ABELIAN VARIETIES

BRYDEN CAIS

A canonical reference for the subject is Mumford's book [6], but Mumford generally works over an algebraically closed field (though his arguments can be modified to give results over an arbitrary base field). Milne's article [4] is also a good source and allows a general base field. These notes borrow heavily from van der Geer and Moonen [5], and differ in the main from [6] and [4] in that we give a more natural approach to the theory of the dual abelian variety.

1. Basic properties of abelian varieties

Let k be a field. A *k-variety* is a geometrically integral separated k-scheme of finite type.

1.1. Definitions.

Definition 1.2. A *group scheme* over k is a k-scheme X equipped with k-morphisms $m : X \times X \to X$, $i : X \to X$, and $e : \operatorname{Spec} k \to X$ such that for every k-scheme T, the morphisms m, i, e give $X(T)$ the structure of a group, and induce composition, inversion, and the identity, respectively. If X is a k-variety as well, we call it a *group variety.*

This definition is equivalent to the usual one in terms of the commutativity of certain diagrams by Yoneda's lemma. We remark that when X is geometrically reduced and locally of finite type over k, it suffices to check such diagrams commute on $\overline{k}$-points of X, since $X(\overline{k})$ is dense in the reduced scheme $X_{\overline{k}}$.

Definition 1.3. Let X be a group scheme over k. For any k-scheme T and any point $x \in X(T)$, we define *right translation by x* to be the morphism

$$t_x : X_T \simeq X_T \times_T T \xrightarrow{\mathrm{id}_{X_T} \times x_T} X_T \times_T X_T \xrightarrow{m} X_T,$$

where x_T is the morphism $x_T : T \xrightarrow{x \times \mathrm{id}_T} X \times T = X_T$.

For a T-scheme T' and a T'-point y, we have $t_x(y) = m(y, x)$ in $X(T')$.

Proposition 1.4. *A geometrically reduced k-group scheme X locally of finite type is k-smooth.*

Proof. The subset X^{sm} of k-smooth points is open and dense. Since $(X^{\mathrm{sm}})_{\overline{k}} = (X_{\overline{k}})^{\mathrm{sm}}$ is stable under all translations by $\overline{k}$-points, we conclude that $X_{\overline{k}} = (X_{\overline{k}})^{\mathrm{sm}} = (X^{\mathrm{sm}})_{\overline{k}}$, so $X = X^{\mathrm{sm}}$. ∎

Definition 1.5. An *abelian variety* is a proper group variety.

It follows from Proposition 1.4 that an abelian variety is smooth.

Lemma 1.6. *Let X, Y, Z be k-varieties with X proper over k. If $f : X \times Y \to Z$ is a k-morphism such that $f(X \times \{y\}) = \{z\}$ for some $y \in Y(k)$ and $z \in Z(k)$, then f uniquely factors through $\mathrm{pr}_Y : X \times Y \to Y$.*

Proof. By Galois descent, we can assume $k = k^{\mathrm{sep}}$. Thus, since X is a k-variety (and hence generically k-smooth) with k separably closed, $X(k) \neq \emptyset$. Choose $x \in X(k)$ and define

$$F : Y \xrightarrow{x \times \mathrm{id}} X \times Y \xrightarrow{f} Z.$$

It is necessary and sufficient to show that $f = F \circ \mathrm{pr}_Y$. To check this, we may extend the base field to $\overline{k}$, and thus may assume that k is algebraically closed.

Let U be an affine neighborhood of z and define $V = \mathrm{pr}_Y(f^{-1}(Z - U))$. Since X is proper, pr_Y is a closed map, so V is closed in Y. If P is a k-point of Y not contained in V, then $f(X \times \{P\}) \subset U$ by construction, and since

---

Date: December 17, 2004.
Many thanks go to Brian Conrad, who reviewed innumerable drafts and greatly improved the final version of these notes.

X is proper and U is affine, $f(X \times \{P\})$ is a single point, so $f(X \times \{P\}) = F(P)$. It follows that $F \circ \mathrm{pr}_Y = f$ on $X \times (Y - V)$. Since y is a k-point of $Y - V$, we see that $Y - V$ is nonempty (hence dense in Y since Y is irreducible). Thus, since Z is separated, $F \circ \mathrm{pr}_Y = f$ on all of $X \times Y$. ■

Corollary 1.7. *Every k-morphism $f : X \to Y$ of abelian varieties over k factors as the composition of a homomorphism and a translation: $f = t_{f(e_X)} \circ h$.*

Proof. Let $f : X \to Y$ be a k-morphism of abelian varieties over k and define $h = t_{i_Y(f(e_X))} \circ f$, so $h(e_X) = e_Y$. We claim that h is a homomorphism. To verify this, we must show that the morphisms

$$\varphi : X \times X \xrightarrow{h \times h} Y \times Y \xrightarrow{m_Y} Y$$

$$\psi : X \times X \xrightarrow{m_X} X \xrightarrow{h} Y$$

agree. But it is easy to see that the composite $\xi : X \times X \xrightarrow{\psi \times (i_Y \circ \varphi)} Y \times Y \xrightarrow{m_Y} Y$ satisfies

$$\xi(X \times \{e_X\}) = \xi(\{e_X\} \times X) = \{e_Y\}$$

and hence factors through both projections $X \times X \rightrightarrows X$. Therefore, ξ is the constant map with image $\{e_Y\}$ and $\varphi = \psi$. ■

Corollary 1.8. *The group structure on an abelian variety X is commutative, and is uniquely determined by the point $e \in X(k)$.*

Proof. The morphism $i : X \to X$ satisfies $i(e) = e$, so $i = t_{i(e)} \circ h = h$ for a homomorphism h. Since inversion is a homomorphism on T-points for all k-schemes T, the group structure on X is commutative. If (X, m, i, e) and (X, m', i', e) are two structures of an abelian variety on X (which we distinguish by writing X, X' respectively) then $\mathrm{id}_X : X \to X'$ preserves e and is therefore a homomorphism by Corollary 1.7, so $m = m'$ and $e = e'$. ■

In view of Corollary 1.8, we will often write $x + y$, $-x$, and 0 for $m(x, y)$, $i(x)$, and e respectively.

1.9. **Theorems of the cube and square.** Throughout, we will need a method to prove that certain invertible sheaves are trivial. This is a property that may be checked over an algebraic closure of the ground field, as the following proposition shows.

Proposition 1.10. *Let X/k be a proper variety and K/k any extension of fields. If $\mathscr{L}$ is an invertible sheaf on X that is trivial when pulled back to X_K, it is trivial on X.*

Proof. Since X is a proper k-variety, the natural map $k \to H^0(X, \mathscr{O}_X)$ is an isomorphism. Thus, an invertible sheaf $\mathscr{L}$ on X is trivial if and only if the natural map $H^0(X, \mathscr{L}) \otimes_k \mathscr{O}_X \to \mathscr{L}$ is an isomorphism. The formation of this map of quasi-coherent sheaves is compatible with the flat extension of scalars $k \to K$ that preserves the hypotheses, so we are done.

■

Lemma 1.11. *Let X, Y be complete varieties and let Z be a geometrically connected k-scheme of finite type. If x, y, z are k-points of X, Y, Z such that the restrictions of $\mathscr{L}$ to $\{x\} \times Y \times Z$, $X \times \{y\} \times Z$, and $X \times Y \times \{z\}$ are trivial, then $\mathscr{L}$ is trivial.*

Proof. Let $f : X \times Y \times Z \to Z$ be the structure map, so $\mathscr{O}_Z \to f_* \mathscr{O}_{X \times Y \times Z}$ is an isomorphism since $X \times Y$ is geometrically integral and proper over k. Hence, $\mathscr{L}$ is trivial if and only if $f_* \mathscr{L}$ is invertible and the canonical map $\theta : f^* f_* \mathscr{L} \to \mathscr{L}$ is an isomorphism. The formation of the coherent sheaf $f_* \mathscr{L}$ commutes with extension of the base field, and to check it is invertible it suffices to assume $k = \overline{k}$. Likewise, the formation of the map θ commutes with extension of the base field, and to check that θ is an isomorphism it suffices to check after extension of scalars by an algebraic closure of k. Thus we may assume that k is algebraically closed. The result now follows from [6, pg. 91]. ■

Let X be an abelian variety. For each subset I of $\{1, 2, \ldots, n\}$ let $p_I = p_{i_1 i_2, \ldots i_{\# I}} : X^n \to X$ be the morphism sending $(x_1, \ldots, x_n)$ to $\sum_{i \in I} x_i$.

Theorem 1.12 (Theorem of the cube)**.** *Let $\mathscr{L}$ be an invertible sheaf on an abelian variety X. Then*

$$\Theta(\mathscr{L}) := \bigotimes_{\emptyset \neq I \subset \{1,2,3\}} p_I^* \mathscr{L}^{(-1)^{\# I+1}} = p_{123}^* \mathscr{L} \otimes p_{12}^* \mathscr{L}^{-1} \otimes p_{13}^* \mathscr{L}^{-1} \otimes p_{23}^* \mathscr{L}^{-1} \otimes p_1^* \mathscr{L} \otimes p_3^* \mathscr{L} \otimes p_3^* \mathscr{L}$$

is trivial on $X \times X \times X$.

Proof. The restriction of $\Theta(\mathscr{L})$ to $\{0\} \times X \times X$ is

$$m^* \mathscr{L} \otimes p_2^* \mathscr{L}^{-1} \otimes p_3^* \mathscr{L}^{-1} \otimes m^* \mathscr{L}^{-1} \otimes \mathscr{O}_{X \times X} \otimes p_2^* \mathscr{L} \otimes p_3^* \mathscr{L} = \mathscr{O}_{X \times X}.$$

Similarly, the restrictions to $X \times \{0\} \times X$ and $X \times X \times \{0\}$ are also trivial, and the theorem follows from Lemma 1.11. ■

Remark 1.13. A closer inspection of the proof of Theorem 1.12 shows that the *canonical* trivialization of $\Theta(\mathscr{L})$ along the 0-sections of the factors are compatible along $(0,0)$-sections of pairs of factors, and consequently (by the proof of Lemma 1.11) $\Theta(\mathscr{L})$ is *canonically* trivial on $X \times X \times X$. We will not use this, but it shows that the isomorphisms in Corollaries 1.14–1.17 are canonical.

Corollary 1.14. *Let Y be any k-scheme and X an abelian variety over k. If $f, g, h : Y \to X$ are k-morphisms and $\mathscr{L}$ is an invertible sheaf on X then*

$$(f+g+h)^* \mathscr{L} \otimes (f+g)^* \mathscr{L}^{-1} \otimes (f+h)^* \mathscr{L}^{-1} \otimes (g+h)^* \mathscr{L}^{-1} \otimes f^* \mathscr{L} \otimes g^* \mathscr{L} \otimes h^* \mathscr{L}$$

is trivial on Y.

Proof. The pullback along $(f,g,h) : Y \to X \times X \times X$ of the trivial sheaf $\Theta(\mathscr{L})$ on $X \times X \times X$ is clearly trivial; it is also the sheaf on Y above. ■

Corollary 1.15 (Theorem of the square)**.** *Let X be an abelian variety and $\mathscr{L}$ an invertible sheaf on X. Choose a k-scheme T and $x, y \in X(T)$, and let $\mathscr{L}_T$ denote the pullback of $\mathscr{L}$ to X_T. There is an isomorphism*

$$t_{x+y}^* \mathscr{L}_T \otimes \mathscr{L}_T \simeq t_x^* \mathscr{L}_T \otimes t_y^* \mathscr{L}_T \otimes \mathrm{pr}_T^* \left((x+y)^* \mathscr{L} \otimes x^* \mathscr{L}^{-1} \otimes y^* \mathscr{L}^{-1} \right),$$

where $\mathrm{pr}_T : X_T \to T$ is projection onto T. In particular, if $T = \operatorname{Spec} k$ there is an isomorphism

$$t_{x+y}^* \mathscr{L} \otimes \mathscr{L} \simeq t_x^* \mathscr{L} \otimes t_y^* \mathscr{L}.$$

Proof. Apply Corollary 1.14 to $f = \mathrm{pr}_X : X_T \to X$, $g = x \circ \mathrm{pr}_T : X_T \to X$ and $h = y \circ \mathrm{pr}_T : X_T \to X$, noting that

$$f+g = \mathrm{pr}_X \circ t_x : X_T \to X, \quad f+h = \mathrm{pr}_X \circ t_y : X_T \to X, \quad g+h = (x+y) \circ \mathrm{pr}_T : X_T \to X,$$

and

$$f+g+h = \mathrm{pr}_X \circ t_{x+y} : X_T \to X.$$

■

Definition 1.16. Let X be a commutative k-group scheme. For any $n \in \mathbf{Z}$, we let $[n]_X : X \to X$ be the group morphism corresponding (via Yoneda's Lemma) to multiplication by n on $X(T)$, for every k-scheme T. Where convenient, we abbreviate $[n]_X$ by n.

Corollary 1.17. *Let X be an abelian variety and $\mathscr{L}$ an invertible sheaf on X. Then for all $n \in \mathbf{Z}$ there is an isomorphism*

$$n^* \mathscr{L} \simeq \mathscr{L}^{\otimes (n(n+1)/2)} \otimes (-1)^* \mathscr{L}^{\otimes (n(n-1)/2)}.$$

Proof. Apply Corollary 1.14 with $f = n$, $g = 1$, $h = -1$ to deduce that

$$(n+1)^* \mathscr{L} \otimes \mathscr{L} \simeq n^* \mathscr{L}^{\otimes 2} \otimes (n-1)^* \mathscr{L} \otimes \mathscr{L}^{-1} \otimes [1]_X^* \mathscr{L} \otimes [-1]^* \mathscr{L}$$

Now induct on n in both directions, starting from the easy cases $n = 0, 1, -1$. ■

Theorem 1.18. *Every abelian variety X/k is projective.*

Proof. Choose a nonempty open affine $U \subset X$ and let $D = X \setminus U$ with the reduced structure. We claim that D is a Cartier divisor (that is, its coherent ideal sheaf is invertible). Since X is regular, it is equivalent to say that all generic points of D have codimension 1. Mumford omits this explanation in [6], so let us explain it more generally.

We claim that for any separated normal connected noetherian scheme X and any nonempty affine $U \neq X$, the nowhere dense closed complement $Y = X \setminus U$ with its reduced structure has pure codimension 1. That is, for a generic point $y \in Y$, the local ring $\mathscr{O}_{X,y}$ has dimension 1. The inclusion $i : \operatorname{Spec} \mathscr{O}_{X,y} \to X$ is an affine morphism since X is separated, so $S = i^{-1}(U) = \operatorname{Spec} \mathscr{O}_{X,y} \setminus \{y\}$ is affine, whence the injective map on global sections $\mathscr{O}_{X,y} \to H^0(S, \mathscr{O}_S)$ is not surjective. Since $\mathscr{O}_{X,y}$ is a normal noetherian domain, it is the intersection of all localizations at height 1-primes, and if $\dim \mathscr{O}_{X,y} > 1$ then the local rings at such primes are local rings on S. Since any $f \in H^0(S, \mathscr{O}_S)$ is in each such localization, we conclude that $\mathscr{O}_{X,y} \hookrightarrow H^0(S, \mathscr{O}_S)$ is surjective, a contradiction.

With D now known to be an effective Cartier divisor, it suffices to prove more generally that if $D \subset X$ is *any* (possibly non-reduced) nonempty Cartier divisor with affine open complement $U = X \setminus D$, then the inverse ideal sheaf $\mathscr{O}_X(D)$ is ample on X. In view of the cohomological criterion for ampleness and the fact that our assumptions are preserved by extension of the base field, we can assume $k = \overline{k}$. By [6, pg. 60–61] it suffices to prove that

$$H = \{x \in X(k) \ : \ t_x^* D = D\}$$

is finite (equality of divisors in the definition of H). By making a translation, we may assume $0 \notin D(k)$. Let $U = X \setminus D$ as an open subscheme of X. If $h \in H$ then $h + U = U$, so $h \in U$ since $0 \in U(k)$. That is, $H \subseteq U(k)$. If H is Zariski-closed in $X(k)$ then H will be closed in $U(k)$ and hence is both affine and proper (in the sense of classical algebraic geometry, identifying reduced k-schemes of finite type with their subsets of k-points), whence finite. To show H is Zariski-closed we pick $x \in X(k) \setminus H$ and seek a Zariski-open $V \subseteq X(k)$ around x in $X(k) \setminus H$. Since $x \notin H$, we have $t_x^{-1}(s) \in U(k)$ for some $s \in D(k)$. That is, $-x + s \in U(k)$. Thus, $V = s - U(k)$ is an open neighborhood of x in $X(k)$ contained in $X(k) \setminus H$. ■

2. Isogenies

2.1. Definitions.

Proposition 2.2. *Let $f : X \to Y$ be a homorphism of abelian varieties. The following are equivalent:*

1. *f is surjective and* $\dim X = \dim Y$*.*
2. $\ker(f)$ *is a finite group scheme and* $\dim X = \dim Y$*.*
3. *f is finite, flat, and surjective (so $f_* \mathscr{O}_X$ is a locally free $\mathscr{O}_Y$-module of finite rank).*

Proof. See [4, §8] or [5, Prop. 5.2]. ■

Definition 2.3. Any homomorphism $f : X \to Y$ of abelian varieties satisfying the equivalent properties of Proposition 2.2 will be called an *isogeny*. The *degree* of an isogeny is the degree of the field extension $[k(X) : k(Y)]$.

Since f in Definition 2.3 is affine and $f_* \mathscr{O}_X$ is a locally free $\mathscr{O}_Y$-module of finite rank, we see that for any $y \in Y$, the $k(y)$-scheme $f^{-1}(y) = \operatorname{Spec}((f_* \mathscr{O}_X)_y / \mathfrak{m}_y)$ is $k(y)$-finite with rank equal to the degree of f.

Proposition 2.4. *Let X be an abelian variety. If $n \neq 0$ then $[n]_X$ is an isogeny of degree $n^{2 \dim X}$. Moreover, if* $\operatorname{char}(k) \nmid n$ *then $[n]_X$ is finite étale.*

Proof. Since X is projective, there is an ample $\mathscr{L}$ on X, and since $[-1]_X$ is an automorphism of X, $[-1]_X^* \mathscr{L}$ is also ample. Since $n \neq 0$ it follows from Corollary 1.17 that $[n]_X^* \mathscr{L}$ is ample. Thus the restriction of $\mathscr{L}$ to $\ker[n]_X$ is ample and trivial, which implies that $\ker[n]_X$ has dimension 0, whence $[n]_X$ is an isogeny. To compute the degree of $[n]_X$, one uses intersection theory as in [6, pg. 62].

The immersions $i_1, i_2 : X \rightrightarrows X \times X$ given on points by $i_1(x) = (x, 0)$ and $i_2(x) = (0, x)$ canonically realize the tangent space at the identity $T_0(X \times X)$ as the direct sum $T_0 X \oplus T_0 X$. Moreover, since the composite $X \xrightarrow{i_j} X \times X \xrightarrow{m} X$ is the identity for $j = 1, 2$, the differential $dm : T_0 X \oplus T_0 X \to T_0 X$ is addition of components. It follows by induction that $[n]_X$ induces multiplication by n on $T_0 X$. When $\operatorname{char}(k) \nmid n$, we therefore see that $[n]_X$ is étale at the origin, and hence étale. ■

Corollary 2.5. *If* $\operatorname{char}(k) \nmid n$ *then* $X[n](k^{\mathrm{sep}}) \simeq (\mathbf{Z}/n\mathbf{Z})^{2g}$*. If* $\operatorname{char}(k) = p > 0$*, then* $X[p^m](\overline{k}) \simeq (\mathbf{Z}/p^m\mathbf{Z})^r$ *for some* $0 \leq r \leq g$ *independent of* $m \geq 1$*.*

Proof. We prove only statements concerning n not divisible by $\operatorname{char}(k)$. For the rest, we refer to [5, 5.20]. We remark that the corollary is obvious in characteristic 0 via the complex-analytic theory.

For every divisor d of n, $X[d]$ is an étale group scheme of rank d^{2g} killed by $[d]$; it follows that $X[d](k^{\mathrm{sep}})$ is an abelian group of rank d^{2g} killed by d, and the conclusion follows (exactly as in the case of elliptic curves). ■

Corollary 2.6. *If X/k is an abelian variety then $X(\overline{k})$ is a divisible group.*

Proof. The surjectivity of $[n]_X$ implies that the map on k-points is surjective. ■

Definition 2.7. Let X be a scheme of characteristic $p > 0$. For any affine open $\operatorname{Spec} A$ in X, define the *absolute Frobenius morphism* $\operatorname{Spec} A \to \operatorname{Spec} A$ to be the map induced by the ring homomorphism $f \mapsto f^p$. These morphisms glue to give a morphism, also called the absolute Frobenius,

$$\mathrm{Frob}_X : X \to X$$

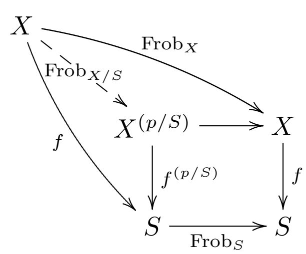
characterized by the properties:

(1) Frob_X is the identity on the underlying topological space of X.
(2) $\mathrm{Frob}_X^{\#} : \mathscr{O}_X \to \mathscr{O}_X$ is given on sections by $f \mapsto f^p$.

Let S be an $\mathbf{F}_p$-scheme and X an S-scheme. The map Frob_X is not in general a morphism of S-schemes. To remedy this situation, we introduce the *relative Frobenius morphism*. Define $X^{(p/S)}$ to be the fiber product $S \times_S X$ given by the morphism $\mathrm{Frob}_S : S \to S$ (it is denoted $X^{(p)}$ if S is understood). The structure morphism $f^{(p/S)} : X^{(p/S)} \to S$ is simply the pullback of X along Frob_S. If $f : X \to S$ is the structure map then $f \circ \mathrm{Frob}_X = \mathrm{Frob}_S \circ f$ due to the p^{th}-power map respecting all ring homomorphisms of $\mathbf{F}_p$-algebras. Thus, there is a unique morphism

$$\mathrm{Frob}_{X/S} : X \to X^{(p/S)}$$

making the diagram



commute.

Example 2.8. If $S = \operatorname{Spec} A$ and $X = \operatorname{Spec} A[T_1, \ldots, T_n]/(h_1, \ldots, h_m)$ then

$$X^{(p/S)} = \operatorname{Spec} A[T_1, \ldots, T_n]/(h_1^{(p)}, \ldots, h_m^{(p)}),$$

where $h^{(p)} = \sum a_I^p T^I$ for $h = \sum a_I T^I$. Also, $\mathrm{Frob}_{X/S} : X \to X^{(p/S)}$ corresponds to $T_i \mapsto T_i^p$. Loosely speaking, $\mathrm{Frob}_{X/S}$ is "p^{th}-power on relative coordinates."

If X is an abelian variety over a field k of characteristic $p > 0$, then the relative Frobenius morphism $F_{X/k}$ is an isogeny because it satisfies Proposition 2.2 (1). In fact, since it is finite flat and the identity on topological spaces, its degree can be computed as the degree of the induced map

$$F_{X/k,e} : \widehat{\mathscr{O}_{X^{(p)},e}} \to \widehat{\mathscr{O}_{X,e}}$$

where $\widehat{\mathscr{O}_{X,e}}$ is the complete local ring at the origin. Arguing as in Example 2.8 and using k-smoothness, we conclude $\deg F_{X/k} = p^{\dim X}$ since the map $k[\![t_1, \ldots, t_d]\!] \to k[\![t_1, \ldots, t_d]\!]$ given by $t_j \mapsto t_j^p$ is finite flat with degree p^d.

2.9. The isogeny category.

Theorem 2.10. *If $f : X \to Y$ is an isogeny of degree n then there exists an isogeny $g : Y \to X$ such that $f \circ g = [n]_Y$ and $g \circ f = [n]_X$.*

Proof. Since $\ker(f)$ is a group scheme of rank n it is killed by $[n]_X$, so by viewing Y as the *fppf* quotient of X modulo $\ker(f)$ (see Proposition 2.2) we see that $[n]_X$ factors as

$$X \xrightarrow{f} Y \xrightarrow{g} X.$$

Then $g \circ (f \circ g) = [n]_X \circ g = g \circ [n]_Y$ and $(f \circ g - [n]_Y) : Y \to Y$ maps Y into $\ker(g)$, a finite group scheme. It follows that $f \circ g - [n]_Y = 0$. ■

Theorem 2.10 shows that "there exists an isogeny from X to Y" is an equivalence relation, and clearly $\mathrm{Hom}(X, Y)$ is torsion-free as a $\mathbf{Z}$-module, due to Corollary 2.6.

Definition 2.11. The *isogeny category* of abelian varieties over k is the $\mathbf{Q}$-linear category whose objects are abelian varieties over k, with morphisms between two objects X, Y given by $\mathbf{Q} \otimes_{\mathbf{Z}} \mathrm{Hom}(X, Y)$.

3. The dual abelian variety

3.1. The Picard functor.

Definition 3.2. Let X be a scheme. We define the Picard group $\mathrm{Pic}(X)$ to be the group (under $\otimes_{\mathscr{O}_X}$) of isomorphism classes of invertible sheaves on X. This is contravariant in X. There is an evident isomorphism of groups

$$\mathrm{Pic}(X) \simeq \check{H}^1(X, \mathscr{O}_X^{\times}) \simeq H^1(X, \mathscr{O}_X^{\times}).$$

In order to study the *relative situation*, we let X and T be S-schemes and define a functor $P_{X/S}$ by

$$P_{X/S}(T) = \mathrm{Pic}(X_T).$$

Observe that this is a contravariant functor. What we would like is for this functor to be representable; however, this is *never* the case if X is nonempty because $P_{X/S}$ is not even a sheaf for the Zariski topology on a k-scheme T in general. In order to obtain a representable functor, we "rigidify" the situation.

From now on we will assume that $X \xrightarrow{f} S$ is a morphism of schemes such that:

(1) The structure map f is quasi-compact and separated.
(2) For all S-schemes T, the natural map $\mathscr{O}_T \to f_{T*}(\mathscr{O}_{X \times_S T})$ is an isomorphism.
(3) There is a section $\epsilon : S \to X$ to f.

These assumptions hold in the situations we wish to study: $S = \mathrm{Spec}\, k$ and X is proper with a k-rational point. By Grothendieck's theory of coherent base change, condition (2) holds more generally whenever $f : X \to S$ is proper, finitely presented, and flat, with geometrically integral fibers.

Definition 3.3. For any S-scheme T let $\epsilon_T : T \to X_T$ be the map induced by ϵ and let $\mathscr{L}$ be an invertible sheaf on X_T. A *rigidification of $\mathscr{L}$ along ϵ_T* (or simply along ϵ) is an isomorphism

$$\alpha : \mathscr{O}_T \xrightarrow{\sim} \epsilon_T^*(\mathscr{L}).$$

We call such a pair $(\mathscr{L}, \alpha)$ an *ϵ-rigidified sheaf*, or simply a *rigidified sheaf* if no confusion will arise, and will abuse notation by writing ϵ for ϵ_T. A homomorphism of rigidified sheaves

$$h : (\mathscr{L}_1, \alpha_1) \to (\mathscr{L}_2, \alpha_2)$$

is a homomorphism of sheaves $h : \mathscr{L}_1 \to \mathscr{L}_2$ making the diagram of sheaves on T

$$\begin{array}{ccc} \mathscr{O}_T & \xrightarrow{\alpha_2} & \epsilon^*\mathscr{L}_2 \\ & \searrow^{\alpha_1} & \downarrow{\scriptstyle \epsilon^* h} \\ & & \epsilon^*\mathscr{L}_1 \end{array}$$

commute.

Observe that a rigidified sheaf has no non-trivial automorphisms: any automorphism $\mathscr{L} \xrightarrow{h} \mathscr{L}$ is an element of

$$\Gamma(X_T, \mathscr{O}_{X_T}) = \Gamma(T, f_{T*}(\mathscr{O}_{X_T})) = \Gamma(T, \mathscr{O}_T)$$

satisfying $\epsilon^*(h) = 1$, so $h = \mathrm{id}$.

Definition 3.4. Let X be an S-scheme satisfying the assumptions (1)–(3) above. We define the contravariant functor $P_{X/S,\epsilon} : \mathfrak{Sch}/S \to \mathfrak{Set}$ by

$$P_{X/S,\epsilon}(T) = \{\text{isomorphism classes of rigidified sheaves } (\mathscr{L}, \alpha) \text{ on } X_T\},$$

where a morphism $T' \to T$ induces a morphism $P_{X/S,\epsilon}(T) \to P_{X/S,\epsilon}(T')$ by pullback of rigidified sheaves.

For every S-scheme T, the set $P_{X/S,\epsilon}$ has the structure of a commutative group: we define the product of $(\mathscr{L}_1, \alpha_1)$, $(\mathscr{L}_2, \alpha_2)$ in $P_{X/S,\epsilon}(T)$ to be the class of

$$(\mathscr{L}_1 \otimes \mathscr{L}_2, \alpha_1 \otimes \alpha_2),$$

where

$$\alpha_1 \otimes \alpha_2 : \mathscr{O}_T \xrightarrow{\sim} \mathscr{O}_T \otimes_{\mathscr{O}_T} \mathscr{O}_T \xrightarrow{\alpha_1 \otimes \alpha_2} \epsilon^*\mathscr{L}_1 \otimes_{\mathscr{O}_T} \epsilon^*\mathscr{L}_2 \xrightarrow{\sim} \epsilon^*(\mathscr{L}_1 \otimes \mathscr{L}_2).$$

Inversion is defined using the dual invertible sheaf. Observe that the group structure on $P_{X/S,\epsilon}(T)$ is functorial in T, so $P_{X/S,\epsilon}$ is a *group functor.* Thus, if $P_{X/S,\epsilon}$ is representable, it is represented by a commutative group scheme.

Theorem 3.5. (1) *If $f : X \to S$ is flat, projective, and finitely presented with geometrically integral fibers then $P_{X/S,\epsilon}$ is represented by a scheme $\mathrm{Pic}_{X/S,\epsilon}$ of locally finite presentation and separated over S.*
(2) *If $S = \operatorname{Spec} k$ and f is proper, then $P_{X/S,\epsilon}$ is represented by a scheme $\mathrm{Pic}_{X/k,\epsilon}$ of locally finite type over S.*

Proof. See Grothendieck [2] for (1) and Murre [8] for (2). ∎

Let us derive some properties of the scheme $\mathrm{Pic}_{X/S,\epsilon}$. We first claim that the functor $\mathrm{Pic}_{X/S,\epsilon}$ does not depend on the choice of rigidifying section ϵ. Let $f : X_T \to T$ be the structure map and suppose we have a rigidification φ_1 of $\mathscr{L} \in \mathrm{Pic}_{X/S}(T)$ along the section $\epsilon_1 : T \to X_T$. For any section $\epsilon_2 : T \to X_T$, observe that for the invertible sheaf

$$\Psi(\mathscr{L}, \epsilon_2) := \mathscr{L} \otimes f^*\epsilon_2^*\mathscr{L}^{-1},$$

its pullback along ϵ_2 is *canonically* trivialized:

$$\epsilon_2^*\Psi(\mathscr{L}, \epsilon_2) \simeq \epsilon_2^*\mathscr{L} \otimes \epsilon_2^* f^*\epsilon_2^*\mathscr{L}^{-1} \simeq \mathscr{O}_T.$$

Moreover, any trivialization $\varphi_2 : \epsilon_2^*\mathscr{L} \xrightarrow{\sim} \mathscr{O}_T$ identifies $\Psi(\mathscr{L}, \epsilon_2)$ with $\mathscr{L}$ and the canonical trivialization above with φ_2. Thus, there are maps $P_{X/S,\epsilon_1}(T) \leftrightarrow P_{X/S,\epsilon_2}(T)$

$$(\mathscr{L}_1, \varphi_1) \longmapsto (\Psi(\mathscr{L}_1, \epsilon_2), \text{canonical trivialization})$$

$$(\Psi(\mathscr{L}_2, \epsilon_1), \text{canonical trivialization}) \longleftarrow\!\shortmid (\mathscr{L}_2, \varphi_2)$$

and one readily checks that these maps are *inverse* to each other. This shows that $P_{X/S,\epsilon_1}$ and $P_{X/S,\epsilon_2}$ are isomorphic as functors, and that the isomorphisms are transitive with respect to a third choice of rigidifying section. In this precise sense, $P_{X/S,\epsilon}$ is "independent of ϵ." From now on, we will feel free to omit the rigidifying section in our notation where convenient.

Example 3.6. If $S = \operatorname{Spec} R$ for a local ring R then $P_{X/S}(R) \simeq \mathrm{Pic}(X)$ via $(\mathscr{L}, \varphi) \mapsto \mathscr{L}$.

We have already remarked that $\mathrm{Pic}_{X/S}$ is an S-group scheme. Under a choice of isomorphism of functors $P_{X/S} \simeq \mathrm{Hom}(-, \mathrm{Pic}_{X/S})$, the identity morphism $\mathrm{Pic}_{X/S} \to \mathrm{Pic}_{X/S}$ gives a *universal* rigidified sheaf $(\mathscr{P}, \nu)$ on $X \times_S \mathrm{Pic}_{X/S}$: for any rigidified sheaf $(\mathscr{L}, \alpha)$ on X_T, there exists a unique morphism $g : T \to \mathrm{Pic}_{X/S}$ such that there exists an isomorphism $(\mathscr{L}, \alpha) \simeq (\mathrm{id}_X \times g)^*(\mathscr{P}, \nu)$, this latter isomorphism clearly being unique due to the rigidification.

Definition 3.7. Let k be a field and suppose that X/k satisfies one of the sets of hypotheses of Theorem 3.5. We define $\mathrm{Pic}^0_{X/k}$ to be the connected component of the identity of $\mathrm{Pic}_{X/k}$. The restriction of $(\mathscr{P}, \nu)$ to $\mathrm{Pic}^0_{X/k}$ is called the *Poincaré sheaf*, $(\mathscr{P}^0, \nu^0)$.

A priori, $\mathrm{Pic}^0_{X/k}$ is merely locally of finite type. However, it is automatically quasi-compact (*i.e.* finite type) due to:

Lemma 3.8. *Let G be a group scheme locally of finite type over a field. The identity component G^0 is an open subgroup scheme that is geometrically connected and of finite type.*

Proof. We follow [5, 3.17]. Let us show first that a connected k-scheme of locally finite type with a rational point is geometrically connected. Let $p : X_{\overline{k}} \to X$ be the projection map. We claim (without using the connectivity or k-rational point hypotheses) that p is both open and closed. It will suffice to show this in the case that X is affine and of finite type, as if $\{U_\alpha\}$ is a covering of X by open affines of finite type then $\{U_{\alpha\overline{k}}\}$ is a covering of $X_{\overline{k}}$ and if $p : U_{\alpha\overline{k}} \to U_\alpha$ is both open and closed, then so is $p : X_{\overline{k}} \to X$. With these reductions, any open or closed $Z \subset X_{\overline{k}}$ is defined over a finite extension K of k (in the sense that it is the base change of an open or closed $Z' \subseteq X_K$), and so it will suffice to show that the finite flat morphism $p : X_K \to X$ is open and closed. As any finite morphism is closed and any flat morphism of finite type between noetherian schemes is open, we conclude that p is open and closed. Now we use the assumptions on X to show that $X_{\overline{k}}$ is connected. Let U be a nonempty closed and open subset of $X_{\overline{k}}$. Then $p(U) = X$ as X is connected, so the unique point over $x \in X$ lies in U. If $X_{\overline{k}} - U$ is nonempty, then the same argument shows $x \in X_{\overline{k}} - U$, an absurdity. Therefore, $X_{\overline{k}} - U$ is empty. Hence $X_{\overline{k}} = U$ and $X_{\overline{k}}$ is connected.

We now claim that G^0 is geometrically irreducible. Since $(G_{\overline{k}})^0 = (G^0)_{\overline{k}}$ by the preceeding paragraph, we may suppose that $k = \overline{k}$. In this case, G^0_{red} is a smooth group scheme by Proposition 1.4. If G^0 were reducible, then G^0_{red} would also be reducible, and since we have shown that G^0 is connected (and its set of irreducible components is locally finite), we can find two distinct irreducible components C_1, C_2 of G^0_{red} with nonempty intersection. For $x \in (C_1 \cap C_2)(k)$ the local ring $\mathscr{O}_{X,x}$ is regular (hence a domain) yet has at least two minimal primes (arising from C_1 and C_2), an absurdity.

Now let $U \subseteq G^0$ be any nonempty open affine. Then since G^0 is geometrically irreducible, $U_{\overline{k}}$ and $g(U^{-1}_{\overline{k}})$ are dense in $G^0_{\overline{k}}$ for any $g \in G^0(\overline{k})$. It follows that $m : U \times U \to G^0$ is surjective, and hence that G^0 is quasi-compact. Therefore, G^0 is of finite type (since G is of locally finite type). ■

We conclude from Lemma 3.8 that $\mathrm{Pic}^0_{X/k}$ is a k-group scheme of finite type whose formation commutes with extension of k. That $\mathrm{Pic}^0_{X/k}$ is separated is a consequence of the following lemma.

Lemma 3.9. *Let k be a field. Then any k-group scheme (G, m, i, e) is separated.*

Proof. Observe that the diagram

$$\begin{array}{ccc} G & \xrightarrow{\Delta_{G/k}} & G \times_k G \\ \downarrow & & \downarrow{\scriptstyle m\circ(\mathrm{id}_G \times i)} \\ \mathrm{Spec}\, k & \xrightarrow[e]{} & G \end{array}$$

is cartesian on T-valued points for every k-scheme T. Thus, by Yoneda's lemma, it is cartesian and $\Delta_{G/k}$ is the base change of the closed immersion $e : \mathrm{Spec}\, k \to G$, and hence a closed immersion. ■

Theorem 3.10. *If X/k is a smooth, proper k-variety with a section $e \in X(k)$ then $\mathrm{Pic}^0_{X/k}$ is proper over $\mathrm{Spec}\, k$.*

Proof. We have seen via Lemmata 3.8 and 3.9 that the k-scheme $\mathrm{Pic}_{X/k}$ is finite type and separated over k. We apply the valuative criterion of properness to $\mathrm{Pic}^0_{X/k}$. Since $\mathrm{Spec}\, R$ is connected for any discrete valuation ring R, it suffices to show that for every discrete valuation ring R containing k with $\mathrm{Frac}(R) = K$, any morphism $\mathrm{Spec}\, K \to \mathrm{Pic}_{X/k}$ extends uniquely to a morphism $\mathrm{Spec}\, R \to \mathrm{Pic}_{X/k}$. That is, given a rigidified invertible sheaf $(\mathscr{L}, \alpha)$ on X_K we must show that there is a unique rigidified invertible sheaf $(\widetilde{\mathscr{L}}, \widetilde{\alpha})$ on X_R restricting to $(\mathscr{L}, \alpha)$. Since X is smooth, X_R is R-smooth and hence regular. Thus, the notions of Cartier divisor and Weil divisor on X_R coincide. Since X_K is a nonempty open subset of X_R, by using scheme-theoretic closure we can extend the sheaf $\mathscr{L}$ on X_K to an invertible sheaf $\widetilde{\mathscr{L}}$ on X_R. We must also show that the rigidification of $\mathscr{L}$ extends to a rigidification of $\widetilde{\mathscr{L}}$. This follows from the fact that given $\alpha \in K^\times$ there is a $K^\times$-scaling of α to a unit of R (since R is a discrete valuation ring). ■

We define $\mathrm{Pic}^0(X) \subseteq \mathrm{Pic}(X) = \mathrm{Pic}_{X/k}(k)$ to be $\mathrm{Pic}^0_{X/k}(k)$, so $\mathrm{Pic}^0(X_K) \cap \mathrm{Pic}(X) = \mathrm{Pic}^0(X)$ inside $\mathrm{Pic}(X_K)$ for any extension of fields K/k. Geometrically, $\mathrm{Pic}^0(X)$ consists of isomorphism classes of invertible sheaves on X that lie in a connected algebraic family with the trivial class.

Theorem 3.11. *The tangent space of* $\mathrm{Pic}_{X/k}$ *at the identity is naturally* k*-isomorphic to* $H^1(X, \mathscr{O}_X)$*.*

Proof. Let $S = \mathrm{Spec}\, k[\varepsilon]/(\varepsilon^2)$. Giving a morphism $S \to \mathrm{Pic}_{X/k}$ sending $\mathrm{Spec}\, k$ to 0 is equivalent to giving an element of the tangent space at 0. This is equivalent to giving an invertible rigidified sheaf $(\mathscr{L}, \alpha)$ on $X \times_k S$ whose restriction to X is trivial, i. e. an element of $\mathrm{Pic}(X_S)$ that restricts to 0 in $\mathrm{Pic}(X)$.

Consider the exact sequence of sheaves on the topological space X,

$$0 \to \mathscr{O}_X \xrightarrow{h} \mathscr{O}_{X_S}^\times \xrightarrow{r} \mathscr{O}_X^\times \to 1,$$

where h is given on sections by $h : f \mapsto 1 + \varepsilon f$ and r is the restriction map (given on sections by mapping ε to zero). This gives rise to a long exact sequence of cohomology:

$$0 \longrightarrow k \longrightarrow (k[\varepsilon]/(\varepsilon^2))^\times \longrightarrow k^\times \longrightarrow H^1(X, \mathscr{O}_X) \longrightarrow \mathrm{Pic}(X_S) \longrightarrow \mathrm{Pic}(X).$$

Since $(k[\varepsilon]/(\varepsilon)^2)^\times \to k^\times$ is surjective, we see that the evident diagram

$$0 \to H^1(X, \mathscr{O}_X) \to \mathrm{Pic}_{X/k}(k[\epsilon]) \to \mathrm{Pic}_{X/k}(k)$$

is exact. This shows that the tangent space at the origin of $\mathrm{Pic}_{X/k}$ and $H^1(X, \mathscr{O}_X)$ are naturally isomorphic as abelian groups. To show that they are isomorphic as k-vector spaces, we must investigate the k-structures on each.

For any covariant functor F on artin local k-algebras R with residue field k such that the natural map

$$F(R' \times_R R'') \to F(R') \times_{F(R)} F(R'')$$

is always bijective (*e.g.* any functor $\mathrm{Hom}_{\mathrm{Spec}\, k}(-, Y)$ for a k-scheme Y), there is a natural k-vector space structure on fibers of $F(k[\epsilon]) \to F(k)$ given by the morphisms

$$\begin{aligned} k[\epsilon] &\to k[\epsilon] \\ \epsilon &\mapsto c\epsilon \end{aligned} \qquad\qquad \begin{aligned} k[\epsilon] \times_k k[\epsilon] \simeq k[\epsilon_1, \epsilon_2]/(\epsilon_1\epsilon_2, \epsilon_1^2, \epsilon_2^2) &\to k[\epsilon] \\ \epsilon_1, \epsilon_2 &\mapsto \epsilon. \end{aligned}$$

If $F = \mathrm{Hom}_{\mathrm{Spec}\, k}(-, Y)$ for a commutative k-group Y locally of finite type over k, the argument with tangent spaces in the proof of Proposition 2.4 shows that the resulting group structure on $\ker(F(k[\epsilon]) \to F(k))$ *agrees* with the group functor structure on F. In this way, the kernel of $\mathrm{Pic}_{X/k}(k[\epsilon]) \xrightarrow{r} \mathrm{Pic}_{X/k}(k)$ inherits a natural structure of a k-vector space. In particular, let $\mathscr{L}, \mathscr{L}'$ be in the kernel of this map, and let $\{U_\alpha\}$ be an open cover of X such that $\mathscr{L}, \mathscr{L}'$ are trivialized by $\{U_\alpha\}$ with transition data $1 + \epsilon f_{\alpha\beta}$, $1 + \epsilon f'_{\alpha\beta}$ on $U_\alpha \cap U_\beta$ respectively (we know the reductions mod ϵ yields the trivial sheaf). Then $\mathscr{L} \otimes \mathscr{L}'$ is trivialized by $\{U_\alpha\}$ with transition data

$$(1 + \epsilon f_{\alpha\beta})(1 + \epsilon f'_{\alpha\beta}) = (1 + \epsilon(f_{\alpha\beta} + f'_{\alpha\beta}))$$

on $U_\alpha \cap U_\beta$. Moreover, multiplication by a scalar c sends $\mathscr{L}$ to the sheaf that is trivialized by $\{U_\alpha\}$ with transition data $1 + c\epsilon f_{\alpha\beta}$ on $U_\alpha \cap U_\beta$.

To understand the k-structure on $H^1(X, \mathscr{O}_X)$, we work with Čech cohomology. Let $\gamma \in H^1(X, \mathscr{O}_X)$ be represented on an open covering $\{U_\alpha\}$ of X by a Čech 1-cocycle $f_{\alpha\beta} \in \mathscr{O}_X(U_\alpha \cap U_\beta)$. Then $h(\gamma)$ is the isomorphism class of the invertible sheaf on X_S which is trivial on each U_α with transition data given by multiplication by $1 + \epsilon f_{\alpha\beta}$. Thus, for any $c, c' \in k$, and $\gamma, \gamma' \in H^1(X, \mathscr{O}_X)$ with γ, γ' represented on a common open covering $\{U_\alpha\}$ by the 1-cocycles $f_{\alpha\beta}, f'_{\alpha\beta}$ respectively, we see that $c\gamma + c'\gamma'$ is represented by the 1-cocycle $cf_{\alpha\beta} + c'f'_{\alpha\beta}$. It follows that the morphism h respects the k-structures, as desired. ■

3.12. **The cohomology of an abelian variety.** When X is an abelian variety, Theorems 3.5 and 3.10 guarantee that $\mathrm{Pic}^0_{X/k}$ is a proper connected k-group scheme. The goal of this section is to use Theorem 3.11 to show that $\mathrm{Pic}^0_{X/k}$ is smooth, hence an abelian variety, and that its dimension is the same as that of X. This is a subtle fact in positive characteristic, as there exist examples of smooth projective surfaces S over algebraically closed fields k with $\mathrm{char}(k) > 0$ such that the proper k-group $\mathrm{Pic}^0_{S/k}$ is not smooth.

3.13. Graded bialgebras.

Definition 3.14. A graded k-bialgebra is an associative graded k-algebra

$$H = \bigoplus_{i \geq 0} H^i$$

with $H^0 = k$, together with a *co-multiplication* map of graded k-algebras $f : H \to H \otimes_k H$, such that for all $h \in H^n$ with $n > 0$,

$$f(h) = h \otimes 1 + 1 \otimes h + \sum_i x_i \otimes y_i,$$

with $x_i \in H^{e_i}$, $y_i \in H^{n-e_i}$ for $e_i > 0$. That is, the components of $f(h)$ in $H \otimes_k H^0 \simeq H$ and $H^0 \otimes_k H$ are h. A graded bialgebra is *anticommutative* if $h_1 h_2 = (-1)^{n_1 n_2} h_2 h_1$ for $h^i \in H^{n_i}$ with $n_i \geq 0$.

Example 3.15. Let V be a vector space over a field k and let $H = \wedge V = \oplus_{i \geq 0} \wedge^i V$ be the exterior algebra on V. Then $H^0 = \wedge^0 V = k$ by definition, and $(f, g) \mapsto f \wedge g$ gives H the structure of a graded anticommutative k-algebra. The diagonal map $V \to V \oplus V$ induces a map of graded k-algebras $H \to \wedge(V \oplus V)$. The identifications $\wedge^i(V \oplus V) \simeq \oplus_{j+k=i} \wedge^j V \otimes \wedge^k V$ show that $\wedge(V \oplus V) \simeq H \otimes H$, so we obtain a map of graded k-algebras $h : H \to H \otimes H$ which is readily seen to be a co-multiplication. Thus, H is an anticommutative graded k-bialgebra.

There is a very important structure theorem for anticommutative graded bialgebras:

Theorem 3.16. *Let k be a perfect field and H a anticommutative graded bialgebra over k. If $H^i = 0$ for all $i > g$ (some g) then H is isomorphic to the associative graded anticommutative k-algebra freely generated by $X_1, \ldots, X_m$ with homogenous degrees r_i and satisfying the relations $X_i^{s_i} = 0$ for $1 < s_i \leq \infty$, with "$s_i = \infty$" understood to mean that there is no relation on X_i.*

Proof. See [1, Theorem 6.1]. ∎

Corollary 3.17. *Let H be an anticommutative graded bialgebra over any field k with $H^0 = k$ and $H^i = 0$ for all $i > g$. Then $\dim_k H^1 \leq g$, with equality only if the canonical map $\wedge H^1 \to H$ is an isomorphism.*

Proof. Since the hypotheses are stable under field extension and the conclusion descends, we may assume that k is perfect. Let $X_1, \ldots, X_m$ be as in Theorem 3.16. The product $X_1 \cdots X_m$ is nonzero (since all $s_i > 1$) and $\sum \deg(X_i) = \deg(\prod X_i) \leq g$, so the number of X_i of degree 1 is at most g; since H^1 is k-linearly spanned by the X_i of degree 1, the first part is immediate and equality holds if and only if $\deg x_i = 1$ for all i. If every X_i has degree 1, then for all i the monomial $X_1 \cdots X_i^2 \cdots X_m$ has degree $g+1$ and is therefore 0. It follows that $X_i^2 = 0$ and the natural map $\wedge H^1 \to H$ is an isomorphism. ∎

Proposition 3.18. *Let X/k be an abelian variety of dimension g. Then $\dim_k H^1(X, \mathscr{O}_X) \leq g$.*

Proof. Define

$$H = H(X, \mathscr{O}_X) = \bigoplus_{i \geq 0} H^i(X, \mathscr{O}_X).$$

Since X is projective, $H^0 = k$. Moreover, Grothendieck's vanishing theorem ensures that $H^i = 0$ for all $i > g$. Cup product gives H the structure of a graded anticommutative k-algebra. Now the Künneth formula shows that using pullback and cup product defines a canonical graded anticommutative k-algebra map

$$H(X, \mathscr{O}_X) \otimes H(X, \mathscr{O}_X) \to H(X \times X, \mathscr{O}_{X \times X})$$

that is an isomorphism. The addition morphism $m : X \times X \to X$ induces a graded k-algebra map

$$h : H(X, \mathscr{O}_X) \to H(X \times X, \mathscr{O}_{X \times X}) \simeq H(X, \mathscr{O}_X) \otimes H(X, \mathscr{O}_X).$$

Similarly, because $m \circ i$ is the identity, the map $i : X \to X \times X$ given by $x \mapsto (x, 0)$ induces a section

$$s : H(X \times X, \mathscr{O}_{X \times X}) \to H(X, \mathscr{O}_X)$$

that identifies H as the direct summand $H \otimes H^0$ of $H \otimes H$, and such that projection of $H \otimes H$ onto this summand sends $h(x)$ to $x \otimes 1$. Similarly, projection onto $H^0 \otimes H$ sends $h(x)$ to $1 \otimes x$. It follows that H is a graded k-bialgebra, satisfying the hypotheses of Corollary 3.17, so $\dim_k H^1 \leq g$. ∎

3.19. **The dual abelian variety.**

Definition 3.20. Let X be an abelian variety and $\mathscr{L} \in \mathrm{Pic}(X)$. The *Mumford sheaf* on $X \times X$ is

$$\Lambda(\mathscr{L}) = m^*\mathscr{L} \otimes \mathrm{pr}_1^*\mathscr{L}^{-1} \otimes \mathrm{pr}_2^*\mathscr{L}^{-1}.$$

Observe that

$$(e \times 1)^*\Lambda(\mathscr{L}) \simeq \mathscr{L} \otimes f^*e^*\mathscr{L}^{-1} \otimes \mathscr{L}^{-1} \simeq f^*e^*\mathscr{L}^{-1}$$

where $f : X \to \mathrm{Spec}\, k$ is the structure morphism and $e^*\mathscr{L}^{-1}$ is an invertible sheaf on $\mathrm{Spec}\, k$, hence trivial. Although there is not a canonical trivialization of $f^*e^*\mathscr{L}^{-1}$, any two trivializations differ by a (unique) $k^\times$-multiple. Choose a trivialization. By the universal property of the pair $(\mathrm{Pic}_{X/k}, \mathscr{P})$ there is a unique k-morphism $\phi_{\mathscr{L}} : X \to \mathrm{Pic}_{X/k}$ such that there exists an isomorphism $\theta : (\mathrm{id}_X \times \phi_{\mathscr{L}})^*\mathscr{P} \xrightarrow{\sim} \Lambda(\mathscr{L})$ as $(e \times 1)$-rigidified sheaves, and if we change the $(e \times 1)$-rigidification of $\Lambda(\mathscr{L})$ it merely scales by some $c \in k^\times$, so by using $c^{-1}\theta$, we see that $\phi_{\mathscr{L}}$ is *independent* of the choice of $(e \times 1)$-rigidification of $\Lambda(\mathscr{L})$.

To understand $\phi_{\mathscr{L}}$ on points $x \in X(k)$, we pull back $\Lambda(\mathscr{L})$ along $X \xrightarrow{(\mathrm{id},x)} X \times X$. We obtain the sheaf

$$t_x^*\mathscr{L} \otimes \mathscr{L}^{-1} \in \mathrm{Pic}(X).$$

Thus, $\phi_{\mathscr{L}}(x) \in \mathrm{Pic}_{X/k}(k) = \mathrm{Pic}(X)$ (see Example 3.6) corresponds to the isomorphism class of the sheaf $t_x^*\mathscr{L} \otimes \mathscr{L}^{-1}$. Since $\mathrm{Pic}_{X/k}(\overline{k}) = \mathrm{Pic}_{X_{\overline{k}}/\overline{k}}(\overline{k})$, the theorem of the square implies that $\phi_{\mathscr{L}} : X \to \mathrm{Pic}_{X/k}$ is a homomorphism on $\overline{k}$-points. Since X is k-smooth, by going up to $\overline{k}$ (where G_{red} is a subgroup of G for any $\overline{k}$-group G locally of finite type, such as $G = \mathrm{Pic}_{X_{\overline{k}}/\overline{k}}$), we conclude that $\phi_{\mathscr{L}}$ is a homomorphism of group schemes. Since $\phi_{\mathscr{L}}(0) = 0$ and X is connected, $\phi_{\mathscr{L}}$ factors through $\mathrm{Pic}^0_{X/k}$. A subtle point is that we do not yet know that $\mathrm{Pic}_{X/k}$ is reduced (and even k-smooth).

Theorem 3.21. *If $\mathscr{L}$ is an invertible sheaf on X classified by a point in $\mathrm{Pic}^0_{X/k}(k) \subseteq \mathrm{Pic}_{X/k}(k) = \mathrm{Pic}(X)$ then $\phi_{\mathscr{L}} = 0$.*

Remark 3.22. This is a partial result toward relating our approach (resting on Grothendieck's general theory of the Picard scheme) with the "bare hands" approach in [6].

Proof. We first relativize the construction of $\phi_{\mathscr{L}}$. For any k-scheme T, we have a group map

$$\tau_e : \mathrm{Pic}(X_T) \to \mathrm{Pic}_{X/k,e}(T) \quad \text{given by} \quad \mathscr{L} \mapsto \mathscr{L}_T \otimes f_T^*e_T^*\mathscr{L}_T^{-1},$$

where $f : X \to \mathrm{Spec}\, k$ is the structure morphism. If T is local (*e.g.* $T = \mathrm{Spec}\, K$ for a field K/k) then $\tau_e(\mathscr{L}) \simeq \mathscr{L}$ is invertible sheaves). Thus, for any $\mathscr{L}$ on X_T we get a map $X_T \to (\mathrm{Pic}_{X/k,e})_T$ via

$$x' \mapsto \tau_\epsilon\left(t_{x'}^*\mathscr{L}_{T'} \otimes \mathscr{L}_{T'}^{-1}\right)$$

for $x' \in X(T')$ for T-schemes T'. This corresponds to a T-map

$$\phi_{\mathscr{L}} : T \times X \to T \times \mathrm{Pic}_{X/k,e}$$

satisfying $\phi_{\mathscr{L}}(T \times \{e\}) = 0$. By geometric connectivity of X, this map factors through $T \times \mathrm{Pic}^0_{X/k,e}$, recovering our earlier definition for $T = \mathrm{Spec}\, k$. On geometric fibers we therefore know that $\phi_{\mathscr{L}}$ is a group-scheme map, and by [7, Proposition 6.1], it follows that $\phi_{\mathscr{L}}$ is a group map. Since $\phi_{\mathscr{L}} + \phi_{\mathscr{L}'} = \phi_{\mathscr{L} \otimes \mathscr{L}'}$, the map $\mathscr{L} \mapsto \phi_{\mathscr{L}}$ defines a map of functors $\phi : \mathrm{Pic}_{X/k} \to \underline{\mathrm{Hom}}(X, \mathrm{Pic}^0_{X/k})$. The content of the theorem is that ϕ vanishes on $\mathrm{Pic}^0_{X/k}$.

Since X is projective and geometrically integral over k, both X and the k-proper $\mathrm{Pic}^0_{X/k}$ are projective over k (for general projective k-varieties X, the scheme $\mathrm{Pic}^0_{X/k}$ is merely quasi-projective). Thus, by Grothendieck's theory of Hom-schemes, the group functor $\underline{\mathrm{Hom}}(X, \mathrm{Pic}^0_{X/k})$ is represented by a k-scheme locally of finite type. To get vanishing of ϕ on $\mathrm{Pic}^0_{X/k}$ it is therefore enough to show that the locally finite type k-scheme $\underline{\mathrm{Hom}}(X, \mathrm{Pic}^0_{X/k})$ is étale, since then it breaks up over $\overline{k}$ as a disjoint union of copies of $\mathrm{Spec}\, \overline{k}$, and ϕ must map connected components of $\mathrm{Pic}_{X_{\overline{k}}/\overline{k}}$ to single points. To show that $\underline{\mathrm{Hom}}(X, \mathrm{Pic}^0_{X/k})$ is étale, we work over $\overline{k}$ and study the tangent space at the origin, which we want to vanish. It is therefore enough to show that the zero map $X \to \mathrm{Pic}^0_{X/k}$ has no nonzero liftings over $k[\epsilon]$. This again follows from [7, Theorem 6.1]. ■

Proposition 3.23. *If $f, g : T \to X$ are k-morphisms with X/k an abelian variety and T any k-scheme, then for all $\mathscr{L}$ on X lying in $\mathrm{Pic}^0_{X/k}(k) \subseteq \mathrm{Pic}_{X/k}(k) = \mathrm{Pic}(X)$ we have*

$$(f+g)^*\mathscr{L} \simeq f^*\mathscr{L} \otimes g^*\mathscr{L}.$$

Proof. By Theorem 3.21 the morphism $\phi_{\mathscr{L}}$ is zero, so $\Lambda(\mathscr{L}) = m^*\mathscr{L} \otimes p_1^*\mathscr{L}^{-1} p_2^*\mathscr{L}^{-1}$ is trivial on $X \times X$. Pulling back by $(f, g) : T \to X \times X$ gives the desired result. ■

Corollary 3.24. *If $\mathscr{L} \in \mathrm{Pic}^0_{X/k}(k)$ then $[n]_X^*\mathscr{L} \simeq \mathscr{L}^{\otimes n}$.*

Proof. Use induction on n and Proposition 3.23. ■

Theorem 3.25. *If $\mathscr{L}$ is an ample invertible sheaf on X then the kernel $K(\mathscr{L})$ of $\phi_{\mathscr{L}} : X \to \mathrm{Pic}^0_{X/k}$ is a finite k-group scheme.*

Proof. See [5, II, 2.17]. ■

We can now finally show that $\mathrm{Pic}_{X/k}$ is smooth when X is an abelian variety.

Theorem 3.26. *Let X be an abelian variety. Then $\mathrm{Pic}_{X/k}$ is smooth and $\mathrm{Pic}^0_{X/k}$ is an abelian variety of the same dimension as X.*

Proof. Since X is projective, there exists an ample invertible sheaf $\mathscr{L}$ on X. Since $\mathrm{Pic}_{X/k}$ is a k-group locally of finite type, it is pure-dimensional. Theorem 3.25 implies that the morphism $\phi_{\mathscr{L}} : X \to \mathrm{Pic}^0_{X/k}$ has finite kernel, from which it follows that $\dim \mathrm{Pic}^0_{X/k} \geq \dim X = g$. Proposition 3.18 and Theorem 3.11 show that $g \geq \dim_k H^1(X, \mathscr{O}_X) \geq \dim \mathrm{Pic}^0_{X/k}$. Combining these, we find that

$$g = \dim X = \dim \mathrm{Pic}^0_{X/k} = \dim_k H^1(X, \mathscr{O}_X) = \dim_k T_{\mathrm{Pic}_{X/k},0},$$

where $T_{\mathrm{Pic}_{X/k},0}$ is the tangent space at the origin. We conclude that $0 \in \mathrm{Pic}^0_{X/k}$ is a smooth point, and since $\mathrm{Pic}_{X/k}$ is a k-group locally of finite type, that $\mathrm{Pic}_{X/k}$ is k-smooth. By Theorem 3.10, the open subgroup $\mathrm{Pic}^0_{X/k}$ is a proper geometrically connected and smooth k-group, so it is a proper group variety over k. ■

Definition 3.27. Let X be an abelian variety. The *dual abelian variety*, denoted X^t, is the abelian variety $\mathrm{Pic}^0_{X/k}$.

Corollary 3.28. *For $1 \leq i \leq g$ cup product induces an isomorphism $\wedge^i H^1(X, \mathscr{O}_X) \xrightarrow{\sim} H^i(X, \mathscr{O}_X)$. In particular, $\dim_k H^1(X, \mathscr{O}_X) = \binom{g}{i}$.*

Proof. In the proof of Theorem 3.26 we showed that $\dim_k H^1(X, \mathscr{O}_X) = g$. Now apply Corollary 3.17 to get the first statement, remembering that the multiplication on $H = \oplus_i H^i(X, \mathscr{O}_X)$ is cup product. The second statement is immediate from the first. ■

Let $f : X \to Y$ be a map of abelian varieties. Then $f \times 1 : X \times Y^t \to Y \times Y^t$ is another such map, and we can consider the pullback of the $(e_Y \times \mathrm{id}_{Y^t})$-rigidified Poincaré sheaf $(\mathscr{P}^0, \nu^0)_Y$ for Y along $f \times 1$. This gives an $(e_X \times \mathrm{id}_{Y^t})$-rigidified invertible sheaf $(f \times 1)^*(\mathscr{P}^0, \nu^0)_Y$ on $X \times Y^t$, so there is a unique morphism of k-schemes $f^t : Y^t \to X^t$ satisfying $(1 \times f^t)^*(\mathscr{P}^0, \nu^0)_X \simeq (f \times 1)^*(\mathscr{P}^0, \nu^0)_Y$. Note that since $(\mathscr{P}^0, \nu^0)_Y$ restricts to $\mathscr{O}_Y$ along the zero-section of Y^t we have $f^t(0) = 0$. Thus, by Corollary 1.7, f^t is a k-group map.

Definition 3.29. The map $f^t : Y^t \to X^t$ of abelian varieties is the *dual morphism.*

Concretely, on T-points f^t is induced by is just pullback along $f \times 1 : X \times T \to Y \times T$. Taking $T = \mathrm{Spec}\,\overline{k}$, we conclude by Corollary 3.24 that $[n]_X^t = [n]_{X^t}$, and more generally by Proposition 3.23 that $(f+g)^t = f^t + g^t$. In particular, by Theorem 2.10 we see that f^t is an isogeny if f is.

Theorem 3.30. *If $f : X \to Y$ is an isogeny of abelian varieties then $f^t : Y^t \to X^t$ is again an isogeny, and there is a canonical isomorphism*

$$\ker(f^t) \xrightarrow{\sim} \ker(f)^D,$$

where for a finite locally free commutative group scheme G over a scheme S,

$$G^D = \underline{\mathrm{Hom}}(G, \mathbf{G}_{\mathrm{m}})$$

is the Cartier dual.

Proof. See [9, Theorem 1.1, Corollary 1.3]. ■

The isomorphism in Theorem 3.30 is induced by the functorial, bilinear pairing

$$e : \ker(f) \times \ker(f^t) \to \mathbf{G}_{\mathrm{m}}$$

given on T-points as follows. Let $x \in Y(T)$ be such that $f_T(x) = 0$ and let $\mathscr{L}$ be an invertible sheaf on Y_T with $f^*\mathscr{L}$ trivial on X_T and fix a trivialization $\iota : f^*\mathscr{L} \xrightarrow{\sim} \mathscr{O}_{X_T}$. Since $f_T(x) = 0$, the diagram

$$\begin{array}{ccc} X_T & \xrightarrow{t_x} & X_T \\ & {\scriptstyle f_T}\searrow \quad \swarrow{\scriptstyle f_T} & \\ & Y_T & \end{array}$$

commutes, and it follows that we have an isomorphism

$$\mathscr{O}_{X_T} \xrightarrow[\sim]{\iota^{-1}} f_T^*\mathscr{L} \simeq t_x^* f_T^*\mathscr{L} \xrightarrow[\sim]{t_x^*(\iota)} t_x^*\mathscr{O}_{X_T} \simeq \mathscr{O}_{X_T} \tag{1}$$

which must be multiplication by a unit $u \in \Gamma(X_T, \mathscr{O}_{X_T}^\times) = \Gamma(T, \mathscr{O}_T^\times) = \mathbf{G}_{\mathrm{m}}(T)$. We define $e(x, \mathscr{L}) = u$. Observe that this is independent of change in ι, as any such change must be via multiplication by a unit $s \in \Gamma(T, \mathscr{O}_T)$, and this does not effect the isomorphism (1).

Let $\mathscr{P}_X$ on $X \times X^t$ be the Poincaré sheaf. Observe that the restriction of $\mathscr{P}_X$ to $X \times \{0\}$ is $\mathscr{O}_X$: this follows from the fact that it induces the morphism $0 \to X^t$. As any two rigidifications of $\mathscr{P}_X$ along $X \times \{0\}$ differ by a unique $k^\times$-multiple, there is a *unique* rigidification of $\mathscr{P}_X$ along $X \times \{0\}$ that agrees when restricted to $\{0\} \times \{0\}$ with the rigidification ν along $\{0\} \times X^t$ that comes with $\mathscr{P}_X$. This rigidified sheaf induces a morphism of k-varieties

$$\kappa_X : X \to X^{tt}$$

satisfying $\kappa_X(0) = 0$ (since the pullback of $(1 \times \kappa_X)^*\mathscr{P}_{X^t}$ to $\{0\} \times X$ along $(0 \times \mathrm{id}_X) : 0 \times X \to X^t \times X$ is trivial). Thus, κ_X is a homomorphism. It is clearly natural in X.

Theorem 3.31. *Let X be an abelian variety. The map κ_X is an isomorphism, and "triple duality" holds: $\kappa_X^t = \kappa_{X^t}^{-1}$.*

Proof. We follow [5, pg. 92]. For abelian varieties A, B, let $s : A \times B \to B \times A$ be the morphism switching the two factors, and fix an invertible sheaf $\mathscr{L}$ on X. There is a canonical isomorphism $s^*\Lambda(\mathscr{L}) \simeq \Lambda(\mathscr{L})$ as follows easily from the definition of $\Lambda(\mathscr{L})$. For any k-scheme T and $x \in X(T)$, the morphism $\phi_{\mathscr{L}}$ takes x to the class of

$$\begin{aligned}(X \times T \xrightarrow{\mathrm{id} \times x} X \times X)^*\Lambda(\mathscr{L}) &\simeq (X \times T \xrightarrow{\mathrm{id} \times x} X \times X \xrightarrow{s} X \times X)^*\Lambda(\mathscr{L}) \\ &\simeq (X \times T \xrightarrow{\mathrm{id} \times x} X \times X \xrightarrow{s} X \times X \xrightarrow{\mathrm{id} \times \phi_{\mathscr{L}}} X \times X^t)^*\mathscr{P}_X \\ &\simeq (X \times T \xrightarrow{\phi_{\mathscr{L}} \times \mathrm{id}} X^t \times T \xrightarrow{\mathrm{id} \times x} X^t \times X \xrightarrow{s} X \times X^t)^*\mathscr{P}_X,\end{aligned}$$

and since $\kappa_X(x)$ corresponds to the sheaf $(X^t \times T \xrightarrow{\mathrm{id} \times x} X^t \times X)^* s^*\mathscr{P}_X$ and $\phi_{\mathscr{L}}^t$ is given by pullback along $X \times T \xrightarrow{\phi_{\mathscr{L}} \times \mathrm{id}} X^t \times T$, the above sheaf is in the class of $\phi_{\mathscr{L}}^t \circ \kappa_X(x)$. This shows that

$$\phi_{\mathscr{L}} = \phi_{\mathscr{L}}^t \circ \kappa_X. \tag{2}$$

As we noted in Definition 3.20, any two rigidifications of $\Lambda(\mathscr{L})$ differ by a unique $k^\times$-multiple. Thus, if the isomorphisms above are not *a priori* isomorphisms of rigidified sheaves, they can be altered by a unique unit scalar to respect the rigidifications. This is why we need not track the rigidifying data in the string of isomorphisms above.

Now let $\mathscr{L}$ be an ample invertible sheaf on X. Then by Theorem 3.25, the kernel $K(\mathscr{L})$ of $\phi_{\mathscr{L}}$ is a finite group scheme, and since $\phi_{\mathscr{L}}^t$ is an isogeny, we see by (2) that κ_X is also an isogeny. Using Theorem 3.30, we compute

$$\mathrm{rank}(K(\mathscr{L})) = \deg(\phi_{\mathscr{L}}) = \deg(\phi_{\mathscr{L}}^t) \cdot \deg(\kappa_X) = \mathrm{rank}(K(\mathscr{L})^D) \cdot \deg(\kappa_X) = \mathrm{rank}(K(\mathscr{L})) \cdot \deg(\kappa_X),$$

so $\deg(\kappa_X) = 1$ and κ_X is an isomorphism.

Finally, we must show $\kappa_{X^t}^{-1} = \kappa_X^t$. By the characterization of the dual morphism, this says

$$(1_X \times \kappa_{X^t}^{-1})^* \mathscr{P}_X \simeq (\kappa_X \times 1_{X^{ttt}})^* \mathscr{P}_{X^{tt}},$$

or equivalently

$$(1_X \times \kappa_{X^t})^* (\kappa_X \times 1_{X^{ttt}})^* \mathscr{P}_{X^{tt}} \simeq \mathscr{P}_X.$$

Letting $s_A : A \times A^t \simeq A^t \times A$ denote the flip isomorphism as above, the left side is isomorphic to

$$\begin{aligned}(\kappa_X \times 1_{X^t})^* (1_{X^{tt}} \times \kappa_{X^t})^* \mathscr{P}_{X^{tt}} &\simeq (\kappa_X \times 1_{X^t})^* s_{X^t}^* \mathscr{P}_{X^t} \\ &\simeq s_X^* (1_{X^t} \times \kappa_X)^* \mathscr{P}_{X^t} \\ &\simeq s_X^* ((s_X^{-1})^* \mathscr{P}_X) \\ &\simeq \mathscr{P}_X,\end{aligned}$$

where we have used the definition of κ_X in the first and third isomorphisms above, and this is what we wanted to show. ■

Remark 3.32. Via the double-duality isomorphism κ_X, the equality (2) may be rephrased as "$\phi_{\mathscr{L}} = \phi_{\mathscr{L}}^t$."

Theorem 3.33. *Let $f : X \to Y$ be an isogeny with kernel Z. Then there is a canonical exact sequence*

$$0 \to Z^D \to Y^t \xrightarrow{f^t} X^t \to 0.$$

Proof. This follows from Theorem 3.30. ■

Remark 3.34. Many of the properties of the dual abelian variety can be summarized as follows. If X, Y are abelian varieties, then the functor $\mathfrak{Sch}/k \to \mathfrak{Ab}$ given by

$$T \mapsto \mathrm{Hom}_T(X_T, Y_T)$$

is representable by a commutative étale k-group scheme, $\underline{\mathrm{Hom}}(X, Y)$, and the map

$$\underline{\mathrm{Hom}}(X, Y) \to \underline{\mathrm{Hom}}(Y^t, X^t)$$

given on points by $f \mapsto f^t$ is a homomorphism of k-group schemes; in particular, $(f+g)^t = f^t + g^t$ and $[n]_X^t = [n]_{X^t}$. See [5, 7.12] for more details.

4. The Tate module and Weil pairings

4.1. The Tate module. Let ℓ be a prime different from $\mathrm{char}(k)$. We have a homomorphism of group schemes

$$\ell : X[\ell^{n+1}] \to X[\ell^n]$$

which gives a $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-equivariant homomorphism of Galois modules

$$\ell : X[\ell^{n+1}](k^{\mathrm{sep}}) \to X[\ell^n](k^{\mathrm{sep}}).$$

These homomorphisms form a projective system of Galois modules.

Definition 4.2. For an abelian variety X/k and a prime $\ell \neq \mathrm{char}(k)$, the *$\ell$-adic Tate module* is

$$T_\ell X \stackrel{\mathrm{def}}{=} \varprojlim_n X[\ell^n](k^{\mathrm{sep}}),$$

with the projective limit taken in the category of $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-modules with respect to the maps above.

The Tate module of an abelian variety X is an extremely useful tool for proving certain finiteness theorems regarding X.

Let $g = \dim X$. By Corollary 2.5, we know that $X[n](k^{\mathrm{sep}}) \simeq (\mathbf{Z}/n\mathbf{Z})^{2g}$ noncanonically, whence $T_\ell X$ is a free $\mathbf{Z}_\ell$-module of rank $2g$. Thus, we may also define

$$V_\ell X \stackrel{\mathrm{def}}{=} \mathbf{Q}_\ell \otimes_{\mathbf{Z}_\ell} T_\ell X.$$

Since multiplication by ℓ commutes with any homomorphism $f : X \to Y$ of abelian varieties, we obtain a map $T_\ell f : T_\ell X \to T_\ell Y$, hence also a map $V_\ell X \to V_\ell Y$, which we denote by $V_\ell f$.

Theorem 4.3. *Let $f : X \to Y$ be an isogeny of abelian varieties with kernel N. Then there is a natural exact sequence*

$$0 \to T_\ell X \xrightarrow{T_\ell f} T_\ell Y \to N_\ell(k^{\mathrm{sep}}) \to 0,$$

where $N_\ell(k^{\mathrm{sep}})$ is the ℓ-primary part of $N(k^{\mathrm{sep}})$. In particular, $V_\ell f : V_\ell X \to V_\ell Y$ is an isomorphism.

Proof. Since

$$0 \to N_\ell(k^{\mathrm{sep}}) \to X[\ell^\infty](k^{\mathrm{sep}}) \to Y[\ell^\infty](k^{\mathrm{sep}}) \to 0$$

is exact (as $X(k^{\mathrm{sep}})$ is ℓ-divisible), and $X[\ell^\infty](k^{\mathrm{sep}}) \simeq (\mathbf{Q}_\ell/\mathbf{Z}_\ell)^{2\dim X}$ is $\mathbf{Z}_\ell$-injective, applying $\mathrm{Hom}_{\mathbf{Z}_\ell}(\mathbf{Q}_\ell/\mathbf{Z}_\ell, -)$ gives an exact sequence

$$0 \to T_\ell X \to T_\ell Y \to \mathrm{Ext}^1(\mathbf{Q}_\ell/\mathbf{Z}_\ell, N_\ell(k^{\mathrm{sep}})) \to 0.$$

Since $N_\ell(k^{\mathrm{sep}})$ is killed by some ℓ^r, and ℓ^r acts as an automorphism on $\mathbf{Q}_\ell$, we conclude that $\mathrm{Ext}^1_{\mathbf{Z}_\ell}(\mathbf{Q}_\ell, N_\ell(k^{\mathrm{sep}})) = 0$ for reasons of bifunctoriality, and hence the connecting map

$$N_\ell(k^{\mathrm{sep}}) = \mathrm{Hom}_{\mathbf{Z}_\ell}(\mathbf{Z}_\ell, N_\ell(k^{\mathrm{sep}})) \xrightarrow{\delta} \mathrm{Ext}^1(\mathbf{Q}_\ell/\mathbf{Z}_\ell, N_\ell(k^{\mathrm{sep}}))$$

induced by

$$0 \to \mathbf{Z}_\ell \to \mathbf{Q}_\ell \to \mathbf{Q}_\ell/\mathbf{Z}_\ell \to 0$$

is an isomorphism. ■

Define

$$\mathbf{Z}_\ell(1) = \varprojlim_n \mu_{\ell^n}(k^{\mathrm{sep}}),$$

with the transition maps given by ℓ^{th}-power. Note that this is a free $\mathbf{Z}_\ell$ module of rank 1 endowed with a continuous action of $\mathrm{Gal}(k^{\mathrm{sep}}/k)$.

Theorem 4.4. *If X is an abelian variety then there is a canonical isomorphism of $\mathbf{Z}_\ell[\mathrm{Gal}(k^{\mathrm{sep}}/k)]$-modules*

$$T_\ell X^t \simeq (T_\ell X)^\vee \otimes_{\mathbf{Z}_\ell} \mathbf{Z}_\ell(1).$$

Proof. By Theorem 3.30, there are canonical isomorphisms of Galois-modules

$$X^t[\ell^n](k^{\mathrm{sep}}) \simeq \mathrm{Hom}(X[\ell^n](k^{\mathrm{sep}}), \mathbf{G}_{\mathrm{m}}(k^{\mathrm{sep}})) = \mathrm{Hom}(X[\ell^n](k^{\mathrm{sep}}), \mu_{\ell^n}(k^{\mathrm{sep}})),$$

so taking projective limits gives the desired result. ■

Theorem 4.5. *Let X, Y be abelian varieties. Then the natural map*

$$\mathbf{Z}_\ell \otimes \mathrm{Hom}_k(X, Y) \to \mathrm{Hom}_{\mathbf{Z}_\ell[\mathrm{Gal}(k^{\mathrm{sep}}/k)]}(T_\ell X, T_\ell Y)$$

is injective.

Proof. We may assume $k = \overline{k}$. See [6, §19, Theorem 3], which is the same as the argument for elliptic curves. ■

Corollary 4.6. *Let X, Y be abelian varieties. Then $\mathrm{Hom}_k(X, Y)$ is a free $\mathbf{Z}$-module of rank at most $4\dim X \dim Y$.*

Proof. Since $T_\ell X$ and $T_\ell Y$ are free $\mathbf{Z}_\ell$-modules of ranks $2\dim X$ and $2\dim Y$ respectively, $\mathrm{Hom}_{\mathbf{Z}_\ell}(T_\ell X, T_\ell Y)$ is a finite, free $\mathbf{Z}_\ell$-module of rank $4\dim X \dim Y$. In the proof of [6, §19, Theorem 3], Mumford shows that $\mathrm{Hom}_{\overline{k}}(X_{\overline{k}}, Y_{\overline{k}})$ is finitely generated as a $\mathbf{Z}$-module (via exactly the same methods as for elliptic curves). The rank bound then follows from Theorem 4.5. ■

Observe that the continuous action of $\mathrm{Gal}(k^{\mathrm{sep}}/k)$ on $T_\ell X$ gives rise to a continuous ℓ-adic representation

$$\rho_\ell : \mathrm{Gal}(k^{\mathrm{sep}}/k) \to \mathrm{GL}(T_\ell X).$$

4.7. **The Weil pairing.** Let $f : X \to Y$ be an isogeny of abelian varieties. By Theorem 3.30, there is a canonical isomorphism $\beta : \ker(f^t) \xrightarrow{\sim} \ker(f)^D$, or in other words, a canonical perfect bilinear pairing of finite flat group schemes

$$\overline{e}_f : \ker(f) \times \ker(f^t) \to \mathbf{G}_{\mathrm{m}}$$

given by $\overline{e}_f(x, y) \stackrel{\text{def}}{=} \beta(y)(x)$. If $n \in \mathbf{Z}$ kills $\ker(f)$ then by perfectness (or the proof of Theorem 2.10) it also kills $\ker(f^t)$ and $\overline{e}_f$ takes values in μ_n.

Definition 4.8. Let X/k be an abelian variety. For a positive integer n, the *Weil n-pairing* is

$$\overline{e}_n = \overline{e}_{n,X} \stackrel{\text{def}}{=} \overline{e}_{[n]_X} : X[n] \times X^t[n] \to \mu_n.$$

We would like to give a concrete description of $\overline{e}_n$ on k-points when $\mathrm{char}(k) \nmid n$. Let $x \in X[n](k)$ and $y \in X^t[n](k)$. Then y is an invertible rigidified sheaf $\mathscr{L} \in \mathrm{Pic}^0_{X/k}(k)$ with $\mathscr{L}^{\otimes n}$ trivial (as a rigidified sheaf). By Corollary 3.24, we have that $n^*\mathscr{L} \simeq \mathscr{L}^{\otimes n}$ is trivial. If we let D be a Weil divisor such that $\mathscr{L} \simeq \mathscr{O}_X(D)$, then $\mathscr{L}^{\otimes n} \simeq \mathscr{O}_X(nD)$ and $[n]^*\mathscr{L} \simeq \mathscr{O}_X([n]^{-1}D)$, so nD and $[n]_X^{-1}D$ are linearly equivalent to 0. It follows that there are functions $f, g \in k(X)^\times$ with $(f) = nD$ and $(g) = [n]_X^{-1}D$. Thus,

$$(f \circ [n]_X) = [n]_X^{-1}(f) = [n]_X^{-1}(nD) = n([n]_X^{-1}D) = n(g) = (g^n),$$

from which it follows that $g^n/(f \circ [n]_X) = \alpha \in k^\times$ Thus, for any $u \in X(\overline{k})$

$$g(u + x)^n = \alpha f(nu + nx) = \alpha f(nu) = g(u)^n,$$

so

$$\frac{g}{g \circ t_x} \in \mu_n(\overline{k}) \cap k(X)^\times = \mu_n(k).$$

Theorem 4.9. *Let $g \in k(X)^\times$ be any function such that $(g) = nD$, where $y = \mathscr{L}(D)$. Then*

$$\overline{e}_n(x, y) = \frac{g}{g \circ t_x} \in \mu_n(k).$$

Proof. We can assume $k = \overline{k}$. See [6, §20] for this case. ■

Proposition 4.10. *Let X/k be an abelian variety and let m, n be integers not divisible by* $\mathrm{char}(k)$. *Choose $x \in X[mn](k^{\mathrm{sep}})$, $y \in X^t[mn](k^{\mathrm{sep}})$. Then*

$$\overline{e}_n(mx, my) = \overline{e}_{mn}(x, y)^m.$$

Proof. We may assume $k = \overline{k}$, and this case is addressed in [6, §20]. The result may also be proved as in [4, §16], by appealing to the explicit description of $\overline{e}_{mn}$ in Theorem 4.9. ■

Letting $n = \ell^r$ and $m = \ell$ for a prime $\ell \neq \mathrm{char}(k)$, we obtain the commutative diagram

$$\begin{array}{ccc} X[\ell^{r+1}](k^{\mathrm{sep}}) \times X^t[\ell^{r+1}](k^{\mathrm{sep}}) & \xrightarrow{\overline{e}_{\ell^{r+1}}} & \mu_{\ell^{r+1}}(k^{\mathrm{sep}}) \\ \downarrow{\scriptstyle \ell\times\ell} & & \downarrow{\scriptstyle \ell} \\ X[\ell^r](k^{\mathrm{sep}}) \times X^t[\ell^r](k^{\mathrm{sep}}) & \xrightarrow{\overline{e}_{\ell^r}} & \mu_{\ell^r}(k^{\mathrm{sep}}) \end{array}$$

of Galois-modules, and hence by passing to the limit we obtain a pairing

$$e_\ell = e_{\ell,X} : T_\ell(X) \times T_\ell(X^t) \to \mathbf{Z}_\ell(1).$$

Proposition 4.11. *Let X/k be an abelian variety and choose a positive integer n not divisible by* $\mathrm{char}(k)$. *Then*

(1) *The pairing e_ℓ is $\mathbf{Z}_\ell$-bilinear and perfect for any prime $\ell \neq$* $\mathrm{char}(k)$.

(2) *If $f : X \to Y$ is a homomorphism of abelian varieties then for any $x \in X[n](k^{\mathrm{sep}})$ and $y \in Y^t[n](k^{\mathrm{sep}})$*

$$\overline{e}_n(x, f^t(y)) = \overline{e}_n(f(x), y).$$

(3) *For any prime $\ell \neq$* $\mathrm{char}(k)$ *and any f as in* (2),

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

Proof. We can assume $k = \overline{k}$. See [6, §20]. ■

Remark 4.12. See [9, Section 1] for a discussion of properties of the Weil pairing on torsion-levels possibly divisible by $\mathrm{char}(k)$.

5. The Weil conjectures

Let κ be a finite field of size q and κ_n an extension of κ of degree n.

Definition 5.1. Let X/κ be κ-scheme of finite type. We define the *zeta function* of X to be

$$Z_X(t) \stackrel{\text{def}}{=} \prod_{x\in X^0} (1 - t^{\deg_\kappa(x)})^{-1} \in \mathbf{Z}[[t]],$$

with X^0 the set of closed points in X.

Since

$$\#X(\kappa_m) = \sum_{d|m} d^{\#\{x\in X^0\ :\ \deg_\kappa(x)=d\}},$$

one also has

$$Z_X(t) = \exp\left(\sum_{m\geq 1} \#X(\kappa_m)\frac{t^m}{m}\right).$$

Here, κ_m is "the" degree-m extension of κ.

Let X/κ be a smooth projective κ-variety of dimension g. In 1949, A. Weil made the following conjectures:

(1) (Rationality) $Z_X(t) \in \mathbf{Q}(t)$.

(2) (Functional Equation) Let $\chi = \Delta.\Delta$ be the self-intersection number of $\Delta \subseteq X \times X$. Then

$$Z_X\left(\frac{1}{q^g t}\right) = \pm q^{g\chi/2} t^\chi Z_X(t).$$

(3) (Riemann Hypothesis) One has

$$Z_X(t) = \frac{P_1(t)\cdots P_{2g-1}(t)}{P_0(t)\cdots P_{2g}(t)},$$

where $P_0(t) = 1 - t$, $P_{2g}(t) = 1 - q^g t$ and for $1 \leq r \leq 2g-1$,

$$P_r(t) = \prod_{i=1}^{\beta_r}(1 - a_{i,r}t) \in \mathbf{Z}[t]$$

for certain algebraic integers $a_{i,r}$ with absolute value $q^{r/2}$ under all embeddings into $\mathbf{C}$.

These statements were proved for curves and abelian varieties by A. Weil in 1948, and in general by B. Dwork, A. Grothendieck, M. Artin, and P. Deligne (and later by Deligne for *any* κ-proper variety X) during 1964–1974.

Let X be an abelian variety over a field k and fix a prime $\ell \neq \mathrm{char}(k)$. Any $\alpha \in \mathrm{End}_k^0(X)$ acts on the $\mathbf{Q}_\ell$-vector space $V_\ell X$ as the homomorphism of rings $T_\ell : \mathrm{End}_k(X) \to \mathrm{End}_{\mathbf{Z}_\ell} T_\ell(X)$ extends to a homomorphism

$$V_\ell : \mathrm{End}_k^0(X) \to \mathrm{End}_{\mathbf{Q}_\ell}(V_\ell(X)).$$

Let $P_{\alpha,\ell}(t)$ be the characteristic polynomial of α acting on $V_\ell(X)$. *A priori*, $P_{\alpha,\ell}$ depends on ℓ, is monic of degree $2\dim X$, and has coefficients in $\mathbf{Q}_\ell$.

Theorem 5.2. *The polynomial* $P_\alpha \stackrel{def}{=} P_{\alpha,\ell}$ *is independent of* ℓ *and has coefficients in* $\mathbf{Q}$. *If* $\alpha \in \mathrm{End}_k(X)$ *then* P_α *has integer coefficients and is monic. Moreover, for any integer* n *we have*

$$P_\alpha(n) = \deg(\alpha - n),$$

where the degree function $\deg : \mathrm{End}_k^0(X) \to \mathbf{Q}$ *is extended from the usual degree map* $\mathrm{End}_k(X) \to \mathbf{Z}$ *by using the quadratic property* $\deg(nf) = n^{2\dim X}\deg(f)$ *for any* $f \in \mathrm{End}_k(X)$ *and* $n \in \mathbf{Z}$.

Proof. We refer to [6, §19] for a proof when $k = \overline{k}$, which suffices. ■

Definition 5.3. The polynomial $P_\alpha(t)$ is called the *characteristic polynomial* of α, the coefficient of $-t^{2\dim X-1}$ is the *trace* of α, denoted $\mathrm{Tr}(\alpha)$, and the constant term of $P_\alpha(t)$ is the *norm* of α, denoted $\mathrm{Nm}(\alpha)$. These are the trace and determinant of $V_\ell(\alpha)$ acting on $V_\ell X$.

Fix an ample invertible sheaf $\mathscr{L}$ on X and let $\phi_{\mathscr{L}} : X \to X^t$ be the corresponding homomorphism; it is an isogeny as it has finite kernel and $\dim X = \dim X^t$. Let $\phi_{\mathscr{L}}^{-1} \in \mathrm{Hom}(X^t, X) \otimes \mathbf{Q}$ be the inverse of $\phi_{\mathscr{L}}$.

Definition 5.4. The *Rosati involution* on $\mathrm{End}_k^0(X)$ with respect to $\mathscr{L}$ (or to $\phi_{\mathscr{L}}$) is the morphism

$$\alpha \mapsto \alpha' = \phi_{\mathscr{L}}^{-1} \circ \alpha^t \circ \phi_{\mathscr{L}}$$

The Rosati involution is an involution because of Remark 3.32 and it has the following properties (see [6, §20]):

(1) If $\alpha, \beta \in \mathrm{End}_k^0(X)$ and $a \in \mathbf{Q}$ then $(a\alpha)' = a\alpha'$, $(\alpha+\beta)' = \alpha' + \beta'$, and $(\alpha\beta)' = \beta'\alpha'$.
(2) If $\ell \neq \mathrm{char}(k)$ then for any $x, y \in V_\ell X$,

$$e_\ell(\alpha x, T_\ell(\phi_{\mathscr{L}})y) = e_\ell(x, T_\ell(\phi_{\mathscr{L}})\alpha' y).$$

(3) The map $\mathrm{End}_k^0(X) \to \mathbf{Q}$ given by $\alpha \mapsto \mathrm{Tr}(\alpha\alpha')$ is a positive-definite quadratic form.

Proposition 5.5. *Let X be an abelian variety and suppose $\alpha \in \mathrm{End}(X)$ satisfies $\alpha'\alpha = a \in \mathbf{Z}$, so $a \geq 0$. Then any root of the characteristic polynomial P_α of α has absolute value $a^{1/2}$ under every embedding into $\mathbf{C}$.*

The proof of Proposition 5.5 will make use of the following lemma:

Lemma 5.6. *Let K be a number field with an involution σ such that for all $x \in K^\times$ one has $\mathrm{Tr}_{K/\mathbf{Q}}(x \cdot \sigma(x)) > 0$. Then K is totally real with $\sigma = \mathrm{id}$ or a CM field with σ acting as complex conjugation.*

Proof. Let $F = K^\sigma$ denote the fixed field of σ. Let r be the number of real embeddings of F, and s the number of complex conjugate pairs of complex embeddings of F. Then there is an isomorphism of $\mathbf{R}$-algebras

$$\mathbf{R} \otimes_{\mathbf{Q}} F \xrightarrow{\sim} \mathbf{R}^r \times \mathbf{C}^s,$$

so $x \mapsto \mathrm{Tr}_{F/\mathbf{Q}}(x^2)$ has signature $(r+s, s)$. Since $\mathrm{Tr}_{F/\mathbf{Q}} = \frac{1}{2}\mathrm{Tr}_{K/\mathbf{Q}}$ on F, the positive-definiteness of $\mathrm{Tr}_{K/\mathbf{Q}}$ ensures that $\mathrm{Tr}_{F/\mathbf{Q}}(x^2) = \mathrm{Tr}_{F/\mathbf{Q}}(x \cdot \sigma x) > 0$ for all $x \in F^\times$, from which it follows that $s = 0$ and hence that F is totally real.

If $K \neq F$, then $K = F(\sqrt{a})$ for some $a \in F^\times$ with $\sigma(\sqrt{a}) = -\sqrt{a}$. Observe that

$$\mathbf{R} \otimes_{\mathbf{Q}} K \simeq (\mathbf{R} \otimes_{\mathbf{Q}} F) \otimes_F K \simeq \prod_\tau \mathbf{R}_\tau \otimes_F K,$$

where the product runs over all embeddings of F, and $\mathbf{R}_\tau$ is $\mathbf{R}$ considered as an F-algebra via τ. Since $\mathbf{R}_\tau \otimes_F K$ is isomorphic to $\mathbf{R} \times \mathbf{R}$ or to $\mathbf{C}$, with σ switching the factors in the first case ($\tau(\alpha) > 0$) and acting as complex conjugation in the second ($\tau(\alpha) < 0$), we see (again using that $\mathrm{Tr}(x \cdot \sigma x) > 0$ for $x \in K^\times$) that the first case cannot occur, and hence that K/F is a purely imaginary extension with σ acting as complex conjugation. ■

Proof of Proposition 5.5. Since $P_\alpha(t) \in \mathbf{Z}[t]$, it will suffice to show that every root of $P_\alpha(t)$ has absolute value $a^{1/2}$. By the positive definiteness of the Rosati involution, if $a = 0$ then $\alpha = 0$. Thus, we may assume $a > 0$ so α is an isogeny. The algebra $\mathbf{Q}[\alpha]$ is finitely generated so $\alpha^{-1} \in \mathbf{Q}[\alpha]$, and since $\alpha' = a\alpha^{-1}$ we see that $\mathbf{Q}[\alpha]$ is stable under the Rosati involution. Let Q_β be the minimal polynomial an element $\beta \in \mathbf{Q}[\alpha]$. We claim that P_β and Q_β have the same roots in $\overline{\mathbf{Q}}$. Indeed, since P_β has $\mathbf{Q}$-coefficients and $P_\beta(\beta) = 0$, we have $Q_\beta | P_\beta$. On the other hand, since P_β is the characteristic polynomial of $T_\ell(\beta) \in \mathrm{End}(T_\ell X)$, any root $\xi \in \overline{\mathbf{Q}}_\ell$ of P_β is an eigenvalue of $T_\ell(\beta)$ so $Q_\beta(\xi)$ is an eigenvalue of $T_\ell(Q_\beta(\beta)) = T_\ell(0) = 0$. Therefore $Q_\beta(\xi) = 0$. We conclude that P_β and Q_β have the same roots in $\overline{\mathbf{Q}}$. In particular, as P_β and Q_β have $\mathbf{Z}$-coefficients, we must in fact have $P_\beta = Q_\beta^{n_\beta}$ for some positive integer n_β. In particular, $n_\beta | 2\dim X$ for all β.

The restriction of the positive-definite bilinear form $(\beta, \gamma) \mapsto \mathrm{Tr}(\beta\gamma')$ to $\mathbf{Q}[\alpha]$ is positive-definite, so $e' = e$ for all primitive idempotents $e \in \mathbf{Q}[\alpha]$ and $\mathbf{Q}[\alpha]$ is semisimple. Thus, $\mathbf{Q}[\alpha]$ is isomorphic to a product of number fields

$$\mathbf{Q}[\alpha] \simeq K_1 \times \cdots \times K_r$$

with the factor decomposition preserved by the Rosati involution.

The identity $P_\beta = Q_\beta^{n_\beta}$ for $\beta \in \mathbf{Q}[\alpha]$ in the first paragraph now shows (by taking β in the Zariski-dense set of elements that primitively generate $\mathbf{Q}[\alpha]$ with components $\beta_i \in K_i$ having pairwise distinct minimal polynomials over $\mathbf{Q}$) that

$$\mathrm{Tr}\big|_{\mathbf{Q}[\alpha]} = \frac{2\dim X}{\dim_{\mathbf{Q}} \mathbf{Q}[\alpha]} \sum \mathrm{Tr}_{K_i/\mathbf{Q}}.$$

Thus, by Lemma 5.6, we see that each K_i is either totally real with the Rosati involution acting as the identity, or a totally imaginary extension of a totally real field with the Rosati involution acting as complex conjugation. Since the roots of $P_\alpha(t)$ are the images of α under the embeddings ϕ_j of each K_i into $\mathbf{C}$ (as P_α and Q_α have the same complex roots) and since

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

we conclude that the roots of P_α have absolute value $a^{1/2}$ under all embeddings into $\mathbf{C}$, as desired. ■

Theorem 5.7. *Let X/κ be an abelian variety over a finite field of size q, and* $\mathrm{Frob}_{X,q}$ *the Frobenius q-endomorphism of X/κ. Let $P = P_{\mathrm{Frob}_{X,q}}$ have roots $a_1, \ldots, a_{2g}$ where $2g = \dim X$. Then*

$$\#X(\kappa_m) = \prod_{i=1}^{2g} (1 - a_i^m)$$

and

$$|a_i| = q^{1/2}.$$

Proof. Since for any morphism $f : Z \to W$ of κ-schemes one has

$$f \circ \mathrm{Frob}_{Z,q} = \mathrm{Frob}_{W,q} \circ f,$$

it follows that the fixed points of $\mathrm{Frob}_{X,q}^m - 1$ acting on $X(\overline{\kappa})$ are precisely the points $X(\kappa_m)$ since κ_m is the set of solutions to $t^{q^m} = t$ in $\overline{\kappa}$.

Now $(d\,\mathrm{Frob}_{X,q}^m)\big|_0 : T_0 X \to T_0 X$ is the zero map, as $Df^{q^m} = 0$ for any derivation D of a ring A of characteristic p and any $f \in A$. Thus, $d(\mathrm{Frob}_{X,q}^m - 1) = -1$, so $\mathrm{Frob}_{X,q} - 1$ is a separable endomorphism, so

$$\#X(\kappa_m) = \#\ker(\mathrm{Frob}_{X,q}^m - 1) = \deg(\mathrm{Frob}_{X,q}^m - 1) = P_{\mathrm{Frob}_X^m}(1),$$

where the last equality uses Theorem 5.2. Since the a_i are the eigenvalues of $\mathrm{Frob}_{X,q}$ acting on $V_\ell X$, it follows that a_i^m are the eigenvalues of $\mathrm{Frob}_{X,q}^m$, and hence that

$$P_{\mathrm{Frob}_{X,q}^m}(t) = \prod_{i=1}^{2g} (t - a_i^m),$$

from which the first part of the theorem follows.

We now claim that for $\alpha = \mathrm{Frob}_{X,q}$ we have $\alpha'\alpha = q$. Indeed, $\alpha'\alpha = \phi_{\mathscr{L}}^{-1}\alpha^t\phi_{\mathscr{L}}\alpha$, so it is enough to check on geometric points $x \in X$ that

$$\alpha^t\phi_{\mathscr{L}}\alpha(x) = q\phi_{\mathscr{L}}(x).$$

The left side is

$$\alpha^* t_{\alpha(x)}^* \mathscr{L} \otimes \alpha^* \mathscr{L}^{-1} = (t_{\alpha(x)}\alpha)^* \mathscr{L} \otimes \alpha^* \mathscr{L}^{-1},$$

and since α is a homomorphism, $t_{\alpha(x)}\alpha = \alpha t_x$. Thus, the above is

$$(\alpha t_x)^* \mathscr{L} \otimes \alpha^* \mathscr{L}^{-1} = t_x^* \alpha^* \mathscr{L} \otimes \alpha^* \mathscr{L}^{-1}.$$

But since α acts on $\mathscr{O}_X$ via $f \mapsto f^q$ and as the identity on the underlying topological space, it follows that

$$\alpha^* \mathscr{L} = \mathscr{L}^{\otimes q},$$

so

$$\alpha^t \phi_{\mathscr{L}} \alpha(x) = t_x^* \mathscr{L}^{\otimes q} \otimes \left(\mathscr{L}^{-1}\right)^{\otimes q} = \phi_{\mathscr{L}}(x)^{\otimes q}.$$

This gives the desired formula $\alpha'\alpha = q$. Now apply Proposition 5.5. ■

References

[1] Borel, A. *Sur la cohomologie des espaces fibrés princepaux et des espace homogènes de groupes de Lie compacts.* Ann. Math., **64** (1953), 115–207.

[2] Grothendieck, A. *Fondements de Géométrie Algébrigqe*, Séminaire Bourbaki, Exp. 232.

[3] Hartshorne, R. "Algebraic Geometry," Springer GTM **52**.

[4] Milne, J. "Abelian Varieties," from http://www.jmilne.org/math

[5] van der Geer, G., Moonen, B. "Abelian Varieties," from http://turing.wins.uva.nl/~bmoonen/boek/BookAV.html

[6] Mumford, D. *Abelian varieties.* Tata inst. of fundamental research, Bombay, 1970.

[7] Mumford, D. *Geometric Invariant Theory*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 2. Folge , Vol. 34 (2002).

[8] Murre, J. *On contravariant functors from the category of preschemes over a field into the category of abelian groups*, Publ. Math. de l'I.H.E.S. **23** (1964), 5–43.

[9] Oda, T. *The first de Rham cohomology group and Dieudonné modules*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 63–135.