ABELIAN VARIETIES

J.S. MILNE

ABSTRACT. These are the notes for Math 731, taught at the University of Michigan in Fall 1991, somewhat revised from those handed out during the course. They are available at `www.math.lsa.umich.edu/~jmilne/`.

Please send comments and corrections to me at jmilne@umich.edu.

v1.1 (July 27, 1998). First version on the web. These notes are in more primitive form than my other notes — the reader should view them as an unfinished painting in which some areas are only sketched in.

CONTENTS

Introduction

The easiest way to understand abelian varieties is as higher-dimensional analogues of elliptic curves. Thus we first look at the various definitions of an elliptic curve.

Fix a ground field k which, for simplicity, we take to be algebraically closed.

0.1. An elliptic curve is the projective curve given by an equation of the form

$$Y^2Z = X^3 + aXZ + bZ^3,\ \Delta \stackrel{\text{df}}{=} 4a^3 + 27b^2 \neq 0. \quad (*)$$

(char $\neq 2, 3$).

0.2. An elliptic curve is a nonsingular projective curve of genus one together with a distinguished point.

0.3. An elliptic curve is a nonsingular projective curve together with a group structure defined by regular maps.

0.4. ($k = \mathbb{C}$) An elliptic curve is complex manifold of the form $\mathbb{C}/\Lambda$ where Λ is a lattice in $\mathbb{C}$.

We briefly sketch the equivalence of these definitions (see also my notes on Elliptic Curves, especially §§5,10).

(0.1) $\implies$(0.2). The condition $\Delta \neq 0$ implies that the curve is nonsingular; take the distinguished point to be $(0 : 1 : 0)$.

(0.2) $\implies$(0.1). Let ∞ be the distinguished point on the curve E of genus 1. The Riemann-Roch theorem says that

$$\dim\ L(D) = \deg(D) + 1 - g = \deg(D)$$

where

$$L(D) = \{f \in k(E) \mid \ \operatorname{div}(f) + D \geq 0\}.$$

On taking $D = 2\infty$ and $D = 3\infty$ successively, we find that there is a rational function x on E with a pole of exact order 2 at ∞ and no other poles, and a rational function y on E with a pole of exact order 3 at ∞ and no other poles. The map

$$P \mapsto (x(P) : y(P) : 1),\ \infty \mapsto (0 : 1 : 0)$$

defines an embedding

$$E \hookrightarrow \mathbb{P}^2.$$

On applying the Riemann-Roch theorem to 6∞, we find that there is relation (*) between x and y, and therefore the image is a curve defined by an equation (*).

(0.1,2) $\implies$(0.3): Let $Div^0(E)$ be the group of divisors of degree zero on E, and let $Pic^0(E)$ be its quotient by the group of principal divisors; thus $Pic^0(E)$ is the group of divisor classes of degree zero on E. The Riemann-Roch theorem shows that the map

$$P \mapsto [P] - [\infty] \colon E(k) \to Pic^0(E)$$

is a bijection, from which $E(k)$ acquires a canonical group structure. It agrees with the structure defined by chords and tangents, and hence is defined by polynomials, i.e., it is defined by regular maps.

(0.3) $\implies$(0.2): We have to show that the existence of the group structure implies that the genus is 1. Our first argument applies only in the case $k = \mathbb{C}$. The Lefschetz trace formula states that, for a compact oriented manifold X and a continuous map $\alpha : X \to X$ with only finitely many fixed points, each of multiplicity 1,

$$\text{number of fixed points} = \mathrm{Tr}(\alpha|H^0(X,\mathbb{Z})) - \mathrm{Tr}(\alpha|H^1(X,\mathbb{Z})) + \cdots$$

If X has a group structure, then, for any nonzero point $a \in X$, the translation map $t_a\colon x \mapsto x + a$ has no fixed points, and so

$$Tr(t_a) \stackrel{\text{df}}{=} \Sigma(-1)^i \,\mathrm{Tr}(t_a|H^i(X,\mathbb{Q})) = 0.$$

The map $a \mapsto \mathrm{Tr}(t_a)\colon X \to \mathbb{Z}$ is continuous, and so $\mathrm{Tr}(t_a) = 0$ also for $a = 0$. But t_0 is the identity map, and

$$\mathrm{Tr}(\mathrm{id}) = \sum(-1)^i \ \dim H^i(X,\mathbb{Q}) = \chi(X) \text{ (Euler-Poincaré characteristic).}$$

Since the Euler-Poincaré characteristic of a complete nonsingular curve of genus g is $2-2g$, we see that if X has a group structure then $g = 1$. [The same argument works over any field if one replaces singular cohomology with étale cohomology.]

We now give an argument that works over any field. If V is an algebraic variety with a group structure, then the sheaf of differentials is free. For a curve, this means that the canonical divisor class has degree zero. But this class has degree $2g-2$, and so again we see that $g = 1$.

(0.4) $\implies$(0.2). The Weierstrass $\wp$-function and its derivative define an embedding

$$z \mapsto (\wp(z) : \wp'(z) : 1) : \mathbb{C}/\Lambda \hookrightarrow \mathbb{P}^2,$$

whose image is a nonsingular projective curve of genus 1 (in fact, with equation of the form (*)).

(0.2) $\implies$(0.4). This follows from topology.

Abelian varieties. Definition (0.1) simply doesn't generalize — there is no simple description of the equations defining an abelian variety of dimension[1] $g > 1$. In general, it is not possible to write down explicit equations for an abelian variety of dimension > 1, and if one could, they would be too complicated to be of use.

I don't know whether (0.2) generalizes. Abelian surfaces are the only minimal surfaces with the Betti numbers

$$1, 4, 6, 4, 1$$

[1]The case $g = 2$ is something of an exception to this statement. Every abelian variety of dimension 2 is the Jacobian variety (see below) of a curve of genus 2, and every curve of genus 2 has an equation of the form

$$Y^2Z^4 = f_0X^6 + f_1X^5Z + \cdots + f_6Z^6.$$

Flynn (Math. Proc. Camb. Phil. Soc. 107, 425–441) has found the equations of the Jacobian variety of such a curve in characteristic $\neq 2, 3, 5$ — they form a set 72 homogeneous equations of degree 2 in 16 variables (they take 6 pages to write out). See: Cassels, J.W.S., and Flynn, E.V., Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2, Cambridge, 1996.

and canonical class linearly equivalent to zero. In general an abelian variety of dimension g has Betti numbers

$$1, \binom{2g}{1}, \ldots, \binom{2g}{r}, \ldots, 1.$$

Definition (0.3) does generalize: we can define an abelian variety to be a nonsingular connected projective[2] variety with a group structure defined by regular maps.

Definition (0.4) does generalize, but with a caution. If A is an abelian variety over $\mathbb{C}$, then

$$A(\mathbb{C}) \approx \mathbb{C}^g/\Lambda$$

for some lattice Λ in $\mathbb{C}^g$ (isomorphism simultaneously of complex manifolds and of groups). However, when $g > 1$, for not all lattices Λ does $\mathbb{C}^g/\Lambda$ arise from an abelian variety. In fact, in general the transcendence degree over $\mathbb{C}$ of the field of meromorphic functions $\mathbb{C}^g/\Lambda$ is $< g$, with equality holding if and only if $\mathbb{C}^g/\Lambda$ is an algebraic (hence abelian) variety. There is a very pleasant criterion on Λ for when $\mathbb{C}^g/\Lambda$ is algebraic (§2).

Abelian varieties and elliptic curves. As we noted, if E is an elliptic curve over an algebraically closed field k, then there is a canonical isomorphism

$$P \mapsto [P] - [0]\colon E(k) \to Pic^0(E).$$

This statement has two generalizations.

(A). Let C be a curve and choose a point $Q \in C(k)$; then there is an abelian variety J, called the Jacobian variety of C, canonically attached to C, and a regular map $\varphi : C \to J$ such that $\varphi(Q) = 0$ and

$$\Sigma\ n_i P_i \mapsto \Sigma\ n_i\ \varphi(P_i)\colon Div^0(C) \to J(k)$$

induces an isomorphism $Pic^0(C) \to J(k)$. The dimension of J is the genus of C.

(B). Let A be an abelian variety. Then there is a "dual abelian variety" $A^\vee$ such that $Pic^0(A) = A^\vee(k)$ and $Pic^0(A^\vee) = A(k)$ (we shall define Pic^0 in this context later). In the case of an elliptic curve, $E^\vee = E$. In general, A and $A^\vee$ are isogenous, but they are not equal (and usually not even isomorphic).

Appropriately interpreted, most of the statements in Silverman's books on elliptic curves hold for abelian varieties, but because we don't have equations, the proofs are more abstract. In fact, every (reasonable) statement about elliptic curves should have a generalization that applies to all abelian varieties. However, for some, for example, the Taniyama conjecture, the correct generalization is difficult to state[3]. To pass from a statement about elliptic curves to one about abelian varieties, replace 1 by g (the dimension of A), and half the copies of E by A and half by $A^\vee$. I give some examples.

[2]For historical reasons, we define them to be complete varieties rather than projective varieties, but they turn out to be projective anyway.

[3]Blasius has pointed out that, by looking at infinity types, one can see that the obvious generalization of the Taniyama conjecture, that every abelian variety over $\mathbb{Q}$ is a quotient of an Albanese variety of a Shimura variety, can't be true.

Let E be an elliptic curve over an algebraically closed field k. For any integer n not divisible by the characteristic the set of n-torsion points on E

$$E(k)_n \approx (\mathbb{Z}/n\mathbb{Z})^2,$$

and there is a canonical nondegenerate pairing

$$E(k)_n \times E(k)_n \to \mu_n(k) \text{ (Weil pairing).}$$

Let A be an abelian variety of dimension g over an algebraically closed field k. For any integer n not divisible by the characteristic,

$$A(k)_n \approx (\mathbb{Z}/n\mathbb{Z})^{2g},$$

and there is a canonical nondegenerate pairing

$$A(k)_n \times A^\vee(k)_n \to \mu_n(k) \text{ (Weil pairing).}$$

Let E be an elliptic curve over a number field k. Then $E(k)$ is finitely generated (Mordell-Weil theorem), and there is a canonical height pairing

$$E(k) \times E(k) \to \mathbb{Z}$$

which becomes nondegenerate when tensored with $\mathbb{Q}$. Let A be an abelian variety over a number field k. Then $A(k)$ is finitely generated (Mordell-Weil theorem), and there is a canonical height pairing

$$A(k) \times A^\vee(k) \to \mathbb{Z}$$

which becomes nondegenerate when tensored with $\mathbb{Q}$.

For an elliptic curve E over a number field k, the conjecture of Birch and Swinnerton-Dyer states that

$$L(E,s) \sim * \frac{[TS(E)][\mathrm{Disc}]}{[E(k)_{\mathrm{tors}}]^2}(s-1)^r \text{ as } s \to 1,$$

where $*$ is a minor term, $TS(E)$ is the Tate-Shafarevich group of E, *Disc* is the discriminant of the height pairing, and r is the rank of $E(k)$. For an abelian variety A, the Tate generalized the conjecture to the statement

$$L(A,s) \sim * \frac{[TS(A)][\mathrm{Disc}]}{[A(k)_{\mathrm{tors}}][A^\vee(k)_{\mathrm{tors}}]}(s-1)^r \text{ as } r \to 1.$$

We have $L(A,s) = L(A^\vee,s)$, and Tate proved that $[TS(A)] = [TS(A^\vee)]$ (in fact the two groups, if finite, are canonically dual), and so the formula is invariant under the interchange of A and $A^\vee$.

REMARK 0.5. We noted above that the Betti number of an abelian variety of dimension g are $1, \binom{2g}{1}, \binom{2g}{2}, ..., \binom{2g}{r}, ..., 1$. Therefore the Lefschetz trace formula implies that $\Sigma(-1)^{r+1}\binom{2g}{r} = 0$. Of course, this can also be proved by using the binomial theorem to expand $(1-1)^{2g}$.

EXERCISE 0.6. Assume $A(k)$ and $A^\vee(k)$ are finitely generated, of rank r say, and that the height pairing

$$\langle \cdot, \cdot \rangle : A(k) \times A^\vee(k) \to \mathbb{Z}$$

is nondegenerate when tensored with $\mathbb{Q}$. Let $e_1, ..., e_r$ be elements of $A(k)$ that are linearly independent over $\mathbb{Z}$, and let $f_1, ..., f_r$ be similar elements of $A^\vee(k)$; show that

$$\frac{|\det(\langle e_i, f_j\rangle)|}{(A(k) : \Sigma\mathbb{Z}e_i)(A^\vee(k) : \Sigma\mathbb{Z}f_j)}$$

is independent of the choice of the e_i and f_j. [This is an exercise in linear algebra.]

The first part of these notes covers the basic theory of abelian varieties over arbitrary fields, and the second part is an introduction to Faltings's proof of Mordell's Conjecture.

Some Notations. Our conventions concerning varieties are the same as those in my notes on Algebraic Geometry, which is the basic reference for these notes. For example, an affine algebra over a field k is a finitely generated k-algebra A such that $A\otimes_k k^{\mathrm{al}}$ has no nonzero nilpotents for one (hence every) algebraic closure k^{al} of k. With such a k-algebra, we associate a ring space $\mathrm{Specm}(A)$ (topological space endowed with a sheaf of k-algebras) and an affine variety over k is a ringed space isomorphic to one of this form. A variety over k is a ringed space $(V, \mathcal{O}_V)$ admitting a finite open covering $V = \cup U_i$ such that $(U_i, \mathcal{O}_V|U_i)$ is an affine variety for each i and which satisfies the separation axiom. If V is a variety over k and $K \supset k$, then $V(K)$ is the set of points of V with coordinates in K and V_K or $V_{/K}$ is the variety over K obtained from V by extension of scalars. Occasionally, we also use schemes.

We often describe regular maps by their actions on points. Recall that a regular map $\phi\colon V \to W$ of k-varieties is determined by the map of points $V(k^{\mathrm{al}}) \to W(k^{\mathrm{al}})$ that it defines. Moreover, to give a regular map $V \to W$ is the same as to give maps $V(R) \to W(R)$, for R running over the affine k-algebras, that are functorial in R (AG 3.29 and AG p135).

Throughout, k is an arbitrary field. The symbol k^{sep} denotes a separable closure of k, i.e., a field algebraic over k such that every separable polynomial in $k[X]$ has a root in k^{sep}. For a vector space N over a field k, $N^\vee$ denotes the dual vector space $\mathrm{Hom}_k(N, k)$.

We use the following notations:

$X \approx Y$	X and Y are isomorphic;
$X \cong Y$	X and Y are canonically isomorphic (or there is a given or unique isomorphism);
$X \overset{\mathrm{df}}{=} Y$	X is defined to be Y, or equals Y by definition;
$X \subset Y$	X is a subset of Y (not necessarily proper).

References. Lang, S., Abelian Varieties, Interscience, 1959.

Lange, H., and Birkenhake, Ch., Complex Abelian Varieties, Springer, 1992.

Milne, J.S., Abelian varieties, in Arithmetic Geometry (ed. Cornell, G., and Silverman) pp103-150 (cited as **AV**).

Milne, J.S., Jacobian varieties, ibid., pp167-212 (cited as **JV**).

Mumford, D., Abelian Varieties, Oxford, 1970.

Murty, V. Kumar, Introduction to Abelian Varieties, CRM, 1993.

Serre: Lectures on the Mordell-Weil theorem, Vieweg, 1989.

Silverman, J., The Arithmetic of Elliptic Curves, Springer, 1986.

Silverman, J., Advanced Topics in the Arithmetic of Elliptic Curves, Springer, 1994.

Weil, A., Sur les Courbes Algébriques et les Variétés qui s'en Déduisent, Hermann, 1948.

Weil, A., Variétés Abéliennes et Courbes Algébriques, Hermann, 1948.

Mumford's book is the only modern account of the subject, but as an introduction it is rather difficult. It treats only abelian varieties over algebraically closed fields; in particular, it does not cover the arithmetic of abelian varieties. Weil's books contain the original account of abelian varieties over fields other than $\mathbb{C}$. Serre's notes give an excellent treatment of some of the arithmetic of abelian varieties (heights, Mordell-Weil theorem, work on Mordell's conjecture before Faltings — the original title "Autour du théorème de Mordell-Weil is more accurate than the English title.). Murty's notes concentrate on the analytic theory of abelian varieties over $\mathbb{C}$ except for the final 18 pages. The book by Lange and Birkenhake is a very thorough and complete treatment of the theory of abelian varieties over $\mathbb{C}$.

Whenever possible, use my other course notes as references (because they are freely available to everyone).

GT: Group Theory (Math 594).
FT: Field and Galois Theory (Math 594).
AG: Algebraic Geometry (Math 631).
ANT: Algebraic Number Theory (Math 676).
MF: Modular Functions and Modular Forms (Math 678).
EC: Elliptic Curves (Math 679).
LEC: Lectures on Etale Cohomology (Math 732).
CFT: Class Field Theory (Math 776).

Part I: Basic Theory of Abelian Varieties

1. Definitions; Basic Properties.

A *group variety* over k is a variety V together with regular maps

$$\begin{array}{rcll} m\colon V\times_k V & \to & V & \text{(multiplication)}\\ \mathrm{inv}\colon V & \to & V & \text{(inverse)}\end{array}$$

and an element $e \in V(k)$ such that the structure on $V(k^{\mathrm{al}})$ defined by m and inv is a group with identity element e.

Such a quadruple (V, m, inv, e) is a group in the category of varieties over k. This means that

$$G \xrightarrow{(\mathrm{id},e)} G\times_k G \xrightarrow{m} G, \qquad G \xrightarrow{(e,\mathrm{id})} G\times_k G \xrightarrow{m} G$$

are both the identity map (so e is the identity element), the maps

$$G \xrightarrow{\Delta} G\times_k G \underset{\mathrm{inv}\times\mathrm{id}}{\overset{\mathrm{id}\times\mathrm{inv}}{\rightrightarrows}} G\times_k G \xrightarrow{m} G$$

are both equal to the composite

$$G \to \operatorname{Specm} k \xrightarrow{e} G$$

(so inv is the map taking an element to its inverse) and the following diagram commutes (associativity)

$$\begin{array}{ccc} G\times_k G\times_k G & \xrightarrow{1\times m} & G\times_k G\\ \downarrow m\times 1 & & \downarrow m\\ G\times_k G & \xrightarrow{m} & G. \end{array}$$

To prove that the diagrams commute, recall that the set where two morphisms of varieties disagree is open (because the target variety is separated, AG 3.8), and if it is nonempty the Nullenstellensatz (AG 1.6) shows that it will have a point with coordinates in k^{al}.

It follows that for every k-algebra R, $V(R)$ acquires a group structure, and these group structures depend functorially on R (AG p76).

Let V be a group variety over k. For a point a of V with coordinates in k, we define $t_a\colon V \to V$ *(right translation by a)* to be the composite

$$\begin{array}{ccccc} V & \to & V\times V & \xrightarrow{m} & V.\\ x & \mapsto & (x,a) & \mapsto & xa \end{array}$$

Thus, on points t_a is $x \mapsto xa$. It is an isomorphism $V \to V$ with inverse $t_{\mathrm{inv}(a)}$.

A group variety is automatically nonsingular: as does any variety, it contains a nonempty nonsingular open subvariety U (AG 4.21), and the translates of U cover V.

By definition, only one irreducible component of a variety can pass through a nonsingular point of the variety (AG p63). Thus a connected group scheme is irreducible.

A connected group variety is geometrically connected, i.e., remains connected when we extend scalars to the algebraic closure. To see this, we have to show that k is algebraically closed in $k(V)$ (AG 9.2). Let U be any open affine neighbourhood of e, and let $A = \Gamma(U, \mathcal{O}_V)$. Then A is a k-algebra with field of fractions $k(V)$, and e is a homomorphism $A \to k$. If k were not algebraically closed in $k(V)$, then there would be a field $k' \supset k$, $k' \neq k$, contained in A. But for such a field, there is no homomorphism $k' \to k$, and *a fortiori,* no homomorphism $A \to k$.

A complete connected group variety is called an *abelian variety.* As we shall see, they are projective, and (fortunately) commutative. Their group laws will be written additively. Thus t_a is now $x \mapsto x + a$ and e is usually denoted 0.

Rigidity. The paucity of maps between projective varieties has some interesting consequences.

THEOREM 1.1 (Rigidity Theorem). *Consider a regular map $\alpha\colon V \times W \to U$, and assume that V is complete and that $V \times W$ is geometrically irreducible. If there are points $u_0 \in U(k)$, $v_0 \in V(k)$, and $w_0 \in W(k)$ such that*

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

then $\alpha(V \times W) = \{u_0\}$.

In other words, if the two "coordinate axes" collapse to a point, then this forces the whole space to collapse to the point.

PROOF. Since the hypotheses continue to hold after extending scalars from k to k^{al}, we can assume k is algebraically closed. Note that V is connected, because otherwise $V \times_k W$ wouldn't be connected, much less irreducible.

We need to use the following facts:

(i) If V is complete, then the projection map $q\colon V \times_k W \to W$ is closed (this is the definition of being complete AG 5.25).

(ii) If V is complete and connected, and $\varphi\colon V \to U$ is a regular map from V into an affine variety, then $\varphi(V) = \{\text{point}\}$ (AG 5.28).

Let U_0 be an open affine neighbourhood of u_0. Because of (i), $Z \overset{\mathrm{df}}{=} q(\alpha^{-1}(U - U_0))$ is closed in W. By definition, Z consists of the second coordinates of points of $V \times W$ not mapping into U_0. Thus a point w of W lies outside Z if and only $\alpha(V \times \{w\}) \subset U_0$. In particular w_0 lies outside Z, and so $W - Z$ is nonempty. As $V \times \{w\} (\approx V)$ is complete and U_0 is affine, $\alpha(V \times \{w\})$ must be a point whenever $w \in W - Z$: in fact, $\alpha(V \times \{w\}) = \alpha(v_0, w) = \{u_0\}$. Thus α is constant on the subset $V \times (W - Z)$ of $V \times W$. As $V \times (W - Z)$ is nonempty and open in $V \times W$, and $V \times W$ is irreducible, $V \times (W - Z)$ is dense $V \times W$. As U is separated, α must agree with the constant map on the whole of $V \times W$. □

COROLLARY 1.2. *Every regular map $\alpha\colon A \to B$ of abelian varieties is the composite of a homomorphism with a translation.*

PROOF. The regular map α will send the k-rational point 0 of A to a k-rational point b of B. After composing α with translation by $-b$, we may assume that $\alpha(0) = 0$. Consider the map

$$\begin{aligned} \varphi\colon A \times A &\to B, \\ \varphi(a, a') &= \alpha(a + a') - \alpha(a) - \alpha(a'). \end{aligned}$$

By this we mean that φ is the difference of the two regular maps

$$\begin{array}{ccc} A \times A & \xrightarrow{m} & A \\ \downarrow{\scriptstyle \alpha\times\alpha} & & \downarrow{\scriptstyle \alpha} \\ B \times B & \xrightarrow{m} & B, \end{array}$$

which is a regular map. Then $\varphi(A \times 0) = 0 = \varphi(0 \times A)$ and so $\varphi = 0$. This means that α is a homomorphism. □

REMARK 1.3. The corollary shows that the group structure on an abelian variety is uniquely determined by the choice of a zero element (as in the case of an elliptic curve).

COROLLARY 1.4. *The group law on an abelian variety is commutative.*

PROOF. Commutative groups are distinguished among all groups by the fact that the map taking an element to its inverse is a homomorphism. Since the negative map, $a \mapsto -a$, $A \to A$, takes the zero element to itself, the preceding corollary shows that it is a homomorphism. □

COROLLARY 1.5. *Let V and W be complete varieties over k with k-rational points v_0 and w_0, 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 $f(v_0) = 0$ and $g(w_0) = 0$.*

PROOF. Set

$$f = h|V \times \{w_0\}, \quad g = h|\{v_0\} \times W,$$

and identify $V \times \{w_0\}$ and $\{v_0\} \times W$ with V and W. On points, $f(v) = h(v, w_0)$ and $g(w) = h(v_0, w)$, and so $k \overset{\text{df}}{=} h - (f \circ p + g \circ q)$ is the map that sends

$$(v, w) \mapsto h(v, w) - h(v, w_0) - h(v_0, w).$$

Thus

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

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

2. ABELIAN VARIETIES OVER THE COMPLEX NUMBERS.

Let A be an abelian variety over $\mathbb{C}$, and assume that A is projective (this will be proved in §6). Then $A(\mathbb{C})$ inherits a complex structure as a submanifold of $\mathbb{P}^n(\mathbb{C})$ (see AG §13). It is a complex manifold (because A is nonsingular), compact (because it is closed in the compact space $\mathbb{P}^n(\mathbb{C})$), connected (because it is for the Zariski topology), and has a commutative group structure. It turns out that these facts are sufficient to allow us to give an elementary description of $A(\mathbb{C}.)$

$A(\mathbb{C})$ **is a complex torus.** Let G be a differentiable manifold with a group structure defined by differentiable[4] maps (i.e., a real Lie group). A *one-parameter subgroup* of G is a differentiable homomorphism $\varphi\colon \mathbb{R} \to G$. In elementary differential geometry one proves that for every tangent vector v to G at e, there is a unique one-parameter subgroup $\varphi_v\colon \mathbb{R} \to G$ such that $\varphi_v(0) = e$ and $(d\varphi_v)(1) = v$ (e.g., Boothby, W., An Introduction to Differentiable Manifolds and Riemannian Geometry, Academic Press, 1975, 5.14). Moreover, there is a unique differentiable map

$$\exp\colon \operatorname{Tgt}_e(G) \to G$$

such that

$$t \mapsto \exp(tv)\colon \mathbb{R} \to \operatorname{Tgt}_e(G) \to G$$

is φ_v for all v; thus $\exp(v) = \varphi_v(1)$ (ibid. 6.9). When we identify the tangent space at 0 of $\operatorname{Tgt}_e(G)$ with itself, then the differential of exp at 0 becomes the identity map

$$\operatorname{Tgt}_e(G) \to \operatorname{Tgt}_e(G).$$

For example, if $G = \mathbb{R}^\times$, then exp is just the usual exponential map $\mathbb{R} \to \mathbb{R}^\times$. If $G = SL_n(\mathbb{R})$, then exp is given by the usual formula:

$$\exp(A) = I + A + A^2/2! + A^3/3! + \cdots,\ A \in SL_n(\mathbb{R}).$$

When G is commutative, the exponential map is a homomorphism. These results extend to complex manifolds, and give the first part of the following proposition.

PROPOSITION 2.1. *Let A be an abelian variety of dimension g over $\mathbb{C}$.*

(a) *There is a unique homomorphism*

$$exp\colon Tgt_0(A(\mathbb{C})) \to A(\mathbb{C})$$

of complex manifolds such that, for each $v \in Tgt_0(A(\mathbb{C})$, $z \mapsto \exp(zv)$ is the one-parameter subgroup $\varphi_v\colon \mathbb{C} \to A(\mathbb{C})$ corresponding to v. The differential of exp *at* 0 *is the identity map*

$$Tgt_0(A(\mathbb{C})) \to Tgt_0(A(\mathbb{C})).$$

(b) *The map* exp *is surjective, and its kernel is a full lattice in the complex vector space $Tgt_0(A(\mathbb{C}))$.*

PROOF. We prove (b). The image H of exp is a subgroup of $A(\mathbb{C})$. Because $d(\exp)$ is an isomorphism on the tangent spaces at 0, the inverse function theorem shows that exp is a local isomorphism at 0. In particular, its image contains an open neighbourhood U of 0 in H. But then, for any $a \in H$, $a+U$ is an open neighbourhood of a in H, and so H is open in $A(\mathbb{C})$. Because the complement of H is a union of translates of H (its cosets), H is also closed. But $A(\mathbb{C})$ is connected, and so any nonempty open and closed subset is the whole space. We have shown that exp is surjective.

Denote $Tgt_0(A(\mathbb{C}))$ by V, and regard it as a real vector space of dimension $2g$. A *lattice* in V is a subgroup of the form

$$L = \mathbb{Z}e_1 + \cdots + Ze_r$$

[4]By differentiable I always mean C^∞.

with $e_1, ..., e_r$ linearly independent over $\mathbb{R}$. Recall that a subgroup L of V is a lattice if and only if it is discrete for the induced topology (ANT 4.14), and that it is discrete if and only if 0 has a neighbourhood U in V such that $U \cap L = \{0\}$ (ANT 4.13). As we noted above, exp is a local isomorphism at 0. In particular, there is an open neighbourhood U of 0 such that $\exp|U$ is injective, i.e., such that $U \cap \mathrm{Ker}(\exp) = 0$. Therefore Ker(exp) is a lattice in V. It must be a full lattice (i.e., $r = 2g$) because otherwise $V/L \approx A(\mathbb{C})$ wouldn't be compact. □

We have shown that, if A is an abelian variety, then $A(\mathbb{C}) \approx \mathbb{C}^g/L$ for some full lattice L in $\mathbb{C}^g$. However, unlike the one-dimensional case, not every quotient $\mathbb{C}^g/L$ arises from an abelian variety. Before stating a necessary and sufficient condition for a quotient to arise in this way, we compute the cohomology of a torus.

The cohomology of a torus. Let $X = V/L$, where V is real vector space of dimension n and L is a full lattice in $\mathbb{R}^n$. Note that X regarded as a differentiable manifold and its point 0 determine both V and L, because $V = \mathrm{Tgt}_0(X)$ and L is the kernel of $\exp\colon V \to X$. We wish to compute the cohomology groups of X.

Recall from algebraic topology (e.g., Greenberg, Lectures on Algebraic Topology, Benjamin, 1967).

2.2. (a) Let X be a topological space, and let $H^*(X, \mathbb{Z}) = \oplus_r H^r(X, \mathbb{Z})$; then cup-product defines on $H^*(X, \mathbb{Z})$ a ring structure; moreover

$$a^r \cup b^s = (-1)^{rs} b^s \cup a^r,\ a^r \in H^r(X, \mathbb{Z}),\ b^s \in H^s(X, \mathbb{Z})$$

(ibid. 24.8).

(b) (Künneth formula): Let X and Y be topological spaces such that $H^r(X, \mathbb{Z})$ and $H^s(Y, \mathbb{Z})$ are free $\mathbb{Z}$-modules for all r, s. Then there is a canonical isomorphism

$$H^m(X \times Y, \mathbb{Z}) \cong \oplus_{r+s=m}\ H^r(X, \mathbb{Z}) \otimes H^s(Y, \mathbb{Z}).$$

The map $H^r(X, \mathbb{Z}) \otimes H^s(Y, \mathbb{Z}) \to H^{r+s}(X \times Y, \mathbb{Z})$ is

$$a \otimes b \mapsto p^*a \cup q^*b \text{ (cup-product)}$$

where p and q are the projection maps $X \times Y \to X, Y$.

(c) If X is a "reasonable" topological space, then

$$H^1(X, \mathbb{Z}) \cong \mathrm{Hom}(\pi_1(X, x), \mathbb{Z})$$

(ibid. 12.1; 23.14).

(d) If X is compact and orientable of dimension d, the duality theorems (ibid. 26.6, 23.14) show that there are canonical isomorphisms

$$H^r(X, \mathbb{Z}) \cong H_{d-r}(X, \mathbb{Z}) \cong H^{d-r}(X, \mathbb{Z})^\vee$$

when all the cohomology groups are torsion-free.

We first compute the dimension of the groups $H^r(X, \mathbb{Z})$. Note that, as a real manifold, $V/L \approx (\mathbb{R}/\mathbb{Z})^n \approx (S^1)^n$ where S^1 is the unit circle. We have

$$H^r(S^1, \mathbb{Z}) = \mathbb{Z}, \mathbb{Z}, 0, \text{ respectively for } r = 0, 1, > 1.$$

Hence, by the Künneth formula,

$H^*((S^1)^2, \mathbb{Z}) = \mathbb{Z},\ \mathbb{Z}^2,\ \mathbb{Z},\ 0, ...$

$H^*((S^1)^3, \mathbb{Z}) = \mathbb{Z},\ \mathbb{Z}^3,\ \mathbb{Z}^3,\ \mathbb{Z},\ 0, ...$

$H^*((S^1)^4, \mathbb{Z}) = \mathbb{Z}$, $\mathbb{Z}^4$, $\mathbb{Z}^6$, $\mathbb{Z}^4$, $\mathbb{Z}$, 0,.....
The exponents form a Pascal's triangle:

$$\dim\ H^r((S^1)^n, \mathbb{Z}) = \left(\begin{array}{c} n \\ r \end{array}\right).$$

Recall from linear algebra (e.g., Bourbaki, N., Algèbre Multilinéaire, Hermann, 1958) that if M is a $\mathbb{Z}$-module, then $\bigwedge^r M$ is the quotient of $\otimes^r M$ by the submodule generated by the tensors $a_1 \otimes \cdots \otimes a_r$ in which two of the a_i are equal. Thus,

$$\mathrm{Hom}(\Lambda^r M, \mathbb{Z}) \cong \{\text{alternating forms } \ f\colon M^r \to \mathbb{Z}\}$$

(a multilinear form is alternating if $f(a_1, ..., a_r) = 0$ whenever two a_i's are equal). If M is free and finitely generated, with basis $e_1, ..., e_d$ say, over $\mathbb{Z}$, then

$$\{e_1 \wedge \ldots \wedge e_{i_r} \mid i_1 < i_2 < \cdots < i_r\}$$

is a basis for $\bigwedge^r M$; moreover, if $M^\vee$ is the $\mathbb{Z}$-linear dual $\mathrm{Hom}(M, \mathbb{Z})$ of M, then the pairing

$$\bigwedge^r M^\vee \times \bigwedge^r M \to \mathbb{Z}, \quad (y_1 \wedge \ldots \wedge y_r, x_1 \wedge \ldots \wedge x_r) \mapsto \det(y_i(x_j))$$

realizes each of $\bigwedge^r M^\vee$ and $\bigwedge^r M$ as the $\mathbb{Z}$-linear dual of the other (ibid. §8, Thm 1).

THEOREM 2.3. *Let X be the torus V/L. There are canonical isomorphisms*

$$\bigwedge^r H^1(X, \mathbb{Z}) \to H^r(X, \mathbb{Z}) \to \mathrm{Hom}(\bigwedge^r L, \mathbb{Z}).$$

PROOF. For any manifold X, cup-product (2.2a) defines a map

$$\bigwedge^r H^1(X, \mathbb{Z}) \to H^r(X, \mathbb{Z}),\ a_1 \wedge \ldots \wedge a_r \mapsto a_1 \cup \ldots \cup a_r.$$

Moreover, the Künneth formula (2.2b) shows that, if for all r this map is an isomorphism for X and Y, then the same is true for $X \times Y$. Since this is obviously true for S^1, it is true for $X \approx (S^1)^n$. This defines the first map and proves that it is an isomorphism.

The space $V \approx \mathbb{R}^n$ is simply connected, and $\exp\colon V \to X$ is a covering map — therefore it realizes V as the universal covering space of X, and so $\pi_1(X, x)$ is its group of covering transformations, which is L. Hence (2.2c)

$$H^1(X, \mathbb{Z}) = \mathrm{Hom}(L, \mathbb{Z}).$$

The pairing

$$\bigwedge^r L^\vee \times \bigwedge^r L \to \mathbb{Z},\ (f_1 \wedge \ldots \wedge f_r, e_1 \wedge \ldots \wedge e_r) \mapsto \det\left(f_i(e_j)\right)$$

realizes each group as the $\mathbb{Z}$-linear dual of the other, and $L^\vee = H^1(X, \mathbb{Z})$, and so

$$\bigwedge^r H^1(X, \mathbb{Z}) \overset{\approx}{\to} \mathrm{Hom}(\bigwedge^r L, \mathbb{Z}).$$

$\square$

Riemann forms. By a complex torus, I mean a quotient $X = V/L$ where V is a complex vector space and L is a full lattice in V.

LEMMA 2.4. *Let V be a complex vector space. There is a one-to-one correspondence between the Hermitian forms H on V and the real-valued skew-symmetric forms E on V satisfying the identity $E(iv, iw) = E(v, w)$, namely,*

$$\begin{aligned} E(v,w) &= Im(H(v,w)); \\ H(v,w) &= E(iv,w) + iE(v,w). \end{aligned}$$

PROOF. Easy exercise. □

EXAMPLE 2.5. Consider the torus $\mathbb{C}/\mathbb{Z}+\mathbb{Z}i$. Then

$$E(x+iy, x'+iy') = x'y - xy',\ H(z,z') = z\bar{z}'$$

are a pair as in the lemma.

Let $X = V/L$ be a complex torus of dimension g, and let E be a skew-symmetric form $L \times L \to \mathbb{Z}$. Since $L \otimes \mathbb{R} = V$, we can extend E to a skew-symmetric $\mathbb{R}$-bilinear form $E_{\mathbb{R}} \colon V \times V \to \mathbb{R}$. We call E a *Riemann form* if

(a) $E_{\mathbb{R}}(iv, iw) = E_{\mathbb{R}}(v, w)$;
(b) the associated Hermitian form is positive definite.

Note that (b) implies the E is nondegenerate, but it is says more.

EXERCISE 2.6. If X has dimension 1, then $\Lambda^2 L \approx \mathbb{Z}$, and so there is a skew-symmetric form $E \colon L \times L \to \mathbb{Z}$ such that every other such form is an integral multiple of it. The form E is uniquely determined up to sign, and exactly one of $\pm E$ is a Riemann form.

We shall say that X is *polarizable* if it admits a Riemann form.

REMARK 2.7. Most complex tori are not polarizable. For an example of a 2-dimensional torus $\mathbb{C}^2/L$ with no nonconstant meromorphic functions, see p104 of Siegel 1962 (listed below p15).

THEOREM 2.8. *A complex torus X is of the form $A(\mathbb{C})$ if and only if it is polarizable.*

PROOF. (Brief sketch.) $\Longrightarrow$: Choose an embedding $A \hookrightarrow \mathbb{P}^n$ with n minimal. There exists a hyperplane H in $\mathbb{P}^n$ that doesn't contain the tangent space to any point on $A(\mathbb{C})$. Then $A \cap H$ is a smooth variety of (complex) dimension $g-1$ (easy exercise). It can be "triangulated" by $(2g-2)$-simplices, and so defines a class in

$$H_{2g-2}(A,\mathbb{Z}) \cong H^2(A,\mathbb{Z}) \cong \mathrm{Hom}(\bigwedge^2 L, \mathbb{Z}),$$

and hence a skew-symmetric form on L — this can be shown to be a Riemann form.

$\Longleftarrow$: Given E, it is possible to construct enough functions (in fact quotients of theta functions) on V to give an embedding of X into some projective space. □

We define a category of polarizable complex tori as follows: the objects are polarizable complex tori; if $X = V/L$ and $X' = V'/L'$ are complex tori, then $\mathrm{Hom}(X, X')$ is the set of maps $X \to X'$ defined by a $\mathbb{C}$-linear map $\alpha \colon V \to V'$ mapping L into L'.

(These are in fact all the complex-analytic homomorphisms $X \to X'$). The following theorem makes (2.7) more precise.

THEOREM 2.9. *The functor $A \mapsto A(\mathbb{C})$ is an equivalence from the category of abelian varieties over $\mathbb{C}$ to the category of polarizable tori.*

In more detail this says that $A \mapsto A(\mathbb{C})$ is a functor, every polarizable complex torus is isomorphic to the torus defined by an abelian variety, and

$$\mathrm{Hom}(A, B) = \mathrm{Hom}(A(\mathbb{C}), A'(\mathbb{C})).$$

Thus the category of abelian varieties over $\mathbb{C}$ is essentially the same as that of polarizable complex tori, which can be studied using only (multi-)linear algebra.

An *isogeny* of polarizable tori is a surjective homomorphism with finite kernel. The *degree* of the isogeny is the order of the kernel.

Let $X = V/L$. Then

$$V^* = \{f : V \to \mathbb{C} \mid f(\alpha v) = \bar{\alpha} f(v)\}$$

is a complex vector space of the same dimension as V. Define

$$L^* = \{f \in V^* | \ f(L) \subset \mathbb{Z}\}.$$

Then L^* is a lattice in V^*, and $X^\vee \stackrel{\mathrm{df}}{=} V^*/L^*$ is a polarizable complex torus, called the *dual torus.*

EXERCISE 2.10. If $X = V/L$, then X_m, the subgroup of X of elements killed by m, is $m^{-1}L/L$. Show that there is a canonical pairing

$$X_m \times (X^\vee)_m \to \mathbb{Z}/m\mathbb{Z}.$$

This is the *Weil pairing.*

A Riemann form on E on X defines a homomorphism $\lambda_E : X \to X^\vee$ as follows: let H be the associated Hermitian form, and let λ_E be the map defined by

$$v \mapsto H(v, \cdot) : V \to V^*.$$

Then λ_E is an isogeny, and we call such a map λ_E a *polarization.* The *degree* of the polarization is the order of the kernel. The polarization is said to be *principal* if it is of degree 1.

EXERCISE 2.11. Show that every polarizable tori is isogenous to a principally polarized torus.

A polarizable complex torus is *simple* if it does not contain a polarizable subtorus X', $X' \neq 0, X$.

EXERCISE 2.12. Show that every polarizable torus is isogenous to a direct sum of simple polarizable tori.

Let E be an elliptic curve over $\mathbb{Q}$. Then $\mathrm{End}(E) \otimes \mathbb{Q}$ is either $\mathbb{Q}$ or a quadratic imaginary extension of $\mathbb{Q}$. For a simple polarizable torus, $\mathrm{End}(X) \otimes \mathbb{Q}$ is a division algebra over a field, and the possible pairs arising in this fashion from a simple abelian variety have been classified (mostly by A.A. Albert).

Notes. There is complete, but very concise, treatment of abelian varieties over $\mathbb{C}$ in Chapter I of Mumford 1970, and a more leisurely account in Murty 1993. The classic account is:

> Siegel, C., Analytic Functions of Several Variables, Lectures IAS Fall 1948; reprinted 1962.

Siegel first develops the theory of complex functions in several variables. See also his books, Topics in Complex Function Theory.See also his books, Topics in Complex Function Theory.

3. Rational Maps Into Abelian Varieties

Throughout this section, all varieties will be irreducible.

Rational maps. We first discuss the general theory of rational maps.

Let V and W be varieties over k, and consider pairs (U, φ_U) where U is a dense open subset of V and φ_U is a regular map $U \to W$. Two such pairs (U, φ_U) and $(U', \varphi_{U'})$ are said to be *equivalent* if φ_U and $\varphi_{U'}$ agree on $U \cap U'$. An equivalence class of pairs is called a *rational map* $\varphi\colon V \dashrightarrow W$. A rational map φ is said to be *defined* at a point v of V if $v \in U$ for some $(U, \varphi_U) \in \varphi$. The set U_1 of v at which φ is defined is open, and there is a regular map $\varphi_1\colon U_1 \to W$ such that $(U_1, \varphi_1) \in \varphi$ — clearly, $U_1 = \cup_{(U,\varphi_U)\in\varphi} U$ and we can define φ_1 to be the regular map such that $\varphi_1|U = \varphi_U$ for all $(U, \varphi_U) \in \varphi$.

The following examples illustrate the major reasons why a rational map $V \dashrightarrow W$ may not extend to a regular map on the whole of V.

(a) Let W be a proper open subset of V; then the rational map $V \dashrightarrow W$ represented by $\mathrm{id}\colon W \to W$ will not extend to V. To obviate this problem, we should take W to be complete.

(b) Let C be the cuspidal plane cubic curve $Y^2 = X^3$. There is a regular map $\mathbb{A}^1 \to C$, $t \mapsto (t^2, t^3)$, which defines an isomorphism $\mathbb{A}^1 \smallsetminus \{0\} \to C \smallsetminus \{0\}$. The inverse of this isomorphism represents a rational map $C \dashrightarrow \mathbb{A}^1$ which does not extend to a regular map because the map on function fields doesn't send the local ring at $0 \in \mathbb{A}^1$ into the local ring at $0 \in C$. Roughly speaking, a regular map can only map a singularity to a worse singularity. To obviate this problem, we should take V to be nonsingular (in fact, nonsingular is no more helpful than normal).

(c) Let P be a point on a nonsingular surface V. It is possible to "blow-up" P and obtain a surface W and a morphism $\alpha\colon W \to V$ which restricts to an isomorphism $W \smallsetminus \alpha^{-1}(P) \to V \smallsetminus P$ but for which $\alpha^{-1}(P)$ is the projective line of "directions" through P. The inverse of the restriction of α to $W \smallsetminus \alpha^{-1}(P)$ represents a rational map $V \dashrightarrow W$ that does not extend to all V, even when V and W are complete — roughly speaking, there is no preferred direction through P, and hence no obvious choice for the image of P.

In view of these examples, the next theorem is best possible.

Theorem 3.1. *A rational map $\varphi\colon V \dashrightarrow W$ 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. (Sketch). Assume first that V is a curve. Thus we are given a nonsingular curve C and a regular map $\varphi\colon U \to W$ on an open subset of C which we want to extend to C. Consider the maps

$$\begin{array}{rcl} U & \to & C \times W \to C \\ u & \mapsto & (u, \varphi(u)),\ (c, w) \mapsto c. \end{array}$$

Let U' be the image of U in $C \times W$, and let Z be its closure. The image of Z in C is closed (because W is complete), and contains U (the composite $U \to C$ is the given inclusion), and so Z maps onto C. The maps $U \to U' \to U$ are isomorphisms, and it follows easily that $Z \to C$ is an isomorphism (this uses that C is nonsingular). Now the restriction of the projection map $C \times W \to W$ to $Z(\approx C)$ is the extension of φ to C we are seeking.

The general case can be reduced to the case of a curve. [For the experts on scheme theory, let U be the largest subset on which φ is defined, and suppose that $V - U$ has codimension 1. Then there is a prime divisor Z in $V - U$. Its associated local ring is a discrete valuation ring $\mathcal{O}_Z$ with field of fractions $k(V)$. The map φ defines a morphism of schemes Spec $k(V) \to W$, which the above argument shows extends to a morphism Spec $\mathcal{O}_Z \to W$, and this contradicts the fact that Z lies outside the largest set of definition for φ.] □

Rational maps into abelian varieties.

THEOREM 3.2. *A rational map $\alpha\colon V \dashrightarrow A$ from a nonsingular variety to an abelian variety is defined on the whole of V.*

PROOF. Combine Theorem 3.1 with the next lemma. □

LEMMA 3.3. *Let $\varphi\colon V \dashrightarrow G$ be a rational map from a nonsingular variety to a group variety. Then either φ is defined on all of V or the points where it is not defined form a closed subset of pure codimension 1 in V (i.e., a union of prime divisors).*

PROOF. Define a rational map

$$\Phi\colon V \times V \dashrightarrow G,\ (x, y) \mapsto \varphi(x) \cdot \varphi(y)^{-1}.$$

More precisely, if (U, φ_U) represents φ, then Φ is the rational map represented by

$$U \times U \overset{\varphi_U \times \varphi_U}{\to} G \times G \overset{\mathrm{id} \times \mathrm{inv}}{\to} G \overset{m}{\to} G.$$

Clearly Φ is defined at a diagonal point (x, x) if φ is defined at x, and then $\Phi(x, x) = e$. Conversely, if Φ is defined at (x, x), then it is defined on an open neighbourhood of (x, x); in particular, there will be an open subset U of V such that Φ is defined on $\{x\} \times U$. After possible replacing U by a smaller open subset (not necessarily containing x), φ will be defined on U. For $u \in U$, the formula

$$\varphi(x) = \Phi(x, u) \cdot \varphi(u)$$

defines φ at x. Thus φ is defined at x if and only if Φ is defined at (x, x).

The rational map Φ defines a map

$$\varphi^*\colon \mathcal{O}_{G,e} \to k(V \times V).$$

Since Φ sends (x,x) to e if it is defined there, it follows that Φ is defined at (x,x) if and only if

$$\mathrm{Im}(\mathcal{O}_{G,e}) \subset \mathcal{O}_{V\times V,(x,x)}.$$

Now $V\times V$ is nonsingular, and so we have a good theory of divisors (AG §10). For a rational function f on $V\times V$, write

$$\mathrm{div}(f) = \mathrm{div}(f)_0 - \mathrm{div}(f)_\infty,$$

with $\mathrm{div}(f)_0$ and $\mathrm{div}(f)_\infty$ effective divisors — note that $\mathrm{div}(f)_\infty = \mathrm{div}(f^{-1})_0$. Then

$$\mathcal{O}_{V\times V,(x,x)} = \{f \in k(V\times V) \mid \ \mathrm{div}(f)_\infty \text{ does not contain } (x,x)\} \cup \{0\}.$$

Suppose Φ is not defined at x. Then for some $f \in Im(\varphi^*)$, $(x,x) \in \mathrm{div}(f)_\infty$, and clearly Φ is not defined at the points $(y,y) \in \Delta \cap \mathrm{div}(f)_\infty$. This is a subset of pure codimension one in Δ (AG 7.2), and when we identify it with a subset of V, it is a subset of V of codimension one passing through x on which φ is not defined. □

THEOREM 3.4. *Let $\alpha\colon V\times W \to A$ be a morphism from a product of nonsingular varieties into an abelian variety, and assume that $V\times W$ is geometrically irreducible. If*

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

for some $a_0 \in A(k)$, $v_0 \in V(k)$, $w_0 \in W(k)$, then

$$\alpha(V\times W) = \{a_0\}.$$

If V (or W) is complete, this is a special case of the Rigidity Theorem (Theorem 1.1). For the general case, we need two lemmas.

LEMMA 3.5. (a) *Every nonsingular curve V can be realized as an open subset of a complete nonsingular curve C.*
(b) *Let C be a curve; then there is a nonsingular curve C' and a regular map $C' \to C$ that is an isomorphism over the set of nonsingular points of C.*

PROOF. (Sketch) (a) Let $K = k(V)$. Take C to be the set of discrete valuation rings in K containing k with the topology for which the finite sets and the whole set are closed. For each open subset U of C, define

$$\Gamma(U,\mathcal{O}_C) = \cap\{R \mid R \in C\}.$$

The ringed space $(C,\mathcal{O}_C)$ is a nonsingular curve, and the map $V\to C$ sending a point x of V to $\mathcal{O}_{V.x}$ is regular.

(b) Take C' to be the normalization of C. □

LEMMA 3.6. *Let V be an irreducible variety over an algebraically closed field, and let P be a nonsingular point on V. Then the union of the irreducible curves passing through P and nonsingular at P is dense in V.*

PROOF. By induction, it suffices to show that the union of the irreducible subvarieties of codimension 1 passing P and nonsingular at P is dense in V. We can assume V to be affine, and that V is embedded in affine space. For H a hyperplane passing through P but not containing $\mathrm{Tgt}_P(V)$, $V\cap H$ is nonsingular at P. Let V_H be the irreducible component of $V\cap H$ passing through P, regarded as a subvariety of V, and let Z be a closed subset of V containing all V_H. Let $C_P(Z)$ be the tangent cone to Z at P (see AG §4). Clearly,

$$\mathrm{Tgt}_P(V) \cap H = \mathrm{Tgt}_P(V_H) = C_P(V_H) \subset C_P(Z) \subset C_P(V) = \mathrm{Tgt}_P(V),$$

and it follows that $C_P(Z) = \mathrm{Tgt}_P(V)$. As $\dim C_P(Z) = \dim(Z)$ (ibid. p79), this implies that $Z = V$ (ibid. 1.22). □

PROOF. (of 3.4). Clearly we can assume k to be algebraically closed. Consider first the case that V has dimension 1. From the (3.5), we know that V can be embedded into a nonsingular complete curve C, and (3.2) shows that α extends to a map $\bar{\alpha}\colon C \times W \to A$. Now the Rigidity Theorem (1.1) shows that $\bar{\alpha}$ 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 $C' \to C$ be the normalization of C. By composition, α defines a morphism $C' \times W \to A$, which the preceding argument shows to be constant. Therefore $\alpha(C \times W) = \{a_0\}$, and Lemma 3.6 completes the proof. □

COROLLARY 3.7. *Every rational map $\alpha\colon G \dashrightarrow A$ from a group variety to an abelian variety is the composite of a homomorphism $h\colon G \to A$ with a translation.*

PROOF. Theorem 3.2 shows that α is a regular map. The rest of the proof is the same as that of Corollary 1.2. □

Abelian varieties up to birational equivalence. A rational map $\varphi\colon V \dashrightarrow W$ is *dominating* if $\mathrm{Im}(\varphi_U)$ is dense in W for one (hence all) representatives (U, φ_U) of φ. Then φ defines a homomorphism $k(W) \to k(V)$, and every such homomorphism arises from a (unique) dominating rational map (exercise!).

A rational map φ is *birational* if the corresponding homomorphism $k(W) \to k(V)$ is an isomorphism. Equivalently, if there is a rational map $\psi\colon W \to V$ such that $\varphi \circ \psi$ and $\psi \circ \varphi$ are both the identity map wherever they are defined. Two varieties V and W are *birationally equivalent* if there exists a birational map $V \dashrightarrow W$; equivalently, if $k(V) \approx k(W)$.

In general, two varieties can be birationally equivalent without being isomorphic (see the start of this section for examples). In fact, every variety (even complete and nonsingular) of dimension > 1 will be birationally equivalent to many nonisomorphic varieties. However, Theorem 3.1 shows that two complete nonsingular curves that are birationally equivalent will be isomorphic. The same is true of abelian varieties.

THEOREM 3.8. *If two abelian varieties are birationally equivalent, then they are isomorphic (as abelian varieties).*

PROOF. Let A and B be the abelian varieties. A rational map $\varphi\colon A \dashrightarrow B$ extends to a regular map $A \to B$ (by 3.2). If φ is birational, its inverse ψ also extends to a regular map, and the composites $\varphi \circ \psi$ and $\psi \circ \varphi$ will be identity maps because they are on open sets. Hence there is an isomorphism $\alpha\colon A \to B$ of algebraic varieties. After composing it with a translation, it will map 0 to 0, and then Corollary 1.2 shows that it preserves the group structure. □

LEMMA 3.9. *Every rational map $\mathbb{A}^1 \dashrightarrow A$ is constant.*

PROOF. According to (3.2), α extends to a regular map on the whole of $\mathbb{A}^1$. After composing α with a translation, we may suppose that $\alpha(0) = 0$. Then α is a homomorphism,

$$\alpha(x + y) = \alpha(x) + \alpha(y), \text{ all } x, y \in \mathbb{A}^1(k^{\mathrm{al}}) = k^{\mathrm{al}}.$$

But $\mathbb{A}^1 - \{0\}$ is also a group variety, and similarly,

$$\alpha(xy) = \alpha(x) + \alpha(y) + c, \text{ all } x, y \in \mathbb{A}^1(k^{\mathrm{al}}) = k^{\mathrm{al}}.$$

This is absurd, unless α is constant. □

A variety V over an algebraically closed field is said to be *unirational* if there is a dominating rational map $\mathbb{A}^n \dashrightarrow V$ with $n = \dim V$; equivalently, if $k(V)$ can be embedded into $k(X_1, ..., X_n)$ (pure transcendental extension of k). A variety V over an arbitrary field k is said to be *unirational* if $V_{k^{\mathrm{al}}}$ is unirational.

PROPOSITION 3.10. *Every rational map $\alpha\colon V \to A$ from a unirational variety to an abelian variety is constant.*

PROOF. We may assume k to be algebraically closed. By assumption there is a rational map $\mathbb{A}^n \dashrightarrow V$ with dense image, and the composite of this with α extends to a morphism $\beta\colon \mathbb{P}^1 \times ... \times \mathbb{P}^1 \to A$. An induction argument, starting from Corollary 1.5, shows that there are regular maps $\beta_i\colon \mathbb{P}^1 \to A$ such that $\beta(x_1, ..., x_d) = \Sigma\, \beta_i(x_i)$, and the lemma shows that each β_i is constant. □

4. The Theorem of the Cube.

We refer the reader to (AG §11) for the basic theory of invertible sheaves. For a variety V, $\mathrm{Pic}(V)$ is the group of isomorphism classes of invertible sheaves.

Statement and Applications. Roughly speaking, the theorem of the cube says that an invertible sheaf on the product of three complete varieties is trivial if it becomes trivial when restricted to each of the three "coordinate faces".

THEOREM 4.1 (Theorem of the cube). *Let U, V, W be complete geometrically irreducible varieties over k, and let $u_0 \in U(k)$, $v_0 \in V(k)$, $w_0 \in W(k)$ be base points. Then an invertible sheaf $\mathcal{L}$ on $U \times V \times W$ is trivial if its restrictions to*

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

are all trivial.

We defer the proof until later in this section.

COROLLARY 4.2. *Let A be an abelian variety, and let $p_i\colon A \times A \times A \to A$ be the projection onto the i^{th} factor (e.g., $p_2(x, y, z) = y$), let $p_{ij} = p_i + p_j$ (e.g., $p_{23}(x, y, z) = y + z$), and let $p_{123} = p_1 + p_2 + p_3$ (so that $p_{123}(x, y, z) = x + y + z$). For any invertible sheaf $\mathcal{L}$ on A, the sheaf*

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

on A is trivial.

PROOF. Let m, p, q be the maps $A\times A\to A$ sending (x,y) to $x+y$, x, y respectively. The composites of

$$(x,y)\mapsto(x,y,0)\colon A\times A\to A\times A\times A$$

with $p_{123}, p_{12}, p_{23}, \ldots, p_2, p_3$ are respectively $m, m, q, \ldots, q, 0$. Therefore, the restriction of the sheaf in question to $A\times A\times\{0\}$ ($\cong A\times A$) is

$$m^*\mathcal{L}\otimes m^*\mathcal{L}^{-1}\otimes q^*\mathcal{L}^{-1}\otimes p^*\mathcal{L}^{-1}\otimes p^*\mathcal{L}\otimes q^*\mathcal{L}\otimes\mathcal{O}_A,$$

which is obviously trivial. Similarly, its restrictions to $A\times\{0\}\times A$ and $A\times A\times\{0\}$ are both trivial, and so the theorem of the cube implies that it is trivial. □

COROLLARY 4.3. *Let f, g, h be regular maps from a variety V into an abelian variety A. For any invertible sheaf $\mathcal{L}$ on A,*

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

is trivial.

PROOF. The sheaf in question is the inverse image of the sheaf in (4.2) by the map

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

□

For an integer n, let $n_A\colon A\to A$ be the map sending an element of A to its n^{th} multiple, i.e., $n_A(a)=a+a+\cdots+a$ (n summands). This is clearly a regular map; for example, 2_A is the composite

$$A\xrightarrow{\Delta}A\times A\xrightarrow{\text{mult}}A.$$

The map $(-1)_A$ sends a to $-a$ (it is the map denoted by inv at the start of §1).

COROLLARY 4.4. *For any invertible sheaf $\mathcal{L}$ on an abelian variety A,*

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

In particular,

$$\begin{aligned} n_A^*\mathcal{L} &\approx \mathcal{L}^{n^2} \text{ if } \mathcal{L} \text{ is symmetric, i.e., } (-1)_A^*\mathcal{L}\approx\mathcal{L}.\\ n_A^*\mathcal{L} &\approx \mathcal{L}^{n} \text{ if } \mathcal{L} \text{ is antisymmetric, i.e., } (-1)_A^*\mathcal{L}\approx\mathcal{L}^{-1}.\end{aligned}$$

PROOF. On applying the last corollary to the maps n_A, 1_A, $(-1)_A\colon A\to A$, we find that

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

is trivial. In other words

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

We use this to prove the isomorphism by induction on n. For $n=1$, the statement is obvious. Take $n=1$ in (*); then

$$(2)_A^*\mathcal{L}\approx\mathcal{L}^2\otimes\mathcal{L}\otimes(-1)_A^*\mathcal{L}\approx\mathcal{L}^3\otimes(-1)_A^*\mathcal{L}$$

as predicted by the lemma. When we assume the Corollary for n, (*) proves it for $n+1$, because

$$\begin{aligned}[(n+1)^2+(n+1)]/2 &= (n^2+n)-[(n-1)^2+(n-1)]/2+1\\ [(n+1)^2-(n+1)]/2 &= (n^2-n)-[(n-1)^2-(n-1)]/2+1.\end{aligned}$$

□

THEOREM 4.5 (Theorem of the Square). *For any invertible sheaf $\mathcal{L}$ on A and points $a, b \in A(k)$,*

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

PROOF. On applying (4.3) to the maps $x\mapsto x$, $x\mapsto a$, $x\mapsto b$, $A\to A$, we find that

$$t_{a+b}^*\mathcal{L}\otimes t_a^*\mathcal{L}^{-1}\otimes t_b^*\mathcal{L}^{-1}\otimes\mathcal{L}$$

is trivial. □

REMARK 4.6. When we tensor the isomorphism in (4.5) with $\mathcal{L}^{-2}$, we find that

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

In other words, the map

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

is a homorphism. Thus, if $a_1+a_2+\cdots+a_n=0$ (in $A(k)$), then

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

REMARK 4.7. We can restate the above results in terms of divisors. For a divisor D on A, write D_a for the translate $D+a$ of D. Unfortunately, $\mathcal{L}(D_a)=t_{-a}^*\mathcal{L}(D)$, but the minus sign doesn't matter much because $a\mapsto -a$ is a homomorphism[5] (that's what it means to be abelian!). Therefore, for any divisor D on A, the map

$$a\mapsto[D_a-D]\colon A(k)\to\mathrm{Pic}(A)$$

is a homomorphism, where $[*]$ denotes the linear equivalence class of $*$. Hence, if $a_1+a_2+\cdots+a_n=0$, then $\sum D_{a_i}\sim nD$.

For example, let A be an elliptic curve, and let P_0 be the zero element of A. Let D_0 be P_0 regarded as a divisor of degree 1 on A. For any point P on A, the translate D_P of D_0 by P is just P regarded as a divisor (i.e., $D_0+P=D_P$). Therefore, in this case, the last map is

$$P\mapsto[P-P_0]\colon A(k)\to\mathrm{Pic}(A)$$

as in EC 4.7 or Silverman 1986, III 3.4d.

[5]In fact, in this version of the notes, we ignore the sign. Thus, there are some sign differences between when we express things in terms of divisors and in terms of invertible sheaves.

Preliminaries for the proof of the theorem of the cube. We list some facts that are required for the proof of the theorem of the cube.

4.8. Let $\alpha\colon M \to N$ be a homomorphism of free modules of rank 1 over a commutative ring R. Choose bases e and f for M and N, and set $\alpha(e) = rf$, $r \in R$. If α is surjective, then $r \in R^{\times}$, and so α is bijective. Consequently, a surjective homomorphism $\mathcal{L} \to \mathcal{L}'$ of invertible sheaves is an isomorphism (because it is on stalks).

4.9. Let V be a variety over k, and consider the structure map $\alpha\colon V \to \operatorname{Specm}\ k$. Because $\operatorname{Specm} k$ consists of a single point, to give a coherent sheaf on it the same as to give a finite-dimensional vector space over k. For a sheaf of $\mathcal{O}_V$-modules $\mathcal{M}$ on V, $\alpha_*\mathcal{M} = \Gamma(V, \mathcal{M})$. For a vector space M over k, $\alpha^*M = \mathcal{O}_V \otimes_k M$; for example, if $M = ke_1 \oplus \cdots \oplus ke_n$, then $\alpha^*M = \mathcal{O}_V e_1 \oplus \cdots \oplus \mathcal{O}_V e_n$.

4.10. Consider a map $R \to S$ of commutative rings. For any S-module M, there is a natural S-linear map

$$S \otimes_R M \to M,\ s \otimes m \mapsto sm.$$

Similarly, for any regular map $\alpha\colon W \to V$ and coherent $\mathcal{O}_W$-module $\mathcal{M}$, there is a canonical map $\alpha^*\alpha_*\mathcal{M} \to \mathcal{M}$. For the structure map $\alpha\colon V \to \operatorname{Specm}\ k$, this is the map

$$\mathcal{O}_V \otimes_k \Gamma(V, \mathcal{M}) \to \mathcal{M},\ f \otimes m \mapsto f \otimes (m|U),\ f \in \Gamma(U, \mathcal{O}_V).$$

4.11. Consider a homomorphism $\alpha\colon M \to N$ of R-modules. For each maximal ideal $\mathfrak{m}$ in R, α induces a homomorphism $\alpha(\mathfrak{m})\colon M/\mathfrak{m}M \to N/\mathfrak{m}N$ of $R/\mathfrak{m}$-vector spaces. If $\alpha(\mathfrak{m})$ is surjective, then the homomorphism of $R_{\mathfrak{m}}$-modules $\alpha_{\mathfrak{m}}\colon M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is surjective (by Nakayama's lemma).

Consider a homomorphism $\alpha\colon \mathcal{M} \to \mathcal{N}$ of coherent $\mathcal{O}_V$-modules. For each $v \in V$, this induces a homomorphism $\alpha(v)\colon \mathcal{M}(v) \to \mathcal{N}(v)$ of $k(v)$-vector spaces, and if these are surjective for all v, then Nakayama's lemma shows that α is surjective. If further $\mathcal{M}$ and $\mathcal{N}$ are invertible sheaves, then (5.1) shows that α is an isomorphism.

4.12. Let V be a complete variety over k, and let $\mathcal{M}$ be a locally free sheaf of $\mathcal{O}_V$-modules. For any field K containing k, $\mathcal{M}$ defines a sheaf of $\mathcal{O}_{V_K}$-modules $\mathcal{M}'$ on V_K in an obvious way, and

$$\Gamma(V_K, \mathcal{M}') = \Gamma(V, \mathcal{M}) \otimes_k K.$$

If D is a divisor on a smooth complete variety V, and D' is the inverse image of D on V_K, then

$$L(D') = L(D) \otimes_k K.$$

Here

$$L(D) = \{f \in k(V)^{\times} \mid divv(f) + D \geq 0\} = \Gamma(V, \mathcal{L}(D))$$

(AG p146).

4.13. Let V be a complete variety, and let $\mathcal{L}$ be a locally free sheaf on V. If $\mathcal{L}$ becomes trivial on V_K for some field $K \supset k$, then it is trivial on V.

PROOF. Recall (AG 11.3) that an invertible sheaf on a complete variety is trivial if and only if it and its dual have nonzero global sections. Thus the statement follows from (4.11). □

4.14. Consider a regular map $V \to T$ of varieties over k. For any $t \in T$, the fibre of the map over t is a variety over the residue field $k(t)$:

$$\begin{array}{ccccc} V & \overset{j_t}{\leftarrow} & V_t & \overset{\mathrm{df}}{=} & V \times_k \mathrm{Specm}(k(t)) \\ \downarrow \varphi & & \downarrow \varphi_t & & \\ T & \overset{i_t}{\leftarrow} & t & = & \mathrm{Specm}(k(t)). \end{array}$$

If k is algebraically closed, then $k(t) = k$. We can think of the map $V \to T$ as a family of varieties (V_t) parametrized by th e points of T.

Now let V and T be varieties over k, and consider the projection map $q\colon V \times T \to T$. Thus we have the "constant" family of varieties: the fibre $V_t = V_{k(t)}$ is the variety over $k(t)$ obtained from V by extending scalars. Let $\mathcal{L}$ be an invertible sheaf on $V \times T$. For each $t \in T$, we obtain an invertible sheaf $\mathcal{L}_t$ on V_t by pulling back by the map $V_t \to V \times T$. We regard $\mathcal{L}$ as a family of invertible sheaves $(\mathcal{L}_t)$ on "V" parametrized by the points of T. When k is algebraically closed, $V_t = V$, and so this is literally true.

4.15. Let $\alpha\colon V \to T$ be a proper map — for example, α could be the projection map $q\colon W \times T \to T$ where W is a complete variety (see AG 5.25; AG p107). For any coherent sheaf $\mathcal{M}$ on V, $\alpha_*\mathcal{M}$ is a coherent sheaf on T.

Now consider an invertible sheaf $\mathcal{L}$ on $V \times T$, and assume that V is complete so that $q_*\mathcal{L}$ is coherent. The function

$$t \mapsto \dim_{k(t)} \Gamma(V_t, \mathcal{L}_t)$$

is upper semicontinuous (it jumps on closed subsets). If it is constant, say equal to n, then $q_*\mathcal{L}$ is locally free of rank n, and the canonical map $(q_*\mathcal{L})(t) \to \Gamma(V_t, \mathcal{L}_t)$ is an isomorphism.

PROOF. It is quite difficult to prove that $q_*\mathcal{L}$ is coherent — for a proof in the language of schemes when V is projective, see Hartshorne II.5.19. [We know that for any complete variety V over k, $\Gamma(V, \mathcal{O}_V) = k$, which is certainly a finite-dimensional vector space. When we allow a finite number of poles of bounded order, we still get a finite-dimensional vector space, i.e., for any divisor D on V, $dim_k\ L(D)$ is finite. When V is nonsingular, this says that $\Gamma(V, \mathcal{L})$ is finite-dimensional for any invertible sheaf $\mathcal{L}$ on V.]

Note that, if we assumed that $(q_*\mathcal{L})(t)$ had constant dimension then it would follow from (AG 11.1) that $q_*\mathcal{L}$ was locally free of rank n. However, our assumption that $\Gamma(V_t, \mathcal{L}_t)$ has constant dimension is easier to check, and more useful.

We omit the proof. See Mumford 1970, II.5. □

The seesaw principle. If an invertible sheaf $\mathcal{L}$ on $V \times T$ is of the form $q^*\mathcal{N}$ for some invertible sheaf $\mathcal{N}$ on T, then $\mathcal{L}_t$ is the inverse image of the restriction of $\mathcal{N}$ to t, and is therefore trivial. There is a converse to this statement.

Theorem 4.16. *Let V and T be varieties over k with V complete, and let $\mathcal{L}$ be an invertible sheaf on $V \times T$. If $\mathcal{L}_t$ is trivial for all $t \in T$, then there exists an invertible sheaf $\mathcal{N}$ on T such that $\mathcal{L} \approx q^*\mathcal{N}$.*

Proof. By assumption, $\mathcal{L}_t$ is trivial for all $t \in T$, and so $\Gamma(V_t, \mathcal{L}_t) \approx \Gamma(V_t, \mathcal{O}_V) = k(t)$. Therefore (4.14) shows that the sheaf $\mathcal{N} \overset{\mathrm{df}}{=} q_*(\mathcal{L})$ is invertible. Consider the canonical map (4.9)

$$\alpha\colon q^*\mathcal{N} = q^*q_*\mathcal{L} \to \mathcal{L}.$$

Look at this on the fibre $V_t \to \mathrm{Specm}\ k(t)$. As $\mathcal{L}_t \approx \mathcal{O}_{V_t}$, the restriction of α to V_t is isomorphic to the natural map (see 4.8, 4.9) $\alpha_t\colon \mathcal{O}_{V_t} \otimes_{k(t)} \Gamma(V_t, \mathcal{O}_{V_t}) \to \mathcal{O}_{V_t}$, which is an isomorphism. In particular, for any point in $w \in V_t$, the map

$$\alpha(w)\colon (q^*\mathcal{N})(w) \to \mathcal{L}(w)$$

of sheaves on w is an isomorphism. Now (4.10) shows that α is an isomorphism. □

Corollary 4.17. *Let V and T be varieties over k with V complete, and let $\mathcal{L}$ and $\mathcal{M}$ be invertible sheaves on $V \times T$. If $\mathcal{L}_t \approx \mathcal{M}_t$ for all $t \in T$, then there exists an invertible sheaf $\mathcal{N}$ on T such that $\mathcal{L} \approx \mathcal{M} \otimes q^*\mathcal{N}$.*

Proof. Apply (4.15) to $\mathcal{L} \otimes \mathcal{M}^{-1}$. □

Corollary 4.18 (Seesaw principle). *Suppose that, in addition to the hypotheses of (4.16), $\mathcal{L}_v \approx \mathcal{M}_v$ for at least one $v \in V(k)$. Then $\mathcal{L} \approx \mathcal{M}$.*

Proof. The previous corollary shows that $\mathcal{L} \approx \mathcal{M} \otimes q^*\mathcal{N}$ for some $\mathcal{N}$ on T. On pulling back by the map $t \mapsto (v, t)\colon T \hookrightarrow V \times T$, we obtain an isomorphism $\mathcal{L}_v \approx \mathcal{M}_v \otimes q^*\mathcal{N}_v$. As $\mathcal{L}_v \approx \mathcal{M}_v$ and $(q^*\mathcal{N})_v = \mathcal{N}$, this shows that $\mathcal{N}$ is trivial. □

The next result shows that the triviality of $\mathcal{L}_t$ in the theorem needs only to be checked for t in some dense subset of T.

Proposition 4.19. *Let V be a complete variety, and let $\mathcal{L}$ be an invertible sheaf on $V \times T$. Then $\{t \in T \mid \mathcal{L}_t \text{ is trivial}\}$ is closed in T.*

Proof. It is the intersection of $\mathrm{Supp}(q_*\mathcal{L})$ and $\mathrm{Supp}(q_*\mathcal{L}^\vee)$ (see AG p143 and 11.3). □

Proof of the theorem of the cube. After (4.12), we may assume that the ground field k is algebraically closed. Because $\mathcal{L}|U \times V \times \{w_0\}$ is trivial, the Seesaw Principle and Proposition 4.18 show that it suffices to prove that $\mathcal{L}|z \times W$ is trivial for a dense set of z in $U \times V$. The next lemma shows that we can assume that V is a curve.

Lemma 4.20. *Let P and Q be points of an irreducible variety over an algebraically closed field k. Then there is an irreducible curve C on V passing through both P and Q.*

Proof. If V itself is a curve or $P = Q$, then there is nothing to prove, and so we assume that $\dim\ V > 1$ and $P \neq Q$. Chow's lemma (Mumford, Introduction to Algebraic Geometry, 1966, p115) says the following: For any complete variety V, there exists a projective variety W and a surjective birational morphism $W \to V$.

If we can prove the lemma for W, then clearly we obtain it for V, and so we may assume V to be projective.

By induction on dim V, it suffices to find a proper closed irreducible subvariety Z of V passing through P and Q. Let $\varphi\colon V^* \to V$ be the blow-up of V at $\{P, Q\}$. Thus the restriction of φ to $V^* \setminus \varphi^{-1}\{P, Q\}$ is an isomorphism onto $V \setminus \{P, Q\}$, and the inverse images of P and Q are disjoint divisors on V^*. The variety V^* is again projective — we choose a closed immersion $V^* \hookrightarrow \mathbb{P}^n$ with n minimal. Bertini's Theorem[6] states that, for a general hyperplane H in $\mathbb{P}^n$, $H \cap V^*$ will be irreducible — here "general" means "for all hyperplanes in an open subset of the dual projective space". Choose such an H. Then

$$\dim H \cap V^* + \dim \varphi^{-1}(P) = 2 \dim V - 2 \geq \dim V,$$

and so $(H \cap V^*) \cap \varphi^{-1}(P)$ is nonempty (AG 7.23). Similarly, $(H \cap V^*) \cap \varphi^{-1}(Q)$ is nonempty, and so the image of $H \cap V^*$ in V is a proper closed irreducible subvariety of V passing through P and Q. □

Thus we can now assume that V is a complete curve, and (by passing to its normalization) a complete nonsingular curve. Now the proof requires nothing more than what we have proved already and the Riemann-Roch theorem for a curve, and so should have been included in the notes (Mumford, Abelian Varieties, p57-58).

Restatement in terms of divisors. We can restate the above results in terms of divisors. Let V and T be nonsingular varieties over k with V complete, and let D be a divisor on $V \times T$. There is an open subset of $t \in T$ for which, for each prime divisor Z occurring in D, $Z \cap V_t$ has codimension one in V_t, and, for such t, intersection theory defines a divisor $D_t \stackrel{\text{df}}{=} D \cdot V_t$. If $D_t \sim D_0$ (a constant divisor on V) for all t in some open subset of T, then

$$D \sim D_0 \times T + V \times D'$$

for some divisor D' on T. (This is the original seesaw principle — see Lang p241).

Let V and W be complete varieties. A *divisorial correspondence* between V and W is a divisor D on $V \times W$. A divisorial correspondence is said to be *trivial* if it is of the form $V \times D + D' \times W$ where D and D' are divisors on V and W. The seesaw principal gives a criterion for triviality.

5. Abelian Varieties are Projective

Some history. We defined an abelian variety to be a complete group variety, and in this section we prove that it is projective. Of course, we could have avoided this problem by simply defining an abelian variety to be projective, but this would be historically incorrect.

In 1940 Weil announced the proof of the Riemann hypothesis for curves over finite fields, based on a theory of Jacobian varieties of curves over finite fields that did

[6]Jouanolou, J-P., Théorèmes de Bertini et Applications, Birkhäuser, 1983, 6.3; also Grothendieck's EGA5.

not at the time exist[7] . Weil developed the theory of abelian varieties and Jacobian varieties over fields other than $\mathbb{C}$ in the 1940's. At the time he couldn't prove that his Jacobian varieties were projective. This forced him to introduce the notion of an "abstract" variety, i.e., a variety that is not embedded in projective space, and to completely rewrite the foundations of algebraic geometry. In particular, he had to develop a new intersection theory since the then existing theory used that the variety was embedded in projective space. In 1946 he published his "Foundations of Algebraic Geometry", and in 1948 his two books on abelian varieties and Jacobian varieties in which he proved the Riemann hypothesis for curves and abelian varieties.

For me, his work during these years is one of the great achievements of twentieth century mathematics, but its repercussions for mathematics were not all good. In his foundations he made little use of commutative algebra and none of sheaf theory. Beginning in about 1960 Grothendieck completely rewrote the foundations of algebraic geometry in a way so different from that of Weil that a generation of mathematicians who had learnt algebraic geometry from Weil's Foundations found that they had to learn the subject all over again if they wanted to stay current — many never did.

About the same time as Weil, Zariski was also rewriting the foundations of algebraic geometry, but he based his approach on commutative algebra, which leads very naturally into Grothendieck's approach. Unfortunately, Zariski did not complete his book on the foundations of algebraic geometry, but only (with the help of Samuel) his volumes on Commutative Algebra ("the child of an unborn parent").

Barsotti (1953), Matsusaka (1953), and Weil (1957) proved that abelian varieties are projective. Here we present Weil's proof.

Embedding varieties in projective space. For simplicity, in this subsection, we assume k to be algebraically closed. Let V be a complete nonsingular variety over k. A nonempty linear equivalence class of effective divisors on V is called a *complete linear system.* Thus, if $\mathfrak{d}$ is a complete linear system and $D_0 \in \mathfrak{d}$, then $\mathfrak{d}$ consists of all the effective divisors of the form

$$D_0 + \operatorname{div}(f),\ f \in k(V)^\times,$$

i.e.,

$$\mathfrak{d} = \{D_0 + \operatorname{div}(f) \mid f \in L(D_0)\}.$$

For any subspace $W \subset L(D_0)$,

$$\{D_0 + \operatorname{div}(f) \mid f \in W\}$$

is called a *linear system.*

For example, if V is a closed subvariety of $\mathbb{P}^n$, then

$$\{V \cap H \mid H \text{ a hyperplane in } \mathbb{P}^n\}$$

is a linear system. Conversely, we shall associate with a complete linear system on V a rational map $V \dashrightarrow \mathbb{P}^n$, and we shall find conditions on the linear system sufficient to ensure that the map identifies V with a closed subvariety of $\mathbb{P}^n$.

[7]At the time, April 1940, Weil was in a military prison at Rouen as the result of "un différend avec les autorités françaises au sujet de mes "obligations" militaires". Weil said "En d'autres circonstances, une publication m'aurait paru bien prématurée. Mais, en avril 1940, pouvait-on se croire assuré du lendemain?"

Let D_0 be a divisor in $\mathfrak{d}$, and let $f_0, f_1, \dots, f_n$ be a basis for $L(D_0)$. There is a rational map

$$P \mapsto (f_0(P) : f_1(P) : \dots : f_n(P)) \colon V \dashrightarrow \mathbb{P}^n.$$

It is defined at P provided no f_i has a pole at P and at least one f_i is nonzero at P — this is an open set of V.

When we change the basis, we only change the map by a projective linear transformation. When we replace D_0 by a linearly equivalent divisor, say by $D = D_0 + \mathrm{div}(f)$, then $f_0/f, \dots, f_n/f$ will be a basis for $L(D)$, and it defines the same rational map as D. Thus, up to a projective linear transformation, the rational map depends only on the linear system $\mathfrak{d}$.

Suppose there exists an effective divisor E such that $D \geq E$ for all $D \in \mathfrak{d}$. Such an E is called a *fixed divisor* of $\mathfrak{d}$. Clearly, $\mathfrak{d} - E \overset{\mathrm{df}}{=} \{D - E \mid D \in \mathfrak{d}\}$ is also a complete linear system: If $D_0 \in \mathfrak{d}$, so that $\mathfrak{d}$ consists of all divisors of the form

$$D_0 + div(f),\ f \in L(D_0),$$

then $\mathfrak{d} - E$ consists of all divisors of the form

$$D_0 - E + div(f),\ f \in L(D_0 - E) = L(D_0).$$

Moreover, $\mathfrak{d} - E$ defines the same map into projective space as $\mathfrak{d}$.

Henceforth, we assume that $\mathfrak{d}$ has no fixed divisor.

A point P of V is said to be a *base point* of $\mathfrak{d}$ if $P \in Supp(D)$ for all $D \in \mathfrak{d}$. Every point of a fixed divisor is a base point but, even when there is no fixed divisor, there may be base points.

PROPOSITION 5.1. *The rational map $\varphi \colon V \dashrightarrow \mathbb{P}^n$ defined by $\mathfrak{d}$ is defined at P if and only if P is not a base point of $\mathfrak{d}$.*

PROOF. Suppose P is not a base point of $\mathfrak{d}$, and let D_0 be an element of $\mathfrak{d}$ such that $P \notin Supp(D_0)$. Let $f_0, \dots, f_n$ be a basis for $L(D_0)$. Because $\mathfrak{d}$ has no fixed divisor, $\mathrm{div}(f_i/f_0) = D_i - D_0$ for some $D_i \geq 0$. Because $P \notin Supp(D_0)$, no f_i/f_0 can have a pole at P, and so the map $P \mapsto (\frac{f_1}{f_0}(P), \dots, \frac{f_n}{f_0}(P))$ is well-defined at P. □

Suppose $\mathfrak{d}$ has no base points, and let $\varphi \colon V \dashrightarrow \mathbb{P}^n$ be the corresponding rational map. If φ is an isomorphism onto a closed subvariety of $\mathbb{P}^n$, then

$$\mathfrak{d} = \{\varphi^{-1}(H) \mid H \text{ a hyperplane in } \mathbb{P}^n\}$$

(with the grain of salt that $\varphi^{-1}(H)$ will not always be a divisor).

DEFINITION 5.2. (a) A linear system $\mathfrak{d}$ is said to *separate points* if for any pair of points $P, Q \in V$, there exists a $D \in \mathfrak{d}$ such that

$$P \in D,\ Q \notin D.$$

(b) A linear system $\mathfrak{d}$ is said to *separate tangent directions* if for every $P \in V$ and nonzero tangent t to V at P, there exists a divisor $D \in \mathfrak{d}$ such that $P \in D$ but $t \notin \mathrm{Tgt}_P(D)$. (If f is a local equation for D near P, then $\mathrm{Tgt}_P(D)$ is the subspace of $\mathrm{Tgt}_P(V)$ defined by the equation $(df)_P = 0$. Geometrically, the condition means that only one prime divisor Z occurring in D can pass through P, that Z occurs with multiplicity 1 in D, and that $t \notin \mathrm{Tgt}_P(Z)$.)

Proposition 5.3. *Assume that $\mathfrak{d}$ has no base points. Then the map $\varphi\colon V \to \mathbb{P}^n$ defined by $\mathfrak{d}$ is a closed immersion if and only if $\mathfrak{d}$ separates points and separates tangent directions.*

Proof. From the above remarks, the condition is obviously necessary. For the sufficiency, see, for example, Hartshorne, Algebraic Geometry, 1977, II, 7.8.2. □

Theorem 5.4. *Every abelian variety A is projective.*

Proof. The first step is to show that there exists a finite set of prime divisors Z_i such that $\Sigma\, Z_i$ separates 0 from the remaining points of V, and separates the tangent directions at 0. More precisely, we want that:

(a) $\cap Z_i = \{0\}$ (here 0 is the zero element of A);
(b) $\cap Tgt_0(Z_i) = \{0\}$ (here 0 is the zero element of $Tgt_0(A)$).

To prove this we verify that any two points of 0 and P of A are contained in an open affine subvariety of A. Let U be an open affine neighbourhood of 0, and let $U+P$ be its translate by P. Choose a point u of $U \cap (U+P)$. Then

$$\begin{aligned} u \in U+P &\Longrightarrow 0 \in U+P-u, \\ u+P \in U+P &\Longrightarrow P \in U+P-u, \end{aligned}$$

and so $U' \overset{\text{df}}{=} U+P-u$ is an open affine neighbourhood of both 0 and P. Identify U' with a closed subset of $\mathbb{A}^n$, some n. There is a hyperplane H in $\mathbb{A}^n$ passing through 0 but not P, and we take Z_1 to be the closure of $H \cap U'$ in A. If there is a P' on Z_1 other than 0, choose Z_2 to pass through 0 but not P'. Continue in this fashion. Because A has the descending chain condition for closed subsets, this process will end in a finite set of Z_i's such that $\cap Z_i = \{0\}$.

Now choose any open affine neighbourhood U of P, and let $t \in Tgt_0(P)$. Suppose $t \in Tgt_0(Z_i)$ for all i. Embed $U \hookrightarrow \mathbb{A}^n$, and choose a hyperplane H through 0 such that $t \notin H$, and add the closure Z of $H \cap A$ in A to the set $\{Z_i\}$. Continue in this way until (b) holds.

Now let D be the divisor $\sum Z_i$ where $(Z_i)_{1 \le i \le n}$ satisfies conditions (a) and (b). I claim the $3D$ defines an embedding of A into $\mathbb{P}^n$, some n.

For any family $\{a_1, ..., a_n; b_1, ..., b_n\}$ of points on A, the Theorem of the Square shows that

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

This construction gives a very large class of divisors in the complete linear system defined by $3D$.

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

$$\begin{aligned} &\{b_1 \mid Z_{1,b_1} \text{ passes through } b\} \\ &\{b_1 \mid Z_{1,-a_1-b_1} \text{ passes through } b\} \end{aligned}$$

are proper closed subsets of A. Therefore, it is possible to choose a b_1 that lies on neither. Similarly, a_i and b_i for $i \geq 2$ can be chosen so that none of 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 $\Sigma_i(Z_{i,a_i} + Z_{i,b_i} + Z_{i,-a_i-b_i})$ but b

is not, which shows that the linear system defined by $3D$ separates points. The proof that it separates tangents is similar. □

Ample divisors. Let V be a nonsingular complete variety. A divisor D on V is *very ample* if the complete linear system it defines gives a closed immersion of V into $\mathbb{P}^n$. A divisor D is *ample* if nD is very ample for some $n > 0$. There are similar definitions for invertible sheaves.

The above theorem shows that there exists an ample divisor on an abelian variety A. It is known (but difficult to prove) that if D is ample on A, then $3D$ is very ample.

EXAMPLE 5.5. Let A be an elliptic curve, and let $D = 3P_0$, where P_0 is the zero element for the group structure. There are three independent functions $1, x, y$ on A having poles only at P_0, and there having no worse than a triple pole, that define an embedding of A into $\mathbb{P}^3$. Thus D is very ample, and P_0 (regarded as a divisor) is ample. Since there is nothing special about P_0 (ignoring the group structure), we see that, for any point P, the divisor P is ample. In fact, it follows easily (from the Riemann-Roch theorem), that D is ample if and only if $\deg D > 0$, and that if $\deg\ D > 3$, then D is very ample.

Something similar is true for any curve C: a divisor D on C is ample if and only if $\deg\ D > 0$, and D is very ample if $\deg\ D > 2g+1$. (See Hartshorne, ibid., p307-308.)

PROPOSITION 5.6. (a) *If D and D' are ample, so also is $D + D'$.*

(b) *If D is an ample divisor on V, then $D|W$ is ample for any closed subvariety W of V (assuming $D|W$ is defined).*

(c) *A divisor D on V is ample if and only if its extension of scalars to k^{al} is ample on $V_{k^{al}}$.*

(d) *A variety V has an ample divisor if $V_{k^{al}}$ has an ample divisor.*

PROOF. (a) By definition, there exists an n such that both nD and nD' are very ample. Hence the functions in $L(nD)$ define an embedding of V into projective space. Because nD' is very ample, it is linearly equivalent to an effective divisor D. Now $L(nD + D) \supset L(nD)$, and so $nD + D$ is very ample, which implies that $nD + nD'$ is very ample (it defines the same complete linear system as $nD + D$).

(b) The restriction of the map defined by D to W is the map defined by the restriction of D to W.

(c) The map obtained by extension of scalars from the map $V \to \mathbb{P}^n$ defined by D is that defined by $D_{k^{\mathrm{al}}}$ (cf. 4.11).

(d) Let D be an ample divisor on $V_{k^{\mathrm{al}}}$. Then D will be defined over some finite extension k' of k, and so the set $\{\sigma D \mid \sigma \in \mathrm{Aut}(k^{\mathrm{al}}/k)\}$ is finite. Let D_0 be the sum of the distinct σD's — by (a), D_0 will be again ample. Then D_0 is defined over a finite purely inseparable extension of k. If k is perfect, then D_0 is defined over k; otherwise, $p^m D_0$ will be defined over k for some power p^m of the characteristic of k. □

6. Isogenies

Let $\alpha\colon A \to B$ be a homomorphism of abelian varieties. The fibre over $0 \in B$ is called the *kernel*, $\mathrm{Ker}(\alpha)$, of α. It is a closed subvariety of A, and hence is complete. Since it inherits a group structure from that on A, it is a group variety whose connected component is an abelian variety (possibly a single point).

[If we used schemes instead of varieties, we would define the kernel to be the scheme-theoretic fibre over 0. In characteristic zero, all group schemes are reduced, and so there is no essential difference between the two notions.]

A homomorphism $\alpha\colon A \to B$ of abelian varieties is called an *isogeny* if it is surjective, and has finite kernel (i.e., the kernel has dimension zero).

PROPOSITION 6.1. *For a homomorphism $\alpha\colon A \to B$ of abelian varieties, the following are equivalent:*

(a) *α is an isogeny;*
(b) $\dim\ A = \dim\ B$ *and α is surjective;*
(c) $\dim\ A = \dim\ B$ *and $Ker(\alpha)$ is finite;*
(d) *α is finite, flat, and surjective.*

PROOF. Because A is complete, $\alpha(A)$ is a closed subvariety of B (AG 5.27). For any point $b \in \alpha(A)$, t_b defines an isomorphism of $\alpha^{-1}(0)_{k(b)} \to \alpha^{-1}(b)$. Thus, up to an extension of scalars, all fibres of the map α over points of $\alpha(A)$ are isomorphic. In particular, they have the same dimension.

Recall, (AG 8.6) that, for $b \in \alpha(A)$,

$$\dim\ \alpha^{-1}(b) \geq \dim\ A - \dim\ \alpha(A),$$

and that equality holds on an open set. Therefore the preceding remark shows that, for $b \in \alpha(A)$,

$$\dim\ \alpha^{-1}(b) = \dim\ A - \dim\ \alpha(A).$$

The equivalence of (a), (b), and (c) follows immediately from this equality.

It is clear that (d) implies (a), and so assume (a). The above arguments show that every fibre has dimension zero, and so the map is quasi-finite. Now we use the following elementary result: if $\beta \circ \alpha$ is proper and β is separated, then α is proper (Hartshorne, Algebraic Geometry, 1977, p102). We apply this to the sequence of maps

$$A \xrightarrow{\alpha} B \longrightarrow \mathrm{pt}$$

to deduce that α is proper. Now (AG 6.24) shows that α, being proper and quasi-finite, is finite. Hence (see 4.14), $\alpha_*\mathcal{O}_A$ is a coherent $\mathcal{O}_B$-module, and (AG 11.1) shows that it is locally free. □

The *degree* of an isogeny $\alpha\colon A \to B$ is its degree as a regular map, i.e., the degree of the field extension $[k(A) : \alpha^*k(B)]$. If α has degree d, then $\alpha_*\mathcal{O}_A$ is locally free of rank d. If α is separable, then it is étale (because of the homogeneity, if one point were ramified, every point would be); if further k is algebraically closed, then every fibre of $A \to B$ has exactly $\deg(\alpha)$ points.

Recall that $n_A\colon A \to A$ for the regular map that (on points) is

$$a \mapsto na = a + \cdots + a.$$

THEOREM 6.2. *Let A be an abelian variety of dimension g. Then $n_A\colon A \to A$ is an isogeny of degree n^{2g}. It is always étale when k has characteristic zero, and it is étale when k has characteristic $p \neq 0$ if and only if p does not divide n.*

PROOF. From (5.4, 5.6), we know that there is a very ample invertible sheaf $\mathcal{L}$ on A. The sheaf $(-1)_A^*\mathcal{L}$ is again very ample because $(-1)_A\colon A \to A$ is an isomorphism, and so $\mathcal{L} \otimes (-1)_A^*\mathcal{L}$ is also ample (see 5.6a). But it is symmetric:

$$(-1)_A^*(\mathcal{L} \otimes (-1)_A^*\mathcal{L}) = \mathcal{L} \otimes (-1)_A^*\mathcal{L}$$

because $(-1)(-1) = 1$.

Thus we have a symmetric very ample sheaf on A, which we again denote by $\mathcal{L}$. From (4.4) we know that $(n_A)^*\mathcal{L} \approx \mathcal{L}^{n^2}$, which is again very ample. Let $Z = \mathrm{Ker}(n_A)$. Then $(n_A)^*\mathcal{L}|Z \approx \mathcal{L}^{n^2}|Z$, which is both ample and trivial. For a connected variety V, $\mathcal{O}_V$ can be very ample only if V consists of a single point. This proves that $\mathrm{Ker}(n_A)$ has dimension zero.

Fix a very ample symmetric invertible sheaf $\mathcal{L}$, and write it $\mathcal{L} = \mathcal{L}(D)$. Then (AG 10.10),

$$(n_A^*D \cdot \ldots \cdot n_A^*D) = \deg(n_A) \cdot (D \cdot \ldots \cdot D).$$

But $n_A^*D \sim n^2D$, and so

$$(n_A^*D \cdot \ldots \cdot n_A^*D) = (n^2D \cdot \ldots \cdot n^2D) = n^{2g}(D \cdot \ldots \cdot D).$$

This implies that $\deg(n_A) = n^{2g}$, provided we can show that $(D \cdot \ldots \cdot D) \neq 0$. But we chose D to be very ample. Therefore it defines an embedding $A \hookrightarrow \mathbb{P}^n$, some n, and the linear system containing D consists of all the hyperplane sections of A (at least, it is once remove any fixed component). Therefore, in forming $(D \cdot \ldots \cdot D)$ we can replace D with any hyperplane section of A. We can find hyperplanes $H_1, \ldots, H_g$ in $\mathbb{P}^n$ such that $H_1 \cap A, \ldots, H_g \cap A$ will intersect properly, and then

$$((H_1 \cap A) \cdot \ldots \cdot (H_g \cap A)) = \deg(A) \neq 0.$$

(In fact one can even choose the H_i so that the points of intersection are of multiplicity one, so that $(\cap H_i) \cap A$ has exactly $\deg(A)$ points.)

The differential of a homomorphism $\alpha\colon A \to B$ of abelian varieties is a linear map $(d\alpha)_0\colon \mathrm{Tgt}_0(A) \to \mathrm{Tgt}_0(B)$. It is true, but not quite obvious, that

$$d(\alpha + \beta)_0 = (d\alpha)_0 + (d\beta)_0,$$

i.e., $\alpha \mapsto (d\alpha)_0$ is a homomorphism. (The first $+$ uses the group structure on B; the second uses the vector space structure on $\mathrm{Tgt}_0(B)$; it needs to be checked that they are related.) Therefore, $(dn_A)_0 = n$ (multiplication by n, $x \mapsto nx$). Since $\mathrm{Tgt}_0(A)$ is a vector space over k, this is an isomorphism if char k does not divide n, and it is zero otherwise. In the first case, n_A is étale at 0, and hence (by homogeneity) at every point; in the second it isn't. □

REMARK 6.3. Assume k is separably closed. For any n not divisible by the characteristic of k,

$$A_n(k) \stackrel{\text{df}}{=} \mathrm{Ker}(n\colon A(k) \to A(k))$$

has order n^{2g}. Since this is also true for any m dividing n, $A_n(k)$ must be a free $\mathbb{Z}/n\mathbb{Z}$-module of rank $2g$ (easy exercise using the structure theorem for finite abelian groups).

Fix a prime $\ell \neq char\ k$, and define

$$T_\ell A = \varprojlim A_{\ell^n}(k).$$

In down-to-earth terms, an element of $T_\ell A$ is an infinite sequence

$$(a_1, a_2, ..., a_n, ...),\ a_n \in A(k),$$

with $\ell a_n = a_{n-1}$, $\ell a_1 = 0$ (and so, in particular, $a_n \in A(k)_{\ell^n}$). One shows that $T_\ell A$ is a free $\mathbb{Z}_\ell$-module of rank $2g$. It is called the *Tate module* of A.

When k is not algebraically closed, then one defines

$$T_\ell A = \varprojlim A_{\ell^n}(k^{sep}).$$

There is an action of $\mathrm{Gal}(k^{sep}/k)$ on this module, which is of tremendous interest arithmetically — see later.

REMARK 6.4. Let k be algebraically closed of characteristic $p \neq 0$. In terms of varieties, all one can say is that $\#A_p(k) = p^r$, $0 \leq r \leq g$. The typical case is $r = g$ (i.e., this is true for the abelian varieties in an open subset of the moduli space). In terms of schemes, one can show that

$$\mathrm{Ker}(p\colon A \to A) = (\mathbb{Z}/p\mathbb{Z})^r \times \alpha_p^{2g-2r} \times \mu_p^r,$$

where α_p is the group scheme $\mathrm{Spec}\, k[T]/(T^p)$, and $\mu_p = Spec\ k[T]/(T^p - 1)$. Both μ_p and α_p are group schemes whose underlying set has a single point. For a k-algebra R,

$$\begin{aligned} \alpha_p(R) &= \{r \in R \mid r^p = 0\} \\ \mu_p(R) &= \{r \in R^\times \mid r^p = 1\}. \end{aligned}$$

REMARK 6.5. Let $\alpha\colon A \to B$ be an isogeny. If $Ker(\alpha) \subset A_n$, then α factors into

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} A, \quad \beta \circ \alpha = n_A$$

Note that $\deg(\alpha) \cdot \deg(\beta) = n^{2g}$.

7. THE DUAL ABELIAN VARIETY.

Let $\mathcal{L}$ be an invertible sheaf on A. It follows from the theorem of the square (4.5; 4.6) that the map

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

is a homomorphism. Consider the sheaf $m^*\mathcal{L} \otimes p^*\mathcal{L}^{-1}$ on $A \times A$, where m and p are the maps

$$A \times A \to A,\ (a, b) \mapsto a + b,\ (a, b) \mapsto a$$

respectively. We can regard it as a family of invertible sheaves on A (first factor) parametrized by A (second factor). Let

$$K(\mathcal{L}) = \{a \in A \ \mid (m^*\mathcal{L} \otimes p^*\mathcal{L}^{-1})|A \times \{a\} \text{ is trivial}\}.$$

According to (4.18), this is a closed subset of A. Its definition commutes with extension of scalars (because of 4.12).

Note that $m \circ (x \mapsto (x, a)) = t_a$ and $p \circ (x \mapsto (x, a)) = \mathrm{id}$, and so

$$(m^*\mathcal{L} \otimes p^*\mathcal{L}^{-1}) \mid A \times \{a\} = t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}.$$

Hence

$$K(\mathcal{L})(k) = \{a \in A(k) \mid \lambda_{\mathcal{L}}(a) = 0\}.$$

PROPOSITION 7.1. *Let $\mathcal{L}$ be an invertible sheaf such that $\Gamma(A, \mathcal{L}) \neq 0$; then $\mathcal{L}$ is ample if and only if $K(\mathcal{L})$ has dimension zero.*

PROOF. We can suppose that k is algebraically closed (because of 4.11, 5.6). We prove only that

$$\mathcal{L} \text{ ample } \implies K(\mathcal{L}) \text{ has dimension zero.}$$

Assume $\mathcal{L}$ is ample, and let B be the connected component of $K(\mathcal{L})$ passing through 0. It is an abelian variety (possible zero) and $\mathcal{L}_B \overset{\text{df}}{=} \mathcal{L}|B$ is ample on B (5.6b). Because, $t_b^*\mathcal{L}_B \approx \mathcal{L}_B$ for all $b \in B$, which implies that the sheaf $m^*\mathcal{L}_B \otimes p^*\mathcal{L}_B^{-1} \otimes q^*\mathcal{L}_B^{-1}$ on $B \times B$ is trivial (apply 7.4 below). On taking the inverse image of this sheaf by the regular map

$$B \to B \times B,\ b \mapsto (b, -b)$$

we find that $\mathcal{L}_B \otimes (-1_B)^*\mathcal{L}_B$ is trivial on B. But, as we saw in the proof of (6.2), $\mathcal{L}_B$ ample implies $\mathcal{L}_B \otimes (-1_B)^*\mathcal{L}_B$ ample. As in the proof of (6.2), the fact that the trivial invertible sheaf on B is ample implies that $\dim B = 0$, and so $B = 0$. □

REMARK 7.2. Let D be an effective divisor, and let $\mathcal{L} = \mathcal{L}(D)$. By definition, $\Gamma(A, \mathcal{L}(D)) = L(D)$, and so if D is effective, then $\Gamma(A, \mathcal{L}(D)) \neq 0$. Therefore, the proposition shows that that D is ample if and only if the homomorphism

$$\lambda_D \colon A(k^{al}) \to \operatorname{Pic}(A_{k^{al}}),\ a \mapsto D_a - D,$$

has finite kernel.

EXAMPLE 7.3. Let A be an elliptic curve, and let D be an effective divisor on A. We have seen (5.5) that

$$D \text{ is ample } \iff \deg(D) > 0.$$

Moreover, we know that $\lambda_D = (\deg\ D)^2 \lambda_{D_0}$ where $D_0 = P_0$ (zero element of A). Hence

$$\lambda_D \text{ has finite kernel } \iff \deg(D) > 0.$$

Thus Proposition 7.1 is easy for elliptic curves.

Definition of Pic$^0(A)$. For a curve C, $\operatorname{Pic}^0(C)$ is defined to be the subgroup of $\operatorname{Pic}(C)$ of divisor classes of degree 0. Later, we shall define $\operatorname{Pic}^0(V)$ for any complete variety, but first we define $\operatorname{Pic}^0(A)$ for A an abelian variety. From the formula $\lambda_D = (\deg D)^2 \lambda_D$ in (7.3), on an elliptic curve

$$\deg(D) = 0 \iff \lambda_D = 0.$$

This suggests defining $\operatorname{Pic}^0(A)$ to be the set of isomorphism classes of invertible sheaves $\mathcal{L}$ for which $\lambda_{\mathcal{L}} = 0$

PROPOSITION 7.4. *For an invertible sheaf on A, the following conditions are equivalent:*

(a) $K(\mathcal{L}) = A$;

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

PROOF. The equivalence of (a) and (b) is obvious from the definition of $K(\mathcal{L})$. Condition (c) implies that

$$(m^*\mathcal{L} \otimes p^*\mathcal{L}^{-1})|(A \times \{a\}) \approx q^*\mathcal{L}|A \times \{a\},$$

which is trivial, and so $(c) \Longrightarrow (a)$. The converse follows easily from the

Seesaw Principle (4.17) because (a) implies that $m^*\mathcal{L} \otimes p^*\mathcal{L}^{-1}|A \times \{a\}$ and $q^*\mathcal{L}|A \times \{a\}$ are both trivial for all $a \in A(k^{\mathrm{al}})$, and $m^*\mathcal{L} \otimes p^*\mathcal{L}^{-1}|\{0\} \times A = \mathcal{L} = q^*\mathcal{L}|\{0\} \times A$. □

We define $\mathrm{Pic}^0(A)$ to be the set of isomorphism classes of invertible sheaves satisfying the conditions of (7.4). I often write $\mathcal{L} \in \mathrm{Pic}^0(A)$ to mean that the isomorphism class of $\mathcal{L}$ lies in $\mathrm{Pic}^0(A)$.

REMARK 7.5. Let $\alpha, \beta \colon V \rightrightarrows A$ be two regular maps. Their sum $\alpha + \beta$ is the composite $m \circ (\alpha \times \beta)$. If $\mathcal{L} \in \mathrm{Pic}^0(A)$, then

$$(\alpha + \beta)^*\mathcal{L} \approx \alpha^*\mathcal{L} \otimes \beta^*\mathcal{L}.$$

This follows from applying $(\alpha \times \beta)^*$ to the isomorphism in (7.4c). Thus the map

$$Hom(V, A) \to Hom(\mathrm{Pic}^0(A), \mathrm{Pic}(V))$$

is a homomorphism of groups. In particular,

$$\mathrm{End}(A) \to \mathrm{End}(\mathrm{Pic}^0(A))$$

is a homomorphism. When we apply this to $n_A = 1_A + \cdots + 1_A$, we find that $(n_A)^*\mathcal{L} \approx \mathcal{L}^n$. Contrast this to the statement that $(n_A)^*\mathcal{L} \approx \mathcal{L}^{n^2}$ when $\mathcal{L}$ is symmetric. They are not contradictory, because

$$\mathcal{L} \in Pic^0(A) \Rightarrow (-1)_A^*\mathcal{L} \approx \mathcal{L}^{-1},$$

i.e., $\mathcal{L}$ is antisymmetric.

REMARK 7.6. Let $\alpha \colon A \to B$ be an isogeny. If $\mathrm{Ker}(\alpha) \subset A_n$, then α factors into

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C \qquad \beta \circ \alpha = n.$$

(Because α identifies B with the quotient of A by the subgroup (scheme) $\mathrm{Ker}(\alpha)$ (see 7.10), and β exists because of the universal properties of quotients.)

The dual abelian variety. The points of the dual abelian, or Picard, variety $A^\vee$ of A should parametrize the elements of $\mathrm{Pic}^0(A)$.

Consider a pair $(A^\vee, \mathcal{P})$ where $A^\vee$ is an algebraic variety over k and $\mathcal{P}$ is an invertible sheaf on $A \times A^\vee$. Assume

(a) $\mathcal{L}|_{A \times \{b\}} \in \mathrm{Pic}^0(A_b)$ for all $b \in A^\vee$, and
(b) $\mathcal{P}|_{\{0\} \times A^\vee}$ is trivial.

We call $A^\vee$ the *dual abelian variety* of A, and $\mathcal{P}$ the *Poincaré sheaf,* if the pair $(A^\vee, \mathcal{P})$ has the following universal property: for any pair $(T, \mathcal{L})$ consisting of a variety T over k and an invertible sheaf $\mathcal{L}$ such that

(a') $\mathcal{L}|_{A \times \{t\}} \in \mathrm{Pic}^0(A_t)$ for all $t \in T$, and

(b') $\mathcal{P}|_{\{0\}\times T}$ is trivial,

there is a unique regular map $\alpha\colon T \to A$ such that $(1\times\alpha)^*\mathcal{P} \approx \mathcal{L}$.

REMARK 7.7. (a) If it exists, the pair $(A^\vee, \mathcal{P})$ is uniquely determined by the universal property up to a unique isomorphism.

(b) The Picard variety commutes with extension of scalars, i.e., if $(A^\vee, \mathcal{P})$ is the Picard variety of A over k, then $((A^\vee)_K, \mathcal{P}_K)$ is the Picard variety of A_K.

(c) The universal property says that

$$\operatorname{Hom}(T, A^\vee) \cong \{\text{invertible sheaves on } \ A \times T \text{ satisfying } (a'),\ (b')\}/\approx .$$

In particular

$$A^\vee(k) = \operatorname{Pic}^0(A).$$

Hence every isomorphism class of invertible sheaves on A lying in $\operatorname{Pic}^0(A)$ is represented exactly once in the family

$$\{\mathcal{P}_b \mid b \in A^\vee(k)\}.$$

(d) The condition (b) is a normalization.

(e) It follows from the construction of $A^\vee$ (see below) that it is an abelian variety of the same dimension as A.

(f) There is a canonical isomorphism $H^1(A, \mathcal{O}_A) \to \operatorname{Tgt}_0(A^\vee)$ (Zariski cohomology).

LEMMA 7.8. *For any invertible sheaf $\mathcal{L}$ on $t_a^*\mathcal{L}\otimes\mathcal{L}^{-1} \in Pic^0(A)$.*

PROOF. I prefer to prove this in terms of divisors. Let D be a divisor on A; we have to show that, for all $a \in A$, $[D_a - D] \in \operatorname{Pic}^0(A)$, i.e., that $(D_a - D)_b - (D_a - D) \sim 0$ for all $b \in A$. But

$$(D_a - D)_b - (D_a - D) = D_{a+b} + D - (D_a + D_b) \sim 0$$

by the theorem of the square. □

Once we've shown Picard varieties exist, we'll see that map $A \mapsto A^\vee$ is a functor, and has the property to be a good duality, namely, $A^{\vee\vee} \cong A$. The last statement follows from the next theorem. First it is useful to define a *divisorial correspondence* between two abelian varieties to be an invertible sheaf $\mathcal{L}$ on $A \times B$ whose restrictions to $\{0\} \times B$ and $A \times \{0\}$ are both trivial. Let s be the "switch" map $(a, b) \mapsto (b, a)\colon A \times B \to B \times A$. If $\mathcal{L}$ is a divisorial correspondence between A and B, then $s^*\mathcal{L}$ is a divisorial correspondence between B and A.

THEOREM 7.9. *Assume char $k = 0$. Let $\mathcal{L}$ be a divisorial correspondence between A and B. Then the following conditions are equivalent:*

(a) *$(B, \mathcal{L})$ is the dual of A;*
(b) *$\mathcal{L}|A \times \{b\}$ trivial $\implies b = 0$;*
(c) *$\mathcal{L}|\{a\} \times B$ trivial $\implies a = 0$;*
(d) *$(A, s^*\mathcal{L})$ is the dual of B.*

PROOF. This is not difficult—see Mumford 1970, p81. □

Construction of the dual abelian variety. To construct the dual abelian variety, one must form quotients of varieties by the action of a finite group (group scheme in nonzero characteristic). Since this is quite elementary in characteristic zero, we sketch the proof. For simplicity, we assume that k is algebraically closed.

PROPOSITION 7.10 (Existence of quotients.). *Let V be an algebraic variety, and let G be a finite group acting on V by regular maps (on the right). Assume that every orbit of G is contained in an open affine subset of V. Then there is a variety W and a finite regular map $\pi\colon V \to W$ such that*

(a) *as a topological space, (W, π) is the quotient of V by G, i.e., $W = V/G$ as a set, and $U \subset W$ is open $\iff \pi^{-1}(U)$ is open;*
(b) *for any open affine $U \subset W$, $\Gamma(U, \mathcal{O}_U) = \Gamma(\pi^{-1}(U), \mathcal{O}_V)^G$.*
The pair (W, π) is uniquely determined up to a unique isomorphism by these conditions. The map π is surjective, and it is étale if G acts freely, i.e., if $gx = x \Longrightarrow g = 1$.

PROOF. See Mumford 1970, p66, or Serre, J.-P., Groupes Algébriques et Corps de Classes, Hermann, Paris, 1959, p57. □

The variety W in the theorem is denoted by V/G and called the *quotient* of V by G.

REMARK 7.11. We make some comments on the proof of the proposition.

(a) It is clear that the conditions determine (W, π) uniquely.

(b) If V is affine, to give an action of G on V on the right is the same as to give an action of G on $\Gamma(V, \mathcal{O}_V)$ on the left. If $V = \mathrm{Specm}(R)$, then clearly we should try defining

$$W = \mathrm{Specm}(S),\ S = R^G.$$

To prove (7.10) in this case, one shows that R is a finite R-algebra, and verifies that W has the required properties. This is all quite elementary (ibid.).

(c) Let $v \in V$, and let U be open affine subset of V containing $\{vg \mid g \in G\}$. Then $\cap Ug$ is again an open affine (see AG 3.26) and contains v; it is also stable under the action of G. Therefore V is covered by open affines stable under the action of G, and we can construct the quotient affine by affine, as in (b), and patch them together to get W.

(d) The final statement is not surprising: if G acts effectively (i.e., $G \to Aut(V)$ is injective), then the branch points of the map $V \to W$ are the points x such that $\mathrm{Stab}(x) \neq \{e\}$.

(e) When V is quasi-projective (e.g., affine or projective) every finite set is contained in an open affine, because for any finite subset of $\mathbb{P}^n$, there exists a hyperplane missing the set, and we can take $U = V \cap H$ (AG 5.23). Therefore each orbit of G is automatically contained in an open affine subset.

(f) The pair (W, π) has the following universal property: any regular map $\alpha\colon V \to W'$ that is constant on the orbits of G in V factors uniquely into $\alpha = \alpha' \circ \pi$.

(g) Lest the reader think that the whole subject of quotients of varieties by finite groups is trivial, I point out that there exists a nonsingular variety V of dimension 3 on which $G = \mathbb{Z}/2Z$ acts freely and such that V/G does not exist in any reasonable way as an algebraic variety (Hironaka, Annals 1962). This is a minimal example: the 3 can't be replaced by 2, nor the 2 by 1. The quotient fails to exist because there exists an orbit that is not contained in an open affine subvariety.

REMARK 7.12. Assume k is algebraically closed. Let A be an abelian variety over k, and let G be a finite subgroup of A. Then we can form the quotient $B = A/G$. It is an abelian variety, and $\pi\colon A \to B$ is an isogeny with kernel G.

Recall that an isogeny $\alpha\colon A \to B$ is separable if the field extension $k(A) \supset k(B)$ is separable. This is equivalent to saying that α is étale, because it is then étale at one point (see AG 8.10b), and so it is étale at all points by homogeneity.

Let $\alpha\colon A \to B$ be a separable isogeny (for example, any isogeny of degree prime to the characteristic), and let $G = \mathrm{Ker}(\alpha)$. From the universal property of A/G, we have a regular map $A/G \to B$. This is again separable, and it is bijective. Because B is nonsingular, this implies that it is an isomorphism (see AG 6.20): $B = A/G$.

Now consider two separable isogenies $\beta\colon A \to B$, $\gamma\colon A \to C$, and suppose that $\mathrm{Ker}(\beta) \subset \mathrm{Ker}(\gamma)$. On identifying B with $A/\mathrm{Ker}(\beta)$ and using the universal property of quotients, we find that there is a (unique) regular map $\delta\colon B \to C$ such that $\delta \circ \beta = \gamma$. Moreover, δ is automatically a homomorphism (because it maps 0 to 0).

For example, suppose $\alpha\colon A \to B$ is a separable isogeny such that $\mathrm{Ker}(\alpha) \supset A_n$. Then $\alpha = \beta \circ n_A$ for some isogeny $\beta\colon A \to B$, i.e., α is divisible by n in $\mathrm{Hom}(A, B)$.

Let $W = V/G$. We shall need to consider the relation between sheaves on V and sheaves on W. By a *coherent G-sheaf* on V, we mean a coherent sheaf $\mathcal{M}$ of $\mathcal{O}_V$-modules together with an action of G on $\mathcal{M}$ compatible with its action on V.

PROPOSITION 7.13. *Assume that the finite group G acts freely on V, and let $W = V/G$. The map $\mathcal{M} \mapsto \pi^*\mathcal{M}$ defines an equivalence from the category of coherent $\mathcal{O}_W$-modules to the category of coherent G-sheaves on V under which locally free sheaves of rank r correspond to locally free sheaves of rank r.*

PROOF. See Mumford 1970, p70. □

The next result is very important.

PROPOSITION 7.14. *If $\mathcal{L}$ is ample, then $\lambda_{\mathcal{L}}$ maps A onto $Pic^0(A)$.*

PROOF. See Mumford 1970, §8, p77; or Lang 1959, p99. □

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

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

on $A \times A$. Then $\mathcal{L}^*|_{\{0\}\times A} = \mathcal{L} \otimes \mathcal{L}^{-1}$, which is trivial, and for a in $A(k)$, $\mathcal{L}^*|_{A\times\{a\}} = t_a^*\mathcal{L} \otimes \mathcal{L}^{-1} = \varphi_{\mathcal{L}}(a)$, which, as we have just seen, lies in $\mathrm{Pic}^0(A)$. Therefore, $\mathcal{L}^*$ defines a family of sheaves on A parametrized by A such that $(\mathcal{L}^*)_a = \varphi_{\mathcal{L}}(a)$. If $\mathcal{L}$ is ample, then (7.14) shows that each element of $\mathrm{Pic}^0(A)$ is represented by $(\mathcal{L}^*)_a$ for a (nonzero) finite number of a in A. Consequently, if $(A^\vee, \mathcal{P})$ exists, then there is a unique isogeny $\varphi\colon A \to A^\vee$ such that $(1 \times \varphi)^*\mathcal{P} = \mathcal{L}^*$. Moreover $\varphi = \lambda_{\mathcal{L}}$, and the fibres of $A \to A^\vee$ are the equivalence classes for the relation "$a \sim b$ if and only if $\mathcal{L}_a \approx \mathcal{L}_b$".

In characteristic zero, we even know what the kernel of φ is, because it is determined by its underlying set: it equals $K(\mathcal{L})$. Therefore, in this case we define $A^\vee$ to be the quotient $A/K(\mathcal{L})$, which exists because of (7.10, 7.11e). The action of $K(\mathcal{L})$ on the second factor of $A \times A$ lifts to an action on $\mathcal{L}^*$ over $A \times A$, which corresponds by (7.13) to a sheaf $\mathcal{P}$ on $A \times A^\vee$ such that $(1 \times \varphi_{\mathcal{L}})^*\mathcal{P} = \mathcal{L}^*$.

We now check that the pair $(A^\vee, \mathcal{P})$ just constructed has the correct universal property for families of sheaves $\mathcal{M}$ parametrized by normal varieties over k (in particular, this will imply that it is independent of the choice of $\mathcal{L}$). Let $\mathcal{M}$ on $A \times T$ be such a family, and let $\mathcal{F}$ be the invertible sheaf $p_{12}^*\mathcal{M} \otimes p_{13}^*\mathcal{P}^{-1}$ on $A \times T \times A^\vee$, where p_{ij} is the projection onto the $(i,j)^{th}$ factor. Then

$$\mathcal{F}|_{A\times(t,b)} \approx \mathcal{M}_t \otimes \mathcal{P}_b^{-1},$$

and so if we let Γ denote the closed subset of $T \times A^\vee$ of points (t,b) such $\mathcal{F}|_{A\times(t,b)}$ is trivial, then Γ is the graph of a map $T \to A^\vee$ sending a point t to the unique point b such that $\mathcal{P}_b \approx \mathcal{F}_t$. Regard Γ as a closed subvariety of $T \times A^\vee$. Then the projection $\Gamma \to T$ has separable degree 1 because it induces a bijection on points (see AG 8.10). As k has characteristic zero, it must in fact have degree 1, and now the original form of Zariski's Main Theorem (AG 6.17) shows that $\Gamma \to T$ is an isomorphism. The morphism $f\colon T \approx \Gamma \xrightarrow{q} A^\vee$ has the property that $(1 \times f)^*\mathcal{P} = \mathcal{M}$, as required.

When k has nonzero characteristic, the theory is the same in outline, but the proofs become technically much more complicated. The dual variety $A^\vee$ is still the quotient of A by a subgroup $\mathcal{K}(\mathcal{L})$ having support $K(\mathcal{L})$, but $\mathcal{K}(\mathcal{L})$ need not be reduced: it is now subgroup *scheme* of V. One defines $\mathcal{K}(\mathcal{L})$ to be the maximal subscheme of A such that the restriction of $m^*\mathcal{L} \otimes q^*\mathcal{L}^{-1}$ to $\mathcal{K}(\mathcal{L}) \times A$ defines a trivial family on A. Then one defines $A^\vee = A/\mathcal{K}(\mathcal{L})$. The proof that this has the correct universal property is similar to the above, but involves much more. However, if one works with schemes, one obtains more, namely, that $(A^\vee, \mathcal{P})$ has the universal property in its definition for any *scheme* T. See Mumford 1970, Chapter III.

REMARK 7.15. The construction of quotients of algebraic varieties by group schemes is quite subtle. For algebraic spaces, the construction is much easier. Thus, it is more natural to define $A^\vee$ as the algebraic space quotient of A by $\mathcal{K}(\mathcal{L})$. The same argument as in §5 shows that a complete algebraic space having a group structure is a projective algebraic variety.

8. The Dual Exact Sequence.

Let $\alpha\colon A \to B$ be a homomorphism of abelian varieties, and let $\mathcal{P}_B$ be the Poincaré sheaf on $B \times B^\vee$. According to the definition of the dual abelian variety in the last section, the invertible sheaf $(\alpha \times 1)^*\mathcal{P}_B$ on $A \times B^\vee$ gives rise to a homomorphism $\alpha^\vee\colon B^\vee \to A^\vee$ such that $(1 \times \alpha^\vee)^*\mathcal{P}_A \approx (\alpha \times 1)^*\mathcal{P}_B$. On points $\alpha^\vee$ is simply the map $\mathrm{Pic}^0(B) \to \mathrm{Pic}^0(A)$ sending the isomorphism class of an invertible sheaf on B to its inverse image on A.

THEOREM 8.1. *If $\alpha\colon A \to B$ is an isogeny with kernel N, then $\alpha^\vee\colon B^\vee \to A^\vee$ 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 Mumford 1970, §15 p143. □

The statement about the kernels requires explanation. If the degree of α is prime to the characteristic of k, then N is an algebraic group of dimension zero over k, and the dual is taken in the following sense: if k is separably closed, N can be identified with the abstract group $N(k)$, which is finite and commutative; then

$$N^\vee = \mathrm{Hom}(N, \mu_n(k^{\mathrm{sep}})),$$

where n is any integer killing N and μ_n is the group of n^{th} roots of 1 in k^{sep}. If k is not separably closed, then $N(k^{\mathrm{sep}})$ has an action of $\mathrm{Gal}(k^{\mathrm{sep}}/k)$, and $N^\vee(k^{\mathrm{sep}})$ has the induced action.

In nonzero characteristic, there is a duality theory $N \mapsto N^\vee$ for finite group schemes. For example, $(\mathbb{Z}/pZ)^\vee = \mu_p$, and $\alpha_p^\vee = \alpha_p$. It has the property to be a good duality: $N^{\vee\vee} = N$.

There is another approach to Theorem 8.1 which offers a different insight. Let $\mathcal{L}$ be an invertible sheaf on A whose class is in $\mathrm{Pic}^0(A)$, and let L be the line bundle associated with $\mathcal{L}$. The isomorphism $p^*\mathcal{L} \otimes q^*\mathcal{L} \to m^*\mathcal{L}$ of (7.4) 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 8.2. *Let $G(\mathcal{L})$ denote L with the zero section removed; then, for some k-rational point e of $G(\mathcal{L})$, m_L defines on $G(\mathcal{L})$ the structure of a commutative group variety with identity element e relative to which $G(\mathcal{L})$ is an extension of A by $\mathbb{G}_m$.*

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

$$E(\mathcal{L}) : 0 \to \mathbb{G}_m \to G(\mathcal{L}) \to A \to 0.$$

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

PROPOSITION 8.3. *The map $\mathcal{L} \mapsto E(\mathcal{L})$ defines an isomorphism $Pic^0(A) \to Ext^1_k(A, \mathbb{G}_m)$.*

Proofs of these results can be found in Serre, J.-P., Groupes algébriques et corps de classes, Hermann, 1959, 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

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

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

ASIDE 8.4. It is not true that there is a pairing $A \times A^\vee \to ?$, at least not in the category of abelian varieties. It is possible to embed the category of abelian varieties into another category which has many of the properties of the category of vector spaces over $\mathbb{Q}$; for example, it has tensor products, duals, etc. In this new category, there exists a map $h(A) \otimes h(A^\vee) \to \mathbb{Q}$ which can be thought of as a pairing. The new category is the category of *motives,* and $h(A)$ is the motive attached to A.

9. Endomorphisms

Notation: We write $A \sim B$ if there is an isogeny $A \to B$; then $\sim$ is an equivalence relation (because of 6.5).

Decomposing abelian varieties. An abelian variety A is said to be *simple* if there does not exist an abelian variety $B \subset A$, $0 \neq B \neq A$.

Proposition 9.1. *For any abelian variety A, there are simple abelian subvarieties $A_1, ..., A_n \subset A$ such that the map*

$$A_1 \times ... \times A_n \to A,\ (a_1, ..., a_n) \mapsto a_1 + \cdots + a_n$$

is an isogeny.

Proof. By induction, it suffices to prove the following statement: let B be a subvariety of A, $0 \neq B \neq A$; then there exists an abelian variety $B' \subset A$ such that the map

$$B \times B' \to A,\ (b, b') \mapsto b + b'$$

is an isogeny.

Let i denote the inclusion $B \hookrightarrow A$. Choose an ample sheaf $\mathcal{L}$ on A, and define B' to be the connected component of the kernel of

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

passing through 0. Then B' is an abelian variety. From (AG, §8) we know that

$$\dim\ B' \geq \dim\ A - \dim\ B.$$

The restriction of the morphism $A \to B^\vee$ to B is $\lambda_{\mathcal{L}|B} \colon B \to B^\vee$, which has finite kernel because $\mathcal{L}|B$ is ample (7.1, 5.6b). Therefore $B \cap B'$ is finite, and the map $B \times B' \to A$, $(b, b') \mapsto b + b'$ is an isogeny. □

Remark 9.2. The above proof should be compared with a standard proof for the semisimplicity of a representation of a finite group G on a finite-dimensional vector space over a field Q of characteristic zero. Thus let V be a finite dimensional vector space over Q with an action of G, and let W be a G-stable subspace: we want to construct a complement W' to W, i.e., a G-stable subspace such that the map $W \oplus W' \to V$, $w, w' \mapsto w + w'$ is an isomorphism. I claim that there is a G-invariant positive-definite form $\psi \colon V \times V \to Q$. Indeed, choose any positive-definite form ψ_0 and let $\psi = \sum\ g\psi_0$. Let $W' = W^\perp$. It is stable under G because W is and ψ is G-invariant. There are at most $\dim W$ independent constraints on a vector to lie in W' and so $\dim W' \geq \dim V - \dim W$. On the other hand, $\psi|W$ is nondegenerate (because it is positive-definite), and so $W \cap W' = \{0\}$. This proves that $W \oplus W' \cong V$.

The form ψ defines an isomorphism of $Q[G]$-spaces $V \to V^\vee$, $x \mapsto \psi(x, \cdot)$, and W' is the kernel of $V \to V^\vee \to W^\vee$. For abelian varieties, we only have the map $A \to A^\vee$, but in many ways having a polarization on A is like having a positive-definite bilinear form on A.

Let A be a simple abelian variety, and let $\alpha \in \mathrm{End}(A)$. The connected component of $\mathrm{Ker}(\alpha)$ containing 0 is an abelian variety, and so it is either A or 0. Hence α is either 0 or an isogeny. In the second case, there is an isogeny $\beta \colon A \to A$ such that

$\beta\circ\alpha = n$, some $n \in \mathbb{Q}$. This means that α becomes invertible in $\mathrm{End}(A)\otimes\mathbb{Q}$. From this it follows that $\mathrm{End}(A)\otimes\mathbb{Q}$ is a division algebra, i.e., it is ring, possibly noncommutative, in which every nonzero element has an inverse. (Division algebras are also called skew fields.)

Let A and B be simple abelian varieties. If A and B are isogenous, then

$$\mathrm{End}(A)\otimes\mathbb{Q} \approx \mathrm{Hom}(A,B)\otimes\mathbb{Q}\approx \mathrm{End}(B)\otimes\mathbb{Q}.$$

More precisely, $\mathrm{Hom}(A,B)\otimes\mathbb{Q}$ is a vector space over $\mathbb{Q}$ which is a free right $\mathrm{End}(A)\otimes\mathbb{Q}$-module of rank 1, and a free left $\mathrm{End}(B)\otimes\mathbb{Q}$ module of rank 1. If they are not isogenous, then $\mathrm{Hom}(A,B)=0$.

Let A be a simple abelian variety, and let $D=\mathrm{End}(A)\otimes\mathbb{Q}$. Then $\mathrm{End}(A^n)=M_n(D)$ ($n\times n$ matrices with coefficients in D).

Now consider an arbitrary abelian variety A. We have

$$A \sim A_1^{n_1}\times\cdots\times A_r^{n_r}$$

where each A_i is simple, and A_i is not isogenous to A_j for $i\neq j$. The above remarks show that

$$\mathrm{End}(A)\otimes\mathbb{Q}\approx\prod M_{n_i}(D_i),\ D_i=\mathrm{End}\,(A_i)\otimes(A_i)\otimes\mathbb{Q}.$$

Shortly, we shall see that $\mathrm{End}(A)\otimes\mathbb{Q}$ is finite-dimensional over $\mathbb{Q}$.

The representation on $T_\ell A$. Let A be an abelian variety of dimension g over a field k. Recall that, for any n not divisible by the characteristic of k, $A_n(k^{\mathrm{sep}})$ has order n^{2g} (see 6.3), and that we define $T_\ell A = \varprojlim A_{\ell^n}(k^{\mathrm{sep}})$.

LEMMA 9.3. *Let Q be a torsion abelian group, and let (as always) Q_n be the subgroup of elements of order dividing n. Suppose there exists a d such that $\#Q_n=n^d$ for all integers n. Then $Q\approx(\mathbb{Q}/\mathbb{Z})^d$.*

PROOF. The hypothesis implies that for every n, Q_n is a free $\mathbb{Z}/nZ$-module of rank d. The choice of a basis for it determines isomorphisms

$$Q_n\overset{\approx}{\to}(\mathbb{Z}/n\mathbb{Z})^d\overset{\approx}{\to}(n^{-1}\mathbb{Z}/\mathbb{Z})^d,\quad \sum a_ie_i\mapsto(a_1,a_2,\dots)\mapsto(\frac{a_1}{n},\frac{a_2}{n},\dots).$$

If n_1 is a multiple of n, then choose a basis for Q_{n_1} compatible with the basis for Q_n. This gives an isomorphism

$$Q_{n_1}\overset{\approx}{\to}(n_1^{-1}\mathbb{Z}/\mathbb{Z})^d$$

extending the previous map. Continue in this fashion. □

REMARK 9.4. Let Q be an ℓ-primary torsion group, and suppose $\#Q_{\ell^n}=(\ell^n)^d$ all $n>0$. Set $\ell^{-\infty}\mathbb{Z}=\cup\ell^{-n}\mathbb{Z}$ (inside $\mathbb{Q}$). Then

$$Q\approx\ell^{-\infty}\mathbb{Z}/\mathbb{Z}=\mathbb{Q}_\ell/\mathbb{Z}_\ell.$$

These remarks show that

$$A(k^{\mathrm{sep}})_{tors}\approx(\mathbb{Q}/\mathbb{Z})^{2g}$$

(ignoring p-torsion in characteristic p) and that, for $\ell\neq char\ k$,

$$A(k^{\mathrm{sep}})(\ell)\approx(\ell^{-\infty}\mathbb{Z}/\mathbb{Z})^{2g}\cong(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}.$$

Recall that

$$\mathbb{Z}_\ell = \varprojlim \ \mathbb{Z}/\ell^n\mathbb{Z}$$

where the transition maps are the canonical quotient maps $\mathbb{Z}/\ell^{n+1}\mathbb{Z} \to \mathbb{Z}/\ell^n\mathbb{Z}$. Thus an element of $\mathbb{Z}_\ell$ can be regarded as an infinite sequence

$$\alpha = (a_1, ..., a_n, ...)$$

with $a_n \in \mathbb{Z}/\ell^n\mathbb{Z}$ and $a_n \equiv a_{n-1} \bmod \ell^{n-1}$. Alternatively,

$$\mathbb{Z}_\ell = \varprojlim \ \ell^{-n}\mathbb{Z}/\mathbb{Z}$$

where the transition map $\ell^{-n-1}\mathbb{Z}/\mathbb{Z} \to \ell^{-n}\mathbb{Z}/\mathbb{Z}$ is multiplication by ℓ. Thus an element of $\mathbb{Z}_\ell$ can be regarded as an infinite sequence

$$\alpha = (b_1, ..., b_n, ...)$$

with $b_n \in \ell^{-\infty}\mathbb{Z}/\mathbb{Z}$, $\ell b_1 = 0$, and $\ell b_n = b_{n-1}$.

For any abelian group Q, define

$$T_\ell Q = \varprojlim \ Q_{\ell^n}.$$

The above discussion shows that $T_\ell(\ell^{-\infty}\mathbb{Z}/\mathbb{Z}) = \mathbb{Z}_\ell$. On combining these remarks we obtain the following result (already mentioned in §6):

Proposition 9.5. *For $\ell \neq$ char k, $T_\ell A$ is a free $\mathbb{Z}_\ell$-module of rank $2g$.*

A homomorphism $\alpha\colon A \to B$ induces a homomorphism $A_n(k^{\text{sep}}) \to B_n(k^{\text{sep}})$, and hence a homomorphism

$$T_\ell\alpha\colon T_\ell A \to T_\ell B,\ (a_1, a_2, ...) \mapsto (\alpha(a_1), \alpha(a_2), ...).$$

Therefore T_ℓ is a functor from abelian varieties to $\mathbb{Z}_\ell$-modules.

Lemma 9.6. *For any prime $\ell \neq p$, the natural map*

$$\operatorname{Hom}(A, B) \to \operatorname{Hom}_{\mathbb{Z}_\ell}(T_\ell A, T_\ell B)$$

is injective. In particular, $\operatorname{Hom}(A, B)$ *is torsion-free.*

Proof. Let α be a homomorphism such that $T_\ell\alpha = 0$. Then $\alpha(P) = 0$ for every $P \in A(k^{\text{sep}})$ such that $\ell^n P = 0$ for some n. Consider a simple abelian variety $A' \subset A$. Then the kernel of $\alpha|A'$ is not finite because it contains A'_{ℓ^n} for all n, and so $\alpha|A' = 0$. Hence α is zero on every simple abelian subvariety of A, and (9.1) implies it is zero on the whole of A. □

Remark 9.7. Let $k = \mathbb{C}$. The choice of an isomorphism $A(\mathbb{C}) \approx \mathbb{C}^g/\Lambda$ determines isomorphisms $A_n(\mathbb{C}) \cong n^{-1}\Lambda/\Lambda$. As $n^{-1}\Lambda/\Lambda \cong \Lambda \otimes (\mathbb{Z}/n\mathbb{Z})$,

$$T_\ell(A) \cong \varprojlim \ \ell^{-n}\Lambda/\Lambda \cong \varprojlim \ \Lambda \otimes (\ell^{-n}\mathbb{Z}/\mathbb{Z}) \cong \Lambda \otimes (\varprojlim \ \ell^{-n}\mathbb{Z}/\mathbb{Z}) = \Lambda \otimes \mathbb{Z}_\ell.$$

[Note: tensor products don't alwasy commute with inverse limits; they do in this case because Λ is a free $\mathbb{Z}$-module of finite rank.] Thus (2.3)

$$T_\ell A = H_1(A, \mathbb{Z}) \otimes \mathbb{Z}_\ell.$$

One should think of $T_\ell A$ as being "$H_1(A, \mathbb{Z}_\ell)$". In fact, this is true, not only over $\mathbb{C}$, but over any field k — $T_\ell A$ is the first étale homology group of A (see LEC).

The characteristic polynomial of an endomorphism. Suppose first that $k = \mathbb{C}$. An endomorphism α of A defines an endomorphism of $H_1(A, \mathbb{Q})$, which is a vector space of dimension $2g$ over $\mathbb{Q}$. Hence characteristic polynomial P_α of α is defined:

$$P_\alpha(X) = \det(\alpha - X|H_1(A, \mathbb{Q})).$$

It is monic, of degree $2g$, and has coefficients in $\mathbb{Z}$ (because α preserves the lattice $H_1(A, \mathbb{Z})$). More generally, we define the characteristic polynomial of any element of $\mathrm{End}(A) \otimes \mathbb{Q}$ by the same formula.

We want to define the characteristic polynomial of an endomorphism of an abelian variety defined over a field an arbitrary field.. Write $V_\ell A = T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ $(= T_\ell A \otimes_{\mathbb{Z}} \mathbb{Q})$. When $k = \mathbb{C}$, $V_\ell A \cong H_1(A, \mathbb{Q}) \otimes \mathbb{Q}_\ell$, and so it natural to try definining

$$P_\alpha(X) = \det(\alpha - X|V_\ell A), \quad \ell \neq char\ k.$$

However, when $k \neq \mathbb{C}$, it is not obvious that the polynomial one obtains is independent of ℓ, nor even that it has coefficients in $\mathbb{Q}$. Instead, following Weil, we adopt a different approach.

Lemma 9.8. *Let α be an endomorphism of a free $\mathbb{Z}$-module Λ of finite rank such that $\alpha \otimes 1\colon \Lambda \otimes \mathbb{Q} \to \Lambda \otimes \mathbb{Q}$ is an isomorphism. Then*

$$(\Lambda : \alpha\Lambda) = |\det(\alpha)|.$$

Proof. Suppose there exists a basis $e_1, ..., e_n$ of Λ relative to which the matrix of α is diagonal, say $\alpha e_i = m_i e_i$ for $i = 1, \ldots, n$.. Then $(\Lambda : \alpha\Lambda) = |\prod m_i|$ and $\det(\alpha) = \prod m_i$. The general case is left as an exercise to the reader. (See Serre, Corps Locaux, 1962, III.1, and elsewhere.) □

Consider an endomorphism α of an abelian variety A over $\mathbb{C}$, and write $A = \mathbb{C}^g/\Lambda$, $\Lambda = H_1(A, \mathbb{Z})$. Then $\mathrm{Ker}(\alpha) = \alpha^{-1}\Lambda/\Lambda$. If α is an isogeny, then $\alpha\colon \Lambda \to \Lambda$ is injective, and it defines a bijection

$$\mathrm{Ker}(\alpha) = \alpha^{-1}\Lambda/\Lambda \to \Lambda/\alpha\Lambda.$$

Therefore, for an isogeny $\alpha\colon A \to A$,

$$\deg(\alpha) = |\det(\alpha|H_1(A, \mathbb{Q}))| = |P_\alpha(0)|.$$

More generally, for any integer r,

$$\deg(\alpha - r) = |P_\alpha(r)|.$$

We are almost ready to state our theorem. Let $\alpha \in \mathrm{End}(A)$. If α is an isogeny, we define $\deg(\alpha)$ as before; otherwise, we set $\deg(\alpha) = 0$.

Theorem 9.9. *Let $\alpha \in \mathrm{End}(A)$. There is a unique monic polynomial $P_\alpha \in \mathbb{Z}[X]$ of degree $2g$ such that $P_\alpha(r) = \deg(\alpha - r)$ for all integers r.*

Remark 9.10. The uniqueness is obvious: if P and Q are two polynomials such that $P(r) = Q(r)$ for all integers r, then $P = Q$, because otherwise $P - Q$ would have infinitely many roots.

Remark 9.11. For $\alpha \in \mathrm{End}(A)$ and $n \in \mathbb{Z}$,

$$\deg(n\alpha) = \deg(n_A) \cdot \deg(\alpha) = n^{2g}\ \deg(\alpha).$$

We can use this formula to extend the definition of deg to $\mathrm{End}(A)\otimes\mathbb{Q}$. Since $\mathrm{End}(A)$ is torsion-free, we can identify $\mathrm{End}(A)$ with a submodule of $\mathrm{End}(A)\otimes\mathbb{Q}$. For $\alpha\in\mathrm{End}(A)\otimes\mathbb{Q}$, define

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

if n is any integer such that $n\alpha\in\mathrm{End}(A)$. The previous formula shows that this is independent of the choice of n. Similarly, once we have proved the theorem, we can define

$$P_\alpha(X)=n^{-2g}\ P_{n\alpha}(nX),\ \alpha\in\mathrm{End}(A)\otimes\mathbb{Q},\ n\alpha\in\mathrm{End}(A).$$

Then $P_\alpha(X)$ is a monic polynomial of degree $2g$ with rational coefficients, and

$$P_\alpha(r)=\deg(\alpha-r),\text{ any }\ r\in\mathbb{Q}.$$

To prove the theorem we shall prove the following: fix $\alpha\in\mathrm{End}(A)\otimes\mathbb{Q}$; then the map $r\mapsto\deg(\alpha-r)$, $\mathbb{Q}\to\mathbb{Q}$, is given by a polynomial in r of the correct form. In fact, we shall prove a little more.

A function $f\colon V\to K$ on a vector space V over a field K is said to be a *polynomial function* of degree d if for every finite linearly independent set $\{e_1,...,e_n\}$ of elements of V, $f(x_1e_1+...x_ne_n)$ is a polynomial function of degree d in the x_i with coefficients in K (i.e., there is a polynomial $P\in K[X_1,\dots,X_n]$ such that $f(x_1e_1+...x_ne_n)=P(x_1,\dots,x_n)$ for all $(x_1,\dots,x_n)\in K^n$). A *homogeneous polynomial function* is defined similarly.

LEMMA 9.12. *Let V be a vector space over an infinite field K, and let $f\colon V\to K$ be a function such that, for all v,w in V, $x\mapsto f(xv+w)\colon K\to K$ is a polynomial in x with coefficients in K; then f is a polynomial function.*

PROOF. We show by induction on n that, for every subset $\{v_1,...,v_n,w\}$ 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

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

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

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

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

PROPOSITION 9.13. *The function $\alpha\mapsto\deg(\alpha)\colon\mathrm{End}(A)\otimes\mathbb{Q}\to\mathbb{Q}$ is a homogeneous polynomial function of degree $2g$ in $\mathrm{End}(A)\otimes\mathbb{Q}$.*

PROOF. According to the lemma, to show that $\deg(\alpha)$ is a polynomial function, it suffices to show that $\deg(n\alpha+\beta)$ is a polynomial in n for fixed $\alpha,\beta\in\mathrm{End}(A)\otimes\mathbb{Q}$. But we already know that deg is homogeneous of degree $2g$, i.e., we know

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

and using this one sees that it suffices to prove that $\deg(n\alpha+\beta)$ is a polynomial of degree $\leq 2g$ for $n \in \mathbb{Z}$ and fixed $\alpha, \beta \in \mathrm{End}(A)$. Let D be a very ample divisor on A, and let $D_n = (n\alpha+\beta)^*D$. Then (AG 10.10)

$$(D_n \cdot \ldots \cdot D_n) = \deg(n\alpha+\beta)\cdot(D \cdot \ldots \cdot D)$$

and so it suffices to show that (D_n^g) is a polynomial of degree $\leq 2g$ in n. Corollary (4.3) applied to the maps $n\alpha+\beta$, α, $\alpha\colon A \to A$ and the sheaf $\mathcal{L} = \mathcal{L}(D)$ shows that

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

i.e.,

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

An induction argument now shows that

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

and so

$$\deg(n\alpha+\beta)\cdot(D^g) = (D_n^g) = (\frac{n(n-1)}{2})^g(D'^g) + \ldots$$

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

We can now prove (9.9). Proposition 9.13 shows that, for each α in $\mathrm{End}(A)\otimes\mathbb{Q}$, there is a polynomial $P_\alpha(X) \in \mathbb{Q}[X]$ of degree $2g$ such that, for all rational numbers r, $P_\alpha(r) = \deg(\alpha - r_A)$. It remains to show that P_α is monic and has integer coefficients when $\alpha \in \mathrm{End}(A)$. Let D be an ample symmetric divisor on A; then

$$P_\alpha(-n) \stackrel{\mathrm{df}}{=} \deg(\alpha+n) = (D_n^g)/(D^g),\ D_n = (\alpha+n)^*D,$$

and the calculation in the proof of (9.13) shows that

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

with $D' = (2_A)^*D - 2D \sim 2D$. It follows now that P_α is monic and that it has integer coefficients.

We call P_α the *characteristic polynomial* of α and we define the *trace* $\mathrm{Tr}(\alpha)$ of α by the equation

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

The representation on $T_\ell A$ (continued). We know that $\mathrm{Hom}(A,B)$ injects into $\mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell A, T_\ell B)$, which is a free $\mathbb{Z}_\ell$-module of rank $2\dim(A)\times 2\dim(B)$. Unfortunately, this doesn't show that $\mathrm{Hom}(A,B)$ is of finite rank, because $\mathbb{Z}_\ell$ is not finitely generated as a $\mathbb{Z}$-module. What we need is that

$e_1, \ldots, e_r$ linearly independent over $\mathbb{Z} \Longrightarrow T_\ell(e_1), \ldots, T_\ell(e_r)$ linearly independent over $\mathbb{Z}_\ell$,

or equivalently, that

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

is injective.

Note: The situation is similar to that in which we have a $\mathbb{Z}$-module M contained in a finite-dimensional real vector space V. In that case we want M to be a lattice in

V. Clearly, M needn't be finitely generated, but even if it is, it needn't be a lattice — consider $M = \{m + n\sqrt{2} \mid m, n \in \mathbb{Z}\} \subset \mathbb{R}$. The way we usually prove that such an M is a lattice is to prove that it is discrete in V. Here we use the existence of P_α to prove something similar for $\mathrm{Hom}(A, B)$.

THEOREM 9.14. *For any abelian varieties A and B, and $\ell \neq$ char k, the natural map*

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

is injective, with torsion-free cokernel. Hence $\mathrm{Hom}(A, B)$ *is a free $\mathbb{Z}$-module of finite rank $\leq 4 \dim(A) \dim(B)$.*

LEMMA 9.15. *Let $\alpha \in \mathrm{Hom}(A, B)$; if α is divisible by ℓ^n in $\mathrm{Hom}(T_\ell A, T_\ell B)$, then it is divisible by ℓ^n in* $\mathrm{Hom}(A, B)$.

PROOF. The hypothesis implies α is zero on A_{ℓ^n}, and so we can apply the last statement in (7.12) to write $\alpha = \beta \circ \ell^n$. □

We first prove (9.14) under the assumption that $\mathrm{Hom}(A, B)$ is finitely generated over $\mathbb{Z}$. Let $e_1, ..., e_m$ be a basis for $\mathrm{Hom}(A, B)$, and suppose that $\sum a_i T_\ell(e_i) = 0$, $a_i \in \mathbb{Z}_\ell$. For each i, choose a sequence of integers $n_i(r)$ converging ℓ-adically to a_i. Then $|n_i(r)|_\ell$ is constant for r large, i.e., the power of ℓ dividing $n_i(r)$ doesn't change after a certain point. But for r large $T_\ell(\sum n_i(r)e_i) = \sum n_i(r)T_\ell(e_i)$ is close to zero in $\mathrm{Hom}(T_\ell A, T_\ell B)$, which means that it is divisible by a high power of ℓ, and so each $n_i(r)$ is divisible by a high power of ℓ. The contradicts the earlier statement.

Thus it remains to prove that $\mathrm{Hom}(A, B)$ is finitely generated over $\mathbb{Z}$. It follows from (9.1) that we can suppose A and B to be simple, and then that $A = B$.

LEMMA 9.16. *If A is simple, then* $\mathrm{End}(A)$ *is finitely generated over $\mathbb{Z}$.*

PROOF. It suffices to show that if $e_1, ..., e_m$ are linearly independent over $\mathbb{Z}$ in $\mathrm{End}(A)$, then $T_\ell(e_1), ...T_\ell(e_m)$ are linearly independent over $\mathbb{Z}_\ell$ in $\mathrm{End}(T_\ell A)$.

Let P be the polynomial function on $\mathrm{End}(A) \otimes \mathbb{Q}$ such that $P(\alpha) = \deg(\alpha)$ for all $\alpha \in \mathrm{End}(A)$. Because A is simple, a nonzero endomorphism α of A is an isogeny, and so $P(\alpha)$ is a positive integer. Let M be the $\mathbb{Z}$-submodule of $\mathrm{End}(T_\ell A)$ generated by the e_i. The map $P\colon \mathbb{Q}M \to \mathbb{Q}$ is continuous for the real topology because it is a polynomial in the coordinates, and so $U = \{v | P(v) < 1\}$ is an open neighbourhood 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 (ANT 4.14). Hence there is a common denominator for the elements of $\mathbb{Q}M \cap \mathrm{End}\ A$:

(*) there exists an integer n such that $\mathbb{Q}M \cap \mathrm{End}\ A \subset n^{-1}M$.

Suppose that $T_\ell(e_1), ..., T_\ell(e_m)$ are linearly dependent, so that there exist $a_i \in \mathbb{Z}_\ell$ such that $\Sigma\ a_i T_\ell(e_m) = 0$. For each i, choose a sequence of integers $n_i(r)$ converging to a_i. The same arguments as in the last proof show that, for large r, $\Sigma\ n_i(r)e_i$ is divisible by a high power of ℓ in $\mathrm{End}(A)$, but that the power of ℓ dividing each $n_i(r)$ becomes constant. Choose an integer s so large that, for some i, $n_i(r)/\ell^s \notin n^{-1}\mathbb{Z}$ for r large. Then, for large r, $(1/\ell^s)\Sigma\ n_i(r)e_i$ will lie in $\mathbb{Q}M \cap \mathrm{End}\ A$ but not $n^{-1}M$. □

REMARK 9.17. Recall that for a field k, the *prime field* of k is its smallest subfield. Thus the prime field of k is $\mathbb{Q}$ if char $k = 0$ and it is $\mathbb{F}_p$ if char $k = p \neq 0$. Suppose that k is finitely generated over its prime field k_0, so that k has finite transcendence degree and is a finite extension of a pure transcendental extension. For example, k could be any number field or any finite field. Let $\Gamma = \mathrm{Gal}(k^{\mathrm{al}}/k)$, and let A and B be abelian varieties over k. In 1963, Tate conjectured that

$$\mathrm{Hom}(A,B)\otimes\mathbb{Z}_\ell \to \mathrm{Hom}(T_\ell A, T_\ell B)^\Gamma.$$

Here the superscript Γ means that we take only the $\mathbb{Z}_\ell$-linear homomorphisms $T_\ell A \to T_\ell B$ that commute with the action of Γ.

Tate proved this in 1966 for a finite field; Zarhin proved it for many function fields in characteristic p, and Faltings proved in char 0 in the same paper in which he first proved the Mordell conjecture — see §21 below.

The Néron-Severi group. For a complete nonsingular variety V, $Pic(V)/Pic^0(V)$ is called the *Néron-Severi group* $NS(V)$ of V. Severi proved that $NS(V)$ is finitely generated for varieties over $\mathbb{C}$, and Néron proved the same result over any field k (whence the name). Note that, for a curve C over an algebraically closed field k, the degree map gives an isomorphism $NS(C) \to \mathbb{Z}$ (if k is not algebraically closed, the image may be of finite index in $\mathbb{Z}$ — the curve may not have a divisor class of degree 1).

For abelian varieties, we can prove something stronger than the Néron-Severi theorem.

COROLLARY 9.18. *The Néron-Severi group of an abelian variety is a free $\mathbb{Z}$-module of rank $\leq 4g^2$, $g = \dim(A)$.*

PROOF. Clearly $\mathcal{L} \mapsto \lambda_{\mathcal{L}}$ defines an injection $NS(A) \hookrightarrow \mathrm{Hom}(A, A^\vee)$, and so this follows from (9.14). □

REMARK 9.19. The group $NS(A)$ is a functor of A. Direct calculations show that t_a acts as the identity on $NS(A)$ for all a in $A(k)$ (because $\lambda_{t_a^*\mathcal{L}} = \lambda_{\mathcal{L}}$) and n acts as n^2 (because -1 acts as 1, and so $n^*\mathcal{L} \equiv \mathcal{L}^{n^2}$ in $NS(A)$ by 4.4).

The representation on $T_\ell A$ (continued). As we noted above, P_α should be the characteristic polynomial of α acting on $V_\ell A$, any $\ell \neq$ *char* k. Here we verify this.

PROPOSITION 9.20. *For all $\ell \neq char(k)$, $P_\alpha(X)$ is the characteristic polynomial of α acting on $V_\ell A$; hence the trace and degree of α are the trace and determinant of α acting on $V_\ell A$.*

We need two elementary lemmas.

LEMMA 9.21. *12.21. Let $P(X) = \Pi(X - a_i)$ and $Q(X) = \Pi(X - b_i)$ be monic polynomials of the same degree with coefficients in $\mathbb{Q}_\ell$; if $|\Pi\ F(a_i)|_\ell = |\Pi\ F(b_i)|_\ell$ for all $F \in \mathbb{Z}[T]$, then $P = Q$.*

PROOF. By continuity, P and Q will satisfy the condition for all F with coefficients in $\mathbb{Z}_\ell$, and even in $\mathbb{Q}_\ell$. Let d and e be the multiplicities of a_1 as a root of P and Q respectively — we shall prove the lemma by verifying that $d = e$.

Let $\alpha \in \mathbb{Q}_\ell^{\mathrm{al}}$ be close to a_1, but not equal to a_1. Then

$$\begin{aligned} |P(\alpha)|_\ell &= |\alpha - a_1|_\ell^d \prod_{a_i \neq a_1} |\alpha - a_i| \\ |Q(\alpha)|_\ell &= |\alpha - a_1|_\ell^e \prod_{b_i \neq a_1} |\alpha - b_i|. \end{aligned}$$

Let F be the minimum polynomial of α over $\mathbb{Q}_\ell$, and let $m = \deg F$. Let Σ be a set of automorphisms σ of $\mathbb{Q}_\ell^{\mathrm{al}}$ such $\{\sigma\alpha \mid \sigma \in \Sigma\}$ is the set of distinct conjugates of α. Then,

$$\prod_i F(a_i) = \prod_{\sigma,i} (a_i - \sigma\alpha).$$

Because σ permutes the a_i,

$$\prod_i (a_i - \sigma\alpha) = \prod_i (\sigma a_i - \sigma\alpha),$$

and because the automorphisms of $\mathbb{Q}_\ell^{\mathrm{al}}$ preserve valuations,

$$|(\sigma a_i - \sigma\alpha)|_\ell = |a_i - \alpha|_\ell.$$

Hence

$$|\prod_i F(a_i)|_\ell = |\prod_i (a_i - \alpha)|_\ell^m.$$

Similarly,

$$|\prod_i F(b_i)|_\ell = |\prod_i (b_i - \alpha)|_\ell^m$$

and so our hypothesis implies that

$$|\alpha - a_1|_\ell^d \prod_{a_i \neq a_1} |\alpha - a_i| = |\alpha - a_1|_\ell^e \prod_{b_i \neq a_1} |\alpha - b_i|.$$

As α approaches a_1 the factors not involving a_1 will remain constant, from which it follows that $d = e$. □

Lemma 9.22. *Let E be an algebra over a field K, and let $\delta\colon E \to K$ 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 $P = \Pi(X - a_i)$ be the polynomial such that $P(x) = \delta(\alpha - x)$. Then $\delta(F(\alpha)) = \pm \Pi F(a_i)$ for any $F \in K[T]$.*

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

$$\delta(F(\alpha)) = \delta(\prod_j (\alpha - b_j)) = \prod_j P(b_j) = \prod_{i,j} (b_j - a_i) = \pm \prod_i F(a_i).$$

□

Proof. We now prove (9.20). Clearly we may assume $k = k_s$. For any $\beta \in \mathrm{End}(A)$,

$$|\deg(\beta)|_\ell = |\#(\mathrm{Ker}(\beta))|_\ell = \#(\mathrm{Ker}(\beta)(\ell))^{-1} = \#(\mathrm{Coker}(T_\ell\beta))^{-1} = |\det(T_\ell \circ \beta)|_\ell.$$

Consider $\alpha \in \mathrm{End}(A)$, and let $a_1, a_2, \ldots$ be the roots of P_α. Then for any polynomial $F \in \mathbb{Z}[T]$, by 9.22,

$$|\Pi\ F(a_i)|_\ell = |\deg F(\alpha)|_\ell = |\det T_\ell(F(\alpha))|_\ell = |\Pi\ F(b_i)|_\ell$$

where the b_i are the eigenvalues of $T_\ell\beta$. By Lemma 9.21, this proves the proposition. $\square$

Study of the endomorphism algebra $\mathrm{End}(A)\otimes\mathbb{Q}$**.** Let D be a simple algebra (not necessarily commutative) of finite-degree over its centre K (a field). The reduced trace and reduced norm of D over K satisfy

$$\mathrm{Tr}_{D/K}(\alpha)=[D:K]Trd_{D/K}(\alpha),\ \mathrm{Nm}_{D/K}(\alpha)=Nrd_{D/K}(\alpha)^{[D:K]},\ \alpha\in D.$$

When D is a matrix algebra, $D\approx M_r(K)$, then the reduced trace of α is the trace of α regarded as a matrix and the reduced norm of α is its determinant. In general, $D\otimes_K L\approx M_r(L)$ for some finite Galois extension L of K, and the reduced trace and norm of an element of D can be defined to be the trace and determinant of its image in $M_r(L)$ — these are invariant under the Galois group, and so lie in K. Similarly, the reduced characteristic polynomial of α in D/K satisfies

$$P_{D/K,\alpha}(X)=(\Pr d_{D/K,\alpha}(X))^{[D:K]}.$$

For a simple algebra D of finite degree over $\mathbb{Q}$, we define

$$\mathrm{Tr}_{D/\mathbb{Q}}=\mathrm{Tr}_{K/\mathbb{Q}}\circ\mathrm{Tr}\,d_{D/K},\quad \mathrm{Nm}_{D/\mathbb{Q}}=\mathrm{Nm}_{K/\mathbb{Q}}\circ Nrd_{D/K},$$

where K is the centre of D. Similarly, we define $P_{D/\mathbb{Q},\alpha}(X)$ to agree with the usual characteristic polynomial when D is commutative and the reduced characteristic polynomial when D has centre $\mathbb{Q}$.

PROPOSITION 9.23. *Let K be a $\mathbb{Q}$-subalgebra of* $\mathrm{End}(A)\otimes\mathbb{Q}$*. (in particular, K and* $\mathrm{End}(A)\otimes\mathbb{Q}$ *have the same identity element), and assume that K is a field. Let $f=[K:\mathbb{Q}]$. Then $V_\ell(A)$ is a free $K\otimes_{\mathbb{Q}}\mathbb{Q}_\ell$-module of rank $(2\dim A)/f$. Therefore, the trace of α (as an endomorphism of A) is $(2g/f)\,\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$ and $\deg(\alpha)=\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)^{2g/f}$.*

PROOF. In fact, we shall prove a stronger result in which D is assumed only to be a division algebra (i.e., we allow it to be noncommutative). Let K be the centre of D, and let $d=\sqrt{[D:K]}$ and $f=[K:\mathbb{Q}]$. If $D\otimes_{\mathbb{Q}}\mathbb{Q}_\ell$ is again a division algebra, then $V_\ell(A)\approx V^{2g/fd^2}$ where V is any simple $D\otimes_{\mathbb{Q}}\mathbb{Q}_\ell$-module (up to isomorphism, there is only one simple module over a division algebra; see CFT 1.16). In general, $D\otimes_{\mathbb{Q}}\mathbb{Q}_\ell$ will decompose into a product

$$D\otimes_{\mathbb{Q}}\mathbb{Q}_\ell=\prod D_i$$

with each D_i a simple algebra over $\mathbb{Q}_\ell$ (if $K\otimes_{\mathbb{Q}}\mathbb{Q}_\ell=\prod K_i$ is the decomposition of $K\otimes_{\mathbb{Q}}\mathbb{Q}_\ell$ into product of fields, then $D_i=D\otimes_K K_i$ — see CFT 2.15). Let V_i be a simple $M_{r_i}(D_i)$-module. Then $V_\ell(A)\approx\oplus m_iV_i$ for some $m_i\geq 0$. We shall that the m_i are all equal..

Let $\alpha\in D$. The characteristic polyomial $P_\alpha(X)$ of α as an endomorphism of A is monic of degree $2\dim A$ with coefficients in $\mathbb{Q}$, and it is equal to the characteristic polynomial of $V_\ell(\alpha)$ acting on the $\mathbb{Q}_\ell$-vector space $V_\ell(A)$.

From the above decomposition of $D\otimes_{\mathbb{Q}}\mathbb{Q}_\ell$, we find that

$$P_{D/\mathbb{Q},\alpha}(X)=\prod P_{D_i/\mathbb{Q}_\ell,\alpha}(X).$$

From the isomorphism of $D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-modules $V_\ell(A) \approx \oplus m_i V_i$, we find that

$$P_\alpha(X) = \prod P_{D_i/\mathbb{Q}_\ell,\alpha}(X)^{m_i}.$$

If we assume that α generates a maximal subfield of D, so that $P_{D/\mathbb{Q},\alpha}(X)$ is irreducible, then the two equations show that any monic irreducible factor of $P_\alpha(X)$ in $\mathbb{Q}[X]$ shares a root with $P_{D/\mathbb{Q},\alpha}(X)$, and therefore equals it. Hence $P_\alpha(X) = P_{D/\mathbb{Q},\alpha}(X)^m$ for some integer m, and each m_i equals m. □

COROLLARY 9.24. *Let $\alpha \in \mathrm{End}(A) \otimes \mathbb{Q}$, and assume $\mathbb{Q}[\alpha]$ is a product of fields. Let $C_\alpha(X)$ be the characteristic polynomial of α acting on $\mathbb{Q}[\alpha]$ (e.g., if $\mathbb{Q}[\alpha]$ is a field, this is the minimum polynomial of α); then*

$$\{a \in \mathbb{C} \mid C_\alpha(a) = 0\} = \{a \in \mathbb{C} \mid P_\alpha(a) = 0\}.$$

10. Polarizations and Invertible Sheaves

As Weil pointed out, for many purposes, the correct higher dimensional analogue of an elliptic curve is not an abelian variety, but a polarized abelian variety.

A *polarization*[8] λ of an abelian variety A is an isogeny $\lambda\colon A \to A^\vee$ such that, over k^{al}, λ becomes of the form $\lambda_{\mathcal{L}}$ for some ample sheaf $\mathcal{L}$ on $A_{k^{\mathrm{al}}}$. Unfortunately, this is not quite the same as requiring that λ itself be of the form $\lambda_{\mathcal{L}}$ for $\mathcal{L}$ an ample invertible sheaf on A (AV, 13.2).

The *degree* of a polarization is its degree as an isogeny. An abelian variety together with a polarization is called a *polarized abelian variety.* When λ has degree 1, (A, λ) is said to belong to the *principal family*, and λ is called a *principal polarization.*

There is the following very interesting theorem (Mumford 1970, p150).

THEOREM 10.1. *Let $\mathcal{L}$ be an invertible sheaf on A, and let*

$$\chi(\mathcal{L}) = \sum (-1)^i \dim_k H^i(A, \mathcal{L}) \text{ (Zariski cohomology).}$$

(a) *The degree of $\lambda_{\mathcal{L}}$ is $\chi(\mathcal{L})^2$.*
(b) *(Riemann-Roch) If $\mathcal{L} = \mathcal{L}(D)$, then $\chi(\mathcal{L}) = (D^g)/g!$.*
(c) *If* $\dim K(\mathcal{L}) = 0$, *then $H^r(A, \mathcal{L})$ is nonzero for exactly one integer.*

If $\mathcal{L}$ is ample, we know $\dim K(\mathcal{L}) = 0$. If $\mathcal{L}$ is very ample, we know that $\Gamma(A, \mathcal{L}) \neq 0$, and so the theorem implies that $H^r(A, \mathcal{L}) = 0$ for all $r \neq 0$.

A Finiteness Theorem. Up to isomorphism, there are only finitely many elliptic curves over a finite field k, because each such curve can be realized as a cubic curve in $\mathbb{P}^2$ and there are only finitely many cubic equations in three variables with coefficients in k. Using Theorem 10.1 it is possible to extend this result to abelian varieties.

THEOREM 10.2. *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.*

[8] This notion of polarization differs slightly from Weil's original definition.

Using Theorem 10.1, one shows that A can be realized as a variety of degree $3^g d(g!)$ in $\mathbb{P}^{3^g d-1}$. The Chow form of such a variety is homogeneous of degree $3^g d(g!)$ in each of $g+1$ sets of $3^g d$ variables, and it determines the isomorphism class of the variety. There are only finitely many such polynomials with coefficients in k.

Remark 10.3. Theorem 10.2 played a crucial role in Tate's proof of his conjecture (9.17) over finite fields (see later).

11. The Etale Cohomology of an Abelian Variety

Let V be a variety over a field k. When $k=\mathbb{C}$, we can endow V with the complex topology, and form the cohomology groups $H^i(V,\mathbb{Q})$. Weil was the first to observe that various phenomena, for example the numbers of points on varieties, behaved as if the whole theory (cohomology groups, Poincaré duality theorems, Lefschetz traces formula...) continued to exist, even in characteristic p, and with the same Betti numbers. It is not clear whether Weil actually believed that such a theory should exist, or that it just appeared to exist.

Serre pointed out that there couldn't exist cohomology groups with coefficients in $\mathbb{Q}$ and the correct Betti numbers functorially attached to a variety in characteristic p. For example, if A is a supersingular elliptic curve in characteristic p, $\mathrm{End}(A)\otimes\mathbb{Q}$ a division algebra of dimension 4 over $\mathbb{Q}$; if $H^1(A,\mathbb{Q})$ had dimension 2 over $\mathbb{Q}$, then it would have dimension 1/2 over $\mathrm{End}(A)\otimes\mathbb{Q}$, which is nonsense. However, $\mathrm{End}(A)\otimes\mathbb{Q}_\ell\approx M_2(Q_\ell)$, $\ell\neq p$, and so there is no reason there should not be a vector space $H^1(A,\mathbb{Q}_\ell)$ of dimension 2 over $\mathbb{Q}_\ell$ functorially attached to A — in fact, we know there is, namely $V_\ell A$ (better, its dual).

Grothendieck constructed such a theory, and called in étale cohomology (see my book or notes LEC).

For abelian varieties, the étale cohomology groups are what you would expect given the complex groups (AV, §15).

Theorem 11.1. *Let A be an abelian variety of dimension g over a separably closed field k, and let ℓ be a prime different from char(k).*

(a) *There is a canonical isomorphism*

$$H^1(A_{et},\mathbb{Z}_\ell)\xrightarrow{\approx}\mathrm{Hom}_{Z_\ell}(T_\ell A,Z_\ell).$$

(b) *The cup-product pairings define isomorphisms*

$$\Lambda^r H^1(A_{et},\mathbb{Z}_\ell)\to H^r(A_{et},Z_\ell) \text{ for all } r.$$

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

Remark 11.2. The following three algebras are isomorphic:
(i) $H^*(A,\mathbb{Z}_\ell)$ with its cup-product structure;
(ii) the exterior algebra $\Lambda^* H^1(A,\mathbb{Z}_\ell)$ with its wedge-product structure;
(iii) the dual of $\Lambda^* T_\ell A$ with its wedge-product structure.

12. Weil Pairings

For an elliptic curve A over a field k, and an integer m not divisible by the characteristic of k, one has a canonical pairing

$$A(k^{\mathrm{al}})_m \times A(k^{\mathrm{al}})_m \to \mu_m(k^{\mathrm{al}})$$

where $\mu_m(k^{\mathrm{al}})$ is the group of m^{th} roots of 1 in k^{al} ($\approx \mathbb{Z}/m\mathbb{Z}$). This pairing is nondegenerate, skew-symmetric, and commutes with the action of $\mathrm{Gal}(k^{\mathrm{al}}/k)$.

For an abelian variety A, this becomes a pairing

$$e_m\colon A(k^{\mathrm{al}})_m \times A^\vee(k^{\mathrm{al}})_m \to \mu_m(k^{\mathrm{al}}).$$

Again, it is nondegenerate, and it commutes with the action of $Gal(k^{\mathrm{al}}/k)$. When combined with a polarization

$$\lambda\colon A \to A^\vee$$

this becomes a pairing

$$e_m^\lambda\colon A_m(k^{\mathrm{al}}) \times A_m(k^{\mathrm{al}}) \to \mu_m(k^{\mathrm{al}}),\ e_m^\lambda(a,b) = e_m(a,\lambda b).$$

The e_m-pairing can be defined as follows. For simplicity, assume k to be algebraically closed. Let $a \in A_m(k)$ and let $a' \in A_m^\vee(k) \subset Pic^0(A)$. If a' is represented by the divisor D on A, then m_A^*D is linearly equivalent to mD (see 7.5; m_A is the map $x \mapsto mx\colon A \to A$), which, by assumption, is linearly equivalent to zero. Therefore there are rational functions f and g on A such that $mD = (f)$ and $m_a^*D = (g)$. Since

$$\mathrm{div}(f \circ m_A) = m_A^*(\mathrm{div}(f)) = m_A^*(mD) = m(m_A^*D) = \mathrm{div}(g^m),$$

we see that $g^m/f \circ m_A$ is rational function on A without zeros or poles — it is therefore a constant function c on A. In particular,

$$g(x+a)^m = cf(mx+ma) = cf(mx) = g(x)^m.$$

Therefore $g/g \circ t_a$ is a function on A whose m^{th} power is one. This means that it is an m^{th} root of 1 in $k(A)$ and can be identified with an element of k. Define

$$e_m(a,a') = g/g \circ t_a.$$

Lemma 12.1. *Let m and n be integers not divisible by the characteristic of k. Then for all $a \in A_{m^n}(k)$ and $a' \in A_{m^n}^\vee(k)$,*

$$e_{m^n}(a,a')^n = e_m(na, na').$$

Proof. See my original article (or prove it as an exercise). □

Let $\mathbb{Z}_\ell(1) = \varprojlim \mu_{\ell^n}$ for ℓ a prime not equal to the characteristic of k. The lemma allows us to define a pairing $e_\ell\colon T_\ell A \times T_\ell A^\vee \to \mathbb{Z}_\ell(1)$ by the rule

$$e_\ell((a_n),(a_n')) = (e_{\ell^n}(a_n,a_n')).$$

For a homomorphism $\lambda\colon A \to A^\vee$, we define pairings

$$e_\ell^\lambda\colon T_\ell A \times T_\ell A \to \mathbb{Z}_\ell(1),\ (a,a') \mapsto e_\ell(a,\lambda a').$$

If $\lambda = \lambda_{\mathcal{L}}$, $\mathcal{L} \in Pic(A)$, then we write $e_\ell^{\mathcal{L}}$ for e_ℓ^λ.

Proposition 12.2. *There are the following formulas: for a homomorphism* $\alpha\colon A\to B$,

(a) $e_\ell(a,\alpha^\vee(b))=e_\ell(\alpha(a),b)$, $a\in T_\ell A$, $b\in T_\ell B$;
(b) $e_\ell^{\alpha^\vee\circ\lambda\circ f}(a,a')=e_\ell^\lambda(f(a),f(a'))$, $a,a'\in T_\ell A$, $\lambda\in\mathrm{Hom}(B,B^\vee)$;
(c) $e_\ell^{f*\mathcal{L}}(a,a')=e_\ell^{\mathcal{L}}(f(a),f(a'))$, $a,a'\in T_\ell A$, $\mathcal{L}\in Pic(B)$.
Moreover,
(d) $\mathcal{L}\mapsto e_\ell^{\mathcal{L}}$ *is a homomorphism* $Pic(A)\to\mathrm{Hom}(\Lambda^2T_\ell A,\mathbb{Z}_\ell(1))$; *in particular,* $e_\ell^{\mathcal{L}}$ *is skew-symmetric.*

Proof. See AV (or prove it as an exercise). □

For more on these pairings, see AV, §16.

13. The Rosati Involution

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

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

This has the following obvious properties:

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

For any $a,a'\in T_\ell A\otimes\mathbb{Q}$, $\ell\neq char(k)$,

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

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

Proposition 13.1. *Assume that k is algebraically closed. Then the map*

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

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

Proof. Omitted. □

Note that, in general, this set will *not* be subalgebra of $\mathrm{End}(A)\otimes\mathbb{Q}$, because α and β can be fixed by $\dagger$ without $\alpha\beta$ being fixed.

The next result is very important.

Theorem 13.2. *The bilinear form*

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

is positive definite, i.e., $Tr(\alpha\circ\alpha^\dagger)>0$ for $\alpha\neq0$. More precisely, let D be the ample divisor defining the polarization used in the definition of $\dagger$; then

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

Proof. As D is ample and $\alpha^*(D)$ is effective, the intersection number $(D^{g-1}.\alpha^*(D))$ is positive. Thus the second statement implies the first. The second statement is proved by a calculation, which we omit. □

Two 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 nonisomorphic direct factors. These were included in my article AV because Faltings used them in his original proof of the Mordell conjecture. We will come across them again later (§22).

THEOREM 13.3. *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.*

In other words: given an abelian variety A, it is possible to endow it with a polarization of degree d in only finitely many essentially different ways.

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

14. The Zeta Function of an Abelian Variety

We write $\mathbb{F}_q$ for a finite field with q elements, $\mathbb{F}$ for an algebraic closure of $\mathbb{F}_q$, and $\mathbb{F}_{q^m}$ for the unique subfield of $\mathbb{F}$ with q^m elements. Thus the elements of $\mathbb{F}_{q^m}$ are the solutions of $c^{q^m} = c$.

For a variety V over $\mathbb{F}_q$, the Frobenius map $\pi_V \colon V \to V$ is defined to be 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 $V = \mathbb{P}^n = Proj(k[X_0, ..., X_n])$, then π_V is defined by the homomorphism of rings

$$X_i \mapsto X_i^q \colon k[X_0, ..., X_n] \to k[X_0, ..., X_n]$$

and induces the map on points

$$(x_0 \colon ... : x_n) \mapsto (x_0^q : ... : x_n^q) : \mathbb{P}^n(\mathbb{F}) \to \mathbb{P}^n(\mathbb{F}).$$

For any regular map $\varphi \colon W \to V$ of varieties over $\mathbb{F}_q$, it is obvious that $\varphi \circ \pi_W = \pi_V \circ \varphi$. Therefore, if $V \hookrightarrow \mathbb{P}^n$ is a projective embedding of V, then π_V induces the map $(x_0 : ... : x_n) \mapsto (x_0^q : ... : x_n^q)$ on $V(\mathbb{F})$. Thus $V(\mathbb{F}_q)$ is the set of fixed points of $\pi_V \colon V(\mathbb{F}) \to V(\mathbb{F})$.

Let A be an abelian variety over $\mathbb{F}_q$. Then π_A maps 0 to 0 (because $0 \in V(\mathbb{F}_q)$), and so it is an endomorphism of A. Recall that its characteristic polynomial P_π is a monic polynomial of degree $2g$, $g = \dim(A)$, with coefficients in $\mathbb{Z}$.

THEOREM 14.1. *Write $P_\pi(X) = \Pi(X - a_i)$. Then*

(a) *$\#A(\mathbb{F}_{q^m}) = \prod_{i=1}^{2g}(1 - a_i^m)$ for all $m \geq 1$, and*
(b) *(Riemann hypothesis) $|a_i| = q^{\frac{1}{2}}$.*

Hence

$$|\#A(\mathbb{F}_q) - q^g| \leq 2g \cdot q^{g-\frac{1}{2}} + (2^{2g} - 2g - 1)q^{g-1}.$$

PROOF. We first deduce the inequality from the preceding statements. Take $m = 1$ in (a) and expand out to get

$$\#A(\mathbb{F}_q) = a_1 \cdots a_{2g} - \sum_{i=1}^{2g} a_1 \cdots a_{i-1}a_{i+1} \cdots a_{2g} + \cdots$$

The first term on the right is an integer, and in fact a positive integer because it is $P_\pi(0) = \deg(\pi)$, and (b) shows that it has absolute value q^g. Hence it equals q^g (actually, it easy to prove directly that $\deg(\pi) = q^g$). The Riemann hypothesis shows that each term $a_1 \cdots a_{i-1}a_{i+1} \cdots a_{2g}$ has absolute value $= q^{g-\frac{1}{2}}$, and so the sum has absolute value $\leq 2g \cdot q^{g-\frac{1}{2}}$. There are $(2^g - 2g - 1)$ terms remaining, and each has absolute value $\leq q^{g-1}$, whence the inequality.

We first prove (a) in the case $m = 1$. The kernel of

$$\pi - \mathrm{id}\colon A(\mathbb{F}) \to A(\mathbb{F})$$

is $A(\mathbb{F}_q)$. I claim that the map

$$(d\pi)_0\colon Tgt_0(A) \to Tgt_0(A)$$

is zero — in fact, that this is true for any variety. In proving it, we can replace A with an open affine neighbourhood U, and embed U into $\mathbb{A}^m$ some m in such a way that 0 maps to the origin 0. The map $(d\pi)_0$ on $Tgt_0(U)$ is the restriction of the map $(d\pi)_0$ on $Tgt_0(\mathbb{A}^m)$. But $\pi\colon \mathbb{A}^m \to A^m$ is given by the equations $Y_i = X_i^q$, and $d(X_i^q) = qX_i^{q-1} = 0$ (in characteristic p). We now find that

$$d(\pi - \mathrm{id})_0 = (d\pi)_0 - (d(id))_0 = -1.$$

Hence $\pi - 1$ is étale at the origin, and so, by homogeneity, it is étale at every point — each point in the kernel occurs with multiplicity 1. Therefore,

$$\#A(\mathbb{F}_q) = \deg(\pi - \mathrm{id}).$$

But, from the definition of P_π, we know that

$$\deg(\pi - \mathrm{id}) = P_\pi(1),$$

and this is $\Pi(1 - a_i)$.

When we replace π with π^m in the above argument, we find that

$$\#A(\mathbb{F}_{q^m}) = P_{\pi^m}(1).$$

Recall (9.20) that $a_1, ..., a_{2g}$ can be interpreted as the eigenvalues of π acting on $T_\ell A$. Clearly π^m has eigenvalues $a_1^m, ..., a_{2g}^m$, and so

$$P_{\pi^m}(X) = \Pi(X - a_i^m),\ P_{\pi^m}(1) = \Pi(1 - a_i^m)$$

which proves (a) for a general m. □

Part (b) follows from the next two lemmas.

LEMMA 14.2. *Let † be the Rosati involution on* $\mathrm{End}(A) \otimes \mathbb{Q}$ *defined by a polarization of A; then* $\pi_A^\dagger \circ \pi_A = q_A$.

PROOF. Let D be the ample divisor on A defining the polarization; thus $\lambda(a) = [D_a - D]$. We have to show that

$$\pi^\vee \circ \lambda \circ \pi = q\lambda.$$

Recall that, on points, $\pi^\vee$ is the map

$$[D'] \mapsto [\pi^* D'] \colon Pic^0(A) \to Pic^0(A).$$

Let D' be a divisor on A (or, in fact any variety defined over $\mathbb{F}_q$). If $D' = \mathrm{div}(f)$ near $\pi(P)$, then, by definition, $\pi^* D' = \mathrm{div}(f \circ \pi)$ near P. But $\pi(P) = P$ and $f \circ \pi = f^q$ (this was the definition of π), and $\mathrm{div}(f^q) = q\,\mathrm{div}(f)$; thus $\pi^* D' = qD$.

Next observe that, for any homomorphism $\alpha \colon A \to A$ and any point a on A,

$$\alpha \circ t_a(x) = \alpha(a + x) = \alpha(a) + \alpha(x) = t_{\alpha(a)} \circ \alpha(x).$$

We can now prove the lemma. For any $a \in A(\mathbb{F})$, we have

$$\begin{aligned}
(\pi^\vee \circ \lambda \circ \pi)(a) &= \pi^*[D_{\pi(a)} - D] \\
&= [\pi^* t^*_{\pi(a)} D - \pi^* D] \\
&= [(t_{\pi(a)} \circ \pi)^* D - \pi^* D] \\
&= [(\pi \circ t_a)^* D - \pi^* D] \\
&= [t^*_a \pi^* D - \pi^* D] \\
&= [t^*_a qD - qD] \\
&= q\lambda(a),
\end{aligned}$$

as required. □

LEMMA 14.3. *Let A be an abelian variety over a field k (not necessarily finite). Let α be an element of* $\mathrm{End}(A) \otimes \mathbb{Q}$ *such that $\alpha^\dagger \circ \alpha$ is an integer r; for any root a of P_α in $\mathbb{C}$, $|a|^2 = r$.*

PROOF. Note that $\mathbb{Q}[\alpha]$ is a commutative ring of finite-dimension over $\mathbb{Q}$; it is therefore an Artin ring. According to (Atiyah and MacDonald 1969, Chapter 8)[9], it has only finitely many prime ideals $\mathfrak{m}_1, ..., \mathfrak{m}_n$ each of which is also maximal, every element of $\cap \mathfrak{m}_i$ is nilpotent, and $\mathbb{Q}[\alpha]/\cap \mathfrak{m}_i$ is a product of fields

$$\mathbb{Q}[\alpha]/\cap \mathfrak{m}_i = K_1 \times ... \times K_n,\ K_i = \mathbb{Q}[\alpha]/\mathfrak{m}_i.$$

We first show that $\cap \mathfrak{m}_i = 0$, i.e., that $\mathbb{Q}[\alpha]$ has no nonzero nilpotents. Note that $\mathbb{Q}[\alpha]$ is stable under the action of $\dagger$. Let $a \neq 0 \in \mathbb{Q}[\alpha]$. Then $b \overset{\text{df}}{=} a^\dagger \cdot a \neq 0$, because $\mathrm{Tr}(a^\dagger \cdot a) > 0$. As $b^\dagger = b$, $\mathrm{Tr}(b^2) = \mathrm{Tr}(b^\dagger \cdot b) > 0$, and so $b^2 \neq 0$. Similarly, $b^4 \neq 0$, and so on, which implies b is not nilpotent, and so neither is a.

Any automorphism τ of $\mathbb{Q}[\alpha]$ permutes the maximal ideals $\mathfrak{m}_i$; it therefore permutes the factors K_i, i.e., there is a permutation σ of $\{1, 2, ..., n\}$ and isomorphisms $\tau_i \colon K_i \to K_{\sigma(i)}$ such that $\tau(a_1, ..., a_n) = (b_1, ..., b_n)$ with $b_{\sigma(i)} = \tau_i(a_i)$. In the case that $\tau = \dagger$, σ must be the trivial permutation, for otherwise $\mathrm{Tr}(a^\dagger \cdot a)$ would not always be positive (consider $(a_1, 0, 0, ...)$ if $\sigma(1) \neq 1$). Hence $\dagger$ preserves the factors of $\mathbb{Q}[\alpha]$, and is a positive-definite involution on each of them.

[9] In fact, it is easy to prove this directly. Let $f(X)$ be a monic polynomial generating the kernel of $\mathbb{Q}[X] \to \mathbb{Q}[\alpha]$. Then $\mathbb{Q}[X]/(f(X)) \cong \mathbb{Q}[\alpha]$, and the maximal ideals of $\mathbb{Q}[\alpha]$ correspond to the distinct irreducible factors of $f(X)$.

The involution † extends by linearity (equivalently by continuity) to a positive-definite involution of $\mathbb{Q}[\alpha]\otimes\mathbb{R}$. The above remarks also apply to $\mathbb{Q}[\alpha]\otimes\mathbb{R}$: it is a product of fields, and † preserves each factor and is a positive-definite involution on each of them. But now each factor is isomorphic to $\mathbb{R}$ or to $\mathbb{C}$. The field $\mathbb{R}$ has no nontrivial automorphisms at all, and so † must act on a real factor of $\mathbb{Q}[\alpha]\otimes\mathbb{R}$ as the identity map. The field $\mathbb{C}$ has only two automorphisms of finite order: the identity map and complex conjugation. The identity map is not positive-definite, and so † must act on a complex factor as complex conjugation.

We have shown: for any homomorphism $\rho\colon \mathbb{Q}[\alpha] \to\mathbb{C}$, $\rho(\alpha^\dagger) = \overline{\rho(\alpha)}$. Thus, for any such homomorphism, $r = \rho(\alpha^\dagger \cdot \alpha) = |\rho(\alpha)|^2$, and so every root of the minimum polynomial of α in $\mathbb{Q}[\alpha]/\mathbb{Q}$ has absolute value $r^{\frac{1}{2}}$. Now (9.24) completes the proof. □

REMARK 14.4. We have actually proved the following: $\mathbb{Q}[\pi]$ is a product of fields, stable under the involution †; under every map $\tau\colon \mathbb{Q}[\pi] \to C$, $\tau(\pi) = \overline{\tau(\pi)}$, and $|\tau\pi| = q^{\frac{1}{2}}$.

The zeta function of a variety V over k is defined to be the formal power series

$$Z(V,t) = \exp(\sum_{m\geq 1} N_m \frac{t^m}{m}), \qquad N_m = \#A(\mathbb{F}_{q^m}).$$

Thus

$$Z(V,t) = 1 + (\sum N_m \frac{t^m}{m}) + \frac{1}{2}(\sum N_m \frac{t^m}{m})^2 + \cdots \in \mathbb{Q}[[t]].$$

COROLLARY 14.5. *Let $P_r(t) = \prod(1-a_{i,r}\, t)$, where the $a_{i,r}$ for a fixed r run through the products $a_{i_1}a_{i_2}...a_{i_r}$, $0 < i_1 < ... < i_r \leq 2g$, a_i a root of $P(t)$. Then*

$$Z(A,t) = \frac{P_1(t)\cdots P_{2g-1}(t)}{P_0(t)P_2(t)\cdots P_{2g-2}P_{2g}(t).}$$

PROOF. Take the logarithm of each side, and use (14.1a) and the identity (from calculus)

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

□

REMARK 14.6. (a) The polynomial $P_r(t)$ is the characteristic polynomial of π acting on $\Lambda^r T_\ell A$.

(b) Let $\zeta(V,s) = Z(V,q^{-s})$; then (14.1b) implies that the zeros of $\zeta(V,s)$ lie on the lines $Re(s) = 1/2$, $3/2, ...,$ $(2g-1)/2$ and the poles on the lines $Re(s) = 0, 1, ..., 2g$, whence its name “Riemann hypothesis”.

15. FAMILIES OF ABELIAN VARIETIES

Let S be a variety over k. A *family of abelian varieties over* S is a proper smooth map $\pi\colon \mathcal{A} \to S$ with a law of composition

$$\text{mult}\colon \mathcal{A}\times_S \mathcal{A} \to \mathcal{A}$$

such that each fibre is an abelian variety. A *homomorphism* of families of abelian varieties is a regular map $\alpha\colon \mathcal{A} \to \mathcal{B}$ compatible with the structure maps $\mathcal{A} \to S$,

$\mathcal{B} \to S$, and with the multiplication maps. Many results concerning abelian varieties extend to families of abelian varieties.

PROPOSITION 15.1 (Rigidity Lemma). *Let S be a connected variety, and let $\pi\colon \mathcal{V} \to S$ be a proper flat map whose fibres are geometrically connected varieties; let $\pi'\colon \mathcal{V}' \to S$ be a variety over S, and let $\alpha\colon \mathcal{V} \to \mathcal{V}'$ be a morphism of varieties over S. If for some point s of S, the image of the fibre $\mathcal{V}_s$ in $\mathcal{V}'_s$ is a single point, then f factors through S (that is, there exists a map $f'\colon S \to \mathcal{V}'$ such that $f = f' \circ \pi$).*

PROOF. Mumford, D., Geometric Invariant Theory, Springer, 1965, 6.1. □

COROLLARY 15.2. *(a) Every morphism of families of abelian varieties carrying the zero section into the zero section is a homomorphism.*

(b) The group structure on a family of abelian varieties is uniquely determined by the choice of a zero section.

(c) A family of abelian varieties is commutative.

PROOF. (a) Apply the proposition to the map $\varphi\colon \mathcal{A} \times \mathcal{A} \to \mathcal{B}$ defined as in the proof of (1.2).

(b) This follows immediately from (a).

(c) The map $a \mapsto a^{-1}$ is a homomorphism. □

The next result is a little surprising: it says that a constant family of abelian varieties can't contain a nonconstant subfamily.

PROPOSITION 15.3. *Let A be an abelian variety over a field k, and let S be a variety over k such that $S(k) \neq \emptyset$. For any injective homomorphism $\alpha\colon \mathcal{B} \hookrightarrow A \times S$ of families of abelian varieties over S, there is an abelian subvariety B of A (defined over k) such that $\alpha(\mathcal{B}) = B \times S$.*

PROOF. Let $s \in S(k)$, and let $B = \mathcal{B}_s$ (fibre over s). Then α_s identifies B with a subvariety of A. The map $h\colon \mathcal{B} \hookrightarrow A \times S \twoheadrightarrow (A/B) \times S$ has fibre $B_s \to A \to A/B_s$ over s, which is zero, and so (15.1) shows that $h = 0$. It follows that $\alpha(\mathcal{B}) \subset B \times S$. In fact, the two are equal because their fibres over S are connected and have the same dimension. □

Recall that a finitely generated extension K of a field k is *regular* if it is linearly disjoint from k^{al}; equivalently, if $K = k(V)$ for some variety V over k.

COROLLARY 15.4. *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 $\alpha\colon A_K \to B_K$ is defined over k.*

PROOF. (a) Let V be a variety over k such that $k(V) = K$. After V has been replaced by an open subvariety, we can assume that B extends to a family of abelian varieties over V. 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. 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. $\square$

THEOREM 15.5. *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 $\alpha\colon B_K \to A$ with finite kernel having the following universal property: for any abelian variety B' and homomorphism $\alpha'\colon B'_K \to A$ with finite kernel, there exists a unique homomorphism $\varphi\colon B' \to B$ such that $\alpha' = \alpha \circ \varphi_K$.*

PROOF. Consider the collection of pairs (B, α) with B an abelian variety over k and α a homomorphism $B_K \to A$ with finite kernel, and let A^* be the abelian subvariety of A generated by the images the α. Consider two pairs (B_1, α_1) and (B_2, α_2). Then the identity component C of the kernel of $(\alpha_1, \alpha_2)\colon (B_1 \times B_2)_K \to A$ is an abelian subvariety of $B_1 \times B_2$, which (15.4) 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 $\alpha_1(B_1)$ and $\alpha_2(B)$. It is now clear that there is a pair (B, α) such that the image of α is A^*. Divide B by the largest subgroup scheme N of $\mathrm{Ker}(\alpha)$ to be defined over k. Then it is not difficult to see that the pair $(B/N, \alpha)$ has the correct universal property (given $\alpha'\colon B'_K \to A$, note that for a suitable C contained in the kernel of $(B/N)_K \times B'_K \to A$, the map $b \mapsto (b, 0)\colon B/N \to (B/N) \times B'/C$ is an isomorphism). $\square$

REMARK 15.6. The pair (B, α) 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 Lang 1959, VIII).

Mordell-Weil theorem. Recall that, for an elliptic curve A over a number field K, $A(K)$ is finitely generated (EC §11). More generally, there is the following theorem.

THEOREM 15.7. *Let A be an abelian variety over a field K that is finitely generated over the prime field. Then $A(K)$ is finitely generated.*

PROOF. For elliptic curves over $\mathbb{Q}$, this was proved by Mordell; for Jacobian varieties, it was proved by Weil in his thesis (Weil stated his result in terms of curves, since Jacobian varieties hadn't been defined over any fields except $\mathbb{C}$ at the time); it was proved for abelian varieties over number fields by Taniyama; the extension to other fields was made by Lang and Néron. For a proof for abelian varieties over number fields, see Serre 1989, Chapter 4. $\square$

Clearly, one needs some condition on K in order to have $A(K)$ finitely generated — if K is algebraically closed, $A(K)_{tors}$ is never finitely generated. However, Lang and Néron proved the following result.

THEOREM 15.8. *Assume K is finitely generated (as a field) over k, and that k is algebraically closed in K. Let (B, α) be the K/k trace of A. Then $A(K)/\alpha(B)(k)$ is finitely generated.*

16. Abelian Varieties over Finite Fields

For a field k, we can consider the following category:

objects: abelian varieties over k;

morphisms: $Mor(A, B) = \mathrm{Hom}(A, B) \otimes \mathbb{Q}$.

This is called the *category of abelian varieties up to isogeny*, $\mathbf{Isab}(k)$, over k because two abelian varieties become isomorphic in $\mathbf{Isab}(k)$ if and only if they are isogenous. It is $\mathbb{Q}$-linear category (i.e., it is additive and the Hom-sets are vector spaces over $\mathbb{Q}$) and (9.1) implies that every object in $\mathbf{Isab}(k)$ is a direct sum of a finite number of simple objects. In order to describe such a category (up to a nonunique equivalence), it suffices to list the isomorphism classes of simple objects and, for each class, the endomorphism algebra. The theorems of Honda and Tate, which we now explain, allow this to be done in the case $k = \mathbb{F}_q$.

For abelian varieties A and B, we use $\mathrm{Hom}^0(A, B)$ to denote $\mathrm{Hom}(A, B) \otimes \mathbb{Q}$ — it is a finite-dimensional $\mathbb{Q}$-vector space.

Let A be a abelian variety over $\mathbb{F}_q$, and let $\pi = \pi_A$ be the Frobenius endomorphism of A. Then π commutes with all endomorphisms of A, and so lies in the centre of $\mathrm{End}^0(A)$. If A is simple, then $\mathrm{End}^0(A)$ is a division algebra. Therefore, in this case, $\mathbb{Q}[\pi]$ is a field (not merely a product of fields). An isogeny $A \to B$ of simple abelian varieties defines an isomorphism $\mathrm{End}^0(A) \to \mathrm{End}^0(B)$ carrying π_A into π_B, and hence mapping $\mathbb{Q}[\pi_A]$ isomorphically onto $\mathbb{Q}[\pi_B]$.

Define a *Weil q-integer* to be an algebraic integer such that, for every embedding $\sigma\colon \mathbb{Q}[\pi] \hookrightarrow \mathbb{C}$, $|\sigma\pi| = q^{\frac{1}{2}}$, and let $W(q)$ be the set of Weil q-integers in $\mathbb{C}$. Say that two elements π and π' are *conjugate*, $\pi \sim \pi'$, if any one of the following (equivalent) conditions holds:

(a) π and π' have the same minimum polynomial over $\mathbb{Q}$;
(b) there is an isomorphism $\mathbb{Q}[\pi] \to \mathbb{Q}[\pi']$ carrying π into π';
(c) π and π' lie in the same orbit under the action of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ on $W(q)$.

For any simple abelian variety A, the image of π_A in $\mathbb{Q}^{\mathrm{al}}$ under any homomorphism $\mathbb{Q}[\pi_A] \hookrightarrow \mathbb{Q}^{\mathrm{al}}$ is a Weil q-integer, well-defined up to conjugacy (see 14.1). The remark above, shows that the conjugacy class of π_A depends only on the isogeny class of A.

Theorem 16.1. *The map $A \mapsto \pi_A$ defines a bijection*

$$\{\text{simple abelian varieties}/\mathbb{F}_q\}/(\text{isogeny}) \to W(q)/(\text{conjugacy}).$$

Proof. The injectivity was proved by Tate and the surjectivity by Honda. We discuss the proof below. □

To complete the description of $\mathbf{Isab}(\mathbb{F}_q)$ in terms of Weil q-integers, we have to describe the division algebra $\mathrm{End}^0(A) \otimes \mathbb{Q}$ in terms of π_A, but before we can do that, we need to review the classification of division algebras over a number field — see CFT Chapter IV.

A *central simple algebra* over a field k is a k-algebra R such that:

(a) R is finite-dimensional over k;
(b) k is the centre of R;
(c) R is a simple ring (i.e., it has no 2-sided ideals except the obvious two).

If R is also a division algebra, we call it a *central division algebra* over k.

LEMMA 16.2. *If R and S are central simple algebras over k, then so also is $R \otimes_k S$.*

PROOF. CFT IV.2.8. □

For example, if R is a central simple algebra over k, then so also is $M_r(R) = R \otimes_k M_r(k)$. Here $M_r(R)$ is the R-algebra of $r \times r$ matrices with coefficients in R.

PROPOSITION 16.3 (Wedderburn's theorem). *Every central simple algebra R over k is isomorphic to $M_r(D)$ for some $r \geq 1$ and central division algebra D over k; moreover r is uniquely determined by R, and D is uniquely determined up to isomorphism.*

PROOF. CFT IV.1.9, 2.14. □

The *Brauer group* $Br(k)$ of a field is defined as follows. Its elements are the isomorphism classes of central division algebras over k. If D and D' are two such algebras, then, according to (16.2, 16.3) $D \otimes_k D'$ is isomorphic $M_r(D'')$ for some central division algebra D over k, and we set $[D] \cdot [D'] = [D'']$. This is a group — the identity element is $[k]$, and $[D]^{-1} = [D^{opp}]$ where D^{opp} has the same underlying set and addition, but the multiplication is reversed (if $ab = c$ in D, then $ba = c$ in D^{opp}).

THEOREM 16.4. *For any local field k, there is a canonical homomorphism*

$$\mathrm{inv}\colon Br(k) \hookrightarrow \mathbb{Q}/\mathbb{Z}$$

If k is nonarchimedean, inv *is an isomorphism; if $k = \mathbb{R}$, then the image is $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$; if $k = \mathbb{C}$, then $Br(k) = 0$.*

PROOF. CFT p108 and CFT IV.4.3. □

REMARK 16.5. (a) In fact, $Br(k) = 0$ for any algebraically closed field k.

(b) The nonzero element of $Br(\mathbb{R})$ is represented by the usual (i.e., Hamilton's original) quaternions, $\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$.

THEOREM 16.6. *For a number field k, there is an exact sequence*

$$0 \to Br(k) \to \oplus_v Br(k_v) \to \mathbb{Q}/\mathbb{Z} \to 0$$

Here the sum is over all primes of k, the first map sends $[D]$ to $\Sigma[D \otimes_k k_v]$, and the second map sends (a_v) to $\Sigma\ inv(a_v)$.

PROOF. See CFT VIII.2.2 — it is no easier to prove than the main theorem of abelian class field theory. □

REMARK 16.7. For a number field k and prime v, write $inv_v(D)$ for $inv_{k_v}(D \otimes k_v)$. The theorem says that a central division algebra D over k is uniquely determined up to isomorphism by its invariants $inv_v(D)$; moreover, a family (i_v), $i_v \in \mathbb{Q}/\mathbb{Z}$, arises from a central division algebra over k if and only if $i_v = 0$ for all but finitely many v, $i_v \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ if v is real, and $i_v = 0$ if v is complex, and $\Sigma\ i_v = 0$ (in $\mathbb{Q}/\mathbb{Z}$).

We need one further result.

THEOREM 16.8. *For a central division algebra D over a number field k, the order of $[D]$ in $\mathrm{Br}(k)$ is $\sqrt{[D:k]}$. It is also equal to the least common denominator of the numbers $\mathrm{inv}_v(D)$.*

PROOF. Since the order of an element of $\oplus\mathbb{Q}/\mathbb{Z}$ is the least common denominator of its components, the second statement follows directly from Theorem 16.6. The first is stated in Artin, Thrall, and Nesbitt, Rings with Minimum Condition, 1946, p94, and proved in Reiner, I., Maximal Orders, 32.19 (and the next version of these notes). □

We now finally state our theorem.

THEOREM 16.9. *Let A be a simple abelian variety over $\mathbb{F}_q$; let $D = \mathrm{End}^0(A)$ and let $\pi \in D$ be the Frobenius element of A. Then:*

(a) *The centre of D is $\mathbb{Q}[\pi]$; therefore, D is a central division algebra over $\mathbb{Q}[\pi]$.*
(b) *For a prime v of $\mathbb{Q}[\pi]$, let $i_v = \mathrm{inv}_v(D)$. Then $\|\pi\|_v = q^{-i_v}$ (here $\|\cdot\|_v$ is the normalized valuation at the prime v; hence $\mathrm{inv}_v(D) = 1/2$ if v is real, and $inv_v(D) = 0$ if v doesn't divide p or ∞); equivalently,*
$$\mathrm{inv}_v(D) = \frac{ord_v(\pi)}{ord_v(q)}[\mathbb{Q}[\pi]_v : \mathbb{Q}_p].$$
(c) $2\dim(A) = [D:\mathbb{Q}[\pi]]^{\frac{1}{2}} \cdot [\mathbb{Q}[\pi]:\mathbb{Q}]$.

PROOF. This was proved by Tate (Inventiones Math. 1966) who, however, neglected to publish the proof of (b) (see Waterhouse and Milne, Proc. Symp. Pure Math., AMS XX, 1971). □

The injectivity of the map $A \mapsto [\pi_A]$ in (16.1) follows easily from Tate's theorem:
$$\mathrm{Hom}(A,B)\otimes\mathbb{Q}_\ell \cong \mathrm{Hom}(V_\ell A, V_\ell B)^\Gamma,\ \Gamma = \mathrm{Gal}(\mathbb{F}/\mathbb{F}_q).$$
In fact, the canonical generator of $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$ acts on $V_\ell A$ and $V_\ell B$ as π_A and π_B respectively, and these action are semisimple (i.e., over some extension of $\mathbb{Q}_\ell$ there exist bases of eigenvectors). It is now an easy exercise in linear algebra to prove that:
$$\mathrm{Hom}(V_\ell A, V_\ell B)^\Gamma = \#\{(i,j)|\ a_i = b_j\}$$
where $P_{\pi_A}(X) = \Pi(X-a_i)$, $P_{\pi_B}(X) = \Pi(X-b_j)$.

The surjectivity was proved by Honda. I will only sketch the main idea. Obviously, we have to construct over $\mathbb{F}_q$ sufficient abelian varieties to exhaust all the conjugacy classes of Weil numbers, but we can't write the equations for a single abelian variety of dimension > 2 over $\mathbb{F}_q$, so how do we proceed? We construct (special) abelian varieties over $\mathbb{C}$, realize them over number fields, and then reduce their equations modulo p, to obtain abelian varieties over finite fields.

Recall (EC 10.22) that, for an elliptic curve A over $\mathbb{C}$, either $\mathrm{End}^0(A)=\mathbb{Q}$ or $\mathrm{End}^0(A)=E$, a quadratic imaginary number field. The first case is typical; the second is special. In the second case, A is said to have complex multiplication by E.

In higher dimensions something similar holds. An algebraic number field E is said to be a *CM-field* (complex multiplication) if it is quadratic totally imaginary extension of a totally real field F. Equivalent definition: there is an involution $\iota \neq 1$ of E such that for every embedding $\tau\colon E \to \mathbb{C}$, complex conjugation acts on τE as

$\tau\iota\tau^{-1}$. An abelian variety A is said to have *complex multiplication* by the CM-field E if $E \subset \mathrm{End}(A) \otimes \mathbb{Q}$ and

(a) $2\dim\ A = [E : \mathbb{Q}]$, and
(b) for some polarization of A, the Rosati involution on $\mathrm{End}(A) \otimes \mathbb{Q}$ stabilizes E, and acts on it as ι.

Typically, an abelian variety of dimension g over $\mathbb{C}$ has $\mathrm{End}(A) \otimes \mathbb{Q} = \mathbb{Q}$; the opposite extreme is that A has complex multiplication (of course, now there are many intermediate possibilities).

Let A be an abelian variety defined over a nonarchimedean local field k (so k is the field of fractions of a complete discrete valuation ring R, with maximal ideal $\mathfrak{m}$ say; let $R/\mathfrak{m} = k_0$). Embed A into projective space $\mathbb{P}^n$, and let $\mathfrak{a} \subset k[X_0, ..., X_n]$ be the ideal corresponding to A. Let $\mathfrak{a}_0$ be the image of $\mathfrak{a} \cap R[X_0, ..., X_n]$ in $k_0[X_1, ..., X_n] = R[X_0, ...]/\mathfrak{m}R[X_0, ...]$. It defines a variety A_0 over k_0. In general A_0 may be singular, and it may depend on the choice of the embedding of A into projective space. However, if the embedding can be chosen so that A_0 is nonsingular, then A_0 is independent of all choices, and it is again an abelian variety. In this case, we say that A has *good reduction*, and we call A_0 the reduced variety. When A is an abelian variety over a number field k, then we say A has good reduction at a finite prime v of k if A_{k_v} has good reduction (k_v =completion of k at v).

PROPOSITION 16.10. *Let A be an abelian variety over $\mathbb{C}$ with complex multiplication by E. Then A has a model over some number field k, and, after possibly replacing k with a larger number field, A will have good reduction at every prime of k.*

PROOF. Omitted. □

We can construct all abelian varieties over $\mathbb{C}$ with complex multiplication by a fixed CM-field E (up to isogeny) as follows. Let $[E : \mathbb{Q}] = 2g$; the embeddings $E \hookrightarrow \mathbb{C}$ fall into g conjugate pairs $\{\varphi, \iota \circ \varphi\}$ (here ι is complex conjugation on $\mathbb{C}$). A *CM-type* for E is a choice of g embeddings $\Phi = \{\varphi_1, ..., \varphi_g\}$ of E into $\mathbb{C}$, no two of which differ by complex conjugation (thus there are 2^g different CM-types on E). Let Φ also denote the map

$$E \to \mathbb{C}^g,\ x \mapsto (\varphi_1(x), ..., \varphi_g(x)),$$

and define $A = \mathbb{C}^g/\Phi(\mathcal{O}_E)$. This is a complex torus, which has a Riemann form, and hence is an abelian variety. Evidently we can let $x \in \mathcal{O}_E$ act on A as $\Phi(x)$, and so A has complex multiplication by E.

Thus, starting from a CM-field E and a CM-type Φ, we get an abelian variety A, initially over $\mathbb{C}$. Proposition 16.10 says that A will be defined over some number field, and moreover (after possibly replacing the number field by a finite extension) it will reduce to an abelian variety over some finite field $\mathbb{F}_q$. What is the Weil integer of this abelian variety?

Given a CM-field E and a CM-type Φ, we can a construct a Weil integer as follows. Let $\mathfrak{p}$ be a prime ideal of E lying over p. Then $\mathfrak{p}^h$ is principal for some h, say $\mathfrak{p}^h = (a)$. I claim that $\pi \overset{\mathrm{df}}{=} \Pi_{\varphi\in\Phi}\varphi(a^{2n})$ is Weil q-integer for some power q of p and that, if n is taken large enough, it is independent of the choice of the element a generating $\mathfrak{p}^h$.

Note first that

$$\pi \cdot \bar{\pi} = \Pi_{\varphi\in\Phi}\varphi(a^{2n}) \cdot \overline{\varphi(a^{2n})} = \Pi_{\varphi\in \mathrm{Hom}(E,\mathbb{C})}\varphi(a^{2n}) = (\mathrm{Nm}_{E/\mathbb{Q}}\, a^n)^2,$$

which is a positive integer. The ideal

$$(\mathrm{Nm}_{E/\mathbb{Q}}\, a) = \mathrm{Nm}_{E/\mathbb{Q}}\, \mathfrak{p} = (p)^f,$$

where $f = f(\mathfrak{p}/p)$ (residue class field degree) — see ANT 4.1. Thus $\pi \cdot \bar{\pi} = q$, where $q = p^{2nf(\mathfrak{p}/p)}$. Similarly, one shows that the conjugates of π have this property, so that π is a Weil q-integer.

Next note that the unit theorem (ibid. 5.7) implies that

$$\mathrm{rank}(U_E) = g - 1 = \mathrm{rank}(U_F),$$

where U_E and U_F are the groups of units in E and F. Let $n = (U_E : U_F)$. A different generator of $\mathfrak{p}^h$ will be of the form $a \cdot u$, $u \in U_E$, and $u^n \in U_F$. But $\{\varphi_1|F, ..., \varphi_g|F\}$ is the full set of embeddings of F into $\mathbb{R}$, and so for any $c \in F$, $\Pi_{\varphi\in\Phi}\varphi c = \mathrm{Nm}_{F/\mathbb{Q}}\, c$; in particular, if $c \in U_F$, then $\Pi_{\varphi\in\Phi}\varphi c = \mathrm{Nm}_{F/\mathbb{Q}}\, c$ is a unit in $\mathbb{Z}$, i.e., it is ± 1. Hence $\Pi_{\varphi}(\varphi(au)^{2n}) = \pi \cdot \mathrm{Nm}_{F/\mathbb{Q}}(u^n)^2 = \pi \cdot (\pm 1)^2 = 1$.

After this miraculous calculation, it will come as no surprise that:

THEOREM 16.11. *Let A be the abelian variety $\mathbb{F}_q$ obtained by reduction from an abelian variety of CM-type (E, Φ). Then the Weil q-integer associated to A is that constructed by the above procedure.*

PROOF. This is the main theorem of Shimura and Taniyama, Complex Multiplication of Abelian Varieties and its Applications to Number Theory, 1961. □

After these observations, it is an exercise in number theory to prove that the map in (16.1) is surjective. For the details, see (Honda, J. Math. Soc. Japan 20, 1968, 83-95), or, better, (Tate, Séminaire Bourbaki, 1968/69, Exposé 352, Benjamin, New York).

17. Jacobian Varieties

Let C be a nonsingular projective curve over a field k. We would like to define an abelian variety J, called the Jacobian variety of C, such that $J(k) = Pic^0(C)$ (functorially). Unfortunately, this is not always possible: clearly, we would want that $J(k^{\mathrm{sep}}) = Pic^0(C_{k^{\mathrm{sep}}})$; but then

$$J(k^{\mathrm{sep}})^\Gamma = J(k) = Pic^0(C_{k^{\mathrm{sep}}})^\Gamma,\ \Gamma = \mathrm{Gal}(k^{\mathrm{sep}}/k),$$

and it is not always true that $\mathrm{Pic}^0(C_{k^{\mathrm{sep}}})^\Gamma = Pic^0(C)$. However, this is true when $C(k) \neq \emptyset$.

ASIDE 17.1. Let C be a category. An object X of C defines a contravariant functor

$$h_X : C \to Sets,\ T \mapsto \mathrm{Hom}(T, X).$$

Moreover $X \mapsto h_X$ defines a functor $C \to Fun(C, \mathbf{Sets})$ (category of contravariant functors from C to sets). We can think of $h_X(T)$ as being the set of "T-points" of X. It is very easy to show that the functor $X \mapsto h_X$ is fully faithful, i.e., $\mathrm{Hom}(X,Y) = \mathrm{Hom}(h_X, h_Y)$ — this is the Yoneda Lemma (AG 3.34). Thus C can be regarded as a full subcategory of $Fun(C, \mathbf{Sets})$: X is known (up to a unique isomorphism) once we know the functor it defines, and every morphism of functors $h_X \to h_Y$ arises from a unique morphism $X \to Y$. A contravariant functor $F : C \to Sets$ is said to be *representable* if it is isomorphic to h_X for some object X of C, and X is then said to *represent* F.

Definition of the Jacobian variety. For varieties V and T over k, set $V(T) = \mathrm{Hom}(T, V) = h_V(T)$. For a nonsingular variety T,

$$P_C^0(T) = Pic^0(C \times T)/q^*Pic^0(T)$$

(families of invertible sheaves of degree zero on C parametrized by T, modulo trivial families–cf. (4.16)). This is a contravariant functor from the category of varieties over k to the category of abelian groups.

THEOREM 17.2. *Assume $C(k) \neq \emptyset$. The functor P_C^0 is represented by an abelian variety J.*

PROOF. We shall sketch the proof later. □

From (17.1), we know that J is uniquely determined. It is called the *Jacobian variety* of C.

A *pointed variety* over k is a pair (T, t) with T a variety over k and $t \in T(k)$. We always regard an abelian variety as a pointed variety by taking the distinguished point to be 0. *A divisorial correspondence* between two pointed varieties (S, s) and (T, t) is an invertible sheaf $\mathcal{L}$ on $S \times T$ whose restrictions to $S \times \{t\}$ and $\{s\} \times T$ are both trivial.

PROPOSITION 17.3. *Let $P \in C(k)$, and let $J = Jac(C)$. There is a divisorial correspondence $\mathcal{M}$ on $C \times J$ that is universal in the following sense: for any divisorial correspondence $\mathcal{L}$ on $C \times T$ (some pointed variety T) such that $\mathcal{L}_t$ is of degree 0 for all t, there is a regular map $\varphi : T \to J$ sending the distinguished point of T to 0 and such that $(1 \times \varphi)^*\mathcal{M} \approx \mathcal{L}$.*

PROOF. See JV 1.2. □

REMARK 17.4. (a) The Jacobian variety is defined even when $C(k) = \emptyset$; however, it then doesn't (quite) represent the functor P (because the functor is not representable). See JV p168.

(b) The Jacobian variety commutes with extension of scalars, i.e., $Jac(C_{k'}) = (Jac(C))_{k'}$ for any field $k' \supset k$.

(c) Let $\mathcal{M}$ be the sheaf in (17.3); as x runs through the elements of $J(k)$, $\mathcal{M}_x$ runs through a set of representatives for the isomorphism classes of invertible sheaves of degree 0 on C.

(d) Fix a point P_0 in $J(k)$. There is a regular map $\varphi_{P_0} : C \to J$ such that, on points, φ_{P_0} sends P to $[P - P_0]$; in particular, φ_{P_0} sends P_0 to 0. The map φ_{Q_0} differs from φ_{P_0} by translation by $[P_0 - Q_0]$ (regarded as a point on J).

(e) The dimension of J is the genus of C. If C has genus zero, then $Jac(C) = 0$ (this is obvious, because $\mathrm{Pic}^0(C) = 0$, even when one goes to the algebraic closure). If C has genus 1, then $Jac(C) = C$ (provided C has a rational point; otherwise it differs from C — because $Jac(C)$ always has a point).

Construction of the Jacobian variety. Fix a nonsingular projective curve over k. For simplicity, assume $k = k^{\mathrm{al}}$. We want to construct a variety such that $J(k)$ is the group of divisor classes of degree zero on C. As a first step, we construct a variety whose points are the effective divisors of degree r, some $r > 0$. Let $C^r = C \times C \times \ldots \times C$ (r copies). A point on C^r is an ordered r-tuple of points on C. The symmetric group on r letters, S_r, acts on C^r by permuting the factors, and the points on the quotient variety $C^{(r)} \stackrel{\mathrm{df}}{=} C^r/S_r$ are the unordered r-tuples of points on C. But an unordered r-tuple is just an effective divisor of degree r, $\Sigma\ P_i$. Thus

$$C^{(r)} = Div^r(C) \stackrel{\mathrm{df}}{=} \{\text{effective divisors of degree } \ r \text{ on } \ C\}.$$

Write π for the quotient map $C^r \to C^{(r)}$, $(P_1, \ldots, P_r) \mapsto \sum\ P_i$.

LEMMA 17.5. *The variety $C^{(r)}$ is nonsingular.*

PROOF. In general, when a finite group acts freely on a nonsingular variety, the quotient will be nonsingular. In our case, there are points on C^r whose stabilizer subgroup is nontrivial, namely the points $(P_1, \ldots, P_r)$ in which two (or more) P_i coincide, and we have to show that they don't give singularities on the quotient variety. The worst case is a point $Q = (P, \ldots, P)$, and here one can show that

$$\widehat{\mathcal{O}}_Q \cong k[[\sigma_1, \ldots, \sigma_r]],$$

the power series ring in the elementary symmetric functions $\sigma_1, \ldots, \sigma_r$ in the X_i, and this is a regular ring. See JV 3.2. $\square$

Let $\mathrm{Pic}^r(C)$ be the set of divisor classes of degree r. For a fixed point P_0 on C, the map

$$[D] \mapsto [D + rP_0]\colon \mathrm{Pic}^0(C) \to \mathrm{Pic}^r(C)$$

is a bijection (both $\mathrm{Pic}^0(C)$ and $\mathrm{Pic}^r(C)$ are fibres of the map $\deg\colon Pic(C) \to \mathbb{Z}$). This remains true when we regard $\mathrm{Pic}^0(C)$ and $\mathrm{Pic}^r(C)$ as functors of varieties over k (see above), and so it suffices to find a variety representing the $\mathrm{Pic}^r(C)$.

For a divisor of degree r, the Riemann-Roch theorem says that

$$\ell(D) = r + 1 - g + \ell(K - D)$$

where K is the canonical divisor. Since $\deg(K) = 2g - 2$, $\deg(K - D) < 0$ and $\ell(K - D) = 0$ when $\deg(D) > 2g - 2$. Thus,

$$\ell(D) = r + 1 - g > 0, \text{ if } \ r = \deg(D) > 2g - 2.$$

In particular, every divisor class of degree r contains an effective divisor, and so the map

$$\varphi : \{\text{effective divisors of degree } \ r\} \to Pic^r(C),\ D \mapsto [D]$$

is surjective when $r > 2g - 2$. We can regard this as a morphism of functors

$$\varphi\colon C^{(r)} \twoheadrightarrow \ Pic^r(C).$$

Suppose that we could find a section s to φ, i.e., a morphism of functors $s\colon \mathrm{Pic}^r(C) \to C^{(r)}$ such that $\varphi \circ s = id$. Then $s \circ \varphi$ is a morphism of functors

$C^{(r)} \to C^{(r)}$ and hence by (17.1) a regular map, and we can form the fibre product:

$$\begin{tikzcd} C^{(r)} \arrow[d, "{(1,s\circ\varphi)}"'] & J' \arrow[l] \arrow[d] \\ C^{(r)} \times C^{(r)} & C^{(r)}. \arrow[l, "\Delta"'] \end{tikzcd}$$

Then

$$J'(k) = \{(a,b) \in C^{(r)} \times C^{(r)} \mid a = b, \quad b = s \circ \varphi(a)\} \overset{b \mapsto \varphi(b)}{\to} Pic^r(C)$$

is an isomorphism. Thus we will have constructed the Jacobian variety; in fact J' will be a closed subvariety of $C^{(r)}$. Unfortunately, it is not possible to find such a section: the Riemann-Roch theorem tells us that, for $r > 2g-2$, each divisor class of degree r is represented by an $(r-g)$-dimensional family of effective divisors, and there is no nice functorial way of choosing a representative. However, it is possible to do this " locally", and so construct J' as a union of varieties, each of which is a closed subvariety of an open subvariety of $C^{(r)}$. For the details, see JV §4.

18. Abel and Jacobi

Abel 1802-29.

Jacobi 1804-1851.

Let $f(X,Y) \in \mathbb{R}[X,Y]$. We can regard the equation $f(X,Y) = 0$ as defining Y (implicitly) as a multivalued function of X. An integral of the form,

$$\int g(Y)dX$$

with $g(Y)$ a rational function, is called an abelian integral, after Abel who made a profound study of them. For example, if $f(X,Y) = Y^2 - X^3 - aX - b$, then

$$\int \frac{dX}{Y} = \int \frac{dX}{(X^3 + aX + b)^{\frac{1}{2}}}$$

is an example of an abelian integral — in this case it is a elliptic integral, which had been studied in the eighteenth century. The difficulty with these integrals is that, unless the curve $f(X,Y) = 0$ has genus 0, they can't be evaluated in terms of the elementary functions.

Today, rather than integrals of multivalued functions, we prefer to think of differentials on a Riemann surface, e.g., the compact Riemann surface (i.e., curve over $\mathbb{C}$) defined by $f(X,Y) = 0$.

Let C be a compact Riemann surface. Recall[10] that C is covered by coordinate neigbourhoods (U,z) where U can be identified with an open subset of $\mathbb{C}$ and z is the complex variable; if (U_1, z_1) is a second open set, then $z = u(z_1)$ and $z_1 = v(z)$ with u and v holomorphic functions on $U \cap U_1$. To give a differential form ω on C, one has to give an expression $f(z)dz$ on each (U,z) such that, on $U \cap U_1$,

$$f(u(z_1)) \cdot u'(z_1) \cdot dz_1 = f_1(z_1) \cdot dz_1.$$

[10] See Cartan, H., Elementary Theory of Analytic Functions of One or Several Complex Variables, Addison Wesley, 1963, especially VI.4.

A differential form is *holomorphic* if each of the functions $f(z)$ is holomorphic (rather than meromorphic). Let ω be a differential on C and let γ be a path in $U \cap U_1$; then

$$\int_\gamma f(z) \circ dz = \int_\gamma f_1(z_1) \circ dz_1.$$

Thus, it makes sense to integrate ω along any path in C.

THEOREM 18.1. *The set of holomorphic differentials on C forms a g-dimensional vector space where g is the genus of C.*

We denote this vector space by $\Gamma(C, \Omega^1)$. If $\omega_1, ..., \omega_g$ is a basis for the space, then every holomorphic differential is a linear combination, $\omega = \Sigma\ a_i\omega_i$, of the ω_i, and $\int_\gamma \omega = a \int_\gamma \omega_i$; therefore it suffices to understand the finite set of integrals $\{\int_\gamma \omega_1, \ldots, \int_\gamma \omega_g\}$.

Recall (from topology) that C is a g-holed torus, and that $H_1(C, \mathbb{Z})$ has a canonical basis $\gamma_1, ..., \gamma_{2g}$ — roughly speaking each γ_i goes once round one hole. The vectors

$$\pi_j = \begin{pmatrix} \int_{\gamma_j} \omega_1 \\ \vdots \\ \int_{\gamma_j} \omega_g \end{pmatrix} \in \mathbb{C}^g,\ j = 1, ..., 2g$$

are called the *period vectors.*

THEOREM 18.2. *The $2g$ period vectors are linearly independent over $\mathbb{R}$.*

Thus $\mathbb{C}^g / \Sigma\ \mathbb{Z}\pi_i$ is a torus. We shall see that in fact it is an abelian variety (i.e., it has a Riemann form), and that it is the Jacobian variety.

Fix a point P_0 on C. If P is a second point, and γ is a path from P_0 to P, then $\omega \mapsto \int_\gamma \omega$ is linear map $\Gamma(C, \Omega^1) \to \mathbb{C}$. Note that if we replace γ with a different path γ' from P_0 to P, then γ' differs from γ by a loop. If the loop is contractible, then $\int_\gamma \omega = \int_{\gamma'} \omega$; otherwise the two integrals differ by a sum of periods.

THEOREM 18.3 (Jacobi inversion formula). *Let ℓ be a linear map $\Gamma(C, \Omega^1) \to \mathbb{C}$; then there exist points $P_1, ..., P_g$ on C and paths γ_i from P to P_i such that*

$$\ell(\omega) = \Sigma \int_{\gamma_i} \omega$$

for all $\omega \in \Gamma(C, \Omega^1)$.

THEOREM 18.4 (Abel). *Let $P_1, ..., P_r$ and $Q_1, ..., Q_r$ be points on C (not necessarily distinct). Then there exists a meromorphic function f on C with poles exactly at the P_i and zeros exactly at the Q_i if and only if, for all paths γ_i from P to P_i and all paths γ_i' from P to Q_i, there exists an element $\gamma \in H_1(C, \mathbb{Z})$ such that*

$$\Sigma \int_{\gamma_i} \omega - \Sigma \int_{\gamma_i'} \omega = \int_\gamma \omega$$

for all $\omega \in \Gamma(C, \Omega^1)$.

Let $\gamma \in H_1(C, \mathbb{Z})$; then

$$\omega \mapsto \int_\gamma \omega$$

is a linear function on the vector space $\Gamma(C,\Omega^1)$, i.e., an element of $\Gamma(C,\Omega^1)^\vee$. Thus we have a map

$$\gamma \mapsto \int_\gamma : H_1(C,\mathbb{Z}) \to \Gamma(C,\Omega^1)^\vee$$

which (18.2) implies is injective. Set

$$J = \Gamma(C,\Omega^1)^\vee / H_1(C,\mathbb{Z}).$$

The choice of a basis for $\Gamma(C,\Omega^1)$ identifies J with $\mathbb{C}^g/\Sigma\ Z\pi_j$, which is therefore a complex torus.

THEOREM 18.5. *The intersection product*

$$H_1(C,\mathbb{Z}) \times H_1(C,\mathbb{Z}) \to \mathbb{Z}$$

is a Riemann form on J. Hence J is an abelian variety.

Fix a point P on C. As we noted above, $\int_P^Q \omega$ doesn't make sense, because it depends on the choice of a path from P to Q. But two choices differ by a loop, and so $\omega \mapsto \int_P^Q \omega$ is well-defined as an element of

$$\Gamma(C,\Omega^1)^\vee / H_1(C,\mathbb{Z}).$$

Thus we have a canonical map $\varphi_P : C \to J$ sending P to 0.

Now consider the map

$$Div^0(C) \to J,\ \Sigma\ n_i P_i \mapsto (\omega \mapsto \Sigma n_i \int_P^{P_i} \omega).$$

The Jacobi inversion formula shows that this map is surjective (in fact it proves more than that). Abel's theorem shows that the kernel of the map is precisely the group of principal divisors. Therefore, the theorems of Abel and Jacobi show precisely that the above map defines an isomorphism

$$Pic^0(C) \to J.$$

References for this section. Griffiths, P., Introduction to Algebraic Curves, AMS, 1989. (Treats algebraic curves over $\mathbb{C}$. Chapter V is on the theorems of Abel and Jacobi.)

Fulton, W., Algebraic Topology, Springer, 1995, especially Chapter 21.

Part II: Finiteness Theorems

At the end of the paper[11] in which he proved that all the rational points on elliptic curve can be obtained from a finite number by the tangent and chord contruction, Mordell made the following remark:

> In conclusion, I might note that the preceding work suggests to me the truth of the following statements concerning indeterminate equations, none of which, however, I can prove. The left-hand sides are supposed to have no squared factors in x, the curves represented by the equations are not degenerate, and the genus of the equations is supposed not less than one.
>
> ....
>
> (3) The equation
>
> $$ax^6 + bx^5y + \dots fxy^5 + gy^6 = z^2$$
>
> can be satisfied by only a finite number of *rational* values of x and y with the obvious extension to equations of higher degree.
>
> (4) The same theorem holds for the equation
>
> $$ax^4 + by^4 + cz^4 + 2fy^2z^2 + 2gz^2x^2 + 2hx^2y^2 = 0.$$
>
> (5) The same theorem holds for any homogeneous equation of genus greater than unity, say, $f(x, y, z) = 0$.

Statement (5) became known as Mordell's conjecture. In this part of the course, we discuss Faltings's famous paper which, among other things, proves Mordell's conjecture. In the years since it was published, there have been some improvements and simplifications.

Throughout, "(algebraic) number field" will mean a finite extension of $\mathbb{Q}$.

19. Introduction

Mordell's conjecture. It states:

> if C is a projective nonsingular curve of genus $g \geq 2$ over a number field k, then $C(k)$ is finite.

This was proved by Faltings in May/June 1983:

Clearly we can omit the "projective" — removing points only makes $C(k)$ smaller — and we can omit the "nonsingular" because the map $C' \to C$ from the desingularization (normalization) C' of C to C induces a map $C'(k) \to C(k)$ that becomes bijective when a finite number of points are removed from $C'(k)$ and $C(k)$. However, one must be careful to check that the genus of the *associated complete nonsingular curve* is ≥ 2.

We illustrate this by examining when Faltings's theorem implies that the equation

$$F(X, Y, Z) = \Sigma_{i+j+k=n}\, a_{ijk}\, X^iY^jZ^k = 0,\ a_{ijk} \in k$$

has only finitely many solutions in k (counted in the sense of projective geometry).

[11]Mordell, L.J., On the rational solutions of the indeterminate equations of third and fourth degrees, Proc. Camb. Philos. Soc. 21 (1922), 179–192.

First we need to assume that $F(X,Y,Z)$ is absolutely irreducible, i.e., that it is irreducible and remains so over every extension of k. This is not a serious restriction, because $F(X,Y,Z)$ will factor into absolutely irreducible polynomials over a finite extension k' of k, and we can replace F with one of the factors and k with k'. Thus, we may suppose that $F(X,Y,Z)$ defines a complete geometrically irreducible curve over k. The genus of the associated nonsingular curve is

$$g = \frac{(n-1)(n-2)}{2} - \Sigma\, n_P$$

(Plücker's formula)[12] where the sum is over the singular points on the curve $F(X,Y,Z) = 0$ with coordinates in $\mathbb{C}$. There are formulas for n_P. For example, if P is an ordinary singularity with multiplicity m (AG p61), then

$$n_P = m(m-1)/2.$$

If $g \geq 2$, then Faltings's theorem states that $C(k)$ is finite. For example, the Fermat curve

$$X^n + Y^n = Z^n, \quad n \geq 4,$$

has only finitely many solutions in any number field (up to multiplication by a constant).

If $g = 1$, then either $C(k)$ is empty or there is a map

(finitely generated abelian group) $\to C(k)$

that becomes bijective when a finite number of points are removed from each of the curves. For example, over $\mathbb{Q}[\sqrt[3]{D}]$ for a certain D, the points on

$$X^3 + Y^3 = Z^3$$

form an abelian group of rank ≥ 3. [??]

If $g = 0$, then either $C(k)$ is empty, or there is a map $\mathbb{P}^1(k) \to C(k)$ that becomes bijective when a finite number of points are removed from each of the curves. For example, for the curve

$$X^2 + Y^2 = Z^2$$

there is a bijection

$$\mathbb{P}^1(k) \to C(k), \quad (t:u) \mapsto (t^2 - u^2 : 2tu : t^2 + u^2).$$

There is an algorithm for deciding whether a curve of genus 0 over $\mathbb{Q}$ has a rational point. Thus, except for $g = 1$, we have an algorithm for deciding whether $C(k)$ is finite — therefore, $g = 1$ is the interesting case!

It is possible to give a bound for $\#C(k)$ — this is not entirely clear from Faltings's approach, but it is clear from the Vojta-Faltings-Bombieri approach. However, there is at present no algorithm for finding all the points on C. For this, one would need an effective bound on the heights of the points on C (for a point $P = (x:y:z) \in \mathbb{P}^2(\mathbb{Q})$, $H(P) = \max(|x|,|y|,|z|)$ where x,y,z are chosen to be relatively prime integers). With such a bound N, one would only need to check whether each of the finitely many points P with $H(P) \leq N$ lies on C. Finding an effective bound on the heights appears to be an extremely difficult problem: for example, it was only in

[12] See Fulton, W., Algebraic Curves, Benjamin, 1969, p199 for a proof of Plücker's formula in the case that C has only ordinary singularities.

the 1960's that Baker showed that there was a bound on the heights of the integer solutions of $Y^2 = X^3 + k$ (for which he received the Fields medal).

Heuristic argument for the conjecture. Let C be a complete nonsingular curve over a number field k, and let J be its Jacobian variety. If $C(k)$ is empty, then it is certainly finite. Otherwise there is an embedding $C \hookrightarrow J$. Consider the diagram:

$$\begin{array}{ccc} C(\mathbb{C}) & \hookrightarrow & J(\mathbb{C}) \\ \uparrow & & \uparrow \\ C(k) = C(\mathbb{C}) \cap J(k) & \hookrightarrow & J(k) \end{array}$$

According to the Mordell-Weil theorem, $J(k)$ is a finitely generated group, and if $g \geq 2$, then

$$\dim C(\mathbb{C}) < \dim J(\mathbb{C}).$$

Since there is no reason to expect any relation between $C(\mathbb{C})$ and $J(k)$ as subsets of $J(\mathbb{C})$, and both are sparse, $C(\mathbb{C}) \cap J(k)$ should be finite. People have tried to make this into a proof, but without success[13].

Finiteness I and its Consequences. Most of the main theorems of Faltings's paper follow from the following elementary statement.

THEOREM 19.1 (Finiteness I). *Let A be an abelian variety over an algebraic number field k. Then, up to isomorphism, there are only finitely many abelian varieties B over k that are isogenous to A.*

In other words, the abelian varieties over k isogenous to A fall into only finitely many isomorphism classes. At first sight, this statement is rather surprising. Let $\alpha \colon A \to B$ be an isogeny. Then $N \stackrel{\text{df}}{=} \operatorname{Ker}(\alpha)$ is a finite subgroup variety of A, and $N(k^{\text{al}})$ is a finite subgroup of $A(k^{\text{al}})$ stable under the action of . Conversely, from every finite subgroup N of $A(k^{\text{al}})$ stable under $\operatorname{Gal}(k^{\text{al}}/k)$ we get an isogeny $A \to A/N$. Clearly, there are infinitely many possible N's, but of course there may be isomorphisms $A/N \approx A/N'$; for example, $A \approx A/A_n$, $A_n = \operatorname{Ker}(A \xrightarrow{n} A)$. The theorem is a rather strong statement about the absence of exotic finite subgroups of $A(k^{\text{al}})$ stable under $\operatorname{Gal}(k^{\text{al}}/k)$, and about the existence of isomorphisms between the quotients A/N.

Finiteness I implies the following theorems:

THEOREM 19.2 (Semisimplicity). *Let A be an abelian variety over a number field k; for all primes ℓ, the action of $\operatorname{Gal}(k^{al}/k)$ on $V_\ell A$ is semisimple.*

THEOREM 19.3 (Tate's conjecture). *For abelian varieties A and B over a number field k, the map*

$$\operatorname{Hom}(A, B) \otimes \mathbb{Z}_\ell \to \operatorname{Hom}(T_\ell A, T_\ell B)^\Gamma,\ \Gamma = \operatorname{Gal}(k^{al}/k),$$

is bijective.

THEOREM 19.4 (Finiteness II). *Given a number field k, an integer g, and a finite set of finite primes S of k, there are only finitely many isomorphism classes of abelian varieties A over k of dimension g having good reduction outside S.*

[13] There has been progress on these questions since the notes were written.

For elliptic curves, Finiteness II was proved by Shafarevich — see Silverman 1986, IX, Theorem 6.1. Faltings's proof is (necessarily) completely different.

That $V_\ell A$ is a semisimple Γ-module means that every subspace W of $V_\ell A$ stable under the action of Γ has a complement W' also stable under Γ, i.e., $V_\ell A = W \oplus W'$ with W' Γ-stable. This implies that $V_\ell A$ is a direct sum of simple $\mathbb{Q}_\ell[\Gamma]$-modules (i.e., subspaces stable under Γ with no nontrivial Γ-stable subspaces).

The action of a finite group on a finite-dimensional vector space over a field of characteristic zero is automatically semisimple (see 9.2). Essentially the same proof as in (9.2) shows that the action of a compact group on a finite-dimensional vector space over $\mathbb{R}$ is semisimple (replace $\sum g\psi$ with $\int g\psi$). However, this is *not* true for a compact group acting on a finite-dimensional vector space over $\mathbb{Q}_\ell$. For example the action of the compact group

$$\Gamma = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid ac = 1, \quad a, b, c \in \mathbb{Z}_\ell\}$$

on $\mathbb{Q}_\ell^2$ is not semisimple because $\{\begin{pmatrix} * \\ 0 \end{pmatrix}\}$ is a Γ-stable subspace having no Γ-stable complement.

The Tate conjecture has been discussed already in (9.17). Faltings's methods also allow one to prove it for a field k finitely generated over $\mathbb{Q}$. It was known (Zarhin, Izv. 1975) that Finiteness II implies the Tate conjecture. Faltings turned things around by

(i) proving a weak form of Finiteness II;

(ii) proving the Tate conjecture;

(iii) deducing Finiteness II.

Finiteness II implies the following result:

THEOREM 19.5 (Shafarevich's conjecture). *Given a number field k, an integer g, and a finite set of finite primes S of k, there are only finitely many isomorphism classes of nonsingular complete curves C over k of genus g having good reduction outside S.*

This is proved by applying Finiteness II to the Jacobians of the curves (see later).

In 1968, Parshin showed that Shafarevich's conjecture implies Mordell's conjecture. The idea of the proof is to attach to a point P in $C(k)$ a covering

$$\varphi_P \colon C_P \to C_{k'}$$

where

(a) (C_P, φ_P) is defined over a fixed finite extension k' of k,
(b) C_P has bounded genus,
(c) C_P has good reduction outside a fixed finite set of primes of k',
(d) φ_P is ramified exactly at P.

The statements (a),(b),(c) and Shafarevich's conjecture show that there are only finitely many curves C_P, and (d) shows that the map $P \mapsto (C_P, \varphi_P)$ is injective. Finally, a classical theorem of de Franchis states that, for fixed C' and C, there can be only finitely many surjective maps $C' \to C$ when C has genus ≥ 2, and so $P \mapsto C_P$ is finite-to-one. (This is the *only* place in the argument that $g \geq 2$ is used!)

The proof of Finiteness I. Here I briefly sketch the proof of Finiteness I. In the next section, we define the notion of semistable reduction for an abelian variety (it is weaker than good reduction), and we note that an abelian variety acquires semistable reduction at every prime after a finite extension of the ground field.

Given an abelian variety A over a number field, Faltings attaches a real number, $h(A)$ to A, called the *Faltings height* of A. The Faltings heights of two isogenous abelian varieties are related, and Faltings proved:

THEOREM 19.6. *Let A be an abelian variety with semistable reduction over a number field k. The set*

$$\{h(B) \mid B \text{ is isogenous to } A\}$$

is finite.

There is natural notion of the height of a point in $\mathbb{P}^n(k)$, namely, if $P = (a_0 : \cdots : a_n)$, then

$$H(P) = \Pi_v \max_i(|a_i|_v).$$

Here the v's run through all primes of k (including the archimedean primes) and $|\cdot|_v$ denotes the normalized valuation corresponding to v. Note that

$$\Pi_v \max_i(|ca_i|_v) = (\Pi_v \max_i(|a_i|_v))(\Pi_v |c|_v) = \Pi_v \max_i(|a_i|_v)$$

because the product formula shows that $\Pi_v |c|_v = 1$. Therefore $H(P)$ is independent of the choice of a representative for P. When $k = \mathbb{Q}$, we can represent P by an n-tuple $(a_0 : \ldots : a_n)$ with the a_i relatively prime integers. Then $\max_i(|a_i|_p) = 1$ for all prime numbers p, and so the formula for the height becomes

$$H(P) = \max_i |a_i| \text{ (usual absolute value).}$$

A fundamental property of heights is that, for any integer N,

$$\mathrm{Card}\{P \in \mathbb{P}^n(k) \mid H(P) \leq N\}$$

is finite. When $k = \mathbb{Q}$, this is obvious.

Using heights on projective space, it is possible to attach another height to an abelian variety. There is a variety V (the *Siegel modular variety*) over $\mathbb{Q}$ that parametrizes isomorphism classes of principally polarized abelian varieties of a fixed dimension g. It has a canonical class of embeddings into projective space

$$V \hookrightarrow \mathbb{P}^n.$$

An abelian variety A over k corresponds to a point $v(A)$ in $V(k)$, and we define the *modular height* of A to be

$$H(A) = H(v(A)).$$

We know that the set of isomorphism classes of principally polarized abelian varieties over k of fixed dimension and bounded modular height is finite.

Note that if we ignore the "principally polarized" in the last statement, and the "semistable" in the last theorem, then they will imply Finiteness I once we relate the two notions of height. Both heights are "continuous" functions on the Siegel modular variety, which has a canonical compactification. If the difference of the two functions h and H extended to the compact variety, then it would be bounded, and we would have proved Finiteness I. Unfortunately, the proof is not that easy, and the hardest part of Faltings's paper is the study of the singularities of the functions as they approach the boundary. One thing that makes this especially difficult is that, in order to control the contributions at the finite primes, this has to be done over $\mathbb{Z}$, i.e., one has to work with a compactification of the Siegel modular *scheme* over $\mathbb{Z}$.

References. The original source is:

Faltings, G., Endlichkeitssätze für Abelsche Varietäten über Zahlkörpern, Invent. Math. 73 (1983), 349-366; Erratum, ibid. 1984, 75, p381. (There is a translation: Finiteness Theorems for Abelian Varieties over Number Fields, in "Arithmetic Geometry" pp 9–27.)

Mathematically, this is a wonderful paper; unfortunately, the exposition, as in all of Faltings's papers, is poor.

The following books contain background material for the proof:

Serre: Lectures on the Mordell-Weil theorem, Vieweg, 1989.

Arithmetic Geometry (ed. Cornell and Silverman), Springer, 1986 (cited as **Arithmetic Geometry**).

There are two published seminars expanding on the paper:

Faltings, G., Grunewald, F., Schappacher, N., Stuhler, U., and Wüstholz, G., Rational Points (Seminar Bonn/Wuppertal 1983/84), Vieweg 1984.

Szpiro, L., et al. Séminaire sur les Pinceaux Arithmétique: La Conjecture de Mordell, Astérisque 127, 1985.

Although it is sketchy in some parts, the first is the best introduction to Faltings's paper. In the second seminar, the proofs are very reliable and complete, and they improve many of the results, but the seminar is very difficult to read.

There are two Bourbaki talks:

Szpiro, L., La Conjecture de Mordell, Séminaire Bourbaki, 1983/84.

Deligne, P., Preuve des conjectures de Tate et Shafarevitch, ibid.

There is a summary of part of the theory in:

Lang, S., Number Theory III, Springer, 1991, Chapter IV.

Faltings's proofs depend heavily on the theory of Néron models of abelian varieties and the compactification of Siegel modular varieties over $\mathbb{Z}$. Recently books have appeared on these two topics:

Bosch, S., Lütkebohmert, W., and Raynaud, M., Néron Models, Springer, 1990.

Chai, Ching-Li and Faltings, G., Degeneration of Abelian Varieties, Springer, 1990.

20. Néron models; Semistable Reduction

Let R be a discrete valuation ring with field of fractions K and residue field k. Let π be a prime element of R, so that $k = R/(\pi)$. We wish to study the reduction[14] of an elliptic curve E over K. For simplicity, we assume $p \neq 2, 3$. Then E can be described by an equation

$$Y^2 = X^3 + aX + b,\ \Delta \stackrel{\text{df}}{=} 4a^3 + 27b^2 \neq 0.$$

By making the substitutions $X \mapsto X/c^2$, $Y \mapsto Y/c^3$, we can transform the equation to

$$Y^2 = X^3 + ac^4X + bc^6,$$

and this is essentially the only way we can transform the equation. A *minimal equation* for E is an equation of this form with $a, b \in R$ for which $ord(\Delta)$ is a minimum. A minimal equation is unique up to a transformation of the form

$$(a, b) \mapsto (ac^4,\ bc^6),\ c \in R^{\times}.$$

Choose a minimal equation for E, and let E_0 be the curve over k defined by the equation mod (π). There are three cases:

(a) E_0 is nonsingular, and is therefore is an elliptic curve. This occurs when $\text{ord}(\Delta) = 0$. In this case, we say that E has *good reduction.*
(b) E_0 has a node. This occurs when $\pi|\Delta$ but does not divide both a and b. In this case $E_0(k)_{nonsing} \stackrel{\text{df}}{=} E_0(k) - \{\text{node}\}$ is isomorphic to $k^{\times}$ as an algebraic group (or becomes so after a quadratic extension of k), and E is said to have *multiplicative reduction.*
(c) E_0 has a cusp. This occurs when π divides both a and b (and hence also Δ). In this case $E_0(k)_{nonsing}$ is isomorphic to k^{+}, and E is said to have *additive reduction.*

The curve E is said to have *semistable reduction* when either (a) or (b) occurs. Now suppose we extend the field from K to L, $[L : K] < \infty$, and choose a discrete valuation ring S with field of fractions L such that $S \cap K = R$. When we pass from K to L, the minimal equation of E remains minimal in cases (a) and (b), but it may change in case (c). For a suitable choice of L, case (c) will become either case (a) or case (b). In other words, if E has good reduction (or multiplicative) reduction over K, then the reduction stays good (or multiplicative) over every finite extension L; if E has additive reduction, then the reduction can stay additive or it may become good or multiplicative over an extension L, and for a suitable extension it will become good or multiplicative.

The proof of the statement is elementary. For example, suppose E has additive reduction, and adjoin a sixth root ϖ of π to K. Then we can replace the equation by

$$Y^2 = X^3 + (a/\varpi^4)X + (b/\varpi^6).$$

If both $ord_L(a/\varpi^4) > 0$ and $ord_L(b/\varpi^6) > 0$, then continue....

These statements extend to abelian varieties, but then become much more difficult to prove.

[14]For another discussion of the Néron models of elliptic curves, see EC §9.

THEOREM 20.1 (Néron). *Let A be an abelian variety over a field K as above. Then there is a canonical way to attach to A an algebraic group A_0 over k.*

REMARK 20.2. In fact Néron proves the following: the functor from smooth schemes over R,

$$S \mapsto \mathrm{Hom}_{Spec\ R}(S, A)$$

is representable by a smooth group scheme $\mathcal{A}$ over R. The scheme $\mathcal{A}$ is unique (because of the Yoneda lemma–see 17.1), and we set $A_0 = \mathcal{A} \times_{Spec\ R} \mathrm{Spec}\ k$. The scheme $\mathcal{A}$ is called the Néron model of A.

A general theorem on algebraic groups shows that A_0 has a filtration:

$$A_0 \supset (A_0)^0 \supset (A_0)^1 \supset 0$$

with $A_0/(A_0)^0$ a finite algebraic group ($(A_0)^0$ is the connected component of A_0 containing the identity element), $(A_0)^0/(A_0)^1$ an abelian variety, and $(A_0)^1$ a commutative affine group scheme. Again there are three cases to consider:

(a) A_0 is an abelian variety. In this case A is said to have *good reduction.*
(b) $(A_0)^1$ is a torus[15] , i.e., after a finite extension of k, $(A_0)^1$ becomes isomorphic to a product of copies $\mathbb{A}^1 - \{0\} = k^\times$.
(c) $(A_0)^1$ contains copies of $\mathbb{A}^1 = k^+$.

The abelian variety A is said to have *semistable reduction* in case (a) or (b).

THEOREM 20.3. *If A has good reduction, then A_0 doesn't change under a finite field extension; if A has semistable reduction, then $(A_0)^0$ doesn't change under a finite field extension; A always acquires semistable reduction after a finite extension.*

The proofs of these theorems are long and quite difficult. Fortunately, for most purposes one only needs the statements, and these are very believable given what is true for elliptic curves.

References. The original paper of Néron (Publ. Math. IHES 21, 1964) is almost unreadable, because it is written in a private language (a relative version of Weil's language). The article of M. Artin in "Arithmetic Geometry" is too concise. In view of this, the book by Bosch, Lütkebohmert, and Raynaud is invaluable. It gives a very complete and detailed treatment of the topic.

21. THE TATE CONJECTURE; SEMISIMPLICITY.

In this section, we prove that Tate's conjecture is implied by Finiteness I. Throughout the section, k is a field and $\Gamma = \mathrm{Gal}(k^{\mathrm{al}}/k)$. We begin with some elementary lemmas.

LEMMA 21.1. *If $\alpha \colon A \to B$ is an isogeny of degree prime to char k, then $\mathrm{Ker}(\alpha)(k^{al})$ is a finite subgroup of $A(k^{al})$ stable under the action of Γ; conversely, every such subgroup arises as the kernel of such an isogeny, i.e., the quotient A/N exists over k.*

[15]This notion should not be confused with that of a complex torus discussed in §2.

PROOF. Over k^{al}, this follows from (7.10). The only additional fact needed is that, if $N(k^{\mathrm{al}})$ is stable under the action of Γ, then the quotient A/N is defined over k. $\square$

LEMMA 21.2. *(a) For any abelian variety A and $\ell \neq char(k)$, there is an exact sequence*

$$0 \to T_\ell A \xrightarrow{\ell^n} T_\ell A \to A_{\ell^n}(k^{al}) \to 0.$$

(b) An isogeny $\alpha\colon A \to B$ of degree prime to char(k) defines an exact sequence

$$0 \to T_\ell A \to T_\ell B \to C \to 0$$

with the order of C equal to the power of ℓ dividing $\deg(\alpha)$..

PROOF. (a) This follows easily from the definition

$$T_\ell A = \{(a_n)_{n\geq 1} |\ a_n \in A_{\ell^n}(k^{\mathrm{al}}), \quad \ell a_n = a_{n-1}, \quad \ell a_1 = 0\}.$$

(b) To prove this, consider the following infinite diagram:

$$\begin{tikzcd}
 & & {} & {} & & \\
0 \arrow[r] & K_n \arrow[r] & B_{\ell^n}(k^{\mathrm{al}}) \arrow[u, "\ell"'] \arrow[r, "\alpha"] & A_{\ell^n}(k^{\mathrm{al}} \arrow[u, "\ell"'] \arrow[r] & C_n \arrow[r] & 0 \\
0 \arrow[r] & K_{n+1} \arrow[u, "\ell"'] \arrow[r] & B_{\ell^{n+1}}(k^{\mathrm{al}}) \arrow[u, "\ell"'] \arrow[r, "\alpha"] & A_{\ell^{n+1}}(k^{\mathrm{al}}) \arrow[u, "\ell"'] \arrow[r] & C_{n+1} \arrow[u] \arrow[r] & 0 \\
 & & {} \arrow[u, "\ell"'] & {} \arrow[u, "\ell"'] & &
\end{tikzcd}$$

For n sufficiently large, $K_n = K_{n+1} = \ldots = K$, say. Because K is finite, it has no element divisible by all powers of ℓ, and so

$$\varprojlim K_n \overset{\mathrm{df}}{=} \{(a_n) |\ a_n \in K_n,\ \ell a_n = a_{n-1},\ \ell a_1 = 0\}$$

is zero. Since $\#B_{\ell^n}(k^{\mathrm{al}}) = (\ell^n)^{2g} = \#A_{\ell^n}(k^{\mathrm{al}})$, we must have $\#K_n = \#C_n$. Therefore $\#C_n$ is constant for n large. The map $C_{n+1} \to C_n$ is surjective; therefore for n large it is bijective, and it follows that $\varprojlim C_m \to C_n$ is a bijection for all large n. On passing to the inverse limit we get an exact sequence

$$0 \to T_\ell B \to T_\ell A \to C \to 0$$

as required. $\square$

Let $\alpha\colon B \to A$ be an isogeny. Then the image of $T_\ell\alpha\colon T_\ell B \to T_\ell A$ is Γ-stable $\mathbb{Z}_\ell$-module of finite index in $T_\ell A$. Our final elementary lemma shows that every such submodule arises from an isogeny α, and even that α can be taken to have degree a power of ℓ.

LEMMA 21.3. *Assume $\ell \neq char(k)$. For any Γ-stable submodule W of finite index in $T_\ell A$, there an abelian variety B and an isogeny $\alpha\colon B \to A$ of degree a power of ℓ such that $\alpha(T_\ell B) = W$.*

PROOF. Choose n so large that $W \supset \ell^n T_\ell A$, and let N be the image of W in $T_\ell A/\ell^n T_\ell A = A_{\ell^n}(k^{\mathrm{al}})$. Then N is stable under the action of Γ, and we define $B = A/N$. Because $N \subset A_{\ell^n}$, the map $\ell^n\colon A \to A$ factors through $A \to A/N$:

$$\begin{tikzcd} A \arrow[rr, "\ell^n"] \arrow[dr, "\beta"'] & & A \\ & A/N \;= B \arrow[ur, "\alpha"'] & \end{tikzcd}$$

It remains to show that $Im(T_\ell\alpha\colon T_\ell B \to T_\ell A) = W$. From the diagram

$$\begin{tikzcd} T_\ell A \arrow[rr, "\ell^n"] \arrow[dr, "T_\ell\beta"'] & & T_\ell A \\ & T_\ell B \arrow[ur, "T_\ell\alpha"'] & \end{tikzcd}$$

it is clear that $Im(T_\ell\alpha) \supset \ell^n T_\ell A$, and so it suffices to show that the image of $Im(T_\ell\alpha)$ in $T_\ell A/\ell^n T_\ell A = A_{\ell^n}(k^{\mathrm{al}})$ is N. But

$$B(k^{\mathrm{al}})_{\ell^n} = \{a \in A(k^{\mathrm{al}}) \mid \ell^n a \in N\}/N,$$

and if $b \in B(k^{\mathrm{al}})_{\ell^n}$ is represented by $a \in A(k^{\mathrm{al}})$, then $\alpha(b) = \ell^n a$. It is now clear that α maps $B(k^{\mathrm{al}})_{\ell^n}$ onto N. $\square$

Let A be an abelian variety over a field k, and let ℓ be a prime $\neq$ *char* k. Consider the following condition (slightly weaker than Finiteness I):

> (*) up to isomorphism, there are only finitely many abelian varieties B isogenous to A by an isogeny of degree a power of ℓ.

LEMMA 21.4. *Suppose A satisfies (*). For any $W \subset V_\ell A$ stable under Γ, there is a $u \in \mathrm{End}(A) \otimes \mathbb{Q}_\ell$ such that $uV_\ell A = W$.*

PROOF. Set $T_\ell = T_\ell A$ and $V_\ell = V_\ell A$. Let

$$X_n = (T_\ell \cap W) + \ell^n T_\ell.$$

This is a $\mathbb{Z}_\ell$-submodule of T_ℓ stable under Γ and of finite index in T_ℓ. Therefore, there is an isogeny

$$f_n\colon B(n) \to A, \text{ such that } \; f_n(T_\ell B(n)) = X_n.$$

According to (*), the $B(n)$ fall into only finitely many distinct isomorphism classes, and so at least one class has infinitely many $B(n)$'s: there is an infinite set I of positive integers such that all the $B(i)$ for $i \in I$ are isomorphic. Let i_0 be the smallest element of I. For each $i \in I$, choose an isomorphism $v_i\colon B(i_0) \to B(i)$, and consider:

$$\begin{array}{ccc} B(i_0) & \xrightarrow{v_i} & B(i) \\ \downarrow{\scriptstyle f_{i_0}} & & \downarrow{\scriptstyle f_i} \\ A & & A \end{array} \qquad \begin{array}{ccc} T_\ell B(i_0) & \longrightarrow & T_\ell B(i) \\ \approx\downarrow{\scriptstyle f_{i_0}} & & \approx\downarrow{\scriptstyle f_i} \\ X_{i_0} & & X_i \end{array}$$

Because f_{i_0} is an isogeny, $u_i \stackrel{\text{df}}{=} f_i v_i {f_{i_0}}^{-1}$ makes sense as an element of $\mathrm{End}(A) \otimes \mathbb{Q}$, and hence as an element of $\mathrm{End}(A) \otimes \mathbb{Q}_\ell$. Moreover, it is clear from the second diagram that $u_i(X_{i_0}) = X_i$. Because $X_i \subset X_{i_0}$, the u_i for $i \in I$ are in the *compact* set $\mathrm{End}(X_{i_0})$, and so, after possibly replacing (u_i) with a subsequence, we can assume (u_i) converges to a limit u in $\mathrm{End}(X_{i_0}) \subset \mathrm{End}(V_\ell A)$. Now $\mathrm{End}(A) \otimes \mathbb{Q}_\ell$ is a subspace of $\mathrm{End}(V_\ell A)$, and hence is closed. Since each u_i lies in $\mathrm{End}(A) \otimes \mathbb{Q}_\ell$, so also does their limit u.

For any $x \in X_{i_0}$, $u(x) = \lim\ u_i(x) \subset \cap X_i$. Conversely, if $y \in \cap X_i$, then there exists for each $i \in I$, an element $x_i \in X_{i_0}$ such that $u_i(x_i) = y$. From the compactness of X_{i_0} again, we deduce that, after possibly replacing I with a subset, the sequence (x_i) will converge to a limit $x \in X_{i_0}$. Now $u(x) = \lim u(x_i) = \lim u_i(x_i) = y$. Thus $u(X_{i_0}) = \cap X_j = T_\ell \cap W$, and it follows that $u(V_\ell A) = W$. □

Before proving the main theorem of this section, we need to review a little of the theory of noncommutative rings (CFT, Chapter IV). By a k-algebra, I will mean a ring R, not necessarily commutative, containing k in its centre and of finite dimension over k, and by an R-module I'll mean an R-module that is of finite dimension over k. If R has a faithful semisimple module, then every R-module is semisimple, and the k-algebra R is said to be *semisimple*. A simple k-algebra, i.e., a k-algebra with no two-sided ideals except for the obvious two, is semisimple (CFT 1.14) and a theorem of Wedderburn says that, conversely, a semisimple k-algebra is a finite product of simple k-algebras.

Another theorem of Wedderburn (CFT IV.1.9) says that every simple k-algebra is isomorphic to $M_n(D)$ for some n and some division k-algebra D.

Let D be a division algebra over k. The right ideals in $M_n(D)$ are the sets of the form $\mathfrak{a}(J)$ with $J \subset \{1, 2, \dots, n\}$ and $\mathfrak{a}(J)$ the set of matrices whose j^{th} columns are zero for $j \notin J$ (CFT IV.1.6). Note that $\mathfrak{a}(J)$ is generated by the idempotent $e = diag(a_1, \dots, a_n)$ with $a_j = 1$ for $j \in J$ and $a_j = 0$ otherwise. On combining this remark with the Wedderburn theorems, we find that every right ideal in a semisimple k-algebra R is generated by an idempotent: $\mathfrak{a} = eR$ for some e with $e^2 = e$.

The *centralizer* $C_E(R)$ of subalgebra R of a k-algebra E consists of the elements γ of E such that $\gamma\alpha = \alpha\gamma$ for all $\alpha \in R$. Let R be a k-algebra and let $E = \mathrm{End}_k(V)$ for some faithful semisimple R-module V; the Double Centralizer Theorem (CFT IV.1.11) says that $C_E(C_E(R)) = R$.

If R is a semisimple k-algebra, then $R \otimes_k k'$ need not be semisimple — for example, if $R = k[\alpha]$ with $\alpha^p \in k$, $\alpha \notin k$, then $R \otimes_k k^{\text{al}}$ contains the nilpotent element $\alpha \otimes 1 - 1 \otimes \alpha$. However, this only happens in characteristic p: if k is of characteristic 0, then R semisimple $\implies R \otimes_k k'$ semisimple.

Let A be an abelian variety. Then $\mathrm{End}(A) \otimes \mathbb{Q}$ is a finite-dimensional algebra over $\mathbb{Q}$ (9.14), and it is isomorphic to a product of matrix algebras over division algebras (see the first subsection of §9). It is, therefore, a semisimple $\mathbb{Q}$-algebra.

THEOREM 21.5. *Let A be an abelian variety over k, and assume that $A \times A$ and A satisfy (*) for some $\ell \neq char(k)$. Then*

(a) *$V_\ell A$ is a semisimple $\mathbb{Q}_\ell[\Gamma]$-module.*
(b) $\mathrm{End}(A) \otimes \mathbb{Q}_\ell = \mathrm{End}(V_\ell A)^\Gamma$.

PROOF. (a) Let W be a Γ-subspace of $V_\ell A$ — we have to construct a complement W' to W that is stable under Γ. Let

$$\mathfrak{a} = \{u \in \mathrm{End}(A) \otimes \mathbb{Q}_\ell \mid uV_\ell A \subset W\}.$$

This is a right ideal in $\mathrm{End}(A) \otimes \mathbb{Q}_\ell$, and $\mathfrak{a}V_\ell A = W$ because the hypothesis on A and (21.4) imply there exists a $u \in \mathrm{End}(A) \otimes \mathbb{Q}_\ell$ such that $uV_\ell A = W$. From the above remarks, we know that $\mathfrak{a}$ is generated by an idempotent e, and clearly $eV_\ell = W$. Because e is idempotent

$$V_\ell A = eV_\ell A \oplus (1-e)V_\ell A = W \oplus W'.$$

Since the elements of Γ commute with the elements of $\mathrm{End}(A) \otimes \mathbb{Q}_\ell$, $W' \overset{\mathrm{df}}{=} (1-e)V_\ell A$ is stable under the action of Γ.

(b) Let C be the centralizer of $\mathrm{End}(A) \otimes \mathbb{Q}_\ell$ in $\mathrm{End}(V_\ell A)$, and let B be the centralizer of C. Because $\mathrm{End}(A) \otimes \mathbb{Q}_\ell$ is semisimple, $B = \mathrm{End}(A) \otimes \mathbb{Q}_\ell$.

Consider $\alpha \in \mathrm{End}(V_\ell A)^\Gamma$ — we have to show that $\alpha \in B$. The graph of α

$$W \overset{\mathrm{df}}{=} \{(x, \alpha x) \mid x \in V_\ell A\}$$

is a Γ-invariant subspace of $V_\ell A \times V_\ell A$, and so there is a $u \in \mathrm{End}(A \times A) \otimes \mathbb{Q}_\ell = M_2(\mathrm{End}(A)) \otimes \mathbb{Q}_\ell$ such that $u(V_\ell(A \times A)) = W$. Let $c \in C$. Then $\begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} \in \mathrm{End}(V_\ell A \times V_\ell A)$ commutes with $\mathrm{End}(A \times A) \otimes \mathbb{Q}_\ell$, and, in particular, with u. Consequently,

$$\begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} W = \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} uV_\ell A = u \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} V_\ell A \subset W.$$

This says that, for any $x \in V_\ell A$, $(cx, c\alpha x) \in W$ =graph of α. Thus α maps cx to $c\alpha x$, i.e., $\alpha cx = c\alpha x$. Thus $c\alpha = \alpha c$, and since this holds for all c, $\alpha \in B = \mathrm{End}(A) \otimes \mathbb{Q}_\ell$. □

COROLLARY 21.6. *Assume (*) holds for abelian varieties over k. Then the map*

$$\mathrm{Hom}(A, B) \otimes \mathbb{Q}_\ell \to \mathrm{Hom}(V_\ell A, V_\ell B)^\Gamma$$

is an isomorphism.

PROOF. Consider the diagram of finite-dimensional vector spaces over $\mathbb{Q}_\ell$:

$$\begin{array}{ccccccccc} \mathrm{End}(V_\ell(A \times B))^\Gamma & = & \mathrm{End}(V_\ell A)^\Gamma & \times & \mathrm{Hom}(V_\ell A, V_\ell B)^\Gamma & \times & \mathrm{Hom}(V_\ell B, V_\ell A)^\Gamma & \times & \mathrm{End}(V_\ell B)^\Gamma \\ \cup & & \cup & & \cup & & \cup & & \cup \\ \mathrm{End}(A \times B) \otimes \mathbb{Q}_\ell & = & \mathrm{End}(A) \otimes \mathbb{Q}_\ell & \times & \mathrm{Hom}(A, B) \otimes \mathbb{Q}_\ell & \times & \mathrm{Hom}(B, A) \otimes \mathbb{Q}_\ell & \times & \mathrm{End}(B) \otimes \mathbb{Q}_\ell. \end{array}$$

The theorem shows that the inclusion at left is an equality, and it follows that the remaining inclusions are also equalities. □

COROLLARY 21.7. *Let R be the image of $\mathbb{Q}_\ell[\Gamma]$ in $\mathrm{End}(V_\ell A)$. Then R is the centralizer of $\mathrm{End}(A) \otimes \mathbb{Q}_\ell$ in $\mathrm{End}(V_\ell A)$.*

PROOF. Theorem 21.5a shows that $V_\ell A$ is a semisimple R-module. As it is also faithful, this implies that R is a semisimple ring. The double centralizer theorem says that $C(C(R)) = R$, and (21.5b) says that $C(R) = \mathrm{End}(A) \otimes \mathbb{Q}_\ell$. On putting these statements together, we find that $C(\mathrm{End}(A) \otimes \mathbb{Q}_\ell) = R$. □

22. Geometric Finiteness Theorems

In this section we prove some finiteness theorems that hold for abelian varieties over any field k. As a corollary, we find that Finiteness I (and hence the Tate conjecture) holds over finite fields. The first theorem says that an abelian variety can be endowed with a polarization of a fixed degree d in only a finite number of essentially different ways.

Theorem 22.1. *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.*

Let (A, λ) and (A', λ') be polarized abelian varieties. From a homomorphism $\alpha\colon A \to A'$, we obtain a map

$$\alpha^*(\lambda') \stackrel{\text{df}}{=} \alpha^\vee \circ \lambda' \circ \alpha\colon A \to A^\vee.$$

When α is an isomorphism and $\alpha^*(\lambda') = \lambda$, we call α an *isomorphism* $(A, \lambda) \to (A', \lambda')$ of polarized abelian varieties.

The theorem can be restated as follows: Let $Pol(A)$ be the set of polarizations on A, and let $\mathrm{End}(A)^\times$ act on $Pol(A)$ by $u \mapsto u^\vee \circ \lambda \circ u$; then there are only finitely many orbits under this action.

Note that $\mathrm{End}(A)^\times = \mathrm{Aut}(A)$. If u is an automorphism of A, and $\mathcal{L}$ is an ample invertible sheaf on A, the $u^*\mathcal{L}$ is also an ample invertible sheaf, and $\lambda_{u^*\mathcal{L}} = u^\vee \circ \lambda_{\mathcal{L}} \circ u$; thus $\mathrm{End}(A)^\times$ *does* act on $Pol(A)$.

Fix a polarization λ_0 of A, and let $\dagger$ be the Rosati involution on $\mathrm{End}(A) \otimes \mathbb{Q}$ defined by λ_0. The map $\lambda \mapsto \lambda_0^{-1} \circ \lambda$ identifies $Pol(A)$ with a subset of the set $(\mathrm{End}(A) \otimes \mathbb{Q})^\dagger$ of elements of $\mathrm{End}(A) \otimes \mathbb{Q}$ fixed by $\dagger$. Because λ_0 is an isogeny, there exists an isogeny $\alpha\colon A^\vee \to A$ such that $\alpha \circ \lambda_0 = n$, some $n \in \mathbb{Z}$, and then $\lambda_0^{-1} = (n_A^{-1}) \circ \alpha$. Therefore the image of

$$Pol(A) \hookrightarrow (\mathrm{End}(A) \otimes \mathbb{Q})^\dagger$$

lies in $L \stackrel{\text{df}}{=} n^{-1}\,\mathrm{End}(A)$.

Let $\mathrm{End}(A)^\times$ act on $\mathrm{End}(A) \otimes \mathbb{Q}$ by

$$\alpha \mapsto u^\dagger \circ \alpha \circ u, \quad u \in \mathrm{End}(A)^\times, \quad \alpha \in \mathrm{End}(A) \otimes \mathbb{Q}.$$

Then L is stable under this action, and the map $Pol(A) \to \mathrm{End}(A) \otimes \mathbb{Q}$ is equivariant for this action, because $u^\vee \circ \lambda \circ u \mapsto \lambda_0^{-1} \circ u^\vee \circ \lambda \circ u = {\lambda_0}^{-1} \circ u^\vee \circ \lambda_0 \circ {\lambda_0}^{-1} \circ \lambda \circ u = u^\dagger \circ ({\lambda_0}^{-1}\lambda) \circ u$.

Note that $\deg({\lambda_0}^{-1} \circ \lambda) = \deg(\lambda_0)^{-1} deg(\lambda)$. Also (see 9.23), for an endomorphism α of A, $\deg(\alpha)$ is a fixed power of $\mathrm{Nm}(\alpha)$ (norm from $\mathrm{End}(A) \otimes \mathbb{Q}$ to $\mathbb{Q}$). Therefore, as λ runs through a subset of $Pol(A)$ of elements with bounded degrees, then ${\lambda_0}^{-1} \circ \lambda$ runs through a subset of L of elements with bounded norms. Thus the theorem is a consequence of the following number theoretic result.

Proposition 22.2. *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 that is stable under the action $\alpha \mapsto u^\dagger \alpha u$ of $R^\times$ on E. Then for any integer N, there are only* *finitely many orbits for the action of $R^\times$ on*

$$S = \{v \in L \mid \mathrm{Nm}(v) \leq N\},$$

i.e., $S/R^\times$ is finite.

An *order* in E is a subring R of E that is a full lattice, i.e., free of rank $\dim(E)$ over $\mathbb{Z}$. In the application, $R = \mathrm{End}(A)$.

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

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

THEOREM 22.3. *Up to isomorphism, an abelian variety A has only finitely many direct factors.*

PROOF. Let B be a direct factor of A, say, $A \approx B \times C$, and define e to be the composite

$$A \approx B \times C \overset{(b,c)\mapsto(b,0)}{\to} B \times C \approx A.$$

Then e is an idempotent (i.e., $e^2 = e$), and B is determined by e up to isomorphism because $B \cong \mathrm{Ker}(1-e)$. Conversely, for any idempotent e of $\mathrm{End}(A)$

$$A = \mathrm{Ker}(1-e) \times \mathrm{Ker}(e).$$

The map $e \mapsto \mathrm{Ker}(1-e)$ is a surjection

$$\{\text{idempotents in } \ \mathrm{End}(A)\} \to \{\text{direct factors of } \ A\}/\approx .$$

Let $u \in \mathrm{End}(A)^\times$. Then $e' = ueu^{-1}$ is also an idempotent in $\mathrm{End}(A)$, and u defines an isomorphism

$$\mathrm{Ker}(1-e) \to \mathrm{Ker}(1-e').$$

Therefore, we have a surjection

$$\{\text{idempotents in } \ \mathrm{End}(A)\}/\,\mathrm{End}(A)^\times \to \{\text{direct factors of } \ A\}/\approx,$$

and so the theorem is a consequence of the following number theoretic result. □

PROPOSITION 22.4. *Let E be a semisimple algebra of finite dimension over $\mathbb{Q}$, and let R be an order in E. Then*

$$\{\textit{idempotents in } \ R\}/R^\times$$

is finite (here $u \in R^\times$ acts by $e \mapsto ueu^{-1}$).

This proposition will again be proved using a general result from the reduction theory of arithmetic subgroups, which we now state.

THEOREM 22.5. *Let G be a reductive group over $\mathbb{Q}$, and let Γ be an arithmetic subgroup of $G(\mathbb{Q})$; let $G \to GL(V)$ be a representation of G on a $\mathbb{Q}$-vector space V, 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 Borel, A., Introduction aux Groupes Arithmétiques, 1958, 9.11. (The theorem is due to Borel and Harish-Chandra, but special cases of it were known to the ancients.) □

Remark 22.6. (a) By an algebraic group we mean an affine group variety. It is *reductive* if it has no closed normal connected subgroup U consisting of unipotent elements (i.e., elements such that $u^n = 1$ for some n). A connected algebraic group G is reductive if and only if the identity component Z^0 of its centre is a torus and G/Z^0 is a semisimple group. For example, GL_n is reductive. The group

$$B = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid ac \neq 0\}$$

is not reductive, because $U = \{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\}$ is a closed normal connected subgroup consisting of unipotent matrices.

(b) Let G be an algebraic group over $\mathbb{Q}$. Then G can be realized as a closed subgroup of $GL_n(\mathbb{Q})$ for some n (this is often taken to be the definition of an algebraic group). Let

$$GL_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) \mid \det(A) = \pm 1\}.$$

Then $GL_n(\mathbb{Z})$ is a group, and we let $\Gamma_0 = GL_n(\mathbb{Z}) \cap G(\mathbb{Q})$. A subgroup Γ of $G(\mathbb{Q})$ is said to be *arithmetic* if it is commensurable with Γ_0, i.e., if $\Gamma \cap \Gamma_0$ is of finite index in both Γ and Γ_0. One can show that, although Γ_0 depends on the choice of the embedding $G \hookrightarrow GL_n$, two embeddings give commensurable groups, and hence the notion of an arithmetic subgroup doesn't depend on the embedding. Let

$$\Gamma(N) = \{A \in G(\mathbb{Q}) \mid \ A \in M_n(\mathbb{Z}), \quad A \equiv I \bmod (N)\}.$$

Then $\Gamma(N)$ is a subgroup of finite index in Γ_0, and so it is arithmetic. An arithmetic subgroup of this type is said to be a *principal congruence subgroup*. [The congruence subgroup problem asks whether every arithmetic subgroup contains a congruence subgroup. It has largely been solved — for some groups G they do; for some groups G they don't.]

(c) By a representation of G on a vector space V we mean a homomorphism $G \to GL(V)$ of algebraic groups. We can regard V itself as an algebraic variety (the choice of a basis for V determines an isomorphism $V \approx \mathbb{A}^n$, $n = \dim(V)$), and we are given mapping of algebraic varieties

$$G \times V \to V.$$

If v is an element of V, then the orbit Gv is the image of the map

$$G \times \{v\} \to V,\ g \mapsto g \cdot v.$$

It is a constructible set, but it need not be closed in general. To check that the orbit is closed, one needs to check that

$$X(k^{\mathrm{al}}) = \{gv \mid g \in G(k^{\mathrm{al}})\}$$

is closed in $V \otimes k^{\mathrm{al}}$ ($\approx \mathbb{A}^n$). One should interprete $L \cap X$ as $L \cap X(k^{\mathrm{al}})$.

We give three applications of (22.5).

APPLICATION 22.7. Let $G = SL_n$, and let $\Gamma = SL_n(\mathbb{Z})$. Then G acts in a natural way on the space V of quadratic forms in n variables with rational coefficients,

$$V = \{\sum a_{ij}\ X_iX_j \mid a_{ij} \in \mathbb{Q}\} = \{\text{symmetric } \ n \times n \text{ matrices, coeffs in } \mathbb{Q}\},$$

— if $q(X) = XAX^{\mathrm{tr}}$, then $(gq)(X) = X \cdot gAg^{\mathrm{tr}} \cdot X^{\mathrm{tr}}$ — and Γ preserves the lattice L of such forms with integer coefficients. Let q be a quadratic form with nonzero discriminant d, and let X be the orbit of q, i.e., the image $G \cdot q$ of G under the map of algebraic varieties $g \mapsto g \cdot q \colon G \to V$. The theory of quadratic forms shows that $X(\mathbb{Q}^{\mathrm{al}})$ is equal to the set of all quadratic forms (with coefficients in $\mathbb{Q}^{\mathrm{al}}$) of discriminant d. Clearly this is closed, and so the theorem shows that $X \cap L$ contains only finitely many $SL_n(\mathbb{Z})$-orbits: the quadratic forms with integer coefficients and discriminant d fall into a finite number of proper equivalence classes.

APPLICATION 22.8. With the notations of (22.4), there exists an algebraic group G over $\mathbb{Q}$ with $G(\mathbb{Q}) = E^\times$ which is automatically reductive (this only has to be checked over $\mathbb{Q}^{\mathrm{al}}$; but $E \otimes \mathbb{Q}^{\mathrm{al}}$ is a product of matrix algebras, and so $G_{\mathbb{Q}^{\mathrm{al}}}$ is a product of GL_n's). Take Γ to be the arithmetic subgroup $R^\times$ of $G(\mathbb{Q})$, 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 again replace $\mathbb{Q}$ by $\mathbb{Q}^{\mathrm{al}}$ and assume E to be a product of matrix algebra; in fact, we may take $E = M_n(k)$. Then the argument in the proof of (4.3) shows that

$$\{\text{idempotents in } \ E\}/E^\times \cong \{\text{direct factors of } \ k^n\}/\approx .$$

But, up to isomorphism, there is only one direct factor of k^n for each dimension $\leq n$. Thus, each idempotent is conjugate to one of the form $e = diag(1, ..., 1, 0, ..., 0)$. If r is the number of 1's, then the orbit of e under $E^\times$ corresponds to the set of subspaces of k^n of dimension r. The latter is a Grassmann variety, which is complete (e.g., the orbit of $e = diag(1, 0, ..., 0)$ corresponds to the set of lines in k^n through the origin, i.e., with $\mathbb{P}^n$), and hence is closed when realized as a subvariety of any variety. Now we can apply Theorem 22.5 to obtain Proposition 22.4.

APPLICATION 22.9. With the notations of (22.2), let G be the algebraic group over $\mathbb{Q}$ such that

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

let $\Gamma = R^\times$, let $V = E$, and let $L \subset V$ the lattice in (4.2). One verifies:

(a) G is a reductive group having Γ as an arithmetic subgroup;
(b) the orbits of G on V are all closed;
(c) for any rational number d, $V_d =_{df} \{v \in V \mid \mathrm{Nm}(v) = d\}$ is the union of a finite number of orbits of G.

Then (22.5) shows that $L \cap V_d$ comprises only finitely many Γ-orbits, as is asserted by (22.1). For details, see AV, §18.

THEOREM 22.10 (Zarhin's trick). *For any abelian variety A, $A^4 \times (A^{\vee 4})$ is principally polarized.*

Since $(A \times A^\vee)^\vee = A^\vee \times A$, there is a canonical isomorphism $A \times A^\vee \to (A \times A^\vee)^\vee$. The problem is to show that there is such an isomorphism that is a polarization, i.e., of the form $\lambda_{\mathcal{L}}$ for some ample invertible sheaf $\mathcal{L}$ — for this we need to replace A with A^4. We sketch the proof of (22.10) (for more details, see AV, §18).

Recall from §16 that there is a canonical nondegenerate pairing

$$e\colon T_\ell A \times T_\ell A^\vee \to \mathbb{Z}_\ell.$$

For each $\lambda\colon A \to A^\vee$, we get a pairing

$$e^\lambda\colon T_\ell A \times T_\ell A \to \mathbb{Z}_\ell, (x, y) \mapsto e(x, \lambda y).$$

Let $\alpha\colon A \to B$ be an isogeny of degree prime to char(k). Let λ be a polarization of B, and let $\lambda' = \alpha^\vee \circ \lambda \circ \alpha\colon A \to A^\vee$; then λ' is a polarization of A, and

$$e^{\lambda'}(\alpha x, \alpha y) = e^\lambda(x, y), \text{ all } \; x, y \in T_\ell A.$$

This statement follows directly from the definitions, but the key point for the proof of (22.10) is that there is a converse: let λ' be a polarization of A; then $\lambda' = \alpha^\vee \circ \lambda \circ \alpha$ for some polarization λ of B if and only if there is a skew-symmetric form $e\colon T_\ell B \times T_\ell B \to \mathbb{Z}_\ell$ such that

$$e^{\lambda'}(\alpha x, \alpha y) = e(x, y), \text{ all } \; x, y \in T_\ell A.$$

This gives an easy criterion for when a polarization passes to a quotient variety. Using it one can prove the following statement:

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

Thus, to prove the theorem, we have to prove that, for every polarized abelian variety (A, λ), there exists an α satisfying this condition for (A^4, λ^4). Lagrange showed that every positive integer is a sum of 4 squares (ANT 4.19). Therefore, there are integers a, b, c, d such that

$$a^2 + b^2 + c^2 + d^2 \equiv -1 \bmod \; m^2,$$

and we let

$$\alpha = \begin{pmatrix} a & -b & -c & -d \\ b & a & d & -c \\ c & -d & a & b \\ d & c & -b & a \end{pmatrix} \in M_4(\mathbb{Z}) \subset \mathrm{End}(A^4).$$

Since α commutes with $\lambda^4 = diag(\lambda, \lambda, \lambda, \lambda)$, we have

$$\alpha(\mathrm{Ker}(\lambda^4)) \subset \mathrm{Ker}(\lambda^4).$$

Moreover, $\alpha^\vee$ is the transpose of α (as a matrix), and so

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

COROLLARY 22.11. *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 (22.10) we know that $(A \times A^\vee)^4$ has a principal polarization, and according to (10.2), the abelian varieties of dimension $8g$ over k having principal polarizations fall into finitely many isomorphism classes. But A is a direct factor of $(A \times A^\vee)^4$, and (22.1) shows that $(A \times A^\vee)^4$ has only finitely many direct factors. □

23. Finiteness I implies Finiteness II.

In this section we assume Finiteness I (up to isomorphism, there are only finitely many abelian varieties over a number field k isogenous to a fixed abelian variety). Hence we can apply Tate's conjecture and the semisimplicity theorem.

We first need a result from algebraic number theory which is the analogue of the theorem that a compact Riemann surface has only finitely many coverings with fixed degree unramified outside a fixed finite set.

THEOREM 23.1. *For any number field K, integer N, and finite set of primes S of K, there are only finitely many fields $L \supset K$ unramified outside S and of degree N (up to K-isomorphism of course).*

PROOF. First recall from ANT, 7.56, that for any prime v and integer N, there are only finitely many extensions of K_v of degree dividing N ($K_v =$ completion of K at v). This follows from Krasner's lemma: roughly speaking, such an extension is described by a monic polynomial $P(T)$ of degree $d|N$ with coefficients in $\mathcal{O}_v$; the set of such polynomials is compact, and Krasner's lemma implies that two such polynomials that are close define the same extension.

Now, recall that $Disc(L/K) = \prod Disc(L_w/K_v)$ (in an obvious sense), and because we are assuming L is ramified only at primes in S, the product on the right is over the primes w dividing a prime v in S. Therefore $Disc(L/K)$ is bounded, and we can apply the the following classical result. □

THEOREM 23.2 (Hermite 1857). *There are only finitely many number fields with a given discriminant (up to isomorphism).*

PROOF. Recall (ANT 4.3) that, for an extension K of $\mathbb{Q}$ of degree n, there exists a set of representatives for the ideal class group of K consisting of integral ideals $\mathfrak{a}$ with

$$\mathbb{N}(\mathfrak{a}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s |Disc_{K/\mathbb{Q}}|^{\frac{1}{2}}.$$

Here s is the number of conjugate pairs of nonreal complex embeddings of K. Since $\mathbb{N}(\mathfrak{a}) > 1$, this implies that

$$|Disc_{K/\mathbb{Q}}| > \left(\frac{\pi}{4}\right)^{2s}\left(\frac{n^n}{n!}\right)^2.$$

Since $\frac{n^n}{n!} \to \infty$ as $n \to \infty$ (by Stirling's formula, if it isn't obvious), we see that if we bound $|Disc_{K/\mathbb{Q}}|$ then we bound n. Thus, it remains to show that, for a fixed n, there are only finitely many number fields with a given discriminant d. Let $D = |d|$.

Let $\sigma_1, \dots, \sigma_r$ be the embeddings of F into $\mathbb{R}$, and let $\sigma_{r+1}, \bar{\sigma}_{r+1}, \dots, \sigma_{r+s}, \bar{\sigma}_{r+s}$ be the complex embeddings. Consider the map

$$\sigma\colon K \to \mathbb{R}^{r+s}, \quad x \mapsto (\sigma_1(x), \dots, \sigma_r(x), \Re\sigma_{r+1}(x), \Im\sigma_{r+1}(x), \dots).$$

In the case that $r \neq 0$, define X to be the set of n-tuples $(x_1, \dots, x_r, y_{r+1}, z_{r+1}, \dots)$ such that $|x_i| < C_i$ and $y_j^2 + z_j^2 < 1$, where $C_1 = \sqrt{D+1}$ and $C_i = 1$ for $i \neq 1$. In the contrary case, define Y to be the set of n-tuples $(y_1, z_1, \dots)$ such that $|y_1| < 1$, $|z_1| < \sqrt{D+1}$, and $y_i^2 + z_i^2 < 1$ for $i > 1$. One checks easily that the volumes of these sets are

$$\mu(X) = 2^r \pi^s \sqrt{1+D}, \quad \mu(Y) = 2\pi^{s-1}\sqrt{1+D},$$

and so both quotients $\mu(X)/2^r\sqrt{D}$ and $\mu(Y)/\sqrt{D}$ are greater than 1. By Minkowski's Theorem (ANT 4.18), there exist nonzero integers in K that are mapped into X or Y, according to the case. Let α be one of them. Since its conjugates are absolutely bounded by a constant depending only on D, the coefficients of the minimum polynomial of α over $\mathbb{Q}$ are bounded, and so there are only finitely many possibilities for α. We shall complete the proof by showing that $K = \mathbb{Q}[\alpha]$. If $r \neq 0$, then $\sigma_1\alpha$ is the only conjugate of α lying outside the unit circle (if it didn't lie outside, then $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) < 1$). If $r = 0$, then $\sigma_1\alpha$ and $\bar{\sigma}_1\alpha$ are the only conjugates of α with this property, and $\sigma_1\alpha \neq \bar{\sigma}_1\alpha$ since otherwise every conjugate of α would lie on the unit circle. Thus, in both cases, there exists a conjugate of α that is distinct from all other conjugates, and so α generates K. □

Let K be a number field, and let L be a Galois extension of K with Galois group G. Let w be a prime of L. The *decomposition group* is

$$D(w) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma w = w\}.$$

The elements of $D(w)$ act continuously on L for the w-adic topology, and therefore extend to the completion L_w of L. In fact L_w is Galois over K_v with Galois group $D(w)$. The group $D(w)$ acts on the residue field $k(w)$, and so we get a homomorphism

$$D(w) \to \mathrm{Gal}(k(w)/k(v)).$$

The kernel is called the *inertia group* $I(w)$. When $I(w) = 1$, L is said to be *unramified over* K at w, and we define the *Frobenius element* Frob_w at w to be the element of $D(w)$ corresponding to the canonical generator of $\mathrm{Gal}(k(w)/k(v))$. Thus Frob_w is the unique element of G such that

$$\mathrm{Frob}_w(\mathfrak{P}_w) = \mathfrak{P}_w, \quad \mathrm{Frob}_w(a) \equiv a^{q_v} \pmod{\mathfrak{P}_w}$$

where $\mathfrak{P}_w$ is the prime ideal of L corresponding to w, $q_v = \#k(w)$, and a is any element of the ring of integers of L. Because L is Galois, the decomposition groups at the primes lying over v are conjugate, and so are the inertia groups. Therefore, if one prime w lying over v is unramified they all are, and $\{\mathrm{Frob}_w \mid w|v\}$ is a conjugacy class in G — we denote it by $(v, L/K)$.

Theorem 23.3 (Chebotarev density theorem). *Let L be a finite Galois extension of a number field K with Galois group G. Let C be a conjugacy class of elements in G. Then the set of primes v of L such that $(v, L/K) = C$ has density $\#C/\#G$.*

PROOF. For a discussion of the theorem, see ANT, 8.26, and for a proof, see CFT, VII 5.4. □

REMARK 23.4. The theorem is effective, i.e., given a class C, there is a known bound B such that there will be a prime v with $\mathbb{N}(v) \leq B$ for which $(v, L/K) = C$.

Now consider an *infinite* Galois extension L over K with Galois group G. Recall (FT, 5.10; Jacobson, Lectures in Abstract Algbra, Vol III, pp 147-151) that G has a natural topology for which it is compact, and that the main theorem of Galois theory holds for infinite extension, except that it now provides a one-to-one correspondence between the intermediate fields M, $L \supset M \supset K$, and the *closed* subgroups of G. The above definitions of decomposition group etc. still make sense for infinite extensions. (One difference: the set of primes ramifying in L may be infinite.)

Let V be a finite dimensional vector space over $\mathbb{Q}_\ell$. A *representation* of $\Gamma \overset{\text{df}}{=} \mathrm{Gal}(K^{\mathrm{al}}/K)$ on V is a continuous homomorphism

$$\rho\colon \Gamma \to \mathrm{GL}(V) =_{df} \mathrm{Aut}(V).$$

The kernel of ρ is a closed normal subgroup of Γ, corresponding to a (possibly infinite) Galois extension L of K. The representation ρ is said to be *unramified* at a prime v of K if v is unramified in L.

We are especially interested in the representation of Γ on $V_\ell A$, A an abelian variety over K. Then the field L in the last paragraph is the smallest extension of K such that all the ℓ-power torsion points of A are rational over it, i.e., such that $A(L)(\ell) = A(K^{\mathrm{al}})(\ell)$.

THEOREM 23.5. *Let A be an abelian variety over a number field K. Let v be a finite prime of K, and let ℓ be a prime distinct from the characteristic of $k(v)$ (i.e., such that $v \nmid \ell$). Then A has good reduction at v if and only if the representation of* $\mathrm{Gal}(K^{al}/K)$ *on $V_\ell A$ is unramified at v.*

PROOF. $\Rightarrow$: For elliptic curves, this is proved in Silverman, 1986, VII 4.1. The proof for abelian varieties is not much more difficult.

$\Leftarrow$: For elliptic curves, see Silverman, 1986, 7.1. As we now explain, the statement for abelian varieties is an immediate consequence of the existence of Néron models (and hence is best called the Néron criterion).

Clearly the statement is really about A regarded as an abelian variety over the local field K_v. As we noted in §20, Néron showed that there is a canonical way to pass from an abelian variety A over K_v to a commutative algebraic group A_0 over the residue field $k = k(v)$. For any prime $\ell \neq \mathrm{char}(k(v))$, the reduction map

$$A(K_v)_{\ell^n} \to A_0(k)_{\ell^n}$$

is a bijection. The algebraic group A_0 doesn't change when K_v is replaced by an *unramified* extension. It has a filtration whose quotients are successively a finite algebraic group F (i.e., an algebraic group of dimension 0), an abelian variety B, a torus T, and an additive group U. We have

$$\dim A = \dim B + \dim T + \dim U.$$

Moreover:

$\#B(k^{\mathrm{al}})_{\ell^n} = \ell^{2n\dim(B)}$;

$\#T(k^{\mathrm{al}})_{\ell^n} = \ell^{n\dim(T)}$, because $T_{k^{\mathrm{al}}} \approx \mathbb{G}_m^{\dim T}$, $\mathbb{G}_m(L) = L^\times$ all fields $L \supset \mathbb{Q}$;
$\#U(k^{\mathrm{al}})_{\ell^n} = 0$, because $U_{k^{\mathrm{al}}} \approx \mathbb{G}_a^{\dim U}$, $\mathbb{G}_a(L) = L$ all fields $L \supset \mathbb{Q}$.

Now suppose that A has good reduction, so that $A_0 = B$. For all n,

$$A(K_v^{\mathrm{un}})_{\ell^n} = A_0(k^{\mathrm{al}})_{\ell^n}$$

has $\ell^{2n\dim A}$ elements, and so $A(K_v^{\mathrm{un}})_{\ell^n} = A(K_v^{\mathrm{al}})_{\ell^n}$. Therefore the action of $\mathrm{Gal}(K_v^{\mathrm{al}}/K_v)$ on $V_\ell A$ factors through $\mathrm{Gal}(K_v^{\mathrm{un}}/K_v)$, which is what it means for the representation of $\mathrm{Gal}(K_v^{\mathrm{al}}/K_v)$ on $V_\ell A$ to be unramified.

On the other hand, if A does not have good reduction, then

$$\#A(K_v^{\mathrm{un}})_{\ell^n} = \#A_0(k^{\mathrm{al}})_{\ell^n} < \ell^{2n\dim A}$$

for n sufficiently large. As

$$A(K_v^{\mathrm{un}})_{\ell^n} = A(K_v^{\mathrm{al}})^{\mathrm{Gal}(K_v^{\mathrm{al}}/K_v^{\mathrm{un}})}$$

this shows that

$$A(K_v^{\mathrm{al}})^{\mathrm{Gal}(K_v^{\mathrm{al}}/K_v^{\mathrm{un}})} \neq A(K_v^{\mathrm{al}})_{\ell^n}, \quad n >> 0.$$

Therefore the representation of the Galois group on $V_\ell A$ is ramified at v. □

COROLLARY 23.6. *If A and B are isogenous over K, and one has good reduction at v, then so also does the other.*

PROOF. The isogeny defines an isomorphism $V_\ell A \to V_\ell B$ commuting with the actions of $\mathrm{Gal}(K^{\mathrm{al}}/K)$. □

Recall that for an abelian variety A over a finite field k with q elements, the characteristic polynomial $P(A,t)$ of the Frobenius endomorphism π of A is a monic polynomial of degree $2g$ in $\mathbb{Z}[t]$, and its roots all have absolute value $q^{\frac{1}{2}}$ (§§9,16). Also, that $P(A,t)$ is the characteristic polynomial of π acting on $V_\ell A$. Now consider an abelian variety A over a number field K, and assume A has good reduction at v. Let $A(v)$ be the corresponding abelian variety over $k(v)$, and define

$$P_v(A,t) = P(A(v),t).$$

For any prime w lying over v, the isomorphism $V_\ell(A) \to V_\ell(A(v))$ is compatible with the map $D(w) \to \mathrm{Gal}(k(w)/k(v))$. Since the canonical generator of $\mathrm{Gal}(k(w)/k(v))$ acts on $V_\ell A(v)$ as π (this is obvious from the definition of π), we see that Frob_w acts on $V_\ell A$ as π, and so $P_v(A,t)$ is the characteristic polynomial of Frob_w acting on $V_\ell A$. If w' also lies over v, then $\mathrm{Frob}_{w'}$ is conjugate to Frob_w, and so it has the same characteristic polynomial.

THEOREM 23.7. *Let A and B be abelian varieties of dimension g over a number field K. Let S be a finite set of primes of K containing all primes at which A or B has bad reduction, and let ℓ be a prime different from the residue characteristics of the primes in S. Then there exists a finite set of primes $T = T(S,\ell,g)$ of K, depending only on S, ℓ, and g and disjoint from $S \cup \{v \mid v|\ell\}$, such that*

$$P_v(A,t) = P_v(B,t) \text{ all } v \in T \Longrightarrow A, B \text{ isogenous.}$$

PROOF. Recall:

(a) A, B have good reduction at $v \in S \Rightarrow V_\ell A$, $V_\ell B$ are unramified at $v \in S$ (provided $v \nmid \ell$) (see 23.5);

(b) the action of $\Gamma =_{df} \mathrm{Gal}(K^{\mathrm{al}}/K)$ on $V_\ell A$ is semisimple (see 21.5; remember we are assuming Finiteness I);

(c) A and B are isogenous if $V_\ell A$ and $V_\ell B$ are isomorphic as Γ-modules (this is the Tate conjecture 21.6).

Therefore, the theorem is a consequence of the following result concerning ℓ-adic representations (take $V = V_\ell A$ and $W = V_\ell B$). $\square$

LEMMA 23.8. *Let (V, ρ) and (W, σ) be semisimple representations of* $\mathrm{Gal}(K^{al}/K)$ *on $\mathbb{Q}_\ell$-vector spaces of dimension d. Assume that there is a finite set S of primes of K such that ρ and σ are unramified outside $S \cup \{v \mid v|\ell\}$. Then there is a finite set $T = T(S, \ell, d)$ of primes K, depending only on S, ℓ, and d and from disjoint from $S \cup \{v \mid v|\ell\}$, such that*

$$P_v(A, t) = P_v(B, t) \text{ all } v \in T \Longrightarrow (V, \rho) \approx (W, \sigma).$$

PROOF. According to Theorem 23.1, there are only finitely many subfields of K^{al} containing K, of degree $\leq \ell^{2d^2}$ over K, and unramfied outside $S \cup \{v \mid v|\ell\}$. Let L be their composite — it is finite and Galois over K and unramified outside $S \cup \{v \mid v|\ell\}$. According to the Chebotarev Density Theorem (23.3), each conjugacy class in $\mathrm{Gal}(L/K)$ is the Frobenius class $(v, L/K)$ of some prime v of K not in $S \cup \{v \mid v|\ell\}$. We shall prove the lemma with T any finite set of such v's for which

$$\mathrm{Gal}(L/K) = \cup_{v \in T}(v, L/K).$$

Let M_0 be a full lattice in V, i.e., the $\mathbb{Z}_\ell$-module generated by a $\mathbb{Q}_\ell$-basis for V. Then $\mathrm{Aut}_{\mathbb{Z}_\ell}(M_0)$ is an open subgroup of $\mathrm{Aut}_{\mathbb{Q}_\ell}(V)$, and so M_0 is stabilized by an open subgroup of $\mathrm{Gal}(K^{\mathrm{al}}/K)$. As $\mathrm{Gal}(K^{\mathrm{al}}/K)$ is compact, this shows that the lattices γM_0, $\gamma \in \mathrm{Gal}(K^{\mathrm{al}}/K)$, form a finite set. Their sum is therefore a lattice M stable under $\mathrm{Gal}(K^{\mathrm{al}}/K)$. Similarly, W has a full lattice N stable under $\mathrm{Gal}(K^{\mathrm{al}}/K)$.

By assumption, there exists a field $\Omega \subset K^{\mathrm{al}}$, Galois over K and unramified outside the primes in $S \cup \{v \mid v|\ell\}$, such that both ρ and σ factor through $\mathrm{Gal}(\Omega/K)$. Because T is disjoint from $S \cup \{v \mid v|\ell\}$, for each prime w of Ω dividing a prime v of T, we have a Frobenius element $\mathrm{Frob}_w \in \mathrm{Gal}(\Omega/K)$.

We are given an action of $\mathrm{Gal}(\Omega/K)$ on M and N, and hence on $M \times N$. Let R be the $\mathbb{Z}_\ell$-submodule of $\mathrm{End}(M) \times \mathrm{End}(N)$ generated by the endomorphisms given by elements of $\mathrm{Gal}(\Omega/K)$. Then R is a ring acting on each of M and N, we have a homomorphism $\mathrm{Gal}(\Omega/K) \to R^\times$, and $\mathrm{Gal}(\Omega/K)$ acts on M and N and through this homomorphism and the action of R on M and N. Note that, by assumption, for any $w|v \in T$, Frob_w has the same characteristic polynomial whether we regard it as acting on M or on N; therefore it has the same trace,

$$\mathrm{Tr}(\mathrm{Frob}_w|M) = \mathrm{Tr}(\mathrm{Frob}_w|N).$$

If we can show that the endomorphisms of $M \times N$ given by the Frob_w, $w|v \in T$, generate R as a $\mathbb{Z}_\ell$-module, then (by linearity) we have that

$$\mathrm{Tr}(r|M) = \mathrm{Tr}(r|N), \text{ all } r \in R.$$

Then the next lemma (applied to $R \otimes \mathbb{Q}_\ell$) will imply that V and W are isomorphic as R-modules, and hence as $\mathrm{Gal}(\Omega/K)$-modules.

Lemma 23.9. *Let k be a field of characteristic zero, and let R be a k-algebra of finite dimension over k. Two semisimple R-modules of finite-dimension over k are isomorphic if they have the same trace.*

Proof. This is a standard result — see Bourbaki, Algèbre Chap 8, §12, no. 1, Prop. 3. □

It remains to show that the endomorphisms of $M \times N$ given by the Frob_w, $w|v \in T$, generate R (as a $\mathbb{Z}_\ell$-module). By Nakayama's lemma, it suffices to show that $R/\ell R$ is generated by these Frobenius elements. Clearly R is a free $\mathbb{Z}_\ell$-module of rank $\leq 2d^2$, and so

$$\#(R/\ell R)^\times < \#(R/\ell R) \leq \ell^{2d^2}.$$

Therefore the homomorphism $\mathrm{Gal}(\Omega/K) \to (R/\ell R)^\times$ factors through $\mathrm{Gal}(K'/K)$ for some $K' \subset \Omega$ with $[K' : K] \leq \ell^{2d^2}$. But such a K' is contained in L, and by assumption therefore, $\mathrm{Gal}(K'/K)$ is equal to $\{\mathrm{Frob}_w \mid w|v \in T\}$. □

Theorem 23.10. *Finiteness I $\Rightarrow$ Finiteness II.*

Proof. Recall the statement of Finiteness II:

given a number field K, an integer g, and a finite set of primes S of K, there are only finitely many isomorphism classes of abelian varieties of K of dimension g having good reduction outside S.

Since we are assuming Finiteness I, which states that each isogeny class of abelian varieties over K contains only finitely many isomorphism classes, we can can replace "isomorphism" with "isogeny" in the statement to be proved.

Fix a prime ℓ different from the residue characteristics of the primes in S, and choose $T = T(S, \ell, g)$ as in the statement of Theorem 5.7. That theorem then says that the isogeny class of an abelian variety A over K of dimension g and with good reduction outside S is determined by the finite set of polynomials:

$$\{P_v(A,t) \mid v \in T\}.$$

But for each v there are only finitely many possible $P_v(A,t)$'s (they are polynomials of degree $2g$ with integer coefficients which the Riemann hypothesis (141.b) shows to be bounded), and so there are only finitely many isogeny classes of A's. □

24. Finiteness II implies the Shafarevich Conjecture.

Recall the two statements:

Finiteness II For any number field K, integer g, and finite set S of primes of K, there are only finitely many isomorphism classes of abelian varieties over K of dimension g having good reduction at all primes not in S.

Shafarevich Conjecture For any number field K, integer $g \geq 2$, and finite set of primes S of K, there are only finitely many isomorphism classes of complete nonsingular curves over K of dimension g having good reduction outside S.

Recall from (22.1) that, for an abelian variety A over a field k, there are only finitely many isomorphism classes of principally polarized abelian varieties (B, λ) over k with $B \approx A$. Therefore, in the statement of Finiteness II, we can replace "abelian variety" with "principally polarized abelian variety".

Recall that associated with any complete smooth curve C over a field k, there is an abelian variety $J(C)$ of dimension $g = \text{genus}(C)$. In fact, $J(C)$ has a canonical *principal* polarization $\lambda(C)$. (We noted in (18.5) that, when $k = \mathbb{C}$, there is a canonical Riemann form; for a general k, see JV §6.)

PROPOSITION 24.1. *Let C be a curve over a number field K. If C has good reduction at a prime v of K, then so also does $Jac(C)$.*

THEOREM 24.2 (Rational version of Torelli's theorem). *Let C be a complete nonsingular curve of genus ≥ 2 over a perfect field k. The isomorphism class of C is uniquely determined by that of the principally polarized abelian variety $(J(C), \lambda(C))$.*

On combining these two results we obtain the following theorem.

THEOREM 24.3. *Finiteness II implies the Shafarevich conjecture.*

PROOF. Let K be an algebraic number field, and let S be a finite set of primes in K. From (24.1) and (24.2) we know that the map $C \mapsto (J(C), \lambda(C))$ defines an injection from the set of isomorphism classes of complete nonsingular curves of genus ≥ 2 to the set of isomorphism classes of principally polarized abelian varieties over K with good reduction outside S. Thus Shafarevich's conjecture follows from the modified version of Finiteness II. $\square$

PROOF. (of 24.1) We are given a complete nonsingular curve C over K that reduces to a complete nonsingular curve $C(v)$ over the residue field $k(v)$. Therefore we have Jacobian varieties $J(C)$ over K and $J(C(v))$ over $k(v)$, and the problem is to show that $J(C)$ reduces to $J(C(v))$ (and therefore has good reduction). It is possible to do this using only varieties, but it is much more natural to use schemes. Let R be the local ring corresponding to the prime ideal $\mathfrak{p}_v$ in $\mathcal{O}_K$. To say that C has good reduction to $C(v)$ means that there is a proper smooth scheme $\mathcal{C}$ over $\operatorname{Spec} R$ whose general and special fibres are C and $C(v)$ respectively. The construction of the Jacobian variety sketched in (§17) works over R (see JV, §8), and gives us an abelian scheme $\mathcal{J}(\mathcal{C})$ over $\operatorname{Spec} R$ whose general and special fibres are $J(C)$ and $J(C(v))$, which is what we are looking for. $\square$

PROOF. (of 24.2) The original Torelli theorem applied only over an algebraically closed field and had no restriction on the genus (of course, Torelli's original paper (1914-15) only applied over $\mathbb{C}$). The proof over an algebraically closed field proceeds by a combinatorial study of the subvarieties of $C^{(r)}$, and is unilluminating (at least to me, even my own exposition in JV, §13).

Now consider two curves C and C' over a perfect field k, and suppose that there is an isomorphism $\beta\colon J(C) \to J(C')$ (over k) sending the polarization $\lambda(C)$ to $\lambda(C')$. Then the original Torelli theorem implies that there is an isomorphism $\gamma\colon C \to C'$ over k^{al}. In fact, it is possible to specify γ uniquely (in terms of β). For any $\sigma \in \operatorname{Gal}(k^{\mathrm{al}}/k)$, the map of curves associated with $\sigma\beta$ is $\sigma\gamma$. But $\sigma\beta = \beta$ (this is what it means to be defined over k), and so $\sigma\gamma = \gamma$, which implies that it too is defined over k (JV, §12, for the details). □

EXERCISE 24.4. Does (24.2) hold if we drop the condition that $g \geq 2$? Hints: A curve of genus 0 over a field k, having no point in k, is described by a homogeneous quadratic equation in three variables, i.e., by a quadratic form in three variables; now apply results on quadratic forms (e.g., CFT, VIII). If C is a curve of genus 1 without a point, then $\mathrm{Jac}(C)$ is an elliptic curve (with a point).

REMARK 24.5. Torelli's theorem (24.2) obviously holds for curves C of genus < 2 over k for which $C(k) \neq \emptyset$ — a curve of genus zero with $C(k) \neq \emptyset$ is isomorphic to $\mathbb{P}^1$; a curve of genus one with $C(k) \neq \emptyset$ *is* its Jacobian variety.

25. SHAFAREVICH'S CONJECTURE IMPLIES MORDELL'S CONJECTURE.

In this section, we write (f) for the divisor $\mathrm{div}(f)$ of a rational function on a curve. A *dyadic prime* of a number field is a prime dividing 2.

The proof that Shafarevich's conjecture implies Mordell's conjecture is based on the following construction (of Kodaira and Parshin).

THEOREM 25.1. *Let K be a number field and let S be a finite set of primes of K containing the dyadic primes. For any complete nonsingular curve C of genus $g \geq 1$ over K having good reduction outside S, there exists a finite extension L of K with the following property: for each point $P \in C(K)$ there exists a curve C_P over L and a finite map $\varphi_P \colon C_P \to C_{/L}$ (defined over L) such that:*

(i) *C_P has good reduction outside $\{w \mid w|v \in S\}$;*
(ii) *the genus of C_P is bounded;*
(iii) *φ_P is ramified exactly at P.*

We shall also need the following classical result.

THEOREM 25.2 (de Franchis). *Let C' and C be curves over a field k. If C has genus ≥ 2, then there are only finitely many nonconstant maps $C' \to C$.*

Using (25.1) and (25.2), we show that Shafarevich's conjecture implies Mordell's conjecture. For each $P \in C(K)$, choose a pair (C_P, φ_P) as in (25.1). Because of Shafarevich's conjecture, the C_P fall into only finitely many distinct isomorphism classes. Let X be a curve over L. If $X \approx C_P$ for some $P \in C(K)$, then we have a nonconstant map $X \approx C_P \overset{\varphi_P}{\to} C_{/L}$ ramified exactly over P, and if $X \approx C_Q$, then we have nonconstant map $X \to C_{/L}$ ramified exactly over Q — if $P \neq Q$, then the maps differ. Thus, de Franchis's Theorem shows that map sending (C_P, φ_P) to the isomorphism class of C_P is finite-to-one, and it follows that $C(K)$ is finite.

Before proving 25.1, we make some general remarks. When is $\mathbb{Q}[\sqrt{f}]$ unramified at $p \neq 2$? Exactly when $\mathrm{ord}_p(f)$ is odd. This is a general phenomenon: if K is the field of fractions of a discrete valuation ring R and the residue characteristic is $\neq 2$, then $K[\sqrt{f}]$ is ramified if and only if $\mathrm{ord}(f)$ is odd. (After a change of variables, $Y^2 - f$ will be an Eisenstein polynomial if $\mathrm{ord}(f)$ is odd, and will be of the form $Y^2 - u$ with u a unit if $\mathrm{ord}(f)$ is even. In the second case, the discriminant is a unit.)

Consider a nonsingular curve C over an algebraically closed field k of characteristic $\neq 2$, and let f be a nonzero rational function on C. Then there is a unique nonsingular curve C' over k and finite map $C' \to C$ such that the corresponding map $k(C) \hookrightarrow k(C')$ is the inclusion $k(C) \hookrightarrow k(C)[\sqrt{f}]$. Moreover, when we write $(f) = 2D + D'$ with D' having as few terms as possible, the remark in the preceding paragraph shows that φ is ramified exactly at the points of support of D'. (If C is affine, corresponding to the ring R, then C' is affine, corresponding to the integral closure of R in $k(C)[\sqrt{f}]$.) For example, consider the case when C is the affine line $\mathbb{A}^1$, and let $f(X) \in k[X]$. Write

$$f(X) = f_1(X) \cdot g(X)^2, \quad f_1(X) \text{ square-free.}$$

Then $k(C') \stackrel{\text{df}}{=} k(X)[\sqrt{f}] = k(X)[\sqrt{f_1}]$, and the curve

$$C' : \quad Y^2 = f_1(X)$$

is nonsingular because $f_1(X)$ does not have repeated roots. The map $C' \to C$, $(x, y) \mapsto x$, is finite, and is ramified exactly over the roots of $f_1(X)$.

When in this last example, we replace the algebraically closed field k with $\mathbb{Q}$, one additional complication occurs: f might be constant, say $f = r$, $r \in \mathbb{Q}$. Then $C' \to \operatorname{Specm} \mathbb{Q}$ is the composite

$$C_{\mathbb{Q}[\sqrt{r}]} \to C \to \operatorname{Specm} C_{\mathbb{Q}[\sqrt{r}]}$$

— here C' is not geometrically connected. This doesn't happen if $\operatorname{ord}_P(f)$ is odd for some point P of C.

Next fix a pair of distinct points P_1, $P_2 \in \mathbb{A}^1(\mathbb{Q})$, and let $f \in \mathbb{Q}(X)$ be such that $(f) = P_1 - P_2$. Construct the C' corresponding to f. Where does C' have good reduction? Note we can replace f with cf for any $c \in \mathbb{Q}^\times$ without changing its divisor. If we want C' to have good reduction on as large a set as possible, we choose

$$f = (X - P_1)/(X - P_2)$$

rather than, say, (*)

$$f = p(X - P_1)/(X - P_2).$$

The curve

$$Y^2 = (X - P_1)/(X - P_2)$$

has good reduction at any prime where P_1 and P_2 remain distinct (except perhaps 2). After these remarks, the next result should not seem too surprising.

LEMMA 25.3. *Let C be a complete nonsingular curve over a number field K, and consider a principal divisor of the form*

$$P_1 - P_2 + 2D, \quad P_1, P_2 \in C(K).$$

Choose an $f \in K(C)^\times$ such that $(f) = P_1 - P_2 + 2D$, and let $\varphi\colon C' \to C$ be the finite covering of nonsingular curves corresponding to the inclusion $K(C) \hookrightarrow K(C)[\sqrt{f}]$. With a suitable choice of f, the following hold:

(a) *The map φ is ramified exactly at P_1 and P_2.*
(b) *Let S be a finite set of primes of K containing those v at which C has bad reduction, those v at which P_1 and P_2 become equal, and all primes dividing 2. If the ring of S-integers is a principal then C' has good reduction at all the primes in S.*

Proof. (a) We have already seen this—it is really a geometric statement.

(b) (Sketch.) By assumption C extends to smooth curve $\mathcal{C}$ over $\operatorname{Spec}(R)$, where R is the ring of S-integers. The Zariski closure of $D' \overset{\text{df}}{=} P_1 - P_2 + 2D$ in $\mathcal{C}$ is a divisor on $\mathcal{C}$ without any "vertical components", i.e., without any components containing a whole fibre $C(v)$ of $\mathcal{C} \to \operatorname{Spec}(R)$. We can regard f as a rational function on $\mathcal{C}$ and consider its divisor as well. Unfortunately, as in the above example (*), it may have vertical components. In order to remove them we have to replace f with a multiple by an element $c \in K$ having exactly the correct value $\operatorname{ord}_{\mathfrak{p}}(c)$ for every prime ideal $\mathfrak{p}$ in R. To be sure that such an element exists, we have to assume that R is principal. □

Remark 25.4. (Variant of the lemma.) Recall that the Hilbert class field K^{HCF} of K is a finite unramified extension in which every ideal in K becomes principal. Even if the ring of S-integers is not principal, there will exist an f as in the theorem in $K^{\text{HCF}}(C)$.

Proposition 25.5. *Let A be an abelian variety over a number field K with good reduction outside a set of primes S. Then there is a finite extension L of K such that $A(K) \subset 2A(L)$.*

Proof. The Mordell-Weil Theorem implies that $A(K)/2A(K)$ is finite, and we can choose L to be any field containing the coordinates of a set of representatives for $A(K)/2A(K)$. [In fact, the proposition is more elementary than the Mordell-Weil Theorem — it is proved in the course of proving the Weak Mordell-Weil Theorem. □

Proof. (of 25.1). If $C(K)$ is empty, there is nothing to prove. Otherwise, we choose a rational point and use it to embed C into its Jacobian. The map $2_J\colon J \to J$ is étale of degree 2^{2g} (see 6.2). When we restrict the map to the inverse image of C, we get a covering $\varphi\colon C' \to C$ that is étale of degree 2^{2g}.

I claim that C' has good reduction outside S, and that each point of $\varphi^{-1}(P)$ has coordinates in a field L that is unramfied over K outside S. To see this, we need to use that multiplication by 2 is an étale map $\mathcal{J} \to \mathcal{J}$ of abelian schemes over $\operatorname{Spec} R_S$ (R_S is the ring of S-integers in K). The inclusion $C \hookrightarrow J$ extends to an inclusion $\mathcal{C} \hookrightarrow \mathcal{J}$ of schemes smooth and proper over $\operatorname{Spec} R_S$, and fibre product of this with $2\colon \mathcal{J} \to \mathcal{J}$ gives an étale map $\mathcal{C}' \overset{\text{df}}{=} \mathcal{C} \times_{\mathcal{J}} \mathcal{J} \to \mathcal{C}$. Therefore $\mathcal{C}' \to \operatorname{Spec} R_S$ is smooth (being the composite of an étale and a smooth morphism), which means that $\mathcal{C}'$ has good reduction outside S. The point P defines an R_S-valued point $\operatorname{Spec}(R_S) \to \mathcal{C}$, and the pull-back of $\mathcal{C}' \to \mathcal{C}$ by this is a scheme finite and étale over $\operatorname{Spec}(R_S)$ whose generic fibre is $\varphi^{-1}(P)$ — this proves the second part of the claim.

For any $Q \in \varphi^{-1}(P)$, $[K(Q) : K] \leq 2^{2g}$. Therefore, according to Theorem 23.1, there will be a finite field extension L_1 of K such that all the points of $\varphi^{-1}(P)$ are rational over L_1 *for all* $P \in C(K)$.

Now choose two distinct points P_1 and P_2 lying over P, and consider the divisor $P_1 - P_2$. According to (25.5), for some finite extension L_2 of L_1, every element of $J(L_1)$ lies in $2J(L_2)$. In particular, there is a divisor D on $C_{/L_2}$ such that $2D \sim P_1 - P_2$. Now replace L_2 with its Hilbert class field L_3. Finally choose an appropriate f such that $(f) = P_1 - P_2 - 2D$, and extract a square root, as in (25.3,25.4). We obtain a map φ_P

$$C_P \to C_{/L_3} \overset{\varphi}{\to} C_{/L_3}$$

over L_3 of degree $2 \cdot 2^{2g}$ that is ramified exactly over P. Now the Hurwitz genus formula

$$2 - 2g(C_P) = (2 - 2g(C)) \cdot \deg \varphi + \sum_{Q \mapsto P} (e_Q - 1)$$

shows that $g(C_P)$ is bounded independently of P. The field L_3 is independent of P, and (by construction) C_P has good reduction outside the primes lying over S.

Thus the proof of Theorem 25.1 is complete. $\square$

PROOF. (of 25.2.) The proof uses some algebraic geometry of surfaces (Hartshorne, Chapter V). Consider a nonconstant map $\varphi \colon C' \to C$ of curves. Its graph $\Gamma_\varphi \subset C' \times C \overset{\mathrm{df}}{=} X$ is a curve isomorphic to C', and is therefore of genus $g' =$ genus C'. Note that

$$\Gamma_\varphi \cdot (\{P'\} \times C) = 1, \qquad \Gamma_\varphi \cdot (C' \times \{P\}) = \#\varphi^{-1}(P) = d, \quad d = \deg(\varphi).$$

The canonical class of X is

$$K_X \equiv (2g-2)(C' \times \{P\}) + (2g'-2)(\{P'\} \times C)$$

and so

$$\Gamma_\varphi \cdot K_X = (2g-2)d + (2g'-2).$$

But the adjunction formula (Hartshorne V.1.5) states that

$$\Gamma_\varphi \cdot K_X = 2g' - 2 - \Gamma_\varphi^2.$$

We deduce that

$$\Gamma_\varphi^2 = -(2g-2)d$$

which is negative, because of our assumption on $g = g(C)$.

Note that d is bounded: the Hurwitz formula says that

$$2g - 2 = d(2g' - 2) + (\text{positive}).$$

Thus, there is an integer N (independent of φ) such that

$$N \leq \Gamma_\varphi^2 < 0.$$

For each polynomial P there exists a Hilbert scheme, Hilb_P, classifying the curves on X with Hilbert polynomial P. We know that Hilb_P is a finite union of varieties V_i (when the ambient space is $\mathbb{P}^n$, it is even connected), and that if $\Gamma \in V_i$, then $\dim V_i = \dim H^0(\Gamma, N_\Gamma)$ (by deformation theory) where N_Γ is the normal bundle. In our case, $N_\Gamma = 0$ since $\Gamma_\varphi^2 < 0$. Thus each V_i is a point. We deduce that

$$\{\Gamma_\varphi \mid \varphi \in \mathrm{Hom}^{\mathrm{noncnst}}(C, C')\}$$

is finite, and since a map is determined by its graph, this proves the theorem.

Alternative approach: Use differential geometry. The condition $g(C) > 1$ implies that $C(\mathbb{C})$ is hyperbolic. $\square$

26. The Faltings Height.

To any abelian variety A over a number field K, Faltings attaches a canonical height $H(A) \in \mathbb{R}$.

The Faltings height of an elliptic curve over $\mathbb{Q}$. Consider first an elliptic curve E over $\mathbb{C}$. We want to attach a number $H(E)$ to E which is a measure of its "size". The most natural first attempt would be to write $E \approx \mathbb{C}/\Lambda$, and define $H(E)$ to be the reciprocal of the area of a fundamental domain for Λ, i.e., if $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, then

$$H(E) = |\omega_1 \wedge \omega_2|^{-1}.$$

Unfortunately this doesn't make sense, because we can scale the isomorphism to make the area of the fundamental domain any positive real number we choose. In order to get a height, we need additional data.

Proposition 26.1. *Let E be an elliptic curve over $\mathbb{C}$. Then each of the following choices determines the remainder:*

(a) *an isomorphism $\mathbb{C}/\Lambda \to E(\mathbb{C})$;*
(b) *the choice of a basis for $\Gamma(E, \Omega^1)$, i.e., the choice of a nonzero holomorphic differential on E;*
(c) *the choice of an equation*

$$Y^2 = 4X^3 - g_2 X - g_3 \qquad (*)$$

for E.

Proof. (a)$\to$(c). There are associated with a lattice Λ, a Weierstrass function $\wp(z)$ and numbers $g_2(\Lambda)$, $g_3(\Lambda)$ for which there is an isomorphism

$$E(\mathbb{C}) = \mathbb{C}/\Lambda \to E' \subset \mathbb{P}^2, \qquad z \mapsto (\wp(z) : \wp'(z) : 1)$$

where E' is the projective curve given by the equation (*).

(c) $\to$ (b). Take $\omega = \frac{dX}{Y}$.

(b) $\to$ (a). From a differential ω on E and an isomorphism $\alpha\colon \mathbb{C}/\Lambda \to E(\mathbb{C})$ we obtain a differential $\alpha^*(\omega)$ on $\mathbb{C}$ invariant under translation by elements of Λ. For example, if α is the map given by $\wp$ and $\omega = \frac{dX}{Y}$, then $\alpha^*(\omega) = \frac{d\wp(z)}{\wp'(z)} = dz$. Thus we should choose the α so that $\alpha^*(\omega) = dz$. This we can do as follows: consider the map $P \mapsto \int_0^P \omega\colon E(\mathbb{C}) \to \mathbb{C}$. This is not well-defined because the integral depends on the choice of the path. However, if γ_1 and γ_2 are generators for $H_1(E, \mathbb{Z})$, then (up to homotopy), two paths from 0 to P will differ by a loop $m_1\gamma_1 + m_2\gamma_2$, and because ω is holomorphic, the integral depends only on the homotopy class of the path. Therefore, we obtain a well-defined map $E(\mathbb{C}) \to \mathbb{C}/\Lambda$, $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, $\omega_i = \int_{\gamma_i} \omega$, which is an isomorphism. □

Now, given a pair (E, ω) over $\mathbb{C}$, we can define

$$H(E,\omega)^{-1} = \frac{i}{2}\int_{E(\mathbb{C})} \omega \wedge \bar{\omega} = \frac{i}{2}\int_D dz \wedge d\bar{z} = \frac{i}{2}\int_D d(x+iy) \wedge d(x-iy) = \int_D dx \wedge dy$$

where D is a fundamental domain for Λ. Thus $H(E,\omega)^{-1}$ is the area of D.

When the elliptic curve is given over $\mathbb{Q}$ (rather than $\mathbb{C}$), then we choose an equation

$$Y^2 = 4X^3 - g_2X - g_3, \quad g_2, g_3 \in \mathbb{Q},$$

and take the differential ω to be dX/Y. When we change the choice of the equation, ω is only multiplied by a nonzero rational number, and so

$$H(E) \stackrel{\text{df}}{=} H(E, \omega)$$

is a well-defined element of $\mathbb{R}^+/\mathbb{Q}^+$, but we can do better: we know that E has a global minimal model i.e., an equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \quad a_i \in \mathbb{Z}, \quad \Delta \text{ minimal.}$$

The Weierstrass (=Néron) differential,

$$\omega = \frac{dX}{2Y + a_1X + a_3}.$$

is well-defined up to a multiplication by a unit in $\mathbb{Z}$, i.e., up to sign. Now $H(E) = H(E, \omega)$ is uniquely determined.

When we consider an elliptic curve over a number field K two complications arise. Firstly, K may have several infinite primes, and so we may have to take the product over their separate contributions. Secondly, and more importantly, $\mathcal{O}_K$ may not be a principal ideal domain, and so there may not be a global minimal equation. Before describing how to get around this last problem, it is useful to consider a more general construction.

The height of a normed module. A *norm* on a vector space M over $\mathbb{R}$ or $\mathbb{C}$ is a mapping $\|\cdot\|\colon M \to \mathbb{R}_{>0}$ such that

$$\|x + y\| \leq \|x\| + \|y\|, \quad \|ax\| = |a|\|x\|, \quad x, y \in M, \quad a \text{ scalar.}$$

Here $|\cdot|$ is the usual absolute value.

Now let K be a number field, and let R be the ring of integers in K. Recall that a fractional ideal in K is a projective R-module of rank 1; conversely, if M is a projective R-module of rank 1, then $M \otimes_R K \approx K$, and the choice of an isomorphism identifies M with a fractional ideal in K. Let M be such an R-module. Suppose we are given a norm $\|\cdot\|_v$ on $M \otimes_R K_v$ for each $v|\infty$. We define the *height* of M (better, of $(M, (\|\cdot\|_v)_{v|\infty})$) to be

$$H(M) = \frac{(M : Rm)}{\prod_{v|\infty} \|m\|_v^{\varepsilon_v}}, \quad m \text{ any nonzero element of } M, \quad \varepsilon_v = \begin{cases} 1 & v \text{ real} \\ 2 & v \text{ complex.} \end{cases}$$

LEMMA 26.2. *The definition is independent of the choice of m.*

PROOF. Recall that, for a finite prime v corresponding to a prime ideal $\mathfrak{p}$, the normalized absolute value is defined by,

$$|a|_v = (R : \mathfrak{p})^{-\mathrm{ord}_v(a)}, \quad \mathrm{ord}_v\colon K \twoheadrightarrow \mathbb{Z},$$

and that for any infinite prime v,

$$|a|_v = |a|^{\varepsilon_v}.$$

Moreover, for the normalized absolute values, the product formula holds:

$$\prod |a|_v = 1.$$

The Chinese remainder theorem shows that

$$M/Rm \approx \oplus_{v \text{ finite}} M_v/R_v m$$

where R_v is the completion of R at v and $M_v = R_v \otimes_R M$. Now M_v is a projective module of rank 1 over R_v, and hence it is free of rank 1 (because R_v is principal), say $M_v = R_v m_v$. Therefore

$$(M_v : R_v m) = (R_v m_v : R_v m) = \left|\frac{m_v}{m}\right|_v,$$

where by m_v/m we mean the unique element a of K_v such that $am = m_v$. Hence we find that (26.2.1)

$$H(M) = \frac{1}{\prod_{v \text{ finite}} \left|\frac{m}{m_v}\right|_v \cdot \prod_{v|\infty} \|m\|_v^{\varepsilon_v}}.$$

It is obvious that the expression on the right is unchanged when m is replaced with am. □

LEMMA 26.3. *In the expression (26.2.1) for $H(M)$, m can be taken to be any element of $M \otimes_R K$. When we define,*

$$h(M) = \frac{1}{[K:\mathbb{Q}]}\ \log H(M),$$

then, for any finite extension L of K,

$$h(R_L \otimes_R M) = h(M).$$

PROOF. Exercise in algebraic number theory. □

The Faltings height of an abelian variety.

PROPOSITION 26.4. *Let V be a smooth algebraic variety of dimension g over a field k.*

(a) *The sheaf of differentials $\Omega^1_{V/k}$ on V is a locally free sheaf of $\mathcal{O}_V$-modules of rank g.*
(b) *If V is a group variety, then Ω^1 is free.*

PROOF. See T. Springer, Linear Algebraic Groups, Birkhäuser, 1981, 3.2, 3.3. □

COROLLARY 26.5. *Let V be a smooth algebraic variety of dimension g over a field k. Then $\Omega^g =_{df} \Lambda^g \Omega^1$ is a locally free sheaf of rank 1, and it is free if V is a group variety.*

PROOF. Immediate from (26.4). □

Let $\mathcal{M}$ be a coherent sheaf on a variety V. For any point $v \in V$ we obtain a vector space $\mathcal{M}(v)$ over the residue field $k(v)$. For example, if V is affine, say $V = \operatorname{Specm}(R)$, then $\mathcal{M}$ corresponds to the R-module $M = \Gamma(V, \mathcal{M})$, and if $v \leftrightarrow \mathfrak{m}$, then $\mathcal{M}(v) = M/\mathfrak{m}M$. Note that, for any open subset U of V containing v, there is a canonical map $\Gamma(U, \mathcal{M}) \to \mathcal{M}(v)$.

PROPOSITION 26.6. *Let V be a complete geometrically connected variety over a field k, and let $\mathcal{M}$ be a free sheaf of finite rank on V. For any $v \in V(k)$, the map $\Gamma(V, \mathcal{M}) \to \mathcal{M}(v)$ is an isomorphism.*

PROOF. For $\mathcal{M} = \mathcal{O}_V$, $\Gamma(V, \mathcal{M}) = k$ (the only functions regular on the whole of a complete variety are the constant functions), and the map is the identity map $k \to k$. By assumption $\mathcal{M} \approx (\mathcal{O}_V)^n$ for some n, and so the statement is obvious. □

PROPOSITION 26.7. *Let A be an abelian variety of dimension g over a field k. The canonical maps*

$$\Gamma(A, \Omega^1) \to \Omega^1(0), \qquad \Gamma(A, \Omega^g) \to \Omega^g(0)$$

are isomorphisms.

PROOF. By 0 we mean the zero element of A. For the proof, combine the last two results. □

Now let A be an abelian variety over a number field K, and let R be the ring of integers in K. Recall from §20 that there is a canonical extension of A to a smooth group scheme $\mathcal{A}$ over $\operatorname{Spec} R$ (the Néron model). The sheaf $\Omega^g_{\mathcal{A}/R}$ of (relative) differential g-forms on $\mathcal{A}$ is a locally free sheaf of $\mathcal{O}_{\mathcal{A}}$-modules of rank 1 (it becomes free of rank 1 when restricted to each fibre, but is not free on the whole of $\mathcal{A}$). There is a section $s\colon \operatorname{Spec} R \to \mathcal{A}$ whose image in each fibre is the zero element. Define $M = s^*\Omega^g_{\mathcal{A}/R}$. It is a locally free sheaf of rank 1 on $\operatorname{Spec} R$, and it can therefore be regarded as a projective R-module of rank 1. We have

$$M \otimes_R K = \Omega^g_{A/K}(0) = \Gamma(A, \Omega^g_{A/K})$$

—the first equality simply says that $\Omega^g_{\mathcal{A}/R}$ restricted to the zero section of $\mathcal{A}$ and then to the generic fibre, is equal to $\Omega^g_{\mathcal{A}/R}$ restricted to the generic fibre, and then to the zero section; the second equality is (26.7).

Let v be an infinite prime of K. We have to define a norm on $M \otimes_K K_v$. But $M \otimes_K K_v = \Gamma(A_{K_v}, \Omega^g_{A_{K_v}/K_v})$, and we can set

$$\|\omega\|_v = \left(\left(\frac{i}{2}\right)^g \int_{A(K_v^{\mathrm{al}})} \omega \wedge \bar{\omega}\right)^{\frac{1}{2}}.$$

Note that $K_v^{\mathrm{al}} = \mathbb{C}$. Now $(M, (\|\cdot\|_v))$ is a normed R-module, and we define the *Faltings height* of A,

$$H(A) = H(M).$$

We can make this more explicit by using the expression (26.2.1) for $H(M)$. Choose a holomorphic differential g-form ω on A/K—this will be our m. It is well-defined up to multiplication by an element of $K^\times$. For a finite prime v, we have a Néron differential g-form ω_v for A/K_v (well-defined up to multiplication by a unit in R_v), and we have

$$H(A) = \frac{1}{\prod_{v \nmid \infty} \left|\frac{\omega}{\omega_v}\right| \cdot \prod_{v|\infty} \left(\left(\frac{i}{2}\right)^g \int_{A(K_v^{\mathrm{al}})} \omega \wedge \bar{\omega}\right)^{\varepsilon_v/2}}$$

For any infinite prime v, choose an isomorphism

$$\alpha\colon \mathbb{C}^g/\Lambda \to A(K_v^{\mathrm{al}})$$

such that $\alpha^*(\omega) = dz_1 \wedge dz_2 \wedge \ldots \wedge dz_g$; then the contribution of the prime v is

$$(\text{volume of a fundamental domain for } \Lambda)^{\frac{\varepsilon_v}{2}}.$$

This is all very explicit when A is an elliptic curve. In this case, ω_v is the differential corresponding to the Weierstrass minimal equation (see above, and Silverman 1986, VII.1). There is an algorithm for finding the Faltings height of an elliptic curve, which has surely been implemented for curves over $\mathbb{Q}$ (put in the coefficients; out comes the height).

Define

$$h(A) = \frac{1}{[K:\mathbb{Q}]}\log H(A).$$

If L is a finite extension of K, it is not necessarily true that $h(A_L) = h(A)$ because the Néron minimal model may change (Weierstrass minimal equation in the case of elliptic curves). However, if A has semistable reduction everywhere, then $h(A)$ is invariant under finite field extensions. We define the *stable Faltings height* of A,

$$h_F(A) = h(A_L)$$

where L is any finite field extension of K such that A_L has stable reduction at all primes of L (see 20.3).

27. The Modular Height.

Heights on projective space. (Serre, 1989, §2). Let K be a number field, and let $P = (x_0 : \ldots : x_n) \in \mathbb{P}^n(K)$. The height of P is defined to be

$$H(P) = \prod_v \max_{0\le i\le n} |x_i|_v.$$

Define

$$h(P) = \frac{1}{[K:\mathbb{Q}]}\log H(P).$$

(Warning: Serre puts the factor $[K:\mathbb{Q}]$ into $H(P)$.)

Proposition 27.1. *For any number C, there are only finitely many points P of $\mathbb{P}^n(K)$ with $H(P) \le C$.*

Note that an embedding $\alpha\colon V \hookrightarrow \mathbb{P}^n$ of an algebraic variety into $\mathbb{P}^n$ defines on it a height function, $H(P) = H(\alpha(P))$.

Proposition 27.2. *Let α_1 and α_2 be two embedding of V into $\mathbb{P}^n$ such that $\alpha_1^{-1}(\text{hyperplane}) \sim \alpha_2^{-1}(\text{hyperplane})$. Then the height functions defined by α_1 and α_2 on V differ by a bounded amount.*

In other words, given a variety V and a very ample divisor on V, we get a height function on $V(K)$, well defined up to a bounded function.

The Siegel modular variety. For any field L, let $\mathcal{M}_{g,d}(L)$ be the set of isomorphism classes of pairs (A,λ) with A an abelian variety over L of dimension g and λ a polarization of A of degree d.

THEOREM 27.3. *There exists a unique algebraic variety $M_{g,d}$ over $\mathbb{C}$ and a bijection $j\colon \mathcal{M}_{g,d}(\mathbb{C}) \to M_{g,d}(\mathbb{C})$ such that:*

(a) *for every point $P \in M_{g,d}$, there is an open neighbourhood U of P and a family $\mathcal{A}$ of polarized abelian varieties over U such that the fibre $\mathcal{A}_Q$ represents $j^{-1}(Q)$ for all $Q \in M_{g,d}$;*
(b) *for any variety T over $\mathbb{C}$, and family $\mathcal{A}$ of polarized abelian varieties over T of dimension g and degree d, the map $T \to M_{g,d}$, $t \mapsto j(\mathcal{A}_t)$, is regular (i.e., is a morphism of algebraic varieties).*

PROOF. Uniqueness: Let (M',j') be a second pair, and consider the map $j' \circ j\colon M_{g,d}(\mathbb{C}) \to M'(\mathbb{C})$. To prove that this is regular, it suffices to prove that it is regular in a neighbourhood of each point P of $M_{g,d}$. But given P, we can find a neighbourhood U of P as in (a), and condition (b) for M' implies that $(j' \circ j)|U$ is regular. Similarly, its inverse is regular.

Existence: This is difficult. Siegel constructed $M_{g,d}$ as a complex manifold, and Satake and others showed about 1958 that it was an algebraic variety. See E. Freitag, Siegelsche Modulfunktionen, Springer, 1983. □

The variety in the theorem is called the *Siegel modular variety*.

EXAMPLE 27.4. The j-invariant defines a bijection

$$\{\text{elliptic curves over } \mathbb{C}\}/\approx\; = \mathcal{M}_{1,1}(\mathbb{C}) \to M_{1,1}(\mathbb{C}), \qquad M_{1,1} = \mathbb{A}^1.$$

(See MF §8.)

Note that the automorphisms of $\mathbb{C}$ act on $\mathcal{M}_{g,d}(\mathbb{C})$.

Let V be a variety over $\mathbb{C}$, and suppose that there is given a model V_0 of V over $\mathbb{Q}$ (AG §9). Then the automorphisms of $\mathbb{C}$ act on $V_0(\mathbb{C}) = V(\mathbb{C})$.

THEOREM 27.5. *There exists a unique model of $M_{g,d}$ over $\mathbb{Q}$ such the bijection $j\colon \mathcal{M}_{g,d}(\mathbb{C}) \to M_{g,d}(\mathbb{C})$ commutes with the two actions of* $\mathrm{Aut}(\mathbb{C})$ *noted above.*

Write $M_{g,d}$ again for this model. For each field $L \supset \mathbb{Q}$, there is a well-defined map

$$j\colon \mathcal{M}_{g,d}(L) \to M_{g,d}(L)$$

that is functorial in L and is an isomorphism whenever L is algebraically closed.

PROOF. This is not difficult[16], given (27.3). □

EXAMPLE 27.6. The model of $M_{1,1}$ over $\mathbb{Q}$ is just $\mathbb{A}^1$ again. The fact that j commutes with the actions of $\mathrm{Aut}(\mathbb{C})$ simply means that, for any automorphism σ of $\mathbb{C}$ and elliptic curve E over $\mathbb{C}$, $j(\sigma E) = \sigma j(E)$—if E has equation

$$Y^2 = X^3 + aX + b$$

[16]That's what my original notes say, but I'm not sure I believe it.

then σE has equation

$$Y^2 = X^3 + \sigma a X + \sigma b,$$

and so this is obvious.

Note that $j\colon \mathcal{M}_{1,1}(L) \to \mathbb{A}^1(L) = L$ will not in general be a bijection unless L is algebraically closed. For example, if $c \in L$, then the curve

$$E_c: \quad Y^2 = X^3 + ac^2 X + bc^3$$

has the same j-invariant as

$$E: \quad Y^2 = X^3 + aX + b$$

but it is not isomorphic to E over L unless c is a square in L.

REMARK 27.7. Let K be a number field, and consider the diagram:

$$\begin{array}{ccc}
\mathcal{M}_{g,d}(K) & \xrightarrow{j} & M_{g,d}(K) \\
\big\downarrow & & \big\downarrow \text{injection} \\
\mathcal{M}_{g,d}(K^{\text{al}}) & \xrightarrow[\text{bijection}]{j} & M_{g,d}(K^{\text{al}})
\end{array}$$

Clearly $j(A,\lambda) = j(A',\lambda')$ if and only if (A,λ) becomes isomorphic to (A',λ') over K^{al}.

The modular height. The proof that $M_{g,d}$ is an algebraic variety shows more, namely, that there is a canonical ample divisor on $M_{g,d}$, and therefore a height function h on $M_{g,d}(K)$, any number field K, well-defined up to a bounded function, and we define the *modular height* of a polarized abelian variety (A,λ) over K by

$$h_M(A,\lambda) = h(j(A,\lambda)).$$

For example, consider the elliptic curve E over $\mathbb{Q}$; write $j(E) = \frac{m}{n}$ with m and n relatively prime integers. Then $h_M(E) = \log \max\{|m|,|n|\}$.

THEOREM 27.8. *For every polarized abelian variety (A,λ) over a number field K,*

$$h_F(A) = h_M(A,\lambda) + O(\log h_M(A,\lambda)).$$

PROOF. Technically, this is by far the hardest part of the proof. It involves studying the two height functions on a compactification of the modular variety over $\mathbb{Z}$ (see Chai and Faltings 1990 for moduli schemes over $\mathbb{Z}$). □

EXERCISE 27.9. Prove (27.8) for elliptic curves.

THEOREM 27.10. *Let K be a number field, and let g, d, C be integers. Up to isomorphism, there are only finitely many polarized abelian varieties (A,λ) over K of dimension g and degree d with semistable reduction everywhere and*

$$h_M(A,\lambda) \le C.$$

REMARK 27.11. The semistability condition is essential, for consider an elliptic curve

$$E: \quad Y^2 = X^3 + aX + b$$

over K. For any $c \in K^{\times}$, $c \notin K^{\times 2}$,

$$E_c: \quad Y^2 = X^3 + ac^2X + bc^3$$

has the same height as E (because it has the same j-invariant), but it is not isomorphic to E over K.

PROOF. We know from (27.1) that $\{P \in M_{g,d}(K) \mid H(P) \leq C\}$ is finite, and we noted above, that (A, λ) and (A', λ') define the same point in $M_{g,d}(K)$ if and only if they become isomorphic over K^{al}. Therefore, it suffices to prove the following statement: Let (A_0, λ_0) be a polarized abelian variety over K with semistable reduction everywhere; then up to K-isomorphism, there are only finitely many (A, λ) over K with semistable reduction everywhere such that $(A, \lambda) \approx (A_0, \lambda_0)$ over K^{al}.

Step 1. Let S be the set of primes of K at which A_0 has bad reduction, and let A be as in the statement. Then S is also the set of primes where A has bad reduction.

Proof: We know that A and A_0 become isomorphic over a finite extension L of K. Because A_0 and A have semstable stable reduction everywhere, when we pass from K to L, bad reduction stays bad reduction and good reduction stays good reduction, and so the set of primes of K where A has bad reduction can be read off from the similar set for L.

Step 2. Now fix an $\ell \geq 3$. There exists a finite extension L of K such that all the A's in the statement have their points of order ℓ rational over L.

Proof: The extension $K(A_\ell)$ of K obtained by adjoining the points of order ℓ is an extension of K of degree $\leq \#\,\mathrm{GL}_{2g}(\mathbb{F}_\ell)\mathbb{Z}/\ell\mathbb{Z})$ unramified outside S and $\{v \mid v|\ell\}$ (see 23.5), and so we can apply (23.1).

Step 3. Every (A, λ) as in the statement becomes isomorphic to (A_0, λ_0) over the field L in the Step 2.

Proof: Recall from AV, 17.5, that any automorphism of (A, λ) that acts as the identity map on the points of order 3 is itself the identity map. We are given that there is an isomorphism $\alpha\colon (A, \lambda) \to (A_0, \lambda_0)$ over K^{al}. Let $\sigma \in \mathrm{Gal}(K^{\mathrm{al}}/L)$. Then $\sigma\alpha$ is a second isomorphism $(A, \lambda) \to (A_0, \lambda_0)$, and $\sigma\alpha$ and α have the same action on the points of order 3 of A. (By definition $(\sigma\alpha)(P) = \sigma(\alpha(\sigma^{-1}P)$, but because σ fixes L, $\sigma^{-1}P = P$ and $\sigma(\alpha P) = \alpha P$.) Hence $\sigma\alpha \circ \alpha^{-1}$ is an automorphism of (A_0, λ_0) fixing the points of order 3, and so it is the identity map. Therefore $\sigma\alpha = \alpha$, and this means α is defined over L.

Step 4. Take the field L in step 2 to be Galois over K. Then the set

$$\{(A, \lambda) \mid (A, \lambda) \approx (A_0, \lambda_0) \text{ over } L\}/(K\text{-isomorphism}) \approx H^1(\mathrm{Gal}(L/K), \mathrm{Aut}(A_L, \lambda_L)).$$

Proof: Given (A, λ), choose an isomorphism $\alpha\colon (A, \lambda) \to (A_0, \lambda_0)$ over L, and let

$$a_\sigma = \sigma\alpha \circ \alpha^{-1}, \quad \sigma \in \mathrm{Gal}(L/K).$$

Then $\sigma \mapsto a_\sigma$ is a crossed homomorphism $\mathrm{Gal}(L/K) \to \mathrm{Aut}(A_L, \lambda_L)$, and it is not difficult to prove that the map sending (A, λ) to the cohomology class of (a_σ) is a bijection.

The group $H^1(\mathrm{Gal}(L/K), \mathrm{Aut}(A_L, \lambda_L))$ is finite because $\mathrm{Gal}(L/K)$ and $\mathrm{Aut}(A_L, \lambda_L))$ are both finite (for the second group, see AV 17.5), and this completes the proof of the Theorem. □

COROLLARY 27.12. *Let K be a number field, and let g, d, C be integers. Up to isomorphism, there are only finitely many polarized abelian varieties (A, λ) over K of dimension g and degree d with semistable reduction everywhere and*

$$h_F(A) \leq C.$$

PROOF. Apply (27.8). □

COROLLARY 27.13. *Let K be a number field, and let g, C be integers. Up to isomorphism, there are only finitely many abelian varieties A over K of dimension g with semistable reduction everywhere and*

$$h_F(A) \leq C.$$

PROOF. We need one more result, namely that $h_F(A) = h_F(A^\vee)$. (This is proved by Raynaud in the Szpiro seminar.) Given an A as in the statement, $B =_{df} (A \times A^\vee)^4$ is a principally polarized abelian variety over K (see 22.9) with semistable reduction everywhere, and

$$h(B) = 8h(A) \leq 8C.$$

Therefore we can apply (27.12) (and 22.3). □

28. The Completion of the Proof of Finiteness I.

It remains to prove:

> **Finiteness I:** Let A be an abelian variety over a number field K. There are only finitely many isomorphism classes of abelian varieties B over K isogenous to A.

THEOREM 28.1. *Let A be an abelian variety over a number field K having semistable reduction everywhere. The set of Faltings heights of abelian varieties B over K isogenous to A is finite.*

Before discussing the proof of (28.1), we explain how to deduce Finiteness I. First assume that A has semistable reduction everywhere. Then so also does any B isogenous to A, and so (27.13) and (28.1) show that the set of isomorphism classes of such B's is finite.

Now consider an arbitrary A. There will be a finite extension L of K such that A acquires semistable reduction over L, and so Finiteness I follows from the next statement: up to isomorphism, there are only finitely many abelian varieties B over K isogenous to a fixed abelian variety B_0 over K, and isomorphic to B_0 over L. (Cf. the proof of the last step of 27.10.)

PROOF. (of 28.1) Faltings's original proof used algebraic geometry, and in particular a theorem of Raynaud's on finite group schemes. In his talks in Szpiro's seminar, Raynaud improved Faltings's results by making them more effective. □

Appendix: Review of Faltings 1983 (MR 85g:11026)

Faltings, G.,
Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. [Finiteness Theorems for Abelian Varieties over Number Fields],
Invent. Math. 73 (1983), 349-366; Erratum,ibid. (1984), 75, 381.

The most spectacular result proved in this paper is Mordell's famous 1922 conjecture: a nonsingular projective curve of genus at least two over a number field has only finitely many points with coordinates in the number field. This result is in fact obtained as a corollary of finiteness theorems concerning abelian varieties which are themselves of at least equal significance. We begin by stating them. Unless indicated otherwise, K will be a number field, Γ the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ of K, S a finite set of primes of K, and A an abelian variety over K. For a prime number l, T_lA will denote the Tate group of A (inverse limit of the groups of l^n-torsion points on A) and $V_lA = \mathbb{Q}_l \otimes_{\mathbb{Z}_l} T_lA$. The paper proves the following theorems.

Theorem 3. *The representation of* Γ *on* V_lA *is semisimple.*

Theorem 4. *The canonical map* $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Z}_l \to \mathrm{End}(T_lA)^\Gamma$ *is an isomorphism.*

Theorem 5. *For given* S *and* g*, there are only finitely many isogeny classes of abelian varieties over* K *with dimension* g *and good reduction outside* S*.*

Theorem 6. *For given* S, g*, and* d*, there are only finitely many isomorphism classes of polarized abelian varieties over* K *with dimension* g*, degree (of the polarization)* d*, and good reduction outside* S*.*

Both Theorem 3 and Theorem 4 are special cases of conjectures concerning the étale cohomology of any smooth projective variety. The first is sometimes called the Grothendieck-Serre conjecture; the second is the Tate conjecture. Theorem 6 is usually called Shafarevich's conjecture because it is suggested by an analogous conjecture of his for curves (see below).

In proving these theorems, the author makes use of a new notion of the height $h(A)$ of an abelian variety: roughly, $h(A)$ is a measure of the volumes of the manifolds $A(\overline{K}_v)$, v an Archimedean prime of K, relative to a Néron differential on A. The paper proves:

Theorem 1. *For given* g *and* h*, there exist only finitely many principally polarized abelian varieties over* K *with dimension* g*, height* $\leq h$*, and semistable reduction everywhere.*

Theorem 2. *Let* $A(\overline{K})(l)$ *be the* l*-primary component of* $A(\overline{K})$*, some prime number* l*, and let* G *be an* l*-divisible subgroup of* $A(\overline{K})(l)$ *stable under* Γ*. Let* G_n *denote the set of elements of* G *killed by* l^n*. Then, for* n *sufficiently large,* $h(A/G_n)$ *is independent of* n*.*

Theorem (*) *Let* A *be an abelian variety over* K *with semistable reduction everywhere; then there is an* N *such that for every isogeny* $A \to B$ *of degree prime to* N*,* $h(A) = h(B)$*.*

The proof of Theorem 4 is modelled on a proof of J. T. Tate for the case of a finite field K [same journal 2 (1966), 134–144; MR 34#5829]. There, Tate makes use of a (trivial) analogue of Theorem 6 for a finite field to show that a special element of $\mathrm{End}(T_l A)^\Gamma$ lies in the image of the map. At the same point in the proof, the author applies his Theorems 1 and 2. An argument of Yu. G. Zarkhin [Izv. Akad. Nauk SSSR Ser. Mat. 39 (1975), no. 2, 272–277; MR 51#8114] allows one to pass from the special elements to a general element. Theorem 3 is proved simultaneously with Theorem 4.

From Theorem 4 in the case of a finite field, it follows that the isogeny class of an abelian variety over a finite field is determined by the characteristic polynomial of the Frobenius element. By making an adroit application of the Chebotarev density theorem (and Theorems 3 and 4), the author shows the following: given S and g, there exists a finite set T of primes of K such that the isogeny class of an abelian variety over K of dimension g with good reduction outside S is determined by the characteristic polynomials of the Frobenius elements at the v in T. (This in fact seems to give an algorithm for deciding when two abelian varieties over a number field are isogenous.) Since the known properties of these polynomials (work of Weil) imply there are only finitely many possibilities for each prime, this proves Theorem 5.

In proving Theorem 6, only abelian varieties B isogenous to a fixed abelian variety A need be considered (because of Theorem 5), and, after K has been extended, A can be assumed to have semistable reduction everywhere. The definition of the height is such that

$$e(B/A) \overset{\mathrm{df}}{=} \exp(2[K:\mathbb{Q}](h(B)-h(A))$$

is a rational number whose numerator and denominator are divisible only by primes dividing the degree of the isogeny between A and B. Therefore (*) shows that there exists an integer N such that e(A/B) involves only the primes dividing N. The isogenies whose degrees are divisible only by the primes dividing N correspond to the Γ-stable sublattices of $\prod_{l|N} T_l A$. From what has been shown about $T_l A$, there exist only finitely many isomorphism classes of such sublattices, and this shows that the set of possible values $h(B)$ is finite. Now Theorem 1 can be applied to prove Theorem 6.

The proof of Theorem 1 is the longest and most difficult part of the paper. The basic idea is to relate the theorem to the following elementary result: given h, there are only finitely many points in $\mathbb{P}^n(K)$ with height (in the usual sense) $\leq h$. The author's height defines a function on the moduli space M_g of principally polarized abelian varieties of dimension g. If M_g is embedded in $\mathbb{P}^n_K$ by means of modular forms rational over K, then the usual height function on $\mathbb{P}^n$ defines a second function on M_g. The two functions must be compared. Both are defined by Hermitian line bundles on M_g and the main points are to show (a) the Hermitian structure corresponding to the author's height does not increase too rapidly as one approaches the boundary of M_g (it has only logarithmic singularities) and (b) by studying the line bundles on compactifications of moduli schemes over $\mathbb{Z}$, one sees that the contributions to the two heights by the finite primes differ by only a bounded amount. This leads to a proof of Theorem 1. (P. Deligne has given a very concise, but clear, account of this part of the paper ["Preuve des conjectures de Tate et de Shafarevitch", Seminaire Bourbaki, Vol. 1983/84 (Paris, 1983/84), no. 616; per revr.].)

The proofs of Theorems 2 and (*) are less difficult: they involve calculations which reduce the questions to formulas of M. Raynaud [Bull. Soc. Math. France 102 (1974), 241–280; MR 547488]. (To obtain a correct proof of Theorem 2, one should replace the A of the proof in the paper by A/G_n, some n sufficiently large.)

Torelli's theorem says that a curve is determined by its canonically polarized Jacobian. Thus Theorem 6 implies the (original) conjecture of Shafarevich: given S and g, there exist only finitely many nonsingular projective curves over K of genus g and good reduction outside S. An argument of A. N. Parshin [Izv. Akad. Nauk SSSR Ser. Mat. 32 (1968), 1191–1219; MR 411740] shows that Shafarevich's conjecture implies that of Mordell: to each rational point P on the curve X one associates a covering $\varphi_P : X_P \to X$ of X; the curve X_P has bounded genus and good reduction outside S; thus there are only finitely many possible curves X_P, and a classical theorem of de Franchis shows that for each X_P there are only finitely many possible φ_P; as the association $P \mapsto (X_P, \varphi_P)$ is one-to-one, this proves that there are only finitely many P.

Before this paper, it was known that Theorem 6 implies Theorems 3 and 4 (and Mordell's conjecture). One of the author's innovations was to see that by proving a weak form of Theorem 6 (namely Theorem 1) he could still prove Theorems 3 and 4 and then could go back to get Theorem 6.

Only one misprint is worth noting: the second incorrect reference in the proof of Theorems 3 and 4 should be to Zarkhin's 1975 paper [op. cit.], not his 1974 paper.

James Milne (1-MI).

Index