CHAPTER V

Abelian Varieties

J. S. MILNE

This chapter reviews the theory of abelian varieties emphasizing those points of particular interest to arithmetic geometers. In the main it follows Mumford's book [16] except that most results are stated relative to an arbitrary base field, some additional results are proved, and étale cohomology is included. Many proofs have had to be omitted or only sketched. The reader is assumed to be familier with [10, Chaps. II, III] and (for a few sections that can be skipped) some étale cohomology. The last section of Chapter VII, "Jacobian Varieties", contains bibliographic notes for both chapters.

Conventions

The algebraic closure of a field k is denoted by $\bar{k}$ and its separable closure by k_s. For a scheme V over k and a k-algebra R, V_R denotes $V \times_{\text{spec}(k)} \text{spec}(R)$, and $V(R)$ denotes $\text{Mor}_k(\text{spec}(R), V)$. By a scheme over k, we shall always mean a scheme of finite type over k.

A variety V over k is a separated scheme of finite type over k such that $V_{\bar{k}}$ is integral (that is, reduced and irreducible). It is nonsingular if $V_{\bar{k}}$ is regular. Note that with these definitions, if V is a variety (and is nonsingular) then V_K is a integral (and is regular) for all fields $K \supset k$, and a product of (nonsingular) varieties is a (nonsingular) variety; moreover, $V(k_s)$ is nonempty. A k-rational point of V is often identified with a closed point v of V such that $k(v) = k$.

All statements are relative to a fixed group field: if V and W are varieties over k, then a sheaf or divisor on V, or a morphism $V \to W$, is automatically meant to be a defined over k (not over some "universal domain" as in the pre-scheme days).

Divisor means Cartier divisor, except that because most of our varieties are nonsingular we can usually think of them as Weil divisors. If $\pi: W \to V$ is a map and D is a divisor on V with local equation f near v, then π^*D (or

$\pi^{-1}D$) is the divisor on W with local equation $f \circ \pi$ near $\pi^{-1}(v)$. The invertible sheaf defined by D is denoted by $\mathscr{L}(D)$.

The tangent space to V at v is denoted by $T_v(V)$. Canonical isomorphisms are often denoted by $=$. The two projection maps $p\colon V \times W \to V$ and $q\colon V \times W \to W$ are always so denoted. The kernel of multiplication by n, $X \to X$, is denoted by X_n. An equivalence class containing x is often denoted by $[x]$.

§1. Definitions

A *group variety* over k is a variety V over k together with morphisms

$$m\colon V \times V \to V \qquad \text{(multiplication)},$$

$$\text{inv}\colon V \to V \qquad \text{(inverse)},$$

and an element $\varepsilon \in V(k)$ such that the structure on $V(\bar{k})$ defined by m and inv is that of a group with identity element ε.

Such a quadruple $(V, m, \text{inv}, \varepsilon)$ is a group in the category of varieties over k, i.e., the diagrams [22, §2] commute. (To see this, note that two morphisms with domain a variety W are equal if they become equal over $\bar{k}$, and that $W(\bar{k})$ is dense in $W_{\bar{k}}$.) Thus, for every k-algebra R, $V(R)$ acquires a group structure, and these group structures depend functorially on R.

For $a \in V(\bar{k})$, the projection map $p\colon V_{\bar{k}} \times V_{\bar{k}} \to V_{\bar{k}}$ induces an isomorphism $V_{\bar{k}} \times \{a\} \xrightarrow{\sim} V_{\bar{k}}$, and we define t_a to be the composite

$$V_{\bar{k}} \approx V_{\bar{k}} \times \{a\} \subset V_{\bar{k}} \times V_{\bar{k}} \xrightarrow{m} V_{\bar{k}}.$$

On points t_a is the translation map $P \mapsto m(P, a)$. Similarly, for any point $a \in V$, there is a translation map $t_a\colon V_{k(a)} \to V_{k(a)}$. In particular, if $a \in V(k)$, then t_a maps V into V.

A group variety is automatically nonsingular: as does any variety, it contains a nonempty, nonsingular open subvariety U, and the translates of $U_{\bar{k}}$ cover $V_{\bar{k}}$.

A complete group variety is called an *abelian variety*. As we shall see, they are projective and (fortunately) commutative. Their group laws will be written additively.

An affine group variety is called a *linear algebraic group*. Each such variety can be realized as a closed subgroup of GL_n for some n [24, 3.4].

≈ means isomorphic.

§2. Rigidity

Theorem 2.1 (Rigidity Theorem). *Let $f\colon V \times W \to U$ be a morphism of varieties over k. If V is complete and*

$$f(V \times \{w_0\}) = \{u_0\} = f(\{v_0\} \times W)$$

for some $u_0 \in U(k)$, $v_0 \in V(k)$, $w_0 \in W(k)$, then $f(V \times W) = \{u_0\}$.

PROOF. Let U_0 be an open affine neighborhood of u_0. The projection map $q\colon V \times W \to W$ is closed (this is what it means for V to be complete), and so the set $Z = q(f^{-1}(U - U_0))$ is closed in W. Note that a closed point w of W lies outside Z if and only if $f(V \times \{w\}) \subset U_0$. In particular, $w_0 \in W - Z$ and so $W - Z$ is a dense open subset of W. As $V \times \{w\}$ is complete and U_0 is affine, $f(V \times \{w\})$ must be a point whenever w is a closed point of $W - Z$, [14, p. 104]; in fact, $f(V \times \{w\}) = f(\{v_0\} \times \{w\}) = \{u_0\}$. Thus f is constant on the dense subset $V \times (W - Z)$ of $V \times W$, and so is constant. □

Corollary 2.2. *Every morphism $f\colon A \to B$ of abelian varieties is the composite of a homomorphism $h\colon A \to B$ with a translation t_a, $a = -f(0) \in B(k)$.*

PROOF. After replacing f with $t_a \circ f$, $a = -f(0)$, we can assume that $f(0) = 0$. Define $\varphi\colon A \times A \to B$ to be $f \circ m_A - m_B \circ (f \times f)$, so that on points $\varphi(a, a') = f(a + a') - f(a) - f(a')$. Then $\varphi(A \times \{0\}) = 0 = \varphi(\{0\} \times A)$, and so the theorem shows that $\varphi = 0$ on $A \times A$. Thus $f \circ m_A = m_B \circ (f \times f)$, which is what we mean by f being a homomorphism. □

Remark 2.3. The corollary shows that the group structure on A is uniquely determined by the choice of a zero element.

Corollary 2.4. *The group law on an abelian variety A is commutative.*

PROOF. Commutative groups are distinguished by the fact that the map taking an element to its inverse is a homomorphism. The preceding corollary shows that inv: $A \to A$ is a homomorphism. □

Corollary 2.5. *Let V and W be complete varieties over k with rational points $v_0 \in V(k)$, $w_0 \in W(k)$, and let A be an abelian variety. Then a morphism $h\colon V \times W \to A$ such that $h(v_0, w_0) = 0$ can be written uniquely as $h = f \circ p + g \circ q$ with $f\colon V \to A$ and $g\colon W \to A$ morphisms such that $f(v_0) = 0$, $g(w_0) = 0$.*

PROOF. Define f to be $V = V \times \{w_0\} \xrightarrow{h} A$ and g to be $W = \{v_0\} \times W \xrightarrow{h} A$, so that $k \overset{\text{df}}{=} h - (f \circ p + g \circ q)$ is the map such that on points $k(v, w) = h(v, w) - h(v, w_0) - h(v_0, w)$. Then

$$k(V \times \{w_0\}) = 0 = k(\{v_0\} \times W),$$

and so the theorem shows that $k = 0$. □

§3. Rational Maps into Abelian Varieties

We improve some of the results in the last section.

Recall [10, I, 4] that a *rational map* $f\colon V \dashrightarrow W$ of varieties is an equivalence class of pairs (U, f_U) with U a dense open subset of V and f_U a morphism

$U \to W$; two pairs (U, f_U) and $(U', f_{U'})$ are equivalent if f_U and $f_{U'}$ agree on $U \cap U'$. There is a largest open subset U of V such that f defines a morphism $U \to W$, and f is said to be *defined* at the points of U.

Theorem 3.1. *A rational map $f: V \dashrightarrow A$ from a nonsingular variety to an abelian variety is defined on the whole of V.*

PROOF. Combine the next two lemmas. □

Lemma 3.2. *A rational map $f: V \dashrightarrow W$ from a normal variety to a complete variety is defined on an open subset U of V whose complement $V - U$ has codimension ≥ 2*

PROOF. Let $f_U: U \to W$ be a representative of f, and let v be a point of $V - U$ of codimension 1 in V (that is, whose closure $\{\overline{v}\}$ has codimension 1). Then $\mathcal{O}_{V,v}$ is a discrete valuation ring (because V is normal) whose field of fractions is $k(V)$, and the valuative criterion of properness [10, II, 4.7] shows that the map $\operatorname{spec}(k(V)) \to W$ defined by f extends to a map $\operatorname{spec}(\mathcal{O}_{V,v}) \to W$. This implies that f has a representative defined on a neighborhood of v, and so the set on which f is defined contains all points of codimension ≤ 1. This proves the lemma. □

Lemma 3.3. *Let $f: V \dashrightarrow G$ be a rational map from a nonsingular variety to a group variety. Then either f is defined on all of V or the points where it is not defined form a closed subset of pure codimension 1 in V.*

PROOF. See [2, 1.3]. □

Theorem 3.4. *Let $f: V \times W \to A$ be a morphism from a product of nonsingular varieties into an abelian variety. If*

$$f(V \times \{w_0\}) = \{a_0\} = f(\{v_0\} \times W)$$

for some $a_0 \in A(K)$, $v_0 \in V(k)$, and $w_0 \in W(k)$, then $f(V \times W) = \{a_0\}$.

PROOF. We can assume k to be algebraically closed. Consider first the case that V has dimension 1. Then V can be embedded in a nonsingular complete curve $\overline{V}$, and (3.1) shows that f extends to a map $\overline{f}: \overline{V} \times W \to A$. Now (2.1) shows that $\overline{f}$ is constant.

In the general case, let C be an irreducible curve on V passing through v_0 and nonsingular at v_0, and let $\tilde{C} \to C$ be the normalization of C. Then f defines a morphism $\tilde{C} \times W \to A$ which the preceding argument shows to be constant. Therefore $f(C \times W) = \{a_0\}$, and the next lemma completes the proof. □

Lemma 3.5. *Let V be an integral scheme of finite type over a field k, and assume*

V is nonsingular at a point $v_0 \in V(k)$; then the union of the integral one-dimensional subschemes passing through v_0 and nonsingular at v_0 is dense in V.

PROOF. By induction it suffices to show that the union of the integral subschemes of codimension 1 passing through v_0 and smooth at v_0 is dense in V. We can assume that V is affine and v_0 is the origin. For H a hyperplane passing through v_0 but not containing $T_{v_0}(V)$, $V \cap H$ is smooth at v_0. Let V_H be the component of $V \cap H$ passing through v_0, regarded as an integral subscheme of V and let Z be a closed subset of V containing all V_H. Regard Z as a reduced subscheme of V, and let $C_{v_0}(Z)$ be the tangent cone to Z at v_0 [14, III.3]. Clearly $T_{v_0}(V) \cap H = T_{v_0}(V_H) = C_{v_0}(V_H) \subset C_{v_0}(Z) \subset C_{v_0}(V) = T_{v_0}(V)$, and it follows that $C_{v_0}(Z) = T_{v_0}(V)$. As $\dim C_{v_0}(Z) = \dim(Z)$ (see [14, III.3, p. 320]), this implies that $Z = V$. □

Corollary 3.6. *Every rational map $f: G \dashrightarrow A$ from a group variety to an abelian variety is the composite of a homomorphism $h: G \to A$ with a translation.*

PROOF. Theorem 3.1 shows that f is a morphism. The rest of the proof is the same as that of (2.2). □

Remark 3.7. The corollary shows that A is determined by $k(A)$ up to the choice of a zero element. In particular, if A and B are abelian varieties and $k(A)$ is isomorphic to $k(B)$, then A is isomorphic to B (as an abelian variety).

Corollary 3.8. *Every rational map $f: \mathbb{P}^1 \dashrightarrow A$ is constant.*

PROOF. The variety $\mathbb{P}^1 - \{\infty\}$ becomes a group variety under addition, and $\mathbb{P}^1 - \{0, \infty\}$ becomes a group variety under multiplication. Therefore the last corollary shows that there exist $a, b \in A(k)$ such that

$$f(x + y) = f(x) + f(y) + a, \quad \text{all} \quad x, y \in \overline{k} = \mathbb{P}^1(\overline{k}) - \{\infty\},$$

$$f(xy) = f(x) + f(y) + b, \quad \text{all} \quad x, y \in \overline{k}^\times = \mathbb{P}^1(\overline{k}) - \{0, \infty\}.$$

This is clearly impossible unless f is constant. □

Recall that a variety V of dimension d is *unirational* if there is an embedding of $\overline{k}(V)$ into a purely transcendental extension $\overline{k}(X_1, \ldots, X_d)$ of $\overline{k}$. Such an embedding corresponds to a rational map $\mathbb{P}^d_k \dashrightarrow V_{\overline{k}}$ whose image is dense in $V_{\overline{k}}$.

Corollary 3.9. *Every rational map from a unirational variety to an abelian variety is constant.*

PROOF. We can suppose k to be algebraically closed. By assumption there is a rational map $\mathbb{A}^d \dashrightarrow V$ with dense image, and the composite of this with a

rational map $f: V \dashrightarrow A$ extends to a morphism $\bar{f}: \mathbb{P}^1 \times \cdots \times \mathbb{P}^1 \to A$. According to (2.5), $\bar{f}(x_1, \ldots, x_n) = \sum f_i(x_i)$ for some morphisms $f_i: \mathbb{P}^1 \to A$, and (3.8) shows that each f_i is constant. □

§4. Review of the Cohomology of Schemes

In order to prove some of the theorems concering abelian varieties, we shall need to make use of results from the cohomology of coherent sheaves. The first of these is Grothendieck's relative version of the theorem asserting that the cohomology groups of coherent sheaves on complete varieties are finite dimensional.

Theorem 4.1. *If $f: V \to T$ is a proper morphism of Noetherian schemes and $\mathscr{F}$ is a coherent $\mathcal{O}_V$-module, then the higher direct image sheaves $R^r f_* \mathscr{F}$ are coherent $\mathcal{O}_T$-modules for all $r \geq 0$.*

PROOF. When f is projective, this is proved in [10, III, 8.8]. Chow's lemma [10, II, Ex. 4.10] allows one to extend the result to the general case [9, III.3.2.1]. □

The second result describes how the dimensions of the cohomology groups of the members of a flat family of coherent sheaves vary.

Theorem 4.2. *Let $f: V \to T$ be a proper flat morphism of Noetherian schemes, and let $\mathscr{F}$ be a locally free $\mathcal{O}_V$-module of finite rank. For each t in T, write V_t for the fibre of V over t and $\mathscr{F}_t$ for the inverse image of $\mathscr{F}$ on V_t.*

(a) *The formation of the higher direct images of $\mathscr{F}$ commutes with flat base change. In particular, if $T = \operatorname{spec}(R)$ is affine and R' is a flat R-algebra, then $H^r(V', \mathscr{F}') = H^r(V, \mathscr{F}) \otimes_R R'$, where $V' = V \times_{\operatorname{spec}(R)} \operatorname{spec}(R')$ and $\mathscr{F}'$ is the inverse image of $\mathscr{F}$ on V'.*

(b) *The function $t \mapsto \chi(\mathscr{F}_t) \overset{\text{df}}{=} \sum (-1)^r \dim_{k(t)} H^r(V_t, \mathscr{F}_t)$ is locally constant on T.*

(c) *For each r, the function $t \mapsto \dim_{k(t)} H^r(V_t, \mathscr{F}_t)$ is upper semicontinuous (that is, it jumps on closed subsets).*

(d) *If T is integral and $\dim_{k(t)} H^r(V_t, \mathscr{F}_t)$ is equal to a constant s for all t in T, then $R^r f_* \mathscr{F}$ is a locally free $\mathcal{O}_T$-module and the natural maps $R^r f_* \mathscr{F} \otimes_{\mathcal{O}_T} k(t) \to H^r(V_t, \mathscr{F}_t)$ are isomorphisms.*

(e) *If $H^1(V_t, \mathscr{F}_t) = 0$ for all t in T, then $R^1 f_* \mathscr{F} = 0$, $f_* \mathscr{F}$ is locally free, and the formation of $f_* \mathscr{F}$ commutes with base change.*

PROOF. (a) The statement is local on the base, and so it suffices to prove it for the particular case in which we have given an explicit statement. In

[16, §5, p. 46], a complex $K^{\cdot}$ of R-modules is constructed such that for all R-algebras R', $H^r(V', \mathscr{F}') = H^r(K^{\cdot} \otimes_R R')$. In our case, R' is flat over R, and so $H^r(K^{\cdot} \otimes_R R') = H^r(K^{\cdot}) \otimes_R R'$, which equals $H^r(V, \mathscr{F}) \otimes_R R'$.

(b), (c), (d). These are proved in [16, §5].

(e). The hypothesis implies that $R^1 f_* \mathscr{F} = 0$ ([10, III, 12.11a]), and it follows that $f_* \mathscr{F} \otimes_{\mathcal{O}_T} k(t) \to H^0(V_t, \mathscr{F}_t)$ is surjective for all t ([10, III, 12.11b]) and so is an isomorphism. Now this last reference (applied with $i = 0$) shows that $f_* \mathscr{F}$ is locally free. □

§5. The Seesaw Principle

We shall frequently need to consider the following situation: V is a variety over k, T is a scheme of finite type over k, and $\mathscr{L}$ is an invertible sheaf on $V \times T$. For $t \in T$, $\mathscr{L}_t$ will then always denote the invertible sheaf $(1 \times t)^* \mathscr{L}$ on $V_t = V_{k(t)} = (V \times T) \times_T t$, where t is the inclusion of $t = \operatorname{spec}(k(t))$ into T. There is the diagram

$$\begin{array}{ccc} (V \times T, \mathscr{L}) & \leftarrow & (V_t, \mathscr{L}_t). \\ \downarrow & & \downarrow \\ T & \xleftarrow{t} & t \end{array}$$

It is often useful to regard $\mathscr{L}$ as defining a family of invertible sheaves on V parametrized by T.

Theorem 5.1. *Let V be a complete variety and T an integral scheme of finite type over k, and let $\mathscr{L}$ and $\mathscr{M}$ be invertible sheaves on $V \times T$. If $\mathscr{L}_t \approx \mathscr{M}_t$ for all $t \in T$, then there exists an invertible sheaf $\mathscr{N}$ on T such that $\mathscr{L} \approx \mathscr{M} \otimes q^* \mathscr{N}$.*

PROOF. By assumption, $(\mathscr{L} \otimes \mathscr{M}^{-1})_t$ is trivial for all $t \in T$, and so $H^0(V_t, (\mathscr{L} \otimes \mathscr{M}^{-1})_t) \approx H^0(V_t, \mathcal{O}_{V_t}) = k(t)$. Therefore (4.2d) shows that the sheaf $\mathscr{N} = q_*(\mathscr{L} \otimes \mathscr{M}^{-1})$ is invertible. Consider the natural map $q^* \mathscr{N} = q^* q_* (\mathscr{L} \otimes \mathscr{M}^{-1}) \xrightarrow{\alpha} \mathscr{L} \otimes \mathscr{M}^{-1}$. As $(\mathscr{L} \otimes \mathscr{M}^{-1})_t \approx \mathcal{O}_{V_t}$, the restriction of α to the fibre V_t is isomorphic to the natural map $\alpha_t: \mathcal{O}_{V_t} \otimes \Gamma(V_t, \mathcal{O}_{V_t}) \to \mathcal{O}_{V_t}$, which is an isomorphism. Now Nakayama's lemma implies that α is surjective, and because both $q^* \mathscr{N}$ and $\mathscr{L} \otimes \mathscr{M}^{-1}$ are invertible sheaves, it follows that α is an isomorphism (if R is a local ring, then a surjective R-linear map $R \to R$ is an isomorphism because it must send 1 to a unit). □

Corollary 5.2 (Seesaw Principle). *Suppose in addition to the hypotheses of the theorem that $\mathscr{L}_v \approx \mathscr{M}_v$ for at least one $v \in V(k)$. Then $\mathscr{L} \approx \mathscr{M}$.*

PROOF. The theorem shows that $\mathscr{L} \approx \mathscr{M} \otimes q^* \mathscr{N}$ for some $\mathscr{N}$ on T. On pulling back by $T = \{v\} \times T \subset V \times T$, we obtain an isomorphism

$\mathscr{L}_v \approx \mathscr{M}_v \otimes q^*\mathscr{N}_v$. As $\mathscr{L}_v \approx \mathscr{M}_v$ and $(q^*\mathscr{N})_v = \mathscr{N}$, this shows that $\mathscr{N}$ is trivial. □

The next result shows that the condition $\mathscr{L}_t \approx \mathscr{M}_t$ of the theorem needs only to be checked for t in some dense subset of T (for example, it needs only to be checked for t the generic point of T).

Theorem 5.3. *Let V be a complete variety, and let $\mathscr{L}$ be an invertible sheaf on $V \times T$. Then $\{t \in T \mid \mathscr{L}_t \text{ is trivial}\}$ is closed in T.*

Lemma 5.4. *An invertible sheaf $\mathscr{L}$ on a complete variety is trivial if and only if both it and its dual $\mathscr{L}^{-1}$ have nonzero global sections.*

PROOF. The sections define nonzero homomorphisms $s_1: \mathcal{O}_V \to \mathscr{L}$ and $s_2: \mathcal{O}_V \to \mathscr{L}^{-1}$. The dual of s_2 is a homomorphism $s_2^\vee: \mathscr{L} \to \mathcal{O}_V$, and $s_2^\vee \circ s_1$, being nonzero, is an isomorphism (note that $\operatorname{Hom}(\mathcal{O}_V, \mathcal{O}_V) = H^0(V, \mathcal{O}_V) = k$). Because $\mathscr{L}$ is an invertible sheaf, this implies that s_1 is also an isomorphism. □

PROOF OF (5.3). The lemma identifies the set of t for which $\mathscr{L}_t$ is trivial with the set of t for which both $\dim H^0(V_t, \mathscr{L}_t) > 0$ and $\dim H^0(V_t, \mathscr{L}_t^{-1}) > 0$. Part (c) of (4.2) shows that this set is closed. □

Remark 5.5. Let V, T, and $\mathscr{L}$ be as at the start of the section with V complete. We shall say that $\mathscr{L}$ defines a *trivial family* of sheaves on T if $\mathscr{L} \approx q^*\mathscr{N}$ for some invertible sheaf $\mathscr{N}$ on T. According to (5.1), in the case that T is integral, $\mathscr{L}$ defines a trivial family if and only if each $\mathscr{L}_t$ is trivial. Returning to the general situation, let Z be the closed subset of T determined by (5.3). Clearly Z has the following property: A morphism $f: T' \to T$ from an integral scheme to T factors through Z if and only if $(1 \times f)^*\mathscr{L}$ defines a trivial family on V. This result can be significantly strengthened: there exists a unique closed subscheme Z of T (not necessarily reduced) such that a morphism $f: T' \to T$ (with T' not necessarily integral) factors through the inclusion morphism $Z \subset T$ if and only if $(1 \times f)^*\mathscr{L}$ defines a trivial family on V. See [16, §10, p. 89].

§6. The Theorems of the Cube and the Square

Theorem 6.1 (Theorem of the Cube). *Let U, V, W be complete varieties over k with base points $u_0 \in U(k)$, $v_0 \in V(k)$, $w_0 \in W(k)$. An invertible sheaf $\mathscr{L}$ on $U \times V \times W$ is trivial if its restrictions to $\{u_0\} \times V \times W$, $U \times \{v_0\} \times W$, and $U \times V \times \{w_0\}$ are all trivial.*

PROOF. Because $\mathscr{L}|U \times V \times \{w_0\}$ is trivial, the seesaw principle shows that it suffices to prove that $\mathscr{L}|z \times W$ is trivial for a dense set of z in $U \times V$. Next

one shows that U can be taken to be a complete curve ((3.5) accomplishes this reduction when u_0 is nonsingular). This case is proved in [16, §6, pp. 57–58] when k is algebraically closed, and the next lemma shows that we may assume that. □

Lemma 6.2. *Let $\mathscr{L}$ be an invertible sheaf on a complete variety V over a field k; if $\mathscr{L}$ becomes trivial on $V_{\bar{k}}$ then it is trivial on V.*

PROOF. The triviality of $\mathscr{L}$ on $V_{\bar{k}}$ implies that both $H^0(V_{\bar{k}}, \mathscr{L})$ and $H^0(V_{\bar{k}}, \mathscr{L}^{-1})$ are nonzero. As $H^0(V_{\bar{k}}, \mathscr{L}^{\pm 1}) = H^0(V, \mathscr{L}^{\pm 1}) \otimes_k \bar{k}$ (see (4.2a)), Lemma 5.4 shows that $\mathscr{L}$ is trivial. □

Remark 6.3. At least in the case that k is algebraically closed, it is not necessary to assume in (6.1) that W is complete [16, §6, p. 55], nor even that it is a variety [16, §10, p. 91].

Corollary 6.4. *Let A be an abelian variety, and let $p_i: A \times A \times A \to A$ be the projection onto the ith factor; let $p_{ij} = p_i + p_j$ and $p_{ijk} = p_i + p_j + p_k$. For any invertible sheaf $\mathscr{L}$ on A, the sheaf*

$$p_{123}^*\mathscr{L} \otimes p_{12}^*\mathscr{L}^{-1} \otimes p_{23}^*\mathscr{L}^{-1} \otimes p_{13}^*\mathscr{L}^{-1} \otimes p_1^*\mathscr{L} \otimes p_2^*\mathscr{L} \otimes p_3^*\mathscr{L}$$

on $A \times A \times A$ is trivial.

PROOF. The restriction of the sheaf to $\{0\} \times A \times A\ (= A \times A)$ is

$$m^*\mathscr{L} \otimes p^*\mathscr{L}^{-1} \otimes m^*\mathscr{L}^{-1} \otimes q^*\mathscr{L}^{-1} \otimes \mathcal{O}_{A\times A} \otimes p^*\mathscr{L} \otimes q^*\mathscr{L},$$

which is trivial. Similarly its restrictions to $A \times \{0\} \times A$ and $A \times A \times \{0\}$ are trivial, which implies that it is trivial on $A \times A \times A$. □

Corollary 6.5. *Let f, g, h be morphisms from a variety V to an abelian variety A. For any invertible sheaf $\mathscr{L}$ on A, the sheaf*

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

on V is trivial.

PROOF. The sheaf in question is the inverse image of the sheaf in (6.4) by $(f, g, h): V \to A \times A \times A$. □

Corollary 6.6. *Consider the map $n_A: A \to A$ equal to multiplication by n. For all invertible sheaves $\mathscr{L}$ on A,*

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

In particular,

$$n_A^*\mathscr{L} \approx \mathscr{L}^{n^2} \quad \text{if } \mathscr{L} \text{ is symmetric (i.e., } \mathscr{L} \approx (-1)_A^*\mathscr{L})$$
$$n_A^*\mathscr{L} \approx \mathscr{L}^{n} \quad \text{if } \mathscr{L} \text{ is antisymmetric (i.e., } \mathscr{L}^{-1} \approx (-1)_A^*\mathscr{L}).$$

PROOF. On applying the last corollary to the maps n_A, 1_A, $(-1)_A$: $A \to A$ we find that $(n+1)_A^* \mathscr{L}^{-1} \otimes n_A^* \mathscr{L}^2 \otimes (n-1)_A^* \mathscr{L}^{-1} \approx \mathscr{L}^{-1} \otimes (-1)^* \mathscr{L}^{-1}$. This fact can be used to prove the corollary by induction, starting from the easy cases $n = 0, 1, -1$. □

Theorem 6.7 (Theorem of the Square). *For all invertible sheaves $\mathscr{L}$ on an abelian variety A and points $a, b \in A(k)$,*

$$t_{a+b}^* \mathscr{L} \otimes \mathscr{L} \approx t_a^* \mathscr{L} \otimes t_b^* \mathscr{L}.$$

PROOF. Apply (6.5) with f the identity map on A and g and h the constant maps with images a and b. □

Remark 6.8. When tensored with $\mathscr{L}^{-2}$, the isomorphism in (6.7) becomes

$$t_{a+b}^* \mathscr{L} \otimes \mathscr{L}^{-1} \approx (t_a^* \mathscr{L} \otimes \mathscr{L}^{-1}) \otimes (t_b^* \mathscr{L} \otimes \mathscr{L}^{-1}).$$

Thus the map $\varphi_{\mathscr{L}}$,

$$a \mapsto t_a^* \mathscr{L} \otimes \mathscr{L}^{-1}: A(k) \to \mathrm{Pic}(A),$$

is a homomorphism. Therefore, if $\sum_{i=1}^n a_i = 0$ in $A(k)$, then

$$t_{a_1}^* \mathscr{L} \otimes t_{a_2}^* \mathscr{L} \otimes \cdots \otimes t_{a_n}^* \mathscr{L} \approx \mathscr{L}^n.$$

Remark 6.9. We write $\sim$ for linear equivalence of divisors, so that $D \sim D'$ if and only if $\mathscr{L}(D) \approx \mathscr{L}(D')$. Also, we write D_a for the translate $t_a D = D + a$ of D. Note that $t_a^* \mathscr{L}(D) = \mathscr{L}(t_a^{-1} D) = \mathscr{L}(D_{-a})$. The isomorphisms in (6.7) and (6.8) become the relations:

$$D_{a+b} + D \sim D_a + D_b, \qquad a, b \in A(k),$$

$$\sum_{i=1}^n D_{a_i} \sim nD, \qquad \text{if } \sum a_i = 0 \text{ in } A(k).$$

§7. Abelian Varieties Are Projective

For D a divisor on a variety V we write

$$L(D) = \{f \in k(V) \mid (f) + D \geq 0\} \cup \{0\} = H^0(V, \mathscr{L}(D)),$$

$$|D| = \{(f) + D \mid f \in L(D)\} = \text{the complete linear system containing } D.$$

A projective embedding of an elliptic curve can be constructed as follows: let $D = P_0$, where P_0 is the zero element of A, and choose a suitable basis 1, x, y of $L(3D)$; then the map $A \to \mathbb{P}^2$ defined by $\{1, x, y\}$ identifies A with the cubic projective curve

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

(See [10, IV, 4.6].) This argument can be extended to every abelian variety.

Theorem 7.1. *Every abelian variety is projective.*

PROOF. We first prove this under the assumption that the abelian variety A is defined over an algebraically closed field.

Recall [10, II, 7.8.2] that a variety is projective if it has a very ample linear system, and that a linear system $\mathfrak{d}$ is very ample if:

(a) it separates points (for any pair a, b of distinct closed points on the variety, there is a D in $\mathfrak{d}$ such that $a \in D$ but $b \notin D$); and
(b) it separates tangent vectors (for any closed point a and tangent vector t to the variety at a, there exists a $D \in \mathfrak{d}$ such that $a \in D$ but $t \notin T_a(D)$).

The first step of the proof is to show that there exists a linear system that separates 0 from the other points of A and separates tangent vectors at 0. More precisely, we show that there exists a finite set $\{Z_i\}$ of prime divisors on A such that:

(a) $\bigcap Z_i = \{0\}$; and
(b) for any $t \in T_0(A)$ there exists a Z_i such that $t_i \notin T_0(Z_i)$.

The second step is to show that if $D = \sum Z_i$, then $|3D|$ is very ample.

The existence of the set $\{Z_i\}$ is an immediate consequence of the observations:

(i) for any closed point $a \neq 0$ of A, there is a prime divisor Z such that $0 \in Z$, $a \notin Z$;
(ii) for any $t \in T_0(A)$, there is a prime divisor Z passing through 0 such that $t \notin T_0(Z)$.

The proof of (ii) is obvious: choose an open affine neighborhood U of 0, let Z_0 be an irreducible component of $A \cap H$ where H is any hyperplane through 0 not containing t, and take Z to be the closure of Z_0. The proof of (i) will be equally obvious once we have shown that 0 and a are contained in a single open affine subset of A. Let U again be an open affine neighborhood of 0, and let $U + a$ be its translate by a. Choose a closed point u of $U \cap (U + a)$. Then both u and $u + a$ lie in $U + a$, and so $U + a - u$ is an open affine neighborhood of both 0 and a.

Now let D be the divisor $\sum Z_i$ where $(Z_i)_{1 \leq i \leq n}$ satisfies (a) and (b). For any family $(a_i, b_i)_{1 \leq i \leq n}$ of closed points of A, the theorem of the square (6.9) shows that

$$\sum_i (Z_{i,a_i} + Z_{i,b_i} + Z_{i,-a_i-b_i}) \sim \sum_i 3Z_i = 3D.$$

Let a and b be distinct closed points of A. By (a), for some i, say $i = 1$, Z_i does not contain $b - a$. Choose $a_1 = a$. Then Z_{1,a_1} passes through a but not b. The sets

$$\{b_1 \mid Z_{1,b_1} \text{ passes through } b\},$$

$$\{b_1 \mid Z_{1,-a_1-b_1} \text{ passes through } b\},$$

are proper closed subsets of A. Therefore, it is possible to choose a b_1 that lies in neither. Similarly a_i and b_i for $i \geq 2$ can be chosen so that none of the Z_{i,a_i}, Z_{i,b_i}, or $Z_{i,-a_i-b_i}$ passes through b. Then a is in the support of $\sum(Z_{i,a_i} + Z_{i,b_i} + Z_{i,-a_i-b_i})$ but b is not, which shows that $|3D|$ separates points. The proof that it separates tangents is similar.

The final step is to show that if $A_{\bar{k}}$ is projective, then so also is A_k. Let D be an ample divisor on $A_{\bar{k}}$; then D is defined over a finite extension of k, and the following statements explain how to construct from D an ample divisor on A.

(a) Let D be a divisor on A; if $|D_{\bar{k}}|$ is very ample, then so also is $|D|$. (The map $A_{\bar{k}} \subset \mathbb{P}^n$ defined by $|D_{\bar{k}}|$ is obtained by base change from that defined by $|D|$.)
(b) If $|D_1|$ and $|D_2|$ are ample, then so also is $|D_1 + D_2|$. (See [10, II, Ex. 7.5].)
(c) If D is a divisor on $A_{k'}$, where k' is a finite Galois extension of k with Galois group G, then $\sum \sigma D$, $\sigma \in G$, arises from a divisor on A. (This is obvious.)
(d) If D is a divisor on $A_{k'}$, where k' is a finite purely inseparable extension of k such that $k'^{p^m} \subset k$, then $p^m D$ arises from a divisor on A. (Regard D as the Cartier divisor defined by a family of pairs (f_i, U_i'), $f_i \in k'(A)$, and let U_i be the image of U_i' in A; then $k'(A)^{p^m} \subset k(A)$, and so the pairs $(f_i^{p^m}, U_i)$ define a divisor on A whose inverse image on $A_{k'}$ is $p^m D$.) □

Corollary 7.2. *Every abelian variety has a symmetric ample invertible sheaf.*

PROOF. According to the theorem, it has an ample invertible sheaf $\mathscr{L}$. As multiplication by -1 is an isomorphism, $(-1)^*\mathscr{L}$ is ample, and therefore $\mathscr{L} \otimes (-1)^*\mathscr{L}$ is ample [10, II, Ex. 7.5] and symmetric. □

Remark 7.3. If $\mathscr{L}$ is an ample invertible sheaf on A, then by definition $\mathscr{L}^n$ is very ample for some n. It is an important theorem that in fact $\mathscr{L}^3$ will be very ample (see [16, §17, p. 163]). The three is needed, as in the above proof, so that one can apply the theorem of the square.

§8. Isogenies

Let $f: A \to B$ be a homomorphism of abelian varieties. The kernel N of f in the sense of [22, §2] is a closed subgroup scheme of A of finite type over k. When k has characteristic zero, N is reduced [22, §3], and so its identity component N^0 is an abelian variety (possibly zero); in general, N will be an extension of a finite group scheme by an abelian variety. If f is surjective and has finite kernel then it is called an *isogeny*.

Proposition 8.1. *For a homomorphism $f: A \to B$ of abelian varieties, the following statements are equivalent:*

(a) *f is an isogeny;*
(b) *$\dim A = \dim B$ and f is surjective;*
(c) *$\dim A = \dim B$ and $\mathrm{Ker}(f)$ is a finite group scheme;*
(d) *f is finite, flat, and surjective.*

PROOF. As $f(A)$ is closed in B, the equivalence of the first three statements follows from the theorem on the dimension of fibres of morphisms; see [14, I.8].

Clearly (d) implies (a), and so assume (a). Because f is a homomorphism, the translation map t_b can be used to show that the (scheme-theoretic) fibre $f^{-1}(b)$ is isomorphic to $f^{-1}(0)_{k(b)}$. Therefore f is quasi-finite. It is also projective ([10, II, Ex. 4.9]), and this shows that it is finite ([10, III, Ex. 11.2]). The sheaf $f_*\mathscr{O}_A$ is a coherent $\mathscr{O}_B$-module, and $\dim_{k(b)}(f_*\mathscr{O}_A \otimes k(b)) = \dim_k(f_*\mathscr{O}_A \otimes k(0))$ is independent of b, and so (4.2d) shows that $f_*\mathscr{O}_A$ is locally free. □

The *degree* of an isogeny $f: A \to B$ is defined to be the order of the kernel of f (as a finite group scheme); equivalently, it is the rank of $f_*\mathscr{O}_A$ as a locally free $\mathscr{O}_B$-module. Clearly, $\deg(g \circ f) = \deg(g)\deg(f)$. Let $n = \deg(f)$; then $\mathrm{Ker}(f) \subset \mathrm{Ker}(n_A)$ and so n_A factors as $n_A = g \circ f$ with g an isogeny $B \to A$.

For an integer n we write n_A, or simply n, for the morphism $a \mapsto na: A \to A$.

Theorem 8.2. *Let A be an abelian variety of dimension g, and let $n > 0$ be an integer. Then $n_A: A \to A$ is an isogeny of degree n^{2g}; it is étale if and only if the characteristic of k does not divide n.*

PROOF. From (7.2) we know there is an ample symmetric invertible sheaf $\mathscr{L}$ on A, and according to (6.6) $n_A^*\mathscr{L} \approx \mathscr{L}^{n^2}$. The restriction of an ample invertible sheaf to a closed subscheme is again ample, and so the restriction of $n_A^*\mathscr{L}$ to $\mathrm{Ker}(n_A)$ is both trivial and ample. This is impossible unless $\mathrm{Ker}(n_A)$ has dimension zero. We have shown that n_A is an isogeny.

In proving that n_A has degree n^{2g} we shall use some elementary intersection theory from [21, IV.1]. Clearly we may assume k is algebraically closed.

Let V be a smooth projective variety of dimension g. If $D_1, \ldots, D_g$ are effective divisors on V such that $\bigcap D_i$ has dimension zero, then their intersection number is defined by the equations

$$(D_1, \ldots, D_g) = \sum_v (D_1, \ldots, D_g)_v \qquad (\text{sum over } v \in \textstyle\bigcap D_i),$$

$$(D_1, \ldots, D_g)_v = \dim_k(\mathscr{O}_{V,v}/(f_{1,v}, \ldots, f_{g,v})),$$

where $f_{i,v}$ is a local equation for D_i near v. The definition is extended by linearity to noneffective divisors whose components intersect properly. Then one checks that $(D_1, \ldots, D_g)$ is unchanged if each D_i is replaced by a linearly equivalent divisor and shows that this can be used to extend the definition to all g-tuples of divisors (loc. cit.). In particular $(D^g) = (D, D, \ldots)$ is defined.

Lemma 8.3. *Let V and W be smooth projective varieties of dimension g, and let*

$f: W \to V$ be a finite flat map of degree d. Then for any divisors $D_1, \dots, D_g$ on V

$$(f^*D_1, \dots, f^*D_g) = d(D_1, \dots, D_g).$$

PROOF. It suffices to prove the equality in the case that the D_i are effective and $\bigcap D_i$ is finite. Let $v \in \bigcap D_i$. Then $(f_*\mathcal{O}_W) \otimes_{\mathcal{O}_V} \mathcal{O}_{V,v} = \prod_{f(w)=v} \mathcal{O}_{W,w}$, which is therefore a free $\mathcal{O}_{V,v}$-module of rank d. If $f_{i,v}$ is a local equation for D_i near v, then $f_{i,v} \circ f$ is a local equation for f^*D_i near each of the points in $f^{-1}(v)$. Therefore

$$\begin{aligned}\sum_{f(w)=v} (f^*D_1, \dots, f^*D_g)_w &= \sum_{f(w)=v} \dim_k(\mathcal{O}_{W,w}/(f_{1,v} \circ f, \dots, f_{g,v} \circ f)) \\ &= \dim_k((\prod_{f(w)=v} \mathcal{O}_{W,w}) \otimes_{\mathcal{O}_{V,v}} (\mathcal{O}_{V,v}/(f_{1,v}, \dots, f_{g,v}))) \\ &= d(D_1, \dots, D_g)_v. \qquad \square\end{aligned}$$

We apply this theory to a divisor D on A such that D is linearly equivalent to $(-1)^*D$ (i.e., such that $\mathcal{L}(D)$ is symmetric). Let $d = \deg(n_A)$. Then (8.3) shows that $((n_A^*D)^g) = d(D^g)$, but (6.6) shows that n_A^*D is linearly equivalent to n^2D and therefore that $((n_A^*D))^g = ((n^2D)^g) = n^{2g}(D^g)$. These equalities imply $d = n^{2g}$ provided we can find a D for which $(D^g) \neq 0$. Choose D to be very ample (see (7.2)), and let $A \subset \mathbb{P}^N$ be the embedding defined by $|D|$. Then for any hyperplane sections $H_1, \dots, H_g$ of A in $\mathbb{P}^N$, $(D^g) = (H_1, \dots, H_g)$, and this is obviously positive.

It remains to prove the second assertion of the theorem. For a homomorphism $f: A \to B$, let $(df)_0: T_0(A) \to T_0(B)$ be the map on tangent spaces defined by f. It is neither surprising nor difficult to show that $d(f+g)_0 = (df)_0 + (dg)_0$ (cf. [16, §4, p. 42]). Therefore $(dn_A)_0$ is multiplication by n on the k-vector-space $T_0(A)$, and so $(dn_A)_0$ is an isomorphism (and n_A is étale at zero) if and only if the characteristic of k does not divide n. By using the translation maps, one shows that a homomorphism is étale at zero if and only if it is étale at all points. $\square$

Remark 8.4. If k is separably algebraically closed and n is not divisible by its characteristic, then the theorem says that the kernel $A_n(k)$ of $n: A(k) \to A(k)$ has n^{2g} elements. As this is also true for all n' dividing n, it follows that $A_n(k)$ is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank $2g$. Therefore for all primes $l \neq \text{char}(k)$, $T_lA \overset{\text{df}}{=} \varprojlim A_{l^n}(k)$ is a free $\mathbb{Z}_l$-module of rank $2g$. Note that an element $a = (a_n)$ of T_lA is a sequence $a_1, a_2, a_3, \dots$ of elements of $A(k)$ such that $la_1 = 0$ and $la_n = a_{n-1}$ for all n.

When k is not separably algebraically closed then we define $T_lA = T_lA_{k_s}$. In this case there is a continuous action of $\text{Gal}(k_s/k)$ on T_lA.

Remark 8.5. Assume that k is algebraically closed of characteristic $p \neq 0$. Then $A_p \overset{\text{df}}{=} \text{Ker}(p_A)$ is a finite group scheme of order p^{2g} killed by p. Therefore (see [22]) $A_p \approx (\mathbb{Z}/p\mathbb{Z})^r \times \mu_p^s \times \alpha_p^t$ for some r, s, t such that $r + s + t = 2g$. It is known that $r = s$ and $r \leq g$ (the inequality is a consequence of the fact that

[ere: Suppose A is a supersingular elliptic curve. Then Milne claims ... Mat claims this is completely wrong; since $E[p]$ is not killed by ... He says A_p is ...]

$(dp_A)_0 = 0$). All values of r, s, and t are possible subject to these constraints. The case $r = g$ is the "general" case. For example when $g = 1$, then $r = 0$ only for supersingular elliptic curves and there are only finitely many of these over a given k [16, §22, p. 216].

§9. The Dual Abelian Variety: Definition

Let $\mathcal{L}$ be an invertible sheaf on A. Recall (6.8) that the map

$$\varphi_{\mathcal{L}}: A(k) \to \text{Pic}(A), \qquad a \mapsto t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}$$

is a homomorphism. Define

$$K_{\mathcal{L}} = \{a \in A \mid \text{the restriction of } m^*\mathcal{L} \otimes q^*\mathcal{L}^{-1} \text{ to } \{a\} \times A \text{ is trivial}\}.$$

According to (5.3), $K_{\mathcal{L}}$ is a closed subset of A, and we regard it as a reduced subscheme of A. For a in $A(k)$, the maps

$$A = \{a\} \times A \subset A \times A \underset{q}{\overset{m}{\rightrightarrows}} A$$

$$\text{send} \quad P \longmapsto (a, P) \begin{matrix} \mapsto a + P \\ \mapsto P \end{matrix},$$

and so $m^*\mathcal{L} \otimes q^*\mathcal{L}^{-1}|_{\{a\} \times A}$ can be identified with $t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}$ on A. Thus

$$K_{\mathcal{L}}(k) = \{a \in A(k) \mid t_a^*\mathcal{L} \approx \mathcal{L}\}.$$

Note that (6.2) implies that the definition of $K_{\mathcal{L}}$ commutes with a change of the base field.

Proposition 9.1. *Let $\mathcal{L}$ be an invertible sheaf such that $H^0(A, \mathcal{L}) \neq 0$. Then $\mathcal{L}$ is ample if and only if $K_{\mathcal{L}}$ has dimension zero, i.e., if and only if $t_a^*\mathcal{L} \approx \mathcal{L}$ on $A_{\bar{k}}$ for only a finite set of $a \in A(\bar{k})$.*

PROOF. Let s be a nonzero global section of $\mathcal{L}$, and let D be its divisor of zeros. Then D is effective and $\mathcal{L} = \mathcal{L}(D)$, and so the result [16, §6, p. 60] applies. $\square$

We shall be more concerned in this section with the $\mathcal{L}$ of opposite type.

Proposition 9.2. *For $\mathcal{L}$ an invertible sheaf on A, the following conditions are equivalent:*

(a) $K_{\mathcal{L}} = A$;
(b) $t_a^*\mathcal{L} \approx \mathcal{L}$ *on* $A_{\bar{k}}$ *for all* $a \in A(\bar{k})$;
(c) $m^*\mathcal{L} \approx p^*\mathcal{L} \otimes q^*\mathcal{L}$.

PROOF. The equivalence of (a) and (b) follows from the remarks in the first paragraph of this section. Clearly (c) implies that for all $a \in A$,

$m^*\mathscr{L} \otimes q^*\mathscr{L}^{-1}|_{\{a\}\times A} \approx p^*\mathscr{L}|_{\{a\}\times A}$, which is trivial. Thus (c) implies (a), and the converse follows easily from the seesaw principle (5.2) because $m^*\mathscr{L} \otimes q^*\mathscr{L}^{-1}|_{\{a\}\times A}$ and $p^*\mathscr{L}|_{\{a\}\times A}$ are both trivial for all $a \in A$ and $m^*\mathscr{L} \otimes q^*\mathscr{L}^{-1}|_{A\times\{0\}} = \mathscr{L} = p^*\mathscr{L}|_{A\times\{0\}}$. □

Define $\mathrm{Pic}^0(A)$ to be the group of isomorphism classes of invertible sheaves on A satisfying the conditions of (9.2). Note that if f and g are maps from some k-scheme S into A and $\mathscr{L} \in \mathrm{Pic}^0(A)$, then

$$(f+g)^*\mathscr{L} \approx (f,g)^*m^*\mathscr{L} \overset{(c)}{\approx} (f,g)^*(p^*\mathscr{L} \otimes q^*\mathscr{L}) \approx f^*\mathscr{L} \otimes g^*\mathscr{L}.$$

From this it follows that $n^*\mathscr{L} \approx \mathscr{L}^n$ all $n \in \mathbb{Z}$, $\mathscr{L} \in \mathrm{Pic}^0(A)$.

Remark 9.3. An invertible sheaf $\mathscr{L}$ lies in $\mathrm{Pic}^0 A$ if and only if it occurs in an algebraic family containing a trivial sheaf, i.e., there exists a connected variety T and an invertible sheaf $\mathscr{M}$ on $A \times T$ such that, for some $t_0, t_1 \in T(k)$, $\mathscr{M}_{t_0}$ is trivial and $\mathscr{M}_{t_1} \approx \mathscr{L}$. The sufficiency of the condition can be proved directly using the theorem of the cube [16, §8, (vi)]; the necessity follows from the existence of the dual abelian variety (see below).

Roughly speaking, the dual (or Picard) variety $A^\vee$ of A is an abelian variety over k such that $A^\vee(\bar{k}) = \mathrm{Pic}^0(A_{\bar{k}})$; moreover, there is to be an invertible sheaf (the Poincaré sheaf) $\mathscr{P}$ on $A \times A^\vee$ such that for all $a \in A^\vee(\bar{k})$, the inverse image of $\mathscr{P}$ on $A \times \{a\} = A_{\bar{k}}$ represents a as an element of $\mathrm{Pic}^0(A_{\bar{k}})$. One usually normalizes $\mathscr{P}$ so that $\mathscr{P}|_{\{0\}\times A^\vee}$ is trivial.

The precise definition is as follows: an abelian variety $A^\vee$ is the *dual* abelian variety of A and an invertible sheaf $\mathscr{P}$ on $A \times A^\vee$ is the *Poincaré* sheaf if:

(a) $\mathscr{P}|_{\{0\}\times A^\vee}$ is trivial and $\mathscr{P}|_{A\times\{a\}}$ lies in $\mathrm{Pic}^0(A_{k(a)})$ for all $a \in A^\vee$; and
(b) for every k-scheme T and invertible sheaf $\mathscr{L}$ on $A \times T$ such that $\mathscr{L}|_{\{0\}\times T}$ is trivial and $\mathscr{L}|_{A\times\{t\}}$ lies in $\mathrm{Pic}^0(A_{k(t)})$ for $t \in T$, there is a unique morphism $f: T \to A^\vee$ such that $(1 \times f)^*\mathscr{P} \approx \mathscr{L}$.

Remark 9.4. (a) Clearly the pair $(A^\vee, \mathscr{P})$ is uniquely determined up to a unique isomorphism by these conditions.

(b) On applying condition (b) with $T = \mathrm{spec}\, K$, K a field, one finds that $A^\vee(K) = \mathrm{Pic}^0(A_K)$. In particular $A^\vee(\bar{k}) = \mathrm{Pic}^0(A_{\bar{k}})$, and every element of $\mathrm{Pic}^0(A_{\bar{k}})$ is represented exactly once in the family $(\mathscr{P}_a)_{a\in A^\vee(\bar{k})}$. The map $f: T \to A^\vee$ in condition (b) sends $t \in T(\bar{k})$ to the unique $a \in A^\vee(k)$ such that $\mathscr{L}_t \approx \mathscr{P}_a$.

(c) By using the description of tangent vectors in terms of maps from the dual numbers to $A^\vee$ [10, II, Ex. 2.8], one can show easily that there is a canonical isomorphism $T_0(A^\vee) \overset{\approx}{\to} H^1(A, \mathscr{O}_A)$; in particular, $\dim A^\vee = \dim A$. In the case that $k = \mathbb{C}$, there is an isomorphism $H^1(A, \mathscr{O}_A) \overset{\approx}{\to} H^1(A^{an}, \mathscr{O}_{A^{an}})$ (cohomology relative to the complex topology), and one shows that $\exp: T_0(A^\vee) \to A(\mathbb{C})$ induces an isomorphism $H^1(A^{an}, \mathscr{O}_{A^{an}})/H^1(A^{an}, \mathbb{Z}) \overset{\approx}{\to} A(\mathbb{C})$.

One expects of course that $A^{\vee\vee} = A$. Mumford [16] gives an elegant proof of this.

Proposition 9.5. *Let $\mathscr{P}$ be an invertible sheaf on the product $A \times B$ of two abelian varieties of the same dimension, and assume that the restrictions of $\mathscr{P}$ to $A \times \{0\}$ and $\{0\} \times B$ are both trivial. Then B is the dual of A and $\mathscr{P}$ is the Poincaré sheaf if and only if $\chi(A \times B, \mathscr{P}) = \pm 1$.*

PROOF. [16, §13, p. 131]. □

Note that the second condition is symmetric between A and B; therefore if $(B, \mathscr{P})$ is the dual of A, then $(A, s^*\mathscr{P})$ is the dual of A, where $s: B \times A \to A \times B$ is the morphism switching the factors.

§10. The Dual Abelian Variety: Construction

We can include only a brief sketch—for the details, see [16, §8, §§10–12].

Proposition 10.1. *Let $\mathscr{L}$ be an invertible sheaf on A; then the image of $\varphi_{\mathscr{L}}: A(k) \to \mathrm{Pic}(A)$ is contained in $\mathrm{Pic}^0(A)$; if $\mathscr{L}$ is ample and k is algebraically closed, then $\varphi_{\mathscr{L}}$ maps onto $\mathrm{Pic}^0(A)$.*

PROOF. Let $b \in A(k)$; in order to show that $\varphi_{\mathscr{L}}(b)$ is in $\mathrm{Pic}^0(A)$, we have to check that $t_a^*(\varphi_{\mathscr{L}}(b)) = \varphi_{\mathscr{L}}(b)$ for all $a \in A(\bar{k})$. But

$$t_a^*(\varphi_{\mathscr{L}}(b)) = t_a^*(t_b^*\mathscr{L} \otimes \mathscr{L}^{-1}) = t_{a+b}^*\mathscr{L} \otimes (t_a^*\mathscr{L})^{-1},$$

which the theorem of the square (6.7) shows to be isomorphic to

$$t_b^*\mathscr{L} \otimes \mathscr{L}^{-1} = \varphi_{\mathscr{L}}(b).$$

This shows that $\varphi_{\mathscr{L}}$ maps into $\mathrm{Pic}^0(A)$, and for the proof that it maps onto, we refer the reader to [16, §8, p. 77]. □

Let $\mathscr{L}$ be an invertible sheaf on A, and consider

$$\mathscr{L}^* = m^*\mathscr{L} \otimes p^*\mathscr{L}^{-1} \otimes q^*\mathscr{L}^{-1}$$

on $A \times A$. Then $\mathscr{L}^*|_{\{0\}\times A} = \mathscr{L} \otimes \mathscr{L}^{-1}$, which is trivial, and for a in $A(\bar{k})$, $\mathscr{L}^*|_{A\times\{a\}} = t_a^*\mathscr{L} \otimes \mathscr{L}^{-1} = \varphi_{\mathscr{L}}(a)$, which, as we have just seen, lies in $\mathrm{Pic}^0(A_{\bar{k}})$. Therefore, if $\mathscr{L}$ is ample, then $\mathscr{L}^*$ defines a family of sheaves on A parametrized by A such that each element of $\mathrm{Pic}^0(A_{\bar{k}})$ is represented by $\mathscr{L}_a^*$ for a (nonzero) finite number of a in $A(\bar{k})$. Consequently, if $(A^\vee, \mathscr{P})$ exists, then there is a unique isogeny $\varphi: A \to A^\vee$ such that $(1 \times \varphi)^*\mathscr{P} = \mathscr{L}^*$. Moreover $\varphi = \varphi_{\mathscr{L}}$, and the fibres of $A(\bar{k}) \to A^\vee(\bar{k})$ are the equivalence classes for the relation "$a \sim a'$ if and only if $\mathscr{L}_a \approx \mathscr{L}_{a'}$".

In characteristic zero, we even know what the kernel of φ as a finite

subgroup scheme of A must be because it is determined by its underlying set: it equals $K_{\mathscr{L}}$ with its unique reduced subscheme structure. Therefore, in this case we define $A^\vee$ to be the quotient $A/K_{\mathscr{L}}$ (see [16, §7, p. 66 or §12, p. 111] for the construction of quotients). The action of $K_{\mathscr{L}}$ on the second factor of $A \times A$ lifts to an action on $\mathscr{L}^*$ over $A \times A$, and on forming the quotient we obtain a sheaf $\mathscr{P}$ on $A \times A^\vee$ such that $(1 \times \varphi_{\mathscr{L}})^*\mathscr{P} = \mathscr{L}^*$.

Assume further that k is algebraically closed. It easy to check that the pair $(A^\vee, \mathscr{P})$ just constructed has the correct universal property for families of sheaves $\mathscr{M}$ parametrized by normal k-schemes. Let $\mathscr{M}$ on $A \times T$ be such a family, and let $\mathscr{F}$ be the invertible sheaf $q_{12}^*\mathscr{M} \otimes q_{13}^*\mathscr{P}^{-1}$ on $A \times T \times A^\vee$, where q_{ij} is the projection onto the (i, j)th factor. Then $\mathscr{F}|_{A\times(t,b)} \approx \mathscr{M}_t \otimes \mathscr{P}_b^{-1}$, and so if we let Γ denote the closed subset of $T \times A^\vee$ of points $(t; b)$ such $\mathscr{F}|_{A\times(t,b)}$ is trivial, then $\Gamma(k)$ is the graph of a map $T(k) \to A^\vee(k)$ sending a point t to the unique point b such that $\mathscr{P}_b \approx \mathscr{F}_t$. Regard Γ as a closed reduced subscheme of $T \times A^\vee$. Then the projection $\Gamma \to T$ has separable degree 1 because it induces a bijection on points (see [21, II, 5]). As k has characteristic zero, it must in fact have degree 1, and now the original form of Zariski's Main Theorem [14, III.9, p. 413] shows that $\Gamma \to T$ is an isomorphism. The morphism $f\colon T \approx \Gamma \xrightarrow{q} A^\vee$ has the property that $(1 \times f)^*\mathscr{P} = \mathscr{M}$, as required.

When k has nonzero characteristic, then $A^\vee$ is still the quotient of A by a subgroup $\mathscr{K}_{\mathscr{L}}$ having support $K_{\mathscr{L}}$, but $\mathscr{K}_{\mathscr{L}}$ need not be reduced. Instead one defines $\mathscr{K}_{\mathscr{L}}$ to be the maximal *subscheme* of A such that the restriction of $m^*\mathscr{L} \otimes q^*\mathscr{L}^{-1}$ to $\mathscr{K}_{\mathscr{L}} \times A$ defines a trivial family on A (see 5.5), and takes $A^\vee = A/\mathscr{K}_{\mathscr{L}}$. The proof that this has the correct universal property is similar to the above, but involves much more.

§11. The Dual Exact Sequence

Let $f\colon A \to B$ be a homomorphism of abelian varieties, and let $\mathscr{P}_B$ be the Poincaré sheaf on $B \times B^\vee$. The invertible sheaf $(f \times 1)^*\mathscr{P}_B$ on $A \times B^\vee$ gives rise to a homomorphism $f^\vee\colon B^\vee \to A^\vee$ such that $(1 \times f^\vee)^*\mathscr{P}_A \approx (f \times 1)^*\mathscr{P}_B$. On points f is simply the map $\mathrm{Pic}^0(B) \to \mathrm{Pic}^0(A)$ sending the isomorphism class of an invertible sheaf on B to it inverse image on A.

Theorem 11.1. *If $f\colon A \to B$ is an isogeny with kernel N, then $f^\vee\colon B^\vee \to A^\vee$ is an isogeny with kernel $N^\vee$, the Cartier dual of N. In other words, the exact sequence*

$$0 \to N \to A \to B \to 0$$

gives rise to a dual exact sequence

$$0 \to N^\vee \to B^\vee \to A^\vee \to 0.$$

PROOF. See [16, §15, p. 143]. □

There is another approach to this theorem which offers a different insight. Let $\mathscr{L}$ be an invertible sheaf on A whose class is in $\mathrm{Pic}^0(A)$, and let L be the line bundle associated with $\mathscr{L}$. The isomorphism $p^*\mathscr{L} \otimes q^*\mathscr{L} \to m^*\mathscr{L}$ of (9.2) gives rise to a map $m_L\colon L \times L \to L$ lying over $m\colon A \times A \to A$. The absence of nonconstant regular functions on A forces numerous compatibility properties of m_L, which are summarized by the following statement.

Proposition 11.2. *Let $G(\mathscr{L})$ denote L with the zero section removed; then, for some k-rational point e of $G(\mathscr{L})$, m_L defines on $G(\mathscr{L})$ the structure of a commutative group variety with identity element e relative to which $G(\mathscr{L})$ is an extension of A by $\mathbb{G}_m$.*

Thus $\mathscr{L}$ gives rise to an exact sequence

$$E(\mathscr{L})\colon 0 \to \mathbb{G}_m \to G(\mathscr{L}) \to A \to 0.$$

The commutative group varieties over k form an abelian category, and so it is possible to define $\mathrm{Ext}_k^1(A, \mathbb{G}_m)$ to be the group of classes of extensions of A by $\mathbb{G}_m$ in this category. We have:

Proposition 11.3. *The map $\mathscr{L} \mapsto E(\mathscr{L})$ defines an isomorphism*

$$\mathrm{Pic}^0(A) \to \mathrm{Ext}_k^1(A, \mathbb{G}_m).$$

Proofs of these results can be found in [20, VII, §3]. They show that the sequence

$$0 \to N^\vee(k) \to B^\vee(k) \to A^\vee(k)$$

can be identified with the sequence of Exts

$$0 \to \mathrm{Hom}_k(N, \mathbb{G}_m) \to \mathrm{Ext}_k^1(B, \mathbb{G}_m) \to \mathrm{Ext}_k^1(A, \mathbb{G}_m).$$

(The reason for the zero at the left of the second sequence is that $\mathrm{Hom}_k(A, \mathbb{G}_m) = 0$.)

The isomorphism in (11.3) extends to any base [17, III.18]. This means that if we let $\mathscr{E}xt^r$ denote Ext in the category of sheaves on the flat site over spec(k) (see [13, III.1.5(e)]), then $A^\vee$ can be identified with the sheaf $\mathscr{E}xt^1(A, \mathbb{G}_m)$, and the exact sequence

$$0 \to N^\vee \to B^\vee \to A^\vee \to 0$$

can be identified with

$$0 \to \mathscr{H}om(N, \mathbb{G}_m) \to \mathscr{E}xt^1(B, \mathbb{G}_m) \to \mathscr{E}xt^1(A, \mathbb{G}_m) \to 0.$$

§12. Endomorphisms

The main result in this section is that $\mathrm{End}^0(A) \overset{\mathrm{df}}{=} \mathrm{End}(A) \otimes \mathbb{Q}$ is a finite-dimensional semisimple algebra over $\mathbb{Q}$. As in the classical case, the semi-simplicity follows from the existence of approximate complements for abelian

subvarieties. If W is a subspace of a vector space V, one way of constructing a complement W' for W is to choose a nondegenerate bilinear form on V and take $W' = W^{\perp}$; equivalently, choose an isomorphism $V \to \check{V}$ and take W' to be the kernel of $V \to \check{V} \to \check{W}$. The same method works for abelian varieties.

Proposition 12.1. *Let B be an abelian subvariety of A; then there is an abelian variety $B' \subset A$ such that $B \cap B'$ is finite and $B + B' = A$, i.e., such that $B \times B' \to A$ is an isogeny.*

PROOF. Choose an ample sheaf $\mathscr{L}$ on A and define B' to be the reduced subscheme of the zero component of the kernel of $A \xrightarrow{\phi_{\mathscr{L}}} A^{\vee} \to B^{\vee}$; this is an abelian variety. From the theorem on the dimension of fibres of morphisms, $\dim B' \geq \dim A - \dim B$. The restriction of the morphism $A \to B^{\vee}$ to B is $\phi_{\mathscr{L}|B}\colon B \to B^{\vee}$, which has finite kernel because $\mathscr{L}|B$ is ample. Therefore $B \cap B'$ is finite, and so $B \times B' \to A$ is an isogeny. □

Define an abelian variety to be *simple* if it has no proper nonzero abelian subvarieties. Then, as in the classical case, each abelian variety A is isogenous to a product $\prod A_i^{r_i}$ of powers of nonisogenous simple abelian varieties A_i; the r_i are uniquely determined and the A_i are uniquely determined up to isogeny. Each $\mathrm{End}^0(A_i)$ is a skew field, $\mathrm{End}^0(A_i^{r_i})$ is equal to the matrix algebra $M_{r_i}(\mathrm{End}^0(A_i))$, and $\mathrm{End}^0(A) = \prod \mathrm{End}^0(A_i^{r_i})$.

Lemma 12.2. *For any prime $l \neq \mathrm{char}(k)$, the natural map*

$$\mathrm{Hom}(A, B) \to \mathrm{Hom}_{\mathbb{Z}_l}(T_l A, T_l B)$$

is injective; in particular, $\mathrm{Hom}(A, B)$ is torsion free.

PROOF. Let $\varphi\colon A \to B$ be a homomorphism such that $T_l\varphi = 0$; then $\varphi(A_{l^m}(\bar{k})) = 0$ for all n. For any simple abelian subvariety A' of A, this implies that the kernel of $\varphi|A'$ is not finite and therefore must equal the whole of A'. It follows that $\varphi = 0$. □

A function $f\colon V \to K$ on a vector space V over a field K is said to be a (*homogeneous*) *polynomial function* of degree d if for every finite linearly independent set $\{e_1, \dots, e_n\}$ of elements of V, $f(x_1e_1 + \cdots + x_ne_n)$ is a (homogenous) polynomial function of degree d in the x_i with coefficients in K.

Lemma 12.3. *Assume K is infinite, and let $f\colon V \to K$ be a function such that $f(xv + w)$ is a polynomial in x with coefficients in K, for all v, w in V; then f is a polynomial function.*

PROOF. We show by induction on n that, for every subset $\{v_1, \dots, v_n, w\}$ of V, $f(x_1v_1 + \cdots + x_nv_n + w)$ is a polynomial in the x_i. For $n = 1$, this is true by hypothesis; assume it for $n - 1$. The original hypothesis applied with $v = v_n$ shows that

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

for some d, with the a_i functions $k^{n-1} \to k$. Choose distinct elements $c_0, \dots, c_d$ of K; on solving the system of linear equations

$$f(x_1v_1 + \cdots + x_{n-1}v_{n-1} + c_jv_n + w) = \sum a_i(x_1, \dots, x_{n-1})c_j^i, \quad j = 0, 1, \dots, d,$$

for a_i, we obtain an expression for a_i as a linear combination of the terms $f(x_1v_1 + \cdots + x_{n-1}v_{n-1} + c_jv_n + w)$, which the induction assumption says are polynomials in $x_1, \dots, x_{n-1}$. □

Let A be an abelian variety of dimension g over k. For $\varphi \in \mathrm{End}(A)$, we define $\deg \varphi$ to be the degree of φ in the sense of Section 8 if φ is an isogeny and otherwise we set $\deg \varphi = 0$. As $\deg(n\varphi) = \deg n_A \deg \varphi = n^{2g} \deg \varphi$, we can extend this notion to all of $\mathrm{End}^0(A)$ by setting $\deg \varphi = n^{-2g} \deg(n\varphi)$ if $n\varphi \in \mathrm{End}(A)$.

Proposition 12.4. *The function $\varphi \mapsto \deg \varphi\colon \mathrm{End}^0(A) \to \mathbb{Q}$ is a homogeneous polynomial function of degree $2g$ on $\mathrm{End}^0(A)$.*

PROOF. As $\deg(n\varphi) = n^{2g} \deg \varphi$, the lemma shows that it suffices to prove that $\deg(n\varphi + \psi)$ is a polynomial of degree $\leq 2g$ in n for $n \in \mathbb{Z}$ and fixed φ, $\psi \in \mathrm{End}(A)$. Let D be a very ample divisor on A, and let $D_n = (n\varphi + \psi)^*D$. Then (see (8.3)), $\deg(n\varphi + \psi)(D^g) = (D_n^g)$, where $g = \dim A$, and so it suffices to prove that (D_n^g) is a polynomial of degree $\leq 2g$ in n. Corollary (6.5) applied to the maps $n\varphi + \psi$, φ, $\varphi\colon A \to A$ and the sheaf $\mathscr{L} = \mathscr{L}(D)$ shows that

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

i.e., $$D_{n+2} - 2D_{n+1} + D_n = D', \quad \text{where} \quad D' = 2(\varphi^*D) - (2\varphi)^*D.$$

An induction argument now shows that

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

and so

$$(D_n^g) = \left(\frac{n(n-1)}{2}\right)^g (D'^g) + \cdots$$

is a polynomial in n of degree $\leq 2g$. □

Theorem 12.5. *For any abelian varieties A and B, $\mathrm{Hom}(A, B)$ is a free $\mathbb{Z}$-module of finite rank $\leq 4 \dim A \dim B$; for each prime $l \neq \mathrm{char}(k)$, the natural map*

$$\mathrm{Hom}(A, B) \otimes \mathbb{Z}_l \to \mathrm{Hom}(T_l A, T_l B)$$

is injective with torsion-free cokernel.

PROOF. Clearly it suffices to prove the second statement.

Lemma 12.6. *Let $\varphi \in \mathrm{Hom}(A, B)$; if φ is divisible by l^n in $\mathrm{Hom}(T_lA, T_lB)$, then it is divisible by l^n in $\mathrm{Hom}(A, B)$.*

PROOF. The hypothesis implies that φ is zero on $A_{l^n}(\bar{k})$. As A_{l^n} is an étale subgroup scheme of A, this means that φ is zero on A_{l^n} and therefore factors as $\varphi = \varphi' \circ l^n$:

$$\begin{array}{ccccccc} 0 & \to & A_{l^n} & \to & A & \xrightarrow{l^n} & A \to 0 \\ & & & \searrow^{\varphi} & \downarrow{\scriptstyle \varphi'} & & \\ & & & & B & & \end{array}$$

□

Lemma 12.7. *If A is simple, then $\mathrm{End}(A) \otimes \mathbb{Z}_l \to \mathrm{End}(T_lA)$ is injective.*

PROOF. We have to show that if $e_1, \dots, e_r$ are linearly independent over $\mathbb{Z}$ in $\mathrm{End}(A)$, then $T_l(e_1), \dots, T_l(e_r)$ are linearly independent over $\mathbb{Z}_l$ in $\mathrm{End}(T_lA)$. Let P be the polynomial function on $\mathrm{End}^0(A)$ such that $P(\varphi) = \deg(\varphi)$ for all φ. Note that every nonzero element φ of $\mathrm{End}(A)$ is an isogeny, and therefore $P(\varphi)$ is a positive integer. Let M be the $\mathbb{Z}$-submodule of $\mathrm{End}^0(A)$ generated by the e_i. The map $P: \mathbb{Q}M \to \mathbb{Q}$ is continuous for the real topology, and so $U = \{v \mid P(v) < 1\}$ is an open neighborhood of 0. As $(\mathbb{Q}M \cap \mathrm{End}\ A) \cap U = 0$, we see that $\mathbb{Q}M \cap \mathrm{End}(A)$ is discrete in $\mathbb{Q}M$, and therefore is a finitely generated $\mathbb{Z}$-module. It follows that:

(*) there exists an integer N such that $N(\mathbb{Q}M \cap \mathrm{End}\ A) \subset M$.

Suppose that $T_l(e_1), \dots, T_l(e_r)$ are linearly dependent, so that there exist $a_i \in \mathbb{Z}_l$, not all divisible by l, such that $\sum a_i T_l(e_i) = 0$. Choose integers n_i close to the a_i for the l-adic topology. Then $T_l(\sum n_i e_i) = \sum n_i T_l(e_i)$ is divisible by a high power of l in $\mathrm{End}(T_lA)$, and so $\sum n_i e_i$ is divisible by a high power of l in $\mathrm{End}(A)$. This contradicts (*) when the power is sufficiently great, because then, for some m, $(N/l^m)\sum n_i e_i$ will lie in $N(\mathbb{Q}M \cap \mathrm{End}\ A)$ but not M. □

We are now ready to prove (12.5). Because $\mathrm{Hom}(A, B)$ and $\mathrm{Hom}(T_lA, T_lB)$ are direct summands of $\mathrm{End}(A \times B)$ and $\mathrm{End}(T_l(A \times B))$, it suffices to prove (12.5) in the case that $A = B$. Lemma 12.7 shows that $\mathrm{End}^0(A)$ is finite dimensional over $\mathbb{Q}$ if A is simple, and this implies that it is finite dimensional for all A. It follows that $\mathrm{End}(A)$ is finitely generated over $\mathbb{Z}$ because it is obviously torsion-free. Clearly now condition (*) holds, and so the same argument as above shows that $\mathrm{End}(A) \otimes \mathbb{Z}_l \to \mathrm{End}(T_lA)$ is injective. Lemma 12.6 shows that its cokernel is torsion-free. □

Define the *Néron–Severi group* $\mathrm{NS}(A)$ of an abelian variety to be the quotient group $\mathrm{Pic}(A)/\mathrm{Pic}^0(A)$. Clearly $\mathscr{L} \mapsto \varphi_{\mathscr{L}}$ defines an injection $\mathrm{NS}(A) \hookrightarrow \mathrm{Hom}(A, A^\vee)$, and so (12.5) has the following consequence.

Corollary 12.8. *The Néron–Severi group of an abelian variety is a free $\mathbb{Z}$-module of finite rank.*

Characteristic Polynomial of an endomorphism.

Proposition 12.4 shows that, for each α in $\mathrm{End}^0(A)$, there is a polynomial $P_\alpha(X) \in \mathbb{Q}[X]$ of degree $2g$ such that, for all rational numbers r, $P_\alpha(r) = \deg(\alpha - r_A)$. Let $\alpha \in \mathrm{End}(A)$, and let D be an ample symmetric divisor on A; then the calculation in the proof of (12.4) shows that

$$P_\alpha(-n) = \deg(\alpha + n) = (D_n^g)/(D^g),$$

where $D_n = (n(n-1)/2)D' + n(\alpha + 1_A)^*D - (n-1)\alpha^*D$, with

$$D' = 2D - 2_A^*D \sim 2D.$$

In particular, we see that P_α is monic and that it has integer coefficients when $\alpha \in \mathrm{End}(A)$. We call P_α the *characteristic polynomial* of α and we define the *trace* of α by the equation

$$P_\alpha(X) = X^{2g} - \mathrm{Tr}(\alpha)X^{2g-1} + \cdots + \deg(\alpha).$$

Proposition 12.9. *For all $l \neq \mathrm{char}(k)$, $P_\alpha(X)$ is the characteristic polynomial of α acting on $T_lA \otimes \mathbb{Q}_l$; hence the trace and degree of α are the trace and determinant of α acting on $T_lA \otimes \mathbb{Q}_l$.*

PROOF. We need two elementary lemmas.

Lemma 12.10. *Let $P(X) = \prod(X - a_i)$ and $Q(X) = \prod(X - b_i)$ be monic polynomials of the same degree with coefficients in $\mathbb{Q}_l$; if $|\prod F(a_i)|_l = |\prod F(b_i)|_l$ for all $F \in \mathbb{Z}[T]$, then $P = Q$.*

PROOF. See [12, VII, 1, Lemma 1]. □

Lemma 12.11. *Let E be an algebra over a field K, and let $\delta: E \to K$ be a polynomial function on E (regarded as a vector space over K) such that $\delta(\alpha\beta) = \delta(\alpha)\delta(\beta)$ for all $\alpha, \beta \in E$. Let $\alpha \in E$, and let $P = \prod(X - a_i)$ be the polynomial such that $P(x) = \delta(\alpha - x)$. Then $\delta(F(\alpha)) = \pm\prod F(a_i)$ for any $F \in K[T]$.*

PROOF. After extending K, we may assume that the roots $b_1, b_2, \dots$ of F and of P lie in K; then

$$\begin{aligned} \delta(F(\alpha)) &= \delta\left(\prod_j (\alpha - b_j)\right) = \prod_j \delta(\alpha - b_j) = \prod_j P(b_j) = \prod_{i,j}(b_j - a_i) \\ &= \pm\prod_i F(a_i). \end{aligned}$$

□

We now prove (12.9). Clearly we may assume $k = k_s$. For any $\beta \in \mathrm{End}(A)$

$$\begin{aligned} |\deg(\beta)|_l &= |\#(\mathrm{Ker}(\beta))|_l = \#(\mathrm{Ker}(\beta)(l))^{-1} \\ &= \#(\mathrm{Coker}(T_l\beta))^{-1} = |\det(T_l\beta)|_l. \end{aligned}$$

Consider $\alpha \in \mathrm{End}(A)$, and let $a_1, a_2, \dots$ be the roots of P_α. Then for any

polynomial $F \in \mathbb{Z}[T]$.

$$|\textstyle\prod F(a_i)|_l = |\deg F(\alpha)|_l \qquad \text{by (12.11)}$$
$$= |\det T_l(F(\alpha))|_l$$
$$= |\textstyle\prod F(b_i)|_l, \qquad \text{by (12.11)}$$

where the b_i are the eigenvalues of $T_l\beta$. By Lemma 12.10, this proves the proposition. □

Let D be a simple algebra of finite degree over $\mathbb{Q}$, and let K be the centre of D. The reduced trace and reduced norm of D over K satisfy

$$\mathrm{Tr}_{D/K}(\alpha) = [D:K]\,\mathrm{Trd}_{D/K}(\alpha), \qquad \mathrm{N}_{D/K}(\alpha) = \mathrm{Nrd}_{D/K}(\alpha)^{[D:K]}, \qquad \alpha \in D.$$

We shall always set $\mathrm{Trd} = \mathrm{Tr}_{K/\mathbb{Q}} \circ \mathrm{Trd}_{D/K}$ and $\mathrm{Nrd} = \mathrm{N}_{K/\mathbb{Q}} \circ \mathrm{Nrd}_{D/K}$. Let $V_1, \dots, V_f$, $f = [K:\mathbb{Q}]$, be the nonisomorphic representations of D over $\bar{\mathbb{Q}}$; each has degree d where $d^2 = [D:K]$. The representation $V = \bigoplus V_i$ is defined over $\mathbb{Q}$ and is called the reduced representation of D. For any α in D, $\mathrm{Trd}(\alpha) = \mathrm{Tr}(\alpha|V)$ and $\mathrm{Nrd}(\alpha) = \mathrm{Det}(\alpha|V)$.

Proposition 12.12. *Let D be a simple subalgebra of $\mathrm{End}^0(A)$ (this means D and $\mathrm{End}^0(A)$ have the same identity element), and let d, f, K, and V be as above. Then $2g/fd$ is an integer, and $\mathbb{Q}_l \otimes T_l A$ is a direct sum of $2g/fd$ copies of $\mathbb{Q}_l \otimes_{\mathbb{Q}} V$; consequently $\mathrm{Tr}(\alpha) = (2g/fd)\,\mathrm{Trd}(\alpha)$ and $\deg(\alpha) = \mathrm{Nrd}(\alpha)^{2g/fd}$ for all α in D.*

PROOF. Assume $\mathbb{Q}_l \otimes T_l V$ becomes isomorphic to $\bigoplus m_i V_i$ over $\bar{\mathbb{Q}}_l$, $m_i \geq 0$, and let σ_i be the embedding of K into $\bar{\mathbb{Q}}$ corresponding to V_i. Then, for any α in K, the characteristic polynomial of α on V_i is $(X - \sigma_i\alpha)^d$, and so $P_\alpha(X) = \prod (X - \sigma_i\alpha)^{dm_i}$. As $P_\alpha(X)$ has coefficients in $\mathbb{Q}$, it follows easily that the m_i must be equal. □

Remark 12.13. The group $\mathrm{NS}(A)$ is a functor of A. Direct calculations show that t_a acts as the identity on $\mathrm{NS}(A)$ for all a in $A(k)$ (because $\varphi_{t_a^*\mathscr{L}} = \varphi_{\mathscr{L}}$) and n acts as n^2 (because -1 acts as 1, and so $n^*\mathscr{L} = \mathscr{L}^{n^2}$ in $\mathrm{NS}(A)$ by (6.6)).

§13. Polarizations and the Cohomology of Invertible Sheaves

For many purposes the correct higher dimensional analogue of an elliptic curve is not an abelian variety but a polarized abelian variety.

A *polarization* λ on an abelian variety A is an isogeny $\lambda: A \to A^\vee$ such that $\lambda_{\bar{k}} = \varphi_{\mathscr{L}}$ for some ample invertible sheaf $\mathscr{L}$ on $A_{\bar{k}}$. The *degree* of a polarization is its degree as an isogeny. An abelian variety together with a polarization is called a *polarized abelian variety*; there is an obvious notion of a morphism of polarized abelian varieties. If λ has degree 1, then (A, λ) is said to belong to the *principal family* and λ is said to be a *principal polarization*.

Example 13.1. If A has dimension 1, then $\mathrm{NS}(A) = \mathbb{Z}$. For each integer d, there is a unique polarization of degree d^2; it is $\varphi_{\mathscr{L}}$ where $\mathscr{L} = \mathscr{L}(D)$ for D any effective divisor of degree d.

Remark 13.2. If λ is a polarization, there need not exist an $\mathscr{L}$ on A such that $\lambda = \varphi_{\mathscr{L}}$. Suppose, for example, that k is perfect and $G = \mathrm{Gal}(\bar{k}/k)$. By assumption, there is an $\mathscr{L}$ on $A_{\bar{k}}$ such that $\varphi_{\mathscr{L}} = \lambda_{\bar{k}}$. As $\lambda_{\bar{k}}$ is fixed by the action of G on $\mathrm{Hom}(A_{\bar{k}}, A_{\bar{k}}^\vee)$, the class $[\mathscr{L}]$ of $\mathscr{L}$ in $\mathrm{NS}(A_{\bar{k}})$ will also be fixed by G. Unfortunately this does not imply that $[\mathscr{L}]$ lifts to an element of $\mathrm{Pic}(A)$: there is a sequence of Galois cohomology groups

$$0 \to A^\vee(k) \to \mathrm{Pic}(A) \to \mathrm{NS}(A_{\bar{k}})^G \to H^1(G, A^\vee(\bar{k}))$$

and the obstruction in $H^1(G, A^\vee(\bar{k}))$ may be nonzero. However, if k is finite, an easy lemma [16, §21, p. 205] shows that $H^1(G, A^\vee(\bar{k})) = 0$ and therefore $\lambda = \varphi_{\mathscr{L}}$ for some $\mathscr{L}$ in $\mathrm{Pic}(A)$.

There is an important formula for the degree of a polarization, which it is convenient to state as part of a more general theorem.

Theorem 13.3. *Let $\mathscr{L}$ be an invertible sheaf on A, and write*

$$\chi(\mathscr{L}) = \textstyle\sum (-1)^i \dim_k H^i(A, \mathscr{L}).$$

(a) *The degree of $\varphi_{\mathscr{L}}$ is $\chi(\mathscr{L})^2$.*
(b) *(Riemann–Roch). If $\mathscr{L} = \mathscr{L}(D)$, then $\chi(\mathscr{L}) = (D^g)/g!$.*
(c) *If $\dim K_{\mathscr{L}} = 0$, then there is exactly one integer r for which $H^r(A, \mathscr{L})$ is nonzero.*

PROOF. Combine [16, §16, p. 150] with (4.2a). □

Exercise 13.4. Verify (13.3) for elliptic curves using only the results in [10, IV].

Remark 13.5. The definition of polarization we have adopted is the one that is most useful for moduli questions. It differs from Weil's original notion (see [12, p. 193], [19, §5]).

§14. A Finiteness Theorem

Theorem 14.1. *Let k be a finite field, and let g and d be positive integers. Up to isomorphism, there are only finitely many abelian varieties A over k of dimension g possessing a polarization of degree d^2.*

PROOF. First assume dim $A = 1$. Then A automatically has a polarization of degree 1, defined by $\mathscr{L} = \mathscr{L}(P)$ for any $P \in A(k)$. The linear system $|3P|$ defines an embedding $A \subset \mathbb{P}^2$, and the image is a cubic curve in $\mathbb{P}^2$. The cubic curve is determined by a polynomial of degree 3 in three variables. As there are only finitely many such polynomials with coefficients in k, we have shown that there are only finitely many isomorphism classes of A's.

The proof in the general case is essentially the same. By (13.2) we know there exists an ample invertible sheaf $\mathscr{L}$ on A such that $\varphi_{\mathscr{L}}$ is a polarization of degree d^2. Let $\mathscr{L} = \mathscr{L}(D)$; then, by (13.3), $\chi(\mathscr{L}) = d$ and $(D^g) = \chi(\mathscr{L})g! = d(g!)$. As $\mathscr{L}^3 = \mathscr{L}(3D)$, $\chi(\mathscr{L}^3) = ((3D)^g)/g! = 3^g d$. Moreover $\mathscr{L}^3$ is very ample (see (7.3)); in particular $H^0(A, \mathscr{L}^3) \neq 0$, and so (13.3c) shows that $\dim H^0(A, \mathscr{L}^3) = \chi(\mathscr{L}^3) = 3^g d$. The linear system $|3D|$ therefore gives an embedding $A \subset \mathbb{P}^{3^g d - 1}$.

Recall [21, I.6] that if V is a smooth variety of dimension g in $\mathbb{P}^N$, then the *degree* of V is $(D_1, \dots, D_g)$ where $D_1, \dots, D_g$ are hyperplane sections of V. Moreover, there is a polynomial, called the *Cayley* or *Chow form* of V,

$$F_V(a_0^{(0)}, \dots, a_N^{(0)}; \dots; a_0^{(g)}, \dots, a_N^{(g)})$$

associated with V, which is a polynomial separately homogeneous of degree $\deg V$ in each of $g + 1$ sets of $N + 1$ variables. If we regard each set of variables $a_0^{(i)}, \dots, a_N^{(i)}$ as defining a hyperplane,

$$H^{(i)}\colon a_0^{(i)} X_0 + \cdots + a_N^{(i)} X_N = 0,$$

then F_V is defined by the condition:

$$F_V(H^{(0)}, \dots, H^{(g)}) = 0 \Leftrightarrow A \cap H^{(0)} \cap \cdots \cap H^{(g)} \text{ is nonempty.}$$

A theorem states that F_V uniquely determines V.

Returning to the proof of (14.1), we see that the degree of A in $\mathbb{P}^{3^g d - 1}$ is $((3D)^g) = 3^g d(g!)$. It is therefore determined by a polynomial F_A of degree $3^g d(g!)$ in each of $g + 1$ sets of $3^g d$ variables with coefficients in k. There are only finitely many such polynomials.

Remark 14.2. Of course, Theorem 14.1 is trivial if one assumes the existence of moduli varieties. However, everything used in the above proof (and much more) is required for the construction of moduli varieties.

Remark 14.3. The assumption that A has a polarization of a given degree plays a crucial role in the above proof. Nevertheless, we shall see in (18.9) below that it can be removed from the statement of the theorem.

§15. The Étale Cohomology of an Abelian Variety

The usual cohomology groups $H^r(A(\mathbb{C}), \mathbb{Z})$ of an abelian variety are described by the statements:

(a) A representation of $A(\mathbb{C})$ as a quotient $A(\mathbb{C}) = \mathbb{C}^g/L$ determines an isomorphism $H^1(A(\mathbb{C}), \mathbb{Z}) \xrightarrow{\approx} \operatorname{Hom}(L, \mathbb{Z})$.
(b) The cup-product pairings define isomorphisms

$$\Lambda^r H^1(A(\mathbb{C}), \mathbb{Z}) \xrightarrow{\approx} H^r(A(\mathbb{C}), \mathbb{Z}) \quad \text{for all } r.$$

To prove (a), note that $\mathbb{C}^g$ is the universal covering space of $A(\mathbb{C})$, and that L is its group of covering transformations. Therefore, $\pi_1(A(\mathbb{C}), 0) = L$, and for any pointed manifold (M, m), $H^1(M, \mathbb{Z}) = \operatorname{Hom}(\pi_1(M, m), \mathbb{Z})$. Statement (b) can be proved by observing that $A(\mathbb{C})$ is homeomorphic to a product of $2g$ circles and using the Künneth formula (see [16, §1, p. 3]), or by using the same argument as that given below for the étale topology.

Theorem 15.1. *Let A be an abelian variety of dimension g over an algebraically closed field k, and let l be a prime different from* $\operatorname{char}(k)$.

(a) *There is a canonical isomorphism $H^1(A_{et}, \mathbb{Z}_l) \xrightarrow{\approx} \operatorname{Hom}_{\mathbb{Z}_l}(T_l A, \mathbb{Z}_l)$.*
(b) *The cup-product pairings define isomorphisms*

$$\Lambda^r H^1(A_{et}, \mathbb{Z}_l) \xrightarrow{\approx} H^r(A_{et}, \mathbb{Z}_l) \quad \textit{for all } r.$$

In particular, $H^r(A_{et}, \mathbb{Z}_l)$ is a free $\mathbb{Z}_l$-module of rank $\binom{2g}{r}$.

PROOF. If $\pi_1^{et}(A, 0)$ now denotes the étale fundamental group, then $H^1(A, \mathbb{Z}_l) = \operatorname{Hom}_{\text{conts}}(\pi_1^{et}(A, 0), \mathbb{Z}_l)$. For each n, $l_A^n\colon A \to A$ is a finite étale covering of A with group of covering transformations $\operatorname{Ker}(l_A^n) = A_{l^n}(k)$. By definition $\pi_1^{et}(A, 0)$ classifies such coverings, and therefore there is a canonical epimorphism $\pi_1^{et}(A, 0) \twoheadrightarrow A_{l^n}(k)$ (see [13, I.5]). On passing to the inverse limit, we get an epimorphism $\pi_1^{et}(A, 0) \twoheadrightarrow T_l A$, and consequently an injection $\operatorname{Hom}_{\mathbb{Z}_l}(T_l A, \mathbb{Z}_l) \subset H^1(A, \mathbb{Z}_l)$.

To proceed further we need to work with other coefficient groups. Let R be $\mathbb{Z}_l$, $\mathbb{F}_l$, or $\mathbb{Q}_l$, and write $H^*(A)$ for $\bigoplus_{r \geq 0} H^r(A_{et}, R)$. The cup-product pairing makes this into a graded, associative, anticommutative algebra. There is a canonical map $H^*(A) \otimes H^*(A) \to H^*(A \times A)$, which the Künneth formula shows to be an isomorphism when R is a field. In this case, the addition map $m\colon A \times A \to A$ defines a map

$$m^*\colon H^*(A) \to H^*(A \times A) = H^*(A) \otimes H^*(A).$$

Moreover, the map $a \mapsto (a, 0)\colon A \to A \times A$ identifies $H^*(A)$ with the direct summand $H^*(A) \otimes H^0(A)$ of $H^*(A) \otimes H^*(A)$. As $m \circ (a \mapsto (a, 0)) = \mathrm{id}$, the projection of $H^*(A) \otimes H^*(A)$ onto $H^*(A) \otimes H^0(A)$ sends $m^*(x)$ to $x \otimes 1$. As the same remark applies to $a \mapsto (0, a)$, this shows that

$$m^*(x) = x \otimes 1 + 1 \otimes x + \sum x_i \otimes y_i, \qquad \deg(x_i), \deg(y_i) > 0.$$

Lemma 15.2. *Let H^* be a graded, associative, anticommutative algebra over a perfect field K. Assume that there is map $m^*\colon H^* \to H^* \otimes H^*$ satisfying the above identity. If $H^0 = K$ and $H^r = 0$ for all r greater than some integer d, then*

$\dim(H^1) \le d$, and when equality holds, H^* is isomorphic to the exterior algebra on H^1.

PROOF. A fundamental structure theorem for Hopf algebras [3, Theorem 6.1] shows that H^* is equal to the associative algebra generated by certain elements x_i subject only to the relations imposed by the anticommutativity of H^* and the nilpotence of each x_i. The product of the x_i has degree $\sum \deg(x_i)$, from which it follows that $\sum \deg(x_i) \le d$. In particular, the number of x_i of degree 1 is $\le d$; as this number is equal to the dimension of H^1, this shows that its dimension is $\le d$. When equality holds, all the x_i must have degree 1; moreover their squares must all be zero because otherwise there would be a nonzero element $x_1 x_2 \dots x_i^2 \dots x_d$ of degree $d+1$. Hence H^* is identified with the exterior algebra on H^1. □

When R is $\mathbb{Q}_l$ or $\mathbb{F}_l$, the conditions of the lemma are fulfilled with $d = 2g$ [13, VI, 1.1]. Therefore $H^1(A, \mathbb{Q}_l)$ has dimension $\le 2g$. But $H^1(A, \mathbb{Q}_l) = H^1(A, \mathbb{Z}_l) \otimes \mathbb{Q}_l$, and so the earlier calculation shows that $H^1(A, \mathbb{Q}_l)$ has dimension $2g$. The lemma now shows that $H^r(A, \mathbb{Q}_l) = \Lambda^r(H^1(A, \mathbb{Q}_l))$, and, in particular, that its dimension is $\binom{2g}{r}$. This implies that $H^r(A, \mathbb{Z}_l)$ has rank $\binom{2g}{r}$. The exact sequence [13, V, 1.11]

$$\cdots \to H^r(A, \mathbb{Z}_l) \xrightarrow{l} H^r(A, \mathbb{Z}_l) \to H^r(A, \mathbb{F}_l) \to H^{r+1}(A, \mathbb{Z}_l) \xrightarrow{l} H^{r+1}(A, \mathbb{Z}_l) \to \cdots$$

now shows that $\dim(H^1(A, \mathbb{F}_l)) \ge 2g$, and so the lemma implies that this dimension equals $2g$ and that $\dim(H^r(A, \mathbb{F}_l)) = \binom{2g}{r}$. On looking at the exact sequence again, we see that $H^r(A, \mathbb{Z}_l)$ must be torsion-free for all r. Consequently, $\Lambda^r H^1(A, \mathbb{Z}_l) \to H^r(A, \mathbb{Z}_l)$ is injective because it becomes so when tensored with $\mathbb{Q}_l$, and it is surjective because it becomes so when tensored with $\mathbb{F}_l$. This completes the proof.

Remark 15.3. In the course of the above proof, we have shown that the maximal abelian l-quotient of $\pi_1^{et}(A, 0)$ is isomorphic to $T_l A$. In fact, it is known that $\pi_1^{et}(A, 0) = TA$, where $TA = \varprojlim A_n(k)$. In order to prove this one has to show that the all finite étale coverings of A are isogenies. This is accomplished by the following theorem ([14, §18, p. 167]): *Let A be an abelian variety over an algebraically closed field, and let $f: B \to A$ be a finite étale covering with B connected; then it is possible to define on B the structure of an abelian variety relative to which f is an isogeny.*

Remark 15.4. We have shown that the following three algebras are isomorphic:

(i) $H^*(A, \mathbb{Z}_l)$ with its cup-product structure;
(ii) $\Lambda^* H^1(A, \mathbb{Z}_l)$ with its wedge-product structure;
(iii) the dual of $\Lambda^* T_l A$ with its wedge-product structure.

If we denote the pairing

$$T_l A \times H^1(A, \mathbb{Z}_l) \to \mathbb{Z}_l$$

by $\langle \cdot | \cdot \rangle$, then the pairing

$$\Lambda^r T_l A \times H^r(A, \mathbb{Z}_l) \to \mathbb{Z}_l$$

is determined by

$$(a_1 \wedge \cdots \wedge a_r, b_1 \cup \cdots \cup b_r) = \det(\langle a_i | b_j \rangle).$$

See [5, §8].

Remark 15.5. Theorem 15.1 is still true if k is only separably closed (see [13, II, 3.17]). If A is defined over a field k, then the isomorphism

$$\Lambda^* \operatorname{Hom}(T_l, \mathbb{Z}_l) \to H^*(A_{k_s}, \mathbb{Z}_l)$$

is compatible with the natural actions of $\operatorname{Gal}(k_s/k)$.

§16. Pairings

As we discussed in Section 11, if M and N denote the kernels of an isogeny f and its dual $f^\vee$, then there is a canonical pairing $M \times N \to \mathbb{G}_m$ which identifies each group scheme with the Cartier dual of the other. In the case that f is multiplication by m, $m_A: A \to A$, then $f^\vee$ is $m_{A^\vee}: A^\vee \to A^\vee$, and so the general theory gives a pairing $\overline{e}_m: A_m \times A_m^\vee \to \mathbb{G}_m$. If we assume further that m is not divisible by the characteristic of k, then this can be identified with a nondegenerate pairing of $\operatorname{Gal}(\bar{k}/k)$-modules

$$\overline{e}_m: A_m(\bar{k}) \times A_m^\vee(\bar{k}) \to \bar{k}^\times.$$

This pairing has a very explicit description. Let $a \in A_m(\bar{k})$ and let $a' \in A_m^\vee(\bar{k}) \subset \operatorname{Pic}^0(A_{\bar{k}})$. If a' is represented by the divisor D on $A_{\bar{k}}$, then $m_A^{-1}D$ is linearly equivalent to mD (see the paragraph following (9.2)), which is linearly equivalent to zero. Therefore there are functions f and g on $A_{\bar{k}}$ such that $mD = (f)$ and $m_A^{-1}D = (g)$. Since the divisor

$$(f \circ m_A) = m_A^{-1}((f)) = m_A^{-1}(mD) = m(m_A^{-1}D) = (g^m),$$

we see that $g^m/f \circ m_A$ is a constant function c on $A_{\bar{k}}$. In particular,

$$g(x+a)^m = \operatorname{cf}(mx + ma) = \operatorname{cf}(mx) = g(x)^m.$$

Therefore $g/g \circ t_a$ is a function on $A_{\bar{k}}$ whose mth power is one. This means that it is an mth root of 1 in $\bar{k}(A)$ and can be identified with an element of $\bar{k}$. It is shown in [16, §20, p. 184] that $\overline{e}_m(a, a') = g/g \circ t_a$.

Lemma 16.1. *Let m and n be integers not divisible by the characteristic of k. Then for all $a \in A_{mn}(\bar{k})$ and $a' \in A_{mn}^\vee(\bar{k})$,*

$$\overline{e}_{mn}(a, a')^n = \overline{e}_m(na, na').$$

PROOF. Let D represent a', and let $(mn)_A^{-1}(D) = (g)$ and $m_A^{-1}(nD) = (g')$. Then

$$(g' \circ n_A) = n_A^{-1}((g')) = n_A^{-1}(m_A^{-1}(nD) = n(mn)_A^{-1}(D) = (g^n),$$

and so $g^n = c(g' \circ n_A)$ for some constant function c. Therefore

$$(g(x)/g(x+a))^n = g'(nx)/g'(nx+na),$$

and this equals $\bar{e}_m(na, na')$ for all x. $= \frac{g'(x)}{g'(x+na)}$ since $\frac{g'(x)}{g'(x+na)}$ is a constant function since it is an nth root of unity. □

Regard $\bar{e}_m$ as taking values in $\mu_m = \{\zeta \in \bar{k} \mid \zeta^m = 1\}$, and let $\mathbb{Z}_l(1) = \varprojlim \mu_{l^n}$ for l a prime not equal to the characteristic of k. (Warning: We sometimes write $\mathbb{Z}_l(1)$ additively and sometimes multiplicatively.) The lemma allows us to define a pairing e_l: $T_l A \times T_l A^\vee \to \mathbb{Z}_l(1)$ by the rule

$$e_l((a_n), (a_n')) = (\bar{e}_{l^n}(a_n, a_n')).$$

For a homomorphism λ: $A \to A^\vee$, we define pairings

$$\bar{e}_m^\lambda \colon A_m \times A_m \to \mu_m, \qquad (a, a') \mapsto \bar{e}_m(a, \lambda a'),$$

$$e_l^\lambda \colon T_l A \times T_l A \to \mathbb{Z}_l(1), \qquad (a, a') \mapsto e_l(a, \lambda a').$$

If $\lambda = \varphi_{\mathscr{L}}$, $\mathscr{L} \in \mathrm{Pic}(A)$, then we write $\bar{e}_m^{\mathscr{L}}$ and $e_l^{\mathscr{L}}$ for $\bar{e}_m^\lambda$ and e_l^λ.

Lemma 16.2. *There are the following formulas: for a homomorphism f: $A \to B$,*

(a) $\bar{e}_m(a, f^\vee(b)) = \bar{e}_m(f(a), b)$, $\quad a \in A_m, b \in B_m$;
(b) $e_l(a, f^\vee(b)) = e_l(f(a), b)$, $\quad a \in T_l A, b \in T_l B$;
(c) $e_l^{f^\vee \circ \lambda \circ f}(a, a') = e_l^\lambda(f(a), f(a'))$, $\quad a, a' \in T_l A, \lambda \in \mathrm{Hom}(B, B^\vee)$;
(d) $e_l^{f^* \mathscr{L}}(a, a') = e_l^{\mathscr{L}}(f(a), f(a'))$, $\quad a, a' \in T_l A, \mathscr{L} \in \mathrm{Pic}(B)$.

Moreover,

(e) $\mathscr{L} \mapsto e_l^{\mathscr{L}}$ *is a homomorphism* $\mathrm{Pic}(A) \to \mathrm{Hom}(\Lambda^2 T_l A, \mathbb{Z}_l(1))$.

PROOF. Let a and b be as in (a); let the divisor D on B represent b, and let $m_B^{-1} D = (g)$. Then $\bar{e}_m(f(a), b) = g(x)/g(x + f(a))$ for all x. On the other hand, $f^{-1} D$ represents $f^\vee(b)$ on A, and $m_A^{-1} f^{-1} D = f^{-1} m_B^{-1} D = (g \circ f)$, and so $\bar{e}_m(a, f^\vee(b)) = g(f(x))/g(f(x) + f(a))$. This proves (a), and (b) and (c) follow immediately. Formula (d) follows from (c) because

$$\varphi_{f^* \mathscr{L}}(a) = t_a^* f^* \mathscr{L} \otimes f^* \mathscr{L}^{-1} = f^* t_{fa}^* \mathscr{L} \otimes f^* \mathscr{L}^{-1} = f^*(\varphi_{\mathscr{L}}(fa))$$
$$= f^\vee \circ \varphi_{\mathscr{L}} \circ f(a),$$

which shows that $\varphi_{f^* \mathscr{L}} = f^\vee \circ \varphi_{\mathscr{L}} \circ f$. Finally, (e) follows from the fact that $\varphi_{\mathscr{L} \otimes \mathscr{L}'} = \varphi_{\mathscr{L}} + \varphi_{\mathscr{L}'}$.

Example 16.3. Let A be an abelian variety over $\mathbb{C}$. The exact sequence of sheaves on $A(\mathbb{C})$ (here $\mathscr{O}_A$ denotes the sheaf of holomorphic functions on $A(\mathbb{C})$)

$$0 \to \mathbb{Z} \to \mathscr{O}_A \xrightarrow{e^{2\pi i(\cdot)}} \mathscr{O}_A^\times \to 0$$

gives rise to an exact sequence

$$H^1(A(\mathbb{C}), \mathbb{Z}) \to H^1(A(\mathbb{C}), \mathscr{O}) \to H^1(A(\mathbb{C}), \mathscr{O}^\times) \to H^2(A(\mathbb{C}), \mathbb{Z}) \to H^2(A(\mathbb{C}), \mathscr{O}).$$

As $H^1(A(\mathbb{C}), \mathscr{O}^\times) = \mathrm{Pic}(A)$ and $H^1(A(\mathbb{C}), \mathscr{O})/H^1(A(\mathbb{C}), \mathbb{Z}) = A^\vee(\mathbb{C})$ (see (9.4c)), we can extract from this an exact sequence

$$0 \to \mathrm{NS}(A) \to H^2(A(\mathbb{C}), \mathbb{Z}) \to H^2(A(\mathbb{C}), \mathscr{O}_A).$$

Let $\lambda \in \mathrm{NS}(A)$, and let E^λ be its image in $H^2(A(\mathbb{C}), \mathbb{Z})$. Then (see Section 15) E^λ can be regarded as a skew-symmetric form on $H_1(A(\mathbb{C}), \mathbb{Z})$. It is a non-degenerate Riemann form if and only if λ is ample. As was explained above, λ induces a pairing e_l^λ, and it is shown in [16, §24, p. 237] that the diagram

$$\begin{array}{ccccc} E^\lambda\colon & H_1(A, \mathbb{Z}) & \times & H_1(A, \mathbb{Z}) & \to \mathbb{Z} \\ & \downarrow & & \downarrow & \downarrow \\ e_l^\lambda\colon & T_l A & \times & T_l A & \to \mathbb{Z}_l(1) \end{array}$$

commutes with a minus sign if the maps $H^1(A(\mathbb{C}), \mathbb{Z}) \to T_l A$ are taken to be the obvious ones and $\mathbb{Z} \to \mathbb{Z}_l(1)$ is taken to be $m \mapsto \zeta^m$, $\zeta = (\ldots, e^{2\pi i/l^n}, \ldots)$; in other words, $e_l^\lambda(a, a') = \zeta^{-E^\lambda(a, a')}$.

In the remainder of this section, we shall show how étale cohomology can be used to give short proofs (except for the characteristic k part) of some important results concerning polarizations. Proofs not using étale cohomology can be found in [16, §§20, 23].

The family of exact sequences of sheaves

$$0 \to \mu_{l^n} \to \mathbb{G}_m \xrightarrow{l^n} \mathbb{G}_m \to 0,$$

$l \neq \mathrm{char}(k)$, $n \geq 1$, plays the same role for the étale topology that the exponential sequence in (16.3) plays for the complex topology. As $\mathrm{Pic}(A) = H^1(A, \mathbb{G}_m)$ (étale cohomology), these sequences give rise to cohomology sequences

$$0 \to \mathrm{Pic}(A_{\bar{k}})/l^n \mathrm{Pic}(A_{\bar{k}}) \to H^2(A_{\bar{k}}, \mu_{l^n}) \to H^2(A_{\bar{k}}, \mathbb{G}_m)_{l^n} \to 0.$$

Note that $\mathrm{Pic}^0(A_{\bar{k}}) = A^\vee(\bar{k})$ is divisible, and so $\mathrm{Pic}(A_{\bar{k}})/l^n \mathrm{Pic}(A_{\bar{k}}) = \mathrm{NS}(A_{\bar{k}})/l^n \mathrm{NS}(A_{\bar{k}})$. On passing to the inverse limit over these sequences, we get an exact sequence

$$0 \to \mathrm{NS}(A_{\bar{k}}) \otimes \mathbb{Z}_l \to H^2(A_{\bar{k}}, \mathbb{Z}_l(1)) \to T_l H^2(A_{\bar{k}}, \mathbb{G}_m) \to 0,$$

where $T_l M$ for any group M is $\varprojlim M_{l^n}$. Note that $T_l M$ is always torsion-free. As in the above example, an element λ of $\mathrm{NS}(A_{\bar{k}})$ defines a skew-symmetric pairing E_l^λ: $T_l A \times T_l A \to \mathbb{Z}_l(1)$, and one can show as in the previous case that $E_l^\lambda = -e_l^\lambda$ (in fact, this provides a convenient alternative definition of e_l^λ in the case that λ arises from an element of $\mathrm{NS}(A_{\bar{k}})$).

We now assume that k is algebraically closed.

Theorem 16.4. *Let f: $A \to B$ be an isogeny of degree prime to the characteristic of k, and let $\lambda \in \mathrm{NS}(A)$. Then $\lambda = f^*(\lambda')$ for some $\lambda' \in \mathrm{NS}(B)$ if and only if, for*

all l dividing $\deg(f)$*, there exists an* e_l *in* $\mathrm{Hom}(\Lambda^2 T_l B, \mathbb{Z}_l(1))$ *such that* $e_l^\lambda(a, a') = e_l(f(a), f(a'))$ *all* $a, a' \in T_l A$.

PROOF. The necessity is obvious from (16.2c). For the converse, consider for each $l \neq \mathrm{char}(k)$ the commutative diagram

$$\begin{array}{ccccc} 0 \to \mathrm{NS}(A) \otimes \mathbb{Z}_l & \to & H^2(A, \mathbb{Z}_l(1)) & \to & T_l(H^2(A, \mathbb{G}_m)) \\ \uparrow & & \uparrow & & \uparrow \\ 0 \to \mathrm{NS}(B) \otimes \mathbb{Z}_l & \to & H^2(B, \mathbb{Z}_l(1)) & \to & T_l(H^2(B, \mathbb{G}_m)). \end{array}$$

The right-hand vertical arrow is injective because there exists an isogeny $f'\colon B \to A$ such that $f \circ f'$ is multiplication by $\deg(f)$ on B (see Section 8) and $T_l(H^2(B, \mathbb{G}_m)$ is torsion-free. A diagram chase now shows that λ is in the image of $\mathrm{NS}(B) \otimes \mathbb{Z}_l \to \mathrm{NS}(A) \otimes \mathbb{Z}_l$ for all l dividing $\deg(f)$, and the existence of f' shows that it is in the image for all remaining primes. This implies that it is in the image of $\mathrm{NS}(B) \to \mathrm{NS}(A)$ because $\mathrm{NS}(A)$ is a finitely generated $\mathbb{Z}$-module. □

Corollary 16.5. *Assume* $l \neq \mathrm{char}(k)$. *An element* λ *of* $\mathrm{NS}(A)$ *is divisible by* l^n *if and only if* e_l^λ *is divisible by* l^n *in* $\mathrm{Hom}(\Lambda^2 T_l A, \mathbb{Z}_l(1))$.

PROOF. Apply the proposition to $l_A^n\colon A \to A$. □

Proposition 16.6. *Assume* $\mathrm{char}(k) \neq 2$, l. *A homomorphism* $\lambda\colon A \to A^\vee$ *is of the form* $\varphi_{\mathscr{L}}$ *for some* $\mathscr{L} \in \mathrm{Pic}(A)$ *if and only if* e_l^λ *is skew-symmetric.*

PROOF. If λ is in the subgroup $\mathrm{NS}(A)$ of $\mathrm{Hom}(A, A^\vee)$, we already know that e_l^λ is skew-symmetric. Conversely, suppose e_l^λ is skew-symmetric, and let $\mathscr{L}$ be the pull-back of the Poincaré sheaf $\mathscr{P}$ by $(1, \lambda)\colon A \to A \times A^\vee$. For all $a, a' \in T_l A$,

$$\begin{aligned} e_l(a, \varphi_{\mathscr{L}} a') = e_l^{\mathscr{L}}(a, a') &= e_l^{\mathscr{P}}((a, \lambda a), (a', \lambda a')) && \text{(by 16.2d)} \\ &= e_l(a, \lambda a') - e_l(a', \lambda a) && \text{(see the next lemma)} \\ &= e_l^\lambda(a, a') - e_l^\lambda(a', a) \\ &= 2e_l^\lambda(a, a') && \text{(because } e_l^\lambda \text{ is skew-symmetric)} \\ &= e_l(a, 2\lambda a'). \end{aligned}$$

As e_l is nondegenerate, this shows that $2\lambda = \varphi_{\mathscr{L}}$, and (16.5) shows that $\mathscr{L}$ is divisible by 2 in $\mathrm{NS}(A)$. □

Lemma 16.7. *Let* $\mathscr{P}$ *be the Poincaré sheaf on* $A \times A^\vee$. *Then*

$$e_l^{\mathscr{P}}((a, b), (a', b')) = e_l(a, b') - e_l(a', b)$$

for $a, a' \in T_l A$ *and* $b, b' \in T_l A^\vee$.

PROOF. Because $\mathbb{Z}_l(1)$ is torsion-free, it suffices to prove the identity for b and b' in a subgroup of finite index in $T_l A^\vee$. Therefore we can assume that $b = \lambda c$ and $b' = \lambda c'$ for some polarization $\lambda = \varphi_{\mathscr{L}}$ of A and elements c and c' of $T_l A$. From Section 10 we know that $(1 \times \lambda)^* \mathscr{P} = m^* \mathscr{L} \otimes p^* \mathscr{L}^{-1} \otimes q^* \mathscr{L}^{-1}$, and so

$$\begin{aligned} e_l^{\mathscr{P}}((a, b), (a', b')) &= e_l^{(1 \times \lambda)^* \mathscr{P}}((a, c), (a', c')) \\ &= e_l^{\mathscr{L}}(a + c, a' + c') - e_l^{\mathscr{L}}(a, a') - e_l^{\mathscr{L}}(c, c') \\ &= e_l^{\mathscr{L}}(a, c') - e_l^{\mathscr{L}}(a', c) \\ &= e_l(a, b') - e_l(a', b). \end{aligned}$$

□

For a polarization $\lambda\colon A \to A^\vee$, define

$$e^\lambda\colon \mathrm{Ker}(\lambda) \times \mathrm{Ker}(\lambda) \to \mu_m$$

as follows: suppose m kills $\mathrm{Ker}(\lambda)$, and let a and a' be in $\mathrm{Ker}(\lambda)$; choose a b such that $mb = a'$, and let $e^\lambda(a, a') = \overline{e}_m(a, \lambda b)$; this makes sense because $m(\lambda b) = \lambda(mb) = 0$. Also it is independent of the choice of b and m because if $mnb' = a'$ and $nc = a$, then

$$\overline{e}_{mn}(a, \lambda b') = \overline{e}_{mn}(c, \lambda b')^n = \overline{e}_m(a, \lambda n b') \qquad \text{(by 16.1)}$$

and so

$$\begin{aligned} \overline{e}_{mn}(a, \lambda b')/\overline{e}_m(a, \lambda b) = \overline{e}_m(a, \lambda(nb' - b)) &= \overline{e}_m^\lambda(a, nb' - b) \\ &= \overline{e}_m^\lambda(nb' - b, a)^{-1} \\ &= 1 \quad \text{as } \lambda a = 0. \end{aligned}$$

Let $a = (a_n)$ and $a' = (a'_n)$ be in $T_l A$. If $\lambda a_m = 0 = \lambda a'_m$ for some m, then

$$e^\lambda(a_m, a'_m) = \overline{e}_{l^m}(a_m, \lambda a'_{2m}) = \overline{e}_{l^{2m}}(a_{2m}, \lambda a'_{3m})^{l^m} = \overline{e}_{l^{2m}}^\lambda(a_{2m}, a'_{2m}).$$

Note that this implies that e^λ is skew-symmetric.

Proposition 16.8. *Let* $f\colon A \to B$ *be an isogeny of degree prime to* $\mathrm{char}(k)$, *and let* $\lambda\colon A \to A^\vee$ *be a polarization of* A. *Then* $\lambda = f^*(\lambda')$ *for some polarization* λ' *on* B *if and only if* $\mathrm{Ker}(f) \subset \mathrm{Ker}(\lambda)$ *and* e^λ *is trivial on* $\mathrm{Ker}(f) \times \mathrm{Ker}(f)$.

PROOF. We will assume the second condition and construct an e_l in $\mathrm{Hom}(\Lambda^2 T_l B, \mathbb{Z}_l(1))$ such that $e_l^\lambda(a, a') = e_l(fa, fa')$ for all a, a' in $T_l A$; then (16.4) will show the existence of λ'. Let $b, b' \in T_l B$; for some m there will exist $a, a' \in T_l A$ such that $l^m b = f(a)$ and $l^m b' = f(a')$. If we write $a = (a_n)$ and $a' = (a'_n)$, then these equations imply that $f(a_m) = 0 = f(a'_m)$, and therefore that a_m and a'_m are in $\mathrm{Ker}(\lambda)$ and that $e^\lambda(a_m, a'_m) = 0$. The calculation preceding the statement of the proposition now shows that $\overline{e}_{l^{2m}}^\lambda(a_{2m}, a'_{2m}) = 0$ and therefore that $e_l^\lambda(a, a')$ is divisible by l^{2m}. We can therefore define $e_l(b, b') = l^{-2m} e_l^\lambda(a, a')$. This proves the sufficiency of the second condition, and the necessity is easy. □

Remark 16.9. The degrees of λ and λ' are related by $\deg(\lambda) = \deg(\lambda')\cdot\deg(f)^2$, because $\lambda = f^\vee\circ\lambda'\circ f$.

Corollary 16.10. *Let A be an abelian variety having a polarization of degree prime to* $\mathrm{char}(k)$. *Then A is isogenous to a principally polarized abelian variety.*

PROOF. Let λ be a polarization of A, and let l be a prime dividing the degree of λ. Choose a subgroup N of $\mathrm{Ker}(\lambda)$ of order l, and let $B = A/N$. As e^λ is skew-symmetric, it must be zero on $N\times N$, and so the last proposition implies that B has a polarization of degree $\deg(\lambda)/l^2$. □

Corollary 16.11. *Let λ be a polarization of A, and assume that* $\mathrm{Ker}(\lambda)\subset A_m$ *with m prime to* $\mathrm{char}(k)$. *If there exists an element α of* $\mathrm{End}(A)$ *such that* $\alpha(\mathrm{Ker}(\lambda))\subset\mathrm{Ker}(\lambda)$ *and $\alpha^\vee\circ\lambda\circ\alpha = -\lambda$ on A_{m^2}, then $A\times A^\vee$ is principally polarized.*

PROOF. Let $N = \{(a,\alpha a)\mid a\in\mathrm{Ker}(\lambda)\}\subset A\times A$. Then $N\subset\mathrm{Ker}(\lambda\times\lambda)$, and for $(a,\alpha a)$ and $(a',\alpha a')$ in N

$$\begin{aligned} e^{\lambda\times\lambda}((a,\alpha a),(a',\alpha a')) &= e^\lambda(a,a') + e^\lambda(\alpha a,\alpha a')\\ &= \overline{e}_m(a,\lambda b) + \overline{e}_m(a,\alpha^\vee\circ\lambda\circ\alpha(b)) \quad \text{where} \quad mb = a'\\ &= \overline{e}_m(a,\lambda b) + \overline{e}_m(a,-\lambda b)\\ &= 0. \end{aligned}$$

Therefore, (16.8) applied to $A\times A\to(A\times A)/N$ and the polarization $\lambda\times\lambda$ on $A\times A$ shows that $(A\times A)/N$ is principally polarized. The kernel of $(a,a')\mapsto(a,\alpha a+a')\colon A\times A\to(A\times A)/N$ is $\mathrm{Ker}(\lambda)\times\{0\}$, and so the map induces an isomorphism $A^\vee\times A\to(A\times A)/N$. □

Remark 16.12 (Zarhin's Trick). Let A and λ be as in the statement of the corollary. Then there always exists an α satisfying the conditions for (A^4,λ^4) and therefore $(A\times A^\vee)^4$ is principally polarized. To see this choose integers a,b,c,d such that $a^2+b^2+c^2+d^2\equiv -1 \pmod{m^2}$, and let

$$\alpha = \begin{bmatrix} a & -b & -c & -d\\ b & a & d & -c\\ c & -d & a & b\\ d & c & -b & a\end{bmatrix} \in M_4(\mathbb{Z})\subset\mathrm{End}(A).$$

Clearly $\alpha(\mathrm{Ker}(\lambda^4))\subset\mathrm{Ker}(\lambda^4)$. Moreover $\alpha^\vee$ can be identified with the transpose α^{tr} of α (as a matrix), and so

$$\alpha^\vee\circ\lambda^4\circ\alpha = \alpha^{\mathrm{tr}}\circ\lambda^4\circ\alpha = \lambda^4\circ\alpha^{\mathrm{tr}}\circ\alpha.$$

But $\alpha^{\mathrm{tr}}\circ\alpha = (a^2+b^2+c^2+d^2)I_4$.

Remark 16.13. In [16, §§20, 23] there is a different and much more profound treatment of the above theory using finite group schemes. In particular, it is possible to remove the restrictions on l or a degree being prime to the characteristic in the results (16.4) through (16.12).

Remark 16.14. Some of the above results extend to fields that are not algebraically closed. For example, if A is an abelian variety over a perfect field, then (16.5) implies immediately that a polarization λ of A can be written as l^m times a polarization if and only if e_l^λ is divisible by l^m; similarly (16.11) implies that the same result holds over a perfect field. On the other hand (16.10) seems to be false unless one allows a field extension (roughly speaking, it is necessary to divide out by half the kernel of the polarization λ, which need not be rational over k).

§17. The Rosati Involution

Fix a polarization λ on A. As λ is an isogeny $A\to A^\vee$, it has an inverse in $\mathrm{Hom}^0(A^\vee,A)\overset{\mathrm{df}}{=}\mathrm{Hom}(A^\vee,A)\otimes\mathbb{Q}$. The *Rosati involution* on $\mathrm{End}^0(A)$ corresponding to λ is

$$\alpha\mapsto\alpha^\dagger = \lambda^{-1}\circ\alpha^\vee\circ\lambda.$$

This has the following obvious properties:

$$(\alpha+\beta)^\dagger = \alpha^\dagger+\beta^\dagger,\qquad (\alpha\beta)^\dagger = \beta^\dagger\alpha^\dagger,\quad a^\dagger = a \qquad \text{for } a\in\mathbb{Q}.$$

For any $a,a'\in T_lA\otimes\mathbb{Q}$, $l\neq\mathrm{char}(k)$,

$$e_l^\lambda(\alpha a,a') = e_l(\alpha a,\lambda a') = e_l(a,\alpha^\vee\circ\lambda a') = e_l^\lambda(a,\alpha^\dagger a'),$$

from which it follows that $\alpha^{\dagger\dagger} = \alpha$.

Remark 17.1. The second condition on α in (16.11) can now be stated as $\alpha^\dagger\circ\alpha = -1$ on A_{m^2} (provided $\alpha^\dagger$ lies in $\mathrm{End}(A)$).

Proposition 17.2. *Assume that k is algebraically closed. Then the map*

$$\mathscr{L}\mapsto\lambda^{-1}\circ\varphi_{\mathscr{L}},\ \mathrm{NS}(A)\otimes\mathbb{Q}\to\mathrm{End}^0(A),$$

identifies $\mathrm{NS}(A)\otimes\mathbb{Q}$ *with the subalgebra of* $\mathrm{End}^0(A)$ *of elements fixed by* $\dagger$.

PROOF. Let $\alpha\in\mathrm{End}^0(A)$, and let l be an odd prime $\neq\mathrm{char}(k)$. According to (16.6), $\lambda\circ\alpha$ is of the form $\varphi_{\mathscr{L}}$ if and only if $e_l^{\lambda\circ\alpha}(a,a') = -e_l^{\lambda\circ\alpha}(a',a)$ for all $a,a'\in T_lA\otimes\mathbb{Q}$. But

$$e_l^{\lambda\circ\alpha}(a,a') = e_l^\lambda(a,\alpha a') = -e_l^\lambda(\alpha a',a) = -e_l(a',\alpha^\vee\circ\lambda(a)),$$

and so this is equivalent to $\lambda\circ\alpha = \alpha^\vee\circ\lambda$, that is, to $\alpha = \alpha^\dagger$. □

Theorem 17.3. *The bilinear form*

$$(\alpha, \beta) \mapsto \mathrm{Tr}(\alpha \circ \beta^\dagger)\colon \mathrm{End}^0(A) \times \mathrm{End}^0(A) \to \mathbb{Q}$$

is positive definite. More precisely, if $\lambda = \varphi_{\mathscr{L}(D)}$, *then*

$$\mathrm{Tr}(\alpha \circ \alpha^\dagger) = \frac{2g}{(D^g)}(D^{g-1} \cdot \alpha^*(D)).$$

PROOF. As D is ample and $\alpha^*(D)$ is effective, the intersection number $(D^{g-1} \cdot \alpha^*(D))$ is positive. Thus the second statement implies the first. Clearly it suffices to prove it with k algebraically closed.

Lemma 17.4. *Let A be an abelian variety over an algebraically closed field, and let $\mathbb{Z}_l(g) = \mathbb{Z}_l(1)^{\otimes g}$. Then there is a canonical generator ε of $\mathrm{Hom}(\Lambda^{2g}(T_lA), \mathbb{Z}_l(g))$ with the following property: if $D_1, \dots, D_g$ are divisors on A and $e_i = e_l^{\mathscr{L}(D_i)} \in \mathrm{Hom}(\Lambda^2 T_l A, \mathbb{Z}_l(1))$, then $e_1 \wedge \cdots \wedge e_g$ is the multiple $(D_1, D_2, \dots, D_g)\varepsilon$ of ε.*

PROOF. See [16, §20, Theorem 3, p. 190]. (From the point of view of étale cohomology, ε corresponds to the canonical generator of $H^{2g}(A, \mathbb{Z}_l(g))$, which is equal to the cohomology class of any point on A. If c_i is the class of D_i in $H^2(A, \mathbb{Z}_l(1))$, then the compatibility of intersection products with cup-products shows that $(D_1, \dots, D_g)\varepsilon = c_1 \cup \cdots \cup c_g$. Consequently, the lemma follows from (15.4).) □

PROOF OF (17.3). From the lemma, we find that

$$e_l^\lambda \wedge \cdots \wedge e_l^\lambda = (D^g)\varepsilon,$$

$$e_l^\lambda \wedge \cdots \wedge e_l^\lambda \wedge e_l^{\alpha^*(\lambda)} = (D^{g-1} \cdot \alpha^*(D))\varepsilon.$$

It suffices therefore to show that, for some basis $a_1, \dots, a_{2g}$ of $T_lA \otimes \mathbb{Q}$,

$$\frac{\langle a_1 \wedge \cdots \wedge a_{2g} | e_l^\lambda \wedge \cdots \wedge e_l^\lambda \wedge e_l^{\alpha^*(\lambda)} \rangle}{\langle a_1 \wedge \cdots \wedge a_{2g} | e_l^\lambda \wedge \cdots \wedge e_l^\lambda \rangle} = \frac{1}{2g}\mathrm{Tr}(\alpha \circ \alpha^\dagger).$$

(See (15.4).) Choose the basis $a_1, a_2, \dots, a_{2g}$ so that

$$e_l^\lambda(a_{2i-1}, a_{2i}) = 1 = -e_l^\lambda(a_{2i}, a_{2i-1}), \qquad i = 1, 2, \dots, g,$$

$$e_l^\lambda(a_i, a_j) = 0, \qquad \text{otherwise.}$$

Let $f_1, \dots, f_{2g}$ be the dual basis; then for $j \neq j'$,

$$\langle a_i \wedge a_{i'} | f_j \wedge f_{j'} \rangle = \begin{vmatrix} f_j(a_i) & f_{j'}(a_i) \\ f_j(a_{i'}) & f_{j'}(a_{i'}) \end{vmatrix} = \begin{cases} 1 & \text{if } i = j,\ i' = j', \\ -1 & \text{if } i = j',\ i' = j, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore $e_l^\lambda = \sum_{i=1}^g f_{2i-1} \wedge f_{2i}$, and so $e_l^\lambda \wedge \cdots \wedge e_l^\lambda = g!(f_1 \wedge \cdots \wedge f_{2g})$.

Thus

$$\langle a_1 \wedge \cdots \wedge a_{2g} | e_l^\lambda \wedge \cdots \wedge e_l^\lambda \rangle = \langle a_1 \wedge \cdots \wedge a_{2g} | g!(f_1 \wedge \cdots \wedge f_{2g}) \rangle = g!.$$

Similarly,

$$\begin{aligned} &\langle a_1 \wedge \cdots \wedge a_{2g} | e_l^\lambda \wedge \cdots \wedge e_l^\lambda \wedge e_l^{\alpha^*(\mathscr{L})} \rangle \\ &= (g-1)! \sum_{i=1}^g e_l^\lambda(\alpha a_{2i-1}, \alpha a_{2i}) \\ &= \frac{(g-1)!}{2} \sum (e_l^\lambda(a_{2i-1}, \alpha^\dagger \alpha a_{2i}) + e_l^\lambda(\alpha^\dagger \alpha a_{2i-1}, a_{2i})) \\ &= \frac{g!}{2g}\mathrm{Tr}(\alpha^\dagger \alpha), \end{aligned}$$

which completes the proof. □

Proposition 17.5. *Let λ be a polarization of the abelian variety A.*

(a) *The automorphism group of (A, λ) is finite.*
(b) *For any integer $n \geq 3$, an automorphism of (A, λ) acting as the identity on $A_n(\bar{k})$ is equal to the identity.*

PROOF. Let α be an automorphism of A. In order for α to be an automorphism of (A, λ), we must have $\lambda = \alpha^\vee \circ \lambda \circ \alpha$, and therefore $\alpha^\dagger \alpha = 1$, where $\dagger$ is the Rosati involution defined by λ. Consequently,

$$\alpha \in \mathrm{End}(A) \cap \{\alpha \in \mathrm{End}(A) \otimes \mathbb{R} \mid \mathrm{Tr}(\alpha^\dagger \alpha) = 2g\},$$

and the first of these sets is discrete in $\mathrm{End}(A) \otimes \mathbb{R}$, while the second is compact. This proves (a).

Assume further that α acts as the identity on A_n. Then $\alpha - 1$ is zero on A_n, and so it is of the form $n\beta$ with $\beta \in \mathrm{End}(A)$ (see (12.6)). The eigenvalues of α and β are algebraic integers, and those of α are roots of 1 because it has finite order. The next lemma shows that the eigenvalues of α equal 1.

Lemma 17.6. *If ζ is a root of 1 such that for some algebraic integer γ and rational integer $n \geq 3$, $\zeta = 1 + n\gamma$, then $\zeta = 1$.*

PROOF. If $\zeta \neq 1$, then after raising it to a power, we may assume that it is a primitive pth root of 1 for some prime p. Then $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1 - \zeta) = p$, and so the equation $1 - \zeta = -n\gamma$ implies $p = \pm n^{p-1} N(\gamma)$. This is impossible because p is prime. □

We have shown that α is unipotent and therefore that $\alpha - 1 = n\beta$ is nilpotent. Suppose that $\beta \neq 0$. Then $\beta' = \beta^\dagger \beta \neq 0$, because $\mathrm{Tr}(\beta^\dagger \beta) > 0$. As $\beta' = \beta'^\dagger$, this implies that $\mathrm{Tr}(\beta'^2) > 0$ and so $\beta'^2 \neq 0$. Similarly, $\beta'^4 \neq 0$, and so on, which contradicts the nilpotence of β. □

Remark 17.7. Let (A, λ) and (A', λ') be polarized abelian varieties over a field k, and assume that A and A' have all their points of order n rational over k for some $n \geq 3$. Then any isomorphism $\alpha: (A, \lambda) \to (A', \lambda')$ defined over the separable closure k_s of k is automatically defined over k because, for all $\sigma \in \mathrm{Gal}(k_s/k)$, $\alpha^{-1} \circ \sigma\alpha$ is an automorphism of (A, λ) fixing the points of order n and therefore is the identity map.

Remark 17.8. On combining the results in Section 12 with (17.3), we see that the endomorphism algebra $\mathrm{End}^0(A)$ of a simple abelian variety A is a skew field together with an involution $\dagger$ such that $\mathrm{Tr}(\alpha \circ \alpha^\dagger) > 0$ for all nonzero α.

§18. Two More Finiteness Theorems

The first theorem shows that an abelian variety can be endowed with a polarization of a fixed degree d in only a finite number of essentially different ways. The second shows that an abelian variety has only finitely many non-isomorphic direct factors.

Theorem 18.1. *Let A be an abelian variety over a field k, and let d be an integer; then there exist only finitely many isomorphism classes of polarized abelian varieties (A, λ) with λ of degree d.*

Fix a polarization λ_0 of A, and let $\dagger$ be the Rosati involution on $\mathrm{End}^0(A)$ defined by λ_0. The map $\lambda \mapsto \lambda_0^{-1} \circ \lambda$ identifies the set of polarizations of A with a subset of the set $\mathrm{End}^0(A)^\dagger$ of elements of $\mathrm{End}^0(A)$ fixed by $\dagger$. As $\mathrm{NS}(A_{\bar{k}})$ is a finitely generated abelian group, there exists an N such that all the $\lambda_0^{-1} \circ \lambda$ are contained in a lattice $L = N^{-1}\mathrm{End}(A)^\dagger$ in $\mathrm{End}^0(A)^\dagger$. Note that L is stable under the action

$$\alpha \mapsto u^\dagger \alpha u, \qquad u \in \mathrm{End}(A)^\times, \qquad \alpha \in \mathrm{End}^0(A)$$

of $\mathrm{End}(A)^\times$ on $\mathrm{End}^0(A)$.

Let λ be a polarization of A, and let $u \in \mathrm{End}(A)^\times$. Then u defines an isomorphism $(A, u^\vee \circ \lambda \circ u) \xrightarrow{\approx} (A, \lambda)$, and $\lambda_0^{-1} \circ (u^\vee \circ \lambda \circ u) = u^\dagger \circ (\lambda_0^{-1} \circ \lambda) \circ u$. Thus to each isomorphism class of polarized abelian varieties (A, λ), we can associate an orbit of $\mathrm{End}(A)^\times$ in L. Recall (12.12) that the map $\alpha \mapsto \deg(\alpha)$ is a positive power of the reduced norm on each simple factor of $\mathrm{End}^0(A)$, and so Nrd is bounded on the set of elements of L with degree d. These remarks show that the theorem is a consequence of the following result on algebras.

Proposition 18.2. *Let E be a finite-dimensional semisimple algebra over $\mathbb{Q}$ with an involution $\dagger$, and let R be an order in E. Let L be a lattice in $E^\dagger$ that is stable under the action $e \mapsto u^\dagger e u$ of $R^\times$ on E. Then for any integer d, $\{v \in L \mid \mathrm{Nrd}(v) \leq d\}$ is the union of a finite number of orbits.*

This proposition will be proved using a general result from the reduction theory of arithmetic subgroups.

Theorem 18.3. *Let G be a reductive group over $\mathbb{Q}$, and let Γ be an arithmetic subgroup of G; let $G \to \mathrm{Gl}(V)$ be a representation of G over $\mathbb{Q}$, and let L be a lattice in V that is stable under Γ. If X is a closed orbit of G in V, then $L \cap X$ is the union of a finite number of orbits of Γ.*

PROOF. See [4, 9.11]. □

Remark 18.4. (a) An algebraic group G is *reductive* if its identity component is an extension of a semisimple group by a torus. A subgroup Γ of $G(\mathbb{Q})$ is *arithmetic* if it is commensurable with $G(\mathbb{Z})$ for some $\mathbb{Z}$-structure on G.

(b) The following example may give the reader some idea of the nature of the above theorem. Let $G = \mathrm{SL}_n$, and let $\Gamma = \mathrm{SL}_n(\mathbb{Z})$. Then G acts in a natural way on the space V of quadratic forms in n variables with rational coefficients, and Γ preserves the lattice L of such forms with integer coefficients. Let q be a quadratic form with nonzero discriminant d. By the orbit X of q we mean the image $G \cdot q$ of G under the map of algebraic varieties $g \mapsto g \cdot q: G \to V$. The theory of quadratic forms shows that $X(\bar{\mathbb{Q}})$ is equal to the set of all quadratic forms (with coefficients in $\bar{\mathbb{Q}}$) of discriminant d. Clearly this is closed, and so the theorem shows that $X \cap L$ contains only finitely many $\mathrm{SL}_n(\mathbb{Z})$-orbits: the quadratic forms with integer coefficients and discriminant d fall into a finite number of proper equivalence classes.

We shall apply (18.3) with G a reductive group such that

$$G(\mathbb{Q}) = \{e \in E \mid \mathrm{Nrd}(e) = \pm 1\},$$

$\Gamma = R^\times$, $V = E^\dagger$, and $L \subset V$ the lattice in (18.2). In order to prove (18.2), we shall show

(a) there exists a reductive group G over $\mathbb{Q}$ with $G(\mathbb{Q})$ as described and having Γ as an arithmetic subgroup;
(b) the orbits of G on V are all closed;
(c) for any rational number d, $V_d \overset{\mathrm{df}}{=} \{v \in V \mid \mathrm{Nrd}(v) = d\}$ is the union of a finite number of orbits of G.

Then (18.3) will show $L \cap V_d$ comprises only finitely many Γ-orbits, as is asserted by (18.2).

To prove (a), embed E into some matrix algebra $M_n(\mathbb{Q})$. Then the condition that $\mathrm{Nrd}(e) = \pm 1$ can be expressed as a polynomial equation in the matrix coefficients of e, and this polynomial equation defines a linear algebraic group G over $\mathbb{Q}$ such that $G(S) = \{e \in E \otimes S \mid \mathrm{Nrd}(e) = \pm 1\}$ for all $\mathbb{Q}$-algebras S. Over $\bar{\mathbb{Q}}$, E is isomorphic to a product of matrix algebras $\prod M_{n_i}(\bar{\mathbb{Q}})$; consequently, $G(\bar{\mathbb{Q}}) = \{(e_i) \in \prod \mathrm{GL}_{n_i}(\bar{\mathbb{Q}}) \mid \prod \det(e_i) = \pm 1\}$. From this it is clear that the identity component of G is an extension of $\prod \mathrm{PGL}_{n_i}$

by a torus, and so G is reductive. It is easy to see that Γ is an arithmetic subgroup of $G(\mathbb{Q})$.

To prove (b), we need the following lemma from the theory of algebras with involution.

Lemma 18.5. *Let E be a semisimple algebra over an algebraically closed field K of characteristic zero, and let $\dagger$ be an involution of E fixing the elements of K. Then every element e of E such that $e^\dagger = e$ can be written $e = ca^\dagger a$ where c is in the centre of E and $\mathrm{Nrd}(a) = 1$.*

PROOF. Lacking a good proof, we make use of the classification of pairs $(E, \dagger)$. Each pair is a direct sum of pairs of the following types:

(A_n) $E = M_n(K) \times M_n(K)$ and $(e_1, e_2)^\dagger = (e_2^{tr}, e_1^{tr})$;
(B_n) E is the matrix algebra $M_n(K)$ and $e^\dagger = e^{tr}$;
(C_n) $E = M_{2n}(K)$ and $e^\dagger = J^{-1}e^{tr}J$ with J an invertible alternating matrix.

(See, for example, [25].) In the cases (B_n) and (C_n), the lemma follows from elementary linear algebra; in the case (A_n), $e = (e', e'^{tr})$, and we can take $c = d(I_n, I_n)$ and $a = (e'/d, I_n)$, where $d = \det(e')^{1/n}$. □

From the lemma, we see that if G_e is the isotropy group at $e \in V$, then there is an isomorphism $g \mapsto ag: G_e \to G_1$ defined over $\bar{\mathbb{Q}}$. In particular, all isotropy groups have the same dimension, and therefore all orbits of G in V have the same dimension. This implies that they are all closed, because every orbit of minimal dimension is closed (see, for example, [11, 8.3]).

It remains to prove (c). Let $v, v' \in V_d \otimes \mathbb{C}$, and write $v = ca^\dagger a$, $v' = c'a'^\dagger a'$ with c, c' and a, a' as in the lemma. Clearly v and v' are in the same orbit if and only if c and c' are. Note that c and c' lie in $V_d \otimes \mathbb{C}$. Let Z be the subalgebra of the centre of $E \otimes \mathbb{C}$ of elements fixed by $\dagger$. Then c and c' are in Z, and they lie in the same orbit of G if $c/c' \in Z^2$. But Z is a finite product of copies of $\mathbb{R}$ and $\mathbb{C}$, and so $Z^\times/Z^{\times 2}$ is finite. □

Corollary 18.6. *Let k be a finite field, and let g and d be positive integers. Up to isomorphism, there are only finitely many polarized abelian varieties (A, λ) over k with $\dim A = g$ and $\deg \lambda = d^2$.*

PROOF. From (14.1) we know that there are only finitely many possible A's, and (18.1) shows that for each A there are only finitely many λ's. □

We come now to the second main result of this section. An abelian variety A' is said to be a *direct factor* of an abelian variety A if $A \approx A' \times A''$ for some abelian variety A''.

Theorem 18.7. *Up to isomorphism, an abelian variety A has only finitely many direct factors.*

PROOF. To each direct factor A' of A, there corresponds an element e of $\mathrm{End}(A)$ defined by $A \xrightarrow{\approx} A' \times A'' \xrightarrow{p} A' \to A' \times A'' \xrightarrow{\approx} A$. Moreover $e^2 = e$, and A' is determined by e because it equals the kernel of $1 - e$. If $e' = ueu^{-1}$ with u in $\mathrm{End}(A)^\times$, then $u(1 - e)u^{-1} = 1 - e'$, and so e and e' correspond to isomorphic direct factors. These remarks show that the theorem is a consequence of the next lemma. □

Lemma 18.8. *Let E be a semisimple algebra of finite dimension over $\mathbb{Q}$, and let R be an order in E. Then $R^\times$, acting on the set of idempotents of R by inner automorphisms, has only finitely many orbits.*

PROOF. Apply (18.3) with G the algebraic group such that $G(\mathbb{Q}) = E^\times$; take Γ to be the arithmetic group $R^\times$, V to be E with G acting by inner automorphisms, and L to be R. Then the idempotents in E form a finite set of orbits under G, and each of these orbits is closed. In proving these statements we may replace $\mathbb{Q}$ by $\bar{\mathbb{Q}}$ and assume E to be a matrix algebra. Then each idempotent is conjugate to one of the form $e = \mathrm{diag}(1, \dots, 1, 0, \dots, 0)$, and the stabilizer G_e of e is a parabolic subgroup of G and so G/G_e is a projective variety (see [11, 21.3]) which implies that its image Ge in V is closed. □

Corollary 18.9. *Let k be a finite field; for each integer g, there exist only finitely many isomorphism classes of abelian varieties of dimension g over k.*

PROOF. Let A be an abelian variety of dimension g over k. From (16.12) we know that $(A \times A^\vee)^4$ has a principal polarization, and according to (14.1), the abelian varieties of dimension $8g$ over k having principal polarizations form only finitely many isomorphism classes. The result therefore follows from (18.7). □

§19. The Zeta Function of an Abelian Variety

Throughout this section, A will be an abelian variety over a finite field k with q elements, and k_m will be the unique subfield of $\bar{k}$ with q^m elements. Thus the elements of k_m are the solutions of $c^{q^m} = c$. We write N_m for the order of $A(k_m)$.

Theorem 19.1. *There are algebraic integers $a_1, \dots, a_{2g}$ such that:*

(a) *the polynomial $P(X) = \prod(X - a_i)$ has coefficients in $\mathbb{Z}$;*
(b) *$N_m = \prod(1 - a_i^m)$ for all $m \geq 1$; and*
(c) *(Riemann hypothesis) $|a_i| = q^{1/2}$.*

In particular, $|N_m - q^m| \leq 2gq^{m-1/2} + (2^g - 2g - 1)q^{m-1}$.

The proof will use the Frobenius morphism. For a variety V over k, this is

defined to be the morphism $\pi_V: V \to V$ which is the identity map on the underlying topological space of V and is the map $f \mapsto f^q$ on $\mathcal{O}_V$. For example, if $V = \mathbb{P}^n = \text{Proj}(k[X_0, \dots, X_n])$, then π_V is defined by the homomorphism of rings

$$X_i \mapsto X_i^q: k[X_0, \dots, X_n] \to k[X_0, \dots, X_n]$$

and induces the map on points

$$(x_0 : \dots : x_n) \mapsto (x_0^q : \dots : x_n^q): \mathbb{P}^n(\bar{k}) \to \mathbb{P}^n(\bar{k}).$$

For any map $\varphi: W \to V$, it is obvious that $\varphi \circ \pi_W = \pi_V \circ \varphi$. Therefore, if $A \subset \mathbb{P}^n$ is a projective embedding of A, then π_A induces the map $(x_0 : \dots : x_n) \mapsto (x_0^q : \dots : x_n^q)$ on $A(\bar{k})$. In particular, we see that the kernel of $1 - \pi_A^m: A(\bar{k}) \to A(\bar{k})$ is $A(k_m)$. Note that π_A maps zero to zero, and therefore (see (2.2)) is a homomorphism. Clearly π always defines the zero map on tangent spaces (look at its action on the cotangent space), and so $d(1 - \pi_A^m)_0: T_0(A) \to T_0(A)$ is the identity map. Therefore, $1 - \pi_A^m$ is étale, and the order N_m of its kernel in $A(\bar{k})$ is equal to its degree. Let P be the characteristic polynomial of π_A. It is a monic polynomial of degree $2g$ with integer coefficients, and if we let $a_1, \dots, a_{2g}$ be its roots, then (12.9) shows that $\prod(X - a_i^m)$ is the characteristic polynomial of π_A^m. Consequently,

$$N_m = \deg(\pi_A^m - 1) = \prod(1 - a_i^m).$$

This proves (a) and (b) of the theorem with the added information that P is the characteristic polynomial of π_A. Part (c) follows from the next two lemmas.

Lemma 19.2. *Let $\dagger$ be the Rosati involution on $\text{End}^0(A)$ defined by a polarization of A; then $\pi_A^\dagger \circ \pi_A = q_A$.*

PROOF. As was noted in (13.2), the polarization will be defined by an ample sheaf $\mathcal{L}$ on A. We have to show that $\pi_A^\vee \circ \varphi_{\mathcal{L}} \circ \pi_A = q\varphi_{\mathcal{L}}$. It follows from the definition of π_A that $\pi_A^* \mathcal{L} \approx \mathcal{L}^q$. Therefore, for all $a \in A(\bar{k})$,

$$\pi_A^\vee \circ \varphi_{\mathcal{L}} \circ \pi_A(a) = \pi_A^*(t_{\pi a}^* \mathcal{L} \otimes \mathcal{L}^{-1}) = t_a^*(\pi_A^* \mathcal{L}) \otimes (\pi_A^* \mathcal{L})^{-1} = q\varphi_{\mathcal{L}}(a),$$

as required. □

Lemma 19.3. *Let α be an element of $\text{End}^0(A)$ such that $\alpha^\dagger \circ \alpha$ is an integer r; for any root a of P_α, $|a|^2 = r$.*

PROOF. Note that $\mathbb{Q}(\alpha)$ is stable under $\dagger$. The argument terminating the proof of (17.5) shows that $\mathbb{Q}(\alpha)$ contains no nilpotent elements, and therefore is a product of fields. The tensor product $\mathbb{Q}(\alpha) \otimes \mathbb{R}$ is a product of copies of $\mathbb{R}$ and $\mathbb{C}$. Moreover $\dagger$ extends to an $\mathbb{R}$-linear involution of $\mathbb{Q}(\alpha) \otimes \mathbb{R}$, and $\text{Tr}(\beta^\dagger \beta) \geq 0$ for all $\beta \neq 0$, with inequality holding on a dense subset. It follows easily that each factor K of $\mathbb{Q}(\alpha) \otimes \mathbb{R}$ is stable under $\dagger$ and that $\dagger$ is the

identity map if K is real, and is complex conjugation if K is complex. Thus, for each homomorphism ι of $\mathbb{Q}(\alpha)$ into $\mathbb{C}$, $\iota(\alpha^\dagger)$ is the complex conjugate of $\iota\alpha$. The hypothesis of the theorem therefore states that $|\iota\alpha|^2 = r$, which, in essence, is also the conclusion. □

The zeta function of a variety V over k is defined to be the formal power series $Z(V, t) = \exp(\sum N_m t^m/m)$.

Corollary 19.4. *Let $P_r(t) = \prod(1 - a_{i,r}t)$, where the $a_{i,r}$ run through the products $a_{i_1} a_{i_2} \dots a_{i_r}$, $0 < i_1 < \dots < i_r \leq 2g$, a_i a root of $P(t)$.*

Then

$$Z(A, t) = \frac{P_1(t) \dots P_{2g-1}(t)}{[P_0(t) \dots P_{2g}(t)]}.$$

PROOF. Take the logarithm of each side, and use the identity

$$-\log(1 - t) = 1 + t + t^2/2 + t^3/3 + \cdots.$$ □

Remark 19.5. (a) The polynomial $P_r(t)$ is the characteristic polynomial of π acting on $\Lambda^r T_l A$.

(b) Let $\zeta(V, s) = Z(V, q^{-s})$; then (19.1c) implies that the zeros of $\zeta(V, s)$ lie on the lines $\text{Re}(s) = 1/2, 3/2, \dots, (2g - 1)/2$ and the poles on the lines $\text{Re}(s) = 0, 1, \dots, 2g$.

Remark 19.6. The isomorphism $\Lambda^r T_l A \approx H^r(A_{\text{et}}, \mathbb{Q}_l)^\vee$ and the above results show that

$$N_m = \sum(-1)^r \text{Tr}(\pi | H^r(A_{\text{et}}, \mathbb{Q}_l))$$

and that

$$Z(A, t) = \prod \det(1 - \pi t | H^r(A_{\text{et}}, \mathbb{Q}_l))^{(-1)^r}.$$

§20. Abelian Schemes

Let S be a scheme; a group scheme $\pi: \mathcal{A} \to S$ over S is an *abelian scheme* if π is proper and smooth and the geometric fibres of π are connected. The second condition means that, for all maps $\bar{s} \to S$ with $\bar{s}$ the spectrum of an algebraically closed field, the pull-back $\mathcal{A}_{\bar{s}}$ of $\mathcal{A}$ to $\bar{s}$ is connected. In the presence of the first condition, it is equivalent to the fibres of π being abelian varieties. Thus an abelian scheme over S can be thought of as a continuous family of abelian varieties parametrized by S.

Many results concerning abelian varieties extend to abelian schemes.

Proposition 20.1 (Rigidity Lemma). *Let S be a connected scheme, and let $\pi: \mathcal{V} \to S$ be a proper flat map whose fibres are varieties; let $\pi': \mathcal{V}' \to S$ be a*

second S-scheme, and let $f: \mathscr{V} \to \mathscr{V}'$ be a morphism of S-schemes. If for some point s of S, the image of $\mathscr{V}_s$ in $\mathscr{V}'_s$ is a single point, then f factors through S (that is, there exists a map $f': S \to \mathscr{V}'$ such that $f = f' \circ \pi$).

PROOF. See [15, 6.1]. □

Corollary 20.2. (a) *Every morphism of abelian schemes carrying the zero section into the zero section is a homomorphism.*
(b) *The group structure on an abelian scheme is uniquely determined by the choice of a zero section.*
(c) *An abelian scheme is commutative.*

PROOF. (a) Apply the proposition to the map $\varphi: \mathscr{A} \times \mathscr{A} \to \mathscr{B}$ defined as in the proof of (2.2).
(b) This follows immediately from (a).
(c) The map $a \mapsto a^{-1}$ is a homomorphism. □

Our next result shows that an abelian variety cannot contain a non-constant algebraic family of subvarieties.

Proposition 20.3. *Let A be an abelian variety over a field k, and let S be a k-scheme such that $S(k) \neq \emptyset$. For any injective homomorphism $f: \mathscr{B} \subset A \times S$ of abelian schemes over S, there is an abelian subvariety B of A (defined over k) such that $f(\mathscr{B}) = B \times S$.*

PROOF. Let $s \in S(k)$, and let $B = \mathscr{B}_s$. Then f_s identifies B with a subvariety of A. The map $h: \mathscr{B} \xrightarrow{f} A \times S \twoheadrightarrow (A/B) \times S$ has fibre $B_s \to A \to A/B_s$ over s, which is zero, and so (20.1) shows that $h = 0$. It follows that $f(\mathscr{B}) = B \times S$. □

Recall that a finitely generated extension K of a field k is *regular* if it is linearly disjoint from $\bar{k}$.

Corollary 20.4. *Let K be a regular extension of a field k.*

(a) *Let A be an abelian variety over k. Then every abelian subvariety of A_K is defined over k.*
(b) *If A and B are abelian varieties over k, then every homomorphism $\alpha: A_K \to B_K$ is defined over k.*

PROOF. (a) There exists a variety V over k such that $k(V) = K$. After V has been replaced by an open subvariety, we can assume that B extends to an abelian scheme over V (cf. (20.9) below). If V has a k-rational point, then the proposition shows that B is defined over k. In any case, there exists a finite Galois extension k' of k and an abelian subvariety B' of $A_{k'}$ such that $B'_{Kk'} = B_{Kk'}$ as subvarieties of $A_{Kk'}$. The equality uniquely determines B' as a subvariety of $A_{k'}$. As σB has the same property for any $\sigma \in \mathrm{Gal}(k'/k)$, we must have $\sigma B = B$, and this shows that B is defined over k.

(b) Part (a) shows that the graph of α is defined over k. □

Theorem 20.5. *Let K/k be a regular extension of fields, and let A be an abelian variety over K. Then there exists an abelian variety B over k and a homomorphism $f: B_K \to A$ with finite kernel having the following universal property: for any abelian variety B' and homomorphism $f': B'_K \to A$ with finite kernel, there exists a unique homomorphism $\varphi: B' \to B$ such that $f' = f \circ \varphi_K$.*

PROOF. Consider the collection of pairs (B, f) with B an abelian variety over k and f a homomorphism $B_K \to A$ with finite kernel, and let A^* be the abelian subvariety of A generated by the images the f. Consider two pairs (B_1, f_1) and (B_2, f_2). Then the identity component C of the kernel of $(f_1, f_2): (B_1 \times B_2)_K \to A$ is an abelian subvariety of $B_1 \times B_2$, which (20.4) shows to be defined over k. The map $(B_1 \times B_2/C)_K \to A$ has finite kernel and image the subvariety of A generated by $f_1(B_1)$ and $f_2(B)$. It is now clear that there is a pair (B, f) such that the image of f is A^*. Divide B by the largest subgroup scheme N of $\mathrm{Ker}(f)$ to be defined over k. Then it is not difficult to see that the pair $(B/N, f)$ has the correct universal property (given $f': B'_K \to A$, note that for a suitable C contained in the kernel of $(B/N)_K \times B'_K \to A$, the map $b \mapsto (b, 0): B/N \to (B/N) \times B'/C$ is an isomorphism). □

Remark 20.6. The pair (B, f) is obviously uniquely determined up to a unique isomorphism by the condition of the theorem; it is called the *K/k-trace* of A. (For more details on the K/k-trace and the reverse concept, the K/k-image, see [12, VIII].)

Proposition 20.7. *Let $\mathscr{A}$ be an abelian scheme of relative dimension g over S, and let $n_{\mathscr{A}}$ be multiplication by n on $\mathscr{A}$. Then $n_{\mathscr{A}}$ is flat, surjective, and finite, and its kernel $\mathscr{A}_n$ is a finite flat group scheme over S of order n^{2g}. Moreover $n_{\mathscr{A}}$ (and therefore its kernel) is étale if and only if n is not divisible by any of the characteristics of the residue fields of S.*

PROOF. The map $n_{\mathscr{A}}$ is flat because $\mathscr{A}$ is flat over S and multiplication by n is flat on each fibre of $\mathscr{A}$ over S (see Section 8). (For the criterion of flatness used here, see [7, IV, 5.9] or [6, III, 5.4, Prop. 2.3].) Moreover $n_{\mathscr{A}}$ is proper [10, II, 4.8e] with finite fibres, and hence is finite (see, for example, [13, I, 1.10]). It follows that $\mathscr{A}_n$ is flat and finite, and (8.2) shows that it has order n^{2g}. The remaining statement also follows from (8.2). □

Corollary 20.8. *Let S be an connected normal scheme, and let A be an abelian variety over the field of rational functions k of S. Assume that A extends to an abelian scheme over S, and let n be an integer which is prime to the characteristics of the residue fields of S. Then for any point $P \in A(k)$, the normaliza-*

tion of S in $k(n^{-1}P)$ is étale over S. (By $k(n^{-1}P)$ we mean the field generated over k by the coordinates of the points Q such that $nQ = P$.)

PROOF. The hypotheses imply that $\mathscr{A}_n$ is étale over S. Let k' be the composite of the fields of rational functions of the components of $\mathscr{A}_n$, and let k'' be the Galois closure of k'. Then the normalization of S in k'' is étale over S and $A_n(k'')$ has n^{2g} elements. We may replace k with k'' and so assume A has all its points of order n rational in k. The point P extends (by the valuative criterion of properness) to a section s of $\mathscr{A}$ over S. The pull-back of the covering $n_{\mathscr{A}}\colon \mathscr{A} \to \mathscr{A}$ to S by means of the section s is a finite étale covering $S' \to S$, and s lifts to a section in $\mathscr{A}(S')$. Let S_0 be any connected component of S'; then the field K of rational functions of S contains $k(n^{-1}P)$, and S_0 is the normalization of S in K. □

Remark 20.9. Let S be an integral Noetherian scheme, and let A be an abelian variety over its field of rational functions K. Choose a projective embedding $A \subset \mathbb{P}^n$ and let $\mathscr{A}$ be the closure of A in $\mathbb{P}^n_S$. Then $\pi\colon \mathscr{A} \to S$ is projective, and its generic fibre is a smooth variety. As $\mathscr{O}_S \to \pi_*\mathscr{O}_{\mathscr{A}}$ is an isomorphism at the generic point and $\mathscr{O}_S$ and $\pi_*\mathscr{O}_{\mathscr{A}}$ are coherent, there will be an open subset over which it is an isomorphism and therefore over which π has connected fibres [10, III, 11.5]. The existence of a section implies the fibres will be geometrically connected there. Also there will be an open subset over which $\mathscr{A}$ is smooth [10, III, Ex. 10.2], and an open subset where the group structure extends. These remarks show that there is an open subset U of S such that $\mathscr{A}$ extends to an abelian scheme over U.

When S is locally the spectrum of a Dedekind domain, we can be more precise. Then the projective embedding of A determines a unique extension of A to a flat projective scheme $\pi\colon \mathscr{A} \to S$ (see [10, III, 9.8]). The R-module $\pi_*\mathscr{O}_{\mathscr{A}}$ is finitely-generated (because π is proper) and torsion-free (because π is flat). It is therefore a projective R-module, and its rank is one because its tensor product with K is $\Gamma(A, \mathscr{O}_A) = K$. Now, as before, the geometric fibres of $\mathscr{A}$ are connected. We conclude: the choice of a projective embedding defines a flat projective extension $\mathscr{A}$ of A to S; $\mathscr{A}$ will be an abelian scheme over an open set U of S.

It is clear from looking at the example of an elliptic curve, that the extended scheme $\mathscr{A}$ over S depends on the choice of the projective embedding of A, but [2, 1.4] shows that its restriction to U does not. The purpose of the theory of Néron models is to replace $\mathscr{A}$ by a "minimal" (nonproper) extension which is unique.

Using the above results, it is possible to give a short proof of a weak form of the Mordell–Weil theorem.

Theorem 20.10. *Let A be an abelian variety over a number field k, and let n be integer such that all points of A of order n are rational over k. Then $A(k)/nA(k)$ is a finite group.*

PROOF. Let $a \in A(k)$, and let $b \in A(\bar{k})$ be such that $nb = a$. For σ in the Galois group of $\bar{k}$ over k, define $\varphi_a(\sigma)$ to be $\sigma b - b$. Then $a \mapsto \varphi_a$ defines an injection $A(k)/nA(k) \subset \mathrm{Hom}(G, A_n(k))$.

Let spec(R) be an open subset of the spectrum of the ring of integers of k such that A extends to an abelian scheme $\mathscr{A}$ over spec(R) and n is invertible in R. Let k' be the maximal abelian extension of k of exponent n unramified outside the finite set of primes not corresponding to prime ideals of R. Then (20.8) shows that φ_a factors through the group $\mathrm{Gal}(k'/k)$ for all a. This proves the theorem because k' is a finite extension of k. □

Remark 20.11. Using the theory of heights, one can show that for an abelian variety over a number field k, $A(k)/nA(k)$ finite implies $A(k)$ is finitely generated (see [23]). As the hypothesis of (20.10) always holds after a finite extension of k, this proves the Mordell–Weil theorem: for any abelian variety A over a number field k, $A(k)$ is finitely generated.

Remark 20.12. Let A and B be polarized abelian varieties over a number field k, and assume that they both have good reduction outside a given finite set of primes S; let l be an odd prime. If A and B are isomorphic over $\bar{k}$ (as polarized abelian varieties), then they are isomorphic over an extension k' of k unramified outside S and l and of degree $\leq$ (order of $\mathrm{Gl}_{2g}(\mathbb{F}_l))^2$. (Because the l-torsion points of A and B are rational over such a k', and we can apply (17.7).)

In contrast to abelian varieties, abelian schemes are not always projective, even if the base scheme is the spectrum of an integral local ring of dimension one or an Artinian ring (see [18, XII]). If $\mathscr{A}$ is projective over S, then the dual abelian scheme $\mathscr{A}^\vee$ is known to exist (see [8]); if $\mathscr{A}$ is not projective then $\mathscr{A}^\vee$ exists only as an algebraic space (see [1]). In either case, a *polarization* of $\mathscr{A}$ is defined to be a homomorphism $\lambda\colon \mathscr{A} \to \mathscr{A}^\vee$ such that, for all geometric points $\bar{s}$ of the base scheme S, $\lambda_{\bar{s}}$ is of the form $\varphi_{\mathscr{L}}$ for some ample invertible sheaf $\mathscr{L}$ on $\mathscr{A}_{\bar{s}}$. Alternatively, λ is a polarization if $\lambda_s\colon \mathscr{A}_s \to \mathscr{A}_s^\vee$ is a polarization of abelian varieties for all $s \in S$. If S is connected, then the degree of λ_s is independent of s and is called the *degree* of λ.

For a field k and fixed integers g and d, let $\mathscr{F}_{g,d}$ be the functor associating with each k-scheme of finite type the set of isomorphism classes of polarized abelian schemes of dimension g and which have a polarization of degree d^2.

Theorem 20.13. *There exists a variety $M_{g,d}$ over k and a natural transformation $i\colon \mathscr{F}_{g,d} \to M_{g,d}$ such that:*

(a) *$i(K)\colon \mathscr{F}_{g,d}(K) \to M_{g,d}(K)$ is a bijection for any algebraically closed field containing k;*

(b) *for any variety N over k and natural transformation $j\colon \mathscr{F}_{g,d} \to N$, there is a unique morphism $\varphi\colon M_{g,d} \to N$ such that $\varphi \circ i = j$.*

PROOF. This one of the main results of [15]. □

The variety $M_{g,d}$ is uniquely determined up to a unique isomorphism by the conditions of (20.13); it is the (coarse) *moduli variety* for polarized abelian varieties of dimension g and degree d^2. By introducing level structures, one can define a functor that is representable by a fine moduli variety—see the article by C.-L. Chai in these proceedings.

REFERENCES

[1] Artin, M. Algebraization of formal moduli I, in *Global Analysis*. Princeton University Press: Princeton, NJ, 1969, pp. 21–71.
[2] Artin, M. Néron models, this volume, pp. 213–230.
[3] Borel, A. Sur la cohomologie des espaces fibrés principaux et des espace homogènes de groupes de Lie compacts. *Ann. Math.*, **64** (1953), 115–207.
[4] Borel, A. *Introduction aux Groupes Arithmétiques*. Hermann: Paris, 1958.
[5] Bourbaki, N. *Algèbre Multilinéaire*. Hermann: Paris, 1958.
[6] Bourbaki, N. *Algèbre Commutative*. Hermann: Paris, 1961, 1964, 1965.
[7] Grothendieck, A. *Revêtements Étales et Groupe Fondamental* (SGA1, 1960–61). Lecture Notes in Mathematics, 224. Springer-Verlag: Heidelberg, 1971.
[8] Grothendieck, A.: Technique de descente et théorèmes d'existence en géométrie algébrique V. Les schémas de Picard: Théorèmes d'existence. *Séminaire Bourbaki*, Exposé 232, 1961/62.
[9] Grothendieck, A. (with Dieudonné, J.). Eléments de géométrie algébrique. *Publ. Math. I.H.E.S.*, **4, 8, 11, 17, 20, 24, 28, 32** (1960–67).
[10] Hartshorne, R. *Algebraic Geometry*. Springer-Verlag: Heidelberg, 1977.
[11] Humphreys, J. *Linear Algebraic Groups*. Springer-Verlag: Heidelberg, 1975.
[12] Lang, S. *Abelian Varieties*. Interscience: New York, 1959.
[13] Milne, J. *Étale Cohomology*. Princeton University Press: Princeton, NJ, 1980.
[14] Mumford, D. *Introduction to Algebraic Geometry*. Lecture Notes, Harvard University: Cambridge, MA, 1967.
[15] Mumford D. *Geometric Invariant Theory*. Springer-Verlag: Heidelberg, 1965.
[16] Mumford D. *Abelian Varieties*. Oxford University Press: Oxford, 1970.
[17] Oort, *F. Commutative Group Schemes*. Lecture Notes in Mathematics. Springer-Verlag: Heidelberg, 1966.
[18] Raynaud, M. *Faisceaux Amples sur les Schémas en Groupes et les Espace Homogènes*. Lecture Notes in Mathematics, 119. Springer-Verlag: Heidelberg, 1970.
[19] Rosen, M. (notes by F. McGuinness). Abelian varieties over $\mathbb{C}$, this volume, pp. 79–101.
[20] Serre, J.-P. *Groupes Algèbriques et Corps de Classes*. Hermann: Paris, 1959.
[21] Shafarevich, I. *Basic Algebraic Geometry*. Springer-Verlag: Heidelberg, 1974.
[22] Shatz, S. Group schemes, formal groups, and p-divisible groups, this volume, pp. 29–78.
[23] Silverman, J. The theory of height functions, this volume, pp. 151–166.
[24] Waterhouse, W. *Introduction to Affine Group Schemes*. Springer-Verlag: Heidelberg, 1979.
[25] Weil, A. Algebras with involution and classical groups. *J. Indian Math. Soc.*, **24** (1960), 589–623.

CHAPTER VI

The Theory of Height Functions

JOSEPH H. SILVERMAN

The Classical Theory of Heights

§1. Absolute Values

The following notations and normalizations will be used throughout this chapter:

$K/\mathbb{Q}$ a number field.
M_K the set of absolute values on K extending the usual absolute values on $\mathbb{Q}$. (That is, the p-adic absolute values are normalized so that $|p|_p = 1/p$.)
$\|\cdot\|_v = |\cdot|_v^{[K_v:\mathbb{Q}_v]}$.

§2. Height on Projective Space

The height of a point $P = [x_0, \ldots, x_n]$ in $\mathbb{P}^n(K)$ is a measure of the "arithmetic complexity" of the point.

Definition. The *height of* P (*relative to* K) is defined by the formula

$$H_K(P) = \prod_{v \in M_K} \max\{\|x_0\|_v, \ldots, \|x_n\|_v\}.$$

Remarks. (1) The height of P is well defined (independent of the choice of homogeneous coordinates for P). This is easily checked using the product formula.