Abelian Varieties

These are my live-TeXed notes for the course *Math 232br: Abelian Varieties* taught by Xinwen Zhu at Harvard, Spring 2012. The main reference book is [1]. See also [2] and [3]. Please let me know if you find any typos or mistakes!

[-] **Contents**

Introduction

Euler discovered an addition formula for elliptic integrals

$$\int_0^u \frac{dx}{\sqrt{P(x)}} + \int_0^v \frac{dx}{\sqrt{P(x)}} = \int_0^{F(u,v)} \frac{dx}{\sqrt{P(x)}},$$

where $P(x) = (1-x^2)(1-k^2x^2)$ and $F(u,v)$ is a certain algebraic function. In modern language, the affine equation $y^2 = P(x)$ defines an elliptic curve and the group structure on it gives the addition formula. More generally, let X be an algebraic curve with genus $g(X) \geq 1$, then integration gives a map

$$H_1(X,\mathbb{Z}) \hookrightarrow H^0(X,\Omega_X)^*, \quad \gamma \mapsto \int_\gamma$$

and an isomorphism

$$\mathrm{Pic}^0(X) \to J(X) := H^0(X,\Omega_X)^*/H_1(X,\mathbb{Z}), \quad \sum_i p_i - q_i \mapsto \sum_i \int_{p_i}^{q_i}.$$

$J(X)$ is called the *Jacobian* of X and has a natural group structure.

Theorem 1

a. $J(X)$ is compact (hence is a complex torus).

b. $J(X)$ has a natural (unique) structure as a projective variety.

Proof (Sketch)

a. We need to show that the image of $H_1(X,\mathbb{Z}) \to H^0(X,\Omega_X)^*$ is a lattice. This follows from the isomorphism $H^1_{\mathrm{dR}}(X,\mathbb{R}) \cong H^0(X,\Omega_X)^*$ using Hodge theory.

b. The second part follows from the following theorem and lemma. We only need to construct a symplectic pairing

$$H_1(X,\mathbb{Z}) \times H_1(X,\mathbb{Z}) \to \mathbb{Z}$$

such that the corresponding Hermitian form on $H^0(X,\Omega_X)^*$ is positive definite. This pairing can given by the intersection pairing on X. □

Theorem 2 Let $Y = V/\Lambda$, where $\Lambda \subseteq V = \mathbb{C}^n$ is a lattice. Then the followings are equivalent:

a. Y can be embedded into a projective space.

b. There exists an algebraic variety X such that $X^{\mathrm{an}} \cong Y$.

c. There exists n algebraically independent meromorphic functions on Y.

d. There exists a positive definite Hermitian form $H : V \times V \to \mathbb{C}$ such that $\operatorname{Im} H : \Lambda \times \Lambda$ is integral.

Lemma 1 Let V be a complex vector space and $V_{\mathbb{R}}$ be the underlying real vector space. Then there exists an bijection between Hermitian forms on V and skew-symmetric forms ω on $V_{\mathbb{R}}$ satisfying $\omega(ix,iy) = \omega(x,y)$ given by sending H to $\omega = \operatorname{Im} H$.

Notice that the group law on $J(X)$ is compatible with its algebraic variety structure. This motivates us to make the following definition.

Definition 1 An *abelian variety* over $\mathbb{C}$ is a projective variety with a group law, i.e., the multiplication and inversion are morphisms of algebraic varieties.

So we can associate an abelian variety $J(X)$ to each algebraic curve X with $g(X) \geq 1$.

Another example of abelian varieties comes from number theory. Let $F/\mathbb{Q}$ be a totally real extension of degree g and E/F be am imaginary quadratic extension, i.e., E is a *CM field*. Then $\operatorname{Hom}(E,\mathbb{C})$ has $2g$ elements and the complex conjugation c acts on it.

Definition 2 A *CM-type* is a choice of $\Phi \subseteq \operatorname{Hom}(E,\mathbb{C})$ such that Φ has g elements and $\Phi \cup c(\Phi) = \operatorname{Hom}(E,\mathbb{C})$.

Thus a CM-type gives an isomorphism $E \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{C}^{\Phi}$ by evaluation.

Theorem 3 Let $\mathcal{O}_E$ be the ring of integers of E. Then $\mathbb{C}^{\Phi}/\mathcal{O}_E$ is an abelian variety.

Proof (Sketch) By weak approximation, one can choose an $\alpha \in \mathcal{O}_E$ totally imaginary and $\operatorname{Im} \phi(\alpha) > 0$ for each $\phi \in \Phi$, then

$$E \times E \to \mathbb{Q}, \quad (x,y) \mapsto \operatorname{tr}_{E/\mathbb{Q}}(\alpha x y^*)$$

is positive definite and restricts to an integral pairing $\mathcal{O}_E \times \mathcal{O}_E \to \mathbb{Z}$. □

For any lattice $\Lambda \subseteq \mathbb{C}$ in a 1-dimensional complex vector space, $\mathbb{C}/\Lambda$ is an abelian variety. Suppose $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$, where $\operatorname{Im} \tau > 0$. We define

$$H : \mathbb{C} \times \mathbb{C} \to \mathbb{C}, \quad (z,w) \mapsto z\bar{w}/\operatorname{Im}(\tau).$$

Then H is positive definite and restricts to an integral pairing: $\operatorname{Im} H(1,1) = \operatorname{Im} H(\tau,\tau) = 0$ and $\operatorname{Im} H(1,\tau) = -1$.

Basic questions

Question Is it true that for any lattice Λ in an n-dimensional complex vector space, $\mathbb{C}^n/\Lambda$ is an abelian variety? Conversely, is every abelian variety a complex torus?

The answer to the first question is false: even for $n = 2$, for *almost all* lattices Λ, the complex torus $\mathbb{C}^2/\Lambda$ is not an abelian variety. However, the converse is true: every abelian variety must be a complex torus.

Proposition 1 Let X be a connected complex compact Lie group, then $X \cong V/\Lambda$, where V is a complex vector space and $\Lambda \subseteq V$ is a lattice.

Proof Let $V = \mathrm{Lie}(X)$. The adjoint representation

$$\mathrm{Ad} : X \to GL(V), \quad g \mapsto (\xi \mapsto \mathrm{Ad}_g \xi)$$

is *holomorphic*. But X is compact and connected and $GL(V)$ is an open subset of a complex vector space, hence Ad must be constant. In particular, $ghg^{-1} = h$ and X is commutative. When X is commutative, $\exp : V \to X$ is a group homomorphism and is in fact a covering map. Hence $X \cong V/\Lambda$ for some discrete subgroup $\Lambda \subseteq V$. Moreover, V must be a lattice as X is compact. □

It follows that abelian varieties are complex tori. The following holds for any complex torus, hence any abelian variety.

Corollary 1 Let X be an abelian variety over $\mathbb{C}$ of dimension g. Then

a. X is commutative and divisible. In particular, the multiplication-by-n map $n_X : X \to X$ is a surjective group homomorphism and has kernel $(\mathbb{Z}/n\mathbb{Z})^{2g}$.

b. $\pi_1(X) \cong H_1(X, \mathbb{Z}) \cong \Lambda \cong \mathbb{Z}^{2g}$.

c. Let X, Y be two abelian varieties. Let $\mathrm{Hom}(X, Y)$ be the group of homomorphisms as complex Lie groups from X to Y. Then

$$\mathrm{Hom}(X, Y) \to \mathrm{Hom}(H_1(X, \mathbb{Z}), H_1(Y, \mathbb{Z}))$$

is an injection. (But it is not surjective in general since additional complex structure is needed.)

Now we introduce the general notion of abelian varieties over an arbitrary field. By a *variety* over k, we mean a geometrically integral, separated and finite type k-scheme.

Definition 3 Let k be a field. An *abelian variety* over k is a smooth complete variety together with a point $0 \in X(k)$ and morphisms of algebraic varieties $m : X \times X \to X$, $s : X \to X$ such that X forms a group with multiplication m and inversion s.

Definition 4 Let X, Y be two abelian varieties. A *homomorphism* $f : X \to Y$ is a morphism of algebraic varieties compatible with the group structures. The set of homomorphisms from X to Y is denoted by $\mathrm{Hom}(X, Y)$. The category of abelian varieties is denoted by $\mathbf{AV}_k$.

Remark 1 It turns out every abelian variety is *projective* (cf. Corollary 12). We could replace "complete" by "projective" in our definition, but completeness is more convenient in constructing abelian varieties, since we do not know they are projective a priori.

Question The structure of $X(\bar{k})$ and $X(k)$ as an abstract group.

Theorem 4 Let X be an abelian variety over k. Then $X(\bar{k})$ is commutative and divisible. $n_X : X \to X$ is a surjective homomorphism with kernel $(\mathbb{Z}/n\mathbb{Z})^{2g}$ for $p = \mathrm{char}(k) \nmid n$, or $(\mathbb{Z}/n\mathbb{Z})^i$ for $p \mid n$, where i can be any value between 1 and g.

Theorem 5 (Mordell-Weil) Suppose k is a number field. Then $X(k)$ is a finitely generated abelian group.

Question The structure of $\mathrm{Hom}(X, Y)$.

Since $n_X : X \to X$ is surjective, we know that $\mathrm{Hom}(X, Y)$ is torsion-free. Over complex numbers, $H_1(X, \mathbb{Z})$ is a free abelian group of finite rank, so we know that $\mathrm{Hom}(X, Y)$ is a finite generated abelian group. More generally, over an arbitrary field,

Theorem 6 $\mathrm{Hom}(X, Y)$ is a finite generally free abelian groups.

Let ℓ be a prime different from $p = \mathrm{char}(k)$, then $X[\ell^n] = \ker \ell_X^n \cong (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$. It is a $G = \mathrm{Gal}(\bar{k}/k)$-module as ℓ_X^n is defined over k.

Definition 5 The *ℓ-adic Tate module* $T_\ell(X) := \varprojlim_n X[\ell^n]$. This is a free $\mathbb{Z}_\ell$ module of rank $2g$ with a continuous action of $G = \mathrm{Gal}(\bar{k}/k)$.

The Tate module can be viewed as an analog of the homology group $H_1(X, \mathbb{Z})$. The following result is analogous to the complex case but is harder to prove.

Theorem 7 Let $f : X \to Y$ be a homomorphism of abelian varieties. The induced map

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

is an injection.

Notice that the image of the induced map lies in $\mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(X), T_\ell(Y))^G$. We have the following famous Tate conjecture concerning the image.

Conjecture 1 (Tate) If k is a field finitely generated over its prime field. Then

$$\mathrm{Hom}(X, Y) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(X), T_\ell(Y))^G$$

is a bijection.

The Tate conjecture is proved by Tate for finite fields and by Faltings for number fields. Faltings theorem is much beyond the scope of this course, however, we may have a chance to talk about Tate's proof.

Question Line bundles on abelian varieties.

Theorem 8 There is a short exact sequence

$$1 \to \mathrm{Pic}^0(X) \to \mathrm{Pic}(X) \to \mathrm{NS}(X) \to 1.$$

Here $\mathrm{Pic}^0(X)$ has a natural structure of abelian variety, usually denoted by $\hat{X}$, is called the *dual abelian variety*, and $\mathrm{NS}(X)$ is a finitely generated free abelian group, is called the *Neron-Severi group*.

Question The cohomology of line bundles, Riemann-Roch problems.

Theorem 9 Let $\mathcal{L}$ be an ample line bundle on X. Then $\mathcal{L}^3$ is very ample.

This is useful in constructing moduli spaces of abelian varieties, which we may or may not cover.

Group Structures

Theorem 10 Let X be an abelian variety. Then X is commutative.

We can mimic the complex case and consider the adjoint representation. The issue is that $g \exp(\xi) g^{-1} = \mathrm{Ad}_g \exp(\xi)$ does not hold true in general. Here we take another approach.

Proposition 2 (Rigidity Lemma) Let X be a complete variety and Y, Z be arbitrary varieties. Let $f : X \times Y \to Z$ be a morphism of algebraic varieties such that $f(X \times y_0) = z_0 \in Z$. Then there exists $g : Y \to Z$ such that $= g \circ \mathrm{pr}_z$.

Corollary 2 Let X, Y be two abelian varieties and $f : X \to Y$ be a morphism of algebraic varieties. Then $f(x) = m(h(x), a)$, where $h \in \mathrm{Hom}(X, Y)$ and $a \in Y$.

Proof We may assume $f(0) = 0$. We need to show that f is homomorphism of abelian varieties. Define

$$g : X \times X \to Y, \quad (x, y) \mapsto f(x.y)/(f(x).f(y)).$$

Then $g(x, 0) = g(0, y) = 0$. Then the Rigidity Lemma 2 implies that $g(x.y) = 0$. □

Proof (Proof of Theorem 10) Apply Corollary 2 to the inversion $s : X \times X \to X$. It follows that X is commutative since s is a group homomorphism. □

Proof (Proof of Proposition 2) Without loss of generality, we may assume $k = \bar{k}$. Let $x_0 \in U \subseteq Z$, where U is affine open. Then $f^{-1}(U)$ is open in $X \times Y$. Let $W = X \times Y - f^{-1}(U)$, then W is closed. Because X is complete (hence universally closed), we know that $\mathrm{pr}_2(W)$, the projection of W onto Y, is closed in Y. By construction, $y_0 \notin \mathrm{pr}_2 W$. Hence $V = Y \setminus \mathrm{pr}_2(W)$ is nonempty and open. For any $v \in V$, we have $f(X \times \{v\}) \subseteq U$. Because $X \times \{v\}$ is complete and U is affine, we know that $f(X \times \{v\})$ is a point. So we have proved that $f|_{X \times V} = g \circ \mathrm{pr}_2|_{X \times V}$, where $g(y) = f(x_0, y)$. But everything is separated, hence $f = g \circ \mathrm{pr}_2$. □

Remark 2 Since the group law on an abelian variety is commutative, we shall use $+$ instead of $.$ to denote the multiplication and $(-1)_A$ to denote the inverse map.

The Theorem of the Cube

Lemma 2 Suppose $p = \mathrm{char}(k) \nmid n$, then $n_A : A \to A$ is surjective.

Proof (Sketch) Consider the differential $(dn_A)_0 : T_0A \to T_0A$. It is given by multiplication-by- n. Because $p \nmid n$, $(dn_A)_0$ is an isomorphism. So n_A is smooth, hence surjective. □

However, the above argument fails when $p \mid n$ (the differential is zero). We need to develop some techniques of line bundles on abelian varieties to prove the surjectivity of n_A in general.

Theorem 11 (Theorem of the Cube) Let X, Y be complete varieties and Z be an arbitrary variety. Let $x_0 \in X$, $y_0 \in Y$, $z_0 \in Z$. Let $\mathcal{L}$ be a line bundle on $X \times Y \times Z$. If $\mathcal{L}|_{\{x_0\}\times Y\times Z}$, $\mathcal{L}|_{X\times\{y_0\}\times Z}$, $\mathcal{L}|_{X\times Y\times\{z_0\}}$ are trivial, then $\mathcal{L}$ is trivial.

Before giving the proof, we shall interpret the theorem of the cube in a more conceptual way and draw several consequences of it.

Remark 3 Let $\mathbf{P}_k^+$ be the category of pointed complete varieties i.e. a pairing $(X, x \in X(k))$ over k. Let $T : \mathbf{P}_k^+ \to \mathbf{Ab}$ be a contravariant functor, where $\mathbf{Ab}$ is the category of abelian groups. Let $\pi_i : X_0 \times \cdots X_n \to X_0 \times \cdots \hat{X}_i \cdots \times X_n$ be the projection and σ_i be the i-the inclusion $\sigma_i : X_0 \times \cdots X_n \to X_0 \times \cdots \hat{X}_i \cdots \times X_n$. We define $\alpha_n = \sum T(\pi_i)$ and $\beta_n = \prod T(\sigma_i)$. Under this general setting, the following is always true:

Lemma 3 $T(X_0) \cong \mathrm{Im}\,\alpha_n \oplus \ker \beta_n$.

Definition 6 The functor T is called *of order* n (*linear* when $n = 1$, *quadratic* when $n = 2$) if β_n is injective (equivalently, α_n is surjective).

Example 1 The Theorem of Cube implies that the functor $\mathrm{Pic} : \mathbf{P}_k^+ \to \mathbf{Ab}$ is quadratic: the map

$$\beta_2 : \mathrm{Pic}(X \times Y \times Z) \to \mathrm{Pic}(X \times Y \times \{z_0\}) \times \mathrm{Pic}(X \times \{y_0\} \times Z) \times \mathrm{Pic}(\{x_0\} \times Y \times Z)$$

is injective.

Example 2 Let A be an abelian variety. Then $\mathrm{Hom}_{\mathbf{P}_k^+}(-, A)$ is linear. In fact,

$$\mathrm{Hom}(X \times Y, A) \to \mathrm{Hom}(X, A) \times \mathrm{Hom}(Y, A)$$

is a bijection. For the injectivity, suppose $\beta_1(f) = 0$, then by the Rigidity Lemma 2 we know that $f = g \circ \mathrm{pr}_2 = h \circ \mathrm{pr}_1$, hence $f = 0$. The surjectivity is obvious.

Example 3 Suppose $k = \mathbb{C}$, then $H^2(-, \mathbb{Z}) : \mathbf{P}_{\mathbb{C}}^+ \to \mathbf{Ab}$ is quadratic.

Here come several corollaries of the Theorem of Cube.

Corollary 3 Let X, Y, Z be complete varieties. Then every line bundle on $X \times Y \times Z$ is of the form $p_{12}^*\mathcal{L}_3 \otimes p_{23}^*\mathcal{L}_1 \otimes p_{31}^*\mathcal{L}_2$.

Proof Since $\ker \beta_2 = 0$ is equivalent to $\mathrm{Im}\,\alpha_2 = \mathrm{Pic}(X \times Y \times Z)$. □

Corollary 4 Let A be an abelian variety and X be an arbitrary variety. Let $f, g, h : X \to A$ be three morphisms. Then for any line bundle $\mathcal{L}$ on A,

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

Proof Consider the universal case $X = A \times A \times A$ and f, g, h are the projections. This follows from the Theorem of Cube by restricting to $0 \times A \times A$, $A \times 0 \times A$ and $A \times 0 \times A$. Other cases are pullbacks through $X \xrightarrow{(f,g,h)} A \times A \times A$. □

Corollary 5 Let $\mathcal{L}$ be a line bundle on A. Then $n_A^*\mathcal{L} \cong \mathcal{L}^{(n^2+n)/2} \otimes (-1)^*\mathcal{L}^{(n^2-n)/2}$.

Proof Applying Corollary 4 to the case $f = n_A$, $g = 1_A$ and $h = (-1)_A$, we obtain that

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

Let $M_n = n^*\mathcal{L} \otimes (n-1)^*\mathcal{L}^{-1}$, then $M_{n+1} = M_n \otimes (\mathcal{L} \otimes (-1)^*\mathcal{L})$, thus $M_n = (\mathcal{L} \otimes (-1)^*\mathcal{L})^{n-1} \otimes \mathcal{L}$ as $M_1 = \mathcal{L}$. Hence

$$n^*A = M_n \otimes M_{n-1} \otimes \cdots M_1 = \mathcal{L}^{(n^2+n)/2} \otimes (-1)^*\mathcal{L}^{(n^2-n)/2}.$$

This completes the proof. □

Corollary 6 If $\mathcal{L}$ is symmetric, i.e., $(-1)^*\mathcal{L} \cong \mathcal{L}$, then $n^*\mathcal{L} \cong \mathcal{L}^{n^2}$.

Corollary 7 (Theorem of the Square) For any $x, y \in A$ and $\mathcal{L}$ a line bundle on A, we have

$$T_{x+y}^*\mathcal{L} \otimes \mathcal{L} = T_x^*\mathcal{L} \otimes T_y^*\mathcal{L},$$

where

$$T_a : A \to A, \quad x \mapsto x + a$$

is the translation-by- a map.

Proof Apply Corollary 4 to $f : A \to A, \quad f(A) = x$, $g : A \to A, \quad g(A) = y$ and $h = 1_A$. □

Remark 4 If follows the Theorem of the Square that the map

$$\phi_{\mathcal{L}} : A(k') \to \mathrm{Pic}(A(k')), \quad x \mapsto T_x^* \mathcal{L} \otimes \mathcal{L}^{-1}$$

is a group homomorphism for any line bundle $\mathcal{L}$ on A, where k'/k is any field extension.

Review of cohomology theory on schemes

In order to prove the Theorem of the Cube, we need to digress to review some result on the cohomology of vector bundles over a flat family of varieties in this section.

Let X be a scheme. The category $\mathrm{Qcoh}(X)$ of quasicoherent sheaves on X is an abelian category. If X is further noetherian, we also consider the category $\mathrm{Coh}(X)$ of coherent sheaves on X. Let $f : X \to Y$ be a morphism of schemes, then the pullback functor $f^* : \mathrm{Qcoh}(Y) \to \mathrm{Qcoh}(X)$ has a right adjoint f_*. The *derived functor* of f_* consists of a collection of functors $\{R^i f_* : \mathrm{Qcoh}(X) \to \mathrm{Qcoh}(Y)\}_{i \geq 0}$ together with natural transformations $\delta^i : R^i f_* \mathcal{F}'' \to R^{i+1} f_* \mathcal{F}'$ for each short exact sequence $0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}'' \to 0$ satisfying the following:

a. $R^0 f_* = f_*$.

b. Any short exact sequence $0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}'' \to 0$ gives a long exact sequence

$$\cdots \to R^i f_* \mathcal{F}' \to R^i f_* \mathcal{F} \to R^i f_* \mathcal{F}'' \xrightarrow{\delta^i} R^{i+1} f_* \mathcal{F}' \to \cdots .$$

c. For any commutative diagram of short exact sequences

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathcal{F}' & \longrightarrow & \mathcal{F} & \longrightarrow & \mathcal{F}'' \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathcal{G}' & \longrightarrow & \mathcal{G} & \longrightarrow & \mathcal{G}'' \longrightarrow 0, \end{array}$$

the following diagram commutes

$$\begin{array}{ccc} R^i f_* \mathcal{F}' & \xrightarrow{\delta^i} & R^{i+1} f_* \mathcal{F}'' \\ \downarrow & & \downarrow \\ R^i f_* \mathcal{G}' & \xrightarrow{\delta^i} & R^{i+1} f_* \mathcal{G}''. \end{array}$$

When $Y = \mathrm{Spec}\, R$, we also write $R^i f_* \mathcal{F} =: H^i(X, \mathcal{F})$, the *$i$-th cohomology* of $\mathcal{F}$.

Instead of giving the precise definition of $R^i f_*$, let us review how to compute them (using Cech complexes). Assume $Y = \mathrm{Spec}\, R$ and X is separated (hence the intersection of two affine opens is still affine). Let $\mathcal{U} = \{U_i\}_{i \in I}$ be a cover of X by affine opens. Fixing an order on I, we form the Cech complex of R-modules $C^\cdot(\mathcal{U}, \mathcal{F})$ by

$$C^p(\mathcal{U}, \mathcal{F}) = \prod_{i_0 < \cdots < i_p} \Gamma(U_{i_0} \cap \cdots \cap U_{i_p}, \mathcal{F}).$$

In particular,

$$C^0(\mathcal{U}, \mathcal{F}) = \prod_i \Gamma(U_i, \mathcal{F}), \quad C^1(\mathcal{U}, \mathcal{F}) = \prod_{i<j} \Gamma(U_i \cap U_j, \mathcal{F}).$$

The differential $d^p : C^p(\mathcal{U}, \mathcal{F}) \to C^{p+1}(\mathcal{U}, \mathcal{F})$ is given by

$$(d\sigma)_{i_0 < \cdots < i_{p+1}} := \sum_{j=0}^{p+1} (-1)^j \sigma_{i_0 < \cdots < \widehat{i_j} < \cdots i_{p+1}} |_{U_{i_0} \cap \cdots \cap U_{i_{p+1}}}.$$

Theorem 12 (Comparison theorem) Suppose X is separated, then $H^i(X, \mathcal{F}) = H^i(C^\cdot(\mathcal{U}, \mathcal{F}))$ for any cover $\mathcal{U}$ of affine opens.

Corollary 8 (Kunneth formula) Let X, Y be two separated schemes over a field k. Suppose $\mathcal{F} \in \mathrm{Qcoh}(X)$ and $\mathcal{G} \in \mathrm{Qcoh}(Y)$. Then

$$H^n(X \times Y, \mathcal{F} \boxtimes \mathcal{G}) = \bigoplus_{i+j=n} H^i(X, \mathcal{F}) \otimes_k H^j(Y, \mathcal{F}),$$

where $\mathcal{F} \boxtimes \mathcal{G} = p_1^* \mathcal{F} \otimes p_2^* \mathcal{G}$.

Now let us state two important properties of sheaf cohomology we shall use later without proof.

Theorem 13 Let $f : X \to Y$ be a proper morphism of noetherian schemes. Suppose $\mathcal{F} \in \mathrm{Qcoh}(X)$, then $R^i f_* \mathcal{F} \in \mathrm{Qcoh}(Y)$. In particular, when $Y = \operatorname{Spec} k$, $H^i(X, \mathcal{F})$ is a finite dimensional k-vector space.

Theorem 14 Let $f : X \to Y$ be a proper morphism of noetherian schemes. Let $\mathcal{F} \in \mathrm{Qcoh}(X)$, flat over Y. Then there exists a finite complex

$$0 \to K^0 \to \cdots K^n \to 0$$

of locally free $\mathcal{O}_Y$-modules of finite rank such that for every morphism $u : S \to Y$,

$$R^i g_*(v^* \mathcal{F}) = H^i(u^* K^\cdot),$$

where g and v fit in the pullback diagram

$$\begin{array}{ccc} X \times_Y S & \xrightarrow{v} & X \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle f} \\ S & \xrightarrow{u} & Y. \end{array}$$

Example 4 Consider the situation $f : X \times_k T \to T$. Then for any line bundle $\mathcal{L}$ on $X \times_k T$, $\mathcal{L}$ is flat over T. This the case we will use later (cf. Theorem 15).

Definition 7 Let X be a proper scheme over $\operatorname{Spec} k$ and $\mathcal{F} \in \mathrm{Qcoh}(X)$. We define the *Euler characteristic* $\chi(\mathcal{F}) := \sum_i (-1)^i \dim_k H^i(X, \mathcal{F})$.

Corollary 9 Let $f : X \to Y$ and $\mathcal{F}$ be as in Theorem 14. Then $y \mapsto \chi(\mathcal{F}_y)$ is a locally constant function on Y, where $y \in Y$ and $\mathcal{F}_y = \mathcal{F}|_{X_y}$.

Proof Let $K^\cdot$ be the finite complex in Theorem 14. Then $H^i(X_y, \mathcal{F}_y) = H^i(K^\cdot \otimes_{\mathcal{O}_y} k(y))$. Hence $\chi(\mathcal{F}_y) = \sum_i (-1)^i \dim H^i(K^\cdot \otimes_{\mathcal{O}_y} k(y))$. The result follows from the additivity of the Euler characteristic and the fact that K^i's are locally free. □

Corollary 10 Let $f : X \to Y$ and $\mathcal{F}$ be as in Theorem 14. Then $y \mapsto h^i(y, \mathcal{F}) := \dim_{k(y)} H^i(X_y, \mathcal{F}_y)$ is an upper semicontinuous function, i.e., $\{y \in Y : h^i(y, \mathcal{F}) \geq n\}$ is closed for any n.

Proof By Theorem 14, $h^i(y, \mathcal{F}) = \dim(\ker (d^i \otimes k(y)) - \dim \operatorname{Im}((d^{i-1} \otimes k(y))$, or

$$h^i(y, \mathcal{F}) = \dim(K^i \otimes k(y)) - \dim \operatorname{Im}(d^i \otimes k(y)) - \dim \operatorname{Im}(d^{i-1} \otimes k(y)).$$

Since $\dim(K^i \otimes k(y))$ is locally constant, it is enough to show that $\{y \in Y : \dim \operatorname{Im}(d^i \otimes k(y)) \leq n\}$ is closed. Since d^i is locally given by a matrix, this set is locally cut out by vanishing conditions on the $n \times n$ minors, hence closed. □

Corollary 11 Let $f : X \to Y$ and $\mathcal{F}$ be as in Theorem 14. In addition, assume that Y is connected and reduced. Then then followings are equivalent:

a. $h^i(y, \mathcal{F})$ is locally constant.

b. $R^i f_* \mathcal{F}$ is locally free of finite rank and the natural map $R^i f_* \mathcal{F} \otimes k(y) \to H^i(X_y, \mathcal{F}_y)$ is an isomorphism.

Proof It is clear that (b) implies (a) . Conversely, suppose (a) is true, then $\dim \operatorname{Im}(d^i \otimes k(y))$ is locally constant by the previous proof. So $\operatorname{Im} d^i$ is locally free by the assumption on Y. So the local splitting of the complex ensures that $H^i(X_y, \mathcal{F}_y) = \frac{(\ker d^i) \otimes k(y)}{(\operatorname{Im} d^i) \otimes k(y)} \cong R^i f_* \mathcal{F} \otimes k(y)$. □

Now we apply the above results to the situation $X \times T \to T$ and a line bundle $\mathcal{L}$ on $X \times T$.

Theorem 15 (Seesaw Theorem) Suppose k is algebraically closed, X is a complete variety over k and T is an arbitrary variety over k. Let $\mathcal{L}$ be a line bundle on $X \times T$. Then

a. $T_1 = \{t \in T : \mathcal{L}|_{X \times \{t\}} \text{ is trivial } \}$ is closed.

b. There exists some line bundle $\mathcal{M}$ on T_1 such that $\mathcal{L}|_{X \times T_1} \cong p_2^* \mathcal{M}$.

We need the following easy lemma.

Lemma 4 A line bundle $\mathcal{L}$ on X is trivial if and only $\Gamma(X, \mathcal{L}) \neq 0$ and $\Gamma(X, \mathcal{L}^{-1}) \neq 0$.

Proof Suppose $\Gamma(X, \mathcal{L}) \neq 0$ and $\Gamma(X, \mathcal{L}^{-1}) \neq 0$. Choose two sections $s : \mathcal{O}_X \to \mathcal{L}$ and $t : \mathcal{O}_x \to \mathcal{L}^{-1}$, we obtain a morphism $\mathcal{O}_X \xrightarrow{s} \mathcal{L} \xrightarrow{t^\vee} \mathcal{O}_X$, which is an isomorphism since $\Gamma(X, \mathcal{O}_X) = k$ (X is complete). □

Proof (Proof of the Seesaw Theorem 15) The first part is clear using the above lemma together with the upper semicontinuity (Corollary 10). For the second part, since for any $t \in T_1$, $\dim H^0(X \times \{t\}, \mathcal{L}|_{X \times \{t\}}) = 1$, we

know that $M = (p_2)_* \mathcal{L}$ is locally free of rank 1 by Corollary 11. Then the adjunction map $p_2^* \mathcal{M} \to \mathcal{L}$ is an isomorphism as it is an isomorphism on each fiber. □

Remark 5 When k is not necessarily algebraically closed, $\Gamma(X, \mathcal{O}_X) = k'$ is the algebraic closure of k in $k(X)$. Similarly one can show that there exists $\mathcal{M}$ on $(T_1)_{k'}$ such that $\mathcal{L} = p_2^* M$, where $p_2 : X \times_{k'} (T_1)_{k'} \to (T_1)_{k'}$.

Proof of the Theorem of the Cube

Now let us return to finish the proof of the Theorem of the Cube. We need the following lemma.

Lemma 5 For any x_0, x_1 on X, there exists an irreducible curve $C \subseteq X$ containing x_0, x_1.

Proof The case $\dim X = 1$ is clear. We now assume $\dim X > 1$. Since X is complete, by Chow's Lemma (for any complete variety there is a surjective birational map from a projective variety to it), we may assume that X is projective. Let $f : \tilde{X} \to X$ be the blowup of X at x_0, x_1, then $\tilde{X}$ is also projective. Fixing an embedding $\tilde{X} \hookrightarrow \mathbb{P}^N$, by Bertini's theorem, we can find a general hyperplane H such that $H \cap \tilde{X}$ is irreducible of codimension 1. By construction, $\dim f^{-1}(x_i) \geq 1$, so $H \cap f^{-1}(x_i) \neq 0$. Now the lemma follows from induction on $\dim X$. □

Proof (Proof of the Theorem of the Cube 11) We may assume that X is a smooth projective curve by the above lemma. In fact, it is enough to show that $\mathcal{L}_{\{x\} \times Y \times \{z\}}$ is trivial for all (x, z) from the Seesaw Theorem 15 (applying to $T = X \times Z$). To show this, we can replace X by a curve containing two given points. In addition, we can replace it by its normalization and further assume X is smooth.

Suppose X has genus g. Pick a divisor E on X of degree g such that $H^0(X, \Omega_X(-E)) = 0$ (exercise: we can always do this). Let $\mathcal{M} = p_1^* \mathcal{O}(E) \otimes \mathcal{L}$. By Serre duality,

$$H^1(X \times \{y_0\} \times \{z_0\}, \mathcal{M}|_{X \times \{y_0\} \times \{z_0\}}) = H^1(X, \mathcal{O}(E)) = 0,$$

hence the support $W \subseteq Y \times Z$ of $R^1(p_{23})_* \mathcal{M}$ does not intersect $Y \times \{z_0\}$ by the upper semicontinuity (Corollary 10). Thus the projection of W onto Z is a closed subset not containing z_0. In other words, there is $Z' \subseteq Z$ open containing z_0 such that $R^1(p_{23})_* \mathcal{M}|_{Y \times Z'} = 0$. So we can replace Z by Z' by the Seesaw theorem 15.

In sum, now we can assume $R^1(p_{23})_* \mathcal{M} = 0$. Then

$$\chi(\mathcal{M}|_{X \times \{y_0\} \times \{z_0\}}) = \chi(\mathcal{O}(E)) = g - g + 1 = 1.$$

Since the Euler characteristic does not vary when we move (y, z) (in a flat family) and $h^1(\mathcal{M}|_{X \times \{y\} \times \{z\}}) = 0$, we know that

$$h^0(\mathcal{M}|_{X \times \{y\} \times \{z\}}) = \chi(\mathcal{M}|_{X \times \{y\} \times \{z\}})) = 1.$$

It follows that $\mathcal{N} = (p_{23})_* \mathcal{M} = 0$ is locally free of rank 1 on $Y \times Z$ by Corollary 11.

Let $\{U_i\}$ be an open cover of $Y \times Z$ such that $\mathcal{N}|_{U_i}$ is trivial. We choose a trivialization $\alpha_i : \mathcal{O}_{U_i} \to \mathcal{N}_{U_i}$. Then $\alpha_i(1) \in \Gamma(U_i, \mathcal{N}) = \Gamma(X \times U_i, \mathcal{M})$. Let D_i be the set of zeros of $\alpha_i(1)$. These D_i's can be glued into a codimension 1 closed subset $D \subseteq X \times Y \times Z$ such that $D|_{X \times U_i} = D_i$. So by definition $D_{X \times \{y\} \times \{z\}}$ is the set of zeros of the nonzero section of $\mathcal{M}|_{X \times \{y\} \times \{x\}}$. To show that $\mathcal{L}$ is trivial is equivalent to showing that $\mathcal{M} = p_1^* \mathcal{O}(E)$, or equivalently, $D = E \times Y \times Z$.

Let $p \in X$ such that $p \notin E$, we would like to show that $D \cap (\{p\} \times Y \times Z)$ is empty. This intersection does not meet $\{p\} \times Y \times \{z_0\}$ or $\{p\} \times \{y_0\} \times Z$ as we choose $p \notin E$. The projection of $D \cap (\{p\} \times Y \times Z)$ onto Z is a closed subset T of codimension 1 not containing z_0. So $D \cap (\{p\} \times Y \times Z) = \{p\} \times Y \times T$ as D is of codimension 1. On the other hand, $D \cap (\{p\} \times Y \times Z)$ does not intersect $\{p\} \times \{y_0\} \times Z$, so T is empty. Hence $D \cap (\{p\} \times Y \times Z)$ is empty. □

Remark 6 The proof of the Theorem of Cube is a bit tricky. If you do not like it, here is an easier proof for $k = \mathbb{C}$. By exponential sequence $1 \to \mathbb{Z} \to \mathcal{O}_X \to \mathcal{O}_X^\times \to 1$, we have an exact sequence

$$H^1(X, \mathcal{O}_X) \to H^1(X, \mathcal{O}_X^\times) \to H^1(X, \mathbb{Z}).$$

Then we know that $\mathrm{Pic}(X) = H^1(X, \mathcal{O}_X^\times)$ is quadratic since both $H^1(X, \mathcal{O}_X)$ and $H^2(X, \mathbb{Z})$ are quadratic by Kunneth formulas (cf. Remark 3).

Abelian varieties are projective

In this section, we will use the Theorem of Cube to deduce some deep results of abelian varieties, including the fact that all abelian varieties are projective.

Recall the group homomorphism $\phi_{\mathcal{L}} : A(\bar{k}) \to \mathrm{Pic}(A_{\bar{k}})$ defined in Remark 4. Since

$$\phi_{\mathcal{L}_1 \otimes \mathcal{L}_2} = \phi_{\mathcal{L}_1} \otimes \phi_{\mathcal{L}_2},$$

we obtain a homomorphism $\phi : \mathrm{Pic}(A) \to \mathrm{Hom}(A(\bar{k}), \mathrm{Pic}(A_{\bar{k}}))$.

Definition 8 We define $\mathrm{Pic}^0(A) = \ker \phi$, i.e., $\mathcal{L} \in \mathrm{Pic}^0(A)$ if $T_x^* \mathcal{L} = \mathcal{L}$ for any $x \in A(\bar{k})$.

Thus we have an exact sequence

$$0 \to \mathrm{Pic}^0(A) \to \mathrm{Pic}(A) \to \mathrm{Hom}(A(\bar{k}), \mathrm{Pic}(A_{\bar{k}})).$$

We will see that $\mathrm{Pic}^0(A)$ admits a natural structure of an algebraic variety, hence is an abelian variety (the *dual abelian variety*, cf 22).

Lemma 6 Let $\mathcal{L}$ be a line bundle on A. Then $\mathcal{L} \in \mathrm{Pic}^0(A)$ if and only if $m^* \mathcal{L} \cong p_1^* \mathcal{L} \otimes p_2^* \mathcal{L}$.

Proof "$\Longleftarrow$": Pulling back through $\{x\} \times A \hookrightarrow A \times A \xrightarrow{m} A$, we know $T_x^* \mathcal{L} \cong \mathcal{L}$ for any x.

"$\Longrightarrow$": Let $\mathcal{M} = m^* \mathcal{L} \otimes p_1^* \mathcal{L}^{-1} \otimes p_2^* \mathcal{L}^{-1}$. Then $\mathcal{M}|_{A \times \{x\}}$ and $\mathcal{M}|_{\{x\} \times A}$ are trivial since $T_x^* \mathcal{L} \cong \mathcal{L}$. So $\mathcal{M}$ is trivial the Seesaw Theorem 15. □

Definition 9 For $\mathcal{L} \in \mathrm{Pic}(A)$, we define $K(\mathcal{L}) = \{x \in A(\bar{k}) : T_x^* \mathcal{L} = \mathcal{L}\}$. The it is clear that for $\mathcal{L} \in \mathrm{Pic}^0(A)$, we have $K(\mathcal{L}) = A_{\bar{k}}$.

Lemma 7 $K(\mathcal{L})$ is closed in $A_{\bar{k}}$. (So $K(\mathcal{L})$ has a natural structure of an algebraic group.)

Proof Let $\mathcal{M} = m^* \mathcal{L} \otimes p_2^* \mathcal{L}^{-1}$. Then $K(\mathcal{L}) = \{x \in A(\bar{k}) : \mathcal{M}|_{A \times \{x\}} \text{ is trivial}\}$ is closed by the Seesaw Theorem 15. □

Now we can state the main theorem of this section:

Theorem 16 Let $\mathcal{L} = \mathcal{O}(D)$,where D is an effective divisor on A. Then the followings are equivalent:

a. $\mathcal{L}$ is ample.

b. $K(\mathcal{L})$ is finite.

c. $H(D) = \{x \in A : x + D = D\}$ is finite.

d. The linear system $|2D|$ is base-point-free and defines a finite morphism $A \to |2D|^*$.

This theorem has the following important consequence.

Corollary 12 Every abelian variety is projective.

Proof Pick $U \subseteq A$ an affine open containing 0 and $D = A \setminus U$ a divisor. Then $H(D)$ is closed as it is the projection of the preimage of D under the map $A \times D \xrightarrow{m} A$. So $H(D)$ is complete. But $H(D) \subseteq U$ since we choose $0 \in U$. We conclude that $H(D)$ is a complete variety inside an affine variety, thus is finite. Now the the result follows from Theorem 16. □

Remark 7 In the process of proving the Riemann hypothesis for algebraic curves, Weil constructed the Jacobian of a curve as a (*complete*) abelian variety. But it was not known that abelian varieties are *projective*. Weil thus reestablished the foundation of algebraic geometry and introduced the notion of *abstract varieties*. Unfortunately, the foundation was rewritten by Grothendieck for the second time and Weil's language was mostly abandoned nowadays. The fact that any abelian variety is projective is really deep: it took more than 10 years before it was proved in 1950s.

Proof (Proof of Theorem 16)

(a) implies (b): If not, then the identity connected component $B = K(\mathcal{L})^0$ is an abelian variety of positive dimension. By Lemma 6, $m^* \mathcal{L}|_B = p_1^* \mathcal{L}|_B \otimes p_2^* \mathcal{L}|_B$. Now pulling back through $\mathrm{Id} \times (-1) : B \to B \times B$ we know that $\mathcal{O}_B \cong \mathcal{L}|_B \otimes (-1)^* \mathcal{L}|_B$. Since $\mathcal{L}$ is ample we know that $\mathcal{L}|_B$ is ample. Since (-1) is an automorphism of B, we know that $(-1)^* \mathcal{L}|_B$ is also ample. Hence $\mathcal{O}_B$ is ample, a contradiction.

(b) implies (c): It is clear since $H(D) \subseteq K(\mathcal{L})$ by definition.

(c) implies (d): By the Theorem of the Square 7, we know that $(x + y + D) + D \sim (x + D) + (y + D)$. In particular, $(x + D) + (-x + D) \in |2D|$. To prove the base-point-freeness, for any $u \in A$, we want to find some x such that $u \notin x + D$ and $u \notin -x + D$, or equivalently, $x \notin -u + D, x \notin -u - D$. This can be done since $-u + D$ and $-u - D$ are both divisors. So $|2D|$ is base-point-free (for this part we have not used (c)).

The base-point-free linear system $|2D|$ defines a map $\phi : A \to |2D|^* = \mathbb{P}^N$, which is proper (since A and $\mathbb{P}^N$ are complete). In order to show that it is finite, we only need to show that each fiber $\phi^{-1}(p)$ is finite. If not, then ϕ contracts a curve $C \subseteq A$. Let $E \in |2D|$, then either $E \cap C \supseteq C$ or $E \cap C = \varnothing$. Moreover, for a generic E, $E \cap C = \varnothing$. We know that $(x + D) + (-x + D) \in |2D|$ and does not meet C for a generic $x \in A$. Hence $(x + D)$ does not meet C for a generic x. Using the finiteness of $H(D)$, it remains to prove the following lemma (applying to $E = x + D$.

Lemma 8 Let $C \subseteq A$ be an irreducible curve and E be a divisor such that $E \cap C = \varnothing$. Then for any $x, y \in C$, $x - y + E = E$.

Proof (Proof of the lemma) Let $\mathcal{L} = \mathcal{O}(E)$. Then $\mathcal{L}|_C = \mathcal{O}_C$. The multiplication $m : C \times A \to A$ gives a line bundle $m^*\mathcal{L}$ on $C \times A$. So for any $x \in A$,

$$\chi(T_x^*\mathcal{L}|_C) = \chi(m^*\mathcal{L}|_{C\times\{x\}}) = \chi(m^*\mathcal{L}|_{C\times 0}) = \chi(\mathcal{O}_C)$$

since the Euler characteristic stays the same in a flat family. Hence $\deg(T_x^*\mathcal{L}|_C) = \deg(\mathcal{O}_C) = 0$ by Riemann-Roch. So either $(x - y + E) \supseteq C$ or $(x - y + E) \cap C = \varnothing$. For any $x, y \in C$ and $z \in E$, we have $x \in (x - z) + E$, hence $(x - z) + E \supseteq C$, $z \in x - y + E$. □

(d) implies (a): We may replace $\mathcal{L}$ by $\mathcal{L}^2$. We want to show $\mathcal{O}_A \otimes \Gamma(\mathcal{F} \otimes \mathcal{L}^n) \to \mathcal{F} \otimes \mathcal{L}^n$ is surjective for each coherent sheaf $\mathcal{F}$ and sufficiently large n. Let $\phi : A \to |2D|^* = \mathbb{P}^N$ be the finite morphism in the assumption, then $\phi_*\mathcal{L} = \mathcal{O}_{\mathbb{P}^N}(1)$. Applying ϕ_* we obtain a commutative diagram

$$\begin{array}{ccc} \phi_*(\mathcal{O}_A \otimes \Gamma(\mathcal{F} \otimes \mathcal{L}^n)) & \longrightarrow & \phi_*(\mathcal{F} \otimes \mathcal{L}^n) \\ \downarrow \cong & & \downarrow \\ \mathcal{O}_{\mathbb{P}^N} \otimes \Gamma(\phi_*\mathcal{F} \otimes \mathcal{O}(n)) & \twoheadrightarrow & \phi_*\mathcal{F} \otimes \mathcal{O}(n). \end{array}$$

The lower map is surjective since $\mathcal{O}(1)$ is ample, so the above map is also surjective. (This is the general fact that the pullback of an ample line bundle through a finite morphism is ample). □

Corollary 13 $n_A : A \to A$ is surjective.

Proof By the dimension reason and the homogeneity, we know that n_A is surjective if and only if $\ker n_A$ is finite. Let $\mathcal{L}$ be an ample line bundle (existence ensured by the projectivity). We know that $n_A^*\mathcal{L}$ is ample by Corollary 5. Since $n_A^*\mathcal{L}|_{(\ker n_A)^0}$ is trivial, we know that $(\ker n_A)^0 = 0$. It follows that $\ker n_A$ is finite. □

In the next section we shall show the following properties of n_A.

Theorem 17 Suppose A has dimension g, then

a. $\deg n_A = n^{2g}$.
b. n_A is separable if and only if $p \nmid n$, where $p = \mathrm{char}(k)$.
c. The inseparable degree of p_A is at least p^g.

Isogenies of abelian varieties

Definition 10 Let A, B be two abelian varieties. A homomorphism $\alpha : A \to B$ is called an *isogeny* if α is surjective and has finite kernel. So by Corollary 13, n_A is an isogeny.

Definition 11 Let X be a complete variety of dimension g and $\mathcal{L}$ be a line bundle on X. Let $\mathcal{F}$ be a coherent sheaf on X. Then $P_{\mathcal{L}}(\mathcal{F}, n) = \chi(\mathcal{F} \otimes \mathcal{L}^n)$ is a polynomial of degree $\leq g$ (this is the usual Hilbert polynomial when X is smooth). Let $d_{\mathcal{L}}(\mathcal{F})/g!$ be the leading coefficient $P_{\mathcal{L}}(\mathcal{F}, n)$. We call $d_{\mathcal{L}}(\mathcal{F})$ the *degree* of $\mathcal{F}$ with respect to $\mathcal{L}$. We also write $d_{\mathcal{L}} = d_{\mathcal{L}}(\mathcal{O}_X)$ for short. Note that when the support of $\mathcal{F}$ has dimension $< g$, the degree $d_{\mathcal{L}}(\mathcal{F}) = 0$.

Proposition 3

a. Let $\mathcal{F}$ be a coherent sheaf on X with generic rank r. Then $d_{\mathcal{L}}(\mathcal{F}) = r \cdot d_{\mathcal{L}}$.
b. Let $f : X \to Y$ be a dominant morphism of complete varieties of the same dimension and $\mathcal{L}$ be a line bundle on Y, then $(\deg f)d_{\mathcal{L}} = d_{f^*\mathcal{L}}$.

Assuming Proposition 3, we can prove the following theorem promised before.

Theorem 18 $\deg n_A = n^{2g}$.

Proof Let $\mathcal{L}$ be an ample line bundle on A. Replacing $\mathcal{L}$ with $\mathcal{L} \otimes (-1)^* \mathcal{L}$, we may assume that $\mathcal{L}$ is symmetric. Then $n_A^* \mathcal{L} \cong \mathcal{L}^{n^2}$ (Corollary 6). By Proposition 3, we have $d_{\mathcal{L}^{n^2}} = d_{n_A^* \mathcal{L}} = (\deg n_A) d_{\mathcal{L}}$. On the other hand, since $P_{\mathcal{L}^{n^2}}(\mathcal{O}_X, 1) = P_{\mathcal{L}}(\mathcal{O}_X, n^2)$ by definition, we know that $d_{\mathcal{L}^{n^2}} = n^{2g} d_{\mathcal{L}}$. Hence $\deg n_A = n^{2g}$. □

Now let us come back to the proof of Proposition 3.

Proof (Proof of Proposition 3) For simplicity, we prove the case when X is smooth and f is finite.

a. Let $U \subseteq X$ be open such that $\mathcal{F}|_U \cong \mathcal{O}_U^r$ and $D = X \setminus U$ be a divisor. Since X is smooth, we can form a line bundle $\mathcal{M} := \mathcal{O}(D) = \mathcal{I}_D^{-1}$, where $\mathcal{I}_D$ is the ideal sheaf of D. We have a section $\sigma \in \Gamma(X, \mathcal{M})$ such that the zero locus of σ is D. Choosing a basis $\{e_1, \dots, e_r\}$ of the sections of $\mathcal{F}|_U$, we know that $e_i \otimes \sigma^N$ extends to a section of $\mathcal{F} \otimes \mathcal{M}^N$ on X for any i and N large enough. We get an exact sequence
$$\mathcal{O}_X^{\oplus r} \to \mathcal{F} \otimes \mathcal{M}^N \to \mathcal{T} \to 0.$$
The first map is injective since it is injective on U and $\mathcal{O}_X^{\oplus r}$ is torsion-free on X. The quotient T is torsion and has support in D. Tensoring with $\mathcal{M}^{-N}$, we have an exact sequence
$$0 \to (\mathcal{I}_D)^{\oplus r} \to \mathcal{F} \to \mathcal{T}' \to 0,$$
where T' is torsion and supported on a smaller dimension set (in particular, $d_{\mathcal{L}}(\mathcal{T}') = 0$). Using the additivity of the degrees, we know that
$$d_{\mathcal{L}}(\mathcal{F}) = d_{\mathcal{L}}(\mathcal{T}') + r \cdot d_{\mathcal{L}}(\mathcal{I}_D) = r \cdot d_{\mathcal{L}}(\mathcal{I}_D).$$
Now the result follows from the fact that $d_{\mathcal{L}}(\mathcal{I}_D) = d_{\mathcal{L}}(\mathcal{O}_X)$ since they agree on an open subset and the quotient sheaf has lower dimensional support.

b. By adjunction, $\chi(f^* \mathcal{L}^n) = \chi(f_* \mathcal{O}_X \otimes \mathcal{L}^n)$, thus $d_{f^* \mathcal{L}} = d_{\mathcal{L}}(f_* \mathcal{O}_X)$. Since $f_* \mathcal{O}_X$ is a coherent sheaf of generic rank $\deg f$, we also know that $d_{\mathcal{L}}(f_* \mathcal{O}_X) = (\deg f) \cdot d_{\mathcal{L}}$ by part (a). □

Theorem 19

a. n_A is separable if and only if $p \nmid n$, where $p = \operatorname{char}(k)$.

b. The inseparable degree of p_A is at least p^g.

Proof

a. n_A is separable if and only if n_A is smooth at a generic point, if and only if n_A is smooth at the origin by homogeneity. At the origin, the tangent map $(dn_A)_0$ is multiplication by n, thus is surjective if and only if $p \nmid n$. (Another way: the degree of an inseparable extension is always a power of p, but we know that $\deg n_A = n^{2g}$ by the previous theorem.)

b. Since the tangent map $(dp_A)_0$ is zero, we know that $p_A^* \Omega_{A/k} \to \Omega_{A/k}$ is zero. Hence at the generic point, $p_A^* : \Omega_{k(A)/k} \to \Omega_{k(A)/k}$ is zero. Therefore for any $f \in k(A)$, $d(p_A^* f) = p_A^*(df) = 0$, which implies that $p_A^*(f)$ lies in the kernel $k(A)^p \cdot k$ of the differential map $d : k(A) \to \Omega_{k(A)/k}$. Now the result follows from the fact that $k(A)/k(A)^p \cdot k$ is purely inseparable of degree p^g. □

Corollary 14 Let $A[n] = \ker n_A$ be the n-torsion points of an abelian variety A. Then
$$A[n] \cong \begin{cases} (\mathbb{Z}/n\mathbb{Z})^{2g}, & p \nmid n, \\ (\mathbb{Z}/p^m\mathbb{Z})^i, & n = p^m, \end{cases}$$
where $0 \leq i \leq g$.

Proof $\#A[n] = \#n_A^{-1}(0)$ is equal to the cardinality of the generic fiber, thus is equal to the separable degree of n_A. From the previous theorem, for any prime ℓ, we have $\#A[\ell] = \ell^{2g}$ for $\ell \neq p$ or $\#A[\ell] = \ell^i$ for $\ell = p$. Using the exact sequence
$$0 \to A[\ell] \to A[\ell^n] \xrightarrow{\ell} A[\ell^{n-1}] \to 0,$$
the result now follows from induction. □

Group schemes

We have basically solved the first question in our introduction about the group structures of abelian varieties (cf. Theorem 4). In the sequel, we shall study the Tate modules and dual abelian varieties. We prepare some general

notions of group schemes in this section.

Definition 12 A functor $G : \mathcal{C}^{\mathrm{op}} \to \mathbf{Grp}$ is called a *group functor*. A *group object* in $\mathcal{C}$ is a triple (G, X, α) where G is a group functor and $\alpha : G \cong h_X$ is an isomorphism for some $X \in \mathcal{C}$. Namely, for every $Y \in \mathcal{C}$, one assigns a group structure on the set $h_X(Y) = \mathrm{Hom}_{\mathcal{C}}(Y, X)$ and for any $Z \to Y$, we have a group homomorphism $h_X(Y) \to h_Z(Y)$.

Assume that finite products exist in $\mathcal{C}$ (in particular, the final object exists). Then giving a group object (G, X, α) is equivalent to giving a object X in $\mathcal{C}$ and morphisms $m : X \times X \to X$, $s : X \to X$ and $e : * \to X$ satisfying the usual commutative diagrams:

$$\begin{array}{ccc} X \times X \times X & \xrightarrow{(\mathrm{Id},m)} & X \times X \\ {\scriptstyle (m,\mathrm{Id})}\downarrow & & \downarrow{\scriptstyle m} \\ X \times X & \xrightarrow{m} & X, \end{array} \qquad \begin{array}{ccccc} * \times X & \xrightarrow{(e,\mathrm{Id})} & X \times X & \xleftarrow{(\mathrm{Id},e)} & X \times * \\ & \searrow^{\cong} & \downarrow{\scriptstyle m} & \swarrow_{\cong} & \\ & & X & & \end{array},$$

$$\begin{array}{ccccc} X & \xrightarrow{(\mathrm{Id},s)} & X \times X & \xleftarrow{(s,\mathrm{Id})} & X \\ \downarrow & & \downarrow{\scriptstyle m} & & \downarrow \\ * & \xrightarrow{e} & X & \xleftarrow{e} & *, \end{array}$$

Definition 13 Fix S a (locally) noetherian scheme. A *group scheme* over S is a group object in the category of schemes over S.

Therefore a group scheme can be understood in the above two ways: as a representable group functor, or as a object with a group structure.

Remark 8

a. For any morphism $S' \to S$, the base change $G_{S'}$ of a group scheme G over S has a natural structure of group scheme over S'.

b. We can define the right multiplication of G by an element in G. More precisely, for $T \to G$ and $g \in G(T)$, we have a right multiplication map $R_g : G_T \xrightarrow{\mathrm{Id} \times g} G_T \times_T G_T \xrightarrow{m} G_T$. At the level of T-points, this induces the usual right multiplication R_g on $G_T(T) = G(T)$.

c. Let G be a group scheme over S. Let $H \subseteq G$ be a open (resp. closed) subscheme of G. We say H is an *open* (resp. *closed*) group subscheme of G if the group structure on H is compatible with that of G.

d. Let G, H be two group schemes over S. A morphism $f : G \to H$ is called a *homomorphism* if the following diagram commutes:

$$\begin{array}{ccc} G \times G & \xrightarrow{f \times f} & H \times H \\ \downarrow{\scriptstyle m} & & \downarrow{\scriptstyle m} \\ G & \xrightarrow{f} & H. \end{array}$$

Moreover, we define $\ker f$ to be the pullback

$$\begin{array}{ccc} \ker f & \longrightarrow & G \\ \downarrow & & \downarrow{\scriptstyle f} \\ S & \longrightarrow & H, \end{array}$$

thus $\ker f$ is a group scheme over S. If, in addition, $e : S \to H$ is a closed embedding, then $\ker f$ is a closed group subscheme of G.

Example 5

a. An abelian variety over k is a group scheme over $S = \mathrm{Spec}\, k$.

b. The *additive group* $\mathbb{G}_a$ is defined to be $\mathrm{Spec}\, \mathcal{O}_S[t]$ with the group structure given by $m^* : t \mapsto 1 \otimes t + t \otimes 1$, $s^*(t) = -t$ and $e^*(t) = 0$. Alternatively, the group structure can be described as $\mathbb{G}_a(T) = \Gamma(T, \mathcal{O}_T)$ with usual addition for any S-scheme T.

c. The *multiplicative group* $\mathbb{G}_m$ is defined to be $\mathrm{Spec}\, \mathcal{O}_S[t, t^{-1}]$ with the group structure given by $m^*(t) = t \otimes t$, $s^*(t) = t^{-1}$, $e^*(t) = 1$. Alternatively, the group structure can be described as $\mathbb{G}_m(T) = \Gamma(T, \mathcal{O}_T^{\times})$ with usual multiplication for any S-scheme T.

d. The multiplication-by-n map $n:\mathbb{G}_m\to\mathbb{G}_m$ is defined to be $n(T):\mathbb{G}_m(T)\to\mathbb{G}_m(T)$, $n^*(t)=t^n$. The kernel $\mu_n=\ker n$ is a closed group subscheme and $\mu_n(T)=\{f\in\Gamma(T,\mathcal{O}_T^\times):f^n=1\}$ for any S-scheme T.

e. Let X be an S-scheme. The the *Picard functor* $\mathrm{Pic}_{X/S}:\mathbf{Sch}/S\to\mathbf{Grp}$, sending T to the isomorphism classes of line bundles on X_T modulo the isomorphism classes of line bundles on T, is a group functor. Moreover, if $\mathrm{Pic}_{X/S}$ is representable, then the corresponding scheme is called the *Picard scheme* of X/S. We will study the Picard scheme of an abelian variety later.

Lie algebras and smoothness of group schemes

From now on, we assume that G is a group scheme and the structural morphism $G\to S$ is locally of finite type.

The sheaf of differentials $\Omega_{G/S}$ is a coherent sheaf described as $\mathrm{Hom}_{\mathcal{O}_G}(\Omega_G,\mathcal{M})=\mathrm{Der}_{\mathcal{O}_S}(\mathcal{O}_G,\mathcal{M})$ for any quasicoherent sheaf $\mathcal{M}$ on G. In particular, the elements in $\mathrm{Hom}_{\mathcal{O}_G}(\Omega_G,\mathcal{O}_G)=\mathrm{Der}_{\mathcal{O}_S}(\mathcal{O}_G,\mathcal{O}_G)$ are called the *vector fields* on G. For any base change

$$\begin{array}{ccc} G_T & \xrightarrow{u} & G \\ \downarrow & & \downarrow \\ T & \longrightarrow & S, \end{array}$$

we have $u^*\Omega_G\cong\Omega_{G_T}$ and a natural pullback map $u^*:\mathrm{Hom}(\Omega_G,\mathcal{O}_S)\to\mathrm{Hom}(\Omega_{G_T},\mathcal{O}_T)$. The image of a vector field D on G is a vector field on G_T, which is also denoted by D.

Definition 14 We say D is a *right invariant vector field* if for any T, $g\in G(T)$ and $f\in\mathcal{O}_G$, $DR_g^*(f)=R_g^*D(f)$ holds. Similarly we can define left invariant vector fields on G. We denote the set of left (or right) invariant vector fields on G by $\mathrm{Lie}\,G$. Then $\mathrm{Lie}\,G$ is a sheaf of $\mathcal{O}_S$-modules on S.

Now let us specify the base scheme $S=\mathrm{Spec}\,k$. Let G/k be a group scheme. We defined $\mathrm{Lie}\,G$ as the set of left (or right) invariant vector fields on G, i.e., derivations $D:\mathcal{O}_G\to\mathcal{O}_G$ such that $DL_x^*=L_x^*D$.

Lemma 9 If $D_1,D_2\in\mathrm{Lie}\,G$, then $[D_1,D_2]:=D_1D_2-D_2D_1\in\mathrm{Lie}\,G$. If $p=\mathrm{char}\,k$, then $D^p\in\mathrm{Lie}\,G$.

In other words $\mathfrak{g}=\mathrm{Lie}\,G$ forms a *restricted Lie algebra* (or p-Lie algebra) over k:

Definition 15 A *restricted Lie algebra* $\mathfrak{g}$ over a field k of characteristic p is a Lie algebra together with a map $(-)^{(p)}:\mathfrak{g}\to\mathfrak{g}$ such that

a. $(\lambda x)^{(p)}=\lambda^p x^{(p)}$,

b. $\mathrm{ad}\,x^{(p)}=(\mathrm{ad}\,x)^{(p)}$,

c. $(x+y)^{(p)}=x^{(p)}+y^{(p)}+F_p(\mathrm{ad}\,x,\mathrm{ad}\,y)y$ for some universal non-commutative polynomial F_p depending only on p.

Remark 9 The exact expression of F_p is not important for us, but we will need the fact that $F_p(0,0)=0$, i.e., F_p has no constant term.

Remark 10 If $\mathfrak{g}$ is abelian (we will see this is the case for the Lie algebra of an abelian variety), then $(x+y)^{(p)}=x^{(p)}+y^{(p)}$ and $(-)^{(p)}:\mathfrak{g}\to\mathfrak{g}$ is p-linear.

Let $T_eG:=\mathrm{Hom}_k(\mathfrak{m}_e/\mathfrak{m}_e^2,k)$ be the tangent space of G at the origin e. From Grothendieck's point of view,

$$T_eG=\{\mathrm{Spec}\,\Lambda\xrightarrow{x}G:\mathrm{Spec}\,k\hookrightarrow\mathrm{Spec}\,\Lambda\xrightarrow{x}G\text{ is }e\}=\ker(G(\Lambda)\to G(k)),$$

where $\Lambda=k[\varepsilon]/(\varepsilon^2)$. The multiplication structure of T_eG as a group scheme coincides with its addition structure as a vector space. The tangent space T_eG can be canonically identified with the Lie algebra $\mathrm{Lie}\,G$ as follows.

Proposition 4 The map $\mathrm{Lie}\,G\to T_eG,\quad D\mapsto D|_e:=D(f)\mod m_e^2$ is an isomorphism, where $f\in m_e$.

Before giving the proof, we shall make a remark on another point view of derivations.

Remark 11 Let X/k be a scheme. To give a derivation $D:\mathcal{O}_X\to\mathcal{O}_X$ is the same to giving an automorphism $\tilde{D}:\mathcal{O}_X\otimes_k\Lambda\to\mathcal{O}_X\otimes\Lambda$ as Λ-algebras of the form $f\mapsto f+\varepsilon Df$. In other words, let $\tilde{X}=X\times\mathrm{Spec}\,\Lambda$, then we can view $\tilde{D}$ as a morphism $\tilde{D}:\tilde{X}\to\tilde{X}$ over $\mathrm{Spec}\,\Lambda$ such that its restriction to $X\to X$ over $\mathrm{Spec}\,k$ is the identity. Under this correspondence, for G/k be a group scheme, a derivation D on G is left invariant if and only if

$$\begin{array}{ccc} \tilde{G}\times\tilde{G} & \xrightarrow{\mathrm{Id}\times\tilde{D}} & \tilde{G}\times\tilde{G} \\ \downarrow{\scriptstyle m} & & \downarrow{\scriptstyle m} \\ \tilde{G} & \xrightarrow{\tilde{D}} & \tilde{G} \end{array}$$

is a commutative diagram.

Proof (Sketch) The inverse map $T_eG \to \operatorname{Lie} G$ is given as follows. Let $x \in T_eG \subseteq G(\Lambda)$, then the right translation $R_x : \tilde{G} \to \tilde{G}$ satisfies the above commutative diagram, hence by the previous remark gives a left invariant derivation $D \in \operatorname{Lie} G$. (This is a general fact from Lie theory that vector fields generated by the right translation is left invariant.) □

Let $\Lambda' = \Lambda \otimes_k \Lambda \cong k[\varepsilon_1, \varepsilon_2]/(\varepsilon_1^2, \varepsilon_2^2)$. We have two projections $p_1, p_2 : \operatorname{Spec}\Lambda' \to \operatorname{Spec}\Lambda$ and also a morphism $p_3 : \operatorname{Spec}\Lambda' \to \operatorname{Spec}\Lambda$ given by $\varepsilon \mapsto \varepsilon_1\varepsilon_2$.

Lemma 10 Let $D_1, D_2 \in \operatorname{Lie} G$ and $D_3 = [D_1, D_2]$. Then $p_1^*\tilde{D}_1 p_2^*\tilde{D}_2 p_1^*\tilde{D}_1^{-1} p_2^*\tilde{D}_2^{-1} = p_3^*\tilde{D}_3$.

Remark 12 We omit the proof, which is easy to check by reducing to the affine case. This is an analogy to the fact in differential geometry that $[x, y] = \frac{d}{ds}\frac{d}{dt}\left(\exp(sx)\exp(ty)\exp(-sx)\exp(-ty)\right)$.

Corollary 15 If G is commutative, then $\mathfrak{g} = \operatorname{Lie} G$ is abelian.

Proof For any two derivations D_1 and D_2, we can find $x, y \in T_eG$ such that $\tilde{D}_1 = R_x$ and $\tilde{D}_2 = R_y$, then $R_xR_yR_x^{-1}R_y^{-1} = \mathrm{Id}$ since G is commutative. Now by previous lemma we know that $[D_1, D_2] = 0$. □

Now let G/k be a group scheme of finite type and G^0 be the connected component containing e.

Lemma 11

a. G^0 is open, closed and is a group subscheme of G.

b. G^0 is geometrically irreducible.

c. G^0 is of finite type.

Proof (Sketch)

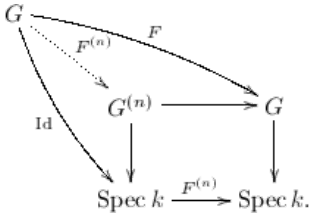
a. The connected component is always closed and it is open since topologically the G/k is locally noetherian. The map $G^0 \times G^0 \xrightarrow{x} G$ factors through G^0 by connectedness, hence G^0 is a group scheme.

b. It is a general fact that if a group scheme over k is connected and contains a rational point, then it is geometrically connected (we do not prove it). Base change to $\bar{k}$ and consider the induced reduced scheme G^0_{red}, then G^0_{red} is a reduced group scheme over $\bar{k}$, hence is smooth. It is connected and smooth, hence is geometrically irreducible.

c. For any U affine open, $U \times U \xrightarrow{m} G^0_{\mathrm{red}}$ is surjective, hence G^0_{red} is quasicompact. It is quasicompact and locally of finite type, hence is of finite type. □

Remark 13 We do not claim that G^0 itself is smooth. In fact there are many examples of reduced group schemes in characteristic p.

Example 6 In characteristic p, the group scheme $\mu_p = \operatorname{Spec} k[t]/(t^p - 1) = \operatorname{Spec} k[t]/(t-1)^p$ and $\alpha_p = \operatorname{Spec} k[t]/(t^p)$ are not reduced, hence not smooth. Let $G^{(n)}$ be the pullback of G via the n-fold Frobenius map $F^{(n)} : \operatorname{Spec} k \to \operatorname{Spec} k$, then we have an induced map $F^{(n)} : G \to G^{(n)}$ via the following diagram



$F^{(1)}$ is a morphism of group schemes (notice that n is not), hence the kernel is a closed group subscheme, called the *Frobenius kernel* of G. Thus μ_p is the Frobenius kernel of $\mathbb{G}_m \to \mathbb{G}_m^{(1)}$ and α_p is the Frobenius kernel of $\mathbb{G}_a \to \mathbb{G}_a^{(1)}$.

Nevertheless, any group scheme over a field k of characteristic 0 is automatically smooth.

Theorem 20 If $\operatorname{char} k = 0$, then G^0 is smooth (hence G is smooth).

Proof (Sketch) We may assume $k = \bar{k}$. We only need to show that every completed local ring (by homogeneity, at the origin e) is isomorphic to the power series ring generated by $\{dx_1, \dots, dx_n\}$, where $\{dx_i\}$ form a basis for $\mathfrak{m}_e/\mathfrak{m}_e^2$. Let $\delta_1, \dots, \delta_n \in T_eG$ be a dual basis, then they give left invariant vector fields $D_1, \dots D_n \in \operatorname{Lie} G$. We thus have a natural map into the completed local ring $k[[x_1, \dots, x_n]] \to \widehat{\mathcal{O}_{G,e}}$. The inverse map is given by the Taylor expansion $f \mapsto \sum \frac{1}{\alpha!} D^\alpha(f)$. □

Picard schemes and dual abelian varieties

Let X/k be a projective variety and assume that we have a rational point $x \in X(k)$. We introduced the Picard functor (cf. Example 5)

$$\operatorname{Pic}_{X/k}(T) = \frac{\{\text{isomorphism classes of line bundles on } X \times T\}}{\{\text{isomorphism classes of line bundles } p^*\mathcal{L}\}},$$

where $p : X \times T \to T$ is the projection. In other words, $\operatorname{Pic}_{X/k}(T)$ consists of isomorphism classes of pairs

$$\{(\mathcal{L}, \alpha) : \mathcal{L} \text{ a line bundle on } X \times T, \alpha : \mathcal{L}_{\{x\}\times T} \cong \mathcal{O}_T\}.$$

Grothendieck proved the following representability theorem of Picard functors (which we will treat as a black box).

Theorem 21

a. $\operatorname{Pic}_{X/k}$ is represented by a scheme (hence a group scheme), which is locally of finite type over k.

b. The connected component $\operatorname{Pic}^0_{X/k}$ is quasiprojective, and is projective if X is smooth.

Example 7 The k-points $\operatorname{Pic}_{X/k}(k) = \operatorname{Hom}(\operatorname{Spec} k, \operatorname{Pic}_{X/k})$ is equal to the groupoid

$$\{(\mathcal{L}, \alpha) : \mathcal{L} \text{ a line bundle on } X, \alpha : \mathcal{L}_x \cong k\}.$$

In other words, we fixed a *rigidification* $\alpha : \mathcal{L}_x \cong k$ of a line bundle $\mathcal{L}$, so that the pair $(\mathcal{L}, \alpha)$ has no nontrivial automorphisms (which is important to the representability) and this groupoid is actually equivalent to a category of sets.

Definition 16 Consider $T = \operatorname{Pic}_{X/k}$, then $\operatorname{Id} \in \operatorname{Hom}(\operatorname{Pic}_{X/k}, \operatorname{Pic}_{X/k})$ it corresponds to a pair $(\mathcal{P}_{\text{univ}}, \alpha_{\text{univ}})$ on $X \times \operatorname{Pic}_{X/k}$. This pair is called the *Poincare sheaf*.

By the functoriality, any line bundle $(\mathcal{L}, \alpha)$ is the pull back $\phi^*(\mathcal{P}_{\text{univ}}, \alpha_{\text{univ}})$ via the map $\phi : T \to \operatorname{Pic}_{X/k}$ corresponding to $(\mathcal{L}, \alpha)$. For $\lambda \in \operatorname{Pic}_{X/k}(k')$, $\mathcal{P}_{\text{univ}}|_{X\times\{\lambda\}}$ is a line bundle on $X_{k'}$ and corresponds to the line bundle represented by λ.

Definition 17 Let $\mathcal{M}$, $\mathcal{N}$ be two line bundles on X. We say that $\mathcal{M}$ and $\mathcal{N}$ are *algebraically equivalent* if there exists $T_1, \dots, T_n$ connected schemes of finite type over k, $\{s_i, t_i\}$ geometric points of T_i and $\mathcal{L}_i$ line bundles on $X \times T_i$ such that

a. $\mathcal{L}_1|_{X\times\{s_1\}} \cong \mathcal{M}_{\bar{k}}$,

b. $\mathcal{L}_i|_{X\times\{t_i\}} \cong \mathcal{L}_{i+1}|_{X\times\{s_{i+1}\}}$, $1 \le i \le n-1$.

c. $\mathcal{L}_n|_{X\times\{t_n\}} \cong \mathcal{N}_{\bar{k}}$.

Lemma 12 Let $\mathcal{L}$ be a line bundle on X and $\lambda \in \operatorname{Pic}_{X/k}(k)$ be the corresponding point. Then $\lambda \in \operatorname{Pic}^0_{X/k}(k)$ if and only if $\mathcal{L}$ and $\mathcal{O}_X$ are algebraically equivalent.

Proof Let $\lambda, 0 \in \operatorname{Pic}^0_{X/k}(k)$. Then composition

$$(\operatorname{Pic}^0_{X/k})_{\text{red}} \hookrightarrow \operatorname{Pic}^0_{X/k} \hookrightarrow \operatorname{Pic}_{X/k}$$

gives an algebraical equivalence between $\mathcal{L}$ and $\mathcal{O}_X$ via $\mathcal{P}_{\text{univ}}$ on $X \times (\operatorname{Pic}^0_{X/k})_{\text{red}}$.

Conversely, suppose $\mathcal{L}$ and $\mathcal{O}_X$ are algebraically equivalent. Then by definition we have a chain of schemes $T_1, \dots, T_n$. Shrinking T_i if necessary, we can equip each $\mathcal{L}_i$ a trivialization α_i on $\{x\} \times T_i$. Then these pairs $(\mathcal{L}_i, \alpha_i)$ gives rise to morphisms $T_i \to \operatorname{Pic}_{X/k}$. By connectedness, all T_i's map into $\operatorname{Pic}^0_{X/k}$. In particular, $\lambda, 0$ lie in the same component. □

Now we apply the above general theory to the case of an abelian variety A together with the rational point $0 \in A(k)$.

Definition 18 We define $\hat{A} := \mathrm{Pic}^0_{A/k}$. It is a connected projective group scheme over k. We will soon see that $\hat{A}$ is *smooth* (even in positive characteristic), so $\hat{A}$ is a variety, called the *dual abelian variety* of A.

Recall we defined (Definition 8) $\mathrm{Pic}^0(A) = \ker(\phi : \mathrm{Pic}(A) \to \mathrm{Hom}(A(\bar{k}), \mathrm{Pic}(A_{\bar{k}}))$, i.e. $\mathcal{L} \in \mathrm{Pic}^0(A)$ if and only if $T_x^*\mathcal{L} \cong \mathcal{L}$ for all $x \in A(\bar{k})$. The notation suggests some connection between $\mathrm{Pic}^0(A)$ and $\mathrm{Pic}^0_{A/k}$.

Theorem 22 $\mathrm{Pic}^0_{A/k}(k) = \mathrm{Pic}^0(A)$.

Proof First we show that $\mathrm{Pic}^0_{A/k}(k) \subseteq \mathrm{Pic}^0(A)$. Let $\mathcal{P} = \mathcal{P}_{\mathrm{univ}}|_{A \times \hat{A}_{\mathrm{red}}}$. Consider $A \times A \times \hat{A} \xrightarrow[p_1, p_2]{m} A \times \hat{A}$ and $\mathcal{M} = m^*\mathcal{P} \otimes p_1^*\mathcal{P}^{-1} \otimes p_2^*\mathcal{P}^{-1}$. Since $\mathcal{P}|_{\{0\} \times \hat{A}}$ and $\mathcal{P}|_{A \times \{0\}}$ are trivial, we know that $\mathcal{M}|_{\{0\} \times A \times \hat{A}}$, $\mathcal{M}|_{A \times \{0\} \times \hat{A}}$ and $\mathcal{M}|_{A \times A \times \{0\}}$ are trivial, therefore $\mathcal{M}$ is trivial by the Theorem of the Cube 11. Therefore $\mathcal{P}$ is translation invariant. By the universality of $\mathcal{P}$, it follows that any line bundle in $\mathrm{Pic}^0_{A/k}(k)$ is translation invariant, thus lies in $\mathrm{Pic}^0(A)$.

Now pick an ample line bundle on A, by the following theorem the map $\phi_{\mathcal{L}} : A(\bar{k}) \to \mathrm{Pic}^0_{A/k}(\bar{k}) \hookrightarrow \mathrm{Pic}^0(A_{\bar{k}})$ is surjective, hence $\mathrm{Pic}^0_{A/k}(\bar{k}) = \mathrm{Pic}^0(A_{\bar{k}})$, therefore $\mathrm{Pic}^0_{A/k}(k) = \mathrm{Pic}^0(A)$. □

Theorem 23 Let $\mathcal{L}$ be an ample line bundle. Then the map

$$\phi_{\mathcal{L}} : A(\bar{k}) \to \mathrm{Pic}^0(A_{\bar{k}}), \quad x \mapsto T_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$$

is surjective.

To prove this theorem, we need the following lemma.

Lemma 13 Let $\mathcal{L} \in \mathrm{Pic}^0(A)$ be a nontrivial line bundle. Then $H^i(A, \mathcal{L}) = 0$ for any i.

Proof First let us show that $H^0(A, \mathcal{L}) = 0$, Otherwise, $\mathcal{L} \cong \mathcal{O}(D)$ for some effective divisor D. Since $\mathcal{L} \in \mathrm{Pic}^0(A)$, we know that $m^*\mathcal{L} = p_1^*\mathcal{L} \otimes p_2^*\mathcal{L}$. Hence $\mathcal{O}_X = (\mathrm{Id} \times(-1))^* m^*\mathcal{L} \cong \mathcal{L} \otimes (-1)^*\mathcal{L}$. Therefore we know that $0 = D + (-1)^* D$, hence $D = 0$.

In general, let k be the smallest integer such that $H^k(A, \mathcal{L}) \neq 0$. The identity map $A \xrightarrow{\{0\} \times \mathrm{Id}} A \times A \xrightarrow{m} A$ gives us an identity map

$$H^k(A, \mathcal{L}) \xrightarrow{m^*} H^k(A \times A, m^*\mathcal{L}) \xrightarrow{(\{0\} \times \mathrm{Id})^*} H^k(A, \mathcal{L}).$$

This implies that $H^k(A \times A, m^*\mathcal{L}) \neq 0$. But Kunneth formula and the minimality of k, we have know $H^k(A \times A, m^*\mathcal{L}) = 0$, a contradiction. □

Proof (Proof of Theroem 23) We may assume $k = \bar{k}$. Assume $\mathcal{M} \in \mathrm{Pic}^0(A)$ is not of the form $T_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$. We let $\mathcal{N} = m^*\mathcal{L} \otimes p_1^*\mathcal{L}^{-1} \otimes p_2^*(\mathcal{L}^{-1} \otimes \mathcal{M}^{-1})$ be a line bundle on $A \times A$. We calculate $H^i(A \times A, \mathcal{N})$ in two ways via the Leray spectral sequences $H^i(A, R^j(p_1)_*\mathcal{N}) \Rightarrow H^{i+j}(A \times A, \mathcal{N})$ and $H^i(A, R^j(p_1)_*\mathcal{N}) \Rightarrow H^{i+j}(A \times A, \mathcal{N})$.

To calculate $H^i(A, R^j(p_1)_*\mathcal{N})$, we look at the fibers $H^i(A, \mathcal{N}|_{\{x\} \times A})$. By construction $\mathcal{N}|_{\{x\} \times A} = T_x^*\mathcal{L} \otimes \mathcal{L}^{-1} \otimes \mathcal{M}^{-1}$ is nontrivial by assumption and belongs to $\mathrm{Pic}^0(A)$. It follows from the previous lemma that $H^i(A, \mathcal{N}_{\{x\} \times A}) = 0$. So $R^j(p_1)_*\mathcal{N} = 0$ by Theorem 11. Hence $H^i(A \times A, \mathcal{N})$ is zero by the first Leray spectral sequence.

On the other hand, we can loot at the fibers $H^i(A, \mathcal{N}|_{A \times \{x\}})$. By construction $\mathcal{N}|_{A \times \{x\}} = T_x^*\mathcal{L} \otimes \mathcal{L}$, which is trivial if and only if $x \in K(\mathcal{L})$. Since $\mathcal{L}$ is ample, $K(\mathcal{L})$ is finite by Theorem 16. Again by the previous lemma, We know that $R^j(p_2)_*\mathcal{N}|_{A - K(\mathcal{L})} = 0$ and $R^j(p_2)_*\mathcal{N}$ is a coherent sheaf supported on a finite set $K(\mathcal{L})$. By the second Leray spectral sequences, we know $H^i(A, R^j(p_2)_*\mathcal{N}) \Rightarrow H^{i+j}(A \times A, \mathcal{N}) = 0$. Because it is supported on a finite set, we conclude that $R^j(p_2)_*\mathcal{N}$ is actually zero for any j. Thus $H^*(A, \mathcal{N}|_{A \times \{x\}}) = 0$. This is a contradiction because $H^*(A, \mathcal{N}|_{A \times \{0\}}) = H^*(A, \mathcal{O}_A) \neq 0$. That completes the proof that $\mathcal{M} \in \mathrm{Pic}^0(A)$ muse be of the form $T_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$. □

We can extend the definition of $\phi_{\mathcal{L}}$ at the level of schemes: for any S-scheme S and $x : S \to A$. We define $\phi_{\mathcal{L}}(x) = T_x^*\mathcal{L}_S \otimes \mathcal{L}_S^*$ on $A \times S$. Because A is connected, we know that $\phi_{\mathcal{L}}$ lands in $\mathrm{Pic}^0_{A/k} = \hat{A}$.

Corollary 16 If $\mathcal{L}$ is ample, then $\phi_{\mathcal{L}}$ is surjective with finite kernel. In particular, $\dim A = \dim \hat{A}$.

Proof It follows from Theorem 16 and 23. □

Theorem 24 $\hat{A} = \mathrm{Pic}^0_{A/k}$ is smooth (hence is an abelian variety).

Remark 14 $\mathrm{Pic}^0_{X/k}$ is always smooth for abelian varieties and curves, but may not be smooth in general (e.g., for some surfaces).

Proof To prove $\hat{A}$ is smooth, it is enough to show $\dim T_0\hat{A} \leq \dim A$ (because $\dim \hat{A} = \dim A$). By definition, $T_0\hat{A} = \ker(\hat{A}(\Lambda) \to \hat{A}(k))$, which is equal to isomorphism classes of triples

$$\{(\mathcal{L}, \alpha, \beta) : \mathcal{L} \text{ a line bundle on } A \times \Lambda, \alpha : \mathcal{L}|_{\{0\}} \cong \mathcal{O}_A, \beta : \mathcal{L}|_{A \hookrightarrow A\times\Lambda} \cong \mathcal{O}_A\}.$$

Recall that isomorphism classes of line bundles on X is identified with $H^1(X, \mathcal{O}_X^\times)$. By the exact sequence

$$0 \to \mathcal{O}_A \to \mathcal{O}_{A\times\Lambda}^\times \to \mathcal{O}_A^\times \to 1,$$

where the first map is given by $f \mapsto (1 + \varepsilon f)$. This exact sequence splits, so we get a split exact sequence

$$0 \to H^1(A, \mathcal{O}_A) \to H^1(A \times \Lambda, \mathcal{O}_{A\times\Lambda}^\times) \to H^1(A, \mathcal{O}_A^\times) \to 0,$$

namely

$$0 \to T_0\hat{A} \to \mathrm{Pic}(A \times \Lambda) \to \mathrm{Pic}(A) \to 0.$$

So we can identify the tangent space $T_0\hat{A}$ with $H^1(A, \mathcal{O}_A)$, which has dimension $\dim A$ as we shall show in the next section using algebraic facts of bialgebras (cf. Corollary 17). □

Remark 15 This is not the best proof: we can really construct a line bundle in $T_0\hat{A}$ using a cocyle in $H^1(A, \mathcal{O}_A)$.

Hopf algebras

Now let X be a complete variety over k such that $H^0(X, \mathcal{O}_k) = k$. Then

a. $H_X = \bigoplus H^i(X, \mathcal{O}_X)$ is a graded commutative k-algebra with the product given by

$$H_X \otimes H_X \cong H_{X\times X} \xrightarrow{\Delta_X^*} H_X.$$

b. Let $X = A$ be an abelian variety. Then we have a further structure: H_A is a cocommutative coalgebra given by

$$m^* : H_A \to H_{A\times A} \cong H_A \otimes H_A.$$

Moreover, for $h \in H^i$,

$$m^*(h) = 1 \otimes h + h \otimes 1 + \sum_{i>j>0} h'_j \otimes h''_{i-j},$$

and $s^* : H_A \cong H_A$. The follow lemma is straightforward.

Lemma 14 (Δ_X^*, m^*, s^*) makes H_A a finite dimensional positively graded commutative and cocommutative Hopf k-algebra such that $H^0 = k$, $m^*(h) = 1 \otimes h + h \otimes 1 + \sum_{i>j>0} h'_j \otimes h'_{i-j}$.

Remark 16 We say a Hopf algebra (or bialgebra) $(H, m, \delta, \Delta, \varepsilon, S)$ is *graded* if H is a graded vector space and all the morphisms preserve the gradings. We say a Hopf algebra (or bialgebra) is *graded commutative* if for any homogeneous elements a, b, we have $ab = (-1)^{\deg a \deg b} ba$. Similarly we can define the notion of *graded cocommutative* Hopf algebras.

Example 8 (Hopf algebras)

a. Let G/k be affine group scheme over k. Then $H = \Gamma(G, \mathcal{O}_G)$ is a commutative Hopf k-algebra. In fact, the category commutative Hopf algebras is equivalent to the category of affine group k-schemes. If G is commutative, then H is cocommutative.

b. The additive group $\mathbb{G}_a = \mathrm{Spec}\, k[t]$ gives a Hopf algebra structure on $k[t]$. If we put t in an *even* degree, then $k[t]$ is graded commutative and *cocommutative*. Similarly for $\alpha_{p^n} = \mathrm{Spec}\, k[t]/(t^{p^n})$ with t put in an even degree.

c. The group scheme $\Lambda = \mathrm{Spec}\, k[t]/(t^2)$ gives $\Lambda_k[t] := k \oplus kt$ with $t^2 = 0$ a Hopf algebra structure. If we put t in *odd* degree (reason: we need $(\Delta \otimes \Delta)(t \otimes t) = 0$), then it is graded commutative and *cocommutative*.

d. If H_1, H_2 are two graded commutative and cocommutative bialgebra, then $H_1 \otimes H_2$ is also a graded commutative and cocommutative bialgebra. For example, $\Lambda_k[t_1] \otimes \Lambda_k[t_2]$ is equal to the exterior algebra $\bigwedge(kt_1 \oplus kt_2)$ since we require that $t_1t_2 = -t_2t_1$.

Theorem 25 (Borel) Let k be a perfect field and H be a positively graded commutative and cocommutative k bialgebra. If $H^0 = k$ and $\dim H^i < \infty$. Then $H \cong H_1 \otimes H_2 \otimes \cdots H_n$, where p_A's are of the form $k[t]$, $k[t]/(t^{p^n})$ or $\Lambda_k[t]$ in the previous examples.

This is a purely algebraic statement and we will not prove it here. We apply this theorem to $H_A = \bigoplus H^i(A, \mathcal{O}_A)$, which is a graded commutative and cocommutative bialgebra.

Corollary 17 Suppose A is an abelian variety over $k = \bar{k}$ of dimension g, then $\dim H^1(A, \mathcal{O}_A) = g$ and $\bigwedge H^1(A, \mathcal{O}_A) \to H_A$ is an isomorphism. In particular, $\bigwedge^i H^1(A, \mathcal{O}_A) \cong H^i(A, \mathcal{O}_A)$ and $h^i(A) = \binom{g}{i}$.

Proof Because $H^n(A, \mathcal{O}_A) = 0$ for $n > g$. By Theorem 25 we know that

$$H_A \cong \bigwedge(V) \otimes k[t_1, \dots, t_n]/(t^{p^{m_1}}, \dots t^{p^{m_b}}),$$

where V is a graded vector space in odd degrees. Let V_1 be the degree 1 piece of V. Because $g \geq \deg(\bigwedge^{\text{top}} V_1) = \dim V_1$, we know that $\dim V_1 \leq g$. But $V_1 \supseteq H^1(A, \mathcal{O}_A) \cong T_0 \hat{A}$ and $\dim T_0 \hat{A} \geq \dim A = g$, which implies that $\dim V_1 = g$ and $V_1 = H^1(A, \mathcal{O}_A)$. Similarly, if $x \in V_d$ (for $d > 1$) or $x = t_i$ is not in $\bigwedge(V_1)$, then the element $x \otimes \bigwedge^g V_1$ has degree greater than g, a contradiction. Hence $H_A = \bigwedge(V_1)$. □

Polarizations and Jacobian varieties

Note that $\phi_{\mathcal{L}} = \phi_{\mathcal{L} \otimes \mathcal{L}'}$ for any $\mathcal{L}^0 \in \mathrm{Pic}^0(A)$. So in some sense the isogeny $\phi_{\mathcal{L}}$ is more fundamental than the ample line bundle $\mathcal{L}$ itself.

Definition 19 A *polarization* of an abelian variety A is an isogeny $\lambda : A \to \hat{A}$ such that $\lambda \otimes \bar{k} = \phi_{\mathcal{L}}$ for some ample line bundle $\mathcal{L}$ on $A_{\bar{k}}$. λ is called a *principal polarization* if λ is an isomorphism (equivalently, $\deg \lambda = 1$).

Remark 17 Note that a polarization does not necessarily come from a line bundle over k (there are counter examples, though hard to construct). The polarization really lives in the image of the map $H^1(A, \mathcal{O}_A^\times) \to H^2(A, \mathbb{Z})$.

Definition 20 Let X be a complete curve over k with a rational point $x_0 \in X(k)$. Then $\mathrm{Pic}_{X/k}$ is representable. We denote $\mathrm{Pic}^0_{X/k}$ by $J(X)$, called the *Jacobian variety* of X.

Our next goal is to show that $J(X)$ is indeed an abelian variety and admits a canonical principal polarization.

Remark 18 By Lemma 12 and the fact in an algebraic family of line bundles the Euler characteristic does not change, we know that

$$J(X)(\bar{k}) = \{\mathcal{L} \text{ a line bundle on } X_{\bar{k}} : \deg \mathcal{L} = 0\}.$$

It is also true that $T_0 J(X) \cong H^1(X, \mathcal{O}_X)$ by the same argument as in the proof of Theorem 24.

Definition 21 For any d, the *Abel-Jacobi map* AJ^d is defined to be

$$AJ^d : X^d \to J(X), \quad (x_1, \dots x_d) \mapsto \mathcal{O}(x_1 + \cdots x_d - d x_0).$$

At the level of S-points, this map can be defined as $x_i \mapsto \mathcal{O}(\Gamma_{x_i})$, where Γ_{x_i} is the graph of $x_i : S \to X$, which is a Cartier divisor inside $X \times S$.

Proposition 5 $J(X)$ is smooth (hence is an abelian variety).

Proof Since $(AJ^d)^{-1}(\mathcal{L}) = \mathbb{P}(\Gamma(X, \mathcal{L}(d x_0)))$, by Riemann-Roch, AJ^d is surjective and the fibers of AJ^d are projective space of dimension $d - g$ as long as $d > 2g - 2$, where g is the genus of X. In particular, $\dim J(X) \geq g$. But we already know that $\dim T_0 J(X) = \dim H^1(X, \mathcal{O}_X) = g$, thus $J(X)$ is smooth. □

Theorem 26 $J(X)$ admits a canonical principal polarization.

We shall construct a canonical ample divisor Θ on $J(X)$ and show that it gives rise to a principal polarization.

Definition 22 We define the *theta divisor* Θ to be the scheme-theoretic image $\mathrm{Im}(AJ^{g-1})$. By definition,

$$\Theta = \{\mathcal{L} \in J(X) : \Gamma(X, \mathcal{L}((g-1)x_0)) \neq 0\}.$$

Example 9 Let us first consider a special case: $X = E$ is an elliptic curve. Then $J(E) \cong E$ and

$$\Theta = \{\mathcal{O}_E(x - x_0) : \Gamma(E, \mathcal{O}_E(x - x_0)) \neq 0\} \cong x_0.$$

It is well known that $\Theta = x_0$ is an ample divisor and $\phi_\Theta : J(E) \to \widehat{J(E)}$ is an isomorphism. So every elliptic curve is canonically principally polarized. From this point of view, the correct generalization of elliptic curves should be *polarized* abelian varieties rather than abelian varieties themselves.

Proof (Theorem 26) Let $AJ^1 : X \to J(X)$. We obtain the pulling back of line bundles $\tau := (AJ^1)^* : \widehat{J(X)} \to J(X)$. It is then enough to show $\tau \circ \phi_\Theta = -\mathrm{Id} : J(X) \to J(X)$. To do this, we now give a different construction of Θ.

Let S be a noetherian scheme. Let $\mathcal{L}$ be a line bundle on $X \times S$ and $\pi : X \times S \to S$ be the projection. We would like to construct a line bundle on S such that for each $s \in S$, the fiber of it is the determinant of the cohomology

$$\bigwedge^{\text{top}} H^0(X, \mathcal{L}|_{X\times\{s\}}) \otimes \bigwedge^{\text{top}} H^1(X, \mathcal{L}|_{X\times\{s\}}^{-1}).$$

By Theorem 14 there exists a complex $K^0 \to K^1$ of locally free sheaves on S of finite rank such that $R^i\pi_*\mathcal{L} \cong H^i(K^\cdot)$. Let

$$\mathcal{D}et_{\mathcal{L}} := \bigwedge^{\text{top}} K^0 \otimes (\bigwedge^{\text{top}} K^1)^{-1}$$

be a line bundle on S, called the *determinant line bundle* of $\mathcal{L}$. This is independent of the choice of the complex $K^0 \to K^1$ and the formulation commutes with any base change.

Example 10 Suppose $S = X$ and Δ is the diagonal $X \to X \times X$. For $\mathcal{L} = \mathcal{O}(-\Delta)$, $\mathcal{D}et_{\mathcal{L}} = \mathcal{O}_X$. For $\mathcal{L} = \mathcal{O}(\Delta)$, we obtain the canonical sheaf $\mathcal{D}et_{\mathcal{L}} = \omega_X$ (exercise).

Now apply to the case $S = J(X)$. We have a universal line bundle $\mathcal{P}$ on $X \times J(X)$. Let $\mathcal{M} = \mathcal{P} \otimes p_1^*\mathcal{O}((g-1)x_0)$. For any $a \in J(X)$, $\mathcal{M}|_{X\times\{a\}} \cong \mathcal{P}|_{X\times\{a\}} \otimes \mathcal{O}((g-1)x_0)$ has degree $g-1$. Hence by Riemann-Roch, $\chi(\mathcal{M}_a) = 0$. Let $K^0 \to K^1$ be the complex on $J(X)$ representing $R^i(p_2)_*\mathcal{M}$ via Theorem 14. We know that $\dim K_a^0 - \dim K_a^1 = \chi(\mathcal{M}_a) = 0$. Therefore $\operatorname{rank} K^0 = \operatorname{rank} K^1$. So the induced map $\psi : \bigwedge^{\text{top}} K^0 \to \bigwedge^{\text{top}} K^1$ is a map between line bundles, hence is either injective or zero. Consider

$$\{a \in J(X) : \psi_a = 0\} = \{a \in J(X) : K_a^0 \to K_a^1 \text{ is not an isomorphism}\}.$$

This is the locus where $h^0(\mathcal{M}_a) > 0$, i.e, $h^0(\mathcal{P}_a \otimes ((g-1)x_0)) > 0$, which is equal to $\operatorname{Im}(AJ^{g-1} : X^{g-1} \to J(X))$. This is exactly the divisor $\Theta \subsetneq J(X)$ and thus ψ is injective.

Using this construction of Θ, we know that $\bigwedge^{\text{top}} K^0 \otimes (\bigwedge^{\text{top}} K^1)^{-1} \subseteq \mathcal{O}_{J(X)}$ is an ideal sheaf. The quotient is supported on Θ, hence is $\mathcal{O}_{n\Theta}$ for some $n \geq 1$. So $\mathcal{D}et_{\mathcal{M}}^{-1} \cong \mathcal{O}(n\Theta)$ for some $n \geq 1$. We claim that $\tau \circ \phi_{\mathcal{D}et_{\mathcal{M}}^{-1}} = -\operatorname{Id} : J(X) \to J(X)$. This is enough because $\phi_{\mathcal{D}et_{\mathcal{L}}^{-1}} = n\phi_\Theta$ implies that $n = 1$ and $\mathcal{D}et_{\mathcal{M}}^{-1} = \mathcal{O}(\Theta)$.

Showing $\tau \circ \phi_{\mathcal{D}et_{\mathcal{M}}^{-1}} = -\operatorname{Id}$ is equivalent to showing that $\tau(\phi_{\mathcal{D}et_{\mathcal{M}}^{-1}}(a)) = -a$ for any $a \in J(X)$, or, $\tau(T_a^*\mathcal{D}et_{\mathcal{M}}^{-1} \otimes \mathcal{D}et_{\mathcal{M}}) = -a$. Note that $\tau(\mathcal{M}) = \mathcal{M}|_{AJ^1(X)}$, this is equivalent to showing that $T_a^*\mathcal{D}et_{\mathcal{M}}^{-1} \otimes \mathcal{D}et_{\mathcal{M}}|_{AJ^1(X)} = -a$. Since $T_a^*\mathcal{D}et_{\mathcal{M}}|_{AJ^1(X)} = \mathcal{D}et_{\mathcal{M}}|_{AJ^1(X)-a}$. By the base change using $X \times X \xrightarrow{\text{Id}\times(AJ^1-a)} X \times J(X)$, it is equal to $\mathcal{D}et_{\mathcal{M}|_{AJ^1(X)-a}}$. Since

$$\mathcal{M}|_{X\times(AJ^1(X)-a)} \cong \mathcal{P} \otimes p_1^*\mathcal{O}((g-1)x_0)|_{AJ^1-a},$$

and

$$\mathcal{P}|_{X\times AJ^1(X)} = \mathcal{O}(\Delta - \{x_0\} \times X),$$

we know that

$$\mathcal{N} := \mathcal{M}|_{X\times(AJ^1(X)-a)} \cong \mathcal{O}(\Delta + (g-1)(\{x_0\} \times X)) \otimes p_1^*\mathcal{P}_a.$$

Lemma 15 Let $\mathcal{L}$ be a line bundle on X and $\mathcal{J} = \mathcal{O}(\Delta) \otimes p_1^*\mathcal{L}$. Then $\mathcal{D}et_{\mathcal{J}} \cong \mathcal{D}et_{\mathcal{O}(\Delta)} \otimes \mathcal{L}$.

Proof By induction, it is enough to prove that $\mathcal{D}et_{\mathcal{O}(\Delta)\otimes p_1^*\mathcal{L}(x)} = \mathcal{D}et_{\mathcal{O}(\Delta)\otimes p_1^*\mathcal{L}} \otimes \mathcal{O}(x)$. By the exact sequence on $X \times X$,

$$0 \to \mathcal{O}(\Delta) \otimes p_1^*\mathcal{L} \to \mathcal{O}(\Delta) \otimes p_1^*\mathcal{L}(x) \to (\iota_x)_*\mathcal{O}(x) \to 0,$$

where $\iota_x : \{x\} \times X \hookrightarrow X \times X$ (the poles only occurs at x when it intersects Δ). All these are flat over the second factor, the result follows from taking the determinant line bundles. □

From this lemma, we know that $\mathcal{D}et_{\mathcal{N}} = \mathcal{D}et_{\mathcal{O}(\Delta+(g-1)(\{x_0\}\times X)} \otimes \mathcal{P}_a$. Since the left hand side is $T_a^*\mathcal{D}et_{\mathcal{M}}|_{X\times AJ^1(X)}$ and the right hand side is $\mathcal{D}et_{\mathcal{M}}|_{X\times AJ^1(X)} \otimes \mathcal{P}_a$, taking the inverses finishes the proof of Theorem 26. □

Duality of abelian varieties

Let G be a commutative finite (hence affine) group scheme over k. Then $H := \Gamma(G, \mathcal{O}_G)$ is a finite dimensional commutative and cocommutative Hopf algebra over k. Let $H^* = \operatorname{Hom}_k(H, k)$ be the dual of H, it has a natural structure of commutative and cocommutative Hopf algebra over k induced by that of H.

Definition 23 $\hat{G} := \operatorname{Spec} H^*$ is a commutative finite group scheme over k, called the *Cartier dual* of G. The natural *dual functor* $\mathbb{D} : G \to \hat{G}$ satisfies $\mathbb{D}^2 = \mathrm{Id}$.

Definition 24 Let G_1, G_2 be two commutative group schemes over S. We define the functor

$$\underline{\mathrm{Hom}}(G_1, G_2) : \mathbf{Sch}/S \to \mathbf{Ab}, \quad T/S \mapsto \mathrm{Hom}_{T\text{-gp sch}}(G_{1,T}, G_{2,T}).$$

Proposition 6 $\hat{G} \cong \underline{\mathrm{Hom}}(G, \mathbb{G}_m)$.

Proof Let R be a k-algebra. We want to show that $\hat{G}(R) = \underline{\mathrm{Hom}}(G, \mathbb{G}_m)(R)$. By definition, $\hat{G}(R) = \mathrm{Hom}_{k\text{-alg}}(H^*, R) = \mathrm{Hom}_{R\text{-alg}}(H_R^*, R)$. Since $H_{R\text{-alg}}(H_R^*, R) \subseteq H_{R\text{-lin}}(H_R^*, R) = H_R$, we may regard an element of $\hat{G}(R)$ as an element of H_R. For $\phi \in H_R$, one can check that $\phi \in H_{R\text{-alg}}(H_R^*, R)$ if and only if $\Delta_R(\phi) = \phi \otimes \phi$ and $\varepsilon_R(\phi)$ is invertible, hence corresponds exactly to the elements of $\mathrm{Hom}_{R\text{-Hopf}}(R[t, t^{-1}], H_R) = \underline{\mathrm{Hom}}(G, \mathbb{G}_m)(R)$. □

Example 11 For $G = \mathbb{Z}/n\mathbb{Z}$, $\hat{G}(R) \cong \{\phi \in R^\times : \phi^n = 1\}$. Therefore $\hat{G} = \mu_n$. One also has $\widehat{\alpha_p} \cong \alpha_p$ (the dual pairing is given by the truncated exponent).

The following is the main result of this section.

Theorem 27 Let $f : A \to B$ be an isogeny of abelian varieties. Then the induced morphism of dual abelian varieties $\hat{f} : \hat{B} \to \hat{A}$ is also an isogeny and $\ker \hat{f} = \widehat{\ker f}$.

Remark 19 Here is an informal reasoning which can be made rigorous. For a line bundle $\mathcal{L}$ on X, we let $L = \mathrm{Tot}(\mathcal{L})$ be the total space $\mathcal{L}$. Then L is a scheme affine over X and $L^\times := L - \{0\}$ is a $\mathbb{G}_m$-torsor. Moreover, for $f : X \to Y$ and $\mathcal{L}$ a line bundle on Y, we have $\mathrm{Tot}(f^*\mathcal{L})^\times = X \times_Y L^\times$. Applying to the case of abelian varieties, we obtain that the dual abelian variety $\hat{A} = \{\mathcal{L} \text{ on } A : m^*\mathcal{L} \cong p_1^*\mathcal{L} \otimes p_2^*\mathcal{L}\}$ can be identified as $\mathbb{G}_m$-torsors $L^\times$ on A satisfying the following commutative diagram

$$\begin{array}{ccc} L^\times \times L^\times & \longrightarrow & L^\times \\ \downarrow & & \downarrow \\ A \times A & \longrightarrow & A. \end{array}$$

These $\mathbb{G}_m$-torsors correspond to central extensions of commutative group schemes

$$1 \to \mathbb{G}_m \to L^\times \to A \to 1.$$

In other words, $\hat{A} \cong \mathrm{Ext}^1(A, \mathbb{G}_m)$. Using this interpretation of dual abelian varieties, applying $\mathrm{Hom}(-, \mathbb{G}_m)$ to the exact sequence $0 \to K \to A \to B \to 0$ gives the required exact sequence

$$0 \to \hat{K} \to \hat{B} \to \hat{A} \to 0$$

as $\mathrm{Hom}(A, \mathbb{G}_m) = 0$ and $\mathrm{Ext}^1(K, \mathbb{G}_m) = 0$.

To prove Theorem 27, we need a theorem of Grothendieck on fppf descent. Let $f : X_0 \to Y$ be a morphism of schemes. Then we have the following morphisms (projections)

$$X_2 = X_1 \times_{X_0} X_1 \underset{p_{23} \cdot p_{13}}{\overset{p_{12}}{\longrightarrow}} X_1 = X_0 \times_Y X_0 \underset{p_2}{\overset{p_1}{\rightrightarrows}} X_0 \to Y.$$

Suppose $\mathcal{F} \in \mathrm{Qcoh}(Y)$, the pullback sheaf $\mathcal{G} = f^*\mathcal{F} \in \mathrm{Qcoh}(X_0)$ has some additional properties:

a. there is a canonical isomorphism $\theta : p_1^*\mathcal{G} \cong p_2^*\mathcal{G}$;

b. restricting to the diagonal we get $\theta|_\Delta = \mathrm{Id}$;

c. if we further pullback to X_2, we obtain a cocycle relation $p_{23}^*(\theta)p_{12}^*(\theta) = p_{13}^*(\theta)$.

Motivated by this, we define the *category of descent data*

$$\mathrm{Desc}(X_0, Y) := \left\{ (\mathcal{G}, \theta) : \begin{array}{c} \mathcal{G} \in \mathrm{Qcoh}(X_0), \theta : p_1^*\mathcal{G} \cong p_2^*\mathcal{G}, \\ \theta|_\Delta = \mathrm{Id}, p_{23}^*(\theta)p_{12}^*(\theta) = p_{13}^*(\theta) \end{array} \right\}.$$

We then have a functor $f^* : \mathrm{Qcoh}(Y) \to \mathrm{Desc}(X_0, Y)$ extending the original functor $f^* : \mathrm{Qcoh}(Y) \to \mathrm{Qcoh}(X_0)$.

Theorem 28 (Grothendieck) If f is fppf (faithfully flat, locally of finite presentation), then f^* is an equivalence of categories.

Applying to our case, we need the following lemma.

Lemma 16 Let $f : A \to B$ be an isogeny of abelian varieties. Then f is fppf.

Proof We only need to check that f is flat, which can be shown by generic flatness since f is a morphism of group varieties. □

Proof (Proof of Theorem 27) $\ker \hat{f}(S)$ equals to

$$\{(\mathcal{L}, \alpha) : \mathcal{L} \text{ line bundle on } B \times S, \alpha : \mathcal{L}|_{\{0\}\times S} \cong \mathcal{O}_S, f^*(\mathcal{L}, \alpha) \cong (\mathcal{O}_{A\times S}, \alpha\},$$

which is exactly the isomorphism classes of $\mathcal{L}$ on $B \times S$ such that $f^*\mathcal{L} \cong \mathcal{O}_{A\times S}$. Now we apply the previous theorem to our case $X_0 = A \times S$, $Y = B \times S$ and $A \times S \xrightarrow{f\times \mathrm{Id}} B \times S$ (it is fppf by the previous lemma), we obtain

$$\ker \hat{f}(S) = \{(\mathcal{O}_{A\times S}, \theta) \in \mathrm{Desc}(A \times S, B \times S)\}.$$

Let $G = \ker f$. Then $X_1 = X_0 \times_Y X_0 \cong A \times S \times G$ with two projections p and m (multiplication on $A \times G$) to $X_0 = A \times S$. Also $X_2 = A \times S \times G \times G$ with three projections p_1, p_2 and m to $X_1 = A \times S \times G$. By construction, $p^*\mathcal{O}_{A\times S} \cong \mathcal{O}_{A\times S\times G}$ and $m^*\mathcal{O}_{A\times S} \cong \mathcal{O}_{A\times S\times G}$, we know that

$$\theta \in \Gamma(A \times S \times G, \mathcal{O}^\times_{A\times S\times G}) = \Gamma(S \times G, \mathcal{O}^\times_{S\times G}),$$

where the latter equality is because A is an abelian (hence projective) variety. Now the condition $\theta|_\Delta = \mathrm{Id}$ can be translated into that $\varepsilon(f) = 1$ for the counit $\varepsilon : \mathcal{O}_G \to k$ since the diagonal map is given by $A \times S \times \{e\} \to A \times S \times G$. Similarly, the cocycle condition can be translated into that $\Delta(f) = f \otimes f$. So

$$\begin{aligned}\ker \hat{f}(S) &= \{f \in \Gamma(S \times G, \mathcal{O}^\times_{S\times G}) : \varepsilon(f) = 1, \Delta(f) = f \otimes f\} \\ &= \mathrm{Hom}(G_S, \mathbb{G}_m) = \hat{G}(S).\end{aligned}$$

It follows that $\ker \hat{f} = \widehat{\ker f}$. □

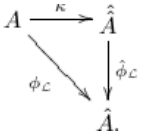
Corollary 18 If f is an isogeny, then $\deg f = \deg \hat{f}$.

Proof Because $\deg f = \dim \Gamma(G, \mathcal{O}_G)$ for $G = \ker f$. □

Definition 25 Let A, B be two abelian varieties over k of the same dimension. A line bundle Q on $A \times B$ is called a *divisorial correspondence* if $Q|_{\{0\}\times B} \cong \mathcal{O}_B$ and $Q|_{A\times\{0\}} \cong \mathcal{O}_A$. A divisorial correspondence Q induces a morphism $\kappa_Q : B \to \hat{A}$ of abelian varieties (in general, a line bundle $\mathcal{L}$ on $A \times S$ gives a morphism $S \to \mathrm{Pic}_A$). The morphism κ_Q is actually a homomorphism since it sends 0 to 0. Let $\sigma : B \times A \cong A \times B$ be the flipping isomorphism. Then we have a homomorphism $\kappa_{\sigma^*Q} : A \to \hat{B}$.

Example 12 Let $\mathcal{P}$ be the Poincare line bundle on $A \times \hat{A}$. Then $\kappa_\mathcal{P} = \mathrm{Id}$ by the definition of $\hat{A}$. Also we have $\kappa_{\sigma^*\mathcal{P}} : A \to \hat{\hat{A}}$. Denote $\kappa = \kappa_{\sigma^*\mathcal{P}}$.

Proposition 7 Let $\mathcal{L}$ be a line bundle on A. The we have the following commutative diagram



Proof Consider $A \times A \xrightarrow{1\times\phi_\mathcal{L}} A \times \hat{A}$. We claim that

$$(1 \times \phi_\mathcal{L})^*\mathcal{P} \cong m^*\mathcal{L} \otimes p_1^*\mathcal{L}^{-1} \otimes p_2^*\mathcal{L}^{-1}.$$

To prove it, we use Seesaw Theorem 15. The restriction to $A \times \{x\}$ of $(1 \times \phi_\mathcal{L})^*\mathcal{P}$ is $T_x^*\mathcal{L} \otimes \mathcal{L}^{-1} = m^*\mathcal{L} \otimes p_1^*\mathcal{L}^{-1} \otimes p_2^*\mathcal{L}^{-1}$. So we only need to show that the restriction to $\{0\} \times A$ of $(1 \times \phi_\mathcal{L})^*\mathcal{P}$ is the same as $m^*\mathcal{L} \otimes p_1^*\mathcal{L}^{-1} \otimes p_2^*\mathcal{L}^{-1}$. This is true because both are trivial and the claim follows. So we have $(1 \times \phi_\mathcal{L})^*\mathcal{P}|_{\{x\}\times A} \cong T_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$. Since the left hand side is $\phi_\mathcal{L}^*(\mathcal{P}|_{\{x\}\times\hat{A}}) = \hat{\phi}_\mathcal{L} \circ \kappa(x)$ (by definition of κ) and the right hand side is $\phi_\mathcal{L}(x)$, the required result then follows. □

Corollary 19 κ is an isomorphism.

Proof Pick $\mathcal{L}$ an ample line bundle, then $\phi_\mathcal{L}$ and $\hat{\phi}_\mathcal{L}$ are isogenies. Because $\phi_\mathcal{L} = \hat{\phi}_\mathcal{L} \circ \kappa$, we know κ is also an isogeny. Now $\deg \phi_\mathcal{L} = \deg \hat{\phi}_\mathcal{L}$ implies that $\deg \kappa = 1$. □

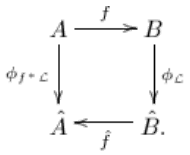
Thus we can identify A and $\hat{\hat{A}}$ via κ. Under this identification we have $\phi_\mathcal{L} = \hat{\phi}_\mathcal{L}$.

Definition 26 A morphism $\lambda : A \to \hat{A}$ is called *symmetric* if $\lambda = \hat{\lambda}$.

Remark 20 Any polarization is be symmetric. So not every isogeny is a polarization because there exists non-symmetric isogenies.

Finally, it is easy to check the following proposition by definition.

Proposition 8 Let $f : A \to B$ be a morphism and $\mathcal{L}$ a line bundle on B. Then $\hat{f} \circ \phi_\mathcal{L} \circ f = \phi_{f^*\mathcal{L}}$, namely we have the following commutative diagram



Finite group schemes and torsion

Definition 27 Let G be a finite group scheme over k. We say

- G is *local* if $G = G^0$ (connected).
- G is *etale* if $k[G]$ is an etale k-algebra. Recall that a k-algebra A of finite type is called *etale* if $\Omega_{A/k} = 0$, equivalently, $A = \prod_i L_i$, where L_i's are finite separable field extensions of k.

Example 13 $\mu_n = \operatorname{Spec} k[x]/(x^n - 1)$ is etale if and only if $(n, p) = 1$. It is local if and only if n is a p-power.

Example 14 α_{p^n} is local.

We will soon see that local group schemes and etale group schemes are building blocks of finite group schemes: the connected component G^0 of G is local k-group and the quotient G/G^0 is etale. Let us study etale group schemes first.

Lemma 17 Fix k^s a separable closure of k. Then the category of finite etale k-algebras (= category of finite etale k-schemes) is equivalent to the category of finite $\operatorname{Gal}(k^s/k)$-sets. The equivalence is given by sending a k-scheme X to $X(k^s)$.

Proof (Sketch) This is basically the main theorem of Galois theory. Let X be a finite etale k-scheme. Then $X(k^s)$ admits a $\operatorname{Gal}(k^s/k)$ action. Conversely, if T is a $\operatorname{Gal}(k^s/k)$-set, we form the k-algebra $(\prod_{t\in T} k^s)^{\operatorname{Gal}(k^s/k)}$, where the action of $\operatorname{Gal}(k^s/k)$ is the diagonal action. □

Corollary 20 The category of etale k-group schemes is equivalent to the category of finite groups with $\operatorname{Gal}(k^s/k)$-action.

Example 15 The etale k-group scheme μ_n, $(n, p) = 1$, corresponds to the finite group $\mu_n(k^s)$ (n-th roots of unity in k^s) with the natural $\operatorname{Gal}(k^s/k)$-action. This action defines $\operatorname{Gal}(k^s/k) \to \operatorname{Aut}(\mu_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ by sending $\sigma \mapsto \chi(\sigma)$, where χ is the cyclotomic character so that $\sigma(\zeta) = \zeta^{\chi(\sigma)}$ for ζ a primitive n-th root of unity.

Proposition 9 Let X be a k-scheme of finite type. Then there exists a finite etale k-scheme $\pi_0(X)$ together with a morphism $q : X \to \pi_0(X)$ which is universal in the following sense: if $q' : X \to Y$ with Y finite etale, then there exists a unique $f : \pi_0(X) \to Y$ such that $q' = f \circ q$. In addition, q is faithfully flat and the fibers of q are connected components of X.

Proof (Sketch) We define $\pi_0(X)$ by $\pi_0(X)(k^s) = \pi_0(X_{k^s})$ together with the natural $\operatorname{Gal}(k^s/k)$-action. Over k^s, $\pi_0(X)$ is a product of copies of k^s and the map $q : X \to \pi_0(X)$ is simply the structure map (clearly flat). This is equivariant with respect to the $\operatorname{Gal}(k^s/k)$-action, therefore descents to k. □

Corollary 21 If G is a k-group scheme of finite type, then $\pi_0(G)$ is an etale k-group scheme and $q : G \to \pi_0(G)$ is a homomorphism.

Corollary 22 Every finite k-group scheme G fits into the following exact sequence (meaning the map $G \to G_{\text{et}}$ is faithfully flat with kernel G_{loc}):

$$1 \to G_{\text{loc}} \to G \to G_{\text{et}} \to 1.$$

Moreover, if k is perfect, this exact sequence splits canonically.

Proof (Sketch) For the first part, we take $G_{\text{loc}} = G^0$ and $G_{\text{et}} = \pi_0(G)$. When k is perfect, G_{red} is a k-group scheme (since when k is perfect, the fiber product of two reduced schemes is still reduced), so we obtain a morphism $G_{\text{red}} \hookrightarrow G$. One can check the composition $G_{\text{red}} \hookrightarrow G \to \pi_0(G)$ is an isomorphism by checking this over k^s. □

Definition 28 Let G be a commutative finite k-group scheme. We say G is *etale-etale* if G is etale and $\hat{G}$ is etale. We define similarly the notion of *etale-local*, *local-etale* and *local-local*.

Corollary 23 Suppose k is perfect. Let G be commutative finite k-group scheme. Then G can be decomposed into a product of these four types of groups

$$G \cong G_{\text{et,et}} \times G_{\text{et,loc}} \times G_{\text{loc,et}} \times G_{\text{loc,loc}}.$$

Moreover, this decomposition is unique.

Proof Apply the previous decomposition twice. □

Remark 21 Suppose k is algebraically closed. All etale-etale k-group schemes must be a product of etale k-group schemes of the form μ_n. Furthermore, we have a non-canonical isomorphism $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$ depending on a choice of primitive root of unity. Similarly, all etale-local k-group schemes must be a product of $\mathbb{Z}/p^n\mathbb{Z}$ and all local-etale k-group schemes must be a product of μ_{p^n}. However, there are a lot of local-local k-group schemes even in this case.

Remark 22 Suppose $\operatorname{char}(k) = 0$. Then $G = G_{\text{et,et}}$ since there are no nontrivial local k-group schemes.

Local groups are more complicated than etale groups. Fortunately, they can be built by more basic blocks.

Definition 29 A local k-group scheme G is called *of height one* if $x^p = 0$ for any $x \in \mathfrak{m}$, where $\mathfrak{m}$ is the maximal ideal at $e \in G$.

Lemma 18 Suppose G is of height one, then the coordinate ring $k[G] \cong k[x_1, \dots, x_n]/(x_1^p, \dots, x_n^p)$. In particular, $\dim k[G]$ is a p-power.

Proof Let $x_i \in \mathfrak{m}$ such that $x_i \mod \mathfrak{m}^2$ form a basis of $\mathfrak{m}/\mathfrak{m}^2$. Since G is local, we know that $k[G]$ is a local ring, thus there is a surjection $k[x_1, \dots, x_n]/(x_1^p, \dots, x_n^p) \to k[G]$. We need to show that there is no relation between $\prod_i {x_i}^{n_i}$ for $0 \le n_i < p$. Taking the dual basis of x_i, we can produce left invariant vector fields D_i on G such that $D_i(x_j) = \delta_{ij} \mod \mathfrak{m}$. Suppose $F = 0$ is a relation with the smallest degree, then $DF = 0$ gives a relation with a lower degree, a contradiction. □

Let G be any k-group scheme of finite type. Let $F : G \to G$ be the Frobenius morphism and $F^{(1)} : G \to G^{(1)}$ be the relative Frobenius (cf. Example 6).

Lemma 19 $F^{(1)}$ is a group homomorphism.

Proof We want to check that for any scheme S, $G(S) \to G^{(1)}(S)$ is a group homomorphism. This is because F commutes with any reasonable base change (in particular, we can base change the multiplication diagram). □

We denote $G^F := \ker F^{(1)}$. The morphism $G^F \to G$ factors through the local group $\operatorname{Spec} \mathcal{O}_{G,e}$ and we have a cartesian diagram of schemes

$$\begin{array}{ccc} \operatorname{Spec} \mathcal{O}_{G,e} & \xrightarrow{F} & \operatorname{Spec} \mathcal{O}_{G^{(1)},e} \\ \downarrow & & \downarrow \\ G & \xrightarrow{F^{(1)}} & G^{(1)}. \end{array}$$

Thus we have a cartesian diagram

$$\begin{array}{ccc} G^F & \longrightarrow & \operatorname{Spec} k \\ \downarrow & & \downarrow \\ \operatorname{Spec} \mathcal{O}_{G,e} & \xrightarrow{F^{(1)}} & \operatorname{Spec} \mathcal{O}_{G^{(1)},e}, \end{array}$$

and $k[G^F] = \mathcal{O}_{G,e}/\mathfrak{m}_{G,e}^{(p)}$ where $\mathfrak{m}^{(p)} = \{x^p, x \in \mathfrak{m}\}$. In particular, G^F is a local group (topologically one point) of height one and $\operatorname{Lie} G^F \cong \operatorname{Lie} G$. We cannot recover G from its Lie algebra, however, we have the following

Theorem 29 The functor $G \mapsto \operatorname{Lie} G$ is an equivalence of categories between height one group schemes and p-Lie algebra.

Proof (Sketch) Let us construct the inverse functor. From a Lie algebra $\mathfrak{g}$, we can construct an associative algebra, its universal enveloping algebra $U\mathfrak{g}$. In fact $U\mathfrak{g}$ is also a cocommutative Hopf algebra, where the comultiplication is given by $\Delta(x) = 1 \otimes x + x \otimes 1$ for any $x \in \mathfrak{g}$ (and extends uniquely to $U\mathfrak{g}$). Futhermore, $\{v \in U\mathfrak{g} : \Delta(v) = 1 \otimes v + v \otimes 1\}$ is exactly $\mathfrak{g}$. Now using the $-^{(p)}$ operation from the p-Lie algebra structure, we define $u\mathfrak{g} = U\mathfrak{g}/(x^p - x^{(p)})_{x \in \mathfrak{g}}$. One can check $u\mathfrak{g}$ is a *finite dimensional* cocommutative Hopf algebra. The inverse functor then sends $\mathfrak{g}$ to $G = \operatorname{Spec}(u\mathfrak{g})^*$. □

Remark 23 When $\operatorname{char}(k) = 0$, there is an analogous equivalence between Lie algebras and formal groups.

Corollary 24 If G is commutative of height one, then $p_G : G \to G$ is zero.

Proof The morphism $p_G : G \to G$ gives $dp_G : \operatorname{Lie} G \to \operatorname{Lie} G$ which is multiplication by p, hence is zero in characteristic p. Now by the previous theorem, we know that $p_G = 0$. □

Corollary 25 If G is local and commutative, then there exists some n such that $n_G : G \to G$ is zero.

Proof By iterating we obatin morphisms

$$G \xrightarrow{F^{(1)}} G^{(1)} \xrightarrow{F^{(1)}} G^{(2)} \to \cdots.$$

Since G is local, this gives inclusions $G^F \hookrightarrow G^{F^{(2)}} \hookrightarrow \cdots G = G^{F^{(n)}}$ for some n (which can be chosen as the dimension of the coordinate ring $k[G]$). Using the previous corollary, G^F is killed by p. By induction we can show that G^{F^i} is killed by p_1 since the image of $p : G^{F^{(i)}} \to G^{F^{(i)}}$ lies in $G^{F^{(i-1)}}$. □

Corollary 26 If G is finite and commutative, then there exists some n such that $n_G : G \to G$ is zero.

Proof Use the decomposition in Corollary 22 and the previous corollary. □

Corollary 27 Let $f : A \to B$ be an isogeny of abelian varieties. Then there exists some $n_A : A \to A$ and an isogeny $g : B \to A$ such that $g \circ f = n_A$.

Proof We need another fact from Grothendieck's descent theory.

> **Theorem 30** Let $f : U \to V$ be faithfully flat, of finite presentation and X be a scheme. Then $\mathrm{Hom}(V, X) \to \mathrm{Hom}(U, X) \rightrightarrows \mathrm{Hom}(U \times_V U, X)$ is an equalizer diagram.

Apply this theorem to $f : A \to B$ and $X = A$. We only need to show that the two compositions $A \times \ker f \cong A \times_B A \to A \xrightarrow{n_A} A$ are the same. This can be done by choosing n killing $\ker f$ (which can be chosen as $\deg f$ from the previous discussion). So n_A factors through $f : A \to B$. □

Remark 24 From the proof one sees that n can be chosen as $\deg f$.

Example 16 The morphism $p_A : A \to A$ factors through the relative Frobenius $F : A \to A^{(1)}$. In other words, there exists $V : A^{(1)} \to A$ such that $VF^{(1)} = p_A$. Then $F^{(1)}VF^{(1)} = F^{(1)}p_A = p_{A^{(1)}}F^{(1)}$ (since Frobenius commutes with any morphism) which implies that $F^{(1)}V = p_{A^{(1)}}$. The morphism V is called the *Verschiebung*.

Lemma 20 The Cartier dual $\widehat{A[n]}$ isomorphic to $\hat{A}[n_{\hat{A}}]$.

Proof By Theorem 27, we only need to show $\hat{n}_A = n_{\hat{A}}$. By definition, the morphism $\hat{n}_A$ sends $\mathcal{L} \in \hat{A}$ to $n_A^*\mathcal{L}$, which is equal to $\mathcal{L}^n$ by Corollary 5 and $(-1)^*\mathcal{L} = \mathcal{L}^{-1}$ for $\mathcal{L} \in \hat{A}$. □

Now write $n = n_1 \cdot p^m$, where $(n_1, p) = 1$. Then $A[n_1]$ and $A[p^m]$ are both closed subgroups of $A[n]$.

Proposition 10 The natural morphism $A[n_1] \times A[p^m] \to A[n]$ is an isomorphism.

Proof By the previous lemma, $A[n_1]$ is etale-etale since $(n_1, p) = 1$. We also know

$$A[p^m]_{\bar{k}} = (A[p^m]_{\bar{k}})_{\mathrm{et,loc}} \times (A[p^m]_{\bar{k}})_{\mathrm{loc,et}} \times (A[p^m]_{\bar{k}})_{\mathrm{loc,loc}}.$$

These two parts together give the decomposition in Corollary 22 for $A[n]$. The result then follows from the uniqueness of such decomposition. □

From Remark 21, we know that

$$(A[n_1])_{\bar{k}} \cong (\mathbb{Z}/n_1\mathbb{Z})^{2g}, \quad (A[p^m]_{\bar{k}})_{\mathrm{et,loc}} \cong (\mathbb{Z}/p^m\mathbb{Z})^r, \quad (A[p^m]_{\bar{k}})_{\mathrm{loc,et}} = \mu_{p^m}^s,$$

for some integers r and s.

Proposition 11 r is an invariant under isogeny (called the p*-rank* of A).

Proof Let $f : A \to B$ be an isogeny and $i = \dim k[\ker f]$. Then f induces a morphism $A[p^m] \to B[p^m]$ and comparing the orders gives $p^{mr_A} \leq i \cdot p^{mr_B}$ for any m, hence $r_A \leq r_B$. By Corollary 27, we have another isogeny $g : B \to A$. By the same reason one knows that $r_A \geq r_B$. □

Corollary 28 $r = s$.

Proof Apply the previous proposition to the isogeny $A \to \hat{A}$ and use Lemma 20. □

Tate modules and p-divisible groups

Recall that (Definition 5) for $\ell \neq p$ we defined the ℓ*-adic Tate module* $T_\ell(A) := \varprojlim_m A[\ell^m](\bar{k})$ (equal to $\varprojlim_m A[\ell^m](k^s)$ since $A[\ell^m]$ is etale). This is a free $\mathbb{Z}_\ell$-module of rank g with a continuous action of $\mathrm{Gal}(\bar{k}/k)$. An isogeny $f : A \to B$ induces an continuous map $T_\ell(f) : T_\ell(A) \to T_\ell(B)$. This notion is valid for any commutative group schemes other than abelian varieties. For example, the ℓ-adic Tate module of the multiplicative group $T_\ell\mathbb{G}_m = \varprojlim_m \mu_{\ell^m} =: \mathbb{Z}_\ell(1)$ is a free $\mathbb{Z}_\ell$ module of rank 1 where $\mathrm{Gal}(\bar{k}/k)$ acts via the cyclotomic character $\chi : \mathrm{Gal}(\bar{k}/k) \to \mathbb{Z}_\ell^\times$.

Definition 30 Suppose M is a free $\mathbb{Z}_\ell$-module of finite rank with an action of $\mathrm{Gal}(\bar{k}/k)$. We define the *Tate twists of* M by $M(n) := M \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell(1)^{\otimes n}$ for $n \geq 0$ and $M(n) := M \otimes_{\mathbb{Z}_\ell} (\mathbb{Z}_\ell(1)^\vee)^{\otimes -n}$ for $n < 0$.

Proposition 12 $(T_\ell A)^\vee(1) \cong T_\ell \hat{A}$.

Proof From $\hat{A}[\ell^m] \cong \widehat{A[\ell^m]}$, we know that

$$\hat{A}[\ell^m](\bar{k}) = \mathrm{Hom}(A[\ell^m]_{\bar{k}}, \mathbb{G}_{m,\bar{k}}) = \mathrm{Hom}(A[\ell^m]_{\bar{k}}, \mu_{\ell^m,\bar{k}}).$$

Passing to the limit we obtain that $T_\ell \hat{A} \cong \mathrm{Hom}(T_\ell A, \mathbb{Z}_\ell(1))$. □

Proposition 13 Let $f : A \to B$ be an isogeny and N be its kernel. Then we have a short exact sequence of $\mathbb{Z}_\ell[\mathrm{Gal}(k^s/k)]$-modules

$$1 \to T_\ell(A) \xrightarrow{T_\ell(f)} T_\ell(B) \to N_\ell(k^s) \to 0,$$

where $N_\ell(k^s)$ is the ℓ-Sylow subgroup of $N(k^s)$.

Proof Observe that

$$\begin{aligned} T_\ell(A) &= \varprojlim A[\ell^m](\bar{k}) = \varprojlim \mathrm{Hom}(\mathbb{Z}/\ell^m\mathbb{Z}, A(\bar{k})) \\ &= \mathrm{Hom}(\varinjlim \mathbb{Z}/\ell^m\mathbb{Z}, A(\bar{k})) = \mathrm{Hom}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, A(\bar{k})). \end{aligned}$$

From the exact sequence

$$0 \to N(\bar{k}) \to A(\bar{k}) \to B(\bar{k}) \to 0,$$

we obtain a long exact sequence

$$\mathrm{Hom}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N(\bar{k})) \to T_\ell(A) \to T_\ell(B) \to \mathrm{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N(\bar{k})) \to \mathrm{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, A(\bar{k}$$

The first term is zero since $N(\bar{k})$ is finite and the last term is o since $A(\bar{k})$ is divisible. So we only need to understand the group $\mathrm{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N(\bar{k}))$. Using the isomorphism $N \cong N_\ell \times N^\ell$, we know that

$$\mathrm{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N(\bar{k})) = \mathrm{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N_\ell(\bar{k}) \times N^\ell(\bar{k})) = \mathrm{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N_\ell(\bar{k}))$$

since $N^\ell(\bar{k})$ is killed by something prime ℓ which is an isomorphism on $\mathbb{Q}_\ell/\mathbb{Z}_\ell$. Now apply $\mathrm{Hom}(-, N_\ell(\bar{k}))$ to the exact sequence

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

gives a long exact sequence

$$\mathrm{Hom}(\mathbb{Q}_\ell, N_\ell(\bar{k})) \to \mathrm{Hom}(\mathbb{Z}_\ell, N_\ell(\bar{k})) \to \mathrm{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N_\ell(\bar{k})) \to \mathrm{Ext}^1(\mathbb{Q}_\ell, N_\ell(\bar{k})).$$

The first and last terms are zero since ℓ^m kills N_ℓ. Therefore

$$\mathrm{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N_\ell(\bar{k})) \cong \mathrm{Hom}(\mathbb{Z}_\ell, N_\ell(\bar{k})) \cong N_\ell(\bar{k}).$$

Since N is etale, we have $N_\ell(\bar{k}) = N_\ell(k^s)$. The result then follows. □

Now let us consider the case $\ell = p$.

Definition 31 We define $T_{p,\mathrm{et}}(A) := \varprojlim A[p^m](\bar{k})$ (equal to $\varprojlim A[p^m]_{\mathrm{et}}(k^s) = \varprojlim A[p^m]_{\mathrm{et}}(\bar{k})$. It is a free $\mathbb{Z}_p$-module of rank r, where r is the p-rank of A.

This p-adic Tate module is not as good as the ℓ-adic Tate module because it only sees the etale quotient part $A[p^m]_{\mathrm{et}}$ and loses other information.

Definition 32 Let S be a base scheme. A *p-divisible group* (or *Barsotti-Tate group*) $\mathbb{X}$ is an inductive system $\{\mathbb{X}_n, \iota_n\}_{n\geq 0}$, where $\mathbb{X}_0 = S$, $\mathbb{X}_n$ is commutative and finite flat over S and $\iota_n : \mathbb{X}_n \hookrightarrow \mathbb{X}_{n+1}$ is a closed embedding such that $p : \mathbb{X}_n \to \mathbb{X}_n$ factors as $p = \pi_n \circ \iota_{n-1}$, where $\pi_n : \mathbb{X}_n \to \mathbb{X}_{n-1}$ is faithfully flat.

Remark 25 For historical reason the p-divisible group is defined to be an inductive system as opposed to the projective system in the ℓ-adic Tate module. Nevertheless, we can also define it as a projective system using π_n.

Example 17 Let A be an abelian variety. Define $A[p^\infty] := \{A[p^n], \iota_n : A[p^n] \hookrightarrow A[p^{n+1}]\}_{n\geq 0}$. This p-divisible group is the right replacement of the p-adic Tate module $T_{p,\mathrm{et}}$. In particular, one can recover $T_{p,\mathrm{et}}$ from $A[p^\infty]$.

Definition 33 Since $p : \mathbb{X}_1 \to \mathbb{X}_1$ kills $\mathbb{X}_1$, we know that $\mathrm{rank}\, \mathcal{O}_{\mathbb{X}_1} = p^h$ for some h. We call the h the *height* of $\mathbb{X}$. By induction, one sees that $\mathrm{rank}\, \mathcal{O}_{\mathbb{X}_n} = p^{nh}$.

Example 18 Let A be an abelian variety of dimension g, then the height of $A[p^\infty]$ is $2g$.

The Poincare complete reducibility and the degree polynomial

Denote by $\mathbf{AV}_k$ the category of abelian varieties over k. This is a quite complicated category to study. We introduce a slightly simpler category.

Definition 34 We define $\mathbf{AV}_k^0$ to be the category of abelian varieties *up to isogeny*: the objects are abelian varieties over k and the morphisms between A and B are elements of $\mathrm{Hom}(A, B) \otimes \mathbb{Q}$.

Lemma 21 Let $f : A \to B$ be an isogeny. Then f is invertible in $\mathbf{AV}_k^0$.

Proof By Corollary 27, there exists isogenies g and h such that $g \circ f = n_A$ and $f \circ h = m_B$, both of which are invertible in $\mathrm{Hom}(A, B) \otimes \mathbb{Q}$. Hence f is invertible. □

Theorem 31 (Poincare complete reducibility) Let $A \subseteq B$ be an abelian subvariety. Then there exists $C \subseteq B$ such that the multiplication morphism $A \times C \to B$ is an isogeny. In other words, abelian varieties are completely reducible in $\mathbf{AV}_k^0$.

Proof Pick an ample line bundle $\mathcal{L}$ on B and write the closed immersion as $\iota : A \hookrightarrow B$. Proposition 8 gives $\phi_{\iota^*\mathcal{L}} = \hat{\iota} \circ \phi_{\mathcal{L}} \circ \iota$ and we know that $\phi_{\iota^*\mathcal{L}}$ has finite kernel since $\phi_{\mathcal{L}}$ does. Let $C = \ker(\hat{\iota} \circ \phi_{\mathcal{L}})_{\mathrm{red}}$. So $\ker(A \times C \to B) = A \cap C = \ker \phi_{\iota^*\mathcal{L}}$ is finite. Since $\hat{A} \to \hat{B}$ is surjective, counting dimensions we know that $A \times C \to B$ is an isogeny. □

Definition 35 An abelian variety A is called *simple* if it does not contain any abelian subvariety other than 0 and A.

Write $\mathrm{Hom}^0(A, B) = \mathrm{Hom}(A, B) \otimes \mathbb{Q}$ and $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes \mathbb{Q}$ for short. The previous lemma implies that if A simple, then $\mathrm{End}^0(A)$ is a division algebra over $\mathbb{Q}$.

Applying the completely reducibility successively we obtain the following corollaries.

Corollary 29 Every abelian variety A is isogenous to $\prod_i A_i^{n_i}$, where A_i's are pairwise non-isogenous simple abelian varieties. Moreover, this decomposition is unique up to permutation.

Remark 26 In fact more is true: $\mathbf{AV}_k^0$ is a semisimple abelian category. (Note that this is not true for $\mathbf{AV}_k$ since the kernel of an isogeny is not necessarily an abelian variety.)

Corollary 30 Let A be an abelian variety, then $\mathrm{End}^0(A)$ is a semisimple algebra over $\mathbb{Q}$, hence can be written as a product of matrix algebra of division algebras $\prod_i M_{n_i}(D_i)$.

Remark 27 We will see that these semisimple algebras are actually finite dimensional.

Definition 36 Let E be a field and V/E be a vector space (not necessarily finite dimensional). A function $f : V \to E$ is called *homogeneous polynomial of degree* n if the restriction of f to any finite dimensional subspace is a polynomial function of degree n, or equivalently, for any $v_1, v_2 \in V$, $f(\lambda_1 v_1 + \lambda_2 v_2)$ is a homogeneous polynomial of degree n in λ_1, λ_2.

Definition 37 Define $\deg : \mathrm{End}\, A \to \mathbb{Z}$ to be $\deg f$ if $f \in \mathrm{End}\, A$ is an isogeny and 0 otherwise.

Theorem 32 There is a unique way to extend $\deg$ to a (homogeneous) polynomial $\mathrm{End}^0(A) \to \mathbb{Q}$ of degree $2g$.

Remark 28 This puts strong restriction on $\mathrm{End}(A)$: $\mathrm{End}(A)$ must be *discrete* in the $\mathbb{Q}$-vector space $\mathrm{End}^0(A)$ (hence cannot be too divisible).

To prove this theorem, we need the following lemma.

Lemma 22 Pick an ample line bundle $\mathcal{L}$ on A such that $\chi(\mathcal{L}) \neq 0$ (this is always true though we did not prove it). Then $\deg f = \frac{\chi(f^*\mathcal{L})}{\chi(\mathcal{L})}$.

Proof (Proof of Theorem 32) The function $\deg : \mathrm{End}(A) \to \mathbb{Z}$ is of degree $2g$ in the sense that $\deg(nf) = n^{2g} \cdot \deg(f)$ by Theorem 18. There is a unique way to extend $\deg$ to $\mathrm{End}^0(A) \to \mathbb{Q}$ such that it is homogeneous function of degree $2g$: for any $\phi \in \mathrm{End}^0(A)$, there exists some m such that $m\phi \in \mathrm{End}(A)$; then $\deg(\phi) = \deg(m\phi)/m^{2g}$. We need to show that this extended function $\deg : \mathrm{End}^0(A) \to \mathbb{Q}$ is actually a polynomial.

It is enough to show that for any $f_1, f_2 \in \mathrm{End}(A)$, $\deg(nf_1 + f_2)$ is a polynomial of n. The previous lemma gives $\deg(nf_1 + f_2) = \frac{\chi((nf_1+f_2)^*\mathcal{L})}{\chi(\mathcal{L})}$. So it suffices to show that $\chi((nf_1 + f_2)^*\mathcal{L})$ is a polynomial of n. Applying Corollary 4 to the case $f = nf_1 + f_2$, $g = f_1$ and $h = f_1$, we know that

$$\mathcal{L}_{n+2} \cong \mathcal{L}_{n+1} + \mathcal{L}_{n+1} + (2f_1)^*\mathcal{L} - \mathcal{L}_n - f_1^*\mathcal{L} - f_1^*\mathcal{L},$$

where $\mathcal{L}_n = (nf_1 + f_2)^*\mathcal{L}$. So

$$\mathcal{L}_{n+2} - \mathcal{L}_{n+1} = \mathcal{L}_{n+1} - \mathcal{L}_n + ((2f_1)^*\mathcal{L} - 2f_1^*\mathcal{L}).$$

Therefore

$$\mathcal{L}_n - \mathcal{L}_{n-1} = \mathcal{L}_1 - \mathcal{L}_0 + (n-1)\mathcal{M},$$

where $\mathcal{M} = (2f_1)^*\mathcal{L} = 2f_1^*\mathcal{L}$ is independent of n. Summing up implies that $\mathcal{L}_n$ is of the form $\frac{n(n-1)}{2}\mathcal{M} + n\mathcal{N} + \mathcal{Q}$ for some $\mathcal{N}$ and $\mathcal{Q}$ independent of n. Hence $\chi(\mathcal{L}_n)$ is a polynomial of n. □

The Riemann-Roch Theorem for abelian varieties

In this section we will prove the following version of Riemann-Roch theorem for abelian varieties.

Theorem 33 (Riemann-Roch) Let $\mathcal{L}$ be a line bundle on A. Then $\chi(\mathcal{L}^n)$ is a homogeneous polynomial of deg g. In particular,

$$\chi(\mathcal{L}^n) = \frac{d_{\mathcal{L}} \cdot n^g}{g!}.$$

Assuming this theorem, we can prove Lemma 22 and thus finish the proof of Theorem 32.

Proof (Proof of Lemma 22) Suppose f is an isogeny. By Proposition 3, $\deg f = d_{f^*\mathcal{L}}/d_{\mathcal{L}}$. This is equal to $\chi(f^*\mathcal{L})/\chi(\mathcal{L})$ using the previous theorem. (Or apply directly the weaker Theorem 34 below).

Now suppose f is not an isogeny. We need to show that $\chi(f^*\mathcal{L}) = 0$. From the previous theorem. $d_{f^*\mathcal{L}} \cdot n^g/g! = \chi(f^*\mathcal{L}^n)$. By the projection formula, this is also equal to $\chi(Rf_*\mathcal{O}_A \otimes \mathcal{L}^n)$. Because f is not an isogeny, the image of f is a proper subvariety X of A. So $\chi(Rf_*\mathcal{O}_A \otimes \mathcal{L}^n)$ is actually a polynomial of degree $< n$, thus $d_{f^*\mathcal{L}} = 0$. □

Remark 29 Note that if $\mathcal{L} = \mathcal{O}(D)$ is very ample, then $d_{\mathcal{L}}$ is the degree of corresponding embedding $A \hookrightarrow \mathbb{P}^N$, which is the self-intersection number D^g. Hence when $\mathcal{L} = \mathcal{O}(D)$ is very ample, $\chi(\mathcal{L}) = D^g/g!$. In general, for an arbitrary $\mathcal{L}$, we can attach the first Chern class $c_1(\mathcal{L}) \in CH^1(A)$ in the first Chow group (when A is defined over $\mathbb{C}$, we can take $c_1(\mathcal{L}) \in H^2(A, \mathbb{Z})$). Then $c_1(\mathcal{L})^g \in CH^g(A)$ and there is a natural degree map $\deg : CH^g(A) \to \mathbb{Z}$ (when A is defined over $\mathbb{C}$, $\deg : H^{2g}(A, \mathbb{Z}) \xrightarrow{\cap[A]} \mathbb{Z}$). The general Riemann-Roch formula says that

$$\chi(\mathcal{L}) = \frac{\deg c_1(\mathcal{L})^g}{g!}.$$

This general formula follows (tautologically) from the very ample case.

Now let us turn to the proof of Theorem 33. Let G be a group scheme over k of finite type and X be a scheme over k of finite type equipped with the trivial G-action.

Definition 38 A G-*torsor* (or, *principal* G-*bundle*) P over X is a scheme P with a right G-action together with a G-equivariant morphism $\pi : P \to X$ such that the natural morphism $P \times_k G \to P \times_X P$ is an isomorphism (the action $P \times G \to P$ factors through $P \times_X P$ since G acts on X trivially).

Example 19 If $f : A \to B$ is an isogeny of abelian varieties. Then $f : A \to B$ is a $\ker f$-torsor over B.

Theorem 34 Suppose G is finite, $\pi : P \to X$ is a G-torsor (hence is finite and $\deg(\pi) = \dim k[G]$) and X is proper. Then for any coherent sheaf $\mathcal{F}$ on X, we have

$$\chi(\pi^*\mathcal{F}) = \deg(\pi) \cdot \chi(\mathcal{F}).$$

Proof Using additivity of the Euler characteristic in short exact sequences and noetherian induction, we can assume the theorem holds for $\dim X < n$ and X is integral. Let r be the generic rank of $\mathcal{F}$. Then there exists $U \subseteq X$ open such that $\mathcal{F}|_U \cong \mathcal{O}_U^r$. Extend $\mathcal{O}_U^r \subseteq \mathcal{F}|_U \oplus \mathcal{O}_U^r$ to a coherent sheaf $\mathcal{E} \subseteq \mathcal{F} \oplus \mathcal{O}_X^r$. The projections $\mathcal{E} \to \mathcal{F}$ and $\mathcal{E} \to \mathcal{O}_X^r$ are isomorphisms on U, hence their kernels and cokernels are supported on lower dimensions. The additivity of the Euler characteristic and induction hypothesis thus allow us reduce to showing the theorem for $\mathcal{O}_X^r$, or for any *one* coherent sheaf on X. Let us prove it for $\mathcal{F} = \pi_*\mathcal{O}_P$, namely to show

$$\chi(\pi^*\pi_*\mathcal{O}_P) = \deg(\pi)\chi(\pi_*\mathcal{O}_P).$$

By the flat base change

$$\begin{array}{ccc} P \times G & \longrightarrow & P \\ \downarrow & & \downarrow \pi \\ P & \xrightarrow{\pi} & X, \end{array}$$

we know that $\pi^*\pi_*\mathcal{O}_P = \mathcal{O}_P \otimes k[G]$. Since $\chi(\pi_*\mathcal{O}_P) = \chi(\mathcal{O}_P)$ (π is finite flat), the result follows. □

Lemma 23 Any line bundle $\mathcal{L}$ on an abelian variety A over $\bar{k}$ can be written as $\mathcal{L} = \mathcal{L}_1 \otimes \mathcal{L}_2$, where $\mathcal{L}_1$ is symmetric and $\mathcal{L}_2 \in \mathrm{Pic}^0(A)$.

Proof We want to find some $\mathcal{L}_2 \in \mathrm{Pic}^0(A)$ such that $\mathcal{L}_1 = \mathcal{L} \otimes \mathcal{L}_2^{-1}$ is symmetric, i.e., $\mathcal{L}_2 \otimes (-1)^*\mathcal{L}_2^{-1} = \mathcal{L} \otimes (-1)^*\mathcal{L}^{-1}$. If $\mathcal{L} \otimes (-1)^*\mathcal{L}^{-1} \in \mathrm{Pic}^0(A)$, then $\mathcal{L}_2 = (\mathcal{L} \otimes (-1)^*\mathcal{L}^{-1})^{1/2}$ works (

$\mathrm{Pic}^0(A)$ is divisible over $\bar{k}$). It remains to prove that $\mathcal{L} \otimes (-1)^* \mathcal{L}^{-1} \in \mathrm{Pic}^0(A)$, which is equivalent to showing that

$$T_x^* \mathcal{L} \otimes \mathcal{L}^{-1} \cong (-1)^* (T_{-x}^* \mathcal{L} \otimes \mathcal{L}^{-1}),$$

since $T_x \circ (-1) = (-1) \circ T_{-x}$. The right-hand-side is equal to $(T_{-x}^* \mathcal{L})^{-1} \otimes \mathcal{L}$ because $T_{-x}^* \mathcal{L} \otimes \mathcal{L}^{-1}$ is in $\mathrm{Pic}^0(A)$. Now it remains to show that

$$T_x^* \mathcal{L} \otimes \mathcal{L}^{-1} = (T_{-x}^* \mathcal{L})^{-1} \otimes \mathcal{L}.$$

This follows from Theorem of the Square. □

Finally,

Proof (Proof of Theorem 33) It is enough to show that $\chi(\mathcal{L}^{m^2 n}) = m^{2g} \chi(\mathcal{L}^n)$. This is true the previous theorem if $\mathcal{L}$ is symmetric (in this case $m_A^* \mathcal{L}^n = \mathcal{L}^{m^2 n}$). In general, Lemma 23 tells us we can write $\mathcal{L} = \mathcal{L}_1 \otimes \mathcal{L}_2$ here $\mathcal{L}_1$ is symmetric and $\mathcal{L}_2 \in \mathrm{Pic}^0(A)$. In particular, $\mathcal{L}_2$ is algebraically equivalent to $\mathcal{O}_A$. Using the invariance of Euler characteristic in algebraic families, we find that

$$\chi(\mathcal{L}^{m^2 n}) = \chi(\mathcal{L}_1^{m^2 n}) = m^{2g} \chi(\mathcal{L}_1) = m^{2g} \chi(\mathcal{L}).$$

This completes the proof. □

Endomorphisms of abelian varieties

Theorem 35 Let A, B be two abelian varieties over k. Then the natural map $\mathrm{Hom}(A, B) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}(T_\ell(A), T_\ell(B))$ is injective. In particular, $\mathrm{Hom}(A, B)$ is a free $\mathbb{Z}$-module of finite rank (as $\mathrm{Hom}(A, B)$ is torsion-free).

Proof Suppose we have isogenies $\prod A_i \to A$ and $B \to \prod B_j$ with A_i, B_j simple. Using the injectivity of $\mathrm{Hom}(A, B) \otimes \mathbb{Z}_\ell \hookrightarrow \prod_{i,j} \mathrm{Hom}(A_i, B_j) \otimes \mathbb{Z}_\ell$, we reduce to the case where A and B are simple. If A and B are not isogenous, then we are done. Otherwise, choosing an isogeny $B \to A$ gives a bijection between $\mathrm{Hom}(A, B)$ and $\mathrm{End}(A)$, thus we are reduced to the case $A = B$. To show this case, it is enough to show that for any $M \subseteq \mathrm{End}(A)$ finitely generated, there is an injection $M \otimes \mathbb{Z}_\ell \to \mathrm{End}(T_\ell(A))$. By Theorem 34, M can not be too divisible. More precisely, let $QM = \{f \in \mathrm{End}(A) : \exists n, nf \in M\}$, then QM is also finitely generated. In fact, $QM = M \otimes \mathbb{Q} \cap \mathrm{End}(A)$ inside $\mathrm{End}^0(A)$ and $M \otimes \mathbb{Q}$ is a finite dimensional $\mathbb{Q}$-vector space. Moreover, $\deg : M \otimes \mathbb{Q} \to \mathbb{Q}$ is a polynomial such that $\deg f \in \mathbb{Z} \setminus \{0\}$ for any $f \in \mathrm{End}(A) \setminus \{0\}$. Therefore QM is discrete inside $M \otimes \mathbb{R}$, hence QM is finitely generated.

Now we may assume that M is finitely generated and $M = QM$. We need to show that $M \otimes \mathbb{Z}_\ell \to \mathrm{End}(T_\ell A)$ is injective. Let $f_1, \ldots, f_r$ be a $\mathbb{Z}$-basis of M. Suppose $\sum_i a_i T_\ell(f_i) = 0$ for $a_i \in \mathbb{Z}_\ell$. If not all $a_i = 0$, we can assume there exists some $a_i \in \mathbb{Z}_\ell^\times$. Choose $a_i' \in \mathbb{Z}$ such that $a_i' \mod \ell = a_i \mod \ell$. Then $T_\ell(\sum a_i' f_i)(T_\ell(A)) \subseteq \ell T_\ell(A)$. Let $f = \sum a_i' f_i$, then $T_\ell(f)(T_\ell(A)) \subseteq \ell T_\ell(A)$, hence $A[\ell] \subseteq \ker f$ by the definition of the Tate module. Thus we can write $f = f' \circ \ell$ by Theorem 30, where $f' : A \to A$ lies in $QM = M$. This implies $\ell \mid a_i'$, a contradiction. □

Corollary 31 The Neron-Severi group $NS(A)$ is a finitely generated free abelian group (of rank $\leq 4g^2$).

Proof By definition, there is an injection $NS(A) = \mathrm{Pic}(A)/\mathrm{Pic}^0(A) \hookrightarrow \mathrm{Hom}(A, \hat{A})$ given by $\mathcal{L} \mapsto \phi_{\mathcal{L}}$. The latter one has finite rank by the previous theorem. □

Corollary 32 $\mathrm{End}^0(A)$ is a finite dimensional semisimple $\mathbb{Q}$-algebra.

Our next goal is to classify the possibilities of the endomorphism algebra $\mathrm{End}^0(A)$.

Definition 39 Let B be a finite dimensional simple $\mathbb{Q}$-algebra. A function $N : B \to \mathbb{Q}$ is called a *norm form* if v is a polynomial and $N(ab) = N(a)N(b)$. A function $T : B \to \mathbb{Q}$ is called a *trace form* if T is linear and $T(ab) = T(ba)$.

Proposition 14 Let B be a finite dimensional simple $\mathbb{Q}$-algebra and $K \subseteq B$ be the center of B (which must be a field). Then there exists a norm form and a trace form $N_{B/K}^0 : B \to K$, $\mathrm{Tr}_{B/K}^0 : B \to K$ (with $\mathrm{Tr}_{B/K}^0(1) = 1$) such that any norm form $N : B \to \mathbb{Q}$ is of the form $N = (N_{K/\mathbb{Q}} \circ N_{B/K}^0)^i$ for some $i \geq 0$ and any trace form $T : B \to \mathbb{Q}$ is of the form $T = \phi \circ \mathrm{Tr}_{B/k}^0$ for some linear map $\phi : K \to \mathbb{Q}$.

Definition 40 $N_{B/K}^0$ is called the *reduced norm* and $\mathrm{Tr}_{B/K}^0$ is called the *reduced trace*.

Proof (Sketch) When $K = \mathbb{Q}$, the norm $N \otimes \bar{K} = (\det)^i$ and descents to K. Similarly, the trace $T \otimes \bar{K} = \phi \circ \mathrm{Tr}$ (as it factors through the 1-dimensional quotient $M_d(\bar{K})/[M_d(\bar{K}), M_d(\bar{K})]$ and also descents to

K.

In general, $B \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} = B \otimes_K K \otimes_{\mathbb{Q}} \otimes \overline{\mathbb{Q}}$. We have $K \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \cong \prod_{K \hookrightarrow \overline{\mathbb{Q}}} \bar{K}$ and $B \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \cong \prod_{K \hookrightarrow \overline{\mathbb{Q}}} M_{d \times d}(\bar{K})$. Thus we find that $N \otimes \overline{\mathbb{Q}} = \prod_{i: K \hookrightarrow \overline{\mathbb{Q}}} (\det)^{n_i}$. Since N comes from K, we know that H_A's are all the same, hence N is of the desired form. The argument is similar for trace forms. □

Theorem 36

a. The degree function $\deg_{\mathbb{Q}_\ell} : \mathrm{End}^0(A) \otimes \mathbb{Q}_\ell$ agrees with $\det : \mathrm{End}(V_\ell(A)) \to \mathbb{Q}_\ell$, where $V_\ell(A) = T_\ell(A) \otimes \mathbb{Q}_\ell$. In other words, for $\phi \in \mathrm{End}^0(A) \otimes \mathbb{Q}_\ell$, $\deg(\phi) = \det(T_\ell(\phi))$.

b. Let $\phi \in \mathrm{End}(A)$ and $P(n) = \det(n - \phi)$ (equal to the characteristic polynomial of $T_\ell(\phi)$). Then $P(x) \in \mathbb{Z}[x]$.

Proof First observe that both $\deg_{\mathbb{Q}_\ell}$ and $\det$ are norm forms on $\mathrm{End}^0(A) \otimes \mathbb{Q}_\ell$. We claim that any $f \in \mathrm{End}(A)$, the ℓ-adic absolute values $|\deg f|_\ell = |\det(T_\ell(f))|_\ell$. This claim implies the first part of the theorem: write $\mathrm{End}^0(A) = \prod_i M_{n_i}(D_i)$, then $\deg = \prod (N_{C(D_i)/\mathbb{Q}_\ell} N^0_{D_i/C(D_i)})^{w_i}$ and $\det = \prod (N_{C(D_i)/\mathbb{Q}_\ell} N^0_{D_i/C(D_i)})^{w_i}$ by the previous proposition; also $\mathrm{End}^0(A)$ is dense in $\mathrm{End}^0(A) \otimes \mathbb{Q}_\ell$.

Now let us show the claim. Since $\mathrm{End}^0(A)$ is dense in $\mathrm{End}^0(A) \otimes \mathbb{Z}_\ell$ and both sides are homogeneous polynomial of degree $2g$, we may only check on $\phi \in \mathrm{End}(A)$. If ϕ is not an isogeny, then $T_\ell(\phi) \otimes \mathbb{Q}$ is not an isomorphism (the image has lower dimension), hence both sides are equal to 0. If ϕ is an isogeny. By the exact sequence in Proposition 13, $T_\ell(\phi)$ is injective and has cokernel $(\ker \phi)_\ell(k^s)$. Therefore $|\deg \phi|_\ell = \ell^{-\#(\ker \phi)_\ell(k^s)}$, which is equal to $|\det \phi|_\ell$.

To see the polynomial $P(x)$ in the second part of the theorem has integer coefficients, we observe that $P(n)$ by definition is an integer for any n, hence $P(x) \in \mathbb{Q}[x]$. Since $\mathrm{End}(A)$ is finite over $\mathbb{Z}$, then there exists $q(x) \in \mathbb{Z}[x]$ such that $q(\phi) = 0$. So all the roots of $q(x)$, hence all roots of $P(x)$ are algebraic integers. But $P(x) \in \mathbb{Q}[x]$, we know that $P(x) \in \mathbb{Z}[x]$. □

Definition 41 Write $P(x) = x^{2g} + a_1 x^{2g-1} + \cdots a_{2g}$ the characteristic polynomial of ϕ. We call $a_{2g} = N\phi = \deg \phi$ the *norm* of ϕ and $a_1 = \mathrm{Tr}\, \phi$ the *trace* of ϕ.

Remark 30 If we decompose $\mathrm{End}^0(A) \cong B_1 \times \cdots \times B_r$ and $\deg(\phi) = \prod_i N^0_{B_i/\mathbb{Q}}(\phi_i)^{m_i}$. Then $\mathrm{Tr}(\phi) = \sum m_i \mathrm{Tr}^0_{B_i/\mathbb{Q}}(\phi_i)$. In fact, $\mathrm{Tr}^0_{B_i/\mathbb{Q}}$ is the second leading coefficient of

$$N^0_{B_i/\mathbb{Q}}(n - \phi) = n^k - \mathrm{Tr}^0_{B_i/\mathbb{Q}} \cdot n^{k-1} + \cdots.$$

Now let us further analyze the struction of $\mathrm{End}^0(A)$. Suppose A is simple and K is the center of the division algebra of $B = \mathrm{End}^0(A)$. Then $[B : K] = d^2$ and $[K : \mathbb{Q}] = e$ for some integers d, e. Thus $N^0_{B/\mathbb{Q}}$ is a polynomial of degree de. Because, $\deg$ is a polynomial of degree $2g$, we obtain the following result.

Proposition 15 If A is simple, then $de \mid 2g$.

This result can be refined as follows.

Proposition 16 If $\mathrm{char}(k) = 0$ and A is simple, then $\dim_{\mathbb{Q}} \mathrm{End}^0(A) = d^2 e \mid 2g$.

Proof By Lefschetz principle, we may assume $k = \mathbb{C}$. Write $A = V/L$ as a $\mathbb{C}$-vector space quotient by a lattice t, then $\mathrm{End}^0(A)$ acts on the $\mathbb{Q}$-vector space $L_{\mathbb{Q}}$ (linear algebra over division algebras still makes sense). So $\dim_{\mathrm{End}^0(A)} L_{\mathbb{Q}} = \frac{2g}{d^2 e} \in \mathbb{Z}$. □

Remark 31 This refinement fails when $\mathrm{char}(k) = p > 0$ (e.g. for supersingular elliptic curves).

Definition 42 An abelian variety A is called of *CM-type* if there exists a commutative subalgebra $B \hookrightarrow \mathrm{End}^0(A)$ of degree $2g$.

Remark 32 When A simple, $\mathrm{End}^0(A)$ is a division algebra and its commutative subalgebras are actually subfields. Since the maximal subfield of a division algebra has degree de, by Proposition 15, de actually equals to $2g$ if A is simple and of CM-type.

Proposition 17 If A is of CM-type by a field F, then A is isogenous to $A_i^{n_i}$ for some A_i simple and of CM-type. If $\mathrm{char}(k) = 0$ and A is simple and of CM-type, then $\mathrm{End}^0(A) = K$ is a commutative field of degree $2g$ over $\mathbb{Q}$.

Proof Since F embeds into $\mathrm{End}^0(A) = \prod_i M_{n_i}(D_i)$, it must embed into some $M_{n_i}(D_i)$. Since the maximal subfield of $M_{n_i}(D_i)$ has degree $n_i d_i e_i$ over $\mathbb{Q}$, we know that $2g \leq n_i d_i e_i$ since A is of CM-type. On the other hand, $n_i d_i e_i \leq \sum_i n_i d_i e_i \leq \sum_i n_i 2g_i = 2g$ by the previous corollary. Therefore all equality must hold: there is only one simple factor A_i and $n_i d_i e_i = n_i g_i = 2g$. The rest follows from the previous proposition and the previous remark: $d^2 e \mid 2g$ implies $d = 1$. □

Weil pairings

To further classify the endomorphism algebras, we need the knowledge of the Weil pairing.

Recall that $(T_\ell A)^\vee(1) \cong T_\ell \hat{A}$ from Proposition 12. The proof of Proposition 12 is indeed not quite complete: in order to take the limit, we need the compatibility of the identifications $\hat{A}[\ell^n] = \mathrm{Hom}(A[\ell^n], \mu_{\ell^n})$ when n varies. More precisely, we need the following commutative diagram

$$\begin{array}{ccc} A[\ell^n] \times \hat{A}[\ell^n] & \longrightarrow & \mu_{\ell^n} \\ {\scriptstyle \ell\times\ell}\uparrow & & \uparrow{\scriptstyle \ell} \\ A[\ell^{n+1}] \times \hat{A}[\ell^{n+1}] & \longrightarrow & \mu_{\ell^{n+1}}. \end{array}$$

In other words, we need to understand the *Weil pairing* $e_n : A[n] \times \hat{A}[n] \to \mu_n$. By definition, this pairing is induced by the duality $\widehat{\ker n_A} \cong \ker \hat{n}_A$.

Let $f : A \to A$ be an isogeny. The duality $\widehat{\ker f} \cong \ker \hat{f}$ is given as follows at the level of $\bar{k}$-points. Suppose $x \in \ker f(\bar{k})$ and $\mathcal{L} \in \ker \hat{f}(\bar{k})$. By definition of $\ker \hat{f}$, we can pick an isomorphism $\beta : f^*\mathcal{L} \cong \mathcal{O}_A$, then $T_x^*\beta : T_x^* f^* \mathcal{L} \to T_x^* \mathcal{O}_A \cong \mathcal{O}_A$. Since $T_x^* f^* \mathcal{L} = f^* T_{f(x)}^* \mathcal{L} = f^*\mathcal{L}$ (notice $f(x) = 0$ as $x \in \ker f$), we know that $T_x^*\beta$ is another isomorphism $f^*\mathcal{L} \cong \mathcal{O}_A$. Hence $T_x^*\beta \circ \beta^{-1}$ is actually a number and the pairing $e_f(x, \mathcal{L})$ takes this value.

Proposition 18 Let $\mathcal{L} \in \hat{A}[m](\bar{k})$ and $x \in A[nm](\bar{k})$. Then

$$e_{nm}(x, \mathcal{L}) = e_m(nx, \mathcal{L}).$$

Proof Choose an isomorphism $\beta : m^*\mathcal{L} \cong \mathcal{O}_A$, then $e_{nm}(x, \mathcal{L}) = T_x^*(n^*\beta) \circ (n^*\beta)^{-1}$, which is equal to $n^*(T_{nx}^*\beta \circ \beta^{-1}) = n^*(e_m(nx, \mathcal{L})) = e_m(nx, \mathcal{L})$. □

Remark 33 This proposition implies that $e_{\ell^n}(\ell x, \ell\mathcal{L}) = e_{\ell^n}(\ell x, \mathcal{L})^\ell = e_{\ell^{n+1}}(x, \mathcal{L})^\ell$. Hence prove the desired commutativity of the previous diagram.

Remark 34 By the same argument, in general, for $f : A \to B$ an isogeny, we have

$$e_{\ell^\infty}(T_\ell(f)(x), y) = e_{\ell^\infty}(x, T_\ell \hat{f}(y))$$

for any $x \in T_\ell(A)$ and $y \in T_\ell(\hat{B})$.

Let us slightly rewrite the Weil pairing in a more explicit form. Let $\mathcal{L} = \mathcal{O}(D)$ for some Cartier divisor D. D gives an embedding $i : \mathcal{L} \to \mathcal{K}_A$, where $\mathcal{O}_A$ is the sheaf of rational functions on A. Composing $\beta : n^*\mathcal{L} \cong \mathcal{O}_A$ with $i : \mathcal{L} \hookrightarrow \mathcal{K}_A$, we obtain a rational function $g = n^* i \circ \beta^{-1}(1) \in n^*\mathcal{K}_A = \mathcal{K}_A$. In other words, the divisor $(g^{-1}) = n^{-1}D$. Therefore we have (a bit more explicitly)

$$e_n(x, \mathcal{L}) = \frac{T_x^* g}{g} = \frac{g(z + x)}{g(z)}$$

for any $z \in A$.

Theorem 37 Suppose $\mathcal{L}$ is a line bundle on A. The bilinear pairing

$$E^{\mathcal{L}} : T_\ell(A) \times T_\ell(A) \xrightarrow{1\times\phi_{\mathcal{L}}} T_\ell(A) \times T_\ell(\hat{A}) \xrightarrow{e_{\ell^\infty}} \mathbb{Z}_\ell(1)$$

is skew-symmetric.

Remark 35 The dual abelian variety is not seen in the Weil pairing of elliptic curves: the reason is that for elliptic curves we have a canonical choice of a principal polarization given by the line bundle $\mathcal{L} = \mathcal{O}(\{0\})$.

Proof We need to prove that $E^{\mathcal{L}}(x, \phi_{\mathcal{L}}(x)) = 1$. Suppose $x \in A[n]$ and $\mathcal{L} = \mathcal{O}(D)$. Then $\phi_{\mathcal{L}}(x) = T_x^*\mathcal{L} \otimes \mathcal{L}^{-1} = \mathcal{O}(T_x D - D)$. Let g be a rational function such that $(g^{-1}) = n^{-1}(T_x D - D)$. As explained above, we want to show that $T_x^* g = g$. Write $x = ny$ and $E = n^{-1}D$. Then

$$(g^{-1}) = T_{-y}(n^{-1}D) - n^{-1}D = T_{-y}E - E.$$

Therefore

$$(T_{jy}^* g^{-1}) = T_{-(j+1)y}E - T_{-jy}E,$$

and

$$\left(\prod_{j=0}^{n-1} T_{jy}^* g^{-1}\right) = T_{-x}E - E = 0.$$

So $h(z) = \prod_{j=0}^{n-1} g^{-1}(z + jy)$ is a constant. In particular $h(z+y) = h(z)$ implies that $g(x+z) = g(z)$ for any $z \in A$. □

Corollary 33 Let λ be a polarization. Then the pairing $E^\lambda(x,y) = e_{\ell^\infty}(x, T_\ell(\lambda)(y))$ is symplectic (skew-symmetric and nondegenerate).

Proof Note that e_{ℓ^∞} is nondegenerate, the corollary follows since λ is an isogeny (hence has finite kernel). □

More generally, an isogeny $\phi : A \to \hat{A}$ defines a pairing $E^\phi(x,y)$ in a similar fashion. So here is a natural question: does every *symplectic* pairing defined by an isogeny ϕ come from a polarization? It turns out (Theorem 38) this is true over algebraically closed fields (and in general, the twice of it comes from a polarization). Our next goal is to show this fact.

Lemma 24 Let $f : A \to B$ be an isogeny and $\mathcal{L}$ be a line bundle on B. Then

$$E^{f^*\mathcal{L}}(x,y) = E^{\mathcal{L}}(T_\ell(f)(x), T_\ell(f)(y)).$$

Proof It follows from definition and the fact that $\phi_{f^*\mathcal{L}} = \hat{f} \circ \phi_{\mathcal{L}} \circ f$ (Proposition 8). □

Lemma 25 Sending $\mathcal{L}$ to $(\mathcal{L}|_{A\times 0}, \mathcal{L}_{0\times B})$ gives an isomorphism $\widehat{A \times B} \cong \hat{A} \times \hat{B}$. In other words, Pic^0 is a linear functor.

Proof Any line bundle in $\mathrm{Pic}^0(A)$ is translation-invariant. The injectivity then follows from the Theorem of Square 7. So it is an isomorphism since both sides are abelian varieties of the same dimension. □

Proposition 19 Let $\mathcal{P}$ be the Poincare line bundle on $A \times \hat{A}$. Then

$$E^{\mathcal{P}}((x,\hat{x}),(y,\hat{y})) = e_{\ell^\infty}(x,\hat{y}) - e_{\ell^\infty}(y,\hat{x}).$$

(Notice that $T_\ell(A \times \hat{A}) \cong T_\ell(A) \times T_\ell(\hat{A})$.)

Proof By the skew-symmetry, it is enough to show that $E^{\mathcal{P}}((x,0),(y,0)) = E^{\mathcal{P}}((0,\hat{x}),(0,\hat{y})) = 1$ and $E^{\mathcal{P}}((x,0),(0,\hat{y})) = e_{\ell^\infty}(x,\hat{y})$. Denote $i : A \xrightarrow{\mathrm{Id}\times 0} A \times A$, then by Lemma 24 we know that

$$E^{\mathcal{P}}((x,0),(y,0)) = E^{\mathcal{P}}(T_\ell(i)(x), T_\ell(i)(y)) = E^{i^*\mathcal{P}}(x,y) = E^{\mathcal{O}_A}(x,y) = 1,$$

which shows the first part.

By Lemma 25, $\widehat{A \times \hat{A}} \cong \hat{A} \times A$ using duality induced by the Poincare line bundle $\mathcal{P}$ (Corollary 19). Under this identification, we see hat $\phi_{\mathcal{P}} : A \times \hat{A} \to \widehat{A \times \hat{A}}$ is given by $\phi_{\mathcal{P}}((x,\hat{x})) = (\hat{x}, x)$. It follows that

$$E^{\mathcal{P}}((x,0),(0,\hat{y})) = e_{\ell^\infty}((x,0),(\hat{y},0)) = e_{\ell^\infty}(x,\hat{y}),$$

which shows the second part. □

As a consequence, we can prove the following theorem characterizing skew-symmetric pairings: they are "almost" induced from a polarization.

Theorem 38 Let $\phi : A \to \hat{A}$ be a homomorphism. Then the following are equivalent:

a. ϕ is symmetric (i.e., $\phi = \hat{\phi}$).
b. E^ϕ is skew-symmetric.
c. $2\phi = \phi_{\mathcal{L}}$ for some line bundle $\mathcal{L}$.
d. Over $\bar{k}$, $\phi = \phi_{\mathcal{L}'}$ for some $\mathcal{L}'$.

Proof (d) implies (a), (b): we have shown them in Proposition 7 and Theorem 37.

(c) implies (d): this uses the theory of theta groups, see Mumford Section 23, Theorem 3, p. 231.

(b) implies (c): Let $\mathcal{L} = (1 \times \phi)^* \mathcal{P}$. Then Lemma 24 implies that

$$E^{\mathcal{L}}(x,y) = E^{\mathcal{P}}(T_\ell(1\times\phi)(x), T_\ell(1\times\phi)(y)) = E^{\mathcal{P}}((x, T_\ell(\phi)(x)), (y, T_\ell(\phi)(y))).$$

Using the previous proposition, this is equal to $E^\phi(x,y) - E^\phi(y,x)$, hence is equal to $2E^\phi(x,y)$ by the skew-symmetry. It follows that $\phi_{\mathcal{L}} = 2\phi$.

(a) implies (c): Notice that $\phi_{\mathcal{L}} = \phi_{(1\times\phi)^*\mathcal{P}} = \widehat{1\times\phi}\circ\phi_{\mathcal{P}}\circ(1\times\phi)$. Therefore

$$\phi_{\mathcal{L}}(x) = \widehat{1\times\phi}\circ\phi_{\mathcal{P}}(x,\phi(x)) = \widehat{1\times\phi}(\phi(x),x).$$

By the symmetry of ϕ, we know that $\widehat{1\times\phi}(\phi(x),x) = 2\phi(x)$. Therefore $\phi_{\mathcal{L}}(x) = 2\phi(x)$. □

Corollary 34 The Neron-Severi group $NS(A_{\bar{k}}) \hookrightarrow \mathrm{Hom}(A_{\bar{k}}, \hat{A}_{\bar{k}})$ can be identified with the symmetric homomorphisms from $A_{\bar{k}}$ to $\hat{A}_{\bar{k}}$.

Remark 36 Over k, both side should be replaced by certain *etale group schemes*.

Proof Use the equivalence of (a) and (d) in the previous theorem. □

Rosati involutions

Now we shall move back to study the endomorphisms of abelian varieties. Pick a polarization $\lambda: A\to\hat{A}$. We define $': \mathrm{End}^0(A)\to\mathrm{End}^0(A), \phi\mapsto\phi'$, where $\phi' = \lambda^{-1}\circ\hat{\phi}\circ\lambda$. The following can be checked directly.

Lemma 26 $(\phi+\psi)' = \phi'+\psi'$, $(\phi\psi)' = \psi'\phi'$ and $\phi'' = \phi$.

Therefore, $': \mathrm{End}^0(A)\to\mathrm{End}^0(A)$ is an anti-involution of $\mathrm{End}^0(A)$. Since the polarization is not necessarily principal, this anti-involution does not necessarily preserve the integral structure $\mathrm{End}(A)$. Moreover, if λ_1, λ_2 are two polarizations, then $\lambda_1 = \lambda_2\circ a$, where $a\in\mathrm{End}^0(A)$. Hence the two Rosati involutions induced by λ_i's are related by a inner automorphism $\phi'^{\lambda_1} = a\circ\phi'^{\lambda_2}a^{-1}$. So only the conjugacy class of the Rosati involution is canonically defined. The following is almost a tautology.

Lemma 27 $E^\lambda(T_\ell(\phi)(x),y) = E^\lambda(x, T_\ell(\phi')(y))$. In other words, $T_\ell: (\mathrm{End}^0(A),') \to (\mathrm{End}(V_\ell(A)), *)$ gives a homomorphism of algebras with anti-involutions, where $*$ is the canonical anti-involution on $\mathrm{End}(V_\ell(A))$ induced by the skew-symmetric pairing E^λ.

Now strong restriction can be put on the structure of $\mathrm{End}^0(A)$.

Theorem 39 The Rosati involution is *positive*: for any nonzero $\phi\in\mathrm{End}^0(A)$, $\mathrm{Tr}(\phi\phi')>0$.

Remark 37 In complex geometry, a polarization on a complex manifold is simply a choice of an ample line bundle, i.e., a line bundle with a metric of positive curvature. This does not generalize to arbitrary fields. But for abelian varieties, the positivity of the Rosati involution somehow reflects the fact that polarizations are coming form *ample* line bundles.

Proof We may assume that $\lambda = \phi_{\mathcal{L}}$ for $\mathcal{L} = \mathcal{O}(H)$ very ample and $\phi\in\mathrm{End}(A)$. We claim that

$$\mathrm{Tr}(\phi\phi') = \frac{2g}{H^g}(H^{g-1}\cdot\phi^{-1}(H)).$$

The theorem easily follows from this claim since H is ample and $\phi^{-1}(p)$ is effective.

To prove the claim, consider the homomorphism $\phi_{\phi^*\mathcal{L}\otimes\mathcal{L}^n}: A\to\hat{A}$. Its degree is equal to

$\deg(n\phi_{\mathcal{L}} - \phi_{\phi^*\mathcal{L}}) = \deg(\phi_{\mathcal{L}}\cdot n - \hat{\phi}\phi_{\mathcal{L}}\phi)$, by the definition of the Rosati involution, this is equal to

$$\deg(\phi_{\mathcal{L}}\cdot n - \phi_{\mathcal{L}}\phi'\phi) = \deg(\phi_{\mathcal{L}})\cdot\deg(n-\phi'\phi) = \deg(\phi_{\mathcal{L}})\cdot P(n).$$

So we need to understand the ratio of the degrees of $\phi_{\phi^*\mathcal{L}\otimes\mathcal{L}^n}$ and $\phi_{\mathcal{L}}$ in order to extract $\mathrm{Tr}(\phi\phi')$, the second leading coefficient of $P(n)$. From Theorem 40 below, we can compute the degrees and obtain

$$P(n) = \frac{\chi(\phi^*\mathcal{L}^{-1}\otimes\mathcal{L}^n)^2}{\chi(\mathcal{L})^2}.$$

By the Riemann-Roch Theorem 33, we know that

$$P(n) = \left(\frac{(nH-\phi^{-1}(H))^g}{H^g}\right)^2 = \frac{1}{(H^g)^2}\left(n^g\cdot H^g - g(H^{g-1}\cdot\phi^{-1}(H))n^{g-1}+\cdots\right)$$

therefore

$$\mathrm{Tr}(\phi\phi') = \frac{2g}{H^g}(H^{g-1}\cdot\phi^{-1}(H)),$$

which finishes the proof. □

Now it remains to prove the following theorem.

Theorem 40 For any $\mathcal{L}$ nondegenerate (i.e., $K(\mathcal{L})$ is finite), $\deg(\phi_{\mathcal{L}}) = \chi(\mathcal{L})^2$.

Remark 38 By Theorem 16, a nondegenerate line bundle asscociated to an effective divisor is automatically ample.

We will not give a complete proof of this theorem. Instead, we will prove that $\deg \phi_{\mathcal{L}} = c \cdot \chi(\mathcal{L})^2$ where c is a constant. This is enough to be applied in the proof of the previous theorem because we only care about the ratio of two Euler characteristics.

Proof Let $\mathcal{M} = (1 \times \phi_{\mathcal{L}})^* \mathcal{P} = m^* \mathcal{L} \otimes p_1^* \mathcal{L}^{-1} \otimes p_2^* \mathcal{L}^{-1}$ (called the *Mumford line bundle* of $\mathcal{L}$) on $A \times A$. The idea is to calculate the Euler characteristic of $\mathcal{M}$ in two ways. On the one hand, by Theorem 34

$$\chi(\mathcal{M}) = \deg \phi_{\mathcal{L}} \cdot \chi(\mathcal{P}).$$

On the other hand, for all $y \notin K(\mathcal{L})$, $\mathcal{M}|_{y \times A}$ is a nontrivial line bundle lies in $\mathrm{Pic}^0(A)$, hence by Lemma 13, all the cohomology vanishes. Hence $\mathcal{M}$ can only have nonvanishing cohomology on $K(\mathcal{L})$, i.e., $R^i p_{1*}(\mathcal{M})$ is supported on the zero dimensional set $K(\mathcal{L})$. The Leray spectral degenerates and we conclude that

$$H^i(A \times A, \mathcal{M}) = \Gamma(A, R^i p_{1*}(\mathcal{M})).$$

By the projection formula, we know that $R^i p_{1*}(\mathcal{M}) = R^i p_{1*}(m^* \mathcal{L} \otimes p_2^* \mathcal{L}^{-1}) \otimes \mathcal{L}^{-1}$, thus

$$H^i(A \times A, \mathcal{M}) = \Gamma(A, R^i p_{1*}(m^* \mathcal{L} \otimes p_2^* \mathcal{L}^{-1})) = H^i(A \times A, m^* \mathcal{L} \otimes p_2^* \mathcal{L}^{-1}).$$

Hence

$$\chi(\mathcal{M}) = \chi(m^* \mathcal{L} \otimes p_2^* \mathcal{L}^{-1}).$$

But $A \times A \xrightarrow{m \times p_2} A \times A$ is an isomorphism, using Kunneth's formula we know that

$$\chi(m^* \mathcal{L} \otimes p_2^* \mathcal{L}^{-1}) = \chi(p_1^* \mathcal{L} \otimes p_2^* \mathcal{L}^{-1}) = \chi(\mathcal{L}) \cdot \chi(\mathcal{L}^{-1}) = \chi(\mathcal{L}) \cdot (-1)^g \chi(\mathcal{L}).$$

Therefore

$$\chi(\mathcal{L})^2 = (-1)^g \chi(\mathcal{P}) \cdot \deg \phi_{\mathcal{L}},$$

as desired. □

Remark 39 In fact, $\chi(\mathcal{P}) = (-1)^g$, though we omit the proof here.

Classification of endomorphism algebras of abelian varieties

As a consequence of the positivity of the Rosati involution (which is deep), we know that if A is a simple abelian variety, then $D = \mathrm{End}^0(A)$ is a finite dimensional division algebra with an anti-involution $' : D \to D$ such that $\mathrm{Tr}^0_{D/\mathbb{Q}}$ is positive. The classification of such algebras is done by Albert and those algebras are called *Albert division algebras* for the obvious reason.

Lemma 28 Let D be an Albert division algebra and K be the center of D (equivalently, let K be an Albert field). Let $K_0 = \{a \in K : a' = a\}$ (it is either the whole K or an index 2 subfield). Then K_0 is totally real and either $K = K_0$ or K is a totally imaginary quadratic extension of K_0.

The proof is easy and purely algebraic.

Proof Let $\{\sigma_i : K_0 \hookrightarrow \mathbb{R}, i = 1, \dots, r_1\}$ and $\{\sigma_{r_1+j} : K_0 \hookrightarrow \mathbb{C}, j = 1, \dots r_2\}$ be the real and (non-conjugate) complex embeddings of K_0 (thus $[K_0 : \mathbb{Q}] = r_1 + 2r_2$). Then we have an isomorphism

$$K_0 \otimes \mathbb{R} \cong \underbrace{\mathbb{R} \times \cdots \mathbb{R}}_{r_1} \times \underbrace{\mathbb{C} \times \cdots \times \mathbb{C}}_{r_2}, \quad (a \otimes 1) \mapsto (\sigma_1(a), \dots, \sigma_{r_1+r_2}(a)).$$

Moreover, the trace is simply the sum of the factors. For $x \in K_0$, $q(x) = \mathrm{Tr}(xx') = \mathrm{Tr}_{K_0/\mathbb{Q}}(x^2) > 0$, we know that $q_{\mathbb{R}}$ is a positive semidefinite quadratic form on $K_0 \otimes \mathbb{R}$ by continuity. But $q(x)$ is nondegenerate, so $q_{\mathbb{R}}$ must be positive definite. It follows that there can not be any complex embeddings, i.e., K_0 is totally real.

If $K = K_0$, there is nothing to prove. Otherwise, $[K : K_0] = 2$ and $K = K_0(\sqrt{\alpha})$ is a quadratic extension. We want to show that each $\sigma_i(\alpha) < 0$. Notice that $K \otimes_{K_0} \mathbb{R}$ is a product of $\mathbb{C}$ (when $\sigma_i(\alpha) < 0$) or $\mathbb{R} \times \mathbb{R}$ (when $\sigma_i(\alpha) > 0$) and the involution acts as the complex conjugation or the flip respectively. By the positivity of the involution, we know that there are no $\mathbb{R} \times \mathbb{R}$ factors, hence $\sigma_i(\alpha) < 0$ for every embedding. □

Now we give the full classification of Albert algebras.

Theorem 41 (Albert) An Albert algebra D is one of the following types:

- Type I: $D = K = K_0$ is totally real.
- Type II: $K = K_0$ is totally real, D is a quaternion algebra over K such $D \otimes_{\mathbb{Q}} \mathbb{R} \cong \prod_{K \hookrightarrow \mathbb{R}} M_2(\mathbb{R})$ with the anti-involution corresponding to transpose of matrices.

- Type III: $K = K_0$ is totally real, D is a quaternion algebra over K with the standard anti-involution $x' = \mathrm{Tr}^0_{D/K} x - x$ such that $D \otimes_{\mathbb{Q}} \mathbb{R} \cong \prod_{K \hookrightarrow \mathbb{R}} \mathbb{H}$, where $\mathbb{H}$ is the Hamilton quaternion algebra over $\mathbb{R}$.
- Type IV: $[K : K_0] = 2$ (K is a CM-field), D is a division algebra over K of dimension d^2. For every finite place v of K, $\mathrm{inv}_v D + \mathrm{inv}_{\sigma(v)} D = 0$, where $\mathrm{inv}_v(D) := [D \otimes_K K_v] \in \mathrm{Br}(K_v) \cong \mathbb{Q}/\mathbb{Z}$ is the local invariant of D and $\sigma : K \to K$ is the automorphism induced by the anti-involution on D. Moreover, if $\sigma(v) = v$, then $\mathrm{inv}_v(D) = 0$. In this case, we have $D \otimes_{\mathbb{Q}} \mathbb{R} \cong \prod_{K \hookrightarrow \mathbb{C}/\sim} M_d(\mathbb{C})$ with the anti-involution corresponding to conjugate transpose.

Remark 40 When $K = K_0$, the anti-involution induces an isomorphism $D \cong D^{\mathrm{op}}$ as central simple algebras over K. But $D \otimes_K D^{\mathrm{op}}$ is always isomorphic to a matrix algebra $M_{d^2}(K)$. Therefore $[D]$ has order either 1 or 2 in $\mathrm{Br}(K)$. Every involution on a quaternion algebra differs from the standard one by an inner automorphism (by the Skolem-Noether theorem). One can then show there are only Type I — Type III. The argument for Type IV is similar. We omit the details of this beautiful proof here.

Suppose $D = \mathrm{End}^0(A)$ for some simple abelian variety A over k. Let us list the numerical invariants of these four types. Write $[K_0 : \mathbb{Q}] = e_0$, $[K : \mathbb{Q}] = e$ and $[D : K] = d^2$. Let $S = \{x \in D : x = x'\}$ and $\eta = \frac{\dim_{\mathbb{Q}} S}{\dim_{\mathbb{Q}} D}$.

Type	e	d	η	$\mathrm{char}(k) = 0$	$\mathrm{char}(k) > 0$
I	e_0	1	1	$\boxed{e \mid g}$	$\boxed{e \mid g}$
II	e_0	2	3/4	$2e \mid g$	$\boxed{2e \mid g}$
III	e_0	2	1/4	$2e \mid g$	$e \mid g$
IV	$2e_0$	d	1/2	$e_0 d^2 \mid g$	$e_0 d \mid g$

Most of the entries are easy to derive using Proposition 15 and 16. The remaining boxed ones follows from the following

Proposition 20 Suppose $D = \mathrm{End}^0(A)$ for some simple abelian variety A over k. If $L \subseteq S$ is a subfield, then $[L : \mathbb{Q}] \mid g$.

Proof We have $NS(A) \otimes \mathbb{Q} \cong \mathrm{Hom}^{0,\mathrm{Sym}}(A, \hat{A})$ by Corollary 34. Picking $\lambda = \phi_{\mathcal{L}}$ b e a polarization gives an isomorphism between $\mathrm{Hom}^0(A, \hat{A})$ and $\mathrm{End}^0(A)$. The symmetric homomorphisms corresponds to the elements of S under the Rosati involution induced by λ. Therefore we have an isomorphism $r : NS(A) \otimes \mathbb{Q} \cong S$. Since the Euler characteristic extends to a homogeneous polynomial $\chi : NS(A) \otimes \mathbb{Q} \to \mathbb{Q}, \quad \mathcal{N} \mapsto \chi(\mathcal{N})$ of degree g, we know $f = \frac{1}{\chi(\mathcal{L})} r_* \chi : S \to \mathbb{Q}$ is also a polynomial function homogeneous of degree g. Explicitly, if $\phi = \lambda^{-1} \phi_{\mathcal{N}}$, then $f(\phi) = \frac{\chi(\mathcal{N})}{\chi(\mathcal{L})}$. By Theorem 40, $f^2(\phi) = \deg \phi_{\mathcal{N}} / \deg \lambda = \deg \phi$. Hence f^2 is a norm. But we already know f is a polynomial, therefore f is also a norm. In this way we obtain a norm of degree g on the field L, hence $[L : \mathbb{Q}]$ must divide g by Proposition 14. □

Remark 41 One might ask to what extent the above restrictions are complete. In characteristic zero, the answer is known due to Albert. On the other hand, not much seems to be known in positive characteristics.

Example 20 In the case of elliptic curves, we have $g = 1$. Applying the above classification result, we know that the endomorphism algebra of an elliptic curve is either $\mathbb{Q}$ (Type I), a quaternion algebra over $\mathbb{Q}$ ramified at ∞ (Type III, when $\mathrm{char}(k) > 0$), or an imaginary quadratic field (Type IV).

Abelian varieties over finite fields

Suppose the base field $k = \mathbb{F}_q$ is a finite field. Recall (Example 6) that we have a (relative) Frobenius morphism $X \to X^{(1)}$, which is a homomorphism when X is a group scheme. Write $q = p^m$, since $F^m = \mathrm{Id}$ and $X^{(m)} \cong X$, we obtain m-fold (relative) Frobenius $F^{(m)} : X \to X^{(m)} \cong X \in \mathrm{Hom}(X, X)$.

Definition 43 Let $X = A$ be an abelian variety. We write $\pi_A := F^{(m)}$ and P_A the characteristic polynomial of π_A. So P_A is a polynomial of degree $2g$ with the constant coefficient $\deg \pi_A = q^g$ by Theorem 36.

Theorem 42

a. $\mathbb{Q}[\pi_A] \subseteq \mathrm{End}^0(A)$ is semisimple.

b. (Riemann Hypothesis) Let ω be a the root of P_A. Then the absolute value of ω is $q^{1/2}$ under any embedding $\mathbb{Q}(\omega) \hookrightarrow \mathbb{C}$.

Remark 42 This case of abelian varieties is the main motivation for Weil to formulate the general Weil conjecture.

Proof Fix $\lambda : A \to \hat{A}$ a polarization. We claim that $\pi_A' \pi_A = q_A$. In fact, by definition the claim is equivalent to $\hat{\pi}_A \lambda \pi_A = q_A \cdot \lambda$. Since $\pi_A = F^{(m)}$ commutes with any morphism, this is equivalent to $\hat{\pi}_A \pi_{\hat{A}} \lambda = q_{\hat{A}} \cdot \lambda$. Thus it is enough to show that $\hat{\pi}_A \pi_{\hat{A}} = q_{\hat{A}}$. At the level of S-points, $\mathcal{L} \in \hat{A}(S)$ is a line bundle on $A \times S$. Its image under $\hat{\pi}_A \pi_{\hat{A}}$ corresponds to the composition

$$S \to \hat{A} \xrightarrow{\pi_{\hat{A}}} \hat{A} \xrightarrow{\hat{\pi}_A} \hat{A}.$$

Tracing through definition we find that the image of $\mathcal{L}$ under $\pi_{\hat{A}}$ is the line bundle $(1 \times F_S^{(m)})^* \mathcal{L}$, and the image of S under $\hat{\pi}_A \pi_{\hat{A}}$ is the line bundle $(\pi_A \times 1)^* (1 \times F_S^{(m)})^* \mathcal{L}$, which is the same as $\mathcal{L}^q$ on $A \times S$. The claim is proved.

Since π_A is an isogeny, we know that π_A is invertible and $\pi_A^{-1} \in \mathbb{Q}[\pi_A]$ (since the constant term of P_A is nonzero). Therefore $\mathbb{Q}[\pi_A]' = \mathbb{Q}[\pi_A]$ by the claim. Let $\mathfrak{a} \subseteq \mathbb{Q}[\pi_A]$ be an ideal, then $\mathfrak{a}' \subseteq \mathbb{Q}[\pi_A]$ is also an ideal. Let $\mathfrak{b} = (\mathfrak{a}')^\perp$ under the bilinear form $Q(x, y) = \mathrm{Tr}(xy')$. The positivity of $'$ implies that $\mathfrak{a} \cap \mathfrak{b} = 0$ by the positivity. A dimension count then shows that $\mathfrak{a} + \mathfrak{b} = \mathbb{Q}[\pi_A]$. Hence $\mathbb{Q}[\pi_A]$ is semisimple. In other words, $\mathbb{Q}[\pi_A]$ is finite etale over $\mathbb{Q}$ (without nilpotents). Since $\mathbb{Q}[\pi_A]$ is commutative, we can write $\mathbb{Q}[\pi_A] = \prod K_i$ as a product of fields. We can check that $'$ fixes K_i by the positivity. So K_i is either totally real or CM by Lemma 28 and for any embedding $j : K_i \hookrightarrow \mathbb{C}$, $j(x') = \overline{j(x)}$. Now if ω is a root of P_A, then $\mathbb{Q}(\omega)$ is some K_i. The second part follows because $|j(\omega)|^2 = j(\omega)\overline{j(\omega)} = j(\omega\omega') = q$. □

Definition 44 A *Weil q-number* is an algebraic integer π such that for every embedding $j : \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$, $|j(\pi)| = q^{1/e}$. Two Weil q-numbers π, π' are called *conjugate* if there exists an isomorphism $\mathbb{Q}(\pi) \cong \mathbb{Q}(\pi')$ sending π to π'. Denote the set of Weil q-numbers by $W(q)$ and the conjugacy classes by $W(q)/\sim$.

Corollary 35 If A is a simple abelian variety, then π_A is a Weil q-number.

Proof $\mathbb{Q}[\pi_A]$ is a field when A is simple. The result follows from the previous theorem. □

Let $\Sigma(\mathbf{AV}^0_{\mathbb{F}_q})$ be the isomorphism classes of simple objects in $\mathbf{AV}^0_{\mathbb{F}_q}$. Then we have a well defined map

$$\Sigma(\mathbf{AV}^0_{\mathbb{F}_q}) \to W(q)/\sim, \quad A \mapsto \pi_A.$$

Here comes the amazing theorem due to Honda-Tate.

Theorem 43 (Honda-Tate) The map $\Sigma(\mathbf{AV}^0_{\mathbb{F}_q}) \to W(q)/\sim$ is a bijection.

Remark 43 This theorem is highly nontrivial, for example, it tells we can start with a Weil number (e.g. $p^{m/2}$ if m is even) to produce an abelian variety!

Lemma 29 Let π be a Weil q-number. Then there are only three cases:

a. $q = p^{2m}$, $\pi = \pm p^m$ and $\mathbb{Q}(\pi) = \mathbb{Q}$.
b. $q = p^{2m+1}$, $\pi = \pm\sqrt{p^{2m+1}}$, $\mathbb{Q}(\pi)$ is totally real and $[\mathbb{Q}(\pi), \mathbb{Q}] = 2$.
c. For any embedding $j : \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$, $j(\pi) \notin \mathbb{R}$, $\mathbb{Q}(\pi)$ is CM.

Proof If there is a real embedding $\mathbb{Q}(\pi) \hookrightarrow \mathbb{R}$, then we must in the first two cases. Assume now $j(\pi) \notin \mathbb{R}$ for any B. Write $\alpha = \pi + q/\pi$, then $\overline{j(\alpha)} = \overline{j(\pi)} + \overline{j(q/\pi)} = j(q/\pi) + j(\pi) = j(\alpha)$ since π is a Weil q-number. We conclude that $\mathbb{Q}(\alpha)$ is totally real. Moreover, π satisfies a quadratic equation $\pi^2 - \alpha\pi + q = 0$ over $\mathbb{Q}(\alpha)$, hence $\mathbb{Q}(\pi)$ is CM. □

The following is the starting point of the famous Tate conjecture.

Theorem 44 (Tate) The injective map (c.f. Theorem 35) $\mathrm{Hom}(A, B) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}_G(T_\ell A, T_\ell B)$ is a bijection, where $G = \mathrm{Gal}(\bar{k}/k)$.

Remark 44 The image of π_A acts as Frob_q^{-1} on $T_\ell(A)$, where $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ is the arithmetic Frobenius. In fact, $(1 \otimes \mathrm{Frob}_q) \circ (\pi_A \otimes 1)$ is the absolute Frobenius of $A \otimes \overline{\mathbb{F}_q}$, hence is the identity.

We omit Tate's beautiful proof but draw some important consequences.

Corollary 36 Let A, B be abelian varieties over $\mathbb{F}_q$. Then the followings are equivalent:

a. B is isogenous to a subabelian variety of A defined over $\mathbb{F}_q$.

b. There is a G-equivariant injective map $V_\ell(B) \to V_\ell(A)$ for some $\ell \neq p$.

c. $P_B \mid P_A$. In particular, when A, B are isogenous over $\mathbb{F}_q$, then we must have $P_B = P_A$. This proves the injectivity of the map $\Sigma(\mathbf{AV}^0_{\mathbb{F}_q}) \to W(q)/\sim$ in Theorem 43.

Proof (a) implies (b) and (b) implies (c) are clear. (b) implies (a) follows from the previous theorem. (c) implies (b) follows from the fact that the Frobenius acts on $V_\ell(A)$ and $V_\ell(B)$ semisimply with characteristic polynomials P_A and P_B respectively. □

The followings are further results on the structure of $\mathrm{End}^0(A)$ for the case of the finite field $\mathbb{F}_q$.

Theorem 45

a. The center of $\mathrm{End}^0(A)$ is $\mathbb{Q}[\pi_A]$.

b. Every abelian variety over $\mathbb{F}_q$ is of CM-type.

c. Assume that A is simple. Let $D = \mathrm{End}^0(A)$ and $K = \mathbb{Q}[\pi_A]$. Then for v a place of K, we have

$$\mathrm{inv}_v D = \begin{cases} 1/2, & v \text{ real}, \\ \frac{\mathrm{ord}_v \pi_A}{\mathrm{ord}_v q}[K_v : \mathbb{Q}_p], & v \mid p, \\ 0, & \text{otherwise}. \end{cases}$$

Proof

a. By the previous theorem, $\mathrm{End}^0(A) \otimes \mathbb{Q}_\ell \cong \mathrm{End}_G(V_\ell(A))$, which means $\mathrm{End}^0(A) \otimes \mathbb{Q}_\ell$ is the commutant of $\mathbb{Q}_\ell[\pi_A]$ in $\mathrm{End}^0(A) \otimes \mathbb{Q}_\ell$. Using the double commutant theorem, we know that $\mathbb{Q}_\ell[\pi_A]$ is the commutant of $\mathrm{End}^0(A) \otimes \mathbb{Q}_\ell$. Namely, $\mathbb{Q}_\ell[\pi_A]$ is the center of $\mathrm{End}^0(A) \otimes \mathbb{Q}_\ell$.

b. We may assume A simple. Write $e = [K : \mathbb{Q}]$ and $d^2 = [D : K]$. Then $ed \mid 2g$. Write $K \otimes \mathbb{Q}_\ell = K_{v_1} \times \cdots \times K_{v_r}$ and $e_i = [K_{v_i} : \mathbb{Q}_\ell]$. Then $\sum e_i = e$ and $V_\ell(A) = V_1 \times \cdots V_r$, where each V_i is a K_{v_i}-vector spaces. Write $d_i = \dim V_i$, then we know that $\sum e_i d_i = 2g$. Also,

$$D \otimes \mathbb{Q}_\ell = \mathrm{End}_G(V_\ell(A)) = \mathrm{End}_{\mathbb{Q}_\ell[\pi_A]}(V_\ell(A)) = \prod \mathrm{End}_{K_i}(V_i),$$

we know that $ed^2 = \sum e_i d_i^2$. Thus

$$\left(\sum e_i\right)\left(\sum e_i d_i^2\right) = \sum e_i e d^2 = e^2 d^2 \leq 4g^2.$$

Now Cauchy-Schwarz implies that the equality must hold. Hence $ed = 2g$ and $d_i = d$. In particular, A is of CM-type.

c. From the proof of (b) we know that $D \otimes \mathbb{Q}_\ell$ splits at all finite places v of K above ℓ, hence $\mathrm{inv}_v D = 0$. When $K = \mathbb{Q}[\pi_A]$ has a real place, D is one of Type I — III in Albert's classification. Type I is impossible by the restriction $e \mid g$ ($d = 1$ and $e = 2g$). For Type II and Type III, $d = 2$ and $e = g$. But the restriction $2e \mid g$ shows that Type II is also impossible. Hence D is of Type III and must ramify at all real places. The information at p can be obtained similarly by the p-divisible group version of Tate conjecture. □

Example 21

a. $\mathbb{Q}(\pi) = \mathbb{Q}$. Then m is even, $\pi = \pm\sqrt{q} \in \mathbb{Q}$ and $P_A(t) = (t \pm \sqrt{q})^2$. Since A is of CM-type by the previous theorem, D must be a quaternion algebra over $\mathbb{Q}$. So $\mathrm{inv}_v D = 0$ for $v \neq \infty, p$ and $\mathrm{inv}_\infty D = 1/2$. Hence $\mathrm{inv}_p D = 1/2$ and $D = \mathbb{Q}_{p,\infty}$ is the unique quaternion algebra over $\mathbb{Q}$ ramified only at ∞, p. We know that $d = 2$ and $g = 1$, thus A is an elliptic curve. The p-rank of A is zero, since the division quaternion algebra $D \otimes \mathbb{Q}_p$ can not acts on $V_{p,\mathrm{et}}(A)$. We say such an elliptic curve A is *supersingular*.

b. $\mathbb{Q}(\pi)$ is totally real and m is odd. Then $\pi = \pm\sqrt{q}$, D is the quaternion algebra over $\mathbb{Q}(\sqrt{p})$ ramified at two real places. We know that $d = e = g = 2$, thus i is an abelian surfaces. When base change to $\mathbb{F}_{q^2}$, $P_{A \otimes \mathbb{F}_{q^2}}(t) = (t - q)^4$. So $A \otimes \mathbb{F}_{q^2}$ is isogenous to the product of two supersingular elliptic curves.

c. $\mathbb{Q}(\pi)$ is an imaginary quadratic extension of $\mathbb{Q}$. Then x_i is an irreducible quadratic polynomial, thus $g=1$ and i is an elliptic curve. Because, $e=2$, we find that $d=1$ and $D=K$. There are two cases:

   a. p does not split in K, then there is only one place over p. Looking at the action of $D\otimes\mathbb{Q}_p$ on $T_{p,et}$, we see that A is a supersingular elliptic curve. We claim that there exists some N such that $\pi^N\in\mathbb{Q}$, or equivalently, π^2/q is a root of unity. Since $\pi^2-\alpha\pi+q=0$, we know that $|\pi^2/q|_v=1$ for any $v\mid\ell$. Since π is a Weil q-number, $|\pi^2/q|_\infty=1$. By the product formula, we know that $|\pi^2/q|_p=1$. So the claim is proved. By the first case $\mathbb{Q}(\pi)=\mathbb{Q}$, $A\otimes\mathbb{F}_{q^N}$ is a supersingular elliptic curve.

   b. p splits in K. Let v_1,v_2 be the two places over p.

We claim this case A is an *ordinary* elliptic curve (i.e., its p-rank is 1). Otherwise the p-rank is 0, there is only local-local part, hence the p-divisible group $A[p^\infty]$ corresponds to a formal group of dimension 1 and height 2, hence $\mathrm{End}^0(A[p^\infty])$ is a quaternion algebra. Because $D\otimes\mathbb{Q}_p\hookrightarrow\mathrm{End}^0(A[p^\infty])$ is an injection and $D\otimes\mathbb{Q}_p\cong\mathbb{Q}_p\times\mathbb{Q}_p$, we obtain a contradiction.

We have proved the following results.

Theorem 46 Let E be an elliptic curve over $\mathbb{F}_q$. Then there are 3 possibilities:

a. $\mathbb{Q}(\pi)=\mathbb{Q}$, E is supersingular, $D=\mathbb{Q}_{p,\infty}$.
b. $\mathbb{Q}(\pi)$ is an imaginary quadratic field, $D=\mathbb{Q}(\pi)$ and p does not splits, E is supersingular,
c. $\mathbb{Q}(\pi)$ is an imaginary quadratic field, $D=\mathbb{Q}(\pi)$ and p splits, E is ordinary.

Theorem 47 All supersingular elliptic curves over $\overline{\mathbb{F}_q}$ are isogenous, with the endomorphism algebra $D=\mathbb{Q}_{p,\infty}$.

We have seen that every abelian variety over a finite field is of CM-type (Theorem 45). The converse is "almost" true.

Theorem 48 (Grothendieck) Let A be an abelian variety over $k=\bar{k}$, $\mathrm{char}(k)>0$. If A is of CM-type, then A is isogenous to an abelian variety defined over a finite field.

Remark 45 The word "isogenous" cannot be replaced by "isomorphic" in this theorem.

We have the following stronger results for elliptic curves.

Theorem 49 Let E be an elliptic curve over $k=\bar{k}$, $\mathrm{char}(k)>0$. Then $D=\mathrm{End}^0(E)=\mathbb{Q}$ if and only if E cannot be defined over a finite field.

Proof Assume that E cannot be defined over $\overline{\mathbb{F}_q}$. Assume $p>2$ for simplicity. We take the Legendre family $E_\lambda: y^2=x(x-1)(x-\lambda)$ for $\lambda\neq0,1$. Assume that λ is transcendental over $\overline{\mathbb{F}_q}$. Let $K_0=\mathbb{F}_q(\lambda)\subseteq k$. We can regard K_0 as the function field of $S_0=\mathbb{A}^1_{\overline{\mathbb{F}_q}}\setminus\{0,1\}$. So we have a family of elliptic curves $\mathcal{E}\to S_0$ and E_λ is the generic fiber of $\mathcal{E}$ with $D=\mathrm{End}^0(E_\lambda)$. Let $K\subseteq k$ be a finite extension of K_0 such that all endomorphisms of E_λ are defined over K. Let S be the normalization of S_0 in K. By base change we obtain a family $\mathcal{E}_S$ over S. Then $D=\mathrm{End}(E_\lambda\otimes_{K_0}K)$ embeds into $\mathrm{End}(\mathcal{E}_s)$ for any closed point $s\in S$ by Proposition 22 below. By choosing two points $s\in S$ such that the two $\mathcal{E}_s$'s are supersingular with different endomorphism algebras, we conclude that $D=\mathbb{Q}$ since it must embed into the two quaternion algebras simultaneously. □

Proposition 21 Let $E_\lambda: y^2=x(x-1)(x-\lambda)$. Assume $\mathrm{char}(k)=p\neq2$ Then E_λ is supersingular if and only if the polynomial

$$h(\lambda)=\sum_{i=0}^{k}\binom{k}{i}^2\lambda^i$$

is zero, where $k=(p-1)/2$. This polynomial is called the *Hasse polynomial*.

Proof See Hartshorne. □

Corollary 37 Over k, there are only finitely many supersingular elliptic curves up to isomorphism. All are defined over $\overline{\mathbb{F}_p}$.

Proof Because the Hasse polynomial only has finitely many zeros. □

Remark 46 We can also count explicitly the number of supersingular elliptic curves defined over $\overline{F}_p$.

Example 22 For $p=3$, $h(\lambda)=\lambda+1$, so $\lambda=-1$. Over $\overline{\mathbb{F}_3}$, there is only one supersingular elliptic curve $E_{-1}: y^2=x^3-x$, which is already defined over $\mathbb{F}_3$. One can show $\pi=\pm\sqrt{-3}$ in this case. So $E_{-1}\otimes\mathbb{F}_9=-3$. The quadratic twist $E': dy^2=x^3-x$ for some $d\in\mathbb{F}_9^\times/(\mathbb{F}_9^\times)^2$ is isomorphic to E over $\mathbb{F}_{81}$. Using the morphism $\phi: E'\to E, (x,y)\mapsto(x,\sqrt{d}y)$, one can check that $\phi^{-1}\pi_E\phi(x,y)=-\pi_{E'}(x,y)$, hence $\pi_{E'}=-\pi_E$ for a quadratic twist. We conclude that $\pi_{E'}=3$. (In general, for $E: y^2=x^3+ax+b$, define the quadratic twist $E': dy^2=x^2+ax+b$. Let $\rho: \mathrm{Gal}(\bar{k}/k)\to GL_2(\mathbb{Q}_\ell)$ and $\rho': \mathrm{Gal}(\bar{k}/k)\to GL_2(\mathbb{Q}_\ell)$ be the corresponding Galois representation arising from the Tate modules. Then $\rho=\rho'\otimes\eta$, where η is the quadratic character of $k(\sqrt{d})/k$.)

Neron models

Proposition 22 Let R be a DVR, A/R be an abelian scheme and $L=\mathrm{Frac}(R)$. Then $\mathrm{End}(A)\cong\mathrm{End}(A_L)$.

Proof Let $\phi: A_L\to A_L$ be an endomorphism. Let $\Gamma_\phi\subseteq A_L\times A_L$ be its image. Take the closure Γ of Γ_ϕ in $A\times_S A$ ($S=\mathrm{Spec}\,R$), then Γ is a proper flat subgroup scheme of $A\times_S A$ (flatness means torsion-freeness over a DVR). We claim that the connected component Γ^0 is smooth (hence is an abelian scheme). Let η be the generic point of the special fiber A_k and $\mathcal{O}_\eta$ be the local ring of A at η.

Then $\mathcal{O}_\eta$ is DVR (1-dimensional). By the properness and valuative criterion, the endomorphism of the generic fiber automatically extends to an open subset U of the special fiber. But $\Gamma^0_k|_{U\times A_k}$ is the graph of the extension. So Γ^0_k is generically reduced, hence reduced, which proves the claim. The first projection is an isomorphism $\Gamma^0\cong A$, because it is a morphism between abelian schemes and is generically an isomorphism. The second projections Γ^0 to A then gives a morphism $A\to A$ extending ϕ. □

Definition 45 Let A be an abelian variety over L, v a discrete valuation of L and $S=\mathrm{Spec}\,\mathcal{O}_v$. Consider the functor $A^\flat: \mathbf{SmSch}/S\to\mathrm{Grp}$ given by $T\mapsto A(T\times_S\mathrm{Spec}\,L)$. If $A^\flat$ is representable, then we say $A^\flat$ is the Neron model of A. So if the Neron model exists, then it is unique.

Proposition 23 If $A\to S$ is an abelian scheme. Then A is the Neron model of A_L. In this case, we say A_L has *good reduction*.

For a general abelian variety, the existence of the Neron model is a highly nontrivial result.

Theorem 50 (Neron) The Neron model exists.

Abelian varieties of CM-type

Let us come back to the case $k=\mathbb{C}$.

Let K be a CM field of degree $2g$ over $\mathbb{Q}$ and (K,Φ) be a CM-type. By Theorem 3 $A_\Phi=\mathbb{C}^{|\Phi|}/\iota(\mathcal{O}_K)$ is an abelian variety with CM by s, where $\iota: K\hookrightarrow\mathbb{C}^{|\Phi|}$ is the embedding obtained by evaluating the elements of Φ.

If $A=\mathbb{C}^g/\Lambda$ is a complex abelian variety of dimension g with CM by K. Then K acts on $H_1(A,\mathbb{Q})=\Lambda\otimes\mathbb{Q}$. Since both K and $H_1(A,\mathbb{Q})$ are $2g$-dimension over $\mathbb{Q}$, we know that $H_1(A,\mathbb{Q})$ is a 1-dimensional K-vector space. Hence $K\otimes\mathbb{C}=\prod_{K\hookrightarrow\mathbb{C}}\mathbb{C}$ acts on $H_1(A,\mathbb{C})=H_1(A,\mathbb{Q})\otimes\mathbb{C}$.

There is a Hodge filtration

$$0\to H^0(A,\Omega_A)\to H^1(A,\mathbb{C})\to H^1(A,\mathcal{O}_A)\to 0.$$

Taking dual gives that

$$0\to(\mathrm{Lie}\,\hat{A})^\vee\to H_1(A,\mathbb{C})\to\mathrm{Lie}\,A\to 0.$$

This is an exact sequence of $K\otimes\mathbb{C}$-modules. Moreover, $K\otimes\mathbb{C}$ acts on $\mathrm{Lie}\,A$ via $K\otimes\mathbb{C}\to\prod_\Psi\mathbb{C}$, where $\Psi\subseteq\mathrm{Hom}(K,\mathbb{C})$ is some subset of cardinality g.

Hodge theory tells us that $H_1(A,\mathbb{C})=\mathrm{Lie}\,A\oplus\overline{\mathrm{Lie}\,A}$. So if Ψ acts on $\mathrm{Lie}\,A$, then $\bar{\Psi}$ acts on $\overline{\mathrm{Lie}\,A}$. Hence (K,Ψ) is actually a CM-type. When we identify $\mathrm{Lie}\,A$ with $\mathbb{C}^{|\Psi|}$, then $\Lambda\otimes\mathbb{Q}\cong\iota(K)$ under the embedding $\iota: K\hookrightarrow\mathbb{C}^{|\Psi|}$. Hence A is isogenous to A_Ψ.

We have proved:

Theorem 51 Let A be an abelian variety over $\mathbb{C}$ with CM-type (K,Φ). Then the abelian variety $A_\Phi = \mathbb{C}^\Phi/(\iota(\mathcal{O}_K))$ is isogenous to A. In other words, a CM-type determines an isogeny class of abelian varieties.

Proposition 24 Let A be an abelian variety over $\mathbb{C}$ with CM by K. Then A is defined over $\overline{\mathbb{Q}}$. In fact, there is a unique model of A over $\overline{\mathbb{Q}}$.

Proof

a. Uniqueness. Suppose $k \subseteq \Omega$ are two algebraically closed fields of characteristic 0. Then $\mathrm{Hom}_k(A,B) \to \mathrm{Hom}_\Omega(A_\Omega, B_\Omega)$ is an isomorphism for any two abelian varieties A, B (actually we can replace C by any separably closed field). In fact, the Hom set is represented by an etale finite group scheme. Observe that $A(k)_{\mathrm{tor}} \cong A(\Omega)_{\mathrm{tor}}$ as $A[n] \cong (\mathbb{Z}/n\mathbb{Z})^g$ over any algebraically closed field. Suppose $f : A_\Omega \to B_\Omega$ and $a \in \mathrm{Aut}(\Omega/k)$. Then we know that $fa = af$ as the torsion subgroups are Zariski dense and they coincide on the torsion subgroups.

b. Existence. Let A be an abelian variety over $\mathbb{C}$ with CM-type (K,Φ). Let $R \subseteq \mathbb{C}$ finitely generated over $\overline{\mathbb{Q}}$ such that A and $K \hookrightarrow \mathrm{End}^0(A)$ are both defined over R. Then we obtain an abelian scheme $\mathcal{A} \to S = \mathrm{Spec}\, R$. For any closed point $s = \mathrm{Spec}\,\overline{\mathbb{Q}} \hookrightarrow S$, K acts on $\mathcal{A}_s$. We claim $\mathcal{A}_s \otimes \mathbb{C}$ is an abelian variety over $\mathbb{C}$ of CM-type (K,Φ). The action of K is clear. To see it has CM-type (K,Φ), we look at the action of $K \otimes_{\mathbb{Q}} \mathcal{O}_{S_{\mathbb{C}}}$ on $\mathrm{Lie}\,\mathcal{A}_{S_{\mathbb{C}}}$. This action factors through (K,Φ) on the generic fiber, hence itself factors through (K,Φ). So $\mathcal{A}_s \otimes \mathbb{C}$ and A are isogenous by the previous theorem. Let N be the kernel of $\mathcal{A}_s \otimes \mathbb{C} \to A$. Since N and $\mathcal{A}_s \otimes \mathbb{C}$ are defined over $\overline{\mathbb{Q}}$, we know that A itself is defined over $\overline{\mathbb{Q}}$. □

Proposition 25 Let A be an abelian of CM-type over a number field k. Let $\mathfrak{p}$ be a prime of k over p. Then after a possible finite base change of k, A has a good reduction at $\mathfrak{p}$.

Proof The proof is based on the following theorem.

Theorem 52 (Neron-Ogg-Shafarevich) For any abelian variety A, A has good reduction at $\mathfrak{p}$ if and only if the inertia subgroup $I_\mathfrak{p} \hookrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}/k)$ acts trivially on $T_\ell A$.

Come back to our case, since A has CM by s, we know that $\mathrm{Gal}(\overline{\mathbb{Q}}/k) \hookrightarrow (\mathrm{End}_{K\otimes\mathbb{Q}_\ell} V_\ell(A))^\times \cong (K\otimes\mathbb{Q}_\ell)^\times$, where the second isomorphism is due to the dimension reason. So $\mathrm{Gal}(\overline{\mathbb{Q}}/k)^{\mathrm{ab}}$ maps to a compact subgroup in $(K\otimes\overline{\mathbb{Q}_\ell})^\times$, hence maps to $(\mathcal{O}_k \otimes \mathbb{Z}_\ell)^\times$. Since $(\mathcal{O}_k \otimes \mathbb{Z}_\ell)^\times$ is pro-ℓ up to finite index and, by local class field theory, the image of $I_\mathfrak{p}$ is pro-p up to finite index, the Neron-Ogg-Shafarevich then tells us A has good reduction after a finite extension. □

Suppose A is an abelian variety with CM-type (K,Φ) and good reduction at $\mathfrak{p}$, then the reduction $\bar{A} = A^\flat \otimes \kappa(\mathfrak{p})$ is an abelian variety over the finite field $\kappa(\mathfrak{p}) = \mathbb{F}_q$, hence gives a Weil q-number π_A. Suppose A' is another abelian variety with CM-type (K,Φ) and good reduction at $\mathfrak{p}$, then $\pi_A^N = \pi_{A'}^N$ for some N since A and A' will be isogenous after a finite extension by the previous proposition. In this way the CM-type (K,Φ) determines the Weil q-number π_A up to roots of unity. Moreover, π_A can be viewed as an element of K by the following lemma.

Lemma 30 The Weil q-numbers corresponding to a CM-type (K,Φ) lie inside $K \subseteq \mathrm{End}^0(\bar{A})$.

Proof Since K is the maximal subfield in $\mathrm{End}^0(V_\ell \bar{A})$ (of degree $2g$), we know that the commutant of K inside $\mathrm{End}^0(V_\ell A)$ is K. The lemma then follows because π_A commutes with the action of K. □

Theorem 53 (Shimura-Taniyama Formula) Assume that k contains K and A is an abelian variety with CM-type (K,Φ) and good reduction at a place $\mathfrak{p} \mid p$ of k. Let $v \mid p$ be a place of K. Then

$$\frac{\mathrm{ord}_v(\pi_A)}{\mathrm{ord}_v(q)} = \frac{\#(\Phi \cap H_v)}{\#H_v},$$

where $H_v = \{i : K \hookrightarrow k : i^{-1}\mathfrak{p} = v\}$.

Remark 47 We omit the proof of this important result. Notice this formula makes sense because changing π_A by a root of unity does not affect the result.

Finally, as an application of the Shimura-Taniyama formula, let us sketch the proof of the Honda-Tate theorem 43.

Proof (Sketch) The injectivity follows from Corollary 36, so we only need to check the surjectivity. Assume $\mathbb{Q}(\pi)$ is a CM field (the real cases are easy). Let D be the division algebra over $\mathbb{Q}(\pi)$ given by Theorem 45, we know that

$ed = 2g$. There exists a CM subfield $K \subseteq D$ containing $\mathbb{Q}(\pi)$ of degree $2g$ over $\mathbb{Q}$ (we omit the details). Fix an algebraic closure $\overline{\mathbb{Q}_p}$ and write $H = \mathrm{Hom}(K, \overline{\mathbb{Q}_p})$. Then $H = \coprod_{v|p} H_v$, where $H_v = \mathrm{Hom}(K_v, \overline{\mathbb{Q}_p})$. We claim that there exists a CM-type (K, Φ) such that for any place $v \mid p$ of s,

$$\frac{\mathrm{ord}_v(\pi)}{\mathrm{ord}_v(q)} = \frac{\#(H_v \cap \Phi)}{\#H_v}.$$

This claim allows us to construct an abelian variety possibly defined over a finite extension (due to the problem of roots of unity) with the required Weil q-number using reduction of complex abelian varieties at a prime. Finally we apply the Weil restriction functor to obtain the required abelian variety with Weil q-number π. □

References

[1] Mumford, D, *Abelian varieties,* Oxford Univ Press, 1970.

[2] Milne, James S., *Abelian Varieties (v2.00),* Available at www.jmilne.org/math/.

[3] Gerard van der Geer and Ben Moonen, *Abelian varieties,* http://staff.science.uva.nl/~bmoonen/boek/BookAV.html.