mathrm{char}\, k$*, n_A is étale, so the n-torsion subgroup $A_n(k) := \ker(n_A)$ has order n^{2g}.*

Proof. Choose a symmetric very ample line bundle $\mathcal{L} = \mathcal{O}(D)$ corresponding to a very ample divisor D. Let Z be the component of $\ker(n_A)$ passing through 0, then $(n_A)^*\mathcal{L}|_Z = (0 : Z \to A)^*\mathcal{L}$ is trivial. On the other hand, $(n_A)^*\mathcal{L}|_Z = \mathcal{L}^{n^2}|_Z$ by symmetry of $\mathcal{L}$, so $(n_A)^*\mathcal{L}|_Z$ is ample when $n \neq 0$. Hence the structure sheaf $\mathcal{O}_Z$ on Z is ample. In fact it is very ample, because any power of $\mathcal{O}_Z$ is itself. Since Z is connected, the global sections of O_Z are constants, so the closed embedding induced from $\mathcal{O}_Z$ is $Z \to \mathbb{P}^0 = \mathrm{Spec}\, k$. Hence Z is a single point (possibly nonreduced). Thus $\dim \ker(n_A) = 0$, so n_A is an isogeny.

To compute the degree of n_A, use the formula Proposition 1.25(a):

$$((n_A^* D)^g) = \deg(n_A)(D^g)$$

Since D is very ample, $(D^g) \neq 0$ by Proposition 1.25(b), we have

$$\deg(n_A) = \frac{((n_A^* D)^g}{(D^g)} = \frac{(n^2 D)^g}{(D^g)} = n^{2g}$$

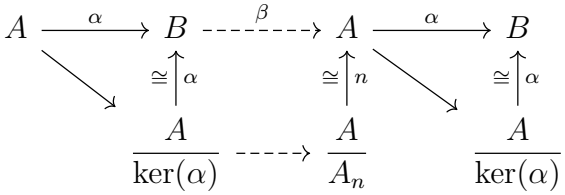
by multilinearity of intersection product.

The étale assertion follows from the discussion after Proposition 1.24. □

Definition 1.28. Two abelian varieties A and B are said to be **isogenous** if there exists an isogeny $\alpha : A \to B$, and we write $A \sim B$.

Proposition 1.29. *Given an isogeny $\alpha : A \to B$ of degree n. Then there is an isogeny $\beta : B \to A$ such that $\alpha \circ \beta = n_B$, $\beta \circ \alpha = n_A$. In particular, isogeneity is an equivalence relation.*

Proof. Let $A_n = \ker(n_A)$, then n_A induces an isomorphism $A/A_n \cong A$, where A/A_n is the quotient of A by the finite group scheme A_n. Similarly $A/\ker(\alpha) \cong B$. Since $n = \deg(\alpha)$ equals to $\#\ker(\alpha)$ times the inseparable degree of α,$\#\ker(\alpha)$ divides n. So n kills $\ker(\alpha)$, and by the universal property of quotient schemes, there is a unique β that fits the following diagram:



All the unlabeled arrows above are quotient maps. Tracing the arrows in the bottom layer, we can see that $\beta \circ \alpha$ and $\alpha \circ \beta$ are both the multiplication map by n. □

1.6 Dual Abelian Varieties: Properties

For an elliptic curve (E, O), we have a one-to-one correspondence $E \xrightarrow{\cong} \mathrm{Pic}^0(E), P \mapsto [P] - [O]$, the divisor class of $[P] - [O]$. Thus we can see that E itself is the moduli space of the set of degree 0 divisor classes. In higher dimension, we will define the dual abelian variety, which is the moduli space of degree 0 divisor classes (a concept to be generalized below), but it is in general not isomorphic to the original abelian variety.

Example 1.30. Let (E, O) be an elliptic curve, and fix a divisor $D = \sum_{i=1}^{r} n_i[P_i]$ in E. It can be shown by the theorem of the square that for any $a \in E$, the translation $D + a := \sum n_i[P_i + a]$. Recall that two divisors of the same degree are linearly equivalent iff the sum of their points (under the group law) are equal. Thus $D + a \sim D$ iff $\sum n_i P_i = \sum n_i(P_i + a) \in E$, so D is translation invariant iff $(\sum n_i)a = O$ for all $a \in E$ iff $\sum n_i = 0$ (since E is never a torsion group). In other words,

$$D \text{ is translation invariant iff } \deg(D) = 0.$$

This motivates the following generalization to abelian varieties:

Definition 1.31. A line bundle $\mathcal{L}$ over an abelian variety A is said to have **degree 0** if $t_a^*\mathcal{L} \cong \mathcal{L}$ for all $a \in A$. Denote by $\mathrm{Pic}^0(A) \subseteq \mathrm{Pic}(A)$ the group of degree 0 line bundles.

Let $\mathcal{L}$ be an arbitrary line bundle on an abelian variety A. Recall the polarization map $\lambda_{\mathcal{L}} : A \to \mathrm{Pic}(A), a \mapsto t_a^*\mathcal{L} \otimes \mathcal{L}^\vee$. Then $\mathcal{L} \in \mathrm{Pic}^0(A)$ iff $\lambda_{\mathcal{L}} = 0$.

Notice that $\lambda_{\mathcal{L}}(a)$ always has degree 0 even when $\mathcal{L}$ does not: given $b \in A$, we have

$$t_b^*\lambda_{\mathcal{L}}(a) \otimes (\lambda_{\mathcal{L}}(a))^\vee = t_b^* t_a^* \mathcal{L} \otimes t_b^* \mathcal{L}^\vee \otimes t_a^* \mathcal{L}^\vee \otimes \mathcal{L}$$

is trivial by the theorem of the square Theorem 1.16. Thus the polarization map can now be better viewed as

$$\lambda_{\mathcal{L}} : A \to \mathrm{Pic}^0(A)$$

The assignment $a \mapsto \lambda_{\mathcal{L}}(a)$ can be realized as an invertible sheaf over A parametrized by A, in the following way. Consider the **Mumford bundle** $\Lambda(\mathcal{L}) = m^*\mathcal{L} \otimes p^*\mathcal{L}^\vee \otimes q^*\mathcal{L}^\vee$ on $A \times A$ (as in Notation 1.10). An easy computation shows

$$\Lambda(\mathcal{L})|_a := \Lambda(\mathcal{L})|_{A \times a} = \lambda_{\mathcal{L}}(a)$$

$$\Lambda(\mathcal{L})|_{0 \times A} = \mathcal{O}_A$$

Notation 1.32. $K(\mathcal{L}) := \ker \lambda_{\mathcal{L}}$

Then $K(\mathcal{L})$ is the triviality locus of $\mathcal{L}'$, which is closed in A by Proposition 1.19.

By the seesaw principle Theorem 1.20, $\mathcal{L} \in \mathrm{Pic}^0(A)$ iff $\lambda_{\mathcal{L}} = 0$ iff $K(\mathcal{L}) = A$ iff $\mathcal{L}'$ is trivial.

As a corollary, degree 0 line bundles are antisymmetric: consider the map $A \to A \times A, a \mapsto (a, -a)$, and pull back the trivial line bundle $\mathcal{L}'$ to A via this map. This yields that $\mathcal{L} \otimes (-1)^*\mathcal{L}$ is trivial.

Proposition 1.33. *If $\mathcal{L}$ is an ample line bundle on A, then $K(\mathcal{L})$ has dimension zero.*

Proof. Let B be the connected component of $K(\mathcal{L})$ passing through 0. Then B is an abelian variety. Let $\mathcal{L}_B$ be the restriction of $\mathcal{L}$ on B. Then $\mathcal{L}_B$ is ample on B by [4, 16.6.G]. Moreover $\mathcal{L}$ is invariant under translation by $b \in B$, and so is $\mathcal{L}_B$. Thus $\mathcal{L}_B \in \mathrm{Pic}^0(B)$, and we see that it is antisymmetric. Consider $\mathcal{L}_B \otimes (-1)_B^*\mathcal{L}_B$. It is trivial and ample on B, and as in the proof of Theorem 1.27, B is a single point. Therefore, $\dim K(\mathcal{L}) = 0$. □

Remark. In fact the converse is true, provided that $\mathcal{L}$ is effective (having a nonzero section).

Now we are ready to define the dual abelian variety $A^\vee$ of A. It should parametrize the group $\mathrm{Pic}^0(A)$.

We use the idea of representable functor. By Yoneda's lemma, an object X in some category C is determined (up to a unique isomorphism) by $h_X := \mathrm{Hom}(-, X)$ as a contravariant functor from C to the category of sets. Hence it suffices to describe what morphisms $T \to A^\vee$ should look like, for any k-variety T. Fortunately we already know what a nice map $T \to \mathrm{Pic}^0(A)$ is: a family of degree 0 invertible sheaves on A indexed by T. By the seesaw principle, such a family is in one-to-one correspondence to an element of P_A^0 as in the following definition:

Definition 1.34. Given an abelian variety A. Define the functor $P_A^0 : k\text{-Var}^{op} \to \mathrm{Set}$ by

$$P_A^0(T) = \{\mathcal{L} \in \mathrm{Pic}(A \times T) : \mathcal{L}_t \in \mathrm{Pic}^0(A), \mathcal{L}|_{0\times T} \cong \mathcal{O}_T\}$$

on objects and induces the following for a morphism $T' \xrightarrow{\alpha} T$:

$$P_A^0(T') \to P_A^0(T), \mathcal{L} \mapsto (1 \times \alpha)^*\mathcal{L}$$

Theorem 1.35 (Existence of Dual Abelian Variety)**.** *The functor P_A^0 is representable by an abelian variety $A^\vee$ (called the **dual abelian variety**) isogenous to A. (In particular $\dim A^\vee = \dim A$.) Moreover the set of k-points $A^\vee(k)$ is isomorphic to $\mathrm{Pic}^0(A)$.*

Before giving the construction, let us explore some properties assuming its existence.

If it is representable by some variety $A^\vee$, then taking $T = \mathrm{Spec}\, k$, we see that the set of k-points $A^\vee(k) = P_A^0(k) = \mathrm{Pic}^0(A)$, as expected. The elememt in $P_A^0(A^\vee)$ corresponding to the identity on $A^\vee$ is an invertible sheaf $\mathcal{P} \in \mathrm{Pic}(A \times A^\vee)$ (called the **Poincaré sheaf**) such that $\mathcal{P}|_{A\times b} = b \in \mathrm{Pic}^0(A)$ for $b \in A^\vee$ and $\mathcal{P}|_{0\times A^\vee}$ is trivial. Given a k-variety T and a family of sheaves $\mathcal{L} \in P_A^0(T)$, we have a morphism $\alpha : T \to A^\vee$ corresponding to $\mathcal{L}$. Look at $P_A^0(A^\vee) \to P_A^0(T)$ induced by α. It sends the sheaf corresponding to $1_{A^\vee}$ to the sheaf corresponding to α, i.e. $(1 \times \alpha)^*\mathcal{P} = \mathcal{L}$. In fact this forces α to be the map $T \to A^\vee : t \mapsto \mathcal{L}_t$, because $\mathcal{L}|_t = (1 \times \alpha)^*\mathcal{P}|_t = \mathcal{P}_{\alpha(t)} = \alpha(t)$.

Proposition 1.36. *The dual abelian variety $A^\vee$ and the Poincaré sheaf $\mathcal{P}$ satisfies the following universal property: for any pair $(T, \mathcal{L})$ consisting of a variety T and a family of sheaves $\mathcal{L} \in P_A^0(T)$, there is a unique map $\alpha : T \to A^\vee$ such that $(1 \times \alpha)^*\mathcal{P} \cong \mathcal{L}$. We also call the pair $(A^\vee, \mathcal{P})$ the dual of A.*

In fact, by a Yoneda like argument, this universal property serves as an equivalent definition of the dual abelian variety.

Now, note that $\mathcal{P}|_{A\times b} = b \in \mathrm{Pic}^0(A)$ for $b \in A^\vee$, so $\mathcal{P}|_{A\times 0}$ is trivial. By definition we also have $\mathcal{P}|_{0\times A^\vee}$ is trivial. So $\mathcal{P}$ is a **divisorial correspondence** between abelian varieties A and $A^\vee$, which means an invertible sheaf whose restrictions to "coordinate axes" $A \times 0$ and $0 \times A^\vee$ are both trivial. Moreover, $\mathcal{P}|_{A\times b} = b$ is trivial only when $b = 0$. In fact this property characterizes the dual abelian variety and the Poincaré sheaf.

Theorem 1.37. *Assume the existence theorem of dual abelian varieties. Let $\mathcal{L}$ be a divisorial correspondence between A and B. Then the followings are equivalent:*

(a) *$(B, \mathcal{L})$ is the dual of A.*

(b) *$\mathcal{L}|_{A\times b}$ is trivial only when $b = 0$.*

(c) $\mathcal{L}|_{a\times B}$ *is trivial only when* $a = 0$.

(d) $(A, \mathcal{L})$ *is the dual of* B.

Proof. [5, p.81] □

Corollary 1.38. $(A^\vee)^\vee \cong A$ *canonically.*

1.7 Dual Abelian Varieties: Construction

Let $\operatorname{char} k = 0$. Fix an ample line bundle $L \in \operatorname{Pic}(A)$.

Proposition 1.39. *The polarization map* $\lambda_{\mathcal{L}} : A \to \operatorname{Pic}^0(A)$ *is onto when* $\mathcal{L}$ *is ample.*

Proof. [5, p.77] □

Thus, as an abstract group, $\operatorname{Pic}^0(A) \cong A/K(\mathcal{L})$. This results in the following construction of the dual:

$$\lambda_{\mathcal{L}} : A \to A^\vee := A/K(\mathcal{L}), \text{ as a quotient by a finite group.}$$

Recall the Mumford bundle $\Lambda(\mathcal{L}) = m^*\mathcal{L} \otimes p^*\mathcal{L}^\vee \otimes q^*\mathcal{L}^\vee$ on $A \times A$ as in the discussion before Notation 1.32. Note that $\Lambda(\mathcal{L})|_{A\times a} = \lambda_{\mathcal{L}}(a)$ is unchanged when a is translated by an element of $K(\mathcal{L})$. We want to view $\Lambda(\mathcal{L})$ as a sheaf on $A \times (A/K(\mathcal{L}))$.

Proposition 1.40. *Let* G *be a finite group acting freely on a quasi-projective variety* X*, and write* $\pi : X \to W = X/G$ *as the quotient map. If an invertible sheaf* $\mathcal{L}$ *admits a* G*-action* ϑ*, namely, a family of isomorphisms* $\mathcal{L} \xrightarrow{\vartheta_g} g^*\mathcal{L}$ *for all* $g \in G$ *satisfying the associativity*

$$\begin{array}{ccccc} & & g^*\mathcal{L} & & \\ & \overset{\vartheta_g}{\nearrow} & & \overset{g^*\vartheta_h}{\searrow} & \\ \mathcal{L} & & \xrightarrow[\vartheta_{hg}]{} & & (hg)^*\mathcal{L}, \end{array}$$

then there is a unique invertible sheaf $\mathcal{M}$ *on* W *such that* $\mathcal{L} = \pi^*\mathcal{M}$*. In fact* $\mathcal{M} \mapsto \pi^*\mathcal{M}$ *gives a one-to-one correspondence between isomorphism classes of invertible sheaves on* W *and the isomorphism classes of pairs* $(\mathcal{L}, \vartheta)$*, an invertible sheaf together with a* G*-action, on* X*.*

Proof. This statement is a special case of [5, p.70], except that an G-action on $\mathcal{L}$ is defined in the following sense:

Definition 1.41. Let G be a finite group acting on a variety X. Let $q : G\times X \to X, (g, x) \mapsto x$ and $\alpha : G \times X \to X, (g, x) \mapsto g(x)$. Let $\mathcal{L}$ be a line bundle on X. A G-**action** on L is an isomorphism $\vartheta : q^*\mathcal{L} \to \alpha^*\mathcal{L}$ as sheaves on $G \times X$, such that the associativity diagram commutes:

$$\begin{array}{ccccc} & & ((h,g,x) \mapsto g(x))^*\mathcal{L} & & \\ & \overset{((h,g,x)\mapsto(g,x))^*\vartheta}{\nearrow} & & \overset{(id\times\alpha)^*\vartheta}{\searrow} & \\ ((h,g,x) \mapsto x)^*\mathcal{L} & & \xrightarrow[(\mu\times id)^*\vartheta]{} & & ((h,g,x) \mapsto h(g(x)))^*\mathcal{L} \end{array}$$

as sheaves on $G \times G \times X$. Here $\mu : G \times G \to G$ denotes the multiplication morphism.

Now since G is finite, we can write $G \times X$ as the disjoint union $\bigsqcup_{g \in G} X_g$, where $X_g \cong X$ is the g-th copy of X. For any $g \in G$, the restriction of $\alpha^*\mathcal{L}$ on X_g is $g^*\mathcal{L}$, and the restriction of $q^*\mathcal{L}$ on X_g is $\mathcal{L}$. To define an isomorphism $\vartheta : q^*\mathcal{L} \to \alpha^*\mathcal{L}$, it suffices to define it piece by piece, $\vartheta_g : g^*\mathcal{L} \to \mathcal{L}$. So the data of a G-action on $\mathcal{L}$ is precisely a family of isomorphisms

$$\vartheta_g : g^*\mathcal{L} \to \mathcal{L}$$

satisfying the associativity. □

Let $K(\mathcal{L})$ act on the second factor of $A \times A$ (i.e. a acts as $1 \times t_a$), then $A \times (A/K(\mathcal{L})) = (A \times A)/K(\mathcal{L})$. Claim $\mathcal{L}'$ is $K(\mathcal{L})$-invariant. For $a \in K(\mathcal{L}), b \in A$, we have

$$(1 \times t_a)^*\mathcal{L}'|_{A \times b} = \mathcal{L}'|_{A \times (a+b)} = \lambda_{\mathcal{L}}(a+b) = \lambda_{\mathcal{L}}(b) = \mathcal{L}'|_{A \times b}$$

$$(1 \times t_a)^*\mathcal{L}'|_{0 \times A} = t_a^*(\mathcal{L}'|_{0 \times A}) \cong \mathcal{O}_A$$

By the seesaw principle Theorem 1.20, we get $(1 \times t_a)^*\mathcal{L}' \cong \mathcal{L}'$.

By Proposition 1.40, there is an invertible sheaf $\mathcal{P}$ on $(A \times A)/K(\mathcal{L}) = A \times A^\vee$ such that $\mathcal{L}' = (1 \times \lambda_{\mathcal{L}})^*\mathcal{P}$. Moreover $\mathcal{P}|_{A \times \lambda_{\mathcal{L}}(a)} = \mathcal{L}'|_{A \times a} = \lambda_{\mathcal{L}}(a)$, so

$$\mathcal{P}|_{A \times b} = b$$

because $\lambda_{\mathcal{L}}$ is onto.

Theorem 1.42 (Existence of Dual Abelian Variety in Characteristic 0)**.** *If* $\operatorname{char} k = 0$*, then* $(A^\vee, \mathcal{P})$ *satisfies the universal property in Proposition* 1.36*.*

Sketch of Proof. It suffices to check $P_A^0(T) = \operatorname{Hom}(T, A^\vee)$. Given a regular map $f : T \to A^\vee$, the family of sheaves associated to f is simply $(1 \times f)^*\mathcal{P}$. Conversely, claim that any map $T \to A^\vee$ coming from a family of sheaves is regular.

For simplicity, we only do the case where T is an irreducible normal k-variety. Let $\mathcal{M}$ be a family of degree 0 sheaves on A indexed by T. Consider $f : T \to A^\vee, t \mapsto \mathcal{M}_t$. We should use an analogue of closed graph theorem to show that f is regular.

Let $\Gamma = \{(t, b) \in T \times A^\vee : \mathcal{M}_t = b\}$ be the graph of f. Claim that it is closed in $T \times A^\vee$. Look at the family of invertible sheaves $\mathcal{F}$ on A indexed by $T \times A^\vee$, such that $\mathcal{F}|_{(t,b)} = \mathcal{M}_t \otimes \mathcal{P}_b^\vee = \mathcal{M}_t \otimes b^\vee$ for $(t, b) \in T \times A^\vee$. (It is indeed a family because $t \mapsto \mathcal{M}_t$ and $b \mapsto \mathcal{P}_b$ both are.) Then Γ is the trivial locus of $\mathcal{F}$, which is closed.

Equip Γ with the induced reduced closed subscheme structure, then Γ is a subvariety of $T \times A^\vee$. The projection $p : \Gamma \hookrightarrow T \times A^\vee \to T$ is a proper morphism (as $A^\vee = A/K(\mathcal{L})$ is projective and closed embeddings are proper). Moreover p is bijective on sets, so in particular, it is quasi-finite. Thus p is a finite map. As p has fiber size 1, and $\operatorname{char} k = 0$ (so p is separable), we have $\deg(q) = 1$, so p induces isomorphism on function fields. In other words, p is birational.

Lemma 1.43. *A birational finite map* $p : X \to Y$ *to a normal variety* Y *is an isomorphism.*

Proof. Without loss of generality, assume $Y = \operatorname{Spec} R$ is affine. Then $X = \operatorname{Spec} S$ with $R \subseteq S \subseteq \operatorname{Frac}(S) = \operatorname{Frac}(R)$ by birationality, and S is module finite (thus integral) over R. But since X is normal, R is integrally closed in K, so $S = R$. □

Now f, being the composition $T \cong \Gamma \hookrightarrow T \times A^\vee \twoheadrightarrow A^\vee$, is regular. □

Remark. When $\operatorname{char} k = p > 0$, the construction is the same in outline, but it is technically much more subtle. The dual $A^\vee$ is still the quotient $A/K(\mathcal{L})$, but we need to equip $K(\mathcal{L})$ with a possibly nonreduced group scheme structure.

In this construction, we have seen that $\lambda_\mathcal{L} : A \to A^\vee$ is an isogeny, which proves the remaining part of Theorem 1.35. An isogeny $A \to A^\vee$ arising this way from an ample line bundle $\mathcal{L}$ is called a **polarization** of A. A polarization of degree 1 is called a **principal polarization**. Thus a principally polarized abelian variety is isomorphic to its dual.

Call a line bundle **nondegenerate** if $\lambda_\mathcal{L}$ is an isogeny. We have seen that a line bundle on an abelian variety is ample if it is nondegenerate and effective (i.e. having a nonzero section). We have the following properties of $\lambda_\mathcal{L}$ for nondegenerate $\mathcal{L}$.

Theorem 1.44. *Let $\mathcal{L}$ be an ample line bundle on an abelian variety A. Recall the Euler characteristic $\chi(\mathcal{L}) := \sum(-1)^i h^i(A, \mathcal{L})$. Then*

(a) $\deg(\lambda_\mathcal{L}) = \chi(\mathcal{L})^2$.

(b) (Riemann Roch) *If $\mathcal{L} = \mathcal{O}(D)$, then $\chi(\mathcal{L}) = (D^g)/g!$.*

(c) *$h^r(A, \mathcal{L})$ is nonzero for exactly one integer $i(\mathcal{L})$, called the **index** of $\mathcal{L}$.*

(d) *If $\alpha : A \to B$ is an isogeny, and $\mathcal{L} \in \operatorname{Pic}(B)$ is nondegenerate, then so is $\alpha^*\mathcal{L}$ and $i(\alpha^*\mathcal{L}) = i(\mathcal{L})$.*

(e) *If $\mathcal{L}, \mathcal{L}' \in \operatorname{Pic}(A)$ are algebraically equivalent (or said equivalently, $\mathcal{L} - \mathcal{L}' \in \operatorname{Pic}^0(A)$), then $i(L) = i(L')$.*

(f) *$i(n\mathcal{L}) = i(\mathcal{L})$ for $n > 0$ and $i(-\mathcal{L}) = g - i(\mathcal{L})$.*

(g) *$i(\mathcal{L}) = 0$ (equivalently, $\mathcal{L}$ is effective) if $\mathcal{L}$ is ample.*

Part of proof. For (a)(b)(c), see [5, p.150]. For (d)(e), see the course note in MATH 731, Fall 2017.

Applying (d) to $[n] : A \to A$, and noting that $[n]^*$ acts as multiplication by n^2 on $\operatorname{NS}(A)$, we get $i(n^2\mathcal{L}) = i(\mathcal{L})$. Using Zarhin's trick (any positive integer is the sum of four squares), we can show that $i(n\mathcal{L}) = i(\mathcal{L})$ for all positive n. The second part $i(-\mathcal{L}) = g - i(\mathcal{L})$ of (f) is just Serre duality, noting that the dualizing sheaf of any group variety is trivial (since the cotangent sheaf is free).

Finally, for (g), note that a very ample line bundle is effective, so $i(\mathcal{L}) = 0$ for very ample $\mathcal{L}$. Choosing a large enough n, we get $i(\mathcal{L}) = i(n\mathcal{L}) = 0$ for ample $\mathcal{L}$. □

In particular, the degree of a polarization is always a square, and for an ample line bundle $\mathcal{L} = \mathcal{O}(D)$, we have $\chi(\mathcal{L}) = h^0(A, \mathcal{L}) > 0$ and $(D^g) = g!h^0(A, \mathcal{L})$. Moreover, adding the part (g) to the discussion before the theorem, we get

Corollary 1.45. *A line bundle on an abelian variety is ample if and only if it is effective and nondegenerate.*

1.8 Dual Homomorphisms and Dual Isogenies

Definition 1.46. Given a homomorphism $\alpha : A \to B$ of abelian varieties, define the **dual homomorphism** $\alpha^\vee : B^\vee \to A^\vee$, where $\mathcal{L} \mapsto \alpha^*\mathcal{L}$ for a degree 0 invertible sheaf $\mathcal{L}$ on B. This map is regular - it comes from the family of sheaves $(\alpha \times 1)^*\mathcal{P}_B$, where $\mathcal{P}_B$ is the Poincaré sheaf on B.

When $\alpha : A \to B$ is an isogeny, it turns out that the dual homomorphism $\alpha^\vee : B^\vee \to A^\vee$ is an isogeny of the same degree as α, called the **dual isogeny**. We state the theorem in characteristic 0.

Theorem 1.47. *If $\alpha : A \to B$ is an isogeny with kernel N, then $\alpha^\vee : B^\vee \to A^\vee$ is an isogeny with kernel isomorphic to the dual group $N^\vee := \mathrm{Hom}(N, k^*) = \{\text{characters of } N\}$, where k^* is the multiplicative group of k.*

Remark. Since N is finite, any group homomorphism $N \to k^*$ must have image in the torsion subgroup of k^*, i.e. roots of unity. Since $\operatorname{char} k = 0$ and k is algebraically closed, the theory of characters in k has no difference from that in $\mathbb{C}$. From there we have the results that $N \cong N^\vee$ noncanonically. In particular $\deg(\alpha) = \#N = \#N^\vee = \deg(\alpha^\vee)$.

Proof. Write $B = A/N$. By Proposition 1.40, an element of $\ker(\alpha^\vee)$, which is an invertible sheaf on B that pulls back to the trivial invertible sheaf on A corresponds to an N-action ϑ on $\mathcal{O}_A$. For $a \in N$, consider

$$\vartheta_a \in \mathrm{Hom}(\mathcal{O}_A, t_a^* \mathcal{O}_A) = \mathrm{Hom}(\mathcal{O}_A, \mathcal{O}_A)$$

Since A is an irreducible projective variety, ϑ_a is the multiplication map by some scalar $\chi(a)$ in k. Since ϑ_a is an isomorphism, $\chi(a) \in k^*$. It can be read from the associativity diagram that $\chi(a)\chi(b) = \chi(a+b)$, meaning χ is a group homomorphism. Conversely, any group homomorphism $A \to k^*$ gives an N-action on $\mathcal{O}_A$ this way. We thus get a bijection $\ker(\alpha^\vee) \cong N^\vee$. It can be shown to be a group isomomorphism.

In particular, $\ker(\alpha)$ is finite, so $\alpha^\vee$ is an isogeny. □

Remark. When $\operatorname{char} k = p > 0$, N may not be reduced, and the scheme-theoretical kernel of $\alpha^\vee$ is the Cartier dual $N^\vee$ of N. It is still a finite group scheme, and $(N^\vee)^\vee = N$.

2 Tate Modules and application to Endomorphisms

2.1 Rational Endomorphisms

Definition 2.1. An **abelian subvariety** B of an abelian variety A is a connected closed subgroup B of A, which is clearly an abelian variety in its own right. A nonzero abelian variety A is said to be **simple** if it has no nonzero proper abelian subvariety.

Proposition 2.2. *For any abelian variety A, there exists simple abelian subvarieties $A_1, ..., A_n \subseteq A$ such that $A_1 \times ... \times A_n \to A, (a_1, ..., a_n) \mapsto \sum a_i$ is an isogeny.*

In particular, $A = A_1 + ... + A_n$ and $\dim A = \sum \dim A_i$.

Proof. If A is simple, we are done. Otherwise, let $0 \subsetneq B \subsetneq A$ be a abelian subvariety. Claim that there exists an complement abelian subvariety $B' \subseteq A$, such that $\alpha : B \times B' \to A, (b, b') \mapsto b + b'$ is an isogeny.

Let $i : B \hookrightarrow A$ denote the inclusion map. Choose a polarization $\lambda_{\mathcal{L}}$ given by ample $\mathcal{L}$ on A, and define B' as the zero component of the kernel

$$i^\vee \circ \lambda_{\mathcal{L}} : A \to A^\vee B^\vee$$

Here the **zero component** of a topological group means its connected component passing through the identity element. We have

$$\dim B' \geq \dim A - \dim B^\vee = \dim A - \dim B$$

Look at the restriction of $i^\vee \circ \lambda_{\mathcal{L}}$ to B. For $b \in B$, we have

$$i^\vee(\lambda_L(b)) = i^*(t_b^*\mathcal{L} \otimes \mathcal{L}^\vee) = t_b^* i^* \mathcal{L} \otimes i^* \mathcal{L}^\vee = \lambda_{i^*\mathcal{L}}(b)$$

Hence $i^\vee \circ \lambda_{\mathcal{L}}|_B = \lambda_{\mathcal{L}|_B}$, so that

$$B \cap B' = \ker(i^\vee \circ \lambda_{\mathcal{L}} \circ i) = \ker(\lambda_{\mathcal{L}|_B})$$

is finite because $\mathcal{L}|_B$ is ample (by Proposition 1.33).

Since the kernel of $\alpha : B \times B' \to A$ consists of $(b, -b)$ with $b \in B \cap B'$, we see that $\ker(\alpha)$ is finite. But $\dim B + \dim B' \geq A$, so α is an isogeny.

Repeating the decomposition process to B, B', we are done by induction on dimensions.

□

In the language of representation theory, this says that every abelian variety is completely reducible, up to isogeny.

Definition 2.3. The category of **abelian varieties up to isogeny**, denoted Isab, has objects abelian varieties and the morphism set between abelian varieties A and B defined by

$$\mathrm{Hom}^0(A, B) := \mathrm{Hom}(A, B) \otimes_{\mathbb{Z}} \mathbb{Q}$$

The composition map

$$\mathrm{Hom}^0(A, B) \times \mathrm{Hom}^0(B, C) \to \mathrm{Hom}^0(A, C)$$

comes from the usual composition map, extended by linearity. To be more specific, since $\mathbb{Q}$ is a localization of $\mathbb{Z}$, and tensor product is preserved by localizations, we have

$$\mathrm{Hom}(A,B)\otimes_{\mathbb{Z}}\mathrm{Hom}(B,C)\otimes_{\mathbb{Z}}\mathbb{Q}=\mathrm{Hom}^0(A,B)\otimes_{\mathbb{Q}}\mathrm{Hom}^0(B,C),$$

so the $\mathbb{Z}$-module homomorphism given by composition

$$\mathrm{Hom}(A,B)\otimes_{\mathbb{Z}}\mathrm{Hom}(B,C)\to\mathrm{Hom}(A,C)$$

gives rise to a morphism of $\mathbb{Q}$-vector spaces

$$\mathrm{Hom}^0(A,B)\otimes_{\mathbb{Q}}\mathrm{Hom}^0(B,C)\to\mathrm{Hom}^0(A,C)$$

Now given an isogeny $\alpha: A\to B$ of degree n, by Proposition 1.29, there is an isogeny $\beta: B\to A$ such that $\alpha\circ\beta=n$, $\beta\circ\alpha=n$. Then $\beta/n\in\mathrm{Hom}^0(B,A)$ is a two-sided inverse of α in the category Isab, so α is an isomorphism in Isab.

As a result, $\mathrm{Hom}^0(A,B)$ only depends on the isogeny classes of A and B.

Note that any element of $\mathrm{Hom}^0(A,B)$ can be written as α/n for some $\alpha\in\mathrm{Hom}(A,B)$ and $n\in\mathbb{Z}-0$: first write it as a finite sum of such, and then take the common denominator.

It is not hard to show that every morphism in $\mathrm{Hom}(A,B)$ that is an isomorphism in Isab must be an isogeny, but we will not use this fact.

The main goal of this section is the following.

Theorem 2.4. *Given abelian varieties A and B, the homomorphism group $\mathrm{Hom}(A,B)$ is a free abelian group of finite rank. Moreover, its rank is at most $4\dim A\dim B$.*

Hence $\mathrm{Hom}(A,B)\subseteq\mathrm{Hom}^0(A,B)$ and $\mathrm{Hom}^0(A,B)$ is a finite dimensional $\mathbb{Q}$-vector space with dimension at most $4\dim A\dim B$.

The idea is to first work on the category Isab to study $\mathrm{Hom}^0(A,B)$. The advantage of this category is the decomposition theorem into simple abelian varieties, which makes the statements about $\mathrm{Hom}^0(A,B)$ can be reduced to the statements about simple abelian varieties. At the same time, we study the Tate module of a general abelian variety, which will be a free $\mathbb{Z}_l$-module of finite rank, and then we establish a number of injectivity results. Finally we bound the dimension of $\mathrm{Hom}^0(A,B)$ using Tate modules, and show that $\mathrm{Hom}(A,B)$ is a topologically discrete lattice in $\mathrm{Hom}^0(A,B)$, which gives the bound of rank of $\mathrm{Hom}(A,B)$.

Lemma 2.5 (Schur's Lemma for Abelian Varieties)**.** *Let $\alpha: A\to B$ be a homomorphism of simple abelian varieties. Then A is either zero or an isogeny.*

Proof. Suppose A is not zero. Then its image is a nonzero abelian subvariety of B, and it must be the whole B since B is simple. Thus α is onto.

Also, the zero component of $\ker(\alpha)$ is a proper abelian subvariety of A, which must be 0 because A is simple. Hence $\ker(\alpha)$ is finite.

Therefore, α is an isogeny. □

Notation 2.6. $\mathrm{End}(A):=\mathrm{Hom}(A,A)$, the **endomorphism ring** of A.

$\mathrm{End}^0(A):=\mathrm{Hom}^0(A,A)$, the **endomorphism algebra** or **rational endomorphism ring** of A.

Corollary 2.7. *If A, B are simple abelian varieties, then*

$$\mathrm{Hom}^0(A,B) = \begin{cases} 0, & A \not\sim B \\ \mathrm{End}^0(A), & A \sim B \end{cases}$$

where $A \sim B$ means A is isogenous to B.

Corollary 2.8. *Let $A \sim A_1^{n_1} \times ... \times A_r^{n_r}$, and $B \sim A_1^{m_1} \times ... \times A_r^{m_r}$, where $A_1, ..., A_r$ are mutually nonisogenous simple abelian varieties and $n_i, m_i \geq 0$, then*

$$\mathrm{Hom}^0(A,B) \cong \prod_{i=1}^{r} M_{m_i \times n_i}(\mathrm{End}^0(A_i))$$

In particular, $\mathrm{End}^0(A) \cong \prod_{i=1}^r M_{n_i}(\mathrm{End}^0(A_i))$.

If A is simple, then any nonzero element of $\mathrm{End}^0(A)$ can be written as α/n, where $\alpha \in \mathrm{End}(A) - 0$ and $n \in \mathbb{Z} - 0$. Since any nonzero endomorphism of A must be isogeny, α/n is invertible. Thus $\mathrm{End}^0(A)$ is a division algebra over $\mathbb{Q}$.

By the decomposition formula of $\mathrm{End}^0(A)$ above, we see that an abelian variety A is simple if and only if $\mathrm{End}^0(A)$ is a division algebra.

2.2 Tate Modules

Throughout this section, we fix a prime ℓ not equal to $\mathrm{char}\, k$.

Consider an abelian variety A of dimension g. From Theorem 1.27, the ℓ^n-torsion subgroup $A_{\ell^n}(k)$ has order $(\ell^n)^{2g}$. For a fixed n, let $G = A_{\ell^n}(k)$, then for any $r > 0$, its ℓ^r-torsion subgroup is $A_{\ell^r}(k)$, which has order ℓ^{2gr}. By the structure theorem of finite abelian groups, the only possible group structure of G satisfying these is $(\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$. Thus $A_{\ell^n}(k) \cong (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$. From now on, we omit (k) from the notations $A(k), A_n(k)$, etc., when it is clear from the context that it refers the abelian group structure.

Notation 2.9. For an abelian group Q, we denote by Q_n the n-torsion subgroup of G. For a prime ℓ, define the **Tate module** of Q to be the inverse limit of the inverse system

$$Q_{\ell^n} \xrightarrow{\ell} Q_{\ell^{n-1}}$$

and denote it by $T_\ell Q$. Here the map ℓ is the multiplication by ℓ.

Also define the ℓ-**primary (torsion) subgroup** of Q as the union of all Q_{ℓ^n} where n ranges over all positive integers, and denote it by $Q(\ell)$. Note that $Q(\ell)$ is always an ℓ-**primary (abelian) group**, meaning an abelian group whose all elements are killed by some power of ℓ. Observe that $T_\ell Q = T_\ell(Q(\ell))$.

We have two observations:

(1) Any ℓ-primary group has a natural $\mathbb{Z}_\ell$-module structure: given $x \in \mathbb{Z}_\ell$, choose a sequence $x_i \in \mathbb{Z}$ that converges ℓ-adically to x. Then for an element q in an ℓ-primary group Q, we define

$$x \cdot q = \lim_{i \to \infty} x_i q$$

Note that because q is killed by a high power of ℓ, $x_i q$ always stablizes, and the limit is independent of the choice of x_i. So there is no analytic convergence issue, but you may think of this limit as the usual limit where Q has the discrete topology.

Since $\mathbb{Z}$ is dense in $\mathbb{Z}_\ell$, every $\mathbb{Z}$-linear map between ℓ-primary groups is $\mathbb{Z}_\ell$-linear. To be specific, if $\alpha : A \to B$ be a homomorphism of ℓ-primary groups, $a \in A$ and $x \in \mathbb{Z}_\ell$, then choosing x_i as above, we get

$$\alpha(x \cdot a) = \alpha(\lim x_i a) = \lim \alpha(x_i a) = \lim x_i \alpha(a) = x \cdot \alpha(a)$$

Hence the category of ℓ-primary groups is a full subcategory of the category of $\mathbb{Z}_\ell$-modules.

(2) The Tate module of any abelian group A has a natural $\mathbb{Z}_\ell$ module structure. We shall consider $A(\ell)$ instead, which is a $\mathbb{Z}_\ell$-module by previous observation. The inverse system defining $T_\ell A$ is a system of $\mathbb{Z}_\ell$-modules, so the inverse limit $T_\ell A$ is a $\mathbb{Z}_\ell$-module. Recall that $T_\ell A = \{(a_1, a_2, ...) : \ell a_1 = 0, \ell a_2 = a_1, ...\}$, then its $\mathbb{Z}_\ell$-module structure can be written as

$$x \cdot (a_i) = (x \cdot a_i) \quad \text{where } (a_1, a_2, ...) \in T_\ell A, x \in \mathbb{Z}_\ell$$

A homomorphism of abelian groups induces a $\mathbb{Z}_\ell$-homomorphism of their Tate modules. Given $\alpha : A \to B$, we have the following diagram of inverse systems of ℓ-primary groups (in particular, a diagram of $\mathbb{Z}_\ell$-modules):

$$\begin{array}{ccccccc} \cdots & \longrightarrow & A_{\ell^n} & \xrightarrow{\ell} & A_{\ell^{n-1}} & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha} & & \\ \cdots & \longrightarrow & B_{\ell^n} & \xrightarrow{\ell} & B_{\ell^{n-1}} & \longrightarrow & \cdots \end{array}$$

(by noting that if a is killed by ℓ^n, then so is $\alpha(a)$), so it induces a $\mathbb{Z}_\ell$-homomorphism on their inverse limits $T_\ell \alpha : T_\ell A \to T_\ell B$.

Hence the Tate module construction is a functor from the category abelian groups to the category $\mathbb{Z}_\ell$ modules. Moreover if we look at the functor T_ℓ : ℓ-primary groups $\to \mathbb{Z}_\ell$-modules, it clearly preserves scalar multiplications in $\mathbb{Z}_\ell$. (If $x : A \to A$ be a scalar multiplication by $x \in \mathbb{Z}_\ell$, then every vertical map in the diagram above is multiplication by x, so the induced map on inverse limit $T_\ell A$ is multiplication by x as well.)

Proposition 2.10. *Let A be an abelian variety over k of dimension g and ℓ be a prime different from* $\operatorname{char} k$. *The Tate module $T_\ell A$ of A is isomorphic to $\mathbb{Z}_\ell^{2g}$, where $\mathbb{Z}_\ell$ is the ring of ℓ-adic integers. The ℓ-primary subgroup of A is isomorphic to $(\ell^{-\infty}\mathbb{Z}/\mathbb{Z})^{2g} \cong (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}$, where $\ell^{-\infty}\mathbb{Z}$ is the localization of $\mathbb{Z}$ at ℓ.*

Proof. Exercise. Key steps: using $A_{\ell^n}(k) \cong (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$, we can prove that $A(\ell) \cong (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}$. Then use $T_\ell \dfrac{\mathbb{Q}_\ell}{\mathbb{Z}_\ell} \cong \mathbb{Z}_\ell$. For details see [1, I.10.3-5]. □

2.3 Injectivity Statements for Tate Modules

Proposition 2.11. *For abelian varieties A, B over k, and $\ell \neq \operatorname{char} k$, we have an injection of abelian groups*

$$\operatorname{Hom}(A, B) \overset{T_\ell}{\hookrightarrow} \operatorname{Hom}_{\mathbb{Z}_\ell}(T_\ell A, T_\ell B) \cong {\mathbb{Z}_\ell}^{4 \dim A \dim B}$$

Notice that $\operatorname{Hom}_{\mathbb{Z}_\ell}(T_\ell A, T_\ell B) \cong \operatorname{Hom}_{\mathbb{Z}_\ell}({\mathbb{Z}_\ell}^{2 \dim A}, {\mathbb{Z}_\ell}^{2 \dim B}) \cong {\mathbb{Z}_\ell}^{4 \dim A \dim B}$.

Proof. Let $\alpha : A \to B$ such that $T_\ell \alpha = 0$. Then for any $(a_i) \in T_\ell A$, $\alpha(a_i) = 0$ for all i. Note that in the inverse system defining $T_\ell A$, each map $\ell : A_{\ell^{i+1}} \to A_{\ell^i}$ is onto because multiplication by ℓ is an isogeny on A. Thus for any $a \in A_{\ell^n}$, we can construct $(a_i) \in T_\ell A$ such that $a_n = a$. It follows that $\alpha(a) = 0$ for any $a \in A(\ell)$, the ℓ-primary torsion subgroup of A.

Claim $\alpha = 0$. As A is generated by simple abelian subvarieties as a group (by Proposition 2.2), we may assume A is simple without loss of generality. Now $\ker(\alpha)$ contains $A(\ell) \cong (\ell^{-\infty}\mathbb{Z}/\mathbb{Z})^{2\dim A}$, which is infinite. So the zero component of $\ker(\alpha)$ is a nonzero abelian subvariety of A, which must be A itself because A is simple. Hence $\alpha = 0$. □

In particular $\mathrm{Hom}(A, B)$ is torsion free, thus $\mathrm{Tor}_i^{\mathbb{Z}}(\mathrm{Hom}(A, B), \mathbb{Z}/n\mathbb{Z}) = 0$ for all $n > 0, i > 0$. (Use the resolution $0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \to 0$ to compute the Tor.) Thus $\mathrm{Hom}(A, B)$ is flat over $\mathbb{Z}$ by [4, 24.4.1]. Apply $(-) \otimes_{\mathbb{Z}} \mathrm{Hom}(A, B)$ to the inclusion map $\mathbb{Z} \hookrightarrow \mathbb{Q}$, we get an injection

$$\mathrm{Hom}(A, B) \hookrightarrow \mathrm{Hom}^0(A, B)$$

We next prove a much stronger injectivity:

Theorem 2.12. *For abelian varieties A, B over k, and $\ell \neq \mathrm{char}\, k$, the following morphism of $\mathbb{Z}_\ell$-modules arisen from T_ℓ (by tensor-hom duality) is injective.*

$$\mathrm{Hom}(A, B) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \hookrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell A, T_\ell B)$$

Lemma 2.13. *Let $\alpha \in \mathrm{Hom}(A, B)$. Suppose $T_\ell \alpha$ is divisible by $\ell^n \in \mathbb{Z}_\ell$ in $\mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell A, T_\ell B)$, then α is divisible by $\ell^n \in \mathbb{Z}$ in $\mathrm{Hom}(A, B)$.*

Proof. For $a \in A_{\ell^n}$, choose $(a_i) \in T_\ell A$ such that $a_n = a$ as in the proof of last proposition. Write $T_\ell \alpha = \ell^n \beta$ and $\beta((a_i)) = (b_i)$, then $T_\ell \alpha((a_i)) = (\ell^n b_i) = (0, ..., 0, \ell^n b_{n+1}, \ell^n b_{n+2}, ...)$ because the $b_i \in B_{\ell^i}$. Comparing the n-th slot, we get $\alpha(a) = \alpha(a_n) = 0$.

Thus α is zero on A_{ℓ^n}. By the universal property of quotient varieties, α factors through $\beta : A/A_{\ell^n} \to B$. Since the quotient map $A \to A_{\ell^n}$ can be identified as $\ell^n : A \to A$, we can identity β as a map from A to B such that $\alpha = \beta \circ \ell^n$. □

Proof of Theorem. It suffices to prove that for any finitely generated subgroup $M \subseteq \mathrm{Hom}(A, B)$, the restricted map $M \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell A, T_\ell B)$ is injective. Since $\mathrm{Hom}(A, B)$ is torsion free, so is M, so M is free of finite rank m. Let $e_1, ..., e_m$ be a basis for M, and suppose $\sum a_i T_\ell(e_i) = 0$ with $a_i \in \mathbb{Z}_\ell$. Claim that $a_i = 0$ for all i.

For each i, choose a sequence of integers a_{ij} that converge ℓ-adically to a_i. Since $\sum a_{ij} e_i - \sum a_i e_i$ goes to zero when j goes to infinity, it is divided by arbitrarily high powers of ℓ when j is large. Hence $T_\ell(\sum a_{ij} e_i) = T_\ell(\sum a_{ij} e_i - \sum a_i e_i)$ is divided by high powers of ℓ when j is large. By the lemma above, $\sum a_{ij} e_i$ is divided by high powers of ℓ when j is large. As e_i's are linear independent, the same is true for its coordinates a_{ij}. Thus $a_i = \lim a_{ij} = 0$. □

Corollary 2.14. *For abelian varieties A and B, $\mathrm{Hom}^0(A, B)$ is a finite dimensional $\mathbb{Q}$-vector space. Moreover, its dimension is at most $4 \dim A \dim B$.*

Proof. Note that $\mathbb{Q}_\ell = \mathrm{Frac}(\mathbb{Z}_\ell)$ is a localization of $\mathbb{Z}_\ell$, in particular flat over $\mathbb{Z}_\ell$. Thus we have injection

$$\mathrm{Hom}^0(A, B) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \hookrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell A, T_\ell B) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong \mathbb{Q}_\ell^{4 \dim A \dim B}$$

Hence $\dim_{\mathbb{Q}} \mathrm{Hom}^0(A, B) = \dim_{\mathbb{Q}_\ell} \mathrm{Hom}^0(A, B) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \leq 4 \dim A \dim B$. □

Note that this is not enough to show that $\mathrm{Hom}(A, B)$ is finitely generated. It is possible to have an infinitely generated torsion free abelian group such that, after applying $(-) \otimes_{\mathbb{Z}} \mathbb{Q}$, it becomes a finite dimensional $\mathbb{Q}$-vector space: $\mathbb{Q}$ is such an example, as $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$. (Localizations are epimorphisms of rings.)

2.4 Charateristic Polynomials as Degrees

Throughout this section, let A be an abelian variety over k of dimension g and ℓ be a prime not equal to $\operatorname{char} k$.

Notation 2.15. For an abelian variety A, define $V_\ell A := T_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. For a morphism α between abelian varieties, define $V_\ell \alpha = T_\ell \alpha \otimes id : V_\ell A \to V_\ell B$. Then V_ℓ is a functor from the category of abelian varieties to the category of (finite dimensional) $\mathbb{Q}_\ell$-vector spaces.

Fix an endomorphism $\alpha \in \operatorname{End}(A)$, where A is an abelian variety of dimension g. Look at the two following functions in $n \in \mathbb{Z}$:

(1) $\deg(\alpha - n) = \deg(n - \alpha)$.

(By convention, a homomorphism between abelian varieties of the same dimension that is *not* an isogeny is said to have degree zero.)

(2) the characteristic polynomial of $V_\ell \alpha \in \operatorname{End}(V_\ell A)$, i.e.

$$P_\alpha(n) := \det(V_\ell \alpha - n) = \det(n - V_\ell \alpha)$$

(note that $V_\ell A$ is even dimensional).

The former obviously takes nonnegative integers as values, but there is no reason to believe it is a polynomial. The latter is obviously a polynomial of degree $2g$, but the coefficients are in $\mathbb{Z}_\ell$, and they may not even lie inside $\mathbb{Q}$. Moreover, it may depend on ℓ. However, amazingly, they are equal, which shows that they are a polynomial of degree $2g$ with coefficients in $\mathbb{Q}$ which takes nonnegative integers as values when evaluating at an integer. This is the goal of this section.

Theorem 2.16. *Let A be an abelian variety of dimension g, and $\alpha, \beta \in \operatorname{End}(A)$, then $\deg(n\alpha + \beta)$ is a rational polynomial in n of degree at most $2g$. Moreover, the **characteristic polynomial** of β defined by $P_\beta(n) := \deg(\beta - n)$ is monic of degree exactly $2g$.*

Proof. Let D be a very ample divisor on A, define $D_n = (n\alpha + \beta)^* D$, then Proposition 1.25 gives

$$\deg(n\alpha + \beta) = \frac{(D_n^g)}{(D^g)}$$

We shall get a recursive formula for D_n. Consider the three maps $n\alpha + \beta, \alpha, \alpha : A \to A$, by Theorem 1.12,

$$D_{n+2} - 2D_{n+1} - (2\alpha)^* D + D_n + 2(\alpha^* D) \sim 0$$

Hence $D_{n+2} - 2D_{n+1} + D_n \sim D' := (2\alpha)^* D - 2(\alpha^* D)$.

Solving this recurrence relation with initial values D_0, D_1, we get

$$D_n \sim \binom{n}{2} D' + nD_1 - (n-1)D_0$$

Taking g-th intersection power, and expand by multilinearity, we get (D_n^g) is a polynomial in n of degree at most $2g$ with coefficients in $\mathbb{Q}$.

Now, as a special case, take $\alpha = 1$, and choose D to be very ample and symmetric (which exists by Lemma 1.26). By Corollary 1.15

$$D' = (2_A)^* D - 2D \sim 4D - 2D = 2D$$

Thus $(D_n)^g = (n(n-1)D + nD_1 - (n-1)D_0)^g$ has leading term $(D^g)n^{2g}$. We get

$$P_\beta(-n) = \deg(\beta + n) = \frac{(D_n)^g}{(D^g)}$$

has leading term n^{2g}. Hence $P_\beta(n)$ has leading term $(-1)^{2g} n^{2g} = n^{2g}$. □

Observe that for an endomorphism α, $\deg(n\alpha) = \deg(n)\deg(\alpha) = n^{2g}\deg(\alpha)$ (even when $n = 0$). We can extend the notion of degree to the ring $\mathrm{End}^0(A)$ of rational endomorphisms by defining

$$\deg(\alpha/n) := \deg(\alpha)/n^{2g}$$

This is well defined by the observation. In fact, by the purely algebraic argument below, one can show that deg is a homogeneous polynomial function of degree $2g$ on $\mathrm{End}^0(A)$.

Definition 2.17. Let M be a module over an infinite integral domain R with fraction field K. A function $f : M \to K$ is called a **polynomial function** if for any $v_1, ..., v_n \in M$, the function $p(x_1, ..., x_n) := f(x_1v_1 + ... + x_nv_n)$ is a polynomial function in $x_1, ..., x_n$ with coefficients in K.

Lemma 2.18. *Let M, R, K be as above, and let $f : M \to K$ be a function such that, for all $v, w \in M$, $x \mapsto f(xv + w) : R \to K$ is a polynomial in x with coefficient in K. Then f is a polynomial function.*

Proof. For the sake of induction, we prove a slightly stronger result: for every $v_1, ..., v_n, w \in M$, $f(x_1v_1 + ... + x_nv_n + w)$ is a polynomial in x_i's. The case $n = 1$ is the hypothesis. For $n > 1$, apply the hypothesis to $x_n(v_n) + (x_1v_1 + ... + x_{n-1}v_{n-1} + w)$ with $x = x_n$,$v = v_n$ and $x_1, ..., x_{n-1}$ fixed, we see that

$$f(x_1v_1 + ... + x_nv_n + w) = a_0(x_1, ..., x_{n-1}) + ... + a_d(x_1, ..., x_{n-1})x_n^d$$

for some d and some functions $a_i : R^{n-1} \to K$. Choose distinct $c_0, ..., c_d$ in R, which is always possible as R is infinite. We obtain the linear system over K

$$f(x_1v_1 + ... + x_{n-1}v_{n-1} + c_jv_n + w) = a_0(x_1, ..., x_{n-1}) + ... + a_d(x_1, ..., x_{n-1})c_n^d$$

solving for $a_i(x_1, ..., x_{n-1})$. The coefficient matrix is the Vandermonde matrix, which is invertible. Hence $a_i(x_1, ..., x_{n-1})$ can be expressed as a linear combination of $f(x_1v_1 + ... + x_{n-1}v_{n-1} + c_jv_n + w)$ $(j = 0, 1, ..., d)$, which are polynomials in $x_1, ..., x_{n-1}$ by induction hypothesis. □

Thus, $\deg : \mathrm{End}(A) \to \mathbb{Q}$ is a polynomial function. In particular, for $\alpha, \beta \in \mathrm{End}(A)$, the function $f_{\alpha,\beta}(m, n) := \deg(m\alpha + n\beta)$ is a polynomial in m, n. Moreover, it is homogeneous of degree $2g$. We are now ready to extend Theorem 2.16 to the rational endomorphism ring.

Theorem 2.19. $\deg : \mathrm{End}^0(A) \to \mathbb{Q}$ *is a polynomial function on the $\mathbb{Q}$-vector space* $\mathrm{End}^0(A)$.

Proof. First, if $\alpha, \beta \in \mathrm{End}(A)$, claim that

$$f_{\alpha,\beta}(r, s) = \deg(r\alpha + s\beta)$$

still holds even when $r, s \in \mathbb{Q}$. Choose a common denominator b such that $r = m/b, s = n/b, m, n \in \mathbb{Z}$. Then

$$\deg(r\alpha + s\beta) = b^{-2g}\deg(m\alpha + n\beta) = b^{-2g}f_{\alpha,\beta}(m, n) = f_{\alpha,\beta}(r, s)$$

because $f_{\alpha,\beta}$ is homogeneous of degree $2g$. (Note that being homogeneous is a property of the polynomial itself, with no reference to the ground ring; though, we arrived at this statement from the values of $f_{\alpha,\beta}$ at integers.)

Now for an arbitrary pair of rational endorphisms, say $\alpha/b, \beta/b \in \mathrm{End}^0(A)$, and $r \in \mathbb{Q}$, we have

$$\deg(r\alpha/b + \beta/b) = f_{\alpha,\beta}(r/b, 1/b),$$

which is a polynomial in r. □

In particular, if we endow the finite dimension $\mathbb{Q}$-vector space $\mathrm{End}^0(A)$ with the classical topology (i.e. the subspace topology inherited from $\mathrm{End}^0(A) \otimes_{\mathbb{Q}} \mathbb{R}$), then deg is a continuous map.

Theorem 2.20. *If A is a simple abelian variety, then $\mathrm{End}(A)$ is a topologically discrete lattice in $\mathrm{End}^0(A)$. In particular (see [6, I.4.2], for example), $\mathrm{End}(A)$ is free of rank at most $4g^2$.*

Proof. It suffices to show that $\{0\}$ is open in $\mathrm{End}(A)$, if $\mathrm{End}(A)$ is given the subspace topology inherited from $\mathrm{End}^0(A)$. But since A is simple, any nonzero endomorphism in A is an isogeny, so its degree is a positive integer. Thus $\mathrm{End}(A) \cap \{v \in \mathrm{End}^0(A) : \deg(v) < 1\} = \{0\}$. As deg is continuous, we are done. □

Corollary 2.21. *For any abelian varieties A, B, the homomorphism group $\mathrm{Hom}(A, B)$ is free of rank at most $4 \dim A \dim B$.*

Proof. The question is unaffected by isogeny. If A is isogenous to A', choose an isogeny $A' \to A$, then we have an exact sequence

$$0 \to \mathrm{Hom}(A, B) \to \mathrm{Hom}(A', B)$$

Since $\mathbb{Z}$ is Noethrian, finite generation of $\mathrm{Hom}(A', B)$ implies that of $\mathrm{Hom}(A, B)$. On the other hand, if B is isogenous to B', choose an isogeny $\beta : B \to B'$. Claim that $\mathrm{Hom}(A, B) \to \mathrm{Hom}(A, B')$ is injective. Suppose $\alpha : A \to B$ satisfies $\beta \circ \alpha = 0$, then $\alpha(A) \subseteq \ker(\beta)$, which is finite as β is an isogeny. Thus $\alpha(A) = 0$.

Therefore, we can assume $A = A_1^{n_1} \times ... \times A_r^{n_r}$, and $B = A_1^{m_1} \times ... \times A_r^{m_r}$, where $A_1, ..., A_r$ are mutually nonisogenous simple abelian varieties and $n_i, m_i \geq 0$. We get

$$\mathrm{Hom}(A, B) \cong \prod_{i=1}^{r} M_{m_i \times n_i}(\mathrm{End}(A_i))$$

is finitely generated by the theorem above.

In particular, as $\mathrm{Hom}(A, B)$ is torsion free, it is free. Thus

$$\mathrm{rk}_{\mathbb{Z}}\mathrm{Hom}(A, B) = \dim_{\mathbb{Q}} \mathrm{Hom}^0(A, B) \leq 4 \dim A \dim B$$

□

As an interesting application, this proves the Néron-Severi theorem for abelian varieties. For a projective smooth variety V such that $\mathrm{Pic}^0(V)$ makes sense (for example, when V is a curve or an abelian variety), define the **Néron-Severi group** as $\mathrm{NS}(V) := \mathrm{Pic}(V)/\mathrm{Pic}^0(V)$. We can ask the question whether $\mathrm{NS}(V)$ is finitely generated over $\mathbb{Z}$. Note that for a curve C, the degree map $\mathrm{NS}(C) \to \mathbb{Z}$ gives an isomorphism. Néron-Severi theorem says that the answer is affirmative in general.

Corollary 2.22. *Let A be an abelian variety of dimension g. Then $\mathrm{NS}(A)$ is free of rank at most $4g^2$.*

Proof. The map $\mathcal{L} \to \lambda_{\mathcal{L}} : \mathrm{Pic}(A) \to \mathrm{Hom}(A, A^\vee)$ has kernel being the set of translation invariant line bundles, which is precisely $\mathrm{Pic}^0(A)$ by definition. Thus $\mathrm{NS}(A) \hookrightarrow \mathrm{Hom}(A, A^\vee)$, and the rest follows from Corollary 2.21. □

Remark. (a) For a smooth projective variety V, we can define $\mathrm{Pic}^0(V)$ as the group of line bundles that are **algebraically equivalent** to the trivial line bundle (see [4, 24.7.5]). This agrees with our definition when V is a curve or an abelian variety. By [4, 20.1.4], the intersection product can be defined on the Néron-Severi group.

(b) Let A be an abelian variety. From the proof of the theorem above, the polarization map $\lambda_H : A \to A^\vee$ only depends on the class of H in $\mathrm{NS}(A)$. Since H is ample iff λ_H is an isogeny, ampleness is well defined for a class in $\mathrm{NS}(A)$.

(c) It is a fact that any line bundle $\mathcal{L}$ on an abelian variety can be decomposed as the product of a symmetric line bundle $\mathcal{M}$ and a degree zero line bundle [Reference needed]. Note that if $\mathcal{L}$ is ample, M is ample as well. As a result, n^* acts as n^2 on the Néron-Severi group.

2.5 Characteristic Polynomials as Determinants

Again fix an abelian variety A over k of dimension g and a prime $\ell \neq \mathrm{char}\, k$. Recall the second definition of characteristic polynomial for an endomorphism $\alpha \in \mathrm{End}(A)$:

$$P_\alpha(X) = \det(V_\ell\alpha - X|_{V_\ell}A)$$

with notations in Notation 2.15.

We shall show that

$$\deg(\alpha - X) = \det(V_\ell\alpha - X)$$

Our ultimate goal is to prove

Theorem 2.23. *For $\alpha \in \mathrm{End}^0(A)$, we have $\deg(\alpha) = \det(V_\ell\alpha)$.*

The key observation is that they have the same ℓ-adic norm. Recall that the **ℓ-adic norm** of a nonzero integer $n = \ell^s q$ where $\gcd(q, \ell) = 1$ is $|n|_\ell := \ell^{-s}$, and $|0|_\ell := 0$. The ℓ-adic norm extends to $\mathbb{Q}_\ell$ in a natural way, and even to the algebraic closure $\overline{\mathbb{Q}_\ell}$ by [6, II.4.8]. In $\overline{\mathbb{Q}_\ell}$, the ℓ-adic norm is invariant under Galois action.

Proposition 2.24. *For $\alpha \in \mathrm{End}^0(A)$, we have $|\deg(\alpha)|_\ell = |\det(V_\ell\alpha)|_\ell$.*

Proof. Since both quantities are multiplicative in α, we may assume $\alpha \in \mathrm{End}(A)$.

For a finite abelian group Q of order $n = \ell^s q$ where $\gcd(q, \ell) = 1$, its ℓ-primary subgroup $Q(\ell)$ has order ℓ^s from the structure theorem of abelian groups. Thus

$$|\#Q|_\ell = 1/\#Q(\ell)$$

Morover, $\deg(\alpha)$ and $\#\ker(\alpha)$ are equal when $\mathrm{char}\, k = 0$ and they differ by a factor of some power of p, when $\mathrm{char}\, k = p > 0$. Since $\ell \neq p$, they still have the same ℓ-adic norm.

Thus

$$|\deg(\alpha)|_\ell = |\#\ker(\alpha))|_\ell = 1/\#\ker(\alpha)(\ell)$$

The following lemmas will show that

$$1/\#\ker(\alpha)(\ell) = 1/\#\mathrm{coker}(T_\ell\alpha) = |\det(V_\ell\alpha)|_\ell$$

(For the first equality, note that $\ker(\alpha)(\ell) = \ker(\alpha : A(\ell) \to B(\ell))$ and $T_\ell(A(\ell)) = T_\ell A = (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}$.) □

Remark. In order to prove $1/\#\ker(\alpha)(\ell) = |\det(V_\ell\alpha)|_\ell$, Lemma 2.26 is enough and we may skip Lemma 2.25. However [1, I.10.20] uses $\operatorname{coker}(T_\ell\alpha)$ as a bridge to connect the other two quantities, so perhaps he has a quick proof of Lemma 2.26.

Lemma 2.25. *Let M be a free $\mathbb{Z}_\ell$-module of rank n, and F an endomorphism of M with nonzero determinant. Then*

$$\#\operatorname{coker}(F) = |\det(F)|_\ell^{-1}$$

Proof. We first prove the case $n = 1$. Now F is the multiplication by some number $a \in \mathbb{Z}_\ell$. Factorize $a = \ell^s q$, where q is a unit in $\mathbb{Z}_\ell$. Then $q : \mathbb{Z}_\ell \to \mathbb{Z}_\ell$ is an isomorphism, so $\operatorname{coker}(a) \cong \operatorname{coker}(\ell^s)$. Thus both sides of the identity do not change if we replace a by ℓ^s. But in this case, the result follows from

$$\operatorname{coker}(\ell^s) = \mathbb{Z}_\ell/(\ell^s) \cong \mathbb{Z}/(\ell^s)$$

(Recall the general fact that for a ring R and a maximal ideal $\mathfrak{m}$, consider its $\mathfrak{m}$-adic completion $\widehat{R}$, then we have a canonical isomorphism $\widehat{R}/\mathfrak{m}^s\widehat{R} \cong R/\mathfrak{m}^s$ for all $s \geq 0$.)

For general $n \geq 1$, we use the Smith normal form to reduce the question to the case where F is an diagonal matrix. Since $\mathbb{Z}_\ell$ is a PID, there exist $n \times n$ invertible matrices U, V and a diagonal matrix D , all with coefficients in $\mathbb{Z}_\ell$, such that $F = UDV$. Here D is called the **Smith normal form**, as is used in the proof of the structure theorem for finitely generated PID modules. We have $\operatorname{coker}(F) \cong \operatorname{coker}(D)$. Since $\det(U), \det(V)$ are invertible in $\mathbb{Z}_\ell$, they have ℓ-adic norm 1. Thus $|\det(F)|_\ell = |\det(D)|_\ell$. So we may replace F by D, and the result follows from $n = 1$ case. □

Lemma 2.26. *Write $S = \mathbb{Q}_\ell/\mathbb{Z}_\ell$, which is a $\mathbb{Z}_\ell$-module. Let $A = S^n$ and $\alpha : A \to A$ be an endomorphism of abelian groups (which is $\mathbb{Z}_\ell$-linear because A is ℓ-primary). Then α is given by an $n \times n$-matrix with coefficients in $\mathbb{Z}_\ell$, and if the kernel is finite, we have*

$$\#\ker(\alpha) = \#\operatorname{coker}(T_\ell\alpha) = |\det(T_\ell\alpha)|_\ell^{-1}$$

Proof. First we consider the case $n = 1$. Claim that the map $\mathbb{Z}_\ell \to \operatorname{End}_{\mathbb{Z}_\ell}(S)$ sending an element $x \in \mathbb{Z}_\ell$ to the scalar multiplication by x on $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ is an isomorphism.

Note that $T_\ell S = \mathbb{Z}_\ell$. Consider the diagram

$$\begin{array}{ccc} & \operatorname{End}_{\mathbb{Z}_\ell}(S) & \\ \nearrow & & \xrightarrow{T_\ell} \\ \mathbb{Z}_\ell & \xrightarrow[id]{} & \operatorname{End}_{\mathbb{Z}_\ell}(T_\ell S) = \mathbb{Z}_\ell \end{array}$$

Thus T_ℓ is surjective. It suffices to show that it is injective as well. Let $\alpha \in \ker(T_\ell)$. For any $a \in S$, say $\ell^s a = 0$, then there is $(a_i) \in T_\ell S$ such that $a_s = a$ (because S_{ℓ^i} is a surjective system). So $0 = T_\ell\alpha((a_i)) = (\alpha(a_i))$, and in particular, $\alpha(a) = 0$.

Hence $\operatorname{End}(S^n) = M_n(\operatorname{End}(S)) = M_n(\mathbb{Z}_\ell)$.

For the statement about the size of kernel, let α be an endomorphism of A. We have just proved that A can be written as an $n \times n$ matrix in $M_n(\mathbb{Z}_\ell)$, and we may assume it takes the Smith normal form. Thus it suffices to do the case $n = 1$. Any unit in $\mathbb{Z}_\ell$ acts as isomorphism on S (as in any $\mathbb{Z}_\ell$-module), so we may assume $\alpha = \ell^s$. We have $S \cong \dfrac{\ell^{-\infty}\mathbb{Z}}{\mathbb{Z}}$, so

$$\ker(\alpha) = \operatorname{Ann}_S \ell^s = \frac{\ell^{-s}\mathbb{Z}}{\mathbb{Z}}$$

has cardinality ℓ^s.

□

Now fix $\alpha \in \mathrm{End}^0(A)$, consider the monic degree-$2g$ polynomials $P_\alpha(X) = \deg(\alpha - X)$ and $Q_\alpha(X) = \deg(V_\ell\alpha - X)$. We know $P_\alpha(X) = Q_\alpha(X)$ for $X \in \mathbb{Q}$. But how does the norm at each point contain enough information for a polynomial? Take a complex polynomial $f \in \mathbb{C}[x]$ as an example. Then its zeros are precisely the points $z \in \mathbb{C}$ where $|f(z)| = 0$. Moreover, the multiplicity d of a zero $z = a$ is the "vanishing order" of $f(z)$ near $z = a$, namely, $|f(z)| \sim |z - a|^d$ for z near a asymptotically. Hence $|f(z)|$ for all $z \in \mathbb{C}$ determines f up to a constant multiple.

However not all zeroes of P_α lies in $\mathbb{Q}$, or even in $\mathbb{Q}_\ell$. Thus we need to extend the result of Proposition 2.24 to $\overline{\mathbb{Q}_\ell}$, and use the analogue idea of vanishing order.

Let $\delta = \deg : \mathrm{End}^0(A) \to \mathbb{Q}, \delta' = \det(V_\ell(-)) : \mathrm{End}^0(A) \to \mathbb{Q}$. As they are both polynomial functions, they can be extended to polynomial functions $\mathrm{End}^0(A) \otimes_{\mathbb{Q}} \overline{\mathbb{Q}_\ell} \to \overline{\mathbb{Q}_\ell}$. (Just choose a basis and view them as polynomials in several variables.) They are both multiplicative, i.e. $\delta(\alpha\alpha') = \delta(\alpha)\delta(\alpha')$ and similarly for δ'.

We have known that δ and δ' have the same ℓ-adic norm on $\mathrm{End}^0(A)$. Since $\mathbb{Q}$ is dense in $\mathbb{Q}_\ell$, this holds for $\mathrm{End}^0(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. The Galois theory argument in [1, I.10.21-22] shows that $|\delta|_\ell = |\delta'|_\ell$ even on $\mathrm{End}^0(A) \otimes_{\mathbb{Q}} \overline{\mathbb{Q}_\ell}$.

Hence we have

$$|P_\alpha(X)|_\ell = |Q_\alpha(X)|_\ell$$

for all $X \in \overline{\mathbb{Q}_\ell}$.

Proof of Theorem 2.23. Choose $a \in \overline{\mathbb{Q}_\ell}$. Write $P_\alpha(X) = (X - a_1)...(X - a_{2g})$ for $a_i \in \overline{\mathbb{Q}_\ell}$. Let d be the times a occurs in a_i's, in other words, the multiplicity of P_α at a. (d could be zero, in which case a is not a zero of P_α.)

When X tends to a but $X \neq a$, $|X - a_i|_\ell$ will tend to a nonzero constant $|a - a_i|_\ell$ when $a_i \neq a$. Thus $|P_\alpha(X)|_\ell$ equals $|X - a|_\ell^d$ times a nonzero constant when X is near a. We write this as

$$|P_\alpha(X)|_\ell \sim |X - a|_\ell^d$$

Similarly, if e is the multiplicity of Q_α at a, we have

$$|Q_\alpha(X)|_\ell \sim |X - a|_\ell^e$$

Since $|P_\alpha(X)|_\ell = |Q_\alpha(X)|_\ell$, we have $|X - a|_\ell^d \sim |X - a|_\ell^e$, or $|X - a|_\ell^{d-e}$ is a constant for X near a. Thus $d = e$.

Hence $P_\alpha = Q_\alpha$. In particular, taking $X = 0$, we get $\deg(\alpha) = \det(V_{\ell\alpha})$. □

Corollary 2.27. *Let* $\mathrm{char}\, k = 0$. *Then the characteristic polynomial* P_α *of an endomorphism* $\alpha \in \mathrm{End}(A)$ *has integer coefficients.*

Proof. Since P_α is the characteristic polynomial of $T_\ell A$, a matrix in $\mathbb{Z}_\ell$, the coefficients of P_α must lie in $\mathbb{Z}_\ell$. But P_α is a rational polynomial, so it coefficients lie in $\mathbb{Z}_\ell \cap \mathbb{Q} = \mathbb{Z}_{(\ell)}$, the localization of $\mathbb{Z}$ at maximal ideal (ℓ). In other words, multiples of ℓ are not allowed in the denominator.

Now let ℓ range over all primes (as $\mathrm{char}\, k = 0$), then coefficients of P_α allow no denominator, so they must be integers. □

Remark. In fact this corollary is true even in positive characteristic. [Reference needed].

Definition 2.28. Let $\alpha \in \mathrm{End}^0(A)$. The **trace** of α is defined as minus the coefficient of the X^{2g-1} term of the characteristic polynomial $P_\alpha(X)$. Clearly $\mathrm{tr}(\alpha)$ is the trace of the linear map $V_\ell\alpha$, so tr is a linear function from $\mathrm{End}^0(A)$ to $\mathbb{Q}$.

3 Jacobians of Curves

Through this section, a **curve** always mean a smooth projective curve over an algebraically closed field k.

The Jacobian of C is the moduli space of degree zero divisor classes on C. We have seen this idea before - the dual of an abelian variety A is the moduli space of degree zero line bundles on A. The following is a generalization of Definition 1.34.

Definition 3.1. Given a smooth projective variety V such that $\mathrm{Pic}^0(V)$ makes sense. Then the **Picard variety** of V is the variety J representing the functor (if exists):

$$P_V^0(T) = \{\text{families of degree 0 invertible sheaves on } V \text{ parametrized by } T$$

on the category of finite-type separable k-schemes (not necessarily reduced).

If a base point $P \in V$ is picked, it can be equivalently stated as

$$P_V^0(T) = \{\mathcal{L} \in \mathrm{Pic}(V \times T) : \mathcal{L}_t \in \mathrm{Pic}^0(V), \mathcal{L}|_{P\times T} \cong \mathcal{O}_T\}$$

Again if we let $T = \operatorname{Spec} k$, we see that $J(k) = \mathrm{Pic}^0(V)$ on points. I think of J in the following way: for any variety T, a set map $f : T \to J = \mathrm{Pic}^0(V)$ is regular iff it comes from a family of degree 0 line bundles on V indexed by T, i.e. there is $\mathcal{L} \in P_V^0(T)$ such that $\mathcal{L}|_t = f(t)$ for all $t \in T$.

There is a canonical sheaf $\mathcal{P}$ on $V \times J$ corresponding to the identity map on J, also called the **Poincaré sheaf**. The Poincaré sheaf for dual abelian varieties is a special case of this. We have $\mathcal{P}|_{V\times b} = b \in \mathrm{Pic}^0(V) = J$.

When $V = C$ is a smooth projective curve, the Picard variety of C is called the **Jacobian variety** or simply the **Jacobian** of C. Let the genus of C be g. If $g = 0$, then $C \cong \mathbb{P}^1$, and $\mathrm{Pic}^0(C)$ is trivial, so the Jacobian of C is a point. If $g = 1$, then C is an elliptic curve, so J is the dual abelian variety of C, which is isomorphic to itself by the classical isomorphism $C \to \mathrm{Pic}^0(C), P \mapsto [P] - [0]$. So the theory of Jacobian varieties is most interesting when $g \geq 2$, and it is indeed an important tool to deal with high genus curves.

Theorem 3.2. *The Jacobian exists, and it is an abelian variety.*

Remark. When k is not algebraically closed, the Jacobian is still defined, but it may not represent the functor P_C^0. It does when C contains a k-point.

The goal of this section is to explore the properties of Jacobians and the application to Weil conjecture of curves, assuming the existence. Though, I will remark on the construction of Jacobians when there is opportunity.

3.1 The canonical embedding to Jacobian

Let C be a smooth projective curve of genus g and J be the Jacobian of C. Recall that $g = h^1(C, \mathcal{O}_C)$.

Theorem 3.3. *The tangent space $T_0(J)$ of J at 0 is canonically isomorphic to $H^1(C, \mathcal{O}_C)$. In particular,* $\dim J = g$.

Proof. Consider the scheme $T = \operatorname{Spec} k[\epsilon]/(\epsilon^2)$. Write $k[\epsilon]$ for this ring here and hereafter. Suppose V is a variety, then giving a morphism from T to V is the same as giving a k-points P on V and a

tangent vector w in $T_P(V)$. The canonical map $J(k[\epsilon]) \to J(k)$ maps the pair (P, w) to the point P. Hence $T_0(J)$ is the kernel of $J(k[\epsilon]) \to J(k)$.

But J represents the functor P^0_C, so $T_0(J)$ can be identified with the kernel of $P^0_C(T) \to P^0_C(k)$, i.e. all families of degree 0 line bundles on C indexed by T that pull back to the trivial line bundle C. Let $C_\epsilon = C \times T = C \times_k k[\epsilon]$. Note that T has only one point, $P^0_C(T)$ is, by definition, the set of invertible sheaf on C_ϵ whose pullback to C has degree zero. Thus the kernel of $P^0_C(T) \to P^0_C(k)$ is precisely the set of invertible sheaves on C_ϵ that restricts to the trivial invertible sheaf on C. In other words,

$$T_0(J) = \ker(\mathrm{Pic}(C_\epsilon) \to \mathrm{Pic}(C)) = \ker(H^1(C_\epsilon, \mathcal{O}^\times_{C\epsilon}) \to H^1(C, \mathcal{O}^\times_C))$$

Note they are just Čech cohomologies of some sheaves on the same topological space C. We shall show $H^1(C, \mathcal{O}_C) \cong T_0(J)$, so it suffices to have an exact sequence $H^1(C, \mathcal{O}_C) \to H^1(C, \mathcal{O}^\times_{C_\epsilon}) \to H^1(C, \mathcal{O}^\times_C)$, given by the short exact sequence of sheaves

$$0 \to \mathcal{O}_C \xrightarrow{\exp} \mathcal{O}^\times_{C_\epsilon} \to \mathcal{O}^\times_C \to 0$$

constructed as follows;

The construction is local, so for the sake of notational simplicity, we pretend C is affine and view $\mathcal{O}_C$ as a k-algebra.

Consider

$$\mathcal{O}_{C_\epsilon} = \mathcal{O}_C \otimes_k k[\epsilon] = \mathcal{O}_C \oplus \mathcal{O}_C\epsilon$$

If $a + b\epsilon \in \mathcal{O}_C \oplus \mathcal{O}_C\epsilon$ is invertible, say $1 = (a + b\epsilon)(c + d\epsilon) = ac + (ad + bc)\epsilon$.

So a must be invertible and $c = 1/a$. Now for arbitrary $b \in \mathcal{O}_C$, we can choose $d = -b/a^2$ to make $ad + bc = 0$. Hence as sets,

$$\mathcal{O}^\times_{C_\varepsilon} = \mathcal{O}^\times_C \oplus \mathcal{O}_C\varepsilon$$

As a caution, note that it is not a direct sum of abelian groups, because the group law is $(a + b\varepsilon)(c + d\varepsilon) = ac + (ad + bc)\varepsilon$ rather than $ac + (b + d)\varepsilon$. However, defining the exponential map

$$\mathcal{O}_C \to \mathcal{O}^\times_{C_\varepsilon}, a \mapsto 1 + a\varepsilon$$

and let $\mathcal{O}^\times_{C_\varepsilon} = \mathcal{O}^\times_C \oplus \mathcal{O}_C\varepsilon \to \mathcal{O}^\times_C$ be the standard projection, we still get an exact sequence

$$0 \to \mathcal{O}_C \xrightarrow{\exp} \mathcal{O}^\times_{C_\varepsilon} \to \mathcal{O}^\times_C \to 0$$

as sheaves of abelian groups. □

Corollary 3.4. *We have a canonical isomorphism $T_0^\vee(J) \cong \Gamma(C, \Omega^1_C)$.*

Proof. Taking dual for Theorem 3.3, we get $T_0(J)^\vee \cong H_1(C, \mathcal{O}_C)^\vee$, which by Serre duality, is isomorphic to $\Gamma(C, \Omega^1_C)$. □

Remark. It can be checked that the correspondence is as follows: given a covector $w \in T_0^\vee(J)$, extend it uniquely to a translation invariant one-form $\omega \in \Gamma(J, \Omega^1(J))$, and then pull back to C by f^P to be defined next.

From now on, assume $g > 0$, and pick a closed point P in C. Consider the map $f^P : C \to J$ sending $Q \to [Q] - [P]$. Note $f^P(P) = 0$.

This map is regular because I claim that it comes from the sheaf $\mathcal{L}^P = \mathcal{O}(\Delta - C \times P - P \times C)$ on $C \times C$, where Δ denotes the diagonal. Rewrite $\mathcal{L}^P = \mathcal{O}(\Delta) - q^*\mathcal{O}(P) - p^*\mathcal{O}(P)$, where $p, q : C \times C \to C$ are the projections to both factors. Then

$$\Delta|_{C\times Q} = \Delta \cap C \times Q = (Q, Q) = [Q] \text{ as a divisor on } C \cong C \times Q.$$

$$q^*[P]|_{C\times Q} = (q \circ (\cdot, Q))^*[P] = \text{const}_Q^*[P] = 0$$
$$p^*[P]|_{C\times Q} = (p \circ (\cdot, Q))^*[P] = id^*[P] = [P]$$

Hence $\mathcal{L}^P|_{C\times Q} = \mathcal{O}([Q] - [P])$. Clearly $\mathcal{L}^P$ is symmetric, so $\mathcal{L}^P|_{P\times C} = \mathcal{L}^P|_{C\times P} = \mathcal{O}(0)$. Thus $\mathcal{L}^P$ is a family of degree 0 sheaves on C indexed by C, so it induces a morphism $f^P : C \to J$.

Notation 3.5. For a point P in a curve C of genus $g > 0$, the **canonical embedding** is the morphism $f^P : C \to J$ determined by $Q \mapsto [Q] - [P]$ on points. Its corresponding line bundle is $\mathcal{L}^P = \mathcal{O}(\Delta - C \times P - P \times C)$.

The terminology "embedding" is justified by the following theorem.

Theorem 3.6. *$f^P : C \to J$ is a closed embedding.*

Proof. Observe that a divisor $[Q] - [P]$ is never principal unless $Q = P$. Otherwise, let $\text{div}(f) = [Q] - [P]$, then it induces a morphism $f : C \to \mathbb{P}^1 = \mathbb{A}^1 \sqcup \infty$. The pullback of $[0]$ is $[Q]$, which has degree 1, so f is a morphism of degree 1, hence an isomorphism. Thus $C \cong \mathbb{P}^1$, a contradiction to $g > 0$.

We shall prove that f^P is injective on points and on tangent spaces. It is easy on points: suppose $f^P(Q) = f^P(Q')$, then $[Q] - [P] \sim [Q'] - [P']$, so $[Q] - [Q']$ is principal, which implies $Q = Q'$.

It remains to show that $(df^P)_Q : T_Q(C) \to T_{f^PQ}(J)$ is injective. As $f^Q = t_{[P]-[Q]} \circ f^P$, $(df^Q)_Q = (dt_{[P]-[Q]})_{f^P(Q)} \circ (df^P)_Q$. But the translation $(dt_{[P]-[Q]})_{f^P(Q)}$ is an isomorphism, so it suffices to show that $(df^Q)_Q$ is injective. Look at the dual $(df^Q)_Q^\vee : T_0^\vee(J) \to T_Q^\vee(C)$. By Corollary 3.4, it can be identified as

$$\Gamma(C, \Omega^1) \xrightarrow{(-)|_Q} T_Q^\vee(C)$$

The dimensions of the source and the target are g and 1, repectively. It suffices to show the kernel has dimension $g - 1$. Clearly the kernel is the space of one-forms on C that has a zero at Q, i.e. $\Gamma(C, \Omega^1(-Q))$. By Riemann-Roch and Serre duality,

$$h^0(C, Q) - h^0(C, \Omega^1(-Q)) = \deg[Q] - g + 1 = 2 - g$$

But $h^0(C, Q) = 1$: clearly $\Gamma(C, Q)$ contains all constant functions. Suppose $f \in \Gamma(C, Q)$ is nonconstant, then it has a simple pole at Q and no pole elsewhere. As $\text{div}(f)$ must have degree 0, $\text{div}(f) = [Q'] - [Q]$ for some $Q' \neq Q$, a contradiction to $g > 0$.

Hence $h^0(C, \Omega^1(-Q)) = g - 1$. □

3.2 Symmetric Powers of a Curve

A degree r effective divisor on C is in one-to-one correspondence to a point in $C^r := C \times ... \times C$, modulo permutation. In other words, it corresponds to a point in the r-th **symmetric power** of C, defined by

Notation 3.7. $C^{(r)} := S_r \setminus C^r$, the quotient of C^r by the action of the symmetric group S_r on the left.

The symmetric power is fundamental in the study of Jacobians in two ways:

(1) $C^{(r)}$ is the moduli space of $\mathrm{Div}^r(C)$, the set of degree r effective divisors on C. If r is large enough, Riemann-Roch shows that any divisor class of degree r has a representative which is effective. Thus $\mathrm{Pic}^r(C)$ is a quotient of $\mathrm{Div}^r(C)$. If this quotient has a "section": $\mathrm{Pic}^r \to \mathrm{Div}^r$ in a functorial way, then we can realize the moduli space of $\mathrm{Pic}^r(C)$ as a closed subvariety of $\mathrm{Div}^r(C) = C^{(r)}$. But this is the Jacobian: $\mathrm{Pic}^r(C) \cong \mathrm{Pic}^0(C)$ as they are cosets of the degree homomorphism $\mathrm{Pic}(C) \twoheadrightarrow \mathbb{Z}$.

Remark. In general, however, a "global' section $\mathrm{Pic}^r \to \mathrm{Div}^r$ may not exist, so we have to define the Jacobian piece by piece and glue them together. Thus the Jacobian variety is only known to be complete (i.e. proper), but not necessarily projective. Compare the second remark after Definition 1.1.

(2) The Θ divisor in J plays a fundamental role in the study of Jacobians. It is the invariant on J such that the pair (J, Θ) can recover the curve C. The Θ divisor is defined as the closed subvariety $f^P(C) + ... + f^P(C)$ ($g-1$ copies) in J. It is the image of $C^{(g-1)} \to J, (P_1, ..., P_{g-1}) \mapsto f(P_1) + ... + f(P_{g-1})$, and we will show that it has codimension 1.

Theorem 3.8. *The symmetric power $C^{(r)}$ of any smooth curve is smooth.*

Proof. [1, III.3.2] □

Again, assume C is a projective smooth curve of genus $g > 0$, and fix a point $P \in C$. Write f for the canonical embedding f^P.

Notation 3.9. Let $f^{(r)}$ denote the canonial map $C^{(r)} \to J, (P_1, ..., P_r) \to f(P_1) + ... + f(P_r)$, and $W^r = f^r(C^{(r)}) = f(C) + ... + f(C)$ (r copies).

Note that the obvious map $f^r : C^r \to J$ is permutation invariant, so it factors through $C^{(r)}$ by the universal property of quotient varieties. On points, it sends D to $D - r[P]$, where D is an effective divisor on C of degree r.

Since $C^{(r)}$ is projective, W^r is closed in J.

Theorem 3.10. *For $r \leq g$, the morphism $f^{(r)} : C^{(r)} \to W^r$ is birational. In particular, $\dim W^r = r$, so $W^g = J$, and $f^{(g)}$ is a birational map from $C^{(r)}$ to J.*

Remark. This, together with Corollary 1.8, says that the Jacobian variety of C is the unique abelian variety birational to $C^{(r)}$. Weil uses this as the definition of Jacobians, and gives an alternative construction. See [1, III.7].

Proof. We just give the proof in $\mathrm{char}\, k = 0$ case. For characteristic p, we need to study the induced maps on tangent spaces. See [1, III.5.1].

Claim that it suffices to show that there is an open subset V of $C^{(r)}$ such that $f^{(r)}$ is injective on U. By the theorem about fiber dimension, we have $\dim W^r = \dim C^{(r)}$. By either generic finiteness or some form of Zariski main theorem, we have a theorem about (generic) fiber size even when $f^{(r)}$ is not finite. Thus $\deg(f^{(r)} : C^{(r)} \to W^r)) = 1$ as $\mathrm{char}\, k = 0$, so $f^{(r)} : C^{(r)} \to W^r)$ is birational.

By the following lemma, there is a open subset U of C^r such that $h^0(C, \sum[P_i]) = 1$ for all $(P_1, ..., P_r) \in C^r$. Claim that for two degree r effective divisors $D = \sum[P_i], D' = \sum[P_i']$ such that $(P_i), (P_i') \in U$, if $D \sim D'$ are linearly equivalent, then $D = D'$. Choose a rational function $f \in k(C)^\times$ such that $D - D' = \mathrm{div}(f)$. Then $\mathrm{div}(f) + D' = D$ is effective, so $f \in \Gamma(C, D')$. But $h^0(C, D') = 1$, so f is a constant, and we have $D = D'$.

Chosse $V = \pi(U)$, where π is the quotient map $C^r \to C^{(r)}$. Then the previous claim shows that $f^{(r)}$ is injective on V. Also, $\pi^{-1}(V) = \bigcup_{g \in S_r} g(U)$ is open, so V is open by the definition of quotient topology. □

Lemma 3.11. *For any $r \leq g$, there is an open subset U of C^r such that $h^0(\sum P_i) = 1$ for $(P_1, ..., P_r)$ in U.*

Proof. [1, III.5.2] has a direct proof. □

3.3 The Theta Divisor

The following is an immediate consequence of the birationality statement.

Proposition 3.12. *$f^P : C \to J$ has the following universal property: any morphism $\varphi : C \to A$ to an abelian variety A that sends P to 0 factors through a unique homomorphism $\alpha : J \to A$ of abelian varieties.*

Proof. Define $F : C^{(g)} \to A$ by $(P_1, ..., P_g) \mapsto \sum \varphi(P_i)$. Since $C^{(g)}$ is birational to J, we get a rational map $\alpha : J \dashrightarrow A$. By Theorem 1.6, α is regular, which is the map we want. □

Remark. We can give the formula for α more explicitly. Consider the diagram

$$\begin{array}{ccc} C^{(g)} & \xrightarrow{F} & A \\ {\scriptstyle f^{(g)}}\downarrow & \nearrow_{\alpha} & \\ J & & \end{array}$$

By construction, $\alpha \circ f^{(g)} = F$ as rational maps. So they are the same as morphisms, and hence the diagram commutes. In other words, α is the unique map such that $\alpha([P_1] + ... + [P_g] - g[P]) = \varphi(P_1) + ... + \varphi(P_g)$.

Remark. This universal property says that J is the **Albanese variety** of C with canonical map f^P. It is a general fact that the Picard variety and Albanese variety of a given variety V are dual abelian varieties. In particular, J is isomorphic to its dual. But we are going to give an explicit isomorphism from $J \to J^\vee$ by a principal polarization.

Definition 3.13. The **theta divisor** of J of (C, P) is the prime divisor $\Theta := W^{g-1}$ as in Notation 3.9.

Theorem 3.14. *Θ is an ample divisor, and the polarization $\lambda_\Theta : J \to J^\vee$ is principal (i.e. an isomorphism). Its* negative *inverse is given by*

$$f^\vee : J^\vee \to J$$

$$b \in \mathrm{Pic}^0(J) \mapsto f^*(b) \in \mathrm{Pic}^0(C) = J$$

where $f = f^P$ is the canonical embedding.

Proof. Note that $f^\vee$ is the induced map of $f : C \to J$ on their Picard varieties (see next section).

The statement that λ_Θ and $f^\vee$ being inverse means

(1) For $a \in J$,

$$f^*(t_a^*(\Theta) - \Theta) = -a \in \mathrm{Pic}^0(C)$$

(2) For $b \in \mathrm{Pic}^0(J)$, let $a = f^*(b) \in \mathrm{Pic}^0(C) = J$,

$$t_a^*(\Theta) - \Theta = -b \in \mathrm{Pic}^0(J)$$

See [1, III.6.9]. □

Corollary 3.15. *Let $\Theta' = m^*\Theta - p^*\Theta - q^*\Theta$ on $J \times J$, as in the discussion above Notation* 1.32. *Recall that L^P is a sheaf on $C \times C$ with $L^P|_{C\times Q} = f(Q)$. Then*

$$(f \times f)^*(\Theta') = -L^P \in \mathrm{Pic}(C \times C)$$

Proof.

$$(f \times f)^*(\Theta')|_{C\times Q} = f^*(\Theta'|_{J\times f(Q)}) = f^*(\lambda_\Theta(f(Q))) = -f(Q)$$

by statement (1) above.

But $L^P|_{C\times Q} = f(Q)$ and $(f \times f)^*(\Theta')|_{P\times C} = f^*(\Theta'|_{0\times J}) = 0$, the result follows from the seesaw principle. □

In light of Theorem 1.44, we get the following.

Corollary 3.16. $(\Theta^g) = g!$

We give one more formula from [7, IV.3] to be used later. [More reference needed]

Proposition 3.17. (Θ^{g-1}) *is numerically equivalent to* $(g-1)!f(C)$ *as* 1*-cycles on* J. *In other words, for any divisor* D *of* J, *we have*

$$(\Theta^{g-1} \cdot D) = (g-1)!(C \cdot D)$$

3.4 Digressions on Albanese and Picard varieties as functors

It is worth pointing out that for all smooth projective varieties V, $\mathrm{Pic}^0(V)$ makes sense and the Picard and Albanese varieties exist as abelian varieties, and they are dual to each other. We have proven these for curves and abelian varieties, and we won't use the version for general projective varieties in this article.

Let $(V_1, P_1), (V_2, P_2)$ be smooth projective varieties with base points chosen, and $\alpha : V_1 \to V_2$ be a morphism sending P_1 to P_2. Let J_1, J_2 be their Picard varieties with Poincaré sheaves $\mathcal{P}_1, \mathcal{P}_2$, and A_1, A_2 be their Albanese varieties with canonical map $f_i : V_i \to A_i$.

By the universal property of Albanese varieties, there is unique map $\mathrm{Alb}(\alpha) = \alpha' : A_1 \to A_2$ such that the diagram

$$\begin{array}{ccc} V_1 & \xrightarrow{\alpha} & V_2 \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} \\ A_1 & \dashrightarrow^{\alpha'} & A_2 \end{array}$$

Clearly this makes Alb a covariant functor from the category of projective varieties to the category of abelian varieties.

On the other hands, we have $\mathrm{Pic}^0(\alpha) = \alpha^\vee : J_2 \to J_1$ defined by $\mathrm{Pic}^0(V_2) \xrightarrow{\alpha^*} \mathrm{Pic}^0(V_1)$ on points. This is regular, as $\alpha^\vee$ comes from $(\alpha \times 1)^*\mathcal{P}_2$ on $V_1 \times J_2$. Indeed

$$((\alpha \times 1)^*\mathcal{P}_2)|_{V_1\times b} = \alpha^*(\mathcal{P}_2|_{V_2\times b}) = \alpha^*(b)$$

Thus Pic^0 is a contravariant functor from the category of projective varieties to the category of abelian varieties.

The duality of Picard and Albanese varieties is given by the canonical isomorphism $f^\vee : A^\vee = \mathrm{Pic}^0(A) \xrightarrow{\cong} \mathrm{Pic}^0(V) = J$. We have known this when V is a curve or an abelian variety.

In fact $\alpha^\vee : J_2 = A_1^\vee \to J_1 = A_1^\vee$ is the dual homomorphism of $\alpha' : A_1 \to A_2$. Applying Pic^0 functor to the commutative diagram above, we get

$$\begin{array}{ccc} J_1 = \mathrm{Pic}^0(V_1) & \xleftarrow{\alpha^\vee} & \mathrm{Pic}^0(V_2) = J_2 \\ {\scriptstyle f_1^\vee}\uparrow\cong & & \cong\uparrow{\scriptstyle f_2^\vee} \\ A_1^\vee = \mathrm{Pic}^0(A_1) & \xleftarrow{(\alpha')^\vee} & \mathrm{Pic}^0(A_2) = A_2^\vee \end{array}$$

When $V_1 = C_1, V_2 = C_2$ are curves, the Albanese varieties are equal to the Jacobians, so α induces a morphism $J_1 = \mathrm{Pic}^0(C_1) \xrightarrow{\alpha'} \mathrm{Pic}^0(C_2) = J_2$ *covariantly*. Applying the remark after Proposition 3.12, with $\varphi : C_1 \to J_2, Q \mapsto f_2(\alpha(Q)) = [\alpha(Q)] - P_2$, we get

$$\alpha'([Q_1] + ... + [Q_g] - g[P_1]) = [\alpha(Q_1)] + ... + [\alpha(Q_1)] - g[P_2]$$

Define the **pushforward** of divisors by

$$\alpha_* : \mathrm{Div}(C_1) \to \mathrm{Div}(C_2), [Q] \mapsto [\alpha(Q)]$$

This is a degree preserving group homomorphism. The map $\alpha_* : \mathrm{Pic}^0(C_1) \to \mathrm{Pic}^0(C_2)$ that α_* induces on degree 0 divisor classes is exactly α', which is well defined. In particular, the pushforward of a principal divisor (which always has degree 0) is principal, so α_* is defined on $\mathrm{Pic}(C_1) \to \mathrm{Pic}(C_2)$.

In summary, the Albanese of a morphism between curves is the pushforward map of degree zero divisor classes.

3.5 The Zeta Function of an Abelian Variety

The goal of the next two sections is to prove the key statements in the Weil conjecture for abelian varieties and curves. We prove the version for abelian varieties in this section, and in next section, we will prove the version for curves by passing to its Jacobian. I will only state and prove the key statements about counting points, and leave the rest to the final section to avoid distraction. It will be a straightforward exercise to translate these into statements about zeta functions, namely, rationality, functional equation and Riemann hypothesis in Weil conjecture.

Let $q = p^r$ be a prime power, $\mathbb{F}_q$ be the finite field of q elements and $k = \overline{\mathbb{F}}_q$ be its algebraic closure. A variety V over $\overline{\mathbb{F}}_q$ is said to be **defined over** $\mathbb{F}_q$ if there is a variety V_0 over $\mathbb{F}_q$ such that $V = V_0 \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q$. Define the **Frobenius endomorphism** $\pi = \pi_q : V \to V$ by

$$\pi = Fr_q \times id : V_0 \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q \to V_0 \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q,$$

where Fr_q is the absolute Frobenius endomorphism on V_0 in the sense of [4, 7.3.S], i.e. identity on topological space and ring map $a \mapsto a^q$ on coordinate ring. Note that the absolute Frobenius gives a natural transformation from the identity functor to itself, on the category of $\mathbb{F}_q$-varieties.

Note that π is an endomorphism of an $\overline{\mathbb{F}}_q$-variety, and if V is a projective varieties in $\mathbb{P}^n_{\overline{\mathbb{F}}_q}$ cut out by $f_1, ..., f_r \in \mathbb{F}_q[X_0, ..., X_n]$, then the effect of π on points is

$$\pi(x_0, ..., x_n) = (x_0^q, ..., x_n^q)$$

Clearly an $\mathbb{F}_q$-point of V is precisely a fixed point of π.

Now let A be an abelian variety of dimension g that is defined over $\mathbb{F}_q$. Note that $0 \in A(\mathbb{F}_q)$. Recall that the characteristic polynomial P_π is a monic rational polynomial of degree $2g$. Let

$P_\pi(X) = \prod_{i=1}^{2g}(X - a_i)$, $a_i \in \mathbb{C}$. The roots a_i of the characteristic polynomial of the Frobenius endomorphism are important invariants of an abelian variety, and they encode most of (if not all) arithmetic properties of an abelian variety.

Note that $\prod a_i = \deg(\pi) = q^g$. The fact that $\deg(\pi) = q^g$ is true for any variety of dimension g. It suffices to prove this for an affine variety $V = V_0 \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q$. By Noether normalization, there is a finite surjective map $f : V_0 \twoheadrightarrow \mathbb{A}^g_{\mathbb{F}_q}$. Consider the naturality diagram of absolute Frobenius

$$\begin{array}{ccc} V_0 & \xrightarrow{\pi} & V_0 \\ \downarrow f & & \downarrow f \\ \mathbb{A}^g_{\mathbb{F}_q} & \xrightarrow{\pi} & \mathbb{A}^g_{\mathbb{F}_q} \end{array}$$

Apply the base change functor to $\overline{\mathbb{F}}_q$, we get a diagram of finite surjective maps

$$\begin{array}{ccc} V & \xrightarrow{\pi} & V \\ \downarrow f & & \downarrow f \\ \mathbb{A}^g_{\overline{\mathbb{F}}_q} & \xrightarrow{\pi} & \mathbb{A}^g_{\overline{\mathbb{F}}_q} \end{array}$$

Since degrees of finite maps are multiplicative, the claim follows from the fact that $\overline{\mathbb{F}}_q[X_1, ..., X_g]$ is a free module over $\overline{\mathbb{F}}_q[X_1^q, ..., X_g^q]$ of rank q^g.

Theorem 3.18. *Wrtie $P_\pi(X) = \prod_{i=1}^{2g}(X - a_i)$, $a_i \in \mathbb{C}$. Let $N_m = \#A(\mathbb{F}_{q^m})$. Then*

(a) $N_m = P_{\pi^m}(1) = \prod_{i=1}^{2g}(1 - a_i^m)$

(b) *(Riemann Hypothesis)* $|a_i| = q^{1/2}$.

Proof. (a) Let us first prove the $m = 1$ case. Since $0 \in A(\mathbb{F}_q)$, $\pi(0) = 0$, so $\pi \in \mathrm{End}(A)$. As $\ker(\pi - id) = A(\mathbb{F}_q)$ is finite, $\pi - id$ is an isogeny. Note that $N_1 = \#\ker(\pi - id)$ and $\deg(\pi - id) = P_\pi(1) = \prod_{i=1}^{2g}(1 - a_i)$, so it suffices to prove that $\pi - id$ is separable.

Recall from Proposition 1.24 that an isogeny is separable iff it is étale. In fact being unramified at the origin is enough, by homogeneity. In light of [4, 21.6.I], we need to show

$$d(\pi - id)_0 : T_0(A) \to T_0(A)$$

is injective.

We have $d(\pi - id)_0 = d\pi_0 - id$ on $T_0(A)$. (Substraction means different things at both sides. This needs proof, and it is a general fact for group varieties.)

Claim that $d\pi_0 = 0$. The question is local, so it suffices to prove it for an arbitrary affine variety $V = \operatorname{Spec} R \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$. The key reason is the computation that $d(X^q) = qX^{q-1}dX = 0$ as $q = 0 \in \mathbb{F}_q$. I give two points of view to prove it formally, as an exercise to practice the definitions:

Geometrically, let $V = V(f_1, ..., f_r) \subseteq \mathbb{A}^n_{\overline{\mathbb{F}}_q}$, $f_i \in \mathbb{F}_q[X_1, ..., X_n]$, then $d\pi_{(x_1,...,x_n)}$ is given by the matrix $[\dfrac{\partial \pi_i}{\partial X_j}] = [\dfrac{\partial X_i^q}{\partial X_j}]$ (where π_i means the i-th coordinate component of π). But

$$\frac{\partial X_i^q}{\partial X_j} = q\frac{\partial X_i^{q-1}}{\partial X_j} = 0$$

as $q = 0 \in \mathbb{F}_q$.

Algebraically, look at $\pi^\sharp : R \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q \to R \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q, f \otimes x \mapsto f^q \otimes x$. Denote $\overline{R} = R \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$, then its induced map on the differential module is $\Omega_{\overline{R}/\overline{\mathbb{F}}_q} \to \Omega_{\overline{R}/\overline{\mathbb{F}}_q}$ with

$$\begin{aligned} d(f \otimes x) \mapsto d(f^q \otimes x) &= d((f \otimes 1)^q (1 \otimes x)) = (1 \otimes x) d((f \otimes 1)^q) \text{ (as } 1 \otimes x \text{ is a scalar in } \overline{\mathbb{F}}_q) \\ &= xq(f^{q-1} \otimes 1) d(f \otimes 1) \text{ (Leibniz rule)} \\ &= 0 \text{ (as } q = 0 \in \mathbb{F}_q) \end{aligned}$$

So the π induces the zero map on the map of differential sheaves, and thus zero on the cotangent space, and hence zero on the tangent space.

Now look at the general $m \geq 1$ case. Since a_i's are the eigenvalues of $V_\ell \pi$ on $V_\ell A$, the eigenvalues of $V_\ell \pi^m$ are a_i^m. Thus

$$P_{\pi^m}(X) = \prod_{i=1}^{2g} (X - a_i^m) \qquad (*)$$

Apply the previous case to $\mathbb{F}_{q^m}$, we get

$$N_m = P_{\pi^m}(1) = \prod_{i=1}^{2g} (1 - a_i^m)$$

(b) See Theorem 4.27.

□

Corollary 3.19. *In the setting of the theorem above,*

(a) *Under some ordering of a_i, we have*

$$a_i = \overline{a_{2g+1-i}} = \frac{q}{a_{2g+1-i}}$$

In other words, the multisets $\{a_i\}$ and $\{q/a_i\}$ are the same.

(b) *(Hasse-Weil inequality) $N_m = q^{mg} + O(q^{\frac{2g-1}{2}m})$.*
More specifically,

$$|N_m - q^{mg}| \leq (q^{m/2} + 1)^{2g} - q^{mg} \sim 2g q^{\frac{2g-1}{2}m}$$

Proof. (a) Since a_i's are the roots of $P_\pi(X)$, which is a real polynomial, they appear in complex conjugates. But since $|a_i| = q^{1/2}$, we have $\overline{a}_i = q/a_i$.

(b) Expand $\prod_{i=1}^{2g}(1 - a_i^m) - q^{mg}$ by the binomial theorem, and we get an upper estimate of its absolute value if we replace each term by its norm. But this will be the same as expanding $\prod_{i=1}^{2g}(1 + (q^{1/2})^m) - q^{mg}$. Note that $\prod a_i = \deg(\pi) = q^g$, so q^{mg} cancels a term in the binomial expansion.

Therefore $|N_m - q^{mg}| \leq (q^{m/2} + 1)^{2g} - q^{mg}$ and the right hand side can be approximated by the derivative $(X^{2g})'|_{X = q^{m/2}}$.

□

3.6 The Zeta Function of a Curve

Let C be a (smooth projective) curve of genus g defined over $\mathbb{F}_q$, and J be its Jacobian. Let $a_1, ..., a_{2g}$ be as in Theorem 3.18. Recall that $|a_i| = q^{1/2}$.

Theorem 3.20. *Let $N_m = |\#C(\mathbb{F}_{q^m})|$. Then*

$$N_m = q^m + 1 - \sum a_i^m$$

In particular, we get the Hasse-Weil inequality $|N_m - q^m - 1| \leq 2gq^{m/2}$.

When $g = 0$, $C = \mathbb{P}^1$, the result is obviously true. From now on assume $g > 0$. By equation (*) in the proof of Theorem 3.18, it suffices to do the case $m = 1$.

We will use an analogue of Lefschetz fixed point theorem to count $\mathbb{F}_q$-points.

Theorem 3.21. *Let C be a curve over an algebraically closed field k, and choose a base point $P \in C$. Let $\alpha : (C, P) \to (C, P)$ be an endomorphism of C fixing P. Let J be the Jacobian of C, and $\alpha' = \mathrm{Alb}(\alpha)$. Denote by Δ the diagonal of C in $C \times C$, and $\Gamma_\alpha = \{(c, \alpha(c)\}$ the graph of α in $C \times C$. Then*

$$(\Gamma_\alpha \cdot \Delta) = 1 - \mathrm{tr}(\alpha') + \deg(\alpha)$$

For convenience, assume C has an $\mathbb{F}_q$-point P. (What if it does not?) Let $\alpha = \pi_C$, then $\alpha(P) = P$. Claim $\alpha' = \pi_J$: consider the naturality diagram of Frobenius

$$\begin{array}{ccc} C & \xrightarrow{\pi_C} & C \\ \downarrow{\scriptstyle f^P} & & \downarrow{\scriptstyle f^P} \\ J & \xrightarrow{\pi_J} & J \end{array}$$

Then $\pi_J = \mathrm{Alb}(\pi_C)$. The trace of π_J is $\sum a_i$, and the degree of π_C is $q^{\dim C} = q$. Moreover, I claim that Γ_{π_C} and Δ intersects transversally, so $(\Gamma_{\pi_C} \cdot \Delta)$ is the cardinality of the fixed points of π_C. Recall that $d\pi_C = 0$ for any variety C over $\mathbb{F}_q$, from the proof of Theorem 3.18. So the tangent space of Γ_{π_C} at any point is the span of vector $(1, 0)$, and the tangent space of Δ is the span of $(1, 1)$. They are linearly independent, so Γ_{π_C} and Δ intersects transversally.

Having these, Theorem 3.20 follows.

The rest of this section will be dedicated to the proof of Theorem 3.21. We first prove a lemma.

Lemma 3.22. *Let A be an abelian variety of dimension g, and H be the class of an ample divisor in $\mathrm{NS}(A)$. For $\alpha \in \mathrm{End}(A)$, let $D_H(\alpha) = (\alpha + 1)^* H - \alpha^*(H) - H$, then*

$$\mathrm{tr}(\alpha) = g\frac{(H^{g-1} \cdot D_H(\alpha))}{(H^g)}$$

Proof. Recall from the proof of Theorem 2.16 that

$$H_n \sim n(n-1)H + nH_1 - (n-1)H_0$$

where $H_n = (\alpha + n)^* H$. (Note that $n*$ acts as n^2 on the Néron-Severi group. See the remark (b) after Corollary 2.22.)

Thus

$$(\alpha + n)^* H \sim Hn^2 + ((\alpha + 1)^* H - \alpha^* H - H)n + \alpha^* H = Hn^2 + D_H(\alpha)n + \alpha^* H$$

Consider

$$P_\alpha(-n) = \deg(\alpha + n) = \frac{\big(((\alpha+n)^*H)^g\big)}{(H^g)} = \frac{((Hn^2 + D_H(\alpha)n + \alpha^*H)^g)}{(H^g)}$$

The n^{2g-1} coefficient of left hand side is $\mathrm{tr}(\alpha)$, and for the right hand side, to get an n^{2g-1} term, we must pick $D_H(\alpha)n$ from one of the g parentheses and Hn^2 from all others. Therefore

$$\mathrm{tr}(\alpha) = g\frac{(H^{g-1} \cdot D_H(\alpha))}{(H^g)}$$

□

Proof of Theorem 3.21. Recall $\Theta' = m^*\Theta - p^*\Theta - q^*\Theta$. Look at $F := f \circ \alpha = \alpha' \circ f : C \to J$. Consider $(f, F) : C \to J \times J$. Let us compute the degree of $(f, F)^*\Theta' \in \mathrm{Pic}(C)$ in two ways.

Use the fact from intersection theory that, let $i : C \hookrightarrow V$ be a closed embedding from a smooth curve C to a smooth projective variety V, and D a divisor on V, then

$$(i(C) \cdot D) = \deg i^*(D)$$

We have

$$(f, F)^*m^*\Theta' = f^*(1+\alpha')^*\Theta \text{ has degree } (f(C) \cdot (1+\alpha')^*\Theta).$$
$$(f, F)^*p^*\Theta' = f^*\Theta \text{ has degree } (f(C) \cdot \Theta).$$
$$(f, F)^*q^*\Theta' = \alpha'^*\Theta \text{ has degree } (f(C) \cdot \alpha^*\Theta).$$

Thus

$$\deg(f, F)^*\Theta' = (f(C) \cdot ((1+\alpha')^*\Theta - \Theta - \alpha^*\Theta)) = (f(C) \cdot D_\Theta(\alpha')) \qquad (1)$$

On the other hand, $(f, F)^*\Theta' = (1, \alpha)^*(f \times f)^*\Theta' = -(1, \alpha)^*\mathcal{L}^P$ by Corollary 3.15, where $\mathcal{L}^P = \Delta - q^*[P] - p^*[P]$. Then

$$\deg(1, \alpha)^*\Delta = (\Gamma_\alpha \cdot \Delta)$$
$$(1, \alpha)^*p^*[P] = 1^*[P] = [P] \text{ has degree } 1.$$
$$(1, \alpha)^*q^*[P] = \alpha^*[P] \text{ has degree } \deg(\alpha).$$

(Recall that the pullback of a degree n divisor on a curve by a degree d finite map has degree nd.)

Thus

$$\deg(f, F)^*\Theta' = -\deg(1, \alpha)^*\mathcal{L}^P = -(\Gamma_\alpha \cdot \Delta) + \deg(\alpha) + 1 \qquad (2)$$

Combining (1) and (2), we get

$$(\Gamma_\alpha \cdot \Delta) = 1 - (f(C) \cdot D_\Theta(\alpha')) + \deg(\alpha)$$

It remains to show that $(f(C) \cdot D_\Theta(\alpha')) = \mathrm{tr}(\alpha')$. By Proposition 3.17, we may replace $f(C)$ by $(g-1)!\Theta^{g-1}$. Recall from Corollary 3.16 that $(\Theta^g) = g!$. Now applying Lemma 3.22 to the ample divisor Θ, we get

$$\mathrm{tr}(\alpha') = g(\Theta^{g-1} \cdot D_\Theta(\alpha'))/(\Theta^g) = g((g-1)!f(C) \cdot D_\Theta(\alpha'))/g! = (f(C) \cdot D_\Theta(\alpha'))$$

□

3.7 Weil Conjecture for Curves and Abelian Varieties

Now you are ready to compute the zeta functions of curves and abelian varieties by yourself. The proofs in this section (probably except the functional equation for abelian varieties) are straightforward computations, and it is the best to do them as exercises rather than reading them.

The **zeta function** of a variety V defined over $\mathbb{F}_q$ is

$$Z(V,t) = \exp\left(\sum_{m=1}^{\infty} N_m \frac{t^m}{m}\right) \in \mathbb{Q}[[t]]$$

where $N_m = \#V(\mathbb{F}_{q^m})$.

As an alternative definition (though we will not use here),

$$Z(V,t) = \prod_{P \in V(\overline{\mathbb{F}}_q)} (1 - t^{\deg P})^{-1} \in \mathbb{Z}[[t]]$$

where $\deg P = [\kappa(P) : \mathbb{F}_q]$. By a direct computation, one can show that $\log Z(V,t) = \sum_{m=1}^{\infty} N_m \frac{t^m}{m}$.

Recall that

$$\sum_{m=1}^{\infty} \frac{X^m}{m} = -\log(1-X) \in \mathbb{Q}[[X]]$$

Theorem 3.23 (Weil Conjecture for Curves)**.** *Let C be a smooth projective curve of genus g defined over $\mathbb{F}_q$. Then*

(a) *(Rationality) $Z(C,t) = \dfrac{P(t)}{(1-t)(1-qt)}$, where $P(t)$ is a degree $2g$ integer polynomial with leading coefficient q^g and constant term 1. In fact, $P(t) = \prod_{i=1}^{2g}(1-a_i t)$, where a_i is as in Theorem 3.20.*

(b) *(Riemann Hypothesis) All zeroes of $P(t)$ has norm $q^{-1/2}$.*

(c) *(Functional Equation) $Z(C, q^{-1}t^{-1}) = q^{1-g}t^{2(1-g)}Z(C,t)$.*

Proof. (a) Recall $N_m(C) = 1 - \sum_{i=1}^{2g} a_i^m + q^m$ from Theorem 3.20. Let us compute $\log Z(C,t)$.

$$\begin{aligned}
\log Z(C,t) &= \sum_{m=0}^{\infty} \frac{t^m}{m}(1 - \sum_{i=1}^{2g} a_i^m + q^m) \\
&= \sum \frac{t^m}{m} - \sum_{i=1}^{2g} \sum \frac{(a_i t)^m}{m} + \sum \frac{(qt)^m}{m} \\
&= -\log(1-t) + \sum_{i=1}^{2g} \log(1-a_i t) - \log(1-qt) \\
&= \log \frac{\prod_{i=1}^{2g}(1-a_i t)}{(1-t)(1-qt)}
\end{aligned}$$

Thus $Z(C,t) = \dfrac{P(t)}{(1-t)(1-qt)}$, where $P(t) = \prod_{i=1}^{2g}(1-a_i t)$. Note that since a_i's are algebraic integers (see the remark after Corollary 2.27), $P(t)$ has coefficients in $\mathbb{Z}$.

(b) This follows from $|a_i| = q^{1/2}$.

(c) By Corollary 3.19(a), $\prod(1 - a_i X) = \prod(1 - qa_i^{-1}X)$. We have

$$\begin{aligned} Z(C, q^{-1}t^{-1}) &= \frac{\prod(1 - a_i(q^{-1}t^{-1}))}{(1 - q^{-1}t^{-1})(1 - q(q^{-1}t^{-1}))} \\ &= \frac{\prod(1 - (qa_i^{-1})(q^{-1}t^{-1}))}{(1 - q^{-1}t^{-1})(1 - t^{-1})} \\ &= \frac{\prod(1 - a_i^{-1}t^{-1})}{(1 - q^{-1}t^{-1})(1 - t^{-1})} \end{aligned}$$

Factoring out denominators, we get

$$\begin{aligned} Z(C, q^{-1}t^{-1}) &= \frac{\left(\prod_{i=1}^{2g}(a_i t - 1)\right) / \left(t^{2g}\prod a_i\right)}{(qt - 1)(t - 1)/qt^2} \\ &= q^{1-g}t^{2(1-g)}Z(C, t) \end{aligned}$$

since $\prod a_i = q^g$.

□

Theorem 3.24 (Weil Conjecture for Abelian Varieties)**.** *Let A be an abelian variety of dimension $g > 0$ defined over $\mathbb{F}_q$. Then*

(a) *(Rationality) $Z(A, t) = \dfrac{P_1(t)P_3(t)...P_{2g-1}(t)}{P_0(t)P_2(t)...P_{2g}(t)}$, where each $P_r(t)$ is an (explicit) integer polynomial of degree $\binom{2g}{r}$ with leading coefficient $(-q^r)^{\binom{2g}{r}}$ and constant term 1.*
The formula for $P_r(t)$ is given by

$$P_r(t) := \prod_{1 \le i_1 < ... < i_r \le 2g} (1 - a_{i_1}...a_{i_r}t)$$

In particular, $P_0(t) = 1 - t$ and $P_{2g}(t) = 1 - q^g t$.

(b) *(Riemann Hypothesis) All zeroes of $P_r(t)$ has norm $q^{-r/2}$.*

(c) *(Functional Equation) $Z(A, q^{-g}t^{-1}) = Z(A, t)$.*

Proof. (a) Recall $N_m(A) = \prod_{i=1}^{2g}(1 - a_i^m)$ from Theorem 3.18. We can expand the product as

$$N_m(A) = \sum_{r=1}^{2g} e_r(-a_1^m, ..., -a_{2g}^m) = \sum_{r=1}^{2g}(-1)^r e_r(a_1^m, ..., a_{2g}^m)$$

where

$$e_r(X_1, ..., X_{2g}) = \sum_{1 \le i_1 < ... < i_r \le 2g} X_{i_1}...X_{i_r}$$

is the elementary symmetric polynomial of degree r in $2g$ variables.

We have $\log Z(A,t) = \sum_{m\geq 1}\sum_{r=1}^{2g} \frac{t^m}{m}(-1)^r e_r(a_1^m,...,a_{2g}^m)$. We sum up with respect to m first:

$$\sum_m \frac{t^m}{m} e_r(a_1^m,...,a_{2g}^m) = \sum_{i_1<...<i_r}\sum_m \frac{(a_{i_1}...a_{i_r}t)^m}{m}$$
$$= \sum_{i_1<...<i_r} -\log(1-a_{i_1}...a_{i_r}t) = -\log P_r(t)$$

if we define $P_r(t) := \prod_{i_1<...<i_r}(1-a_{i_1}...a_{i_r}t)$.

Hence $\log Z(A,t) = \sum_{r=1}^{2g}(-1)^{r+1}\log P_r(t)$, and the desired identity follows.

Finally, since $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ permutes a_i's, the polynomial $P_r(t)$ is stable under Galois action, so P_r is rational. As a_i's are algebraic integers, P_r has coefficients in $\mathbb{Z}$. It has degree $\binom{2g}{r}$ and leading coefficient

$$\prod_{i_1<...<i_r}(-a_{i_1}...a_{i_r}) = (-1)^{\binom{2g}{r}}\prod a_i^{\frac{r}{g}\binom{2g}{r}} = (-q^r)^{\binom{2g}{r}}$$

(b) This follows from $|a_i| = q^{1/2}$.

(c) Rewrite $Z(A,t) = \prod_I (1-a_I t)^{(-1)^{|I|+1}}$, where I ranges over all subsets of $\{1,2,...,2g\}$ and $a_I = \prod_{i\in I} a_i$.

Pair I with its complement $J := \{1,...,2g\} - I$. Note that $|I|$ and $|J|$ have the same parity and $a_I a_J = q^g$. Let us develop a functional equation for $Q_I(t) := (1-a_I t)(1-a_J t)$. Indeed

$$Q_I(q^{-g}t^{-1}) = (1-a_I q^{-g}t^{-1})(1-a_J q^{-g}t^{-1})$$
$$= (1-a_J^{-1}t^{-1})(1-a_I^{-1}t^{-1})$$
$$= (a_J t-1)(a_I t-1)/(a_I a_J t^2) = q^{-g}t^{-2}Q_I(t)$$

Hence $\frac{Z(A,q^{-g}t^{-1})}{Z(A,t)} = (q^{-g}t^{-2})^{-E/2} = q^{gE/2}t^E$, where E is the number of even-sized subsets of $\{1,...,2g\}$ less the number of odd-sized subsets. We have

$$E = \sum_{i=1}^{2g}(-1)^i\binom{2g}{i} = (-1+1)^{2g} = 0$$

Thus $Z(A,q^{-g}t^{-1}) = Z(A,t)$.

□

Remark. (1) The fact that $\deg P_r = \binom{2g}{r}$ is related to the fact that, when $k=\mathbb{C}$, an abelian variety of dimension g has r-th Betti number $\binom{2g}{r}$. Indeed it is topologically a torus $(S^1)^{2g}$, so the claim about Betti numbers follows from Künneth formula.

(2) The proof of functional equation for abelian varieties does not require Riemann Hypothesis, unlike the case of curves. From the computation above, we see that

$$Z(A,q^{-g}t^{-1}) = \pm q^{gE/2}t^E Z(A,t)$$

where E is the alternating sum of Betti numbers. In other words, E is the Euler characteristic (in the sense of singular cohomology, or étale cohomology). This is the version of functional equation that can be generalized to all smooth projective varieties.

4 Polarizations

The purpose of this section is to present a collection of the important results about polarizations and the tools to study them, and to explore the applications and significance of polarizations. There are at least two reasons why we need polarizations:

(a) Some constructions on an ellptic curve E secretly identify $E^\vee$ with E via the unique principal polarization $E \to E^\vee : P \mapsto [P] - [0]$, but for a general abelian variety, we must make a choice of polarization to make these constructions. These constructions include the Weil pairings (studied in 4.1) and dual isogenies (studied in 4.2 as Rosati involution, the higher dimension version).

(b) The collection of abelian varieties of a fixed dimension *together with a polarization of a fixed degree* is much more well behaved than the (bigger) collection of abelian varieties of a fixed dimension. The precise meaning of this is the existence of moduli stack $\mathcal{M}_{g,d}$ of abelian varieties of dimension g polarized at degree d, although this article will never attempt to study or use the theory of moduli. As a result, many finiteness results require us to bound the degree of polarizations.

The Weil pairing is the foundational tool of everything and it deserves an extensive and detailed study.

4.1 Weil Pairings

4.1.1 Basics

To introduce the Weil pairings, we begin with a general construction arisen from the dual exact sequence. Let $\alpha : A \to B$ be an isogeny of abelian varieties over a field k, not necessarily algebraically closed. Then $\ker(\alpha) \subseteq A$ and $\ker(\alpha^\vee) \subseteq B^\vee$ are Cartier dual to each other. In other words,

$$\ker(\alpha^\vee) \cong \mathrm{Hom}_k(\ker(\alpha), \mathbb{G}_m)$$

as k-group schemes.

We thus get a nondegenerate pairing of k-group schemes

$$\ker(\alpha) \times \ker(\alpha^\vee) \to \mathbb{G}_m$$

Note that $\mathrm{Hom}_k(\ker(\alpha)), \mathbb{G}_m)$ defines a k-group schemes as a functor of points $S \mapsto \mathrm{Hom}_S(\ker(\alpha)_S, \mathbb{G}_{m,S})$ for any k-scheme S, where $\ker(\alpha)_S = \ker(\alpha) \times_k S$.

When $S = \operatorname{Spec} k_s$ (the separable closure of k) and $\deg(\alpha)$ is not divisible by $\operatorname{char} k$, α is an étale morphism, so $\ker(\alpha)$ is étale over k. As a result, $\ker(\alpha)_{k_s}$ is just an abstract finite group consisting of reduced points. Thus $\mathrm{Hom}_{k_s}(\ker(\alpha)_{k_s}), \mathbb{G}_{m,k_s}) = \mathrm{Hom}(\ker(\alpha)(k_s), k_s^\times)$, the latter being the group of abstract group homomorphisms. Moreover, it has a $\mathrm{Gal}(k_s/k)$ action by applying the functor of points to any Galois map $k_s \to k_s$. The isomorphism of k-group schemes yields

$$\ker(\alpha^\vee)(k_s) \cong \mathrm{Hom}(\ker(\alpha)(k_s), k_s^\times)$$

which corresponds to a nondegenerate pairing of $\mathrm{Gal}(k_s/k)$-modules

$$e_\alpha : \ker(\alpha)(k_s) \times \ker(\alpha^\vee)(k_s) \to k_s^\times$$

To summarize,

Definition 4.1 (Generalized Weil pairing)**.** Given an isogeny $\alpha : A \to B$ over a field k whose characteristic does not divide $\deg \alpha$, then we have a canonical pairing

$$e_\alpha : \ker(\alpha)(k_s) \times \ker(\alpha^\vee)(k_s) \to k_s^\times$$

which is nondegenerate and Galois equivariant.

The Weil pairing is the special case where α is the multiplication-by-m map $m : A \to A$, where m is not divisible by $\operatorname{char} k$. We denote the Weil pairing by

$$e_m : A[m](k_s) \times A^\vee[m](k_s) \to k_s^\times$$

Note that the left hand side is killed by m, so e_m actually lands in $\mu_m(k_s)$, the group of m-th roots of unity in k_s. From now on, for any k-scheme X, we denote $x \in X(k_s)$ simply by $x \in X$. Note that $A[m](k_s) = A[m](\overline{k})$ for m not divisible by $\operatorname{char} k$.

It worths having an explicit definition of (generalized) Weil pairing by tracing the construction of dual exact sequence, following Theorem 1.47. Consider $\alpha : A \to B$, set $N = \ker(\alpha)$, $N^\vee = \ker(\alpha^\vee)$. The Cartier dual pairing is defined as the following: let $a \in N, b \in N^\vee \subseteq B^\vee = \operatorname{Pic}^0(B)$, we fix a trivialization $i : \alpha^* b \to \mathcal{O}_A$. Then $e_\alpha(a, b)$ is the automorphism of $\mathcal{O}_A$ given by the composition

$$\mathcal{O}_A \xrightarrow{i^{-1}} \alpha^* b = (\alpha \circ t_a)^* b = t_a^* \alpha^* b \xrightarrow{t_a^* i} t_a^* \mathcal{O}_A = O_A$$

Now we translate these to the language of divisors. Let D be a divisor of B that represents b, then b is isomorphic to the subsheaf $\mathcal{O}(D)$ of the constant sheaf $k(B)$ defined by

$$\mathcal{O}_B(D)(U) = \{f \in \Gamma(U, \mathcal{O}_B) : \operatorname{div} f + D|_U \geq 0\}$$

for open subset U of B. Let the trivialization $i : \mathcal{O}_A(\alpha^* D) \to \mathcal{O}_A(0)$ be defined by division by $f \in k(A)$, where $\operatorname{div} f = \alpha^* D$. Then the composition above can be written as

$$\mathcal{O}_A(0) \xrightarrow{f} \mathcal{O}_A(\alpha^* D) = \mathcal{O}_A(t_a^* \alpha^* D) \xrightarrow{(t_a^* f)^{-1}} \mathcal{O}_A(t_a^* 0) = \mathcal{O}_A(0),$$

where every sheaf is viewed as a subsheaf of $k(A)$.

Hence the composition is multiplication by $\dfrac{f}{f \circ t_a}$, and it must be a constant since it gives an automorphism of $\mathcal{O}_A$.

We summarize this as the following proposition.

Proposition 4.2. *Let $\alpha : A \to B$ be an isogeny of abelian varieties over k whose characteristic does not divide* $\deg \alpha$*. Then for $a \in \ker(\alpha), b \in \ker(\alpha^\vee)$, view b as a line bundle on A and let D be a divisor that represents it. Choose a rational function $f \in k(A)$ such that* $\operatorname{div}(f) = \alpha^* D$*. Then* $\dfrac{f}{f \circ t_a}$ *is a constant and*

$$e_\alpha(a, b) = \frac{f}{f \circ t_a} = \frac{f(x)}{f(x + a)}$$

In particular,

Proposition 4.3. *Let A/k be an abelian variety and m is not divisible by* $\operatorname{char} k$*. Given $a \in A[m], b \in A^\vee[m]$, we can compute $e_m(a, b)$ by the following: view b as a line bundle on A and let D be a divisor that represents it. Choose a rational function $f \in k(A)$ such that* $\operatorname{div}(f) = m^* D$*. Then* $\dfrac{f}{f \circ t_a}$ *is a constant and*

$$e_m(a, b) = \frac{f}{f \circ t_a} = \frac{f(x)}{f(x + a)}$$

Note that one can also treat this as the definition of the Weil pairing and then verify directly that Weil pairing is well defined, bilinear, nondegenerate and Galois equivariant, though not as obvious as from the viewpoint of Cartier duality. From now on, however, it is more convenient to develop other properties of Weil pairing using this explicit definition.

Lemma 4.4. *Let m and n are integers not divisible by* $\operatorname{char} k$. *Then for all $a \in A[mn]$ and $b \in A^\vee[mn]$, we have*

$$e_{mn}(a,b)^n = e_m(na, nb)$$

Proof. Let divisor D represent b in $\mathrm{Pic}(A)$. Choose rational function g, g' such that $\mathrm{div} g = m^*(nD)$ and $\mathrm{div} g' = (mn)^* D$.

Then $div(g \circ n) = n^* \mathrm{div}(g) = n^*(m^*(nD)) = n(mn)^* D = n\mathrm{div}(g')$, so that $g(nx) = cg'(x)^n$ for some constant $c \in k_s^\times$. Now

$$\mathrm{RHS} = \frac{g(nx+na)}{nx} = \frac{g \circ n(x+a)}{g \circ n(x)} = \frac{cg'(x+a)^n}{cg'(x)^n} = \left(\frac{g'(x+a)}{g'(x)}\right)^n = \mathrm{LHS}$$

□

Corollary 4.5. *[Compatibility of Weil pairings] For m, n as above,*

$$e_{mn}(a,b) = e_m(a, nb)$$

$$e_{mn}(a,b) = e_m(na, b)$$

whenever it is defined, i.e. $a \in A[m], b \in A^\vee[mn]$ in the first identity and $a \in A[mn], b \in A^\vee[m]$ in the second identity.

Proof. For the first one, write $a = nc$ where $c \in A[mn](k_s) = A[mn](\overline{k})$, using the fact that $A(\overline{k})$ is divisible. So

$$e_{mn}(a,b) = e_{mn}(nc, b) = e_{mn}(c,b)^n = e_m(nc, nb) = e_m(a, nb)$$

The second identity is similar. □

The lemma shows the following diagram commutes for prime $\ell \neq \operatorname{char} k$:

$$\begin{array}{ccccccc} e_{\ell^{n+1}}: & A[\ell^{n+1}] & \times & A^\vee[\ell^{n+1}] & \longrightarrow & \mu_{\ell^{n+1}} \\ & \downarrow \ell & & \downarrow \ell & & \downarrow \ell \\ e_{\ell^n}: & A[\ell^n] & \times & A^\vee[\ell^n] & \longrightarrow & \mu_{\ell^n} \end{array}$$

Take inverse limit, we get a perfect pairing of $\mathbb{Z}_\ell$-modules that is equivariant under the action of $\mathrm{Gal}(k_s/k)$:

$$e_\ell : T_\ell A \times T_\ell A^\vee \to T_\ell \mu =: \mathbb{Z}_\ell(1)$$

Note that $\mathbb{Z}_\ell(1)$ is non-canonically isomorphic to $\mathbb{Z}_\ell$ as $\mathbb{Z}_\ell$-modules, once we fix a compatible system of ℓ^n-th roots of unity. However, the Galois action on $\mathbb{Z}_\ell(1)$ is not trivial, while by $\mathbb{Z}_\ell$ we always mean the trivial $\mathrm{Gal}(k_s/k)$ module. Also, I will write $\mathbb{Z}_\ell(1)$ sometimes additively and sometimes multiplicatively. Finally, the notation e_ℓ is ambiguous as it could denote pairings on ℓ-torsions or on Tate modules, but the meaning will be clear from the source or target of the pairing and I will almost always use e_ℓ to denote the pairing on Tate modules.

Definition 4.6. Let $\lambda : A \to A^\vee$ be a homomorphism. Define the pairing

$$e_m^\lambda(a,b) := e_m(a, \lambda b)$$

for $a, b \in A[m]$ and the pairing

$$e_\ell^\lambda(a,b) := e_\ell(a, \lambda b)$$

for $a, b \in T_\ell A$.

If $\lambda = \lambda_{\mathcal{L}}$ comes from a line bundle L on A, then we may write $e_m^{\mathcal{L}}$, $e_\ell^{\mathcal{L}}$ in place of $e_m^\lambda, e_\ell^\lambda$. Note that $\lambda_{\mathcal{L}}$ is determined by the class of $\mathcal{L}$ in $NS(A) = \mathrm{Pic}(A)/\mathrm{Pic}^0(A)$ and vice versa.

Proposition 4.7. *[Properties of Weil pairings] For a homomorphism $\alpha : A \to B$, the following formulae hold whenever both sides are defined:*

(a) *Adjointness:* $e_m(a, \alpha^\vee(b)) = e_m(\alpha(a), b)$.

(b) $e_m^{\alpha^\vee \circ \lambda \circ \alpha}(a, a') = e_m^\lambda(\alpha(a), \alpha(a'))$ *for* $\lambda \in \mathrm{Hom}(B, B^\vee)$.

(c) $e_m^{\alpha^*\mathcal{L}}(a, a') = e_m^{\mathcal{L}}(\alpha(a), \alpha(a'))$ *for* $\mathcal{L} \in \mathrm{Pic}(B)$.

(d) $e_m^{\lambda\otimes\mu} = e_m^\lambda e_m^\mu$ *for* $\lambda, \mu \in \mathrm{Hom}(A, A^\vee)$.

(e) $e_m^{\mathcal{L}\otimes\mathcal{M}} = e_m^{\mathcal{L}} e_m^{\mathcal{M}}$ *for* $\mathcal{L}, \mathcal{M} \in \mathrm{Pic}(A)$.

(f) *For $\mathcal{L} \in \mathrm{Pic}(A)$, the pairing $e_m^{\mathcal{L}}$ on $A[m]$ is alternating (thus, skew-symmetric).*

By taking $m = \ell^n$ and taking inverse limit, we get similar properties for Weil pairing on Tate modules.

Proof. All the properties are easy exercises except the last one.

(a) Let divisor D on B represent $b \in B^\vee = \mathrm{Pic}^0(B)$, and g be a rational function on B with $\mathrm{div}(g) = m^*D$. Then α^*D represents $\alpha^\vee b$, and $\mathrm{div}(g \circ \alpha) = \alpha^*(m^*D) = m^*(\alpha^*D)$. Hence

$$e_m(a, \alpha^\vee(b)) = \frac{g \circ \alpha(x+a)}{g \circ \alpha(x)} = \frac{\alpha x + \alpha a}{\alpha x} = e_m(\alpha a, b)$$

(b)
$$e_m^{\alpha^\vee \circ \lambda \circ \alpha}(a, a') = e_m(a, \alpha^\vee \circ \lambda \circ \alpha(a')) = e_m(\alpha a, \lambda(\alpha a')) = e_m^\lambda(\alpha a, \alpha a')$$
where the second equality is from adjointness.

(c) By (b), one just need to prove that $\lambda_{\alpha^*\mathcal{L}} = \alpha^\vee \circ \lambda_{\mathcal{L}} \circ \alpha$. Indeed,

$$\lambda_{\alpha^*\mathcal{L}}(a) = t_a^*\alpha^*\mathcal{L} - \alpha^*\mathcal{L} = \alpha^* t_{\alpha(a)}^*\mathcal{L} - \alpha^*\mathcal{L} = \alpha^*(t_{\alpha(a)}^*\mathcal{L} - \mathcal{L}) = \alpha^*\lambda_{\mathcal{L}}(\alpha a)$$

(d) Trivial.

(e) This comes from $\lambda_{\mathcal{L}\otimes\mathcal{M}} = \lambda_{\mathcal{L}} + \lambda_{\mathcal{M}}$.

(f) Let $a \in A[m]$, and we shall show $e_m^{\mathcal{L}}(a,a) = e_m(a, \lambda_{\mathcal{L}}(a)) = 1$. Let D be a divisor representing $\mathcal{L}$, then divisor $t_a^*D - D$ represents $\lambda_{\mathcal{L}}(a)$. Choose rational function $g \in k(A)$ such that $\operatorname{div}(g) = m^*(t_a^*D - D)$. Then $e_m^{\mathcal{L}}(a,a) = g(x)/g(x+a)$ and it suffices to show $g(x) = g(x+a)$.

Choose $b \in A$ such that $mb = a$, by divisibility. Consider the function $f(x) = \prod_{i=1}^m g(x+ib)$, and we have

$$\begin{aligned}
\operatorname{div}(f) &= \sum_{i=1}^m t_{ib}^* \operatorname{div}(g) = \sum_{i=1}^m t_{ib}^* m^*(t_a^*D - D) \\
&= \sum_{i=1}^m m^* t_{ia}^*(t_a^*D - D) \text{ (as } m \circ t_{ib} = t_{ia} \circ m) \\
&= \sum_{i=1}^m m^* t_{(i+1)a}^* D - \sum_{i=1}^m m^* t_{ia}^* D \\
&= 0 \text{ (as } ma = 0)
\end{aligned}$$

Hence $f(x)$ is a constant and $f(x) = f(x+b)$. But this means

$$\prod_{i=1}^m g(x+ib) = \prod_{i=1}^m g(x+b+ib)$$

After cancellation, we get $g(x) = g(x+mb) = g(x+a)$, and we are done.

□

4.1.2 Detecting polarizations using Weil pairings

In this section, we assume k is algebraically closed.

We have seen that e_ℓ^λ is alternating if $\lambda = \lambda_{\mathcal{L}}$ comes from a line bundle. In this section, we shall show that the converse is true if $\operatorname{char} k \neq 2$. We will show a number of results of this flavor, that is, to use the Weil paring induced by λ to detect whether λ comes from a line bundle or furthermore, a polarization. The goal of this section is to prove the Zarhin's trick, which states that $(A \times A^\vee)^4$ is principally polarized for any abelian variety A.

The picture we will keep in mind is the chain of inclusions

$$\operatorname{Pol}^0(A) \subseteq \operatorname{Pol}(A) \subseteq \operatorname{NS}(A) = \frac{\operatorname{Pic}(A)}{\operatorname{Pic}^0(A)} \subseteq \operatorname{Hom}(A, A^\vee) \overset{e_\ell^\bullet}{\hookrightarrow} \operatorname{Hom}_{\mathbb{Z}_\ell}(T_\ell A \otimes T_\ell A, \mathbb{Z}_\ell(1)) \qquad (*)$$

where $\operatorname{Pol}(A) = \{\lambda \in \operatorname{NS}(A) : \lambda : A \to A^\vee \text{ is an isogeny}\}$ and $\operatorname{Pol}^0(A)$ is the set of polarizations in $\operatorname{Pol}(A)$. (These are my temporary notations; I have not seen a name for the "polarizations" arisen from nondegenerate but not necessarily ample line bundles. Milne uses $\operatorname{Pol}(A)$ for the set of polarizations.) The last three objects are groups connected with group homomorphisms; the first two objects are just sets. The last object can be viewed as the set of all bilinear pairings on $T_\ell A$. The last arrow is an inclusion because if $e_\ell^\lambda(a,a') = e_\ell(a, \lambda a') = 0$ for all $a, a' \in T_\ell A$, then $\lambda a' = 0$ by nondegeneracy.

Equivalently, $\operatorname{Pol}(A)$ is the set of algebraic equivalent classes of nondegenerate line bundles and $\operatorname{Pol}^0(A)$ is the set of algebraic equivalent classes of ample line bundles. Note that ampleness is well defined on $\operatorname{NS}(A)$: by Theorem 1.44(e), the index of line bundle is well defined on $\operatorname{Pol}(A)$, and a

nondegenerate line bundle is ample if and only if its index is 0. In other words, $\mathrm{Pol}^0(A)$ is the preimage of 0 under the index map $i : \mathrm{Pol}(A) \to \{0, 1, \cdots, g\}$.

Given an isogeny $\alpha : A \to B$, we define the pullback map $\alpha^* : \mathrm{Hom}(B, B^\vee) \to \mathrm{Hom}(A, A^\vee)$ by $\alpha^*(\lambda) = \alpha^\vee \circ \lambda \circ \alpha$. Then from the proof of Proposition 4.7(c), the chain $(*)$ of inclusions commutes with pullback. From now on, I will view elements of $\mathrm{NS}(A)$ sometimes as line bundles, and sometimes as a homomorphism $A \to A^\vee$.

Following [3, §16], we give a series of important results about polarizations based on the following theorem:

Theorem 4.8. *Let $\alpha : A \to B$ be a isogeny of degree not divisible by $\mathrm{char}\, k$, and let $\lambda \in \mathrm{NS}(A)$. Then $\lambda = \alpha^*(\mu)$ for some $\mu \in \mathrm{NS}(B)$ if and only if for all prime ℓ dividing $\deg \alpha$ (equivalently, for all prime $\ell \neq \mathrm{char}\, k$, there is a pairing $(-,-)$ in $\mathrm{Hom}(\Lambda^2 T_\ell B, \mathbb{Z}_\ell(1))$ such that $e_\ell^\lambda(a, a') = (\alpha(a), \alpha(a'))$ for all $a, a' \in T_\ell A$.*

We postpone the proof of this theorem to the end of this section, after giving its applications.

Corollary 4.9. *Let $\ell \neq \mathrm{char}\, k$. An element λ of $\mathrm{NS}(A)$ is divisible by ℓ^m if and only if e_ℓ^λ is divisible by ℓ^m in $\mathrm{Hom}(\Lambda^2 T_\ell B, \mathbb{Z}_\ell(1))$.*

Proof. Case $m = 2n$ is even:

Let α be the multiplicatin-by-ℓ^n map on A. To apply the theorem to α, note that the degree of ℓ^n is ℓ^{2gn}, which is not divisible by $\mathrm{char}\, k$, and we only need to test the prime ℓ in the theorem. Observing that $(\alpha(a), \alpha(a')) = (\ell^n a, \ell^n a') = \ell^{2n}(a, a')$ for any pairing on $T_\ell A$, it suffices to show that $(\ell^n)^*\lambda = \ell^{2n}\lambda$ on $\mathrm{Hom}(A, A^\vee)$. Indeed, for $\lambda : A \to A^\vee$, we have

$$\alpha^*\lambda = \alpha^\vee \circ \lambda \circ \alpha = \ell^n \circ \lambda \circ \ell^n = \ell^{2n}\lambda.$$

Case m is odd:

If e_ℓ^λ is divisible by ℓ^m, then $\ell e_\ell^\lambda = e_\ell^{\ell\lambda}$ is divisible by ℓ^{m+1}. By the even case, $\ell\lambda$ is divisible by ℓ^{m+1} in $\mathrm{NS}(A)$. But $\mathrm{NS}(A)$ is a free abelian group (see Corollary 2.22), in particular ℓ-torsion free. Thus λ is divisible by ℓ^m in $\mathrm{NS}(A)$.

□

We are ready to prove the statement at the beginning of this section.

Proposition 4.10. *Assume $\mathrm{char}\, k \neq 2$, and $\ell \neq \mathrm{char}\, k$. Then a homomorphism $\lambda : A \to A^\vee$ is in $\mathrm{NS}(A)$ if and only if e_ℓ^λ is alternating.*

Proof. Assume e_ℓ^λ is alternating. Construct $\mathcal{L}$ by the pullback of the Poincaré sheaf $\mathcal{P}$ by $(1, \lambda) : A \to A \times A^\vee$. We claim that:

(a) $\mathcal{L}$ is divisible by 2 in $\mathrm{NS}(A)$;

(b) $\lambda = \lambda_{\mathcal{L}/2}$.

We need the following lemma:

Lemma 4.11. *Let $\mathcal{P}$ be the Poincaré sheaf on $A \times A^\vee$, then*

$$e_\ell^{\mathbb{P}}((a, b), (a', b')) = e_\ell(a, b') - e_\ell(a', b)$$

for $a, a' \in T_\ell A$ and $b, b' \in T_\ell A^\vee$.

Proof. Since $\mathbb{Z}_\ell(1)$ is ℓ-torsion free, it suffices to prove the identity for b and b' in a subgroup of finite index in $T_\ell A^\vee$. Choose $\lambda = \lambda_{\mathcal{L}} \in \mathrm{Pol}(A)$, then $\det(T_\ell \lambda) = \deg(\lambda) \neq 0$, so the image of $T_\ell \lambda$ has finite index in $T_\ell A^\vee$. We can assume $b = \lambda c$ and $b' = \lambda c'$, where $c, c' \in T_\ell A$. Recall that $(1 \times \lambda)^*((P))$ is the Mumford bundle $\Lambda(\mathcal{L}) = m^*\mathcal{L} - p^*\mathcal{L} - q^*\mathcal{L}$ following Notation 1.10. Hence,

$$\begin{aligned}
e_\ell^{\mathcal{P}}((a,b),(a',b')) &= e_\ell^{\mathcal{P}}((1\times\lambda)(a,c),(1\times\lambda)(a',c')) \\
&= e_\ell^{\Lambda(\mathcal{L})}((a,c),(a',c')) && \text{(Proposition 4.7(c))} \\
&= e_\ell(a+c,a'+c') - e_\ell^{\mathcal{L}}(a,a') - e_\ell(c,c') && \text{(Proposition 4.7(e)(c))} \\
&= e_\ell^{\mathcal{L}}(a,c') - e_\ell^{\mathcal{L}}(a',c) && \text{(bilinearity)} \\
&= e_\ell(a,b') - e_\ell(a',b)
\end{aligned}$$

□

Back to the proof of Proposition 4.10.

We shall prove $2\lambda = \lambda_{\mathcal{L}}$ for $\mathcal{L} = (1\times\lambda)^*\mathcal{P}$. Since e_ℓ is nondegenerate, the following computation suffices:

$$\begin{aligned}
e_\ell(a,\lambda_{\mathcal{L}}(a')) = e_\ell(a,a') &= e_\ell^{\mathcal{P}}((a,\lambda a),(a',\lambda a')) && \text{(Proposition 4.7(c))} \\
&= e_\ell(a,\lambda a') - e_\ell(a',\lambda a) && \text{(by lemma)} \\
&= e_\ell^{\lambda}(a,a') - e_\ell^{\lambda}(a',a) \\
&= 2e_\ell^{\lambda}(a,a') && \text{(since } e_\ell^\lambda \text{ is alternating by hypothesis)} \\
&= e_\ell(a,2\lambda a')
\end{aligned}$$

Finally, since $2 \neq \operatorname{char} k$, the corollary above shows $\lambda_{\mathcal{L}}$ is divisible by 2 in $\mathrm{NS}(A)$, so both of the claims (a)(b) are proved.

□

The remaining of the section will give another independent application of Theorem 4.8, leading to the Zarhin's trick.

From now on, we require $\lambda \in \mathrm{Pol}(A)$. Since $\lambda : A \to A^\vee$ is now an isogeny, we have the generalized Weil pairing of λ given by $e_\lambda : \ker(\lambda) \times \ker(\lambda^\vee) \to k_s^\times$. Using the canonical identification $A \to A^{\vee\vee}$, $a \mapsto \mathcal{P}|_{a\times A^\vee} \in \mathrm{Pic}(A^\vee)$ (where $\mathcal{P}$ is the Poincaré sheaf), we may view $\lambda^\vee : A^{\vee\vee} \to A^\vee$ as a map $A \to A^\vee$. We make the following observation that any element of $\mathrm{NS}(A)$ is self-dual:

Lemma 4.12. *Under the canonical identification $A \cong A^{\vee\vee}$, we have $\lambda^\vee = \lambda$ as maps from A to $A^\vee$ if $\lambda = \lambda_{\mathcal{L}}$ is in* $\mathrm{NS}(A)$.

Proof. For $a \in A$, we have

$$\begin{aligned}
\lambda^\vee(a) &= \lambda^*\left(\mathcal{P}|_{a\times A^\vee}\right) \\
&= (x \mapsto (a,\lambda x))^*\mathcal{P} \\
&= (x \mapsto (a,x))^*(1\times\lambda)^*\mathcal{P} \\
&= \Lambda(\mathcal{L})|_{a\times A^\vee} \\
&= (m^*\mathcal{L} - p^*\mathcal{L} - q^*\mathcal{L})_{a\times A^\vee} \\
&= t_a^*(\mathcal{L}) - \mathcal{L} = \lambda_{\mathcal{L}}(a)
\end{aligned}$$

□

Hence we get a bilinear, nondegenerate and Galois equivariant pairing

$$e_\lambda : \ker(\lambda) \times \ker(\lambda) = \ker(\lambda) \times \ker(\lambda^\vee) \to k_s^\times$$

Remark. Milne uses e^λ for this, but this article prefers e_λ because (1) e_λ agrees with the notation of generalized Weil pairings; (2) e^λ has the potential to be confused with e_ℓ^λ, which is totally different.

We have an explicit formula to compute e_λ in terms of Weil pairing e_m. Let m kill $N := \ker(\lambda)$. Then the inclusion $N \hookrightarrow A[m]$ induces a homomorphism of Cartier duals $A^\vee[m] \to N^\vee$. There are two natural ways to define this morphism, and they yield the same map:

Lemma 4.13 (Naturality of dual exact sequence)**.** *Consider a map of exact sequences*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & A & \xrightarrow{f} & B & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \\ 0 & \longrightarrow & N' & \longrightarrow & A' & \xrightarrow{f'} & B' & \longrightarrow & 0 \end{array}$$

where f, f', α and β are all isogenies. Then the following diagram commutes:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Hom}(N, \mathbb{G}_m) & \longrightarrow & B^\vee & \xrightarrow{f^\vee} & A^\vee & \longrightarrow & 0 \\ & & {\scriptstyle \mathrm{Hom}(\alpha, \mathbb{G}_m)}\uparrow & & {\scriptstyle \beta^\vee}\uparrow & & {\scriptstyle \alpha^\vee}\uparrow & & \\ 0 & \longrightarrow & \mathrm{Hom}(N', \mathbb{G}_m)^\vee & \longrightarrow & B'^\vee & \xrightarrow{f'^\vee} & A' & \longrightarrow & 0 \end{array}$$

In other words, $\alpha : N \to N'$ and $\beta^\vee : \ker(f^\vee) \to \ker(f'^\vee)$ are adjoint with respect to generalized Weil parings:

$$\begin{array}{ccccccc} e_f : & N & \times & \ker(f^\vee) & \longrightarrow & \mathbb{G}_m \\ & \downarrow{\scriptstyle \alpha} & & {\scriptstyle \beta^\vee}\uparrow & & \downarrow{\scriptstyle id} \\ e_{f'} : & N' & \times & \ker(f'^\vee) & \longrightarrow & \mathbb{G}_m \end{array}$$

in the sense that for $a \in N, b' \in \ker(f'^\vee)$, we have

$$e_f(a, \beta^\vee(b')) = e_{f'}(\alpha(a), b')$$

Proof. The most inspiring part is to figure out how to state this result. The rest can be done by an easy exercise following the construction of dual exact sequence or by the principle of "what else it could be". □

Now we apply the naturality result to the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & A & \xrightarrow{\lambda} & A^\vee & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \alpha} & & \\ 0 & \longrightarrow & A[m] & \longrightarrow & A & \xrightarrow{m} & A & \longrightarrow & 0 \end{array}$$

where α is the unique map that makes the right hand side square commute, in light of the universal property of quotient group schemes.

We have $e_\lambda(a, \alpha^\vee b) = e_m(a, b)$ for $a \in N, b \in A^\vee[m]$. Note that $\lambda \circ \alpha^\vee = m$.

Write $a' = \alpha^\vee$ and pick $c \in A^\vee[m^2]$ such that $b = mc$. Let $d = \alpha^\vee(c)$, then $md = \alpha^\vee(mc) = a'$ and $\lambda d = \lambda\alpha^\vee(c) = mc = b$. Thus

$$e_\lambda(a, a') = e_m(a, b) = e_m(a, \lambda d)$$

for m that kills $\ker(\lambda)$ and a particular choice of $d \in A[m^2]$ such that $md = a'$.

In fact we can show the formula works as long as m kills a and a' and d is any element of A such that $md = a'$. It suffices to show the right hand side is independent of the choice of m and d.

Proposition 4.14. *Let $\lambda : A \to A^\vee$ be in $\mathrm{Pol}(A)$. Let $a, a' \in \ker(\lambda)$. Choose m to be an integer not divisible by $\mathrm{char}\, k$ that kills a and a', and choose b such that $mb = a'$. Then $e_m(a, \lambda b)$ is independent of the nonunique choices of m and b, and*

$$e_\lambda(a, a') = e_m(a, \lambda b).$$

Proof. For independence of b, suppose $mb = 0$, then $e_m(a, \lambda b) = e_m^\lambda(a, b)$ because now the right hand side makes sense! By skew symmetry, we have $e_m^\lambda(a, b) = -e_m^\lambda(b, a) = -e_m(b, \lambda a) = 0$ by the assumption that $a \in \ker(\lambda)$.

For independence of m, compare the choices m and mn. Choose b such that $mnb = a'$ and set $b' = nb$, then $mb' = a'$. Then the statement boils down to $e_m(a, \lambda nb) = e_{mn}(a, \lambda b)$, but this is Corollary 4.5. □

Remark (Caution). Note that $b \in A[m^2]$, but $m(\lambda b) = \lambda(mb) = \lambda a = 0$, so the Weil pairing above is still defined. However, we can rewrite $e_m(a, \lambda b)$ as $e_m^\lambda(a, b)$ only when $b \in A[m]$, not just when $\lambda b \in A^\vee[m]$. Otherwise, we can easily get a false proof that $e_\lambda(a, a') = 0$ for all $a, a' \in \ker(\lambda)$: choose $mb = a'$, then

$$e_\lambda(a, a') = e_m(a, \lambda b) = e_m^\lambda(a, b) = -e_m^\lambda(b, a) = -e_m(b, \lambda a) = 0.$$

Here the second equality is wrong and worse, the expressions after it are undefined.

Proposition 4.15. *The pairing $e_\lambda : \ker(\lambda) \times \ker(\lambda) \to k_s^\times$ is alternating.*

Proof. Let m kill $\ker(\lambda)$. For $a \in \ker(\lambda)$, we have

$$\begin{aligned} e_\lambda(a, a) &= e_m(a, \lambda b) \\ &= e_m(mb, \lambda b) \\ &= e_{m^2}(b, \lambda b) && \text{(Corollary 4.5)} \\ &= e_{m^2}^\lambda(b, b) && (b \in A[m^2]) \\ &= 0 && \text{(alternating)} \end{aligned}$$

□

Using this pairing, we get an ℓ-independent version of the criterion in Theorem 4.8 in the case where $\lambda \in \mathrm{Pol}(A)$.

Theorem 4.16. *Let $\alpha : A \to B$ be an isogeny of degree not divisible by $\mathrm{char}\, k$, and $\lambda : A \to A^\vee$ be in $\mathrm{Pol}(A)$. Then $\lambda = \alpha^*(\lambda')$ for some $\lambda' \in \mathrm{Pol}(B)$ if and only if $\ker(\alpha) \subseteq \ker(\lambda)$ and e_λ is trivial on $\ker(\alpha) \times \ker(\alpha)$. Moreover, if we assume further that λ is a polarization (i.e. $\lambda \in \mathrm{Pol}^0(A)$), then any such λ' is a polarization.*

Proof. To prove the forward direction, assume $\lambda = \alpha^\vee \circ \lambda' \circ \alpha$, then we get $\ker(\alpha) \subseteq \ker(\lambda)$. Moreover, for $a, a' \in \ker(\alpha)$, choosing m that kills $\ker(\lambda)$ and b such that $a' = mb$, we have

$$\begin{aligned} e_\lambda(a, a') &= e_m(a, \lambda b) = e_m(a, \alpha^\vee \lambda' \alpha(b)) \\ &= e_m(\alpha(a), \lambda' \alpha(b)) \\ &= 0 \qquad (a \in \ker(\alpha)) \end{aligned}$$

where one must be aware that $\lambda'\alpha(b) \in A^\vee[m]$ because $m\lambda'\alpha b = \lambda'\alpha(mb) = \lambda'(\alpha(a)) = 0$, so the second line is defined and adjointness can be applied.

For the backward direction, we observe that if $\lambda = \alpha^\vee \circ \lambda' \circ \alpha$ is an isogeny, then λ' must be an isogeny because both α and $\alpha^\vee$ are. Moreover, if λ is a polarization, then the index of λ is $i(\lambda) = 0$. As pullback does not change the index, we must have $i(\lambda') = 0$, and thus λ' is a polarization.

Hence it suffices to show that $\lambda = \alpha^*(\lambda)$ for some $\lambda \in \mathrm{NS}(B)$. Now the assumption and conclusion are both the same as Theorem 4.8, so we just neeed to construct an alternating pairing $(-,-)_\ell$ on $T_\ell B$ for each ℓ, such that $e_\ell^\lambda(a, a') = (\alpha(a), \alpha(a'))_\ell$ for $a, a' \in T_\ell A$.

Let $b, b' \in T_\ell B$. Since α is an isogeny, there is n and $a, a' \in T_\ell A$ such that $\ell^n b = f(a)$ and $\ell^n b' = f(a')$. We claim that

(a) The element $e_\ell^\lambda(a, a')$ is divisible by ℓ^{2n}.

(b) There is a well-defined pairing on $T_\ell B$ given by $(b, b')_\ell := \ell^{-2n} e_\ell^\lambda(a, a')$ and it does the job.

For an element x of some Tate module, we use x_i to denote its i-th component. Then the n-th component of $\ell^n b = f(a)$ reads $f(a_n) = \ell^n b_n = 0$ and similarly $f(a'_n) = 0$. By the hypothesis of the proposition, a_n, a'_n are killed by λ and $e_\lambda(a_n, a'_n) = 0$. Note that $a'_n = \ell^n a'_{2n}$, so the explicit description of λ shows

$$\begin{aligned} 0 = e_\lambda(a_n, a'_n) &= e_{\ell^n}(a_n, \lambda a'_{2n}) \\ &= e_{\ell^{2n}}(a_{2n}, \lambda a'_{2n}) \qquad \text{(Corollary 4.5)} \\ &= e^\lambda_{\ell^{2n}}(a_{2n}, a'_{2n}) \end{aligned}$$

Following the compatibility diagram

$$\begin{array}{rccccc} e_{\ell^{n+1}}: & A[\ell^{n+1}] & \times & A^\vee[\ell^{n+1}] & \longrightarrow & \mu_{\ell^{n+1}} \\ & \downarrow \ell & & \downarrow \ell & & \downarrow \ell \\ e_{\ell^n}: & A[\ell^n] & \times & A^\vee[\ell^n] & \longrightarrow & \mu_{\ell^n} \end{array}$$

we have $e_\ell^\lambda(a, a') = (e_{\ell^i}(a_i, a'_i)) = \ell^{2n} \left(e^\lambda_{\ell^{i+2n}}(a_{i+2n}, a'_{i+2n})\right)_i$, and the rightmost element $\left(e^\lambda_{\ell^{i+2n}}(a_{i+2n}, a'_{i+2n})\right)_i$ is defined in the Tate module because $\ell^i e^\lambda_{\ell^{i+2n}}(a_{i+2n}, a'_{i+2n}) = e^\lambda_{\ell^{2n}}(a_{2n}, a'_{2n}) = 0$. Thus $e_\ell^\lambda(a, a')$ is divisible by ℓ^{2n}, proving the claim (a).

Next, we check $(b, b')_\ell = \ell^{-2n} e_\ell^\lambda(a, a')$ is independent of the choice of n and a, a'. First we fix n, then by the requirement $\alpha(a') = \ell^n b$, different choices of a' differ by an element a'' of $\ker(\alpha)$. But $\ker(\alpha) \subseteq \ker(\lambda)$, so $\lambda a'' = 0$, and $e_\ell^\lambda(a, a'') = e_\ell(a, \lambda a'') = 0$. Since $\mathbb{Z}_\ell(1)$ is ℓ-torsion free, $(b, b')_\ell$ is independent of the choice of a'. By skew symmetry of the pairing e_ℓ^λ, $(b, b')_\ell$ is independent of a as well. Now we replace n by $n+1$, then we may replace a by ℓa and a' by $\ell a'$ (because we have proven the irrelevance of choices of a and a'). Then the defining expression of $(b, b')_\ell$, namely $\ell^{-2n} e_\ell^\lambda(a, a')$ is replaced by $\ell^{-2(n+1)} e_\ell^\lambda(\ell a, \ell a') = \ell^{-2n} e_\ell^\lambda(a, a')$, which is unchanged.

Hence we have constructed a pairing $(-,-)_\ell$ on $T_\ell B$. It remains to show aht $e_\ell^\lambda(a,a') = (\alpha(a),\alpha(a'))$ for $a,a' \in T_\ell A$. But for $b = \alpha(a), b' = \alpha(a')$, we can choose $n = 1$ and $a = a, a' = a'$, so $(\alpha(a),\alpha(a'))_\ell = \ell^0 e_\ell^\lambda(a,a') = e_\ell^\lambda(a,a')$.

□

Remark. Since $\alpha^*(\lambda') = \alpha^\vee \circ \lambda' \circ \alpha$, if A admits a polarization of degree d that satisfies the hypothesis of the theorem, then B admits a polarization of degree $d/(\deg\alpha)^2$.

Corollary 4.17. *Let A have a polarization of degree not divisble by* $\operatorname{char} k$*. Then A is isogenous to a principally polarized abelian variety.*

Proof. Let λ be a polarization of A. If $\deg\lambda = 1$, we are done. Otherwise let ℓ be a prime dividing $\deg\lambda$. Since ℓ is prime, there is a (necessarily cyclic) subgroup N of $\ker(\lambda)$ of order ℓ, and let $B = A/N$. Since e_λ is alternating, it must be zero on the cyclic group N. Apply the theorem to the quotient map $A \to A/N$, we see that B is isogenous to A and has a polarization of degree $\deg\lambda/\ell^2$. Repeat this process, then noting that the degree of a polarization is always a square, we can reach a principally polarized abelian variety isogenous to A. □

Theorem 4.18 (Zarhin's trick)**.** *Let A be an abelian variety over a field k of characteristic zero (or, if A has an polarization of degree not divisible by* $\operatorname{char} k$*). Then $(A \times A^\vee)^4$ admits a principal polarization.*

Remark. Mumford's theory of theta-groups can remove the characteristic restriction.

We need the next lemma.

Lemma 4.19. *Let λ be a polarization of A and assume* $\ker(\lambda)$ *is killed by m with m not divisible by* $\operatorname{char} k$*. If there is an element $\alpha \in \operatorname{End}(A)$ such that $\alpha(\ker(\lambda)) \subseteq \ker(\lambda)$ and $\alpha^\vee \circ \lambda \circ \alpha = -\lambda$ on $A[m^2]$, then $A \times A^\vee$ is principally polarized.*

Proof. Let $N = \{(a,\alpha(a)) : a \in \ker(\lambda)\}$, a finite subgroup of $A \times A$. Since $\alpha(\ker(\lambda)) \subseteq \ker(\lambda)$, so $\lambda\alpha\ker(\lambda) = 0$ and $(\lambda\times\lambda)(N) = \{(\lambda a, \lambda\alpha a) : a \in \ker(\lambda)\} = 0$. So $N \subseteq \ker(\lambda\times\lambda)$. Let us apply Theorem 4.16 to the isogeny $A \times A \to (A\times A)/N$ and the polarization $\lambda\times\lambda$ on $A\times A$. For $(a,\alpha a),(a',\alpha a') \in N$,

$$\begin{aligned}
e_{\lambda\times\lambda}((a,\alpha a),(a',\alpha a')) &= e_\lambda(a,a') + e_\lambda(\alpha a,\alpha a') && \text{(see the discussion below)}\\
&= e_m(a,\lambda b) + e_m(\alpha a,\lambda(\alpha b)) \text{ where } mb = a'\\
&= e_m(a,\lambda b) + e_m(a,\alpha^\vee\circ\lambda\circ\alpha(b)) && \text{(adjointness)}\\
&= e_m(a,\lambda b) + e_m(a,-\lambda b) && \text{(hypothesis of lemma)}\\
&= 0,
\end{aligned}$$

where the first equality comes from the linear isomorphism of Cartier duals:

$$\begin{aligned}
(\ker\lambda)^\vee \times (\ker\lambda)^\vee &\to \ker(\lambda\times\lambda)^\vee\\
(f,g) &\mapsto \Big((x,y)\mapsto f(x)+g(y) \in \mathbb{G}_m(k_s)\Big)
\end{aligned}$$

Hence we can apply the Theorem 4.16 to see that $(A\times A)/N$ admits a polarization of degree $\deg(\lambda\times\lambda)/|N|^2 = |\ker(\lambda)|^2/|\ker(\lambda)|^2 = 1$, i.e. $(A\times A)/N$ is principally polarized. Finally, the map $A\times A \to (A\times A)/N : (x,y) \mapsto (x, y+\alpha x)$ is onto with kernel $\{(x,y) \in A\times A : x \in \ker(\lambda), y+\alpha x = \alpha x\} = \ker(\lambda)\times 0$, so $(A\times A)/N$ is isomorphic to $A/\ker(\lambda)\times A \cong A^\vee \times A$.

□

Proof of Zarhin's trick. We try to apply the lemma to the polarized abelian variety (A^4, λ^4). Choose m as in the lemma and using the fact that every nonnegative integer is the sum of four squares, we can choose a, b, c, d such that $a^2 + b^2 + c^2 + d^2 = m^2 - 1$. Let α be the quarternion $a + bi + cj + dk$. If the standard real quarternion algebra $\mathbb{H}$ acts on itself via left multiplication, and we identify $\mathbb{H}$ with $\mathbb{R}^4$ via the standard basis $\{1, i, j, k\}$, then we get an algebra embedding that sends conjugation to matrix transposition.

$$\iota : \mathbb{H} \to M_4(\mathbb{R})$$
$$a + bi + cj + dk \mapsto \begin{bmatrix} a & -b & -c & -d \\ b & a & d & -c \\ c & -d & a & b \\ d & c & -b & a \end{bmatrix}$$

Now $\iota(\alpha) \in M_4(\mathbb{Z})$ can be viewed as a morphism in $\mathrm{End}(A^4)$ or $\mathrm{End}((A^4)^\vee)$. It "commutes" with λ^4 in the sense that $\lambda^4 \circ \alpha|_{A^4} = \alpha|_{(A^4)^\vee} \circ \lambda^4$ because λ^4 is a diagonal matrix whose entries commute with entries of α (namely, integers). Hence $\alpha(\ker(\lambda^4)) \subseteq \ker(\lambda^4)$.

Note that the dual morphism of $(a_{ij}) \in \mathrm{End}(A^n) = M_n(\mathrm{End}(A))$ is given by the dual transpose $(a_{ji}^\vee) \in M_n(\mathrm{End}(A^\vee))$. Thus $\alpha^\vee$ is the given by the integer matrix α^T, the transpose of α. We have

$$\alpha^\vee \circ \lambda^4 \circ \alpha = \alpha^T \lambda^4 \alpha = \lambda^4 \alpha^T \alpha = \lambda^4 \overline{\alpha} \alpha = \lambda^4 |\alpha|_{\mathbb{H}}^2 = \lambda^4 (a^2 + b^2 + c^2 + d^2),$$

where $\overline{\alpha}$ is the conjugate of α as a quarternion. Thus $\alpha^\vee \circ \lambda^4 \circ \alpha$ acts as $-\lambda^4$ on $A[m^2]$. □

Now we give the proof of Theorem 4.8 as an appendix of this section, following the quick approach in [3, §16] using étale cohomology.

Analogous to the singular cohomology in complex case, we have the following theorem. Define **ℓ-adic cohomologies** of a scheme X as $H^r(X, \mathbb{Z}_\ell) := \varprojlim_n H^r_{\text{ét}}(X, \mathbb{Z}/\ell^n\mathbb{Z})$, the latter being the étale cohomologies of constant sheaves. While the notation suggests, the ℓ-adic cohomology $H^r(X, \mathbb{Z}_\ell)$ is *not* the same as the étale cohomology of the constant sheaf $\mathbb{Z}_\ell$.

Theorem 4.20. *Let A be an abelian variety of dimension g over an algebraically closed field k, and $\ell \neq \mathrm{char}\, k$ a prime. Then*

(a) *There is a canonical isomorphism $H^1(A, \mathbb{Z}_\ell) \xrightarrow{\cong} \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell A, \mathbb{Z}_\ell)$.*

(b) *The cup product defines isomorphisms*

$$H^r(A, \mathbb{Z}_\ell) \cong \Lambda^r H^1(A, \mathbb{Z}_\ell)$$

In particular, $H^r(A, \mathbb{Z}_\ell)$ is a free $\mathbb{Z}_\ell$-module of rank $\binom{2g}{r}$ and $H^r(A, \mathbb{Z}_\ell)$ is canonically isomorphic to the space of alternating r-multilinear map $T_\ell A \times \cdots \times T_\ell A \to \mathbb{Z}_\ell$.

Proof of Theorem 4.8. Start with the exact sequence of étale sheaves

$$0 \to \mu_{\ell^n} \to \mathbb{G}_m \xrightarrow{\ell^n} \mathbb{G}_m \to 0.$$

Since $\mathrm{Pic}(A) = H^1_{\text{ét}}(A, \mathbb{G}_m)$, the long exact sequence of étale cohomologies gives rise to

$$0 \to \mathrm{Pic}(A)/\ell^n \mathrm{Pic}(A) \to H^2_{\text{ét}}(A, \mu_{\ell^n}) \to H^2_{\text{ét}}(A, \mathbb{G}_m)[\ell^n] \to 0.$$

Note that $\mathrm{Pic}^0(A)$ is divisible, so $\mathrm{Pic}(A)/\ell^n\mathrm{Pic}(A) = \mathrm{NS}(A)/\ell^n\mathrm{NS}(A)$. Now since $\mathrm{NS}(A)$ is a free abelian group, the inverse system $\mathrm{NS}(A)/\ell^{n+1}\mathrm{NS}(A) \xrightarrow{1} \mathrm{NS}(A)/\ell^n\mathrm{NS}(A)$ is surjective and have inverse limit $\mathrm{NS}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. By Mittag-Leffler criterion, the inverse limit sequence is still exact:

$$0 \to \mathrm{NS}(A) \otimes \mathbb{Z}_\ell \to H^2(A, \mathbb{Z}_\ell(1)) \to T_\ell H^2_{\text{ét}}(A, \mathbb{G}_m) \to 0.$$

Note that since k is algebraically closed, there is no Galois action on $\mathbb{Z}_\ell(1)$, so $\mathbb{Z}_\ell(1) \cong \mathbb{Z}_\ell$ as étale sheaves and we know the structure of $H^r(A, \mathbb{Z}_\ell(1))$ by the theorem above. Moreover, one can show that the arrow $\mathrm{NS}(A) \otimes \mathbb{Z}_\ell \to H^2(A, \mathbb{Z}_\ell(1))$ sends λ to $-e_\ell^\lambda$.

Back to the setting of Theorem 4.8. Assume $\alpha : A \to B$ is an isogeny of degree n not divisible by $\operatorname{char} k$, $\lambda \in \mathrm{NS}(A)$, and for all primes $\ell \neq \operatorname{char} k$, the image of λ in $H^2(A, \mathbb{Z}_\ell(1))$ lies in the image of $H^2(B, \mathbb{Z}_\ell(1)) \to H^2(A, \mathbb{Z}_\ell(1))$. We claim that λ comes from $\mathrm{NS}(B) \otimes \mathbb{Z}_\ell$ for *all* ℓ, including $\ell = \operatorname{char} k$.

For $\ell \neq \operatorname{char} k$, consider the diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{NS}(A) \otimes \mathbb{Z}_\ell & \longrightarrow & H^2(A, \mathbb{Z}_\ell(1)) & \longrightarrow & T_\ell H^2(A, \mathbb{G}_m) \\
 & & \uparrow & & \uparrow & & \uparrow \\
0 & \longrightarrow & \mathrm{NS}(B) \otimes \mathbb{Z}_\ell & \longrightarrow & H^2(B, \mathbb{Z}_\ell(1)) & \longrightarrow & T_\ell H^2(B, \mathbb{G}_m)
\end{array}$$

By Proposition 1.29, there exists an isogeny $\beta : B \to A$ such that $\alpha \circ \beta = n_A$ and $\beta \circ \alpha = n_B$. Hence all the vertical arrows in the diagram factor the multiplication-by-n map from both sides. Since $T_\ell H^2(A, \mathbb{G}_m)$ is torsion free (the T_ℓ construction always give a , the right-hand vertical arrow is injective. By diagram chasing, we can see that λ comes from $\mathrm{NS}(B) \otimes \mathbb{Z}_\ell$.

When ℓ does not divide n, every vertical arrow is an isomorphism because n is invertible in $\mathbb{Z}_\ell$. In particular this covers the case $\ell = \operatorname{char} k$ and shows that it suffices to test all ℓ dividing $n = \deg \alpha$.

Now the claim is proved. Finally, the proof is complete after the following lemma. □

Lemma 4.21. *Let $f : A \to B$ be a homomorphism of abelian groups, and $b \in B$ lies in the image of $f_\ell : A \otimes \mathbb{Z}_\ell \to B \otimes \mathbb{Z}_\ell$ for all primes ℓ. Then $b \in f(A)$.*

Proof. Let C be the cokernel of f, then we have an exact sequence

$$A \otimes \mathbb{Z}_\ell \to B \otimes \mathbb{Z}_\ell \to C \otimes \mathbb{Z}_\ell \to 0.$$

For all primes ℓ, we have a chain of flat morphisms $\mathbb{Z} \to \mathbb{Z}_{(\ell)} \to \mathbb{Z}_\ell$, where $\mathbb{Z}_{(\ell)}$ is the localization of $\mathbb{Z}$ at the maximal ideal (ℓ). Moreover the second map is faithfully flat. Now consider the subgroup M of C generated by the image of b in C, and we shall prove $M = 0$. We know that the image of $M \otimes \mathbb{Z}_\ell \to C \otimes \mathbb{Z}_\ell$ is 0 from the hypothesis. Since $\mathbb{Z}_\ell$ is flat over $\mathbb{Z}$, we have $M \otimes \mathbb{Z}_\ell \subseteq C \otimes \mathbb{Z}_\ell$, so $M \otimes \mathbb{Z}_\ell = 0$. As $\mathbb{Z}_\ell$ is faithfully flat over $\mathbb{Z}_{(\ell)}$, we have $M \otimes \mathbb{Z}_{(\ell)} = 0$. This is true for all maximal ideals (ℓ) of $\mathbb{Z}$, and hence $M = 0$. □

4.2 The Rosati Involution

On an elliptic curve E, for an isogeny $\alpha : E \to E$, we can view its dual isogeny $\alpha^\dagger$ as an endomorphism of E (instead of $E^\vee$) via the canonical principal polarization $E \cong E^\vee$. We know

(a) $\dagger$ is an involution on $\mathrm{End}(E)$: $\alpha^{\dagger\dagger} = \alpha$.

(b) $\dagger$ is anti-multiplicative: $(\alpha\beta)^\dagger = \beta^\dagger\alpha^\dagger$.

(c) $\alpha^\dagger\alpha = \alpha\alpha^\dagger = \deg(\alpha)$. In particular, $\alpha^\dagger\alpha$ is a nonnegative integer.

(d) $\alpha + \alpha^\dagger = \mathrm{tr}(\alpha)$, which is an integer.

The existence of such an involution on $\mathrm{End}(E)$ gives lots of information about this algebra (for example, $\mathrm{End}(E)$ can be embedded into a positive-definite quarternion algebra over $\mathbb{Q}$), and one can reduce problems about trace, degree and characteristic polynomial to linear algebra problems in $\mathrm{End}(E)$. This is the key to prove the Riemann hypothesis for elliptic curves over finite fields.

However, for abelian varieties of higher dimension, there are two difficulties. First, there is no canonical polarization, and there may not exist a principal polarization. Second, the properties (c)(d) no longer holds, and we need a more subtle statement of positive definiteness.

Fix a polarization λ on A. As λ is an isogeny, it has an inverse in $\mathrm{Hom}^0(A^\vee, A) := \mathrm{Hom}(A^\vee, A)\otimes_{\mathbb{Z}} \mathbb{Q}$.

Definition 4.22. The **Rosati involution** corresponding to a polariztion λ is given by

$$\dagger : \mathrm{End}^0(A) \to \mathrm{End}^0(A), \alpha \mapsto \alpha^\dagger := \lambda^{-1} \circ \alpha^\vee \circ \lambda$$

The Rosati involution is anti-multiplicative: $\beta^\dagger\alpha^\dagger = \lambda^{-1}\beta^\vee\lambda \circ \lambda^{-1}\alpha^\vee\lambda = \lambda^{-1}(\alpha\beta)^\vee\lambda = (\alpha\beta)^\dagger$. Moreover, it is indeed an involution:

$$\alpha^{\dagger\dagger} = \lambda^{-1}(\lambda^{-1}\alpha^\vee\lambda)^\vee\lambda = \lambda^{-1}\lambda^\vee\alpha(\lambda^{-1})^\vee\lambda = \alpha$$

where the last equality is because any polarization is self dual by Lemma 4.12.

Proposition 4.23. *Assume $k = \overline{k}$, and fix a polarization λ on A. Then the map*

$$\mathrm{NS}^0(A) := \mathrm{NS}(A) \times \mathbb{Q} \to \mathrm{End}^0(A) : \mathcal{L} \mapsto \lambda^{-1}\lambda_{\mathcal{L}}$$

identifies $\mathrm{NS}^0(A)$ *with* $\mathrm{End}^0(A)^\dagger$*, the subset of elements of* $\mathrm{End}^0(A)$ *fixed by* $\dagger$*.*

Proof. Let $\alpha \in \mathrm{End}^0(A)$ and $\ell \neq \mathrm{char}\, k$. By Proposition 4.10, we have $\alpha = \lambda^{-1} \circ \lambda_{\mathcal{L}}$ for some $\mathcal{L} \in \mathrm{NS}^0(A)$ if and only if $e_\ell^{\lambda\circ\alpha}$ is alternating on $T_\ell A \otimes \mathbb{Q}$. (Note that we no longer require $\mathrm{char}\, k \neq 2$ in this rational version of Proposition 4.10 because in the proof, division by 2 is no longer an issue.) Now $e_\ell^{\lambda\circ\alpha}(a', a) = e_\ell(a', \lambda \circ \alpha(a))$ and

$$\begin{aligned} e_\ell^{\lambda\circ\alpha}(a, a') &= e_\ell^{\lambda}(a, \alpha a') \\ &= -e_\ell^{\lambda}(\alpha a', a) && \text{(as } \lambda \text{ is a polarization)} \\ &= -e_\ell(a', \alpha^\vee \circ \lambda(a)) && \text{(adjointness)} \end{aligned}$$

By nondegenercy of Weil pairing, the alternating criterion is equivalent to $\lambda \circ \alpha = \alpha^\vee \circ \lambda$, i.e. $\alpha = \alpha^\dagger$. □

The following is the positivity result analogous to (c) at the beginning of the section.

Theorem 4.24. *The bilinear form* $\mathrm{End}^0(A) \times \mathrm{End}^0(A) \to \mathbb{Q}$ *defined by* $(\alpha, \beta) = \mathrm{tr}(\alpha\beta^\dagger)|_{V_\ell A}$ *is positive definite.*

Proof. The proof uses intersection theory, see [3, §17]. The ampleness of the line bundle inducing the polarization plays a major role here. □

Corollary 4.25. *The group of automorphisms of a polarized abelian variety (A, λ) is finite.*

Proof. The automorphism group is $\{\alpha \in \mathrm{End}(A) : \lambda = \alpha^*(\lambda) = \alpha^\vee \lambda \alpha\} = \{\alpha \in \mathrm{End}(A) : \alpha^\dagger \alpha = 1\} \subseteq \mathrm{End}(A) \cap \{\alpha \in \mathrm{End}(A) \otimes \mathbb{R} : \mathrm{tr}(\alpha^\dagger \alpha) = 2g\}$. By the positive definiteness of the bilinear form in the theorem, $\{\alpha \in \mathrm{End}(A) \otimes \mathbb{R} : \mathrm{tr}(\alpha^\dagger \alpha) = 2g\}$ is homeomorphic to a sphere S^{2g-1}! Since $\mathrm{End}(A)$ is a discrete lattice in $\mathrm{End}(A) \otimes \mathbb{R}$, its intersection with any compact subset is finite. □

Corollary 4.26. *An endomorphism $\alpha \in \mathrm{End}^0(A)$ is called **normal** with respect to a Rosati involution $\dagger$ if $\alpha^\dagger \alpha = \alpha \alpha^\dagger$. Then the endomorphism algebra $\mathrm{End}^0(A)$ has no nonzero nilpotent that is normal.*

Proof. We have a simple proof when A is an elliptic curve. For any $\alpha \neq 0$ in $\mathrm{End}^0(A)$, we have $\deg(\alpha) > 0$, so $\deg(\alpha^n) > 0$ for all $n > 0$. In particular, $\alpha^n \neq 0$. (Note that $\alpha\alpha^\dagger = \alpha^\dagger \alpha = \deg(\alpha)$, so the normality condition is automatic and we proved nothing stronger than the statement of this corollary.)

In general, we need to use the theorem. Say $\alpha \in \mathrm{End}^0(A)$ is nonzero and normal. Set $\beta = \alpha\alpha^\dagger$, then $\mathrm{tr}(\beta)|_{V_\ell A} > 0$, so $\beta \neq 0$. Note that $\beta^\dagger = \dagger$, so $\mathrm{tr}(\beta^2)|_{V_\ell A} = \mathrm{tr}(\beta\beta^\dagger)|_{V_\ell A} > 0$, and $\beta^2 \neq 0$. As $(\beta^2)^\dagger = \beta^2$, we can repeat this argument to get $\beta^4 \neq 0$, and so on. Therefore, β is not nilpotent.

Finally, since α commutes with $\alpha^\dagger$, for any $n > 0$,

$$0 \neq \beta^n = (\alpha\alpha^\dagger)^n = \alpha^n (\alpha^\dagger)^n,$$

so that $\alpha^n \neq 0$. □

Remark. If $\alpha \in \mathrm{End}^0(A)$ is invertible and $\zeta = \alpha\beta$ lies in the center of $\mathrm{End}^0(A)$, then α automatically commutes with β. To see this, we have $\alpha\beta\alpha = \zeta\alpha = \alpha\zeta = \alpha(\alpha\beta)$. As α is invertible, we can multiply both sides by α^{-1} at the left, and we get $\beta\alpha = \alpha\beta$.

As an application of Rosati involution, we prove the Riemann hypothesis in Theorem 3.18.

Theorem 4.27. *Let $k = \mathbb{F}_q$ be the finite field of q elements, A an abelian variety over k, and π the Frobenius map on A_{k_s}. Then all eigenvalues of π on $V_\ell A$ have norm $q^{1/2}$.*

For the purpose of a proof, we fix a polarization λ of A given by an ample line bundle $\mathcal{L}$ defined over k.

Lemma 4.28. $\pi^\dagger \circ \pi = q$.

Proof. We claim that for any line bundle $\mathcal{M}$ on A defined over k, we have $\pi^*\mathcal{M} \cong \mathcal{M}^{\otimes q}$. We view the line bundle $\mathcal{M}$ on the k-variety A, instead of a Galois invariant line bundle on $A_{\overline{k}}$. Then $\pi : A \to A$ is the absolute Frobenius map that gives identity map on underlying topology and induces the map $\pi^\sharp : f \mapsto f^q$ on rings of functions. Let $A = \cup_i U_i$ be a trivialization of $\mathcal{M}$ with system of transition functions (φ_{ij}). Then $\pi^*\mathcal{M}$ is given by the trivialization $\pi^{-1}(U_i) = U_i$ and transition function $(\pi^\sharp \varphi_{ij}) = (\varphi_{ij}^q)$. Hence $\pi^*\mathcal{M} \cong \mathcal{M}^{\otimes q}$.

Now, to prove $\pi^\dagger \circ \pi = q$, it suffices to show $\pi^\vee \lambda_{\mathcal{L}} \pi = q\lambda_{\mathcal{L}}$. Indeed

$$\pi^\vee \lambda_{\mathcal{L}} \pi = \lambda_{\pi^*\mathcal{L}} = \lambda_{q\mathcal{L}} = q\lambda_{\mathcal{L}}$$

because $\mathcal{L}$ is defined over k. □

Proof of Theorem 4.27. Multiplying the lemma by π^{-1} at the right, we get $\pi^\dagger = q\pi^{-1}$. Consider the subalgebra $R = \mathbb{Q}[\pi]$ in $\mathrm{End}^0(A)$, then R is a finitely dimension commutative algebra over $\mathbb{Q}$. In particular there is a $\mathbb{Q}$-polynomial $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$ such that $f(\pi) = 0$. As π is invertible in $\mathrm{End}^0(A)$, we can assume $c_0 \neq 0$ so that $\pi(\pi^{n-1} + \cdots + c_1) = -c_0$. Multiply by π^{-1} at the left, and we have $\pi^{-1} = -c_0^{-1}(\pi^{n-1} + \cdots + c_1) \in R$. Thus $\pi^\dagger = q\pi^{-1} \in R$. Hence, $\dagger$ is an involution of R as a $\mathbb{Q}$-algebra.

For all $\alpha \in R$, we have $\alpha^\dagger \in R$ and it commutes with α (because R is commutative). From the corollary above, R has no nonzero nilpotent. Since $\mathbb{Q}$ is perfect, $S := R \otimes_{\mathbb{Q}} \mathbb{R}$ is reduced. By the structure theorem of reduced Artin algebras over a field, we have

$$S = K_1 \times \cdots \times K_m$$

where K_i are finite field extensions of $\mathbb{R}$ (which must be $\mathbb{R}$ or $\mathbb{C}$).

Now $\dagger$ is an involution of S such that $\alpha^\dagger\alpha \neq 0$ for $\alpha \neq 0$. Any automorphism of S permutes the factors $K_1, ..., K_m$ via isomorphisms. If $\dagger$ permutes the factors nontrivially, say $\dagger(K_1) = K_2$, then for $\alpha := (1, 0, ..., 0) \in K_1 \times \cdots \times K_m$ will have $\alpha^\dagger = (0, 1, 0, ..., 0)$ and $\alpha^\dagger\alpha = 0$, a contradiction. Hence $\dagger$ is of the form

$$\dagger(x_1, ..., x_m) = (\tau_1(x_1), ..., \tau_m(x_m))$$

where $\tau_i : K_i \to K_i$ is a field automorphism of order at most 2. When $K_i \cong \mathbb{C}$, I claim that τ_i must be complex conjugation, because we require $\mathrm{tr}(x_i\tau(x_i)) = 2Re(x_i\tau(x_i)) \geq 0$ for $x_i \in \mathbb{C}$, but when $\tau = id$, $Re(x_i^2)$ will be negative for some x_i.

Now assume $\pi = (a_1, ..., a_m)$, then $\pi^\dagger\pi = q$ implies $|a_i|^2 = a_i\tau(a_i) = q$ for all i. Consider the action of π on S as an $\mathbb{R}$-vector space. Then π acts as multiplication by a_i on K_i. If $K_i \cong \mathbb{C}$, then a_i acts on $\mathbb{C}$ as a dilation by $|a_i|$ followed by a rotation. So all eigenvalues of π on $S = R \otimes_{\mathbb{Q}} \mathbb{R}$ (which is the same as eigenvalues of π on R) have norm $|a_i| = q^{1/2}$. Finally the proof is complete after [1, I.10.24]. □

4.3 Finiteness Results

In this section, the ground field k is no longer algebraically closed. For an abelian variety A over k, a **polarization defined over** k is a k-morphism $\lambda : A \to A^\vee$ that extends to a polarization $\lambda_{k_s} : A_{k_s} \to A^\vee_{k_s}$ given by an ample line bundle on A_{k_s}. One must be cautious that λ may not come from an ample line bundle defined over k. Indeed λ_{k_s} lies in $\mathrm{NS}(A_{k_s})$ and is fixed by $G = \mathrm{Gal}(k_s/k)$, but there is an obstruction to lift it to a line bundle in $\mathrm{Pic}(A)$. Consider the short exact sequence of G-modules

$$0 \to A^\vee(k_s) \to \mathrm{Pic}(A_{k_s}) \to \mathrm{NS}(A_{k_s}) \to 0$$

and taking long exact sequence of profinite group cohomologies, we get

$$0 \to A^\vee(k) \to \mathrm{Pic}(A) \to \mathrm{NS}(A_{k_s})^G \to H^1(G, A^\vee(k_s)).$$

In general the obstruction $H^1(G, A^\vee)$ may not be zero, but a theorem of Lang, 1956 states that $H^1(k, B) = 0$ for finite field k and B a connected algebraic group over k. Hence any polarization of an abelian variety over a finite field k is defined by a line bundle over k.

One importance about polarizations is that polarized abelian varieties of a fixed dimension and fixed (polarization) degree form a moduli space. If we think of it as a variety over a field, then we have the following theorem:

Theorem 4.29. *Let k be a finite field and fix $g, d > 0$. Up to isomorphism, there are only finitely many polarized abelian varieties (A, λ) over k of dimension g and degree d.*

Of course, to formulate and prove the existence of moduli is much harder than a direct proof of the theorem, but the idea of moduli provides a guideline to expect what finiteness results are true.

The proof of this theorem is a combination of the two following results:

Theorem 4.30. *Let k be a finite field and fix $g, d > 0$. Up to isomorphism, there are only finitely many abelian varieties A over k of dimension g that admit a polarization of degree d^2.*

Sketch of Proof. Suppose A/k has dimension g and has a polarization $\lambda = \lambda_{\mathcal{L}}$ of degree d^2. By the discussion above, $\mathcal{L}$ can be chosen to be defined over k. By [5, p.163], $\mathcal{M} = 3\mathcal{L}$ is very ample. By Theorem 1.44, we have $\chi(\mathcal{L}) = d$ and the top intersection power is $(\mathcal{L}^g) = \chi(\mathcal{L})g! = dg!$. As intersection product is multilinear, we get $(\mathcal{M}^g) = 3^g dg!$, so $\chi(\mathcal{M}) = (\mathcal{L}^g)/g! = 3^g d$. Since the cohomology of $\mathcal{M}$ is concentrated at degree 0, we have $h^0(A, \mathcal{M}) = 3^g d$, thus $\mathcal{M}$ induces an embedding $i : A \hookrightarrow \mathbb{P}^{3^g d-1}$. Moreover, the degree of $i(A)$ is given by $(\mathcal{O}(1)^g \cdot \mathcal{O}_{i(A)}) = (\mathcal{O}(1)^g|_{i(A)}) = (\mathcal{M}^g) = 3^g dg!$. By the theory of Cayley-Chow form, for any g, N and finite field k, there are only finitely many g-dimensional subvarieties of $\mathbb{P}^N_k$ of a fixed degree. Finally, any variety has at most one abelian variety structure by rigidity, and we are done. □

Theorem 4.31. *Fix an abelian variety A over any field k and integer $d > 0$. Then there are only finitely many isomorphism classes of polarized abelian variety (A, λ) over k of degree d.*

Proof. Two polarizations λ, λ' define isomorphic polarized abelian varieties if they are related by an automorphism u of A: $\lambda' = u^\vee \lambda u$. Fix a polarization λ_0 and use the Rosati involution with respect to it, then the relation can be rewritten as $\lambda_0^{-1}\lambda' = u^\dagger(\lambda_0^{-1}\lambda)u$. Thus $\lambda_0^{-1}\lambda$ and $\lambda_0^{-1}\lambda'$ lie in the same orbit of the $\mathrm{End}(A)^\times$-action on $\mathrm{End}^0(A)$ given by $x \mapsto u^\dagger x u$. The question reduces to the study of $\mathrm{End}^0(A)$, a finite dimensional $\mathbb{Q}$-algebra with an involution, which can be addressed by some theory of algebraic groups, see [3, §18]. □

We have another result obtained from studying the endomorphism algebra.

Theorem 4.32. *Up to isomorphism, an abelian variety A has only finitely many direct factors.*

Proof. Two direct factors B, B' are said to be isomorphic if there is an automorphism u of A such that $u(B) = B'$. Two direct decompositions $A = B + C = B' + C'$ are isomorphic if there is an automorphism u of A such that $u(B) = B'$ and $u(C) = C'$. Clearly it suffices to show that there are finitely many direct decompositions up to isomorphism.

A direct decomposition $A = B + C$ is in one-to-one correspondence to an idempotent e of $\mathrm{End}(A)$ given by projection $A \to B \hookrightarrow A$. It is easy to see that two idempotents e, e' give isomorphic direct decomposition if and only if there is $u \in \mathrm{End}(A)^\times$ such that $e' = ueu^{-1}$. So the question reduces to showing there are only finitely many such orbits of idempotents. The tool used is again the same theory of algebraic groups as above, see [3, §18]. □

We get our first result whose statement is not related to polarization.

Corollary 4.33. *There are only finitely many abelian varieties of dimension g over a finite field k.*

Proof. Let A be an abelian variety of dimension g over k. By Zarhin's trick, $(A \times A^\vee)^4$ is a principally polarized abelian variety of dimension $8g$ which contains A as a direct factor. Up to isomorphism, there are only finitely many such abelian varieties, and each of them has only finitely many direct factors. □

References

[1] James S. Milne, *Abelian Varieties (v2.00)*. 2008, Available at http://www.jmilne.org/math/

[2] James S. Milne, *Algebraic Geometry (v6.01)*. 2015, Available at http://www.jmilne.org/math/

[3] James S. Milne, *Chapter V: Abelian Varieties*. 1986, Available at http://www.jmilne.org/math/articles/1986b.pdf

[4] Ravi Vakil, *MATH 216: Foundations of Algebraic Geometry*. Dec.29,2015, Available at http://math.stanford.edu/%7vakil/216blog/

[5] David Mumford, *Abelian Varieties*. 1970, Oxford University Press

[6] Jürgen Neukirch, *Algebraic Number Theory*. 1999, Springer-Verlag Berlin Heidelberg

[7] Serge Lang, *Abelian Varieties*. 1959, Springer-Verlag New York