Abelian Varieties

https://phanpu.github.io/

May 2023

Contents

0 Notation and conventions

Remark 0.1. *By a variety over a field k we mean a separated k-scheme of finite type which is geometrically integral.*

Definition 0.2. Let p be a prime number. We say that a scheme X has characteristic p if the unique morphism $X \to \mathrm{Spec}(\mathbb{Z})$ factors through $\mathrm{Spec}(\mathbb{F}_p) \hookrightarrow \mathrm{Spec}(\mathbb{Z})$. This is equivalent to that for every open subset $U \subseteq |X|$ we have $p \cdot 1 = 0$ for $1 \in \mathcal{O}_X(U)$. We say X has characteristic 0 if $X \to \mathrm{Spec}(\mathbb{Z})$ factors through $\mathrm{Spec}(\mathbb{Q}) \hookrightarrow \mathrm{Spec}(\mathbb{Z})$, which is equivalent to that $n \in \mathcal{O}_X(U)^*$ for all $n \in \mathbb{Z}\backslash\{0\}$ and open subset $U \subseteq |X|$.

Proposition 0.3. If $X \to Y$ is a morphism of schemes, and Y has characteristic p (with p a prime number or $p = 0$) then X has characteristic p, too.

Definition 0.4. Let p be a prime number. Let Y be a scheme of characteristic p. Then we have a morphism $\mathrm{Frob}_Y : Y \to Y$, called the absolute Frobenius morphism of Y, it is given by

(a) Frob_Y is the identity on the underlying topological space $|Y|$;

(b) $\mathrm{Frob}_Y^\sharp : \mathcal{O}_Y \to \mathcal{O}_Y$ is given on sections by $f \mapsto f^p$.

Remark 0.5. *If $\pi : X \to S$ is a morphism of schemes, then the absolute Frobenius morphism Frob_X may be not an S-morphism.*

Definition 0.6. Now we consider the relative Frobenius morphism. We define the scheme $X^{(p/S)}$ to be the base change under the morphism Frob_S

$$\begin{tikzcd} X^{(p/S)} \arrow[r, "h"] \arrow[d, "\pi^{(p)}"'] & X \arrow[d, "\pi"] \\ S \arrow[r, "\mathrm{Frob}_S"'] & S \end{tikzcd}$$

Now we have a natural morphism $F_{X/S}$, called the relative Frobenius morphism of X and defined by the following commutative diagram

$$\begin{tikzcd} X \arrow[dr, "F_{X/S}"] \arrow[drr, bend left, "\mathrm{Frob}_X"] \arrow[ddr, bend right, "\pi"'] & & \\ & X^{(p/S)} \arrow[r, "h"] \arrow[d, "\pi^{(p)}"'] & X \arrow[d, "\pi"] \\ & S \arrow[r, "\mathrm{Frob}_S"] & S \end{tikzcd}$$

Example 1. Assume that $S = \mathrm{Spec}(R)$, and $X = \mathrm{Spec}(R[t_1, \cdots, t_m]/I)$ for some ideal $I = (f_1, \cdots, f_n)$. Let $f_i^{(p)}$ be the polynomial obtained from f_i by changing all coefficients of f_i to the pth-power. More explicitly, if $f_i = \sum a_j(\Pi t_i)$, then $f_i^{(p)} = a_j^p(\Pi t_i)$. Then $X^{(p)} = \mathrm{Spec}(R[t_1, \cdots, t_m]/I^{(p)})$ with $I^{(p)} = (f_1^{(p)}, \cdots, f_n^{(p)})$. And the relative Frobenius morphism $F_{X/S} : X \to X^{(p)}$ is given on rings by the homomorphism

$$R[t_1, \cdots, t_m]/I^{(p)} \to R[t_1, \cdots, t_m]/I$$

with $r \mapsto r$ for $r \in R$ and $t_j \mapsto t_j^p$.

Proposition 0.7. For any base change $T \to S$, there is an isomorphism

$$(X^{(p/S)})_T \cong (X_T)^{(p/T)}$$

Definition 0.8. We may define the morphism $\mathrm{Frob}_Y^n : Y \to Y$ to be the nth iterate of the absolute Frobenius morphism $\mathrm{Frob}_Y : Y \to Y$. Similarly, there is an nth iterate of the relative Frobenius morphism $F_{X/S}^n : X \to X^{p^n/S}$.

Remark 0.9. *If $S = \mathrm{Spec}(\mathbb{F}_q)$, where $q = p^n$. If X is an S-scheme, then the absolute Frobenius morphism Frob_X^n is precisely an S-morphism. Indeed,*

$$\mathrm{Frob}_X^n = F_{X/S}^n$$

This is because Frob_S here is exactly id_S. We refer to $\pi_X = \mathrm{Frob}_X^n$ as the geometric Frobenius morphism of X.

More generally, suppose that S is a scheme over $\mathrm{Spec}(\mathbb{F}_q)$. If X is an S-scheme then by an $\mathbb{F}_q$-structure on X we mean a scheme X_0 with an isomorphism of S-schemes

$$X_0 \otimes_{\mathbb{F}_q} S \cong X$$

Then if X is given an $\mathbb{F}_q$-structure, the geometric Frobenius morphism of X_0 induces a geometric Frobenius morphism of X.

1 Definitions and basic examples

We omit the definitions of group varieties and Abelian varieties, as well as their basic properties.

Proposition 1.1. Let X be a group variety over a field k. Then X is smooth over k. If we write $T_{X,e}$ for the tangent space for the at the identity element, there is a natural isomorphism $\mathcal{T}_{X/k} \cong T_{X,e} \otimes_k \mathcal{O}_X$. This induces natural isomorphisms

$$\Omega_{X/k}^n \cong (\bigwedge^n T_{X,e}^\vee) \otimes_k \mathcal{O}_X$$

In particular, $\Omega_{X/k}^g \cong \mathcal{O}_X$, where $g = \dim X$.

Proof. Since X is a variety, the nonsingular points form a nonempty subset of X. Since the property that being nonsingular is stable under translations, X must be nonsingular.

Let $S = \mathrm{Spec}(k[\epsilon]/(\epsilon^2))$, by the exercise II.2.8 in this book, the element $\tau \in T_{x,e}$ corresponds to an S-value point $\tilde{\tau} : S \to X$, which reduce to $e : \mathrm{Spec}(k) \to X$ modulo ϵ.

A vector field on X is defined by an automorphism of X_S which reduce to the identity on X. For any vector $\tilde{\tau} : S \to X$, let $\zeta(\tau)$ be the vector field defined by $t_{\tilde{\tau}}$, that is, defined by

$$X_S = X_S \times_S S \xrightarrow{(id,\tilde{\tau})} X_S \times_S X_S \xrightarrow{m} X_S$$

Then τ corresponds to a global element in $\Gamma(X, \mathcal{T}_{X/k})$. That is, there is a k-linear map

$$T_{X,e} \to \Gamma(X, \mathcal{T}_{X/k})$$

Then these by replacing X with some other open sets we can obtain a homomorphism

$$\alpha : T_{X,e} \otimes_k \mathcal{O}_X \to \mathcal{T}_{X/k}$$

As this is a homomorphism between locally free $\mathcal{O}_X$-modules of the same rank, it suffices to show that α is surjective. If $x \in X$ is a closed point, the map $\alpha_x (\text{mod } \mathfrak{m}_x)$ is

$$T_{x,e} \otimes_k k(x) \to (\mathcal{T}_{X/k})_x \otimes_{\mathcal{O}_{X,x}} k(x) = T_{X,x}$$

which is exactly the map $T_{X,e} \to T_{X,x}$ induced by t_x. Since the map restricting to stalks α_x are surjective, α is also surjective. ■

Corollary 1.2. The only global vector fields on X are the vector fields defined by $t_{\tilde{\tau}}$.

Proof. This follows from $\Gamma(X, \mathcal{O}_X) = k$. ■

Theorem 1.3 (rigidity theorem)**.** Consider a morphism $f : X \times Y \to Z$, and assume that X is complete. If there is a point $y \in Y$ such that $X \times \{y\}$ maps to a fixed point $z \in Z$, then f factors through the projection $p_Y : X \times Y \to Y$.

Proof. Since the hypothesis holds when we extend k to k^{al}, we may assume that k is algebraically closed, we work on the k-rational points.

Choose an affine open neighborhood U of z. Since X is complete, the projection $p_Y : X \times Y \to Y$ is a closed map. Thus, $W \triangleq p_Y(f^{-1}(Z/u))$ is closed in Y. By the assumption, $y \notin W$. Also, for any $y' \notin W$, $f(X \times \{y'\}) \subseteq U$. Considering that U is affine and $X \times \{y'\}$ is complete, we conclude that $f(x \times y')$ consists of a single point. As a result, $f : X \times (Y - W) \to Z$ factors through p_{Y-W}. Note that $X \times Y$ is irreducible, $X \times (Y - W)$ is dense in it. Therefore, f factors through p_Y everywhere. ■

Proposition 1.4. Every morphism $\alpha : X \to Y$ of Abelian varieties is the composite of a homomorphism with a translation.

Proof. Let 0_X be the unit of X as a group. Suppose that the morphism sends 0_X to y. After composing α with the translation $-y$ we may assume that $\alpha(0) = 0$. Now it remains to show that α is precisely a homomorphism of groups, that is, $\alpha(x + x') = \alpha(x) + \alpha(x')$. Consider the map

$$\varphi : X \times X \to Y \quad (x, x') \mapsto \alpha(x + x') - \alpha(x) - \alpha(x')$$

then it is a morphism with $\varphi(X \times \{0\}) = 0 = \varphi(\{0\} \times X)$. By the rigidity theorem we have $\varphi \equiv 0$. ■

Corollary 1.5. (1) If X is a variety over a field k and $0_X \in X(k)$ then there is at most one structure of an Abelian variety on X for which 0_X is the identity element.

(2) The group structures on Abelian varieties are commutative.

Proposition 1.6. Any morphism from $\mathbb{P}^1$ to a group variety is constant.

Proof. A more explicit description of this type of question could be got from section 1.3 from Milne's note. ■

Theorem 1.7. A rational map $\varphi : V \dashrightarrow W$ from a normal variety V to a complete variety W is defined on an open subset $U \subseteq V$ whose complement $V - U$ has codimension ≥ 2.

Proof. Assume first that V is a curve. Then it remains to show that φ can be extended to the whole V, that is, $U = V$.
Suppose that U is an open subset such that $\varphi|_U$ is a morphism. Consider the product $W \times V$, let Z be the closure of

$$\{(\varphi(Q), Q) : Q \in U\}$$

then we have a dominant morphism

$$U \to Z \to V$$

and the image of Z is closed in V since W is complete. Hence we must have $Z \to V$ is surjective. Note that $Z \to V$ is a birational morphism of curves, with V nonsingular, it must be an isomorphism then. Inverting the isomorphism, we obtain a homomorphism $V \to Z \to W$ extending $U \to Z \to W$.
For the general case, let U be a subset on which φ is defined, and suppose that $V - U$ has codimension 1. Then there is a prime divisor $Z \subseteq V - U$. Since V is normal, the corresponding local ring $\mathcal{O}_Z$ is a DVR with fractional field $k(V)$. Note that the map φ defines a morphism $\mathrm{Spec}(k(V)) \to U \to W$, by the valuation of properness, we obtain a morphism $\mathrm{Spec}(\mathcal{O}_Z) \to W$. This implies that φ has a representative defined on an open subset U' such that U' contains the generic point of Z. Thus φ can be defined everywhere. ∎

Lemma 1.8. Let $\varphi : V \dashrightarrow G$ be a rational map from a nonsingular variety to a group variety. Then either φ is defined on all of V or the points where it is not defined form a closed subset of pure codimension 1 in V (i.e., a finite union of prime divisors).

Proof. Define a rational map $\Phi : V \times V \dashrightarrow G$ via $(x, y) \mapsto \varphi(x)\varphi^{-1}(y)$. We first prove that Φ is defined at (x, x) if and only if φ is defined at x.
Clearly if φ is defined on x, then Φ is defined on (x, x) and $\Phi(x, x) = e$.
Conversely if Φ is a morphism defined at (x, x), then by choosing the open neighborhood $\{x\} \times V$ on where Φ is defined, there must be a subset $U \subseteq V$ (not necessarily containing x) on which φ is defined.
For $u \in U$, the homomorphism $\varphi(x) = \Phi(x, u)\varphi(u)$ expands φ at x. Thus Φ is defined at (x, x) if and only if φ is defined at x.
The rational map Φ defines a map

$$\Phi^* : \mathcal{O}_{G,e} \to k(V \times V)$$

Note that if Φ is defined on (x, x), then Φ sends it to $e \in G$. Thus, Φ is defined at (x, x) if and only if

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

Note that the stalk $\mathcal{O}_{V \times V,(x,x)}$ is defined by

$$\{f \in k(V \times V) | \text{there is no prime divisor } Z \text{ such that } (x, x) \in Z \text{ and } v_Z(f) < 0\} \cup \{0\}$$

we have φ is not defined over x if and only if there exists $f \in \mathrm{Im}(\mathcal{O}_{G,e})$ such that $v_{Z_x}(f) < 0$. We identify these prime divisors as a subset of V, its closure is obviously a finite union of prime divisors on which φ is not defined on. ■

Corollary 1.9. A rational map $\alpha : V \dashrightarrow A$ from a nonsingular variety to an Abelian variety is defined on the whole of V.

Proof. This is the consequence of the above two results. ■

Theorem 1.10. Let $\alpha : V \times W \to A$ be a morphism from a product of nonsingular varieties to an Abelian variety, and assume that $V \times W$ is geometrically irreducible (if we further assume that V or W is complete, then it is a special case of the rigidity theorem). If

$$\alpha(V \times \{w_0\}) = \{\alpha_0\} = \alpha(\{v_0\} \times W)$$

for some $\alpha_0 \in A(k)$, $v_0 \in V(k)$, $w_0 \in W(k)$, then

$$\alpha(V \times W) = \{\alpha_0\}$$

Proof. ■

Corollary 1.11. Every rational map $\alpha : G \dashrightarrow A$ from a group variety to an Abelian variety (now α is a morphism) is the composite of a homomorphism $h : G \to A$ with a translation.

Theorem 1.12. If two Abelian varieties are birational equivalent, then they are isomorphic as Abelian varieties.

Proof. The birational map $\varphi : A \to B$ is actually defined on the whole A and is surjective. Hence it is an isomorphism of varieties. By composing a translation the new morphism maps 0 to 0, this morphism is a homomorphism of groups. Then we obtain an isomorphism of Abelian varieties. ■

Proposition 1.13. Every rational map $\mathbb{A}^1 \dashrightarrow A$ or $\mathbb{P}^1 \dashrightarrow A$ is constant.

Proof. Note that α is actually a morphism. After composing a translation we may suppose that $\alpha(0) = 0$ and then α is a homomorphism, that is, $\alpha(a + a') = \alpha(a) + \alpha(a')$. Therefore, α is an additive morphism on $\mathbb{A}^1$.
But $\mathbb{A}^1 - \{0\}$ is also a group variety, there exists a translation $\beta = -\alpha(1)$ defined on A such that $\beta \circ \alpha$ is a group homomorphism mapping 1 to 0. Hence $\alpha(xy) - \alpha(1) = \alpha(x) + \alpha(y) - 2\alpha(1)$ for all $x, y \in \mathbb{A}^1 - \{0\}$. This implies that $\alpha((x-1)(y-1)) = 0$ for all $x, y \in \mathbb{A}^1 - \{0\}$. Obviously it infers that $\alpha \equiv 0$. ■

Definition 1.14. We call that a variety V with dimension n is unirational if there is a dominating rational map $\mathbb{A}^n \dashrightarrow V$; equivalently, $k(V)$ can be embedded into $k(X_1, \cdots, X_n)$. A variety V over an arbitrary field k is said to be unirational if $V_{k^{\mathrm{al}}}$ is unirational.

Proposition 1.15. Every rational map $\alpha : V \dashrightarrow A$ from a unirational variety to an Abelian variety is constant.

Proof. The composite $\mathbb{A}^n \dashrightarrow V \dashrightarrow A$ induces a rational map $\beta : \mathbb{P}^1 \times \mathbb{P}^1 \times \cdots \times \mathbb{P}^1 \dashrightarrow A$, and then the rational map can be extended to the whole space.
By the previous results, there exists morphisms $\beta_i : \mathbb{P}^1 \to A$ such that $\beta(x_1, \cdots, x_d) = \sum \beta_i(x_i)$. Then the morphism is constant. ■

2 Line bundles and divisors on Abelian varieties

In this section we prove that all Abelian varieties are projective.

2.1 The theorem of the square

Remark 2.1. *If L is a line bundle on $X \times Y$, then we define $L_y = i^*L$, where $i : X_y = X \times \{y\} \to X \times Y$.*

Theorem 2.2. Let X and Y be varieties. Assume that X is complete. Let L and M be two line bundles on $X \times Y$. If for all closed points $y \in Y$ we have $L_y \cong M_y$ as sheaves on X_y, then there exists a line bundle N on Y such that $L \cong M \otimes p_Y^* N$.

Proof. Since $L_y \otimes M_y^{-1}$ is the trivial bundle and the variety $X_y = X \times \operatorname{Spec}(k(y)) \to \operatorname{Spec}(k(y))$ is complete, $H^0(X_y, L_y \otimes M_y^{-1}) \cong k(y)$. Thus, by Grauert's result, which can be found in this book III.12.9, the sheaf $(p_Y)_*(L \otimes M^{-1})$ is locally free of rank one.

We shall prove that the pullback $(p_Y)^*(p_Y)_*(L \otimes M^{-1})$ is isomorphic to $L \otimes M^{-1}$ through the canonical morphism

$$\alpha : (p_Y)^*(p_Y)_*(L \otimes M^{-1}) \to L \otimes M^{-1}$$

We first look at its property by restricting on X_y. The induced map is

$$\Gamma(X_y, \mathcal{O}_{X_y}) \otimes_{k(y)} \mathcal{O}_{X_y} \to X_y$$

which is an isomorphism since X_y is complete.

By Nakayama lemma and comparing the rank, we conclude that α is an isomorphism. ■

Corollary 2.3 (See-saw principle)**.** With the same assumptions of above, if additionally we assume that $L_x \cong M_x$ for some points $x \in X$ then $L \cong M$.

Proof. We have $L \cong M \otimes p_Y^* N$. Over $\operatorname{Spec} k(x) \times Y$ this induces that $(p_Y^* N)_x \cong N$ is trivial. ■

Next we prove the theorem of the cube.

Lemma 2.4. Let X and Y be varieties, with X complete. For a line bundle L on $X \times Y$, the set $\{y \in Y | L_y \text{ is trivial}\}$ is closed in Y.

Proof. Note that X_y is complete. Thus, L_y is trivial if and only if $L_y(X_y)$ and $L_y^{-1}(X_y)$ are both non-zero (see this link). Hence

$$\{y \in Y | L_y \text{ is trivial}\} = \{y \in Y | h^0(L_y) > 0\} \cap \{y \in Y | h^0(L_y^{-1}) > 0\}$$

But the functors $y \mapsto h^0(L_y)$ and $y \mapsto h^0(L_y^{-1})$ are upper-continuous on Y, so the two sets of the right side are closed. ■

Proposition 2.5. Let X be a complete variety over a field K, let Y be a k-scheme, and let L be a line bundle on $X \times Y$. Then there exists a closed subscheme $Y_0 \hookrightarrow Y$ which is the maximal subscheme of Y over L which is trivial, i.e.,

(i) the restriction of L to $X \times Y_0$ is the pull back (under p_Y) of a line bundle on Y_0

(ii) if $\varphi : Z \to Y$ is a morphism such that $(id_X \times \varphi)^* L$ is the pullback of a line bundle on Z under p_Z^* then φ factors through Y_0.

Proof. This is a trivial consequence of the existence of the Picard scheme, which we will discuss in section 6. Let $Y \to \mathrm{Pic}_{X/k}$ be the map corresponding to L, then Y_0 is simply the fibre over the zero section of $\mathrm{Pic}_{X/k}$. ■

Lemma 2.6. Let X be a complete variety, and let L be a locally free sheaf on X . If $L_K = (X_K \to X)^* L$ becomes trivial on X_K for some field $K \supseteq k$, then L is trivial on X.

Proof. We reuse the result that an invertible sheaf is trivial if and only if both it and its dual have nonzero global section. Then the result follows obviously from that

$$\dim_K \Gamma(X_K, L_K) = \dim_K(\Gamma(X, L) \otimes_k K) = \dim_k \Gamma(X, L)$$

■

Theorem 2.7. Let X and Y be complete varieties over k and let Z be connected, locally Noetherian k-scheme. Consider points $x \in X$ and $y \in Y$, and let z be a point of Z. If L is a line bundle on $X \times Y \times Z$ whose restrictions to $\{x\} \times Y \times Z$, $X \times \{y\} \times Z$ and $X \times Y \times \{z\}$ are trivial, then L is trivial.

Proof. ■

Remark 2.8. *The analogous statement for line bundles on a product of two complete varieties is generally false. More precise, suppose X and Y are complete k-varieties and L is a line bundle on $X \times Y$. If there exists points $x \in X$ and $y \in Y$ such that L_x and L_y are trivial, it is not true that L is generally trivial.*

Theorem 2.9 (Theorem of the Cube)**.** Let L be a line bundle on X. Then the line bundle

$$\theta(L) = p_{123}^* L \otimes p_{12}^* L^{-1} \otimes p_{13}^* L^{-1} \otimes p_{23}^* L^{-1} \otimes p_1^* L \otimes p_2^* L \otimes p_3 L^*$$

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

Proof. Note that the restriction of L to $\{0\} \times X \times X$ is trivial. ■

Corollary 2.10. Considering the morphism $(f, g, h) : Y \to X \times X \times X$ from a scheme Y to a product of three Abelian varieties. Then we have that the bundle

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

on Y is trivial.

Corollary 2.11 (Theorem of the Square)**.** Although 2.7 has no square version, we can obtain a square analogue of 2.10. This result is mainly why we introduce the theorem of cube.

By taking $f = \mathrm{id},\ g = x,\ h = y : X \to X$, then for all $x, y \in X(k)$,

$$t_{x+y}^* L \otimes L \cong t_x^* L \otimes t_y^* L$$

Corollary 2.12. If L is a line bundle on an Abelian variety X. The map $\varphi_L : X(k) \to \mathrm{Pic}(X)$ given by $x \mapsto [t_x^* L \otimes L^{-1}]$ is a homomorphism.

Corollary 2.13. By making $f = n,\ g = 1,\ h = -1 : X \to X$, we can obtain another consequence of 2.7.

For every line bundle L on X, we have

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

Definition 2.14. We say that a line bundle L is symmetric, if $(-1)^* L \cong L$. As a result, $n^* L \cong L^{n^2}$.

Similarly, we can define anti-symmetric line bundle as $(-1)^* L \cong L^{-1}$. At this time, $n^* L \cong L^n$.

2.2 Projectivity of Abelian varieties

Definition 2.15. Let L be a line bundle on an Abelian variety X. On $X \times X$ we define the Mumford line bundle $\Lambda(L)$ by

$$\Lambda(L) = m^* L \otimes p_1^* L^{-1} \otimes p_2^* L^{-1}$$

Note that the restriction of $\Lambda(L)$ on $\{x\} \times X$ is $t_x^* L \otimes L^{-1}$.

We define $K(L)$ as the maximal closed subscheme of X such that $\Lambda(L)|_{X \times K(L)}$ is trivial on $X \times \{y\}$ for any $y \in K(L)$. As a result, $\Lambda(L)|_{X \times K(L)}$ could be written as $p_2^* M$ for some line bundle M on $K(L)$.

Note that $K(L)$ is compatible with the base change.

Lemma 2.16. Let T be a k-scheme and $x : T \to X$ a T-valued point of X. As usual, define L_T to be the pull-back of L under the morphism $X_T \to X$.

1. The morphism x factors through $K(L)$ if and only if $t_x^* L_T \otimes L_T^{-1}$ is a pull-back of a line bundle on T.

2. If $t_x^* L_T \otimes L_T^{-1} \cong p_T^* M$, then $M \cong x^* T$.

Proof. 1. We rewrite the composite

$$X_T \xrightarrow{t_x} X_T \to X$$

as

$$X_T \xrightarrow{\mathrm{id} \times x} X \times X \xrightarrow{m} X$$

Thus, $t_x^* L_T = (\mathrm{id}_X \times x)^* m^* L$.

Note that we can also rewrite

$$X_T \to X$$

as

$$X_T \xrightarrow{\mathrm{id}\times x} X \times X \xrightarrow{p_1} X$$

We have $L_T = (\mathrm{id}_X \times x)^* p_1^* L$.

Then

$$t_x^* L_T \otimes L_T^{-1} = (\mathrm{id}_X \times x)^*[\Lambda(L) \otimes p_2^* L] = (\mathrm{id}_X \times x)^* \Lambda(L) \otimes (p_T^* x^* L)$$

Recall that $\Lambda(L)|_{X\times K}$ could be written as $p_2^* M$ for any $K \subseteq K(L)$. Thus, x factors through $K(L)$ if and only if $p_T^* M$ for some line bundle M on T.

2. We just compute M through $\alpha : T \xrightarrow{t\mapsto(0,t)} X_T$. We know that $M \cong \alpha^* p_T^* M = \alpha^*(t_x^* L_T \otimes L_T^{-1})$.

Note that the composite

$$T \xrightarrow{\alpha} X_T \xrightarrow{t_x} X_T \to X$$

is exactly the morphism x. Thus, $\alpha^* t_x^* L_T = x^* L$.

Also, the composite

$$T \xrightarrow{\alpha} X_T \xrightarrow{p_X} X$$

is constant. Then the pull-back of L^{-1} factors through a point. Note that L^{-1} is a line bundle, the pull-back of L^{-1} is trivial. Thus, $\alpha^* L_T^{-1}$ is trivial. Therefore, $M \cong x^* T$. ■

From the prove of the above two statements, we can obtain a more interesting result.

Proposition 2.17. We have $\Lambda(L)|_{X\times K(L)} \cong \mathcal{O}_{X\times K(L)}$.

Proposition 2.18. The subscheme $K(L)$ is a subgroup scheme of X.

Proof. The first statement of 2.16 offers us a way to define the group structure on $K(L)(T)$ for any k-scheme T. The theorem of square tells us that this group structure is exactly compatible with the original group structure. ■

We will prove the following fact we will use here in the next section: let X be an Abelian variety, for any closed subgroup scheme $Y \subseteq X$, let Y^0 be the connected component contained the origin, then $Y^0_{\mathrm{red}} \hookrightarrow Y \hookrightarrow X$ is a Abelian subvariety of X.

Lemma 2.19. If L is ample then $K(L)$ is a finite group scheme.

Proof. Obviously we can assume that k is algebraically closed. Set $Y = K(L)^0_{\mathrm{red}} \subseteq X$. Let L' be the restriction of L to Y. The line bundle $\Lambda(L')$ is then trivial on $Y \times Y$. Pulling back through the morphism $Y \xrightarrow{(\mathrm{id}_Y, -\mathrm{id}_Y)} Y \times Y$ we can obtain a trivial line bundle $L' \otimes (-1)^* L'$ on Y.

Note that $(-1)^* L'$ is also ample, thus $L' \otimes (-1)^* L'$ is ample. Hence, every invertible sheaf of Y is generated by the global section. Thus, $\dim(Y) = 0$. ■

Proposition 2.20. Let X be an Abelian variety over an algebraically closed field k. Let $f : X \to Y$ be a morphism of k-varieties. For $x \in X$, let C_x denote the connected component of the fibre over $f(x)$ such that $x \in C_x$, and write F_x for the reduced scheme underlying C_x. Then F_0 is an Abelian subvariety of X and $F_x = t_x(F_0) = x + F_0$ for all $x \in X(k)$.

Proof. Consider the morphism $\varphi : X \times F_x \to Y$ which is the composite

$$X \times F_x \to X \times X \xrightarrow{m} X \xrightarrow{f} Y$$

Clearly $\varphi(\{0\} \times F_x) = \{f(x)\}$. Since F_x is connected and complete, the Rigidity Theorem implies that φ maps the fibres $\{z\} \times F_x$ to a point. Therefore, $f(z + x) = f(z + F_x)$ for any $x' \in C_x$. In particular, let $z = y - x$ we find that $f(y - x + F_x) = f(y)$ for any $x, y \in X(k)$.

Putting $y = z,\ x = 0$ we obtain $f(z + F_0) = f(z)$, which implies that $z + F_0 \subseteq F_z$. Putting $y = 0,\ x = z$ we obtain that $-z + F_z \subseteq F_0$. This shows that $F_z = z + F_0$.

In particular, we have $a + F_0 = F_a = F_0$ for any $a \in F_0$. Therefore, F_0 is a reduced subgroup scheme in X, and then is a Abelian subvariety. ■

Corollary 2.21. Suppose that X is a simple Abelian variety, then every morphism from X to another k-variety is either constant or finite.

Remark 2.22. *Let D be an effective divisor of X, that is, all the coefficients of D are positive. Let $L = \mathcal{O}_X(D)$ be the corresponding line bundle. We claim that linear system $|2D|$ has no base-points, i.e., the sections of $L^{\otimes 2}$ define a morphism of X to projective space. To see this we have to show that for every geometric point $y \in X$ there exists an element $E \in |2D|$ that does not contain y. Now the theorem of square tells us that the divisors of the form*

$$t_x^* D + t_{-x}^* D$$

belong to $|2D|$.

For any given y, it is easily to see that we can find x such that $y \notin \operatorname{Supp}(t_x^* D + t_{-x}^* D)$. As a result, there is a morphism from from X to $\mathbb{P}(\Gamma(X, L^{\otimes 2}))$.

Also, note that we have a morphism

$$X \to \mathbb{P} = |2D|, \quad x \mapsto t_x^* D + t_{-x}^* D$$

Definition 2.23. Assume that k is algebraically closed. For an effective divisor D on X we define the reduced closed subscheme $H(D) \subseteq X$ by

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

Clearly, this is a subgroup scheme.

Lemma 2.24. Assume that k is algebraically closed. Let L be an effective line bundle on the Abelian variety X. Let $f : X \to \mathbb{P}^n$ be the map sending X to a projective space, as referred in the above remark. Let F_0 be the set defined in 2.20 corresponding to f. Then $H(D)^0 = F_0 = K(L)^0_{\mathrm{red}}$.

Proof. Let $x \in F_0$. Then $f \circ t_x = f$. Hence, if $s \in \Gamma(X, L^{\otimes 2})$, then s and $t_x^* s$ have the same divisor. Let t be a section of L with divisor D. This gives $t_x^* D = D$, i.e., $x \in H(D)$. Since F_0 is connected, we find that $F_0 \subseteq H(D)^0$.

Next, obviously, $H(D)^0 \subseteq K(L)^0_{\mathrm{red}}$.

To prove $K(L)^0_{\mathrm{red}} \subseteq F_0$, write L' for the restriction of L to $K(L)^0_{\mathrm{red}}$. We have to show that f sends $x \in K(L)^0_{\mathrm{red}}$ to $f(0)$. It is sufficient to show that L' is trivial. This is trivial, since we find that L is ample. As illustrated in the proof of 2.19, $(-1)^* L' \otimes L'$ is a trivial line bundle. But, L' and $(-1)^* L'$ both have nontrivial global elements, then L' is trivial. ∎

Remark 2.25. *In the next section, we will prove that there exists a quotient $X' = X/F_0$, which is again an Abelian variety. The Stein factorisation of the morphism f is given by $X \twoheadrightarrow X' \hookrightarrow \mathbb{P}^n$, and L is a pull-back of a bundle on X'.*

Proposition 2.26. Let L be a line bundle on an Abelian variety X which has a non-zero global section. If $K(L)$ is a group scheme then L is ample.

Proof. We assume that $k = \bar{k}$. Let D be the divisor corresponding to the given section.

Recall that F_0 is an Abelian variety, it consists of a single point.

Then 2.24 tells us that f is quasi-finite. Since f is also proper, it is finite. By general theory, L is ample. ∎

Corollary 2.27. Let D be an effective divisor on an Abelian variety X over an algebraically closed field. Set $L = \mathcal{O}_X(D)$. Then the following are equivalent:

1. $H(D)$ is finite;
2. $K(L)$ is finite;
3. L is ample.

Definition 2.28. A line bundle L is said to be non-degenerate if $K(L)$ is finite.

An effective line bundle is non-degenerate if and only if it is ample.

Theorem 2.29. An Abelian variety is a projective variety.

Proof. We first prove for the case $k = \bar{k}$. Choose a quasi-affine open subset $U \subsetneq X$ such that $X \backslash U = \bigcup_{i \in I} D_i$ for certain prime divisors D_i. Set $D = \sum D_i$. It suffices to find D such that $H(D)$ is finite. We find D such that $0 \in U$. Then it is easy to find that $H(D) \subseteq U$ through the definition of $H(D)$. But $H(D)$ is proper, then $H(D)$ is finite.

For arbitrary k, we first choose an ample divisor $D \subseteq X_{\bar{k}}$. Note that locally D represents a free module of rank 1 with glueing data in $\bar{k}^*$, we can expand k by creating these number to obtain a line bundle defined on a finite extension K/k, which induces D. If K/k is Galois, then we can construct

$$\tilde{D} = \sum_{\sigma \mathrm{Gal}(K/k)} {}^{\sigma} D$$

This is an ample divisor defined over k. If K/k is purely inseparable such that $\alpha^{p^m} \in k$ for all $\alpha \in K$, then $p^m \cdot D$ is an ample divisor defined over X. ∎

2.3 Projective embeddings of Abelian varieties

Theorem 2.30. No Abelian variety of dimension g can be embedded into $\mathbb{P}^{2g-1}$. No Abelian variety of dimension $g \geq 3$ can be embedded into $\mathbb{P}^{2g}$.

Proof. ∎

3 Basic theory of group schemes

3.1 Definitions and examples

Proposition 3.1. Let G be a scheme over a base scheme S. Then the following data are equivalent:

(i) the structure of an S-group scheme on G

(ii) a group structure on the sets $G(T) = \mathrm{Hom}_S(T, G)$, functorial in $T \in \mathbf{Sch}_{/S}$.

For homomorphisms we have a similar assertion: if G_1 and G_2 are S-group schemes then the following data are equivalent:

(i) a homomorphism of S-group schemes $f : G_1 \to G_2$

(ii) group homomorphisms $f(T) : G_1(T) \to G_2(T)$, functorial in $T \in \mathbf{Sch}_{/S}$.

Example 2. (1) Let S be a base scheme, the additive group over S, denoted by $\mathbb{G}_{a,S}$, corresponds to the functor $T \mapsto \Gamma(T, \mathcal{O}_T) : \mathbf{Sch}_{/S} \to \mathbf{Set}$.

$\mathbb{G}_{a,S}$ can be represented by the scheme $\mathrm{Spec}(R[x])$.

(2) The multiplicative group, denoted by $\mathbb{G}_{m,S}$, corresponds to the functor $T \mapsto \Gamma(T, \mathcal{O}_T)^* : \mathbf{Sch}_{/S} \to \mathbf{Set}$.

As a scheme, $\mathbb{G}_m = \mathrm{Spec}(\mathcal{O}_S[x, x^{-1}])$.

(3) The nth roots of unity $\mu_{n,S}$ corresponds to the functor

$$T \mapsto \{\text{the elements in } \Gamma(T, \mathcal{O}_T)^* \text{ whose order divides } n\}$$

The group scheme can be represented as $\mathcal{O}_S[x, x^{-1}]/(x^n - 1)$, it is a closed subgroup scheme of $\mathbb{G}_{m,S}$.

(4) Suppose that char $(S) = p$, where p is a prime number. Consider the closed subscheme $\alpha_{p^n,S} \subseteq \mathbb{G}_{a,S}$ defined by the ideal (x^{p^n}), that is, $\alpha_{p^n,S} = \mathrm{Spec}(\mathcal{O}_S[x]/(x^{p^n}))$.

If T is a S-scheme, $\alpha_{p^n,S}$ sends T to $\{f \in \Gamma(T, \mathcal{O}_T) | f^{p^n} = 0\}$.

(5) Let M be a group. Let $M_S = \bigoplus_M S$, it has a group structure induced by the group structure on M. As a functor, let $M_S(T)$ be the set of locally constant functions from $|T|$ to M.

(6) (semi-direct product) Let N and Q be two group schemes over a base scheme S. Consider the functor

$$\underline{\mathrm{Aut}}(N) : \mathbf{Sch}_{/S} \to \mathbf{Gr}, \quad T \mapsto \mathrm{Aut}_T(N_T(= N \times_S T))$$

Suppose that we are given a homomorphism of group functors $\rho : Q \to \underline{\mathrm{Aut}}(N)$, then we may define the semi-direct group scheme $N \rtimes_\rho Q$: the underlying scheme is just $N \times_S Q$, the group structure is defined by

$$(n, q) \cdot (n', q') = (n \cdot \rho(g)(n'), q \cdot q')$$

(7) Let $S = \mathrm{Spec}(R)$ be an affine base scheme. Suppose that $G = \mathrm{Spec}(A)$ is an S-group scheme which is affine as a scheme. Then the morphism m, i and e giving G its structure of a group scheme correspond to R-linear homomorphisms

$$\tilde{m} : A \to A \otimes A$$

$$\tilde{i} : A \to A$$

$$\tilde{e} : A \to R$$

with a number of identifies induced by the definition of group schemes.

A unitary R-algebra equipped with maps $\tilde{m}, \tilde{e}$ and $\tilde{i}$ satisfying these identifies is called a Hopf algebra over R. The category of affine group schemes over R is anti-equivalent to the category of commutative R-Hopf algebras.

3.2 Elementary properties of group schemes

Proposition 3.2. (1) An S-group scheme G is separated if and only if the unit section $e : S \to G$ is a closed immersion.

(2) If S is a discrete scheme then every S-group scheme is separated.

Corollary 3.3. Every group scheme over a field k is separate.

Definition 3.4. (1) Let G be an S-group scheme with unit section $e : S \to G$. Define $e_G = e(S) \subseteq G$ (a subscheme of G) to be the image of immersion e.

(2) Let $f : G \to G'$ be a homomorphism of S-group schemes. Then we define the kernel of f to be the subgroup scheme $\mathrm{Ker}(f) = f^{-1}(e_{G'})$ of G.

Definition 3.5. Let G be a group scheme over a field k, it is separated over k. The subscheme e_G is a single point.

Assume that G is locally of finite type over k, then the scheme G is locally Noetherian, hence locally connected. Let G^0 be the connected component of e_G, it is an open subscheme of G. We call G^0 the identity component of G.

Proposition 3.6. Let G be a group scheme, locally of finite type over a field k.

(1) The identity component G^0 is an open and closed subgroup scheme of G which is geometrically irreducible.

(2) The following properties are equivalent:

- $G \otimes_k K$ is reduced for some perfect field $K \supseteq k$.
- the ring $\mathcal{O}_{G,e} \otimes_k K$ is reduced for some perfect field $K \supseteq k$.

- G is smooth over k.
- G^0 is smooth over k.
- G is smooth over k at the origin.

(3) Every connected component of G is irreducible and of finite type over k.

Proof. (1) If G^0 is geometrically connected and (3) holds true, then G^0 is obviously geometrically irreducible. We may show that G^0 is geometrically connected in the following. More generally, we shall prove that if X is a connected k-scheme, locally of finite type, that has a k-rational point $x \in X(k) = \mathrm{Hom}(k, X)$ then X is geometrically connected.

Let $\bar{k}$ be an algebraic closure of k. First we show that the projection $p : X_{\bar{k}} = X \times_k \bar{k} \to X$ is open and closed. Suppose that $\{V_\alpha\}$ is an open covering of X, then $\{V_{\alpha,\bar{k}}\}$ covers $X_{\bar{k}}$. Then the projection $X_{\bar{k}} \to X$ is open (resp. closed) if each $V_{\alpha,\bar{k}} \to V_\alpha$ is open (resp. closed). Hence we may assume that $X = \mathrm{Spec}(A)$ is affine and of finite type over k. Then the result follows immediately.

Suppose that nonempty subsets U_1 and U_2 are both open and closed in $X_{\bar{k}}$. Since X is connected, $p(U_1) = p(U_2) = X$. The unique point $\bar{x}$ lying over $x \in \mathrm{Hom}(k, X)$ is then contained in $U_1 \cap U_2$. Hence $U_1 \cap U_2$ is nonempty and then $X_{\bar{k}}$ is connected.

(2) For a scheme X of finite type over k, we have the following properties (see Illusie theorem 3.7): If X is smooth, then X is regular, hence is reduced (because any regular local ring is a domain); if k is perfect and X is regular, then X/k is smooth. For the second property, there is a more suitable version at this case : https://stacks.math.columbia.edu/tag/056V.

(3) ■

Theorem 3.7 (Catier theorem)**.** Let G be a group scheme, locally of finite type over a field k of characteristic 0. Then G is reduced and smooth over k. (By the above proposition if G is reduced then G is smooth).

Proof. ■

3.3 Cartier duality

Definition 3.8. Let G be a commutative and finite local free over S. Let $A = \pi_*\mathcal{O}_G$. It is a finite locally free sheaf as Hopf $\mathcal{O}_S$-algebra. We define a new sheaf $A^D = \mathrm{Hom}_{\mathcal{O}_S}(A, \mathcal{O}_S)$ with a natural Hopf $\mathcal{O}_S$-algebra structure.

Theorem 3.9 (Catier duality)**.** Let $G : G \to S$ be a commutative S-group scheme which is finite and locally free over S. Write $A = \pi_*\mathcal{O}_G$. Then $G^D = \mathrm{Spec}(A^D)$ is a commutative, finite locallt free S-group scheme which represents the contravariant functor

$$\mathrm{Hom}(G, \mathbb{G}_{m,S}) : \mathbf{Sch}_{/S} \to \mathbf{Gr} \quad T \mapsto \mathrm{Hom}_{\mathbf{GSch}_{/T}}(G_T, \mathbb{G}_{m,T})$$

The homomorphism $G^{DD} \to G$ is an isomorphism.

3.4 The component group of a group scheme

Remark 3.10. *We use $\pi_0(X)$ to represent the topological connected components of X, and $\omega_0(X)$ for its scheme-theoretic analogue.*

Definition 3.11. If X/k is a scheme locally of finite type then $\omega_0(X)$ will be an etale k-scheme, and $X \mapsto \omega_0(X)$ is a covariant functor. Further, if X is a group scheme, then $\omega_0(G)$ inherits a natural structure of group scheme, which is called the component group scheme of G.

Definition 3.12. Let k be a field with a separable algebraic closure k_s and write $\Gamma_k = \mathrm{Gal}(k_s/k)$. By a Γ_k-set we mean a set Y equipped with a continuous left action of Γ_k, the continuity assumption here means that all Γ_k-orbits in Y are finite.

Remark 3.13. *Let $S = \mathrm{Spec}(k)$ for a field k. Let $\boldsymbol{Et}_{/S}$ be the categories of etale schemes over S. Note that every etale scheme X over S can be represented as the union of connected etale schemes $X = \coprod_{\alpha \in I} \mathrm{Spec}(L_\alpha)$ where L_α is a finite separable extension of k. Then there is an equivalence of categories*

$$\boldsymbol{Et}_{/k} \xrightarrow{\text{eq}} (\Gamma_k\text{-}sets)$$

associating to $X \in \boldsymbol{Et}_{/k}$ the $X(k_s)$ with its natural Γ_k-action. To obtain a quasi-inverse, write a Γ_k-set Y as a union of orbits, say $Y = \coprod_{\alpha \in I}(\Gamma_k \cdot y_\alpha)$, let $L_\alpha \supseteq k$ be the finite extension corresponding to the open subgroup $\mathrm{stab}(y_\alpha) \subseteq \Gamma_\alpha$, and associate to Y the S-scheme $\coprod_{\alpha \in I} \mathrm{Spec}(L_\alpha)$.

Proposition 3.14. Let $k \subseteq k_s$ and $\Gamma_k = \mathrm{Gal}(k_s/k)$ be as above. Associating to an etale k-group scheme G the group scheme $G(k_s)$ with its natural Γ_k-action gives an equivalence of categories

$$(\text{etale } k\text{-group schemes}) \xrightarrow{\text{eq}} (\Gamma_k\text{-groups})$$

Remark 3.15. *The proposition tells us that every etale k-group scheme G is a k-form of a constant group scheme.*

In other words, let $M = G(k_s)$. We consider it as an abstract group. Then the constant group scheme M_k/k. The proposition tells us that $M_k \otimes k_s \cong G_{k_s}$.

Proposition 3.16. Let X be a scheme, locally of finite type over a field k. Then there is an etale k-scheme $\omega_0(X)$ and a morphism $q : X \to \omega_0(X)$ over k such that q is universal for k-morphisms from X to an etale k-scheme. The morphism q is faithfully flat, and its fibres are precisely the connected components of X.

Proof. Looks easy to understand, but the proof needs to be created. ∎

Proposition 3.17. Let G be a group scheme, locally of finite type over a field k. In this case, q is a homomorphism.

4 Quotients by group schemes

We only list the results in this section.

4.1 Categorical quotients

Definition 4.1. (1) Let G be a group scheme over a basis S. A left action of G on an S-scheme X is given by a morphism $\rho : G \times_S X \to X$ such that the composition

$$X \xrightarrow{\sim} S \times_S X \xrightarrow{e_G \times id_X} G \times_S X \xrightarrow{\rho} X$$

is the identify on X, and such that the diagram

$$\begin{tikzcd} G \times_S G \times_S X \arrow[r, "id_G \times \rho"] \arrow[d, "m \times id_X"'] & G \times_S X \arrow[d, "\rho"] \\ G \times_S X \arrow[r, "\rho"] & X \end{tikzcd}$$

is commutative. Note that ρ induces a left action of $G(T)$ on $X(T)$.

(2) Given an action ρ as in (1), we define the graph morphism to be $\Psi = \Psi_\rho : G \times_S X \to X \times_S X$ sending $(g, x) \mapsto (g \cdot x, x)$. The action ρ is said to be free, or set-theoretically free if Ψ is a monomorphism of schemes, and is said to be strictly free, or scheme-theoretically free, if Ψ is an immersion.

(3) If T is an S-scheme and $x \in X(T)$ then the stabilizer of x, denoted by G_x, is the subgroup scheme of G_T that represents the functor $T' \mapsto \{g \in G(T') | g \cdot x = x\}$ on T-scheme T'.

Proposition 4.2. An action ρ is free means that for all T and all $x \in X(T)$ the stabilizer G_x is trivial.

Example 3. Let G be a group scheme over S and $H \subseteq G$ is a subgroup scheme then the group law gives an action of H on G. One can check that the action is strictly free.

More generally, if $f : G \to G'$ is a homomorphism of group schemes then we get a natural action of G on G'. The action is free if and only if $\mathrm{Ker}(f)$ is trivial.

Definition 4.3 (categorical case)**.** Let C be a category with finite products. Let G be a group object in C. Let X be an object of C.

(a) A left action of G on X is a morphism $\rho : G \times X \to X$ that induces, for every object T, a left action of the group $G(T)$ on the set $X(T)$.

(b) Let an action of G on X be given. A morphism $q : X \to Y$ in C is said to be G-invariant if $q \circ \rho = q \circ pr_X : G \times X \to Y$. By the Yoneda lemma this is equivalent to the requirement that for every $T \in C$, if $x_1, x_2 \in X(T)$ are two points in the same $G(T)$-orbit then $q(x_1) = q(x_2)$ in $Y(T)$.

(c) Let f, g be two morphisms from W to X in C. We say that a morphism $h : X \to Y$ is a difference cokernel of the pair (f, g) if $h \circ f = h \circ g$ and if h is universal for this property.

(4) Let $\rho : G \times X \to X$ be a leaf action. A morphism $q : X \to Y$ is called a categorical quotient of X by G if q is a difference cokernel for the pair $(\rho, pr_X) : G \times X \rightrightarrows X$. In other words, q is G-invariant, and every G-invariant $X \to Y'$ factors through q.

Remark 4.4. *To study $q : X \to Y$, we can take Y to be our base scheme. Indeed, if q is a categorical quotient of X by G, then $G_Y = G \times_S Y$ acts on X and q is also a categorical quotient of X by G_Y in the category $\boldsymbol{Sch}_{/Y}$. The action of G on X over S is (strictly) free if and only if the action of G_Y on X over Y is (strictly) free.*

4.2 Geometric quotients, and quotients by finite group schemes

Proposition 4.5 (When Γ is finite and X is affine)**.** Let Γ be a finite group acting on an affine scheme $X = \operatorname{Spec}(A)$. Let $B = A^\Gamma \subseteq A$ be the subring of Γ-invariant elements, and set $Y = \operatorname{Spec}(B)$.

(1) The natural morphism $q : X \to Y$ induces a homeomorphism $\Gamma\backslash|X| \xrightarrow{\sim} Y$.

(2) The map $q^\sharp : \mathcal{O}_Y \to q_*\mathcal{O}_X$ induces an isomorphism $\mathcal{O}_Y \xrightarrow{\sim} (q_*\mathcal{O}_X)^\Gamma$.

(3) The ring A is integral over B; the morphism $q : X \to Y$ is quasi-finite, closed and surjective.

Definition 4.6. Let $\rho : G \times_S X \to X$ be an action of an S-group scheme G on an S-scheme X. Consider the continuous

$$|pr_X| : |G \times_S X| \to |X|, \quad |\rho| : |G \times_S X| \to |X|$$

Given $P, Q \in |X|$, write $P \sim Q$ if there a point $R \in |G \times_S X|$ with $|pr_X|(R) = P$ and $|\rho|(R) = Q$. Then $\sim$ is an equivalence relation on $|X|$.

Let $|X|/\sim$ be the set of G-equivalence classes in $|X|$, equipped with the quotient topology. Write $q : |X| \to |X|/\sim$ for the canonical map. Let V be an open subset of $|X|/\sim$ and U its preimage. If $f \in q_*\mathcal{O}_X(V) = \mathcal{O}_X(U)$, then we form the elements $pr_X^\sharp(f)$ and $\rho^\sharp(f)$ in $\mathcal{O}_{G\times_S X}(G\times_S U)$. We say that f is G-invariant if $pr_X^\sharp(f) = \rho^\sharp(f)$. The G-invariant functions f form a subsheaf of rings $(q_*\mathcal{O}_X)^G \subseteq q_X\mathcal{O}_X$ on $|X|/\sim$. We define

$$(G\backslash X)_{\mathrm{rs}} = (|X|/\sim, (q_*\mathcal{O}_X)^G)$$

and write $q : X \to (G\backslash X)_{\mathrm{rs}}$ for the natural morphism of ringed spaces.

If $(G/x)_{\mathrm{rs}}$ is a scheme and q is a morphism of schemes then we say that it is a geometric quotient of X by G. If moreover for every S-scheme T we have that $(G\backslash X)_{\mathrm{rs}} \times_S T \cong (G_T\backslash X_T)_{\mathrm{rs}}$ then we say that $(G\backslash X)_{\mathrm{rs}}$ is a universal geometric quotient.

Proposition 4.7. In the category $\mathbf{RS}_{\backslash S}$, q is a difference cokernel of the pair $(\rho, pr_X) : G\times_S X \rightrightarrows X$. Consequently, if a geometric quotient of X by G exists, that is, $(G\backslash X)_{\mathrm{rs}}$ is a scheme and q us a morphism of schemes, then q is a categorical quotient in $\mathbf{Sch}_{\mathrm{rs}}$.

Lemma 4.8.

Theorem 4.9 (Quotients by finite group schemes)**.** Let G be a finite locally free S-group scheme acting on an S-scheme X. Assume that for every closed point $P \in |X|$ the G-equivalence class of P is contained in an affine open set.

(1) The quotient $Y = (G\backslash X)_{\mathrm{rs}}$ is an S-scheme, which therefore is a geometric quotient of X by G. The canonical morphism $q : X \to Y$ is quasi-finite, integral, closed and surjective. If S is locally Noetherian and X is of finite type over S then q is a finite morphism and Y is of finite type over S, too.

(2) The formation of the quotient is compatible with flat base change. In other words, let $h : S' \to S$ be a flat morphism, then $Y \times_S S' = (G \times_S S'\backslash X \times_S S')_{\mathrm{rs}}$.

(3) If G acts freely then $q : X \to Y$ is finite locally free and the morphism

$$G \times_S X \to X \times_Y X$$

induced by $\Psi = (\rho, pr_X)$ is an isomorphism. Moreover, in this case Y is a universal geometric quotient.

4.3 FPPF quotients

Definition 4.10. Let S be a scheme. We write $(S)_{\mathrm{FPPF}}$ for the big fppf site of S. Write FPPF(S) for the category of sheaves on $(S)_{\mathrm{FPPF}}$. Denote by $\mathbf{ShGr}_{/\mathrm{S}}$ and $\mathbf{ShAb}_{/\mathrm{S}}$ the categories of sheaves of groups, respectively sheaves of Abelian groups, on $(S)_{\mathrm{FPPF}}$. The category $\mathbf{ShAb}_{/\mathrm{S}}$ is Abelian but the other is not.

Definition 4.11. Let G be an S-group scheme acting, by $\rho : G \times_S X \to X$, on an S-scheme X. We write $(G\backslash X)_{\mathrm{fppf}}$, or simply $G\backslash X$, for the fppf sheaf associated to the sheaf

$$T \mapsto G(T)\backslash X(T)$$

If $G\backslash X$ is representable by a scheme Y then we refer to Y as the fppf quotient of X by G.

Proposition 4.12. Let G be an S-group scheme acting freely on an S-scheme X. Suppose that the fppf sheaf $(G\backslash X)_{\mathrm{fppf}}$ is representable by a scheme Y. Write $q : X \to Y$ for the canonical morphism. Then q is an fppf covering and the morphism $\Psi : G \times_S X \to X \times_Y X$ is an isomorphism. This gives a commutative diagram with cartesian squares

$$\begin{tikzcd}
G \times_S X \arrow[r, "\sim"] \arrow[d, "pr_2"'] & X \times_Y X \arrow[r, "pr_1"] \arrow[d, "pr_2"] & X \arrow[d, "q"] \\
X \arrow[r, equal] & X \arrow[r, "q"] & Y
\end{tikzcd}$$

Proof. By the construction of fppf quotient, the morphism $q : X \to Y$ is an epimorphism of fppf sheaves. Then q is an fppf covering. As functors, $G \times_S X \to X \times_Y X$ is an isomorphism, hence by Yoneda lemma, Ψ is an isomorphism. ■

Remark 4.13. *In the situation of the proposition above, if $(G\backslash X)_{\mathrm{fppf}}$ is representable by a scheme, then the action of G on X is strictly free. Indeed, $X \times_Y X$ is a subscheme of $X \times_S X$.*

Definition 4.14. We say a property P of morphisms f of schemes is fppf local on the target if the following two conditions hold:

- P is stable under base change.
- if the base change $g : S' \to S$ is an fppf covering then $P(f) \iff P(f')$, where f' is the base change of f.

Proposition 4.15. Let P be a property of morphisms of schemes which is local on the target for the fppf topology. If $q : X \to Y$ is an fppf quotient of X under the free action of an S-group scheme G, then

$q : X \to Y$ has the property $P \Leftrightarrow pr_2 : G \times_S X \to X$ has the property $P \Leftarrow \pi : G \to S$ has the property P

where moreover the last implication is an equivalence if $X \to S$ is an fppf covering.

Theorem 4.16 (Raynaud)**.** Let G be an S-scheme acting on an S-scheme X.

(1) Suppose that there exists an fppf quotient Y of X by G. Then Y is also a geometric point of X in the category of ringed spaces.

(2) Assume that X is locally of finite type over S, and that G is flat and locally of finite presentation over S. Assume further that the action of G on X is strictly free. If there exists a geometric quotient Y of X by G then Y is also an fppf quotient. Thus, the quotient morphism $q : X \to Y$ in the category of ringed space is an fppf morphism and Y is a universal geometric quotient.

We have the following relations:

$$\begin{tikzcd}
\text{fppf quotient} \arrow[r, Rightarrow] & \text{universal geometric quotient} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \text{universal categorical quotient} \arrow[d, Rightarrow] \\
& \text{geometric quotient} \arrow[r, Rightarrow] \arrow[ul, "\text{under the assumption of (2)}"] & \text{categorical quotient}
\end{tikzcd}$$

Theorem 4.17. Let G be a proper and flat group scheme of finite type over a locally Noetherian basis S. Let $G \times_S X \to X$ define a strictly free action of G on a quasi-projective S-scheme X. Then the fppf quotient $G\backslash X$ is representable by a scheme.

Theorem 4.18. Let G be a flat group scheme of finite type over a locally Noetherian base scheme S. Let $H \subseteq G$ be a closed subgroup scheme which is flat over S. Suppose that we are in one of the following cases:

1. $\dim(S) \leq 1$.
2. G is quasi-projective over S and H is proper over S.
3. H is finite locally free over S such that every fibre $H_s \subseteq G_s$ is contained in an affine open subset of G.

Then the fppf quotient sheaf G/H is representable by an S-scheme. If H is normal in G, then G/H has the group structure of an S-group scheme such that $q : G \to G/H$ is a homomorphism of group schemes.

Corollary 4.19. Let X be an Abelian variety over a field k. If $H \subseteq X$ is a closed subgroup scheme then there exists an fppf quotient $q : X \to Y = X/H$. Y is again an Abelian variety.

4.4 Finite group schemes over a field

Theorem 4.20. If k is a field then the category of commutative group schemes of finite type is an Abelian category.

Definition 4.21. Let G be a finite group scheme over a field k. We say that G is

- etale, if the structural morphism $G \to \operatorname{Spec}(k)$ is etale;
- local, if G is connected.

Next suppose that G is commutative, we say that G is

- etale-etale, if G and G^D are both etale;
- etale-local, if G is etale and G^D is local;
- local-etale, if G is local and G^D is etale;
- local-local, if G and G^D are both local.

(Note that G is obviously finite locally free over k).

Example 4. If char $(k) = 0$ then by Catier theorem every finite commutative k-group scheme is etale-etale.

If char $(k) = p > 0$, then

- $\mathbb{Z}/m\mathbb{Z}$ is etale-etale for $p \nmid m$;
- $\mathbb{Z}/p^n\mathbb{Z}$ is etale-local;
- μ_{p^n} is local-etale;
- α_{p^n} is local-local.

Lemma 4.22. Let G_1 and G_2 be finite group schemes over a field k, with G_1 etale and G_2 local. Then the only morphisms from G_1 to G_2 and from G_2 to G_1 are trivial ones.

Proof. The properties being local and etaleness are stable under base change. Hence we may assume that $k = \bar{k}$. Then $G_{2,\text{red}} \subseteq G_2$ is a connected etale subgroup scheme, hence $G_{2,\text{red}} \cong \operatorname{Spec}(k)$. Now note that any homomorphism $G_1 \to G_2$ factors through $G_{2,\text{red}}$. Similarly, any homomorphism $G_2 \to G_1$ factors through $G_1^0 \cong \operatorname{Spec}(k)$. ■

Proposition 4.23 (connected-etale sequence)**.** Let G be a finite group scheme over a field k. Then G is an extension of an etale k-group scheme $G_{\text{et}} \triangleq \omega_0(G)$ by the local group scheme G^0. Hence we have an exact sequence

$$1 \to G^0 \to G \to G_{\text{et}} \to 1$$

If k is perfect then this sequence splits.

Proof. The exactness of this sequence follows from 3.17.

Now we assume that k is perfect. Then $G_{\text{red}} \subseteq G$ is a closed subgroup scheme. From 3.6 we know that it is smooth. Obviously, it is quasi-finite, then is etale.

We claim that $G_{\text{red}} \hookrightarrow G \to G_{\text{et}}$ is an isomorphism. We assume that $k = \bar{k}$. Then G is a union of copies of G^0. Then the isomorphism is clear. ■

Lemma 4.24. Let S be a connected base scheme. If

$$0 \to G_1 \to G_2 \to G_3 \to 0$$

is an exact sequence of finite locally free S-group schemes then $\operatorname{rank}(G_2) = \operatorname{rank}(G_1) \cdot \operatorname{rank}(G_3)$.

Proposition 4.25. Let char $(k) = p > 0$. Let G be a finite connected k-group scheme. Then the rank of G is a power of p.

Proof. ■

Corollary 4.26. A finite commutative k-group scheme is etale-etale if and only if $p \nmid \text{rank}(G)$.

5 Isogenies

5.1 Definition of an isogeny, and basic properties

We first use two lemmas from algebraic geometry.

Lemma 5.1. (1) Let X and Y be irreducible Noetherian schemes which are both regular and with $\dim(X) = \dim(Y)$. Let $f : X \to Y$ be a quasi-finite morphism. Then f is flat.

(2) Let $f : X \to Y$ be a morphism of finite type between Noetherian schemes, with Y reduced and irreducible. Then there is a non-empty open subset $U \subseteq Y$ such that either $f^{-1}(U) = \varnothing$ or $f : f^{-1}(U) \to U$ is flat.

Proposition 5.2. Let $f : X \to Y$ be a homomorphism of Abelian varieties. Then the following conditions are equivalent:

1. f is surjective and $\dim(X) = \dim(Y)$;
2. $\text{Ker}(f)$ is a finite group scheme and $\dim(X) = \dim(Y)$;
3. f is a finite, flat and surjective morphism.

Remark 5.3. *Note that Y is the FPPF quotient of* $\text{Ker}(f) \to X$. *Thus, if f is a surjective homomorphism between Abelian varieties, then it is flat.*

Definition 5.4. A homomorphism of Abelian varieties is called an isogeny if f satisfies the equivalent conditions in the above proposition. Since it is surjective of varieties, we may define the degree of an isogeny is the degree of the induced function fields extension.

Proposition 5.5. If $f : X \to Y$ is an isogeny then f induces an isomorphism $X/\text{Ker}(f) \xrightarrow{\sim} Y$.

Theorem 5.6. For a morphism of schemes $f : X \to Y$, the following conditions are equivalent:

- f is universally injective, that is, every base change of f is injective.
- f is injective and for every $x \in X$ the residue field $k(x)$ is a purely inseparable extension of $k(f(x))$.
- for every field K, the map $X(K) \to Y(K)$ induced by f is injective.

A morphism satisfies these conditions is called a purely inseparable morphism.

Proof. This proof follows from https://stacks.math.columbia.edu/tag/01S4.

1. $\Rightarrow$ 3.: Note that $X(K)$ can be identified as the set of pairs (x, ϕ) where $x \in X$ and ϕ is an inclusion $k(x) \hookrightarrow K$. The natural map $X(K) \to Y(K)$ sends (x, ϕ) to $(f(x), f^* \circ \phi)$. This is obviously injective.

3. $\Rightarrow$ 1.: For any base change $S' \to S$, suppose that $x_1, x_2 \in X \times_S S'$ map to the same point $s' \in S'$. Choose a field K with two inclusions $k(x_1) \hookrightarrow K$ and $k(x_2) \hookrightarrow K$ which induce the same inclusion $k(s') \hookrightarrow K$, then these define two morphisms $\mathrm{Spec}(K) \to X_{S'}$ and induce the same morphism $\mathrm{Spec}(K) \to S'$. Note that the composite $\mathrm{Spec}(K) \to S' \to S$ can also induced by the composite $\mathrm{Spec}(K) \to X_{S'} \to X \to S$. Thus the composites of the two morphisms $\mathrm{Spec}(K) \to X_{S'}$ with $X_{S'} \to X$ are equal. Therefore, $x_1 = x_2$.

1. + 3. $\Rightarrow$ 2.: If there is a point $x \in X$ such that $k(x)$ is not a purely inseparable extension of $k(f(x))$, we may find a field extension $K/k(f(x))$ such that $k(x)$ has two $k(f(x))$-homomorphisms into K. Then the map $X(K) \to Y(K)$ is not injective, a contradiction.

2. $\Rightarrow$ 3.: This is obvious from that f is injective. ■

Theorem 5.7. Let $f : X \to Y$ be an isogeny.

(1) The following conditions are equivalent:

- The function field $k(X)$ is a separable field extension of $k(Y)$.
- f is an etale morphism.
- $\mathrm{Ker}(f)$ is an etale group scheme.

(2) The following conditions are equivalent:

- The function field $k(X)$ is a purely inseparable field extension of $k(Y)$.
- f is a purely inseparable morphism.
- $\mathrm{Ker}(f)$ is a connected group scheme.

Proof. (1) Y is the etale quotient of $\mathrm{Ker}(f) \to X$. Thus (b) and (c) are equivalent.

Recall that being etale induces that finite separable extensions between corresponding residue fields. Applying this with the generic point X we see that (b) implies (a).

Now we assume that (a) holds true. Recall that a morphism between irreducible schemes sends the generic point to the generic point if and only if the morphism is dominant $(f(\bar{\eta}) \subseteq \overline{f(\eta)})$, f then actually sends the generic point of X to the generic point of Y. Thus the assumption in (a) means that f is unramified at the generic point of X.

To show that f is etale, it suffices to show that f is unramified everywhere, that is, $(\Omega_{X/Y})_x = 0$ for $x \in X$. Since $\Omega_{X/Y}$ is a coherent sheaf, the support of it is a closed subset. Then there is an open subset of X, which contains the generic point of X, $\Omega_{X/Y}$ is 0 on it. Thus, there is a non-empty open subset of X such that the restriction of f is etale. Therefore f is etale everywhere.

(2) The case that (b) implies (a) is obvious.

If (a) holds true, note that f can be factored as $X \to X/(\mathrm{Ker}(f))^0 \to Y$, where $\mathrm{Ker}(f)^0 \subseteq \mathrm{Ker}(f)$ is the connected component of e_X. The kernel of the second isogeny is $\mathrm{Ker}(f)/\mathrm{Ker}(f)^0$, this is etale. By (1) we can find that $\mathrm{Ker}(f)$ is connected.

Finally suppose that $N = \mathrm{Ker}(f)$ is a connected group scheme, choose an affine subscheme $\mathrm{Spec}(A)$. To show that f is purely inseparable, we show that for every K, $X(K) \to Y(K)$ is injective. If $y : \mathrm{Spec}(K) \to Y$ is a K-valued point, then $f^{-1}(y) \supseteq \mathrm{Spec}(A_K)$. Obviously A_K is Artinian local. Then $f^{-1}(y)$ consists of a single point. Then f is purely inseparable. ∎

Proposition 5.8. Every isogeny can be factorized as a composite of an inseparable isogeny and a separable isogeny.

Corollary 5.9. For $n \neq 0$, the morphism $[n]_X$ is an isogeny. If $g = \dim(X)$, we have $\deg([n]_X) = n^{2g}$. If (char $(k), n) = 1$, then $[n]_X$ is separable.

Proof. Choose an ample and symmetric line bundle L on X, then we have $[n]_X^* L \cong L^{\otimes n^2}$. The restriction of $[n]_X^* L$ to $\mathrm{Ker}([n]_X)$ is a trivial bundle which is ample. Since X is projective, this implies that $\mathrm{Ker}([n]_X)$ is finite. Hence $[n]_X$ is an isogeny. ∎

Corollary 5.10. If X is an Abelian variety over an algebraically closed field k then $X(k)$ is a divisible group. That is, for every $P \in X(k)$ and $n \in \mathbb{Z}\backslash\{0\}$ there exists a point $Q \in X(k)$ with $n \cdot Q = P$.

Corollary 5.11. If (char $(k), n) = 1$, then $X(n)(k_s) = X(n)(\bar{k}) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.

Proposition 5.12. If $f : X \to Y$ is an isogeny of degree d then there exists an isogeny $g : Y \to X$ with $g \circ f = [d]_X$ and $f \circ g = [d]_Y$.

5.2 Frobenius and Verschiebung

Proposition 5.13. Let X be a g-dimensional Abelian variety over a field k with char $(k) = p > 0$. Then the relative Frobenius homomorphism $F_{X/k}$ is a purely inseparable isogeny of degree p^g.

Proof. Recall that there is a composition

$$\mathrm{Frob}_X : X \xrightarrow{F_{X/k}} X^{(p)} \to X$$

Since Frob_X is the identity on the topological space $|X|$, the underlying space of $X[F] \triangleq \mathrm{Ker}(F_{X/k})$ only has one point $\{e\}$.

Now we consider an open affine neighborhood $U = \mathrm{Spec}(A)$ of $\{e\}$, where A has the form $k[x_1, \cdots, x_r]/(f_1, \cdots, f_n)$, as X is of finite type over k and every ideal of $k[x_1, \cdots, x_r]$ is finitely generated. Note that e corresponds to the maximal ideal $\mathfrak{m} = (x_1, \cdots, x_n) \subseteq A$. The restriction of $F_{X/k}$ to U, denoted by $F_{U/k}$ is then given by

$$A = k(x_1, \cdots, x_r)/(f_1, \cdots, f_n) \leftarrow A^{(p)} = k[x_1, \cdots, x_r]/(f_1^{(p)}, \cdots, f_n^{(p)})$$

sending x_i to x_i^p, where $f_i^{(p)}$ is obtained from f_i by raising the coefficients to their p-powers. Then $X[F]$ is exactly $\mathrm{Spec}(B)$, where $B = k[x_1, \cdots, x_r]/(x_1^p, \cdots, x_r^p, f_1, \cdots, f_n)$. Since B is finite over k, $X[F]$ is precisely a finite group scheme. Hence, $F_{X/k}$ is an isogeny.

Consider the $\mathfrak{m}$-adic completion of A, suppose that $x_1, \cdots, x_g$ form a basis of $\mathfrak{m}/\mathfrak{m}^2 = T^\vee_{X,e}$, then by the structure theory of complete regular local rings there is an isomorphism

$$\hat{A} \cong k[[t_1, \cdots, t_g]]$$

Then

$$B \cong k[t_1, \cdots, t_g]/(t_1^g, \cdots, t_g^p)$$

In particular, this shows that $\deg(F_{X/k}) = p^g$ and that $X[F]$ is a connected group scheme. ■

Remark 5.14. *Let R be a ring with* char $(p) = p > 0$. *Let A be an R-algebra. Write $T^p(A) = A \otimes_R A \otimes_R A \otimes_R \cdots \otimes_R A$ for the p-fold tensor product of A over R. The symmetric group $\mathfrak{S}_p$ on p letters naturally acts on $T^p(A)$. Write $S^p(A) \subseteq T^p(A)$ for the subalgebra of $\mathfrak{S}_p$-invariants.*

Let $N : T^p(A) \to S^p(A)$ be the map given by

$$N(a_1 \otimes \cdots \otimes a_p) = \sum_{\sigma \in \mathfrak{S}_p} a_{\sigma(1)} \otimes \cdots \otimes a_{\sigma(p)}$$

If $s \in S^p(A)$ is a symmetric tensor and $t \in T^p(A)$ then $N(st) = sN(t)$. It follows that $J = N(T^p(A))$ is an ideal of $S^p(A)$.

Write $U = \mathrm{Spec}(A) \to T = \mathrm{Spec}(R)$. The group $\mathfrak{S}_p$ acts naturally on $U^p_T = U \times_T U \times_T U \times \cdots \times_T U$ (p factors), and the quotient is given by $S^p(U) = \mathrm{Spec}(S^p(A))$. The scheme $S^p(U)$ is called the pth-symmetric power of U over T. Let $U^{[p/T]} \hookrightarrow S^p(U)$ be the closed subscheme defined by J.

Consider the map

$$U \xrightarrow{\Delta} U^p_T \to S^p(U)$$

which corresponds to

$$S^p(A) \to T^p(A) \xrightarrow{a_1 \otimes \cdots \otimes a_p \mapsto a_1 \cdots a_p} A$$

Note that the second map sends $N(a_1 \otimes \cdots \otimes a_p)$ to $p! \cdot a_1 \cdots a_p$, which is 0 since char $(A) = p$. *The map $S^p(A) \to A$ factors by $S^p(A)/J$, and then the morphism $U \to S^p(U)$ factors by $U^{[p/T]}$. We write*

$$F'_{U/T} : U \to U^{[p/T]}$$

for the morphism.

Write $A^{(p/R)}$ for the base change of A under Frob_R. *The relative Frobenius morphism is then given by $U \to U^{(p/T)} = \mathrm{Spec}(A^{(p/R)})$. Note that there is a canonical map*

$$\varphi_{A/R} : A^{(p/R)} \to S^p(A)/J$$

sending $a \otimes r$ to $ra \otimes a \otimes \cdots \otimes a \pmod{J}$. Write $\varphi_{U/T} : U^{[p/T]} \to U^{(p/T)}$ for the morphism of schemes induced by $\varphi_{A/R}$. Then we have $F_{U/T} = \varphi_{U/T} \circ F'_{U/T}$.

Definition 5.15. Consider a base scheme S of characteristic p and an S-morphism $X \to S$. Define $S^p(X)$, the pth symmetric power of X over S, to be the quotient X^p_S under the natural action of $\mathfrak{S}_p$. We can glue those $U^{[p/T]}$ for affine $U \subseteq X$ and $T \subseteq S$ to obtain a locally closed subscheme $X^{[p/S]} \hookrightarrow S^p(X)$. Also, there is a factorization of $F_{X/S}$

$$F_{X/S} = (X \xrightarrow{F'_{X/S}} X^{[p/S]} \xrightarrow{\varphi_{X/S}} X^{(p/S)})$$

By construction, the composition of $F'_{X/S}$ and the inclusion $X^{[p/S]} \hookrightarrow S^p(X)$ is the same as the diagonal $\Delta : X \to X_S^p$ and the natural projection $X_S^p \to S^p(X)$.

$$\begin{tikzcd}
X \arrow[r, "\Delta"] \arrow[d, "F'_{X/S}"'] & X_S^p \arrow[d, "\text{categorical quotient}"] \\
X^{[p/S]} \arrow[r, hook] \arrow[d, "\varphi_{X/S}"'] & S^p(X) \\
X^{(p/S)} &
\end{tikzcd}$$

Lemma 5.16. (1) The construction of $X^{[p/S]}$, as well as the formation of $F'_{X/S}$ and $\varphi_{X/S}$, is functorial in X and compatible with flat base change $T \to S$.

(2) If X is flat over S then $\varphi_{X/S}$ is an isomorphism.

Proposition 5.17. For a commutative S-group scheme G, there is a morphism $m^{(p)} : G_S^p \to G$ given by $(g_1, \cdots, g_p) \mapsto g_1 \cdots g_p$. By the universally property of categorical quotient, the morphism $m^{(p)}$ is $\mathfrak{S}$-invariant and then factors through $S^p(G)$, say via $\bar{m}^{(p)} : S^p(G) \to G$. Then $[p] : G \to G$ factors as $[p] = (G \xrightarrow{F'_{G/S}} X^{[p/S]} \hookrightarrow S^p(G) \xrightarrow{\bar{m}^{(p)}} G)$.

$$\begin{tikzcd}
G \arrow[r, "\Delta"] \arrow[d, "F'_{G/S}"'] & G_S^p \arrow[d, "\text{categorical quotient}"] \\
G^{[p/S]} \arrow[r, hook] \arrow[d, "\varphi_{G/S}"'] & S^p(G) \arrow[d, "\bar{m}^{(p)}"] \\
G^{(p/S)} & G
\end{tikzcd}$$

Definition 5.18. If G is a commutative flat group scheme over a basis S of characteristic p then we define the Verschiebung homomorphism

$$V_{G/S} : G^{(p/S)} \to G$$

to be the composition

$$G^{(p/S)} \xrightarrow{\varphi_{G/S}^{-1}} G^{[p/S]} \hookrightarrow S^p(G) \xrightarrow{\bar{m}^{(p)}} G$$

Proposition 5.19. Let S be a scheme with char $(S) = p > 0$. Let G be a flat S-group scheme.

(1) We have $V_{G/S} \circ F_{G/S} = [p]_G : G \to G$.

(2) If G is finite locally free over S then the Verschiebung is Cartier dual to the Frobenius homomorphism. More precisely, we have $(V_{G/S})^D = F_{G^D/S}$ and $V_{G/S} = (F_{G^D/S})^D$.

Corollary 5.20. Let X be an Abelian variety over a field k with char $(k) = p$. Then the Verschiebung homomorphism $V_{X/k} : X^{(p)} \to X$ is an isogeny of degree p^g. We have $V_{X/k} \circ F_{X/k} = [p]_X$ and $F_{X/k} \circ V_{X/k} = [p]_{X^{(p)}}$.

Remark 5.21. *We can also define the m-iterate of Verschiebung homomorphism like the Frobenius case. Write $F_{X/k}^m : X^{(p^m)} \to X$ for the "mth-power" of Frobenius, then*

$$V_{X/k}^m \circ F_{X/k}^m = [p^m]_X$$

Proposition 5.22. Suppose that char $(k) = p > 0$, there is an integer $f = f(X)$, with $0 \leq f \leq g = \dim(X)$, called the p-rank of X, such that $X[p^m](\bar{k}) \cong (\mathbb{Z}/p^m\mathbb{Z})^f$ for all m. If Y is isogenous to X then $f(Y) = f(X)$.

Proof. We can factor $p^m : X \to X$ as

$$[p^m]_X = (x \xrightarrow{F^m_{X/k}} X^{(p^m)} \xrightarrow{h_1} X' \xrightarrow{h_2} X)$$

where $h_1 \circ F^m_{X/k}$ is purely inseparable and h_2 is a separable isogeny. Recall that $\deg([p^m]_X) = (p^m)^{2g}$ and $\deg(F^m_{X/k}) = p^{mg}$, we have $\deg(h_2) = p^{d(m)}$ for some $0 \leq d(m) \leq gm$.

Let $f = d(1)$. Then $X[p](\bar{k}) \cong (\mathbb{Z}/p\mathbb{Z})^f$. By the exact sequence

$$0 \to X[p^{m-1}](\bar{k}) \to X[p^m](\bar{k}) \xrightarrow{p^{m-1}} X[p](\bar{k}) \to 0$$

we can obtain $X[p^m](\bar{k}) \cong (\mathbb{Z}/p^m\mathbb{Z})^f$. ■

5.3 Density of torsion points

Definition 5.23. Let $i_m : X[p^m] \hookrightarrow X$ be the inclusion homomorphism. We say that $\bigcup_m X[p^m]$ is scheme-theoretically dense in X, if there does not exist a proper closed subscheme $Y \subsetneq X$ such that all i_m factors through Y.

Remark 5.24. *If* char $(k) \neq p$, *we can express the scheme-theoretically dense as topological dense, i.e., the union of $X[p^m]$ is topological dense in X.*

However, if char $(k) = p$, *this is generally not true.*

Theorem 5.25. Let X be an Abelian variety over a field k and let p be a prime number. Then the collection of subschemes $X[p^m]$ is scheme-theoretically dense in X.

Proof. We proof for char $(k) \neq p$ and char $(k) = p$ separately.

First we assume that char $(k) \neq p$. It suffices to show for the case $k = \bar{k}$, since we only need to prove for the underlying topological space. Let $T = \bigcup_m X[p^m]$, and let Y be the smallest closed subscheme such that all i_m factors through Y. Note that Y is indeed the Zariski closure of T. We first prove that Y is a subgroup scheme.

Let $x \in T$, then the translation $t_x : X \to X$ maps T to itself. Because Y and $Y \times Y$ are reduced, $m(Y \times Y) \subseteq Y$. Further, it is clear that the inverse maps T to T. Thus, Y is a subgroup scheme.

Consider the identity component Y^0, it is a Abelian subvariety of X. Let $N = \#\omega_0(Y)$, $g = \dim(X)$ and $h = \dim(Y^0)$. First we have $\#Y^0[p^m](k) \leq p^{2mh}$, then $\#Y[p^m](k) \leq p^{2mh}N$. But we know that $\#Y[p^m](k) = p^{2mg}$. Taking m very large we find that $h = g$. Hence $Y^0 = X$.

Now let char $(k) = p$. Let F^m be the mth power of the Frobenius homomorphism and let $X[F^m]$ be its kernel. We know that $X[F^m] \subseteq X[p^m]$. So it suffices to show that $\bigcup_m X[F^m]$ is scheme-theoretically dense in X. We can prove it using commutative algebra.

Let Y be a closed subscheme such that all inclusions $X[F^m] \to X$ factors through Y. Choose an open affine neighborhood $U = \mathrm{Spec} A$ with $A = k[x_1, \cdots, x_r]/(f_1^{(p^m)}, \cdots, f_n^{(p^m)})$. Then we know that $X[F^m]$ is defined by the ideal $(x_1^{p^m}, \cdots, x_r^{p^m}, f_1, \cdots, f_n) \subseteq A$. Let J be the ideal of $Y \cap U$. Then $J\hat{A}$ is contained in $(x_1^{p^m}, \cdots, x_g^{p^m})$. Note that the intersection of all these ideals is 0 in $\hat{A}$. ■

Proposition 5.26. Let X be an Abelian variety over a field k. If $Y \to X$ is a closed subgroup scheme then the connected component $Y^0 \subseteq Y$ that contains the origin is an open and closed subgroup scheme of Y that is geometrically irreducible. The reduced underlying scheme $Y^0_{\mathrm{red}} \hookrightarrow X$ is an Abelian subvariety of X.

Proof. ■

6 The Picard scheme of an Abelian variety

6.1 Relative Picard functors

Definition 6.1. Let $P_{X/S} : (\mathbf{Sch}_{/S})^0 \to \mathbf{Ab}$ be the contravariant functor

$$P_{X/S} : T \mapsto \mathrm{Pic}(X_T) = H^1(X \times_S T, \mathbb{G}_m)$$

However, this is not representable.

The relative Picard functor $\mathrm{Pic}_{X/S} : (\mathbf{Sch}_{/S})^0 \to \mathbf{Ab}$ is defined to be the fppf sheaf associated to the presheaf $P_{X/S}$. An S-scheme representing $\mathrm{Pic}_{X/S}$ (if such a scheme exists) is called the relative Picard scheme X over S.

Remark 6.2. *We shall consider the following situation:*

$$(*) \qquad \begin{cases} \text{the stucture morphism } f : X \to S \text{ is qcqs.} \\ f_*(\mathcal{O}_{X \times_S T}) = \mathcal{O}_T \text{ for all } S\text{-schemes } T. \\ f \text{ has a section } s : S \to X \end{cases}$$

This holds, for instance, if $S = \mathrm{Spec}(k)$ and X is a complete k-variety with $X(k) \neq \varnothing$.

Definition 6.3. If L is a line bundle on X_T for some S-scheme T, then writing $\epsilon_T : T \to X_T$ for the section induced by ϵ, by a rigidification of L along ϵ_T we mean an isomorphism $\alpha : \mathcal{O}_T \xrightarrow{\sim} \epsilon_T^* L$.

Let (L_1, α_1) and (L_2, α_2) be line bundles on X_T with rigidification along ϵ. By a homomorphism between them we mean a homomorphism of line bundles $h : L_1 \to L_2$ with the property that $(\epsilon^* h) \circ \alpha_1 = \alpha_2$.

Note that to give an endomorphsim of (L, α), it suffices to give an element $h \in \mathrm{Hom}_{\mathcal{O}_{X_T}}(L, L)$ with $\epsilon^*(h) = 1$. Note that $\mathrm{Hom}_{\mathcal{O}_{X_T}}(L, L)$ is the global section of $\mathcal{H}om_{\mathcal{O}_{X_T}}(L, L) = L^{-1} \otimes L = \mathcal{O}_{X_T}$, we have $\mathrm{Hom}_{\mathcal{O}_{X_T}}(L, L) \cong \Gamma(X_T, \mathcal{O}_{X_T}) = \Gamma(T, f_*(\mathcal{O}_{X_T}))$. By the assumption (*), this is equal to $\Gamma(T, \mathcal{O}_T)$.

Definition 6.4. Note that the pairs (L, α) form an Abelian group via the tensor product. We may define a functor $P_{X/S,\epsilon} : (\mathbf{Sch}_{/S})^0 \to \mathbf{Ab}$ by

$$P_{X/S,\epsilon} : T \mapsto \text{ the isomorphsm classes of rigidified line bundle } (L, \alpha) \text{ on } X \times_S T$$

If $h : T' \to T$ is a morphism of S-schemes, then $P_{X/S,\epsilon}(h)$ sends (L, α) to (L', α'), where $L' = (id_X \times h)^* L$ and α' is the pullback of α under h.

Suppose that $P_{X/S,\epsilon}$ is representable by an S-scheme. On $X \times_S P_{X/S,\epsilon}$ we have a universal rigidified line bundle $(\mathcal{P}, v)$, called the Poincare bundle, satisfying the following property: if (L, α) is a line bundle on $X \times_S T$ with along the section ϵ then there exists a unique morphism $g : T \to P_{X/S,\epsilon}$ such that

$$(L, \alpha) \cong (id_X \times g)^* (\mathcal{P}, v)$$

Proposition 6.5. Under the assumption (*),

(1) for every S-scheme T there is a short exact sequence

$$0 \to \operatorname{Pic}(T) \xrightarrow{pr_T^*} \operatorname{Pic}(X_T) \to \operatorname{Pic}_{X/S}(T)$$

this property does not need that f admit a section. If further f admit a section, then the right hand is surjective, that is, the following sequence is exact

$$0 \to \operatorname{Pic}(T) \xrightarrow{pr_T^*} \operatorname{Pic}(X_T) \to \operatorname{Pic}_{X/S}(T) \to 0$$

(2) For any S-scheme T, we have an isomorphism

$$\operatorname{Pic}(X_T)/pr_T^* \operatorname{Pic}(T) \xrightarrow{\sim} P_{X/S,\epsilon}(T)$$

obtained by sending the class of a line bundle L on X_T to the bundle $L \otimes f^* \epsilon_T^* L^{-1}$ with its canonical rigidification.

(3) The functor $P_{X/S,\epsilon}$ is an fppf sheaf.

Corollary 6.6. $P_{X/S,\epsilon} \cong \operatorname{Pic}_{X/S}$ are the functors sending T to

$$\frac{\{\text{line budles on } X_T\}}{\{\text{line bundles of the form } f^* L, \text{ with } L \text{ a line bundle on } T\}}$$

Corollary 6.7. $\operatorname{Pic}_{X/S}$ equals to the Zariski sheaf associated to $P_{X/S}$.

Theorem 6.8. We list some results about representability for the general case (that is, we no longer assume that f satisfies (*)):

(1) If f is flat and projective with geometrically integral fibres then $\operatorname{Pic}_{X/S}$ is representable by a scheme, locally of finite presentation and separated over S.

(2) If f is flat and projective with geometrically reduced fibres, such that all irreducible components of the fibres of f are geometrically irreducible then $\operatorname{Pic}_{X/S}$ is representable by a scheme, locally of finite representation over S.

(3) If $S = \operatorname{Spec}(k)$ and f is proper then $\operatorname{Pic}_{X/S}$ is representable by a scheme that is separated and locally of finite type over k.

Remark 6.9. *Let X be a complete variety over k, then f satisfies (*). Let Y be a k-scheme and let L be a line bundle on $X \times_k Y$. By the above theorem $\mathrm{Pic}_{X/k}$ can be represented by a scheme. Then there is a morphism $Y \to \mathrm{Pic}_{X/k}$. Then the maximal closed subscheme $Y_0 \hookrightarrow Y$ is then the fibre over the zero section of $\mathrm{Pic}_{X/k}$.*

Now we turn to some basic properties of $\mathrm{Pic}_{X/k}$.

Proposition 6.10. Let X be a proper variety over k.

(1) The tangent space of $\mathrm{Pic}_{X/S}$ at the identity element is isomorphic to $H^1(X, \mathcal{O}_X)$. Further, the connected component $\mathrm{Pic}^0_{X/S}$ is smooth over k if and only if $\dim \mathrm{Pic}^0_{X/S} = \dim H^1(X, \mathcal{O}_X)$, and this always holds if char $(k) = 0$.

(2) If X is smooth over k then all connected components of $\mathrm{Pic}_{X/k}$ are complete.

Remark 6.11. *If C is a complete curve over a field k. Then $\mathrm{Pic}_{C/k}$ is a group scheme, locally of finite type, smooth over k.*

In particular, the identity component $\mathrm{Pic}^0_{C/k}$ is a group variety over k. If in addition we assume that C is smooth then $\mathrm{Pic}^0_{C/k}$ is complete, and is therefore an Abelian variety. Then we call $\mathrm{Pic}^0_{C/k}$ the Jacobian of C.

6.2 Digression on graded bialgebras

We quickly list some results.

Definition 6.12. We say that the graded k-algebra $H^\bullet$ is graded-commutative if

$$xy = (-1)^{\deg(x)\deg(y)} yx$$

for all homogeneous $x, y \in H^\bullet$. The algebra $H^\bullet$ is said to be connected if $H^0 = k \cdot 1$. The algebra $H^\bullet$ is said to be of finite type over k if $\dim_k(H^n) < \infty$ for all n.

If $H_1^\bullet$ and $H_2^\bullet$ are graded k-algebra then the graded k-module $H_1^\bullet \otimes_k H_2^\bullet$ inherits the structure of a graded k-algebra: for homogeneous $x, \xi \in H_1^\bullet$ and $y, \eta \in H_2^\bullet$ one sets $(x \otimes y) \cdot (\xi \otimes \eta) = (-1)^{\deg(y)\deg(\xi)} \cdot (x\xi \otimes y\eta)$. Then a graded k-algebra $H^\bullet$ is graded-commutative if and only if the product operation $H^\bullet \otimes H^\bullet \to H^\bullet$ is a homomorphism of graded k-algebras.

Definition 6.13. A graded bialgebra over k is a graded k-algebra $H^\bullet$ together with two homomorphisms of k-algebras

$$\mu : H^\bullet \to H^\bullet \otimes_k H^\bullet \quad \text{called co-multiplication}$$

$$\epsilon : H^\bullet \to k \quad \text{the identity section}$$

such that

$$(\mu \otimes id) \circ \mu = (id \otimes \mu) \circ \mu : H^\bullet \to H^\bullet \otimes_k H^\bullet \otimes_k H^\bullet$$

and

$$(\epsilon \otimes id) \circ \mu : H^\bullet \to H^\bullet$$

Theorem 6.14 (Borel-Hopf structure theorem)**.** Let $H^\bullet$ be a connected, graded-commutative bialgebra of finite type over a perfect field k. Then there exists graded bialgebras $H_i^\bullet$ and an isomorphism of bialgebras

$$H^\bullet \cong H_1^\bullet \otimes_k \cdots \otimes_k H_r^\bullet$$

such that the algebra underlying $H_i^\bullet$ is generated by one element.

Corollary 6.15. With the same hypothesis above, assume that there is an integer g such that $H^n = (0)$ for all $n > g$. Then $\dim_k(H^1) \leq g$. If $\dim_k(H^1) = g$ then $H^\bullet \cong \wedge^\bullet H^1$ as graded bialgebras.

Corollary 6.16. Let X be a group variety over a field k. Then $H^\bullet(X, \mathcal{O}_X)$ has a natural structure of a graded k-bialgebra. We have $\dim_k(H^1(X, \mathcal{O}_X)) \leq \dim(X)$.

Definition 6.17. Let $H^\bullet$ be a graded bialgebra with comultiplication $\mu : H^\bullet \to H^\bullet \otimes_k H^\bullet$. Then an element $h \in H^\bullet$ is called a primitive element if $\mu(h) = h \otimes 1 + 1 \otimes h$.

Proposition 6.18. Let V be a finite dimensional k-vector space, and consider the exterior algebra $\wedge^\bullet V$. Then $V = \wedge^1 V$ is the set of primitive elements in $\wedge^\bullet V$.

6.3 The dual of an Abelian variety

Remark 6.19. *Let X be a complete variety over k. Recall that* $\mathrm{Pic}_{X/k}$ *also represents rigidified the line bundles, let $\mathscr{P}$ be the Poincare bundle on $X \times \mathrm{Pic}_{X/k}$ with a rigidification*

$$\alpha : \mathscr{P}|_{\{e_X\} \times \mathrm{Pic}_{X/k}} \xrightarrow{\sim} \mathcal{O}_{\mathrm{Pic}_{X/k}}$$

along the section $\mathrm{Spec}(k) \hookrightarrow X$*.*

Let L be a line bundle on X. Then there is a uniquely morphism

$$\varphi_L : X \to \mathrm{Pic}_{X/k}$$

given by $x \mapsto [t_x^* L \otimes L^{-1}]$. This morphism satisfies that

$$(id_X \times \varphi_L)^* \mathscr{P} \cong \Lambda(L)$$

Also, this homomorphism is explicitly This homomorphism factors via $\mathrm{Pic}^0_{X/k}$ *since X is connected.*

Theorem 6.20. Let X be an Abelian variety over a field k. Then $\mathrm{Pic}^0_{X/k}$ is reduced, hence it is an Abelian variety. For every ample line bundle L the homomorphism $\varphi_L : X \to \mathrm{Pic}^0_{X/k}$ is an isogeny with kernel $K(L)$. We have $\dim H^1(X, \mathcal{O}_X) = \dim(\mathrm{Pic}^0_{X/k}) = \dim X$.

Proof. Since L is ample, $K(L)$ is a finite group scheme. Thus $\dim(\mathrm{Pic}^0_{X/k}) \geq \dim(X)$. Therefore $\dim(\mathrm{Pic}^0_{X/k}) = \dim(X) = \dim_k(H^1(X, \mathcal{O}_X))$. Then $\mathrm{Pic}^0_{X/S}$ is smooth over k, and hence is reduced. ■

Definition 6.21. The Abelian variety $X^t = \mathrm{Pic}^0_{X/k}$ is called the dual of X. We write $\mathscr{P}$, of $\mathscr{P}_X$, for the Poincare bundle on $X \times X^t$. If $f : X \to Y$ is a homomorphism of Abelian varieties over k then we write $f^t : Y^t \to X^t$ for the induced homomorphism, called the dual of f, such that

$$(id \times f^t)^* \mathscr{P}_X \cong (f \times id)^* \mathscr{P}_Y$$

Remark 6.22. *We use the notation $*^D$ for the Cartier dual of finite group schemes. We use the notation $*^t$ for the dual of Abelian varieties.*

7 Duality

7.1 Formation of quotients and the descent of coherent sheaves

Definition 7.1. Let S be a base scheme. Let $\rho : G \times_S X \to X$ be an action of an S-group scheme G on an S-scheme X. Let F be a coherent sheaf of $\mathcal{O}_X$-modules. Then an action of G on F, compatible with the action ρ, is an isomorphism $\lambda : pr_2^* F \xrightarrow{\sim} \rho^* F$ of sheaves on $G \times_S X$, such that on $G \times_S G \times_S X$ we have a commutative diagram

$$\begin{tikzcd} pr_3^* F \arrow[r, "pr_{23}^*(\lambda)"] \arrow[d, "(m \times id_X)^*(\lambda)"'] & pr_{23}^* \rho^* F \arrow[d, "(id_G \times \rho)^*(\lambda)"] \\ (m \times id_X)^* \rho^* F \arrow[r, equal] & (id_G \times \rho)^* \rho^* F \end{tikzcd}$$

Proposition 7.2. Let $\rho : G \times_S X \to X$ be an action of an S-group scheme G. Suppose that there exists an fppf quotient $p : X \to Y$ of X by G, recall that we have a canonical isomorphism $\Psi : G \times X \to X \times X$. If F is a coherent $\mathcal{O}_Y$ sheaf then the canonical isomorphism $\lambda_{\text{can}} : pr_2^*(p^*F) \xrightarrow{\sim} \rho^*(p^*F)$. This defines a ρ-compatible G-action on p^*F. The functor $F \mapsto (\rho^*F, \lambda_{\text{can}})$ gives an equivalence between the category of coherent $\mathcal{O}_Y$-modules and the category of coherent $\mathcal{O}_X$-modules with ρ-compatible G-actions. This restricts to an equivalence between the category of finite locally free $\mathcal{O}_Y$-modules and the category of finite locally free $\mathcal{O}_X$-modules with G-action.

Proposition 7.3. Let G be a commutative, finite locally free S-group scheme. Let $\rho : G \times_S X \to X$ be a free action of G on an S-scheme X. Let $p : X \to Y$ be the quotient of X by G. Suppose that $f_*(\mathcal{O}_{X_T}) = \mathcal{O}_T$ for all S-scheme T. Then for any S-scheme there is a canonical isomorphism of groups

$$\delta_T : \{\text{isomorphism classes of line bundles } L \text{ on } Y_T \text{ with } p^*L \cong \mathcal{O}_{X_T}\} \xrightarrow{\sim} G^D(T)$$

and this isomorphism is compatible with base change $T' \to T$.

7.2 Two duality theorems

Theorem 7.4. Let $f : X \to Y$ be an isogeny of Abelian varieties. Then $f^t : Y^t \to X^t$ is again an isogeny and there is a canonical isomorphism of schemes

$$\operatorname{Ker}(f)^D \xrightarrow{\sim} \operatorname{Ker}(f^t)$$

Proof. If T is a k-scheme, recall the definition of Y^t, any class in $\operatorname{Ker}(f^t)(T)$ can be represented by a line bundle L on Y_T. Note that f^*L is trivial, then f^*L is of the form pr_T^*M for some line bundle M on T under the projection $pr_T : X_T \to T$. Thus $L' = L \otimes (pr'_T)^* M^{-1}$, where $pr'_T : Y_T \to T$, is a line bundle on Y_T which represents the same class with L in $\operatorname{Ker}(f^t)(T)$, and its inverse image on X_T is just $\mathcal{O}_{X_T}$. Hence, every class in $\operatorname{Ker}(f^t)(T)$ is uniquely represented by a line bundle L on Y_T such that $f^*L \cong \mathcal{O}_{X_T}$.

Then obviously we have $\operatorname{Ker}(f)^D \xrightarrow{\sim} \operatorname{Ker}(f^t)$. In particular, f^t has finite kernel and then is an isogeny. ■

Corollary 7.5. Let $f : X \to Y$ be a homomorphism. Let M be a line bundle on Y and write $L = f^*M$. Then $\varphi_L : X \to X^t$ equals the composition

$$X \xrightarrow{f} Y \xrightarrow{\varphi_M} Y^t \xrightarrow{f^t} X^t$$

If f is an isogeny and M is non-degenerate then L is non-degenerate too, and $\mathrm{rank}(K(L)) = \deg(f)^2 \cdot \mathrm{rank}(K(M))$.

Remark 7.6. *By choosing $T = S = \mathrm{Spec}(k)$, we find that the natural morphism $g : T \hookrightarrow \mathrm{Pic}^0_{X/k}$ gives an isomorphism $(id_X \times g)^*\mathscr{P} \cong \mathcal{O}_X$ under the morphism*

$$X \times \mathrm{Spec}(k) \to X \times \mathrm{Pic}^0_{X/k}$$

This means $\mathscr{P}|_{X\times\{e_X\}} \cong \mathcal{O}_X$. Thus we can choose a rigidification of $\mathscr{P}$ along $X \times \{e_X\}$. Such a rigidification is unique up to the invertible elements in $\Gamma(X, \mathcal{O}_X) = k$. Then there is a unique rigidification alone $X \times \{e_X\}$ such that it agrees the rigidification along $\{0\} \times X^t$ at (e_X, e_X).

Now, let $T = X$, and consider the dual of X^t. Then there is a morphism $\kappa_X : X = T \to X^{tt}$ defined by the rigidification above.

Lemma 7.7. Let L be a line bundle on X. Then $\varphi_L = \varphi_L^t \circ \kappa_X : X \to X^t$.

Proof. Just compute it. ■

Theorem 7.8. Let X be an Abelian variety over a field. Then the homomorphism κ_X is an isomorphism.

Proof. From the above lemma, κ_X is an isogeny. Further, by computing the rank of two sides, we find that $\deg(\kappa_X) = 1$. ■

Corollary 7.9. Let L be a non-degenerate line bundle on X. Then $K(L) \cong K(L)^D$.

Proof. $K(L)$ is exactly the kernel of φ_L. Then $K(L)^D \cong \mathrm{Ker}(\varphi_L^t) \cong K(L)$. ■

7.3 Further properties of $\mathrm{Pic}^0_{X/k}$

Remark 7.10. *We shall associate to L a homomorphism $\varphi_L : X_T \to X_T^t$ for some k-scheme T.*

First we extend the Mumford bundle $\Lambda(L)$ on $X_T \times_T X_T$. Note that $X_T \times_T X_T = (X \times_k X) \times_k T$, we may define

$$\Lambda(L) = (m \times id_T)^*L \otimes p_{13}L^{-1} \otimes p_{23}^*L^{-1}$$

that is, we view T as the base scheme.

Now similarly, there is a morphism

$$\varphi_L : X_T \to \mathrm{Pic}_{X_T/T}$$

which factors through $X_T^t = \mathrm{Pic}^0_{X/k} \times_k T$.

Lemma 7.11. (1) The morphism φ_L only depends on the class of L in $\mathrm{Pic}_{X/k}(T)$.

(2) Let $f : T \to S$ be a morphism of k-schemes. If M is a line bundle on X_S and $L = (id_X \times f)^*M$ on X_T, then $\varphi_L : X_T \to X_T^t$ is the morphism obtained from $\varphi_M : X_S \to X_S^t$.

(3) φ_L is a homomorphism.

Proposition 7.12. Let $K(L) \subseteq X_T$ be the kernel of φ_L. It is just the maximal subscheme of X_T over which $\Lambda(L)$ is trivial.

Lemma 7.13. Let T be a locally Noetherian k-scheme. Write $\pi : X_T \times_T X_T \to T$ for the structure morphism. For a line bundle L on X_T, consider the following conditions:

1. $\varphi_L = 0$.
2. $\Lambda(L) = pr_2^* M$ for some line bundle M on X_T.
3. $\Lambda(L) = \pi^* N$ for some line bundle N on T.
4. $\varphi_{L_t} = 0$ for some $t \in T$.

Then 1. $\iff$ 2. $\iff$ 3. $\Rightarrow$ 4., and if T is connected then all four conditions are equivalent. If these equivalent conditions are satisfied then $N \cong e^* L^{-1}$ and $M = pr_T^* N$, where $e : T \to X_T$ is the identify section.

Remark 7.14. *Let X and Y be two projective varieties over a field k. Then the contravariant functor*

$$\mathrm{Hom}_{\boldsymbol{Sch}}(X, Y) : (\boldsymbol{Sch}_{/k}) \to \boldsymbol{Set} \quad T \mapsto \mathrm{Hom}_{\boldsymbol{Sch}/T}(X_T, Y_T)$$

is representable by a k-scheme, locally of finite type.

Theorem 7.15. Let X and Y be two Abelian varieties over a field k. Then the functor

$$\mathrm{Hom}_{\mathbf{AV}}(X, Y) : (\mathbf{Sch}_{/k}) \to \mathbf{Ab} \quad T \mapsto \mathrm{Hom}_{\mathbf{GSch}_{/T}}(X_T, Y_T)$$

is representable by an etale commutative k-group scheme.

Lemma 7.16. Let T be a connected k-scheme. Let L be a line bundle on X_T. For any two k-valued points $s, t \in T(k)$ we have $\varphi_{L_s} = \varphi_{L_t}$. In particular, $\mathrm{Pic}^0_{X/k} \subseteq \mathrm{Ker}(\varphi)$, where φ is the map sending L to φ_L.

Proof. By 7.13, let $T = X^t$ and $L = \mathscr{P}$, we find that $X^t \subseteq \mathrm{Ker}(\varphi)$. As φ is a homomorphism, it is constant on the connected components.

Let $f : T \to \mathrm{Pic}_{X/K}$ be the morphism corresponding to L. This morphism factors through some connected components C. Let $M = \mathscr{P}|_{X \times C}$. Then φ_L is the pull-back of φ_M. By the above discussion we fine that $\varphi_{M_{f(s)}} = \varphi_{M_{f(t)}}$. ■

Corollary 7.17. Let X, Y be Abelian varieties over k. Then the map

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

given by $f \mapsto f^t$ is a homomorphism of k-group schemes. For any $n \in \mathbb{Z}$, we have $(n_X)^t = n_{X^t}$.

Definition 7.18. Let X be an Abelian variety. We call a homomorphism $f : X \to X^t$ symmetric if $f = f^t$, taking the isomorphism κ_X. Note that $\mathrm{Hom}^{\mathrm{sym}}(X, X^t)$ is exactly the kernel of the endomorphism $\mathrm{Hom}(X, X^t)$ given by $f \mapsto f - f^t$.

Proposition 7.19. The map $\varphi : \mathrm{Pic}_{X/k} \to \mathrm{Hom}(X, X^t)$ sending L to φ_L is a homomorphism of groups, and it factors through $\mathrm{Hom}^{\mathrm{sym}}(X, X^t)$.

Proof. This follows from that $\varphi_L = \varphi_L^t \circ \kappa_X$. ■

Lemma 7.20. Let L be a line bundle on X with $\varphi_L = 0$. If L is not trivial, then $H^i(X, L) = 0$ for all i.

Proof. Since $\varphi_L = 0$, $\Lambda(L)$ is trivial on $X \times X$. Thus $(\alpha + \beta)^* L \cong \alpha^* L \otimes \beta^* L$ for any morphisms $\alpha, \beta : X \to X$. By taking $\alpha = -\beta = id_X$ we may find that $(-1)^* L = L^{-1}$.

First for the group $H^0(X, L) = \Gamma(X, L)$, if there is a nontrivial section s, then $(-1)^* s$ is a nonzero section of $(-1)^* L \cong L^{-1}$. Then both L and L^{-1} have a nontrivial section. Therefore, L is trivial on X, a contradiction.

Let i be the smallest positive integer such that $H^i(X, L) \neq 0$. Consider the composition

$$X \to X \times X \xrightarrow{m} X \quad x \mapsto (x, 0) \mapsto x$$

This induces maps

$$H^i(X, L) \to H^i(X \times X, m^* L) \to H^i(X, L)$$

with the composition is the identify. By Kunneth formula

$$H^i(X \times X, m^* L) \cong H^i(X \times X, p_1^* L \otimes p_2^* L) \cong \sum_{a+b=i} H^a(X, L) \otimes H^b(X, L) = 0$$

The result follows immediately. ■

Proposition 7.21. Let X be an Abelian variety over an algebraically closed field k. Let L be an ample line bundle on X and M a line bundle with $\varphi_M = 0$. Then there is a point $x \in X(k)$ such that $M \cong t_x^* L \otimes L^{-1}$.

Proof. ■

Corollary 7.22. Let X be an Abelian variety over a field k. Then $\mathrm{Pic}^0_{X/k} = \mathrm{Ker}(\varphi)$.

Proof. We already know that $\mathrm{Pic}^0 \subseteq \mathrm{Ker}(\varphi)$. Hence $\mathrm{Ker}(\varphi)$ is the union of some connected components of Pic. But every $\bar{k}$-valued point of $\mathrm{Ker}(\varphi)$ lies in Pic^0. Then the result follows. ■

Corollary 7.23. Let X be an Abelian variety over a field k. Let L be a line bundle on X.

(1) If $[L^n] \in \mathrm{Pic}^0_{X/k}$ for some $n \neq 0$ then $[L] \in \mathrm{Pic}^0_{X/k}$. In particular, if $L^n \cong \mathcal{O}_X$, then $[L] \in \mathrm{Pic}^0_{X/k}$.

(2) We have $[L \otimes (-1)^* L^{-1}] \in \mathrm{Pic}^0_{X/k}$.

(3) We have

$$\begin{aligned}
&[L] \in \mathrm{Pic}^0_{X/k} \\
\iff & n^*L \cong L^n, \ \forall n \in \mathbb{Z} \\
\iff & n^*L \cong L^n, \ \text{for some } n \in \mathbb{Z}\backslash\{0,1\}
\end{aligned}$$

Proof. (1) Since $\varphi : \mathrm{Pic}_{X/k} \to \mathrm{Hom}(X, X^t)$ is a homomorphism of groups, $\varphi_{L^n} = n_{X^t} \cdot \varphi_L = \varphi_L \circ n_X$. If φ_{L^n} is trivial, since n_X is surjective, φ_L is trivial.

(2) By the definition of φ_L we find that $\varphi_{(-1)^*L} = -\varphi_L$ for all L. Thus $L \otimes (-1)^*L^{-1} \in \mathrm{Ker}(\varphi)$.

(3) If $[L] \in \mathrm{Pic}^0_{X/k}$, then on $X \times X$ we have $m^*L \cong p^*L \otimes q^*L$, where p and q are the projections. Then by induction on n we have $n^*L = L^n$.

In general case, $n^*L \cong L^n \otimes [L \otimes (-1)^*L]^{(n^2-n)/2}$, then $n^*L \cong L^n$ for $n \neq 0, 1$ implies that $L \otimes (-1)^*L \in \mathrm{Pic}^0_{X/k}$. By (2) we have $L^2 \in \mathrm{Pic}^0_{X/k}$ and by (1) then $L \in \mathrm{Pic}^0_{X/k}$. ■

Definition 7.24. Define the Neron-severi group scheme $\mathrm{NS}_{X/k}$ to be the fppf quotient of $\mathrm{Pic}_{X/k}$ modulo $\mathrm{Pic}^0_{X/k}$. We also write $\mathrm{NS}(X) = \mathrm{NS}_{X/k}(k)$, it is the $\mathrm{Gal}(k_s/k)$-invariant subset of $\mathrm{NS}_{X/k}(\bar{k})$.

We say that two line bundles L and M are algebraically equivalent, denoted by $L \sim_{\text{alg}} M$, if $[L]$ and $[M]$ have the same image in $\mathrm{NS}(X)$.

Corollary 7.25. The Neron-Severi group $\mathrm{NS}(X)$ is torsion-free. If $n \in \mathbb{Z}$, and L is a line bundle on X then n^*L is algebraically equivalent to L^{n^2}, in other words, $n^* : \mathrm{NS}(X) \to \mathrm{NS}(X)$ is multiplication by n^2.

Proof. For $L \in \mathrm{NS}(X)$, if $L^n = 0$, that is, $L^n \in \mathrm{Pic}^0_{X/k}$, then by 7.23 $L = 0$.

Also by 7.23 (2) and that $n^*L = L^{(n^2+n)/2} \otimes (-1)^*L$, n^*L is algebraically equivalent to L^{n^2}. ■

Corollary 7.26. Recall that there is a natural homomorphism $\varphi : \mathrm{Pic}_{X/k} \to \mathrm{Hom}^{\mathrm{sym}}(X, X^t) \subseteq \mathrm{Hom}(X, X^t)$, since $\varphi_L = 0$ if and only if $L \in \mathrm{Pic}^0_{X/k}$, it factors as

$$\mathrm{Pic}_{X/k} \xrightarrow{q} \mathrm{NS}_{X/k} \hookrightarrow \mathrm{Hom}^{\mathrm{sym}}(X, X^t)$$

7.4 Applications to cohomology

Proposition 7.27. Let X be an Abelian variety with $\dim(X) = g$. Cup-product gives an isomorphism $\bigwedge^\bullet H^1(X, \mathcal{O}_X) \xrightarrow{\sim} H^\bullet(X, \mathcal{O}_X)$. For every p and q we have a natural isomorphism

$$H^q(X, \Omega^p_{X/k}) \cong (\bigwedge^q T_{X^t,0}) \otimes (\bigwedge^p T^\vee_{X,0})$$

The hodge numbers $h^{pq} = \dim^q(X, \Omega^p_{X/k})$ are given by $h^{p,q} = C^p_g C^q_g$.

Proof. By 6.20 and 6.15, cup products induce isomorphisms. Recall that $\Omega^n_{X/k} \cong (\bigwedge^n T^\vee_{X/k}) \otimes \otimes_k \mathcal{O}_X$, then

$$H^q(X, \Omega^p_{X/k}) \cong (\bigwedge^q T_{X^t,0}) \otimes (\bigwedge^p T^\vee_{X,0})$$

■

Corollary 7.28. The morphism n_X on X induces multiplication by n^{p+q} on $H^p(X, \Omega_X^p)$.

Remark 7.29. *There is a Hodge-de Rham spectral sequence*

$$E_1^{p,q} = H^q(X, \Omega_X^p) \Rightarrow H_{\mathrm{dR}}^{p+q}(X/k)$$

on any smooth proper algebraic variety X. Deligne and Illusie show that the spectral sequence degenerates at the E_1-level for k with characteristic 0. But for Abelian varieties, this is also true without for any restriction for k.

Proposition 7.30. There is an exact sequence

$$0 \to H^0(X, \Omega_{X/k}^1) \cong T_{X,0}^\vee \to H_{\mathrm{dR}}^1(X/k) \to H^1(X, \mathcal{O}_X) \to 0$$

7.5 The duality between Frobenius and Verschiebung

Proposition 7.31. Let X be an Abelian variety over a field k of characteristic p. We identify $(X^t)^{(p)} = (X^{(p)})^t$, and we denote this Abelian variety by $X^{t,(p)}$. Then we have

$$F_{X/k}^t = V_{X^t/k}, \quad V_{X/k}^t = F_{X^t/k}$$

Proof. ∎

8 The Theta group of a line bundle (skip)

8.1 The theta group $\mathscr{G}(L)$

Definition 8.1. Let X be an Abelian variety over a field k. Let L be a line bundle on X.

For a k-scheme T define $\mathscr{G}(L)(T)$ to be the set of pairs (x, φ) where $x \in X(T)$ and where $\varphi : L_T \to t_x^* L_T$ is an isomorphism.

By this, we obtain a group functor $\mathscr{G} : (\mathbf{Sch}_{/k} \to \mathbf{Gr})$.

Lemma 8.2. The group functor $\mathscr{G}(L)$ is representable. There is an exact sequence of group schemes

$$0 \to \mathbb{G}_{m,k} \to \mathscr{G}(L) \to K(L) \to 0$$

where the last map is given by $(x, \varphi) \mapsto x$.

Definition 8.3. Consider the morphism

$$[\quad,\quad] : \mathscr{G}(L)^2 \to \mathscr{G}(L)$$

given by

$$(g_1, g_2) \mapsto g_1 g_2 g_1^{-1} g_2^{-1}$$

Since $K(L) = \mathscr{G}(L)/\mathbb{G}_m$ is commutative, the image of this morphism is in $\mathbb{G}_m$. Obviously, this morphism induces a pairing

$$e^L : K(L)^2 \cong (\mathscr{G}/\mathbb{G}_m)^2 \to \mathbb{G}_m$$

called the commutative pairing induced by the theta group.

Proposition 8.4. Obviously the pairing has the following properties:

1. $e^L(x,x)=1$.
2. e^L is bilinear.
3. $e^{f^*L}=e^L\circ(f,f)$.
4. $e^{L\otimes M}=e^L\cdot e^M$.
5. If $L\in \mathrm{Pic}^0_{X/k}$, then $e^L=1$.
6. For $x\in K(L)$ and $y\in K(L^n)$, we have $e^{L^n}(x,y)=e^L(x,ny)$.

Theorem 8.5. Let X be an Abelian variety over a field k. Write $\mathcal{C}$ for the Abelian category of commutative group schemes of finite type over k. Associating $\mathscr{G}(L)$ with L gives an isomorphism

$$X^t(k)\xrightarrow{\sim}\mathrm{Ext}^1_{\mathcal{C}}(X,\mathbb{G}_m)$$

8.2 Descent of line bundles over homomorphisms

Theorem 8.6. Let $f:X\to Y$ be a surjective homomorphism of Abelian varieties. Let L be a line bundle on X. Then there is a bijective correspondence between the $M\in\mathrm{Pic}(Y)$ with $f^*M\cong L$ and the homomorphism $\mathrm{Ker}(f)\to\mathscr{G}(L)$ lying over the natural inclusion $\mathrm{Ker}(f)\hookrightarrow X$.

9 The cohomology of line bundles (skip)

Theorem 9.1. Let X be a g-dimensional Abelian variety over a field k. Let $\mathscr{P}$ be the Poincare bundle on $X\times X^t$. Then

$$R^n(p_2)_*\mathscr{P}=\begin{cases}0 & n\neq g\\ i_0(k) & n=g\end{cases}$$

and

$$H^n(X\times X^t,\mathscr{P})=\begin{cases}0 & n\neq g\\ k & n=g\end{cases}$$

Here $i_0(k)$ denotes the skycraper sheaf at $0\in X^t$ with stalk k.

Theorem 9.2 (Riemann-Roch theorem)**.** If L is a line bundle on a g-dimensional Abelian variety, then

$$\chi(L)=c_1(L)^g/g!,\quad \deg(\varphi_L)=\chi(L)^2$$

Corollary 9.3. Let $f:Y\to X$ be an isogeny. If L is a line bundle on X then $\chi(f^*L)=\deg(f)\cdot\chi(L)$.

Theorem 9.4 (Vanishing theorem)**.** If L is a non-degenerate line bundle, that is, $K(L)$ is finite, then there is a unique integer i such that $H^i(X,L)\neq 0$.

Definition 9.5. Let L be a non-degenerate line bundle then the unique $i=i(L)$ such that $h^i(L)\neq 0$ is called the index of L. Recall that $i(L)=0$, that is, L is effective, then L is ample.

Example 5. For the case X is a curve, $g = 1$. Let D be a divisor on X of degree d. Thus by Riemann-Roch theorem $\chi(L) = h^0(\mathcal{O}(L)) - h^1(\mathcal{O}(L)) = d$. Then

$$D \text{ is degenerate } \iff \varphi_L \text{ is not an isogeny } \iff \deg(\varphi_L) = 0 \iff \chi(L) = 0 \iff d = 0$$

$$D \text{ is non-degenerate with } i(L) = 0 \iff h^0 > 0,\ h^1 = 0 \iff d > 0$$

$$D \text{ is non-degenerate with } i(L) = 1 \iff d < 0$$

Proposition 9.6. (1) Let L be a non-degenerate line bundle on a g-dimensional Abelian variety X. Then $i(L^{-1}) = g - i(L)$.

(2) If T is a locally Noetherian k-scheme and M is a line bundle on $X \times T$ such that all M_t are non-degenerate then the function $t \mapsto i(M_t)$ is locally constant on T. In particular, if L is as in (1) and L' is a line bundle on X with $[L'] \in \mathrm{Pic}^0_{X/k}$ then $i(L) = i(L \otimes L')$.

(3) Let $f : X \to Y$ be an isogeny of degree prime to char (k). If M is a non-degenerate line bundle on Y then f^*M is also non-degenerate and $i^*(f^*M) = i(M)$.

(4) If L is non-degenrate and $m \neq 0$ then L^m is also non-degenerate. Furthermore, if $m > 0$ and char $(k) \nmid m$ then $i(L^m) = i(L)$.

(5) If L_1, L_2 and $L_1 \otimes L_2$ are all non-degenerate then $i(L_1 \otimes L_2) \leq i(L_1) + i(L_2)$.

(6) If H is ample, L and $L \otimes H$ are both non-degenerate then $i(L \otimes H) \leq i(L)$.

Proof. (1) Recall that the canonical sheaf $\Omega^g \cong \mathcal{O}_X$, by Serre duality, $i(L^{-1}) = g - i(L)$.

(2) By the semi-continuous theorem, for all j the function $t \mapsto \dim^j_{k(t)}(X \otimes k(t), M_t)$ is upper semi-continuous. Then the first assertion follows immediately. The second assertion follows by applying this to the Poincare bundle.

(3)

(4) ∎

Theorem 9.7 (Kempf-Mumford-Ramanujam)**.** Let L be a non-degenerate line bundle on an Abelian variety X. Let H be an ample line bundle on X and write $\Phi(t)$ for the Hilbert polynomial of L with respect to H. Then all complex roots of Φ are real, and the index $i(L)$ equals the number of positive roots, counted with multiplicities.

Remark 9.8. *Form this theorem we can also find that if $f : X \to Y$ is an isogeny and L is a non-degenerate line bundle on Y, then $i(L) = i(f^*L)$.*

Theorem 9.9. Let L be a line bundle on an Abelian variety X over a field k. Let H be an ample line bundle on X and write $\Phi(t)$ for the Hilbert polynomial of L with respect to H. Then the multiplicity of 0 as a root of Φ equals the dimension of $K(L)$.

10 Tate modules, p-divisible groups, and the fundamental group

10.1 Tate-ℓ-modules

Definition 10.1. Let X be an Abelian variety over a field k, and let ℓ be a prime number differ from char (k). Then we define the Tate ℓ-module of X, denoted by $T_\ell X$, to be the projective limit of the system $\{X[\ell^n](k_s)\}_{n\in\mathbb{Z}_{\geq 0}}$ with respect to the transition maps $\ell : X[\ell^{n+1}](k_s) \to X[\ell^n](k_s)$.

If char $(k) = p > 0$, we define

$$T_{p,\text{et}}X \triangleq \lim(\{0\} \xleftarrow{p} X[p](\bar{k}) \xleftarrow{p} X[p^2](\bar{k}) \xleftarrow{p} \cdots)$$

Remark 10.2. *The definition of Tate ℓ-module may be reformulated by*

$$T_\ell X = \mathrm{Hom}_{\text{groups}}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, X(k_s))$$

Indeed,

$$\mathrm{Hom}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, X(k_s)) = \varprojlim \mathrm{Hom}(\mathbb{Z}/\ell^n\mathbb{Z}, X(k_s)) = \varprojlim X[\ell^n](k_s)$$

Proposition 10.3. *$T_\ell X$ is a free $\mathbb{Z}_\ell$-module of rank $2g$.*

Remark 10.4. *A homomorphism $f : X \to Y$ gives rise to a $\mathbb{Z}_\ell$-linear, $\mathrm{Gal}(k_s/k)$-equivalent map $T_\ell f : T_\ell X \to T_\ell Y$.*

Further suppose that f is an isogeny with kernel $N \subseteq X$. Applying $\mathrm{Hom}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, -)$ to the exact sequence

$$0 \to N(k_s) \to X(k_s) \to Y(k_s) \to 0$$

we obtain an exact sequence

$$0 \to T_\ell X \xrightarrow{T_\ell f} T_\ell Y \to \mathrm{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N(k_s)) \to \mathrm{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, X(k_s)) \to \mathrm{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, Y(k_s))$$

First we try to understand the term $\mathrm{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N(k_s))$. Write $N = N_\ell \times N^\ell$, where N_ℓ a group of ℓ-power order and N^ℓ a group of order prime to ℓ. Then

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

Next consider the long exact sequence

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

Note that $N_\ell(k_s)$ is finite, suppose it is killed by ℓ^a. Then the multiplication by ℓ^a kills all terms like $\mathrm{Ext}^i(-, N_\ell(k_s))$. But the multiplication by ℓ^a is a bijection of $\mathbb{Q}_\ell$. Therefore, $\mathrm{Ext}^i(\mathbb{Q}_\ell, N_\ell(k_s)) = 0$. Then the exact sequence above gives that

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

But the right hand is equal to $N_\ell(k_s)$, we conclude that

$$\mathrm{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N(k_s)) \cong N_\ell(k_s)$$

Now we turn to the map $\mathrm{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, X(k_s)) \to \mathrm{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, Y(k_s))$*, denote it by* $E^1(f)$*, we claim it is injective. Choose an isogeny* $g : Y \to X$ *such that* $g \circ f = [n]_X$*. Then* $E^1(g \circ f)$ *is multiplication by* n *on* $\mathrm{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, X(k_s))$*. Now we write* $n = \ell^m \cdot n'$ *with* $(n', \ell) = 1$*. Then it suffices to show that* $E^1(\ell^m)$ *is injective. By taking* $Y = X$ *and* $f = [\ell^m]_X$ *the sequence becomes* $0 \to T_\ell X \xrightarrow{\ell^m} T_\ell X \xrightarrow{\delta} \mathrm{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, X[\ell^m](k_s)) = X[\ell^m](k_s) \to \mathrm{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, X(k_s)) \xrightarrow{E^1(\ell^m)} \mathrm{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, X(k_s))$*. Then the injectivity of* $E^1(\ell^m)$ *follows from the surjectivity of* δ*.*

Proposition 10.5. To summarize the above remark, let $f : X \to Y$ be an isogeny of Abelian varieties over a field k, with kernel N. If ℓ is a prime number with $\ell \neq \mathrm{char}\,(k)$, then we have an exact sequence of $\mathbb{Z}_\ell[\mathrm{Gal}(k_s/k)]$-modules

$$0 \to T_\ell X \xrightarrow{T_\ell f} T_\ell Y \to N_\ell(k_s) \to 0$$

Corollary 10.6. Let $V_\ell X = T_\ell X \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. Then the induced map $V_\ell f : V_\ell X \to V_\ell Y$ is an isomorphism.

Remark 10.7. *The construction of the Tate module makes sense for arbitrary varieties. For instance,* $T_\ell \mathbb{G}_a = 0$*. Let* $\mathbb{Z}_\ell(1)$ *denote the Tate module* $T_\ell \mathbb{G}_m$*. As a* $\mathbb{Z}_\ell$*-module, it is free of rank 1. The action of* $\mathrm{Gal}(k_s/k)$ *is therefore given by a character*

$$\chi_\ell : \mathrm{Gal}(k_s/k) \to \mathbb{Z}_\ell^* = \mathrm{GL}(\mathbb{Z}_\ell(1))$$

called the ℓ*-adic cyclotomic character.*

If T *is any* ℓ*-adic representation of* $\mathrm{Gal}(k_s/k)$ *then we define* $T(n)$ *to be*

$$\begin{cases} T \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell(1)^{\otimes n} & n \geq 0 \\ T \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell(-1)^{\otimes -n} & n \leq 0 \end{cases}$$

where $\mathbb{Z}_\ell(1) = \mathbb{Z}_\ell(1)^\vee$*.*

Proposition 10.8. We have a canonical isomorphism

$$T_\ell X^t \cong (T_\ell X)^\vee(1)$$

Proof. We have

$$X^t[\ell^n] = \mathrm{Ker}([\ell^n]_{X^t}) = \mathrm{Ker}([\ell^n])^D = X[\ell^n]^D$$

Hence,

$$X^t[\ell^n](k_s) = X[\ell^n]^D(k_s) \cong \mathrm{Hom}(X[\ell^n](k_s), k_s^*) = \mathrm{Hom}(X[\ell^n](k_s), \mu_{\ell^n}(k_s))$$

as groups with Galois action. Now by taking projective limits we obtain the result. ■

10.2 The p-divisible group

Definition 10.9. Let S be a base scheme. A p-divisible group over S, also called a Barsotti-Tate group over S, is an inductive system

$$\{G_n | i_n : G_n \to G_{n+1}\}_{n \in \mathbb{N}}$$

where:

(1) each G_n is a commutative finite locally free S-group scheme, killed by p^n, and flat when viewed as a sheaf of $\mathbb{Z}/p^n\mathbb{Z}$-modules;

(2) each $i_n : G_n \to G_{n+1}$ is a homomorphism of S-group schemes, inducing an isomorphism $G_n \xrightarrow{\sim} G_{n+1}[p^n]$.

Definition 10.10. A homomorphism of p-divisible groups are defined to be the homomorphisms of inductive systems of group schemes.

Lemma 10.11. *Let S be a scheme. Let p be a prime number. If H is an fppf sheaf of $\mathbb{Z}/p^n\mathbb{Z}$-modules on S then the following are equivalent:*

(1) H is flat as a sheaf of $\mathbb{Z}/p^n\mathbb{Z}$-modules.

(2) $\mathrm{Ker}(p^i) = \mathrm{Im}(p^{n-i})$ for all $i \in \{0, 1, \cdots, n\}$.

Proof. For (1)⇒(2): consider the exact sequence

$$\mathbb{Z}/p^n\mathbb{Z} \xrightarrow{p^{n-i}} \mathbb{Z}/p^n\mathbb{Z} \xrightarrow{p^i} \mathbb{Z}/p^n\mathbb{Z}$$

If H is flat, then by tensor H we obtain a new exact sequence

$$H \xrightarrow{p^{n-i}} H \xrightarrow{p^i} H$$

and we see that (2) holds.

∎

Proposition 10.12. *The morphisms i_n give identifications $G_m \xrightarrow{\sim} G_{m+n}[p^m]$, thus we may treat G_m as the subgroup scheme of G_{m+n}.*

The morphism $[p^m] : G_{m+n} \to G_{m+n}$ then can be factored as $p^m : G_{m+n} \to G_{m+n}[p^n] \subseteq G_{m+n}$. Then there is an induced morphism $p^m : G_{m+n} \to G_m$.

By the above lemma, the sequence

$$0 \to G_m \xrightarrow{i_{m,n}} G_{m+n} \xrightarrow{p^m} G_n \to 0$$

is exact.

Definition 10.13. By the above proposition, there is a limit

$$G = \lim_{\to} G_n$$

in the category of fppf sheaves of Abelian groups. Then G_n can be treated as $G[p^n]$.

If $\{G_n\}$ and $\{H_n\}$ are two p-divisible groups, $G = \lim_{\to} G_n$ and $H = \lim_{\to} H_n$, then the homomorphisms from $\{G_n\}$ and $\{H_n\}$ are just the homomorphisms from G to H as fppf sheaves.

Proposition 10.14. *By passing from the inductive system $\{G_n\}$ to the limit G we can identify the category of p-divisible groups over S as the full subcategory of the category of fppf sheaves in Abelian groups over S.*

An fppf sheaf G comes from a p-divisible if and only if it satisfies the following conditions:

(1) G is p-divisible, that is, $[p]_G$ is an epimorphism;

(2) G is p-torsion, that is, $G = \lim_{\rightarrow} G[p^n]$;

(3) the sub-sheaves $G[p^n]$ are representable by finite locally free S-group scheme.

Definition 10.15. If $G = \lim_{\rightarrow} G_n$ is a p-divisible group over a connected base scheme S, then by definition, G_1 is locally free and killed by p. Then the rank of G_1 equals to p^h for some h. The integer h is called the height of G. Then G_n has rank p^{nh}.

Over an arbitrary basis S, we define the height of a p-divisible group G as the locally constant function $|S| \to \mathbb{Z}_{\geq 0}$ given by $s \mapsto h(G(s))$.

Definition 10.16. Let X be an Abelian variety over a field k. Let p be a prime number. Then we define the p-divisible group of X, notation $X[p^\infty]$, to be the inductive system

$$\{X[p^n]\}_{n\geq 0}$$

with respect to the natural inclusion homomorphisms $X[p^n] \hookrightarrow X[p^{n+1}]$. The group $X[p^\infty]$ has height $2g$.

Proposition 10.17. A homomorphism $f : X \to Y$ of Abelian varieties over k induces a homomorphism $f[p^\infty] : X[p^\infty] \to Y[p^\infty]$ of p-divisible groups.

If f is an isogeny, then $f[p^\infty]$ is an epimorphism of fppf sheaves. If N is the kernel we find an exact sequence of fppf sheaves

$$0 \to N_p \to X[p^\infty] \xrightarrow{f[p^\infty]} Y[p^\infty] \to 0$$

where $N = N_p \times N^p$ with N_p of p-power order and N^p a group scheme with order prime to p.

Definition 10.18. By taking the Catier dual there is a new exact sequence

$$0 \to G_n^D \to G_{m+n}^D \to G_m^D \to 0$$

In particular, taking $m = 1$ this gives homomorphisms $\iota_n : G_n^D \to G_{n+1}^D$. Then the system $\{G_n^D : \iota^n\}$ is again a p-divisible group; it is called the Serre dual of G. It has the same height as G.

A homomorphism $f : G \to H$ induces a dual homomorphism $f^D : H^D \to G^D$.

Proposition 10.19. If X/k is an Abelian variety then we have a canonical isomorphism

$$X^t[p^\infty] \cong X[p^\infty]^D$$

Remark 10.20. *The definition of p-divisible group also makes sense for certain other commutative group varieties. For instance, for any k-algebra R,*

$$\mathbb{G}_m[p^\infty](R) = \{x \in R^* | x^{p^n} = 1 \textit{ for some } n\}$$

The height of $\mathbb{G}_m[p^\infty]$ is 1.

The dual of $\mathbb{G}_m[p^\infty]$ is the p-divisible group $\mathbb{Q}_p/\mathbb{Z}_p$.

Definition 10.21. Let G be a p-divisible group over k, viewed as an fppf sheaf, then we define the Tate p-module by $T_pG = \mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, G(\bar{k}))$.

10.3 The algebraic fundamental group

10.4 The fundamental group of an Abelian variety

We omit the proof of the following two theorems.

Theorem 10.22 (Serre-Lang)**.** Let X be an Abelian variety over a field k. Let Y be a k-variety and $e_Y \in Y(k)$. If $f : Y \to X$ is an etale covering with $f(e_Y) = e_X$ then Y has the structure of an Abelian variety such that f is a separable isogeny.

Corollary 10.23. Let X be an Abelian variety over a field k. Let Ω be an algebraically closed field containing k, and regard $0 = e_X$ as an Ω-valued point of X. Write k_s for the separable closure of k inside Ω. Then there are canonical isomorphisms

$$\pi_1^{\mathrm{alg}}(X_{k_s}, 0) \cong \varprojlim X[n](k_s) \cong \begin{cases} \prod_{\ell} T_\ell X, & \text{char } (k) = 0 \\ T_{p,\mathrm{et}} X \times \prod_{\ell \neq p} T_\ell X & \text{char } (k) = p \end{cases}$$

where the projective limit runs over all maps $X[nm](k_s) \to X[n](k_s)$ given by $P \mapsto m \cdot P$. Further there is a canonical isomorphism

$$\pi_1^{\mathrm{alg}}(X, 0) = \pi_1^{\mathrm{alg}}(X_{k_s}, 0) \rtimes \mathrm{Gal}(k_s/k)$$

Corollary 10.24. Let X be an Abelian variety over a field k, let $k \subseteq k_s$ be a separable algebraic closure, and let ℓ be a prime number with $\ell \neq \text{char } (k)$. Then we have

$$H^1(X_{k_s}, \mathbb{Z}_\ell) \cong (T_\ell X)^\vee = \mathrm{Hom}(T_\ell X, \mathbb{Z}_\ell)$$

as $\mathbb{Z}_\ell$-modules with continuous actions of $\mathrm{Gal}(k_s/k)$. Further we have an isomorphism of graded-commutative $\mathbb{Z}_\ell$-algebras with continuous $\mathrm{Gal}(k_s/k)$-action

$$H^\bullet(X_{k_s}, \mathbb{Z}_\ell) \cong \bigvee^{\bullet}[(T_\ell X)^\vee]$$

11 Polarizations and Weil pairings

11.1 Polarizations

Proposition 11.1. Let X be an Abelian variety. Let $\lambda : X \to X^t$ be a homomorphismm and consider the line bundle $M = (id, \lambda)^* \mathscr{P}_X$ on X. Then $\varphi_M = \lambda + \lambda^t$.

Proof. First we consider the map

$$\varphi_{\mathscr{P}} : X \times X^t \to X^t \times X^{tt}$$

it sends (x, ϵ) to the line bundle $L = [t^*_{x,\epsilon} \mathscr{P} \otimes \mathscr{P}^{-1}]$. We claim that it is exactly the point $(\epsilon, \kappa(x))$. It is sufficient to prove for $(x, 0)$ and $(0, \epsilon)$. Since $\mathscr{P}|_{X \times \{0\}} \cong \mathcal{O}_X$, the sheaf $L|_{X \times \{0\}} = [\mathcal{O}_X] \in X^t$, which corresponds to the point 0 as a scheme. Since $\mathscr{P}|_{\{0\} \times X^t} \cong \mathcal{O}_{X^t}$, we have $L|_{\{0\} \times X^t} \cong [\mathcal{O}_{X^t}] \in X^{tt}$, which corresponds to the point $0 \in X^{tt}$. Thus the claim holds true.

Then $\varphi_M = (id, \lambda) \circ \varphi_{\mathscr{P}} \circ (id, \lambda)^t$ sends x to $\lambda(x) + \lambda^t(x)$. ∎

Proposition 11.2. Let X be an Abelian variety over a field k. Let $\lambda : X \to X^t$ be a homomorphism. Then the following properties are equivalent:

(a) λ is symmetric;

(b) there exists a field extension $k \subseteq K$ and a line bundle L on X_K such that $\lambda_K = \varphi_L$;

(c) there exists a finite separable field extension $k \subseteq K$ and a line bundle L on X_K such that $\lambda_K = \varphi_L$.

Proof. ■

Corollary 11.3. Let X/k be an Abelian variety. Then the homomorphism $\psi : \mathrm{NS}_{X/k} \to \mathrm{Hom}^{\mathrm{sym}}(X, X^t)$ induced by $\varphi : L \mapsto \varphi_L$ is an isomorphism.

Proof. We already know it is an injective morphism. Since both group schemes are etale, we can check it on $\bar{k}$. ■

Corollary 11.4. Let X/k be an Abelian variety. Let $\lambda : X \to X^t$ be a symmetric homomorphism, and write $M = (id, \lambda)^*\mathscr{P}_X$. Let $k \subseteq K$ be a field extension and let L be a line bundle on X_K with $\lambda_K = \varphi_L$.

(1) We have: λ is an isogeny $\iff$ L is non-degenerate $\iff$ M is non-degenerate.

(2) If λ is an isogeny, then L is effective if and only if M is effective.

(3) We have: L is ample if and only if M is effective.

Corollary 11.5. Let X/k be an Abelian variety. Let $\lambda : X \to X^t$ be a homomorphism. Then the following properties are equivalent:

(a) λ is a symmetric isogeny and the line bundle $(id, \lambda)^*\mathscr{P}$ on X is ample;

(b) λ is a symmetric isogeny and the line bundle $(id, \lambda)^*\mathscr{P}$ on X is effective;

(c) there exists a field extension $k \subseteq K$ and an ample line bundle L on X_K such that $\lambda_K = \varphi_L$;

(d) there exists a finite separable field extension $k \subseteq K$ and an ample line bundle L such that $\lambda_K = \varphi_L$.

Definition 11.6. Let X be an Abelian variety over a field k. A polarization of X is an isogeny $\lambda : X \to X^t$ that satisfies the equivalent conditions in the above corollary.

Since $\deg(\lambda) = \chi(L)$ if $\lambda_{\bar{k}} = \varphi_L$, the degree of a polarization is a square. If λ is an isomorphism, that is, λ has degree 1, we call it a principal polarization.

Remark 11.7. *Let X be an Abelian variety over a field k. We have an exact sequence of fppf sheaves*

$$0 \to X^t \to \mathrm{Pic}_{X/k} \to \mathrm{Hom}^{\mathrm{sym}}(X, X^t) \to 0$$

which gives a long exact sequence in fppf cohomology

$$0 \to X^t(k) \to \mathrm{Pic}(X) \to \mathrm{Hom}^{\mathrm{sym}}(X, X^t) \xrightarrow{\partial} H^1_{\mathrm{fppf}}(k, X^t) \to \cdots$$

Proposition 11.8. Let $f : X \to Y$ be an isogeny. If $\mu : Y \to Y^t$ is a polarization of Y, then $f^*\mu = f^t \circ \mu \circ f$ is a polarization of X of degree $\deg(f^*\mu) = \deg(f)^2 \cdot \deg(\mu)$.

Definition 11.9. Let X and Y be Abelian varieties over k. A divisorial correspondence between X and Y is a line bundle L on $X \times Y$ together with rigidification $\alpha : L_{\{0\}\times Y} \xrightarrow{\sim} \mathcal{O}_Y$ and $\beta : L_{X\times\{0\}} \xrightarrow{\sim} \mathcal{O}_X$ that coincide on the fibre over $(0,0)$.

The correspondences between X and Y form a group $\mathrm{Corr}_k(X,Y)$.

Proposition 11.10. Let X/k be an Abelian variety. Then we have a bijection

$$\{\text{polarizaions } \lambda : X \to X^t\} \xrightarrow{\sim} \begin{Bmatrix} \text{symmetric divisorial correspondences } (L,\alpha,\beta) \\ \text{on } X\times X \text{ such that } \Delta_X^* L \text{ is ample} \end{Bmatrix}$$

by associating to a polarization λ the divisorial correspondence (L,α,β) with $L = (id\times\lambda)^*\mathscr{P}_X$ and α,β the pull backs under $id\times\lambda$ of the rigidifications $\alpha_{\mathscr{P}}$ and $\beta_{\mathscr{P}}$.

11.2 Pairings

Definition 11.11. Let $f : X \to Y$ be an isogeny of Abelian varieties over a field k. Write $\beta : \mathrm{Ker}(f^t) \xrightarrow{\sim} \mathrm{Ker}(f)^D$ for the isomorphism.

(1) Define $e_f : \mathrm{Ker}(f)\times\mathrm{Ker}(f^t) \to \mathbb{G}_{m,k}$ to be the perfect bilinear pairing given by $e_f(x,y) = \beta(y)(x)$. If $f = n_X$, then we obtain a pairing

$$e_n : X[n]\times X^t[n] \to \mu_n$$

which we call the Weil pairing.

(2) Let $\lambda : X \to X^t$ be a homomorphism. We write

$$e_n^\lambda : X[n]\times X[n] \to \mu_n$$

for the bilinear pairing given by $e_n^\lambda(x_1,x_2) = e_n(x_1,\lambda(x_2))$. If $\lambda = \varphi_L$ we also write e_n^L instead of e_n^λ.

Proposition 11.12. Let $f : X \to Y$ be an isogeny of Abelian varieties.

(1) For any k-scheme T and points $x \in \mathrm{Ker}(f)(T)$ and $\eta \in \mathrm{Ker}(f^t)(T)$ we have $e_{f^t}(\eta,\kappa_X(x)) = e_f(x,\eta)^{-1}$

(2) Let $\beta_1 : \mathrm{Ker}(f^t) \xrightarrow{\sim} \mathrm{Ker}(f)^D$ and $\beta_2 : \mathrm{Ker}(f^{tt})^{DD} \xrightarrow{\sim} \mathrm{Ker}(f^t)^D$ be the canonical isomorphism, and let $\mathrm{Ker}(f)^{DD} \xrightarrow{\sim} \mathrm{Ker}(f)$ be the canonical isomorphism. Then the isomorphism $\mathrm{Ker}(f) \xrightarrow{\sim} \mathrm{Ker}(f^{tt})$ induced by κ_X equals $-\beta_1\circ\beta_1^D\circ\gamma^{-1}$.

11.3 Existence of polarizations, and Zarhin's trick

Proposition 11.13. Let $\lambda : X \to X^t$ be a symmetric isogeny, and let $f : X \to Y$ be an isogeny.

(1) There exists a symmetric isogeny $\mu : Y \to Y^t$ such that $\lambda = f^*\mu = f^t\circ\mu\circ f$ if and only if $\mathrm{Ker}(f)$ is contained in $\mathrm{Ker}(\lambda)$ and is totally isotropic with respect to the pairing $e_\lambda : \mathrm{Ker}(\lambda)\times\mathrm{Ker}(\lambda) \to \mathbb{G}_m$. If such an isogeny μ exists then it is unique.

(2) Assume that an isogeny μ as in (1) exists. Then μ is a polarization if and only if λ is a polarization.

Corollary 11.14. Let X be an isogeny over an algebraically closed field. Then X is isogenous to an Abelian variety that admits a principal polarization.

Theorem 11.15 (Zarhin's trick)**.** Let X be an Abelian variety over a field k. Then $X^4 \times (X^t)^4$ carries a principal polarization.

12 The endomorphism ring

12.1 First basic result about the endomorphism algebra

Remark 12.1. *Recall that the functor* $\mathrm{Hom}(X,Y) : \boldsymbol{Sch}_{/k} \to \boldsymbol{Gr}$ *sending* T *to* $\mathrm{Hom}_T(X_T, Y_T)$ *is represented by an etale commutative* k*-group scheme. If* $k = k_s$ *and* $K \supseteq k$*, the* k*-valued points* $\mathrm{Hom}_k(X,Y)$ *equals the* K*-valued points* $\mathrm{Hom}_K(X_K, Y_K)$*.*

Theorem 12.2 (Poincare Splitting Theorem)**.** Let X be an Abelian variety over a field k. If $Y \subseteq X$ is an Abelian subvariety, there exists an Abelian subvariety $Z \subseteq X$ such that the homomorphism $f : Y \times Z \to X$ given by $(y,z) \mapsto y + z$ is an isogeny.

Proof. Write $i : Y \hookrightarrow X$ for the inclusion. Choose a polarization $\lambda : X \to X^t$, and let

$$W = \mathrm{Ker}(X \xrightarrow{\lambda} X^t \xrightarrow{i^t} Y^t)$$

Note that the homomorphism $\lambda_Y = i^t \circ \lambda \circ i : Y \to Y^t$ is again a polarization. Then $\mathrm{Ker}(\lambda_Y) = Y \cap W$ is finite.

Now take $Z = W^0_{\mathrm{red}}$, this is indeed an Abelian variety with dimension $\dim W = \dim X - \dim Y$. Since the kernel of $f : Y \times Z \to X$ is contained in $(Y \cap Z) \times (Y \cap Z)$, it is finite, and then f is an isogeny. ■

Definition 12.3. A non-zero Abelian variety X over a field k is said to be simple if X has no Abelian subvarieties other than 0 and X.

Definition 12.4. We say that X is elementary if X is isogenous to a power of a simple Abelian variety, i.e., $X \sim_k Y^m$ for some $m \geq 1$ and Y simple.

Remark 12.5. *We sometimes use the terminology "k-simple" since an Abelian variety which is simple over* k *may not be simple over a field extension. But if* k *is separably closed, then* X_L *is simple for every extension* $L \supseteq k$*.*

Corollary 12.6. A non-zero Abelian variety over k is isogenous to a product of k-simple Abelian varieties.

Definition 12.7. Let k be a field. We define the category of Abelian varieties over k up to isogeny, denoted by $\mathbb{Q}\mathbf{AV}_{/k}$, to be the category with as objects Abelian varieties over k and with

$$\mathrm{Hom}_{\mathbb{Q}\mathbf{AV}_{/k}}(X,Y) = \mathrm{Hom}^0(X,Y) \triangleq \mathrm{Hom}_{\mathbf{AV}_{/k}}(X,Y) \otimes_{\mathbb{Z}} \mathbb{Q}$$

Definition 12.8. If X and Y are Abelian varieties over k then an element $f \in \mathrm{Hom}^0(X,Y)$ is called a quasi-isogeny if f is an isomorphism in the category $\mathbb{Q}\mathbf{AV}_{/k}$. An element $f \in \mathrm{Hom}^0(X,Y)$ is a quasi-isogeny of and only if there is a non-zero integer n such that nf is an isogeny from X to Y.

Corollary 12.9. If X is k-simple then $\mathrm{End}_k^0(X)$ is a division algebra. For X we have

$$\mathrm{End}_k^0(X) \cong M_{m_1}(D_1) \times \cdots \times M_{m_n}(D_n)$$

Lemma 12.10. Let X and Y be Abelian varieties over a field k, and let $f \in \mathrm{Hom}(X, Y)$.

(1) Let ℓ be a prime number, $\ell \neq \mathrm{char}\ (k)$. If $T_\ell(f) \in \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell X, T_\ell Y)$ is divisible by ℓ^m, then $f \in \mathrm{Hom}(X, Y)$ is divisible by ℓ^m.

(2) Let p be a prime number. If $f[p^\infty] \in \mathrm{Hom}(X[p^\infty], Y[p^\infty])$ is divisible by p^m then $f \in \mathrm{Hom}(X, Y)$ is divisible by p^m.

Proof. (1) We have f vanishes on $X[\ell^m](k_s)$. Note that this is etale, hence f factors through $[\ell^m]_X$.

(2) Similar with (1). ■

Proposition 12.11. Let X and Y be Abelian varieties over a field k.

(1) If ℓ is a prime number, $\ell \neq \mathrm{char}\ (k)$ then the $\mathbb{Z}_\ell$-linear map

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

given by $f \otimes c \mapsto c \cdot T_\ell(f)$ is injective and has a torsion-free cokernel.

(2) If p is a prime number, the $\mathbb{Z}_p$-linear map

$$\Phi : \mathrm{Hom}(X, Y) \otimes \mathbb{Z}_p \to \mathrm{Hom}(X[p^\infty], Y[p^\infty])$$

given by $f \otimes c \mapsto c\dot{f}[p^\infty]$ is injective and has a torsion-free cokernel.

Corollary 12.12. For any Abelian varieties X and Y over k, $\mathrm{Hom}(X, Y)$ is a free $\mathbb{Z}$-module of rank at most $4 \dim(X) \dim(Y)$.

Proof. This follows from that $\mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell X, T_\ell Y)$ is a free $\mathbb{Z}_\ell$-module of rank $4 \dim(X) \dim(Y)$ (note that $T_\ell X$ is a free $\mathbb{Z}_\ell$-module of rank $2 \dim(X)$). ■

Corollary 12.13. If X is a g-dimensional Abelian variety over a field k then its Neron-Severi group $\mathrm{NS}(X)$ is a free $\mathbb{Z}$-module at most $4g^2$.

Proof. We have a canonical isomorphism $\mathrm{NS}(X) \xrightarrow{\sim} \mathrm{Hom}^{\mathrm{sym}}(X, X^t)$. ■

Corollary 12.14. Let X and Y be Abelian varieties over a field k. Fix a separable algebraic closure $k \subseteq k_s$. Then there is a finite field extension $k \subseteq K$ inside k_s which is the smallest field extension over which all homomorphisms from X to Y are defined, by which we mean that K has the following properties:

(a) for any field extension $K \subseteq L$ we have $\mathrm{Hom}_K(X_K, Y_K) \xrightarrow{\sim} \mathrm{Hom}_L(X_L, Y_L)$;

(b) if Ω is a field containing k_s and $F \subseteq \Omega$ is a subfield with $k \subseteq F$ and $\mathrm{Hom}_F(X_F, Y_F) \xrightarrow{\sim} \mathrm{Hom}_\Omega(X_\Omega, Y_\Omega)$, then $K \subseteq F$.

Proof. The group scheme $\mathrm{Hom}(X, Y)$ is an etale group scheme. Then the theory is just the Galois descent. ■

12.2 The characteristic polynomial of an endomorphism

Definition 12.15. Let X be an Abelian variety of dimension g over a field k. If W is a $\mathbb{Q}$-vector space then a map $\gamma : \mathrm{End}(X) \to W$ is said to be homogeneous of degree m if $\gamma(n \cdot f) = n^m \cdot \gamma(f)$ for all $f \in \mathrm{End}(X)$ and all $n \in \mathbb{Z}$. Any homogeneous map γ naturally extends to a map $\gamma : \mathrm{End}^0(X) \to W$.

Proposition 12.16. The map $\deg : \mathrm{End}^0(X) \to \mathbb{Q}$ is a homogeneous polynomial map of degree $2g$. This means that if $e_1, \cdots, e_u$ is a basis for $\mathrm{End}^0(X)$ as a $\mathbb{Q}$-vector space, then there is a homogeneous polynomial $D \in \mathbb{Q}[t_1, \cdots, t_u]$ of degree $2g$ such that $\deg(c_1e_1 + \cdots + c_ue_u) = D(c_1, \cdots, c_u)$ for all $c_i \in \mathbb{Q}$.

Definition 12.17. Let X be an Abelian varieties over k. If $f \in \mathrm{End}^0(X)$ then by the proposition above there is a monic polynomial $P = P_f \in \mathbb{Q}[f]$ of degree $2g$ such that $P(n) = \deg([n]_X - f)$ for all $n \in \mathbb{Z}$. We call P the characteristic polynomial of f. If $P = \sum_{i=0}^{2g} a_i t^i$ then we define the trace of f by $\mathrm{tr}(f) = -a_{2g-1}$. Note that $a_0 = \deg(-f) = \deg(f)$, we also call it the norm of f.

Theorem 12.18. Let X be an Abelian variety over a field k. Let ℓ be a prime number different from char (k). For $f \in \mathrm{End}^0(X)$, let $P_{\ell,f} \in \mathbb{Q}_\ell[f]$ be the characteristic polynomial of $V_\ell f \in \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell X)$, that is, $P_{\ell,f}(t) = \det(t \cdot id - V_\ell f)$. Then $P_{\ell,f} = P_f$. In particular, the characteristic polynomial of $V_\ell f$ has coefficients in $\mathbb{Q}$ and is independent of ℓ.

Corollary 12.19. Let $f \in \mathrm{End}^0(X)$, then $P_f(f) = 0 \in \mathrm{End}^0(X)$

Proof. Since $P_{\ell,f}(V_\ell f) = 0 \in \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell X)$, and $P_{\ell,f}(V_\ell f) = P_f(V_\ell f) = V_\ell(P_f(f))$, then $P_f(f) = 0$. ■

Corollary 12.20. If $f \in \mathrm{End}(X)$ then P_f has integral coefficients.

Proof. Let $f \in \mathrm{End}(X)$. Because $\mathrm{End}(X)$ is finitely generated as an additive group, there is a monic polynomial $Q \in \mathbb{Z}[t]$ such that $Q(f) = 0$. Then $V_\ell(Q(f)) = Q(V_\ell f) = 0$. Thus all eigenvalues of $V_\ell f$ are algebraic integers. Hence $P_{\ell,f} = P_f$ has integral coefficients. ■

Corollary 12.21. For $f, g \in \mathrm{End}^0(X)$ we have the relations

$$\deg(fg) = \deg(f) \cdot \deg(g), \quad \mathrm{tr}(f+g) = \mathrm{tr}(f) + \mathrm{tr}(g), \quad \mathrm{tr}(fg) = \mathrm{tr}(gf)$$

12.3 The Rosati involution

Definition 12.22. Let $\lambda : X \to X^t$ be a polarization. Then for any $f \in \mathrm{End}^0(X)$ we can form the element $f^\dagger = \lambda^{-1} \circ f^t \circ \lambda : X \to X$. More explicitly, if $f = (1/m) \cdot g$, and assume that $\mu \circ \lambda = [n]_X$, then $f^\dagger = (1/mn)(\mu \circ g^t \circ \lambda) \in \mathrm{End}^0(X)$. The map $\dagger$ is an involution of the algebra $\mathrm{End}^0(X)$. It is called the Rosati involution associated with λ.

Proposition 12.23. If $\lambda, \mu : X \to X^t$ are two polarizations, then $\alpha \triangleq \lambda^{-1} \circ \mu \in \mathrm{End}^0(X)$. If $\ddagger$ is the Rosati involution of μ, then $f^\ddagger = \alpha^{-1} \circ f^\dagger \circ \alpha$.

Proposition 12.24. Since $\deg(f^\dagger) = \deg(f)$ and $[n]_X^\dagger = [n]_X$, we have $P_{f^\dagger} = P_f$. In particular, $\mathrm{tr}(f^\dagger) = \mathrm{tr}(f)$.

Lemma 12.25. Let X be an Abelian variety over a field k. Let ℓ be a prime number with $\ell \neq \mathrm{char}\ (k)$. Let $\lambda : X \to X^t$ be a homomorphism, and $\dagger$ the associated Rosati involution, and let $E^\lambda : V_\ell X \times X_\ell X \to \mathbb{Q}_\ell(1)$ the Riemann form of λ. Then for all $f \in \mathrm{End}(X)$ and all x, $y \in V_\ell X$ we have

$$E^\lambda(V_\ell f(x), y) = E^\lambda(x, V_\ell f^\dagger(y))$$

Proof. Let $E : V_\ell X \times X_\ell X^t \to \mathbb{Q}_\ell$ be the pairing such that $E^\lambda(x, y) = E(x, (V_\ell \lambda)(y))$.

Then

$$E^\lambda(x, V_\ell f^\dagger(y)) = E(x, (V_\ell\lambda \circ V_\ell f^\dagger)(y)) = E(x, V_\ell(\lambda \circ f^\dagger)(y)) = E(x, (V_\ell f^t \circ V_\ell \lambda)(y))$$

Recall that this equals to $E(V_\ell f(x), V_\ell \lambda(y)) = E^\lambda(V_\ell f(x), y)$. ∎

Proposition 12.26. Let X be an Abelian variety over a field k. Let λ be a polarization of X, and let $f \mapsto f^\dagger$ be the associated Rosati involution on $\mathrm{End}^0(X)$. Then the map $\mathrm{NS}(X) \to \mathrm{End}^0(X)$ sending $[M]$ to $\lambda^{-1} \circ \varphi_M$ induces an isomorphism of $\mathbb{Q}$-vector spaces

$$i : \mathrm{NS}(X) \times \mathbb{Q} \xrightarrow{\sim} \{f \in \mathrm{End}^0(X) | f = f^\dagger\}$$

In particular, the Picard number of X, that is, the rank of $\mathrm{NS}(X)$, equals the $\mathbb{Q}$-dimension of the space of $\dagger$-symmetric elements in $\mathrm{End}^0(X)$.

Proof. Recall that there is a natural isomorphism $\mathrm{NS}(X) \xrightarrow{\sim} \mathrm{Hom}^{\mathrm{sym}}(X, X^t)$, then

$$\mathrm{NS}(X) \otimes \mathbb{Q} \xrightarrow{\sim} \mathrm{Hom}^{0,\mathrm{sym}}(X, X^t)$$

Now consider the isomorphism $\mathrm{Hom}^0(X, X^t) \xrightarrow{\sim} \mathrm{End}^0(X)$ sending f to $\lambda^{-1} \circ f$, the image of f is $\dagger$-symmetric if and only if $f = f^t$. The result then follows. ∎

Theorem 12.27. Let X be an Abelian variety of dimension g over a field k. Let $\dagger$ be the Rosati involution associated with a polarization λ.

(1) If $\lambda = \varpi_L$ for some ample bundle L then for $f \in \mathrm{End}(X)$ we have

$$\mathrm{tr}(ff^\dagger) = 2g \cdot \frac{c_1(L)^{g-1} \cdot c_1(f^*L)}{c_1(L)^g}$$

(2) The bilinear form $\mathrm{End}^0(X) \times \mathrm{End}^0(X) \to \mathbb{Q}$ given by $(f, g) \mapsto \mathrm{tr}(f \cdot g^\dagger)$ is symmetric and positive definite.

Proof. (1)

(2) Reduce to the case $k = \bar{k}$. ∎

12.4 The Albert classification

13 The Fourier transform and the Chow ring (skip)

13.1 The Chow ring

Definition 13.1. Let X be a variety over a field k. The group $Z_r(X)$ of r-cycles on X is defined as the free Abelian group on the r-dimensional closed subvarieties on X. For $r = \dim(X) - 1$ an r-cycle is the same as a Weil divisor.

An r-cycle $\alpha \in Z_r(X)$ is said to be rationally equivalent to 0, denoted by $\alpha \sim 0$ or $\alpha \sim_{\text{rat}} 0$, if there exists $(r+1)$-dimensional subvarieties $W_1, \cdots, W_n$ of X and rational functions $f_i \in k(W_i)^*$ such that $\alpha = \sum_{i=1}^n \operatorname{div}(f_i)$. The cycles rationally equivalent to 0 form a subgroup $Rat_r(X)$ of $Z_r(X)$ and we define the Chow group of r-cycles to be the factor group

$$\mathrm{CH}_r(X) = Z_r(X)/Rat_r(X)$$

We set $\mathrm{CH}^r(X) = \mathrm{CH}_{\dim(X)-r}(X)$, this is called the Chow group of codimension r cycles.

Let $\mathrm{CH}^*(X) = \bigoplus_r \mathrm{CH}^r(X)$ and $\mathrm{CH}^*_{\mathbb{Q}}(X) = \mathrm{CH}^*(X) \otimes \mathbb{Z}\mathbb{Q}$. If X is a no-singular variety, there exists an intersection pairing

$$\mathrm{CH}^r(X) \times \mathrm{CH}^s(X) \to \mathrm{CH}^{r+s}(X) \to \mathrm{CH}^{r+s}(x)$$

which makes $\mathrm{CH}^*(X)$ to be a commutative graded ting with identity. This ring is called the Chow ring of X.

Proposition 13.2. Let $f : X \to Y$ be a morphism of k-varieties. Then we have a pull-back homomorphism $f^* : \mathrm{CH}^*(Y) \to \mathrm{CH}^*(X)$. If f is flat, then f^* is given by $f^*[V] = [f^{-1}(V)]$ for closed subvariety $V \subseteq Y$.

Remark 13.3. *Assume that $f : X \to Y$ is proper, and $V \subseteq X$ is a closed subvariety, then $W = f(V)$ is a closed subvariety of Y. If $\dim(W) = \dim(V)$, let $\deg(V/W)$ be the degree of the field extension $[k(V) : k(W)]$ defined by f, if $\dim(W) < \dim(V)$ let $\deg(V/W) = 0$. We set $f_*[V] = \deg(V/W) \cdot [W]$. Then f_* extends to a homomorphism $f_* : Z_r(X) \to Z_r(Y)$, which induces a homomorphism $f_* : \mathrm{CH}^r(X) \to \mathrm{CH}^r(Y)$.*

Further, we have the projection formula

$$f_*((f^*\eta) \cdot \epsilon) = \eta \cdot f_*\epsilon$$

If there is a Cartesian square

$$\begin{tikzcd} X' \arrow[r, "g"] \arrow[d, "f'"] & X \arrow[d, "f"] \\ Y' \arrow[r, "h"] & Y \end{tikzcd}$$

with h flat and f proper, then we have

$$f'_* g^* \alpha = h^* f_* \alpha$$

Remark 13.4. *Let X be a variety. Let $K^0(X)$ be the Grothendieck group of vector bundles on X. Then $K^0(X)$ has a natural structure of a commutative ring, with product $[E_1]\cdot[E_2] = [E_1 \otimes E_2]$. Let $K_0(X)$ be the Grothendieck group of coherent sheaves on X. Then $K_0(X)$ has a natural structure of a $K^0(X)$-module, by $[E]\cdot[F] = [E \otimes_{\mathcal{O}_X} F]$. If $f : X \to Y$ is a morphism of varieties then we have a natural ring homomorphism $K^0(Y) \to K^0(X)$. If f is proper then we have a homomorphism $f_* : K_0(X) \to K_0(Y)$ given by $f_*[F] = \sum_{i\geq 0}(-1)^i[R^i f_* F]$.*

If X is nonsingular, there is a natural homomorphism $K^0(X) \to K_0(X)$. This is in fact an isomorphism (see Hartshorne ex III.6.9). Then we may write $K(X)$ for $K^0(X)$.

Definition 13.5. There is a ring homomorphism

$$\mathrm{ch} : K(X) \to \mathrm{CH}^*_{\mathbb{Q}}(X)$$

called the Chern character. For a line bundle L with associated divisor class $\ell = c_1(L) \in \mathrm{CH}^1_{\mathbb{Q}}(X)$, it is given by

$$[L] \mapsto e^{\ell}$$

(note that e^{ℓ} only involves a finite sum, as $\mathrm{CH}^i(X) = 0$ for $i > \dim(X)$). Further this gives an isomorphism

$$K_{\mathbb{Q}}(X) \to \mathrm{CH}^*_{\mathbb{Q}}(X)$$

If $f : X \to Y$ is a morphism between non-singular varieties then the Chern character commutes with f^*, that is, $f^*(\mathrm{ch}(\alpha)) = \mathrm{ch}(f^*(\alpha))$ for $\alpha \in K(Y)$.

Definition 13.6. Let X and Y be nonsingular varieties. Elements in $\mathrm{CH}^*_{\mathbb{Q}}(X \times Y)$ are called correspondences from X to Y. For a correspondence $\xi \in \mathrm{CH}^*_{\mathbb{Q}}(X \times Y)$ the transpose correspondence ${}^t\xi = s_*(\xi)$, where $s : X \times Y \to Y \times X$ is the morphism reversing the factors.

Assume Y is complete. If Z is a third non-singular variety then we can compose correspondences: Given $\varphi \in \mathrm{CH}^*_{\mathbb{Q}}(X \times Y)$ and $\psi \in \mathrm{CH}^*_{\mathbb{Q}}(Y \times Z)$ we define their composition, which is a correspondence from X to Z, by

$$\psi \circ \varphi = p_{XZ,*}(p^*_{XY}(\varphi) \cdot p^*_{YZ}(\psi)) \in \mathrm{CH}^*_{\mathbb{Q}}(X \times Z)$$

Here p_{XY} denotes the projection $X \times Y \times Z \to X \times Y$. We have ${}^t(\psi \circ \varphi) = {}^t\varphi \circ {}^t\psi$.

If $f : X \to Y$ is a morphism with graph map $\gamma_f : X \to X \times Y$, then the correspondence $\Gamma_f = [\gamma_f(X)]$ in $\mathrm{CH}^*_{\mathbb{Q}}(X \times Y)$ is called the graph correspondence of f. Note that $\Gamma_f = \gamma_{f,*}([X])$, then $\Gamma_{gf} = \Gamma_g \circ \Gamma_f$.

Assume that X is complete. A correspondence Γ from X to Y gives rise to a homomorphism of groups $\gamma : \mathrm{CH}^*(X) \to \mathrm{CH}^*(Y)$ by

$$\gamma(\alpha) = p_{Y,*}(p^*_X(\alpha) \cdot \Gamma)$$

If $\Gamma = \Gamma_f$ then $\gamma = f_*$. If $\Gamma = {}^t\Gamma_f$ then $\gamma = f^*$.

Lemma 13.7. Let S be a smooth quasi-projective k-scheme. Let $\mathscr{V}(S)$ be the category of smooth projective S-schemes. If we are given S-morphisms $f : X \to Y$ and $g : Y \to Z$, with classes $\alpha \in \mathrm{CH}^*_{\mathbb{Q}}(X \times_S Y)$ and $\beta \in \mathrm{CH}^*_{\mathbb{Q}}(Y \times_S Z)$. Then we have

$$[\Gamma_g] \circ \alpha = (id_X \times g)_*(\alpha) \quad \beta \circ [\Gamma_f] = (f \times id_Z)^*\beta$$

similarly, if $f' : Y \to X$ and $g' : Z \to Y$ are also morphisms in $\mathscr{V}(S)$ then

$$[{}^t\Gamma_{g'}] \circ \alpha = (id_X \times g')^*(\alpha) \quad \beta \circ [{}^t\Gamma_{f'}] = (f' \times id_Z)_*(\beta)$$

14 Jacobian Varieties (skip)

15 Dieudonne theory

15.1 Dieudonne theory for finite commutative group schemes and for p-divisible groups

Definition 15.1. Let R be a commutative ring with identity. Let α be an endomorphism of R. If M_1 and M_2 are (left) R-modules then by an α-linear map $f : M_1 \to M_2$ we mean an additive map with the property that $f(rm) = \alpha(r) \cdot f(m)$ for all $r \in R$ and $m \in M_1$. Such a map is also called a semi-linear map with respect to α.

Remark 15.2. *Consider the module $M_1^{(\alpha)} = R \otimes_{R,\alpha} M_2$ obtained by α. Then an α-linear map $f : M_1 \to M_2$ gives rise to an R-linear homomorphism $f^\sharp : M_1^\alpha \to M_2$ via $f^\sharp(r \otimes m) = r \cdot f(m)$. Conversely, for a R-homomorphism $g : M_1^{(\alpha)} \to M_2$ we can associate the α-linear map $g^\flat : M_1 \to M_2$ defined by $g^\flat(m) = g(1 \otimes m)$. Further, we have*

$$(f^\sharp)^\flat = f, \quad (g^\flat)^\sharp = g$$

Definition 15.3. The skew polynomial ring $R[t; \alpha]$ is the group $R[t]$ equipped the multiplicative operator as

$$t \cdot r = \alpha(r) \cdot t, \quad \forall r \in R$$

In other words, the variable t does not commute with the coefficients but is "α-linear".

Definition 15.4. For the definitions or properties of Dieudonne modules, you can see my note on Demazure's famous book "p-divisible groups".

15.2 Classification up to isogeny

Remark 15.5. *Throughout this section, k denotes a perfect field of characteristic $p > 0$. We write $W = W(k)$ for its ring of Witt vectors, L for the fraction field of W, and σ for the automorphism of W (and also of L) induced by the Frobenius automorphism $x \mapsto x^p$ of k.*

Definition 15.6. If N is a finite dimensional L-vector space, by a W-lattice in L we mean a W-submodule $M \subseteq N$ such that the natural map $M \otimes_W L \to N$ is an isomorphism. (Equivalent: M is free of rank $\dim_L(N)$ as a W-module.)

If M_1 and M_2 are W-lattices in N then so are $M_1 + M_2$ and $M_1 \cap M_2$. We define

$$\chi(M_1 : M_2) = \text{length}_W(M/M_2) - \text{length}_W(M/M_1)$$

where M is any W-lattice in N containing both M_1 and M_2.

Definition 15.7. A pair (N,F) is called an F-isocrystal over k, if N is a finitely-dimensional L-vector space and F is a bijective σ-linear operator $F: N \to N$.

Definition 15.8. Let $a \in \mathbb{Z}$. Then a σ^a-F-crystal over k is a pair (M,F) consisting of a free W-module M of finite rank, together with a σ^a-linear injective map $F: M \to M \otimes_W L$.

A morphism of σ^a-F-crystals $f:(M_1,F_1) \to (M_2,F_2)$ is a homomorphism $f: M_1 \to M_2$ of W-modules (so a W-linear map) such that $f \circ F_1 = F_2 \circ f$. We denote by σ^a-F-$\mathbf{Crys}_{/\mathrm{k}}$ the category of σ^a-F-crystals over k that is thus obtained.

The map F is not required to take values in M it self; it is allowed to have "denominators". If $F(M) \subseteq M$ then we say that the crystal is effective. The condition F is injective implies that the induced map $M \otimes_W L \to M \otimes_W L$ is bijective. We shall use the notation $M_{\mathbb{Q}} = M \otimes_W L = M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = M \otimes_{\mathbb{Z}} \mathbb{Q}$.

Remark 15.9. *If $a=0$ then a σ^a-F-crystal is of course just a finite free W-module M together with a linear injective map $M \to M_{\mathbb{Q}}$.*

If $a=1$ then by an F-crystal we mean a σ-F-crystal, then we write F-$\boldsymbol{Crys}_{/\mathrm{k}}$ for σ-F-$\boldsymbol{Crys}_{/\mathrm{k}}$.

Proposition 15.10. The category $\mathbf{DM}_{/\mathrm{k}}^{\mathrm{free}}$ of torsion-free Dieudonne modules is equivalent to the full subcategory of F-$\mathbf{Crys}_{/\mathrm{k}}$ consisting of all F-crystal (M,F) with $p \cdot M \subseteq F(M) \subseteq M$.

Proof. Since $F(M)$ is of the same dimension with M, pM, F must be injective. As a result, we can define $V = F^{-1}p$. Thus, the Dieudonne ring $\mathbb{D}$ acts on M naturally. We can also verify that this action is torsion-free. ∎

Definition 15.11. A homomorphism of σ^a-F-crystals $f:(M_1,f_1) \to (M_2,f_2)$ is called an isogeny if the induced map $M_{1,\mathbb{Q}} \to M_{2,\mathbb{Q}}$ is bijective. Thus if one wants to study σ^a-F-crystals only up to isogeny, it suffices to know the L-vector space $M_{\mathbb{Q}}$ together with its σ^a-linear Frobenius.

Definition 15.12. Let $a \in \mathbb{Z}$. Then a σ^a-F-isocrystal over k is a pair (N,F) consisting of an L-vector space N of finite dimension, together with a bijective, σ^a-linear endomorphism $F: N \to N$.

A morphism of F-isocrystals $f:(N_1,F_1) \to (N_2,F_2)$ is an L-linear map $f: N_1 \to N_2$ such that $f \circ F_1 = F_2 \circ f$. We denote by σ^a-F-$\mathbf{Isoc}_{/\mathrm{k}}$ the category of σ^a-F-isocrystals over k that is thus obtained.

Proposition 15.13. If (M,F) is a σ^a-F-crystal then $(M_{\mathbb{Q}},F)$ is a σ^a-F-isocrystal. In the other direction, if (N,F) is a σ^a-F-isocrystal then for any W-lattice $M \subseteq N$ the pair $(M,F_{|M})$ is a σ^a-F-crystal.

Remark 15.14. *The category σ^a-F-$\boldsymbol{Isoc}_{/\mathrm{k}}$ is Abelian. The category σ^a-F-$\boldsymbol{Crys}_{/\mathrm{k}}$ is additive but not Abelian. Further, if (M,F) is a σ^a-F-crystal and $M' \subseteq M$ is a primitive W-submodule that is stable under F then M/M' with Frobenius induced by F is again a σ^a-F-crystal. Here we recall that a W-submodule $M' \subseteq M$ is called primitive if M/M' is torsion-free.*

Definition 15.15. Let (M,F) be a σ^a-F-crystal over k. The rank of M as a W-module is called the height of (M,F). Similarly, the height of a σ^a-F-isocrystal (N,F) is defined as the L-dimension of the underlying vector space N.

Writing $N = M_{\mathbb{Q}}$ we have that M and $F(M)$ are both W-lattices in N. Hence there exists integers $r < R$ such that $p^R \cdot M \subseteq F(M) \subseteq p^r \cdot M$, and we can define $\mathrm{ord}(F)$, the p-adic order of F, by

$$\mathrm{ord}(F) = \max\{r \in \mathbb{Z} | F(M) \subseteq p^r \cdot M\}$$

Definition 15.16. Let (M, F) be a σ^a-F-crystal of height h over k. By the theory of modules over a PID there exists ordered W-bases $\{e_1, \cdots, e_h\}$ and $\{f_1, \cdots, f_h\}$ for M, together with integers $r_1 \leq r_2 \cdots \leq r_h$, such that $F(e_i) = p^{r_i} \cdot f_i$ for all i. The sequence of integers r_i does not depend on the chosen bases. The polygon defined by this sequence is called the Hodge polygon of (M, F). We shall denote the Hodge slopes of (M, F) by $\mu_1 < \mu_2 < \cdots < \mu_t$, let $h_i = h_i(M, F)$ be the multiplicity of $i \in \mathbb{Z}$ as Hodge slope, the numbers are called the Hodge numbers. The definition of slopes and multiplicities can be seen in the following remark.

Remark 15.17 (How to draw a graph)**.** *A polygon is given by a finite sequence of rational numbers $r_1 \leq r_2 < \cdots \leq r_n$. One can also describe it by giving a strictly increasing sequence $\lambda_1 < \lambda_2 < \cdots < \lambda_t$ together with multiplicities $m_1, m_2, \cdots, m_t$ (in $\mathbb{Z}_{>0}$), where the λ_j are the values that occur in the sequence of r_i, and m_j is the number of times that λ_j occurs.*

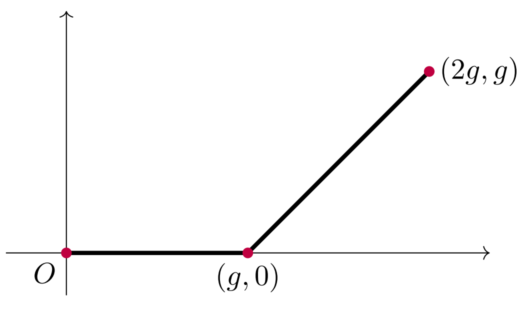
The numbers λ_j are called the slopes of the polygon. In practice it is often convenient to have a graphical representation of a polygon. For this we consider the graph of the piecewise linear continuous function $\phi : [0, n] \to \mathbb{R}$ that has $\phi(0) = 0$ and $\phi(i) = r_1 + r2 + \cdots + r_i$ for $1 \leq i \leq n$, and that is extended linearly between consecutive integers. In terms of the slopes λ_i this means that ϕ is linear with slope λ_j on the interval $[m_1 + \cdots + m_{j-1}, m_1 + \cdots + m_j]$.

Remark 15.18. *Note that, all slopes of the Hodge polygon are integers. The smallest Hodge slope, $\mu_1 = r_1 = \mathrm{ord}(F)$, is the largest integer r such that $F(M) \subseteq p^r \cdot M$, and we can recognize this as the integer the integer defined previously. The largest Hodge slope, r_h, is the smallest integer s such that $p^s \cdot M \subseteq F(M)$.*

Example 6. Let G be a p-divisible group over a perfect field k of characteristic p. We define the Hodge polygon of G to be the Hodge polygon of its Dieudonne module. The only slopes that can occur are 0 and 1, say with multiplicities h_0 and h_1. We have $h_0 + h_1 = h$, the height of G, and $h_1 = \dim(G)$. In particular, since the Dieudonne module of $X[p^\infty]$ is equal to

$$M(X[p^\infty]) = \lim_{\leftarrow} M(X[p^n]) = \lim_{\leftarrow,n} (\lim_{\rightarrow,m} \mathrm{Hom}_K(X[p^n], W_m)) = \lim_{\leftarrow,n} \left((W(k)/p^n W(k))^{2g}\right) = W(k)^{2g}$$

the Hodge polygon of an Abelian variety X of dimension g is the polygon



with g times slope 0 and g times slope 1.

Lemma 15.19. Let k be a perfect field of characteristic p.

(1) Let (M, F) be a σ^a-F-crystal of height h over k. Then for all $n \in \mathbb{N}$ we have

$$\operatorname{ord}(F) \le \frac{\operatorname{ord}(F^n)}{n} \le \frac{\operatorname{ord}\det(F)}{h}$$

(2) Let (N, F) be a σ^a-F-crystal over k. For any W-lattice $M \subseteq N$ the limit

$$\lim_{n\to\infty} \frac{\operatorname{ord}(F_M^n)}{n}$$

exists, and the limit is independent of the choice of the lattice M.

Proof. (1) ■

Definition 15.20. Let (N, F) be a σ^a-F-isocrystal over k. Then we define the first Newton slope of (N, F), notation $\lambda_1 = \lambda_1(N, F)$, to be the number $\lim_{n\to\infty} \operatorname{ord}(F_M^n)/n$, where $M \subseteq N$ is any W-lattice. We will prove that the first Newton slope is a rational number. For a σ^a-F-crystal we let $\lambda_1(M, F) = \lambda_1(M_{\mathbb{Q}}, F)$.

By the above lemma, we have $\mu_1(M, F) \le \lambda_1(M, F) \le \dfrac{\operatorname{ord}\det(F)}{h}$. If $h = 1$, then $\mu_1(M, F) = \lambda_1(M, F)$.

Lemma 15.21. Let (N, F) be a σ^a-F-isocrystal over k. Then we have $\lambda_1(N, p^m F^n) = n \cdot \lambda_1(N, F) + m$ for all $m, n \in \mathbb{Z}$.

Lemma 15.22. Let (N, F) be a σ^a-F-isocrystal of height h over k.

(1) If there exists a W-lattice $M \subseteq N$ such that $F^{h+1}(M) \subseteq p^{-1} \cdot M$, then (N, F) is effective.

(2) Let r, s be integers with $s > 0$ and $\lambda_1(N, F) \ge r/s$. Then there exists a W-lattice $M \subseteq N$ with $F^s(M) \subseteq p^r(M)$.

Proof. (1) Let $M' = M + F(M) + \cdots + F^h(M)$, which is again a W-lattice in N. We have $\sum_{j=0}^{h+1} F^j(M')$ is exactly the space containing $M, F(M), \cdots, F^{2h+1}(M)$. Thus,

$$\sum_{j=0}^{h+1} F^j(M') = \sum_{j=0}^{2h+1} F^j(M) = M' + \sum_{j=0}^{h} (F^{h+1}(M)) \subseteq p^{-1} \cdot M'$$

Now consider the ascending chain

$$M' \subseteq M' + F(M') \subseteq \cdots \subseteq \sum_{j=0}^{h+1} F^j(M') \subseteq p^{-1} \cdot M'$$

As $p^{-1}M'/M'$ is a k-vector space of dimension h, there exists an index $n \in \{0, 1, \cdots, h\}$ with $\sum_{j=0}^{n} F^j(M') = \sum_{j=0}^{n+1} F_j(M')$. Then $M'' = \sum_{j=0}^{n} F_j(M')$ is a lattice with $F(M'') \subseteq M''$, so (N, F) is effective.

(2) Let $F' = p^{1-r(h+1)} F^{s(h+1)}$. We have $\lambda_1(N, F') = s(h+1)\lambda_1(N, F) + 1 - r(h+1) \ge 1$. Hence by the definition of λ_1 for any W-lattice $M \subseteq N$ there exists an $n \in \mathbb{N}$ such that $\operatorname{ord}((F'_M)^n) \ge n$, that is, $(F'_M)^n(M) \subseteq M$. Let $M' = M + F'(M) + \cdots + (F')^{n-1}(M)$. Clearly, $F'(M') \subseteq M'$. Thus $(p^{-r}F^s)^{h+1}(M') \subseteq p^{-1} \cdot M'$. Hence by (1) there exists a W-lattice $M'' \subseteq N$ such that $p^{-r}F^s(M'') \subseteq M''$. ■

Proposition 15.23. Let (N,F) be a σ^a-F-isocrystal of height h over k. Let $d = \operatorname{ord}\det(F)$. Then there exists integers r,s with $0 < s \le h$ and $r \le d$ and a W-lattice $M \subseteq N$ such that $\lambda_1(N,F) = \dfrac{r}{s}$ and $\operatorname{ord}(F_M^s) = r$. In particular, $\lambda_1 \in \mathbb{Q}_{\le \frac{d}{h}}$.

Proof. We can choose integers r,s such that $s \in [1,h]$ and

$$|\lambda_1 - \frac{r}{s}| \le \frac{1}{s(h+1)}$$

Let $F' = p^{-r}F^s$. Thus $|\lambda_1(N,F')| = |s\lambda_1(N,F) - r| \le \dfrac{1}{h+1}$. By the above lemma (2), the inequality $\lambda(N,F') \ge -\dfrac{1}{h+1}$ implies that there exists a W-lattice $M' \subseteq N$ with $(F')^{h+1}(M') \subseteq p^{-1}\cdot M'$. Thus by (i) from the above lemma, there exists a W-lattice $M \subseteq N$ with $F'(M) \subseteq M$. Thus, $\lambda_1(N,F') \ge \operatorname{ord}(F') \ge 0$. By the same argument for $F'' = (F')^{-1}$, we have $\lambda_1(N,F') = 0$. Then $\operatorname{ord}(F'_M) = 0$ and $\lambda_1(N,F) = \dfrac{r}{s}$. And further $\operatorname{ord}((F'_M)^s) = r$. ■

Corollary 15.24. With the same hypothesis above, if there exists integers r and $s > 0$ and a lattice $M \subseteq N$ with $F^s(M) = p^r \cdot M$ then $\lambda_1(N,F) = \dfrac{r}{s} = \dfrac{d}{h}$ and $F^h(M) = p^d \cdot M$. Conversely, if $\lambda_1(N,F) = \dfrac{d}{h}$ then there exists a lattice $M \subseteq N$ such that $F^h(M) = p^d \cdot M$.

Definition 15.25. An F-isocrystal (N,F) is called isoclinic if there exists a W-lattice $M \subseteq N$ and integers r and $s > 0$ such that $F^s(M) = p^r \cdot M$; the quotient r/s is then called the slope of (N,F).

Proposition 15.26. Let k be a perfect field of characteristic p.

(1) If (N,F) is an isoclinic σ^a-F-isocrystal over k then any sub-isocrystal and quotient-isocrystal is isoclinic too, of the same slope.

(2) If (N_1,F_1) and (N_2,F_2) are isoclinic σ^a-F-isocrystals over k of different slopes then

$$\operatorname{Hom}_{\sigma^a-F-\mathbf{Isoc}_{/\mathrm{k}}}((N_1,F_1),(N_2,F_2)) = 0$$

(3) Given a σ^a-F-isocrystal (N,F) over k and one of its slopes $\lambda \in \mathbb{Q}$, there exists a unique maximal sub-isocrystal of (N,F) that is isoclinic of slope λ.

Example 7. Let $\lambda \in \mathbb{Q}$ and write $\lambda = d/h$ with $h > 0$ and $\gcd(d,h) = 1$. Define, for $a \in \mathbb{Z}\backslash\{0\}$, a σ^a-F-crystal $\mathscr{M}_\lambda$ over k by taking $\mathscr{M}_\lambda = W\cdot e_1 \oplus \cdots \oplus W \cdot e_h$ with

$$F(e_i) = \begin{cases} e_{i+1}, & 1 \le i < h \\ p^d, & i = h \end{cases}$$

In terms of modules over the ring $W[F] = W[F;\sigma^a]$ we can also say that we take $\mathscr{M}_\lambda = W[F]/W[F]\cdot(F^h - p^d)$. It is clear that $F^h = p^d$ on $\mathscr{M}_\lambda$, so $\mathscr{M}_\lambda$ is isoclinic of slope λ.

It follows from the above proposition (1) that, for any sub-isocrystal $\mathscr{N}'_\lambda \subseteq \mathscr{N}_\lambda = \mathscr{M}_\lambda \otimes_W L$, $\mathscr{N}'$ is isoclinic of the slope d/h. This means $d'/h' = d/h$. But $\gcd(d,h) = 1$ and $h' \le h$, then $d' = d, h' = h$. Hence $\mathscr{N}_\lambda$ is a simple isocrystal.

Theorem 15.27 (slope decomposition)**.** Let (N,F) be a σ^a-F-isocrystal over a perfect field k of characteristic p. For $\lambda \in \mathbb{Q}$ let (N_λ, F) be the maximal sub-isocrystal that is isoclinic of slope λ. Then we have a decomposition of σ^a-F-isocrystals $(N,F) = \bigoplus_{\lambda\in\mathbb{Q}}(N_\lambda, F)$.

Definition 15.28. Let (N, F) be a σ^a-F-isocrystal over k. We define the Newton polygon of (N, F) to be the polygon whose slopes are the numbers $\lambda \in \mathbb{Q}$ with $N_\lambda \neq 0$, and where we take each λ with multiplicity m_λ equal to the height of (N_λ, F) (i.e. the L-dimension of N_λ).

If (M, F) is a σ^a-F-crystal then we define its Newton polygon to be the Newton polygon of the associated isocrystal $(M_{\mathbb{Q}}, F)$.

Note that $\operatorname{ord}(\bigoplus(M_\lambda, F)) = \min_{\lambda\in\mathbb{Q}}(\operatorname{ord}(M_\lambda, F)) = \min(\lambda_1(N_\lambda, F))$, then $\lambda_1(N, F)$ is exactly the minimal Newton slope.

Lemma 15.29. Let k be an algebraically closed field of characteristic p. Let $v \in \mathbb{Z}\backslash\{0\}$, and write $\mathscr{F} \subseteq k$ be the unique sub-field with $p^{|v|}$ elements.

(1) Let V be a finite dimensional k-vector space, and let $\varphi : V \to V$ be a bijective Frob_k^v-linear map. Further let $V_0 = \{v \in V | \varphi(v) = v\}$, which is an $\mathscr{F}$-subspace of V. Then the natural map $k \otimes_{\mathscr{F}} V_0 \to V$ is an isomorphism.

(2) Let M be a free $W(k)$-module of finite rank, and let $F : M \to M$ be a bijective σ^v-linear map. Further let $M_0 = \{m \in M | F(m) = m\}$, which is an $W(\mathscr{F})$-submodule of M. Then the natural map $W(k) \otimes_{W(\mathscr{F})} M_0 \to M$ is an isomorphism.

Theorem 15.30 (Dieudonne)**.** Let $k = \bar{k}$ be an algebraically closed field of characteristic p, and let $a \in \mathbb{Z}\backslash\{0\}$. Then the category σ^a-F-$\mathbf{Isoc}_{/\mathrm{k}}$ is semisimple. The simple objects are the isocrystals N_λ, for $\lambda \in \mathbb{Q}$. If (N, F) is any σ^a-F-isocrystal over k then we have

$$(N, F) \cong \bigoplus_{\lambda\in\mathbb{Q}} \mathscr{N}_\lambda^{\oplus \frac{m_\lambda}{h(\lambda)}}$$

here $h(\lambda)$ is the height of $\mathscr{N}_\lambda$ and where $m_\lambda = \dim_L(N_L) \in \mathbb{Z}_+$ is the multiplicity of λ as a Newton slope of (N, F).

Remark 15.31. *This statements in the theorem do not hold for $a = 0$.*

Theorem 15.32 (Newton is over Hodge)**.** Let (M, F) be a σ^a-F-crystal of height h over k. Then the Newton polygon of (M, F) lies on or above its Hodge polygon, and the two polygons have the same begin point, namely $(0, 0)$, and end point, namely $(h, \operatorname{ord}\det(F))$.

15.3 The Newton polygon of an Abelian variety

Definition 15.33. Let X be an Abelian variety of dimension g over a field of characteristic $p > 0$. Then X is said to be ordinary if its Newton polygon is given by $0^g 1^g$; this is equivalent to the condition that $f(X) = g$. We say that X is supersingular if its Newton polygon is given by $\left(\frac{1}{2}\right)^{2g}$.

16 Abelian varieties over finite fields

16.1 The eigenvalues of Frobenius

Definition 16.1. Let $q = p^m$ and X a scheme over $\mathbb{F}_q$. Let π_X be the "iterated relative Frobenius" $F^{(m)}_{X/\mathbb{F}_q} : X \to X^{(p^m)}$.

For any $k \supseteq \mathbb{F}_q$, π_X acts on $X(k)$ by sending $x : \mathrm{Spec}(k) \to X$ to $\pi_X \circ x$. This is equal to $\pi_{\mathrm{Spec}(k)} \circ x$.

Proposition 16.2. If we have an embedding $X \hookrightarrow \mathbb{P}^N$ over $\mathbb{F}_q$ then π_X sends $(a_0 : a_1 : \cdots : a_N)$ to $(a_0^q : a_1^q : \cdots : a_N^q)$. Then

$$X(\mathbb{F}_{q^n}) = \{x \in X(\bar{\mathbb{F}}_q) | \pi_X^n(x) = x\}$$

Proposition 16.3. Since for any homomorphism of Abelian varieties $f : X \to Y$ we have $f \circ \pi_X = \pi_Y \circ f$, π_X commutes with all endomorphism of X, and then π_X is in the center of $\mathrm{End}^0(X)$.

Definition 16.4. Let $f_X = P_{\pi_X}$ be the characteristic polynomial of π_X. It is a monic polynomial with degree $2g$ with coefficients in $\mathbb{Z}$.

Proposition 16.5. Let X be an Abelian variety over $\mathbb{F}_q$.

(1) Let ℓ be a prime number, $\ell \neq p$. Then $V_\ell(\pi_X)$ is a semisimple automorphism of $V_\ell X$.

(2) Assume that X is elementary over $\mathbb{F}_q$ (i.e., isogenous to a power of a simple Abelian variety). Then $\mathbb{Q}[\pi_X]$ is a field, and f_X is a power of the minimum polynomial $f_{\mathbb{Q}}^{\pi_X}$ of π_X over $\mathbb{Q}$.

Theorem 16.6. Let X be an Abelian variety of dimension g over $\mathbb{F}_q$.

(1) Every complex root α of f_X has absolute value $|\alpha| = \sqrt{q}$.

(2) If α is a complex root of f_X then so is $\bar{\alpha} = q/\alpha$, and the two roots occur with the same multiplicity. If $\alpha = \sqrt{q}$ or $\alpha = -\sqrt{q}$ occurs as a root then it occurs with even multiplicity.

Proof. (1) If $X = X_1 \times \cdots \times X_s$ then $V_\ell X = V_\ell X_1 \oplus \cdots \oplus V_\ell X_s$ as $\mathbb{Q}_\ell$-modules. Thus $f_X = f_{X_1} \cdots f_{X_s}$. Then it suffices to show when X is simple.

■

Definition 16.7. For Y a scheme of finite type over $\mathbb{F}_q$, then the number $N_n = |Y(\mathbb{F}_{q^n})|$ of $\mathbb{F}_{q^n}$-rational points of Y is finite. Then the zeta function of Y is defined by

$$Z(Y, t) = \exp\left(\sum_{n=1}^{\infty} N_n \cdot \frac{t^n}{n}\right)$$

Theorem 16.8. Let X be an Abelian variety of dimension g over $\mathbb{F}_q$. Let $\{\alpha_1, \cdots, \alpha_{2g}\}$ be the multiset of complex roots of the characteristic polynomial f_X, so that

$$f_X(t) = \prod (t - \alpha_i)$$

If I is a subset of $\{1, \cdots, 2g\}$, define $\alpha_I = \Pi_{i \in I} \alpha_i$.

(1) For any positive integer n we have

$$|X(\mathbb{F}_{q^n})| = \prod_{i=1}^{2g} (1 - \alpha_i^n) = \sum_{j=0}^{2g} (-1)^j \cdot \mathrm{tr}(\pi_X^n; \bigwedge^j V_\ell X)$$

where ℓ is any prime number different from p and where by $\mathrm{tr}(\pi_X^n)$ we mean the trace of the automorphism $\bigwedge^j V_\ell(\pi_X^n)$ of $\bigwedge^j V_\ell X$.

(2) The zeta function of X is given by

$$Z(X,T) = \frac{P_1 P_3 \cdots P_{2g-1}}{P_0 P_2 \cdots P_{2g}}$$

where $P_j \in \mathbb{Z}[t]$ is the polynomial given by

$$P_j = \prod_{|I|=j} (1 - t \cdot \alpha_I) = \det\left(I - t \cdot \pi_X; \bigwedge^j V_\ell X \right)$$

(3) The zeta function satisfies the functional equation $Z(X; \dfrac{1}{q^g t}) = Z(X;t)$

Proof. (1) The characteristic polynomial $P_{\pi_X^n}$ of π_X^n is equal to $\prod(t - \alpha_i^n)$. Note that the kernel of the isogeny $id - \pi_X^n$ on $X(\bar{\mathbb{F}}_q)$ is precisely $X(\mathbb{F}_{q^n})$. Since $\bar{\mathbb{F}}_q$ is algebraically closed, $|X(\mathbb{F}_{q^n})| = \deg(id - \pi_X^n) = P_{\pi_X^n}(1) = \prod_{i=1}^{2g}(1 - \alpha_i^n)$.

Note that for an linear operator $T \in \mathrm{End}(V)$, suppose a_i is an eigenvalue of T such that $T \cdot e_i = a_i \cdot e_i$ for a basis $\{e_i\}$, then $\bigwedge^j T \cdot (e_I) = a_I \cdot (e_I)$, where I is any indexed set with cardinality j and $e_I = \bigwedge_{i \in I} e_i \in \bigwedge^j V$. Thus the set of eigenvalues of $\bigwedge^j T \in \mathrm{End}(\bigwedge^j V)$ is precisely the set of a_I.

Following the above argument the eigenvalues of $\bigwedge^j V_\ell(\pi_X^n)$ are the numbers α_I^n with $|I| = j$. Then the second identity follows by expanding $\prod(1 - \alpha_i^n)$.

(2) We use the following fact: for an endomorphism $\varphi \in \mathrm{End}(V)$ we have an identity of formal power series

$$\exp\left(\sum_{n=1}^{\infty} \mathrm{tr}\,(\varphi^n; V) \cdot \frac{t^n}{n} \right) = \det(id - t \cdot \varphi; V)^{-1}$$

Applying (1) we have

$$\begin{aligned}
Z(X;t) &= \exp\left(\sum_{n=1}^{\infty} \sum_{j=0}^{2g} (-1)^j \cdot \mathrm{tr}\left(\pi_X^n; \bigwedge^j V_\ell X \right) \frac{t^n}{n} \right) \\
&= \prod_{j=0}^{2g} \exp\left(\sum_{n=1}^{\infty} \mathrm{tr}\left(\pi_X^n; \bigwedge^j V_\ell X \right) \cdot \frac{t^n}{n} \right)^{(-1)^j} \\
&= \prod_{j=0}^{2g} \det\left(id - t \cdot \pi_X; \bigwedge^j V_\ell X \right)^{(-1)^{j+1}} \\
&= \prod_{j=0}^{2g} \left[\prod_{|I|=j} (1 - t \cdot a_I) \right]^{(-1)^{j+1}}
\end{aligned}$$

Then the set of $P_j \triangleq \prod_{|I|=j}(1 - t \cdot a_I)$ satisfies the property. Obviously P_j has coefficients in $\mathbb{Z}$ since f_X does.

(3) Note that $\prod_{i=1}^{2g} \alpha_i = q^g$, we have

$$P_{2g-j} = \prod_{|I|=j} \left(1 - \frac{q^g}{\alpha_I} \cdot t \right) = \left[\prod_{|I|=j} \left(-\frac{tq^g}{\alpha_I} \right) \right] \cdot P_j\left(\frac{1}{q^g t} \right) = (-t)^{C_{2g}^j} \cdot q^{C_{2g}^j (2q-j)/2} \cdot P_j\left(\frac{1}{q^g t} \right)$$

Then we can check that

$$Z(X,t) = Z(X, \frac{1}{q^g t})$$

■

16.2 The Hasse-Weil-Serre bound for curves (skip)

16.3 The theorem of Tate

Preliminaries

We first list some properties for Abelian varieties.

Proposition 16.9. Let X and Y be Abelian varieties over a field k.

If ℓ is a prime number, $\ell \neq \text{char }(k)$. Then the map

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

is injective, and has a torsion-free cokernel.

Proposition 16.10. Let X be an Abelian variety over a field k. Also, let ℓ be a prime number with $\ell \neq \text{char }(k)$. For any $\text{Gal}(\bar{k}/k)$-stable submodule W of finite index in $T_\ell X$, then there is an Abelian variety Y and an isogeny $u : Y \to X$ such that W is exactly the image of the induced map

$$T_\ell u : T_\ell Y \to T_\ell X$$

Proposition 16.11 (Zarhin's trick)**.** Let X be an Abelian variety over a field k. Then $X^4 \times (X^D)^4$ carries a principal polarization.

Proposition 16.12. Up to isomorphism, an Abelian varieties has only finitely many direct factors.

The proof

We first do some reductions.

Proposition 16.13. The map

$$T_\ell : \mathbb{Z}_\ell \otimes \text{Hom}(X,Y) \to \text{Hom}(T_\ell X, T_\ell Y)^{\text{Gal}(k_s/k)}$$

is an isomorphism if and only if the map

$$V_\ell : \mathbb{Q}_\ell \otimes \text{Hom}(X,Y) \to \text{Hom}(V_\ell X, V_\ell Y)^{\text{Gal}(k_s/k)}$$

is an is an isomorphism.

Proof. By 16.9 the map T_ℓ is injective and $\text{Coker}(T_\ell)$ is torsion-free (hence free). Then T_ℓ is an isomorphism if and only if $\text{Coker}(T_\ell)$ is free of rank 0, and further equivalently $\text{Coker}(T_\ell) \otimes \mathbb{Q}_\ell$ is a 0th-dimensional vector space. Now the result follows from that $\mathbb{Q}_\ell$ is flat over $\mathbb{Z}_\ell$. ■

Proposition 16.14. If Z is an Abelian variety over k such that

$$\mathbb{Q}_\ell \otimes \mathrm{End}(Z) \to \mathrm{End}(V_\ell Z)^{\mathrm{Gal}(k_s/k)}$$

is an isomorphism, then for any Abelian varieties X, Y over k, the map

$$\mathbb{Q}_\ell \otimes \mathrm{Hom}(X, Y) \to \mathrm{Hom}(V_\ell X, V_\ell Y)^{\mathrm{Gal}(k_s/k)}$$

is an is an isomorphism.

Proof. Let $Z = X \times Y$. Then, there are decompositions

$$\mathbb{Q}_\ell \otimes \mathrm{End}(Z) = \mathbb{Q}_\ell \otimes \mathrm{End}(X) \oplus \mathbb{Q}_\ell \otimes \mathrm{Hom}(X, Y) \oplus \mathbb{Q}_\ell \otimes \mathrm{Hom}(Y, X) \oplus \mathbb{Q}_\ell \otimes \mathrm{End}(Y)$$

$$\mathrm{End}(V_\ell Z)^G = \mathrm{End}(V_\ell X)^G \oplus \mathrm{Hom}(V_\ell X, V_\ell Y)^G \oplus \mathrm{Hom}(V_\ell Y, V_\ell X)^G \oplus \mathrm{End}(V_\ell Y)^G$$

where $G = \mathrm{Gal}(k_s/k)$. The result then follows immediately. ∎

Now we consider a "finiteness condition", which is denoted by $\mathrm{Fin}(X/k)$: up to isomorphism there are finitely may Abelian varieties Y over k for which there is an isogeny $X \to Y$ of degree a power of ℓ.

Lemma 16.15. Under the assumption $\mathrm{Fin}(X/k)$, for every sub-vector space $W \subseteq V_\ell X$ that is stable under $\mathrm{Gal}(k_s/k)$, there exists an element $u \in \mathbb{Q}_\ell \otimes \mathrm{End}(X)$ such that $W = u(V_\ell X)$.

Proof. Let $W_n = W \cap T_\ell X + \ell^n \cdot T_\ell X$. Then $\ell^n \cdot T_\ell X \subseteq W_n \subseteq T_\ell X$. W_n is then of finite index in $T_\ell X$, and by 16.10 it is the image of $T_\ell v_n : T_\ell X_n \to T_\ell X$, where $v_n : X_n \to X$ is an isogeny.

By the assumption $\mathrm{Fin}(X/k)$, there is a sub-sequence $\{n_i\}$ such that

$$X_{n_1} \cong X_{n_2} \cong \cdots$$

Fix an $n \in \{n_i\}$, let w_i be the composite

$$w_i : X \xrightarrow{v_n^{-1}} X_n \xrightarrow{\sim} X_{n_i} \xrightarrow{v_{n_i}} X$$

Then w_i is an element in $\mathbb{Q}_\ell \otimes \mathrm{End}(X)$. Choose an element $u \in \mathbb{Q}_\ell \otimes \mathrm{End}(X)$ be the limit of a sub-sequence. Then $u(V_\ell X) = (\lim v_n(V_\ell X_n)) \otimes \mathbb{Q}_\ell = \mathbb{Q}_\ell \otimes \lim W_n = W$. ∎

Now we return to the proof of Tate conjecture, in fact, we will prove a more general version.

Theorem 16.16. Let X be an Abelian variety over an arbitrary field k, and let ℓ be a prime number different from char (k). Assume that 16.15 is true for X and X^2, then the representation

$$\rho_\ell : \mathrm{Gal}(k_s/k) \to \mathrm{GL}(V_\ell X)$$

is semisimple and the map

$$\mathbb{Q}_\ell \otimes \mathrm{End}(X) \to \mathrm{End}(V_\ell X)^{\mathrm{Gal}(k_s/k)}$$

is an isomorphism.

Proof. Suppose we have a Galois-stable subspace $W \subseteq V_\ell X$. By 16.15, there exists an endomorphism $u \in \mathbb{Q}_\ell \otimes \mathrm{End}(X)$, such that W is exactly the image of $u : V_\ell X \to V_\ell X$. We consider the right ideal $u \cdot (\mathbb{Q}_\ell \otimes \mathrm{End}(X))$, since $\mathbb{Q}_\ell \otimes \mathrm{End}(X)$ is a semi-simple algebra, $u \cdot \mathbb{Q}_\ell \otimes \mathrm{End}(X)$ is generated by an idempotent e. In addition, $W = u(V_\ell X) = e(V_\ell X)$ and its complement is $(1-e)(V_\ell X)$. Obviously, $(1-e)(V_\ell X)$ is also Galois-stable, hence ρ_ℓ is semi-stable.

Let Z be the centralizer of $\mathrm{End}(X)\otimes\mathbb{Q}_\ell$ in $\mathrm{End}(V_\ell X)$, let Y be the centralizer of Z. The double centralizer theorem gives that $Y = \mathrm{End}(X) \otimes \mathbb{Q}_\ell$. Choose an element $\alpha \in \mathrm{End}(V_\ell X)^{\mathrm{Gal}(k_s/k)}$, it suffices to show that $\alpha \in Y$. Consider the graph of α

$$W \triangleq \{(x, ax) | x \in V_\ell X\}$$

this is a Galois-stable subspace of $V_\ell X \times V_\ell X$, and then by 16.15 there exists an element $u \in \mathrm{End}(X \times X) \otimes \mathbb{Q}_\ell$ such that $W = u(V_\ell(X \times X))$. For any $c \in Z$, the matrix $\begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} \in \mathrm{End}(V_\ell X \times V_\ell X)$ commutes with $\mathrm{End}(X \times X) \otimes \mathbb{Q}_\ell$, and in particular, with u. Then $\begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} W \subseteq W$. This says that, for any $x \in V_\ell X$, $(cx, c\alpha x) \in W$. By the definition of the graph, α maps cx to $c\alpha x$, and then α commutes with c. Hence, $\alpha \in Y$. ■

Proposition 16.17 (finiteness theorem)**.** Now all we need is that the condition $\mathrm{Fin}(X/k)$ holds when k is a finite field. Indeed, there is a stronger condition: there are only finitely many Abelian varieties of the dimension g (up to isomorphism) over k.

Proof. By 16.11 and 16.12, it suffices to show that there are finitely many principal polarization Abelian varieties over k. Note that they can be treated as the k-points of the stack $\mathcal{A}_{g,d}(k)$, this is a stack of finite type over k, hence the k-points are finite. ■

Theorem 16.18 (the p-divisible group version)**.** Let X and Y be Abelian varieties over a field of characteristic p. Then the map

$$\Phi : \mathbb{Z}_p \otimes \mathrm{Hom}_{\mathbf{AV}}(X, Y) \to \mathrm{Hom}_{p-\mathrm{div}}(X[p^\infty], Y[p^\infty])$$

is an isomorphism.

Corollary 16.19. Let X and Y be Abelian varieties over a finite field k of characteristic p. Then the following are equivalent:

(a) $X \sim Y$;

(b1) for some $\ell \neq p$ we have $V_\ell X \cong V_\ell Y$ as representations of $\mathrm{Gal}(\bar{k}/k)$;

(b2) for all $\ell \neq p$ we have $V_\ell X \cong V_\ell Y$ as representations of $\mathrm{Gal}(\bar{k}/k)$;

(c1) $X[p^\infty] \sim Y[p^\infty]$;

(c2) $M_{\mathbb{Q}}(X) \cong M_{\mathbb{Q}}(Y)$ as F-isocrystals;

(d) $f_X = f_Y$;

(e1) $Z(X; t) = Z(Y; t)$;

(e2) for all finite field extension $k \subseteq k'$ we have $|X(k')| = |Y(k')|$.

Proof. The conditions $(a) \Rightarrow (b2) \Rightarrow (b1)$ are clear.

Assume that (b1) holds true. Then there is a Galois-equivalent isomorphism $h : V_\ell X \to V_\ell Y$ for some $\ell \neq p$. Possibly after replacing h by $\ell^n h$ for some n, we may assume that $h(T_\ell X) \subseteq T_\ell Y$, so that

$$U = \{h \in \mathrm{Hom}_{\mathrm{Gal}(k_s/k)}(T_\ell X, T_\ell Y) | h \text{ is injective}\}$$

is nonempty. It is ℓ-adically open in $\mathrm{Hom}_{\mathrm{Gal}(k_s/k)}(T_\ell X, T_\ell Y)$. But $\mathrm{Hom}(X, Y) \subseteq \mathbb{Z}_\ell \otimes \mathrm{Hom}(X, Y)$ is ℓ-adically dense, so by Tate theorem there is an element $f \in \mathrm{Hom}(X, Y)$ such that $T_\ell f$ is injective. This f is an isogeny.

Similarly $(a) \iff (c1) \iff (c2)$. ■