Elliptic Curves and Abelian Varieties

Jiacheng Liang

College of Physics, Sichuan University

May 30, 2022

Table of Contents

Background

In mathematics, especially in algebraic geometry, complex analysis and algebraic number theory, Abelian varieties are projective algebraic groups, that is, they are group varieties.

Abelian variety is one of the most studied objects in algebraic geometry, and it is also an indispensable tool for studying many other subjects in algebraic geometry and number theory.

We will see that elliptic curves are exactly Abelian varieties of dim $= 1$, and that any Abelian varieties are automatically commutative, smooth and projective.
In addition, we will see that the variety structure on the Abelian variety with a given base point is unique.

Finally, we will study the separable and inseparable isogeny between Abelian varieties, which is the most important class of morphisms between Abelian varieties.

Background

In mathematics, especially in algebraic geometry, complex analysis and algebraic number theory, Abelian varieties are projective algebraic groups, that is, they are group varieties.

Abelian variety is one of the most studied objects in algebraic geometry, and it is also an indispensable tool for studying many other subjects in algebraic geometry and number theory.

We will see that elliptic curves are exactly Abelian varieties of $\dim = 1$, and that any Abelian varieties are automatically commutative, smooth and projective.
In addition, we will see that the variety structure on the Abelian variety with a given base point is unique.

Finally, we will study the separable and inseparable isogeny between Abelian varieties, which is the most important class of morphisms between Abelian varieties.

Classification of Étale k-schemes

Let k be a field. Choose a separable algebraic closure k_s and write $\Gamma_k := \mathrm{Gal}\,(k_s/k)$. Then Γ_k is a pro-finite group.

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 $\mathrm{Stab}(y)$ is an open subgroup of Γ_k for any $y \in Y$. If X is a connected étale scheme over k, then X is of the form $X = \mathrm{Spec}(L)$, with L a finite separable field extension of k. An arbitrary étale k-scheme can be written as a disjoint union of its connected components, and is therefore of the form $X = \bigsqcup_{\alpha \in I} \mathrm{Spec}\,(L_\alpha)$, where I is some index set and where $k \subset L_\alpha$ is a finite separable extension of fields.

Theorem

The description of étale k-schemes is a matter of Galois theory. More precisely, if $\mathrm{Et}_{/k}$ denotes the category of étale k-schemes there is an equivalence of categories

$$\mathrm{Et}_{/k} \overset{X \mapsto X(k_s)}{\longrightarrow} \Gamma_k\text{-sets}\,.$$

Classification of Étale k-schemes

Let k be a field. Choose a separable algebraic closure k_s and write $\Gamma_k := \mathrm{Gal}\,(k_s/k)$. Then Γ_k is a pro-finite group.

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 $\mathrm{Stab}(y)$ is an open subgroup of Γ_k for any $y \in Y$. If X is a connected étale scheme over k, then X is of the form $X = \mathrm{Spec}(L)$, with L a finite separable field extension of k. An arbitrary étale k-scheme can be written as a disjoint union of its connected components, and is therefore of the form $X = \bigsqcup_{\alpha \in I} \mathrm{Spec}\,(L_\alpha)$, where I is some index set and where $k \subset L_\alpha$ is a finite separable extension of fields.

Theorem

The description of étale k-schemes is a matter of Galois theory. More precisely, if $\mathrm{Et}_{/k}$ denotes the category of étale k-schemes there is an equivalence of categories

$$\mathrm{Ét}_{/k} \overset{X \mapsto X(k_s)}{\longrightarrow} \Gamma_k\text{-sets}\ .$$

Connected components of k-schemes of finite type

Theorem (Connected components)

Let X be a scheme of finite type over a field k. Let Y be a finite étale k-scheme.
(i) There is a finite étale 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 a finite étale k-scheme. By this we mean we have an adjoint pair

$$\omega_0 : \mathrm{FT}_{/k} \rightleftharpoons fi\,\mathrm{ET}_{/k} : U$$

where U is the forgetful functor. And we have $\omega_0 \circ U \cong \mathrm{Id}$.
(ii) The morphism q is faithfully flat, and its fibres are precisely the connected components of X.

Definition

1. Let S be a scheme. A group scheme over S, or an S-group scheme, is an S-scheme $\pi : G \to S$ together with S-morphisms $m : G \times_S G \to G$ (group law, or multiplication), $i : G \to G$ (inverse), and $e : S \to G$ (identity section), such that the following identities of morphisms hold:

$$m \circ (m \times \mathrm{id}_G) = m \circ (\mathrm{id}_G \times m) : G \times_S G \times_S G \to G$$
$$m \circ (e \times \mathrm{id}_G) = j_1 : S \times_S G \to G$$
$$m \circ (\mathrm{id}_G \times e) = j_2 : G \times_S S \to G$$
$$e \circ \pi = m \circ (\mathrm{id}_G \times i) \circ \Delta_{G/S} = m \circ (i \times \mathrm{id}_G) \circ \Delta_{G/S} : G \to G,$$

   where $j_1 : S \times_S G \xrightarrow{\sim} G$ and $j_2 : G \times_S S \xrightarrow{\sim} G$ are the canonical isomorphisms.

2. A group scheme G over S is said to be commutative if, writing $s : G \times_S G \to G \times_S G$ for the isomorphism switching the two factors, we have the identity $m = m \circ s : G \times_S G \to G$.

Definition

1. Let S be a scheme. A group scheme over S, or an S-group scheme, is an S-scheme $\pi : G \to S$ together with S-morphisms $m : G \times_S G \to G$ (group law, or multiplication), $i : G \to G$ (inverse), and $e : S \to G$ (identity section), such that the following identities of morphisms hold:

$$m \circ (m \times \mathrm{id}_G) = m \circ (\mathrm{id}_G \times m) : G \times_S G \times_S G \to G$$
$$m \circ (e \times \mathrm{id}_G) = j_1 : S \times_S G \to G$$
$$m \circ (\mathrm{id}_G \times e) = j_2 : G \times_S S \to G$$
$$e \circ \pi = m \circ (\mathrm{id}_G \times i) \circ \Delta_{G/S} = m \circ (i \times \mathrm{id}_G) \circ \Delta_{G/S} : G \to G,$$

   where $j_1 : S \times_S G \xrightarrow{\sim} G$ and $j_2 : G \times_S S \xrightarrow{\sim} G$ are the canonical isomorphisms.

2. A group scheme G over S is said to be commutative if, writing $s : G \times_S G \to G \times_S G$ for the isomorphism switching the two factors, we have the identity $m = m \circ s : G \times_S G \to G$.

Morphisms of group schemes

Definition

Let $(\pi_1 : G_1 \to S, m_1, i_1, e_1)$ and $(\pi_2 : G_2 \to S, m_2, i_2, e_2)$ be two group schemes over S. A homomorphism of S-group schemes from G_1 to G_2 is a morphism of schemes $f : G_1 \to G_2$ over S such that $f \circ m_1 = m_2 \circ (f \times f) : G_1 \times_S G_1 \to G_2$. (This condition implies that $f \circ e_1 = e_2$ and $f \circ i_1 = i_2 \circ f$.)

Given an S-group scheme G and an integer n, we define $[n] = [n]_G : G \to G$ to be the morphism which on sections - using multiplicative notation for the group law-is given by $g \mapsto g^n$. If $n \geqslant 1$ it factors as

$$[n] = \left(G \xrightarrow{\Delta^n_{G/S}} G^n_S \xrightarrow{m^{(n)}} G \right),$$

where $m^{(n)}$ is the “iterated multiplication map", given on sections by $(g_1, \ldots, g_n) \mapsto g_1 \cdots g_n$. For commutative group schemes $[n]$ is a group morphism usually called “multiplication by n ".

Quotients of algebraic groups

Definition (Algebraic groups)

Let k be a field. An (locally) algebraic group is s a group scheme over k which is of (locally) finite type over k.

Theorem

The category $\boldsymbol{C}_k$ of algebraic groups over a field k is an abelian category.

The theorem above can make us easily construct new algebraic groups from given algebraic groups.

Corollary (Étale-local decomposition of algebraic groups)

Let $G \in \boldsymbol{C}_k$. Then we have an exact sequence in $\boldsymbol{C}_k$.

$$0 \longrightarrow G^0 \longrightarrow G \longrightarrow \omega_0(G) \longrightarrow 0$$

If k is perfect and G is finite over k then this sequence naturally splits, i.e. we have a homomorphic section $G \leftarrow \omega_0(G)$ and natural $G \cong G^0 \times \omega_0(G)$.

Quotients of algebraic groups

Definition (Algebraic groups)

Let k be a field. An (locally) algebraic group is s a group scheme over k which is of (locally) finite type over k.

Theorem

The category $\boldsymbol{C}_k$ of algebraic groups over a field k is an abelian category.

The theorem above can make us easily construct new algebraic groups from given algebraic groups.

Corollary (Étale-local decomposition of algebraic groups)

Let $G \in \boldsymbol{C}_k$. Then we have an exact sequence in $\boldsymbol{C}_k$.

$$0 \longrightarrow G^0 \longrightarrow G \longrightarrow \omega_0(G) \longrightarrow 0$$

If k is perfect and G is finite over k then this sequence naturally splits, i.e. we have a homomorphic section $G \leftarrow \omega_0(G)$ and natural $G \cong G^0 \times \omega_0(G)$.

Quotients of algebraic groups

Definition (Algebraic groups)

Let k be a field. An (locally) algebraic group is s a group scheme over k which is of (locally) finite type over k.

Theorem

The category $\boldsymbol{C}_k$ of algebraic groups over a field k is an abelian category.

The theorem above can make us easily construct new algebraic groups from given algebraic groups.

Corollary (Étale-local decomposition of algebraic groups)

Let $G \in \boldsymbol{C}_k$. Then we have an exact sequence in $\boldsymbol{C}_k$.

$$0 \longrightarrow G^0 \longrightarrow G \longrightarrow \omega_0(G) \longrightarrow 0$$

If k is perfect and G is finite over k then this sequence naturally splits, i.e. we have a homomorphic section $G \leftarrow \omega_0(G)$ and natural $G \cong G^0 \times \omega_0(G)$.

The group structure on elliptic curves

We can prove that any elliptic curve admits a natural (unique) structure of group variety by a technical stuff called relative effective Cartier divisors.

Definition

We define an elliptic curve over a field k to be a pair (C, e) where C is a smooth proper and geometrically integral curve over k of genus 1 (i.e. $dim_k H^1(C, \mathcal{O}_C) = 1$) with $e \in C(k)$ a rational point on C.

Theorem (Main)

Let (C, e) be an elliptic curve over a field k, then $Div^{+,1}_{C/k}(T) \to Pic^1_{C/k}(T)$ is naturally isomorphic for any k-scheme T, where $Div^{+,1}_{C/k}(-)$ is representable by C itself.

Corollary

Let (C, e) be an elliptic curve over a field k, then $Pic^0_{C/k}(-) \cong Pic^1_{C/k}(-)$ is a functor into Abel representable by C with $\mathcal{L}(\Delta) \otimes \pi_1^* \mathcal{L}(-e)$ on $C \times_k C$, and hence induces a natural commutative group k-scheme structure on C with the zero map e.

The group structure on elliptic curves

We can prove that any elliptic curve admits a natural (unique) structure of group variety by a technical stuff called relative effective Cartier divisors.

Definition

We define an elliptic curve over a field k to be a pair (C, e) where C is a smooth proper and geometrically integral curve over k of genus 1 (i.e. $dim_k H^1(C, \mathcal{O}_C) = 1$) with $e \in C(k)$ a rational point on C.

Theorem (Main)

Let (C, e) be an elliptic curve over a field k, then $Div^{+,1}_{C/k}(T) \to Pic^1_{C/k}(T)$ is naturally isomorphic for any k-scheme T, where $Div^{+,1}_{C/k}(-)$ is representable by C itself.

Corollary

Let (C, e) be an elliptic curve over a field k, then $Pic^0_{C/k}(-) \cong Pic^1_{C/k}(-)$ is a functor into Abel representable by C with $\mathcal{L}(\Delta) \otimes \pi_1^* \mathcal{L}(-e)$ on $C \times_k C$, and hence induces a natural commutative group k-scheme structure on C with the zero map e.

The group structure on elliptic curves

We can prove that any elliptic curve admits a natural (unique) structure of group variety by a technical stuff called relative effective Cartier divisors.

Definition

We define an elliptic curve over a field k to be a pair (C, e) where C is a smooth proper and geometrically integral curve over k of genus 1 (i.e. $dim_k H^1(C, \mathcal{O}_C) = 1$) with $e \in C(k)$ a rational point on C.

Theorem (Main)

Let (C, e) be an elliptic curve over a field k, then $Div^{+,1}_{C/k}(T) \to Pic^1_{C/k}(T)$ is naturally isomorphic for any k-scheme T, where $Div^{+,1}_{C/k}(-)$ is representable by C itself.

Corollary

Let (C, e) be an elliptic curve over a field k, then $Pic^0_{C/k}(-) \cong Pic^1_{C/k}(-)$ is a functor into Abel *representable by C with $\mathcal{L}(\Delta) \otimes \pi_1^* \mathcal{L}(-e)$ on $C \times_k C$, and hence induces a natural commutative group k-scheme structure on C with the zero map e.*

Abelian varieties

Definition

An abelian variety (X, m, i, e) is a group scheme over k which is a proper, geometrically integral variety over k. (Notice that we never said the group structure on an abelian variety is commutative! This will be a nontrivial theorem that we will prove.)

We have seen any elliptic curve over k is an abelian variety of dim 1 in the definition. Actually, the converse is true too.

Proposition

Any abelian variety C of dim 1 over k is an elliptic curve.

Note that we have proved that the category $\boldsymbol{C}_k$ of commutative algebraic groups over a field k is an abelian category. Actually, we will see any quotient of an abelian variety is still an abelian variety in the following proposition.

Proposition

Let $f : X \to Y$ be an epimorphism (i.e. fppf homomorphism) in $\boldsymbol{C}_k$. If X is an abelian variety, then so is Y.

Abelian varieties

Definition

An abelian variety (X, m, i, e) is a group scheme over k which is a proper, geometrically integral variety over k. (Notice that we never said the group structure on an abelian variety is commutative! This will be a nontrivial theorem that we will prove.)

We have seen any elliptic curve over k is an abelian variety of dim 1 in the definition. Actually, the converse is true too.

Proposition

Any abelian variety C of dim 1 over k is an elliptic curve.

Note that we have proved that the category C_k of commutative algebraic groups over a field k is an abelian category. Actually, we will see any quotient of an abelian variety is still an abelian variety in the following proposition.

Proposition

Let $f : X \to Y$ be an epimorphism (i.e. fppf homomorphism) in C_k. If X is an abelian variety, then so is Y.

Definition

An abelian variety (X, m, i, e) is a group scheme over k which is a proper, geometrically integral variety over k. (Notice that we never said the group structure on an abelian variety is commutative! This will be a nontrivial theorem that we will prove.)

We have seen any elliptic curve over k is an abelian variety of dim 1 in the definition. Actually, the converse is true too.

Proposition

Any abelian variety C of dim 1 over k is an elliptic curve.

Note that we have proved that the category $\boldsymbol{C}_k$ of commutative algebraic groups over a field k is an abelian category. Actually, we will see any quotient of an abelian variety is still an abelian variety in the following proposition.

Proposition

Let $f : X \to Y$ be an epimorphism (i.e. fppf homomorphism) in $\boldsymbol{C}_k$. If X is an abelian variety, then so is Y.

Smoothness of abelian varieties

Proposition (Smoothness)

Let G be a (locally) algebraic group over a field k, then
(i) The identity component G^0 is an open and closed subgroup scheme of G which is geometrically irreducible.
(ii) The following properties are equivalent:
(a) $G \times_k K$ is reduced for some perfect field K containing k;
(b) G is smooth over k;
(iii) Every connected component of G is irreducible and of finite type over k.

Corollary

Particularly, any abelian variety over a field k is smooth over k.

Lemma (Rigidity lemma)

Let k be a field, and let X be a geometrically reduced, geometrically connected proper k-scheme such that $X(k) \neq \emptyset$. Let Y be an integral k-scheme, and let Z be a separated k-scheme. Let $f : X \times Y \to Z$ be a morphism such that for some $y \in Y(k), f_{|X \times \{y\}}$ factors through a k-valued point $z \in Z(k)$. Then f factors through the projection $p_2 : X \times Y \to Y$.

Corollary

Let X and Y be abelian varieties and let $f : X \to Y$ be a k-morphism. Then f is the composition $f = t_{f(e_X)} \circ h$ of a homomorphism $h : X \to Y$ and a translation $t_{f(e_X)}$ over $f(e_X)$ on Y.

Particularly, if f preserves the basepoint, then f is a homomorphism.

Lemma (Rigidity lemma)

Let k be a field, and let X be a geometrically reduced, geometrically connected proper k-scheme such that $X(k) \neq \emptyset$. Let Y be an integral k-scheme, and let Z be a separated k-scheme. Let $f : X \times Y \to Z$ be a morphism such that for some $y \in Y(k), f_{|X\times\{y\}}$ factors through a k-valued point $z \in Z(k)$. Then f factors through the projection $p_2 : X \times Y \to Y$.

Corollary

Let X and Y be abelian varieties and let $f : X \to Y$ be a k-morphism. Then f is the composition $f = t_{f(e_X)} \circ h$ of a homomorphism $h : X \to Y$ and a translation $t_{f(e_X)}$ over $f(e_X)$ on Y.

Particularly, if f preserves the basepoint, then f is a homomorphism.

Corollary

1. *If X is a geometrically integral proper variety over a field k and $e \in X(k)$ then there is at most one structure of an abelian variety on X for which e is the identity element.*
2. *If (X, m, i, e) is an abelian variety then the group structure on X is commutative, i.e., $m \circ \tau = m : X \times X \to X$, where $\tau : X \times X \to X \times X$ is the morphism switching the two factors. In particular, for every k-scheme T the group $X(T)$ is abelian.*

Theorem (Rigidity of line bundles)

Let X and Y be proper and geometrically integral varieties over k and let Z be a connected, locally noetherian k-scheme. Consider points $x \in X(k)$ and $y \in Y(k)$, and let $z \in Z(k)$ be a point of Z. If L is a line bundle on $X \times Y \times Z$ whose restriction to $\{x\} \times Y \times Z$, to $X \times \{y\} \times Z$ and to $X \times Y \times \{z\}$ is trivial then L is trivial.

Corollary

1. *If X is a geometrically integral proper variety over a field k and $e \in X(k)$ then there is at most one structure of an abelian variety on X for which e is the identity element.*
2. *If (X, m, i, e) is an abelian variety then the group structure on X is commutative, i.e., $m \circ \tau = m : X \times X \to X$, where $\tau : X \times X \to X \times X$ is the morphism switching the two factors. In particular, for every k-scheme T the group $X(T)$ is abelian.*

Theorem (Rigidity of line bundles)

Let X and Y be proper and geometrically integral varieties over k and let Z be a connected, locally noetherian k-scheme. Consider points $x \in X(k)$ and $y \in Y(k)$, and let $z \in Z(k)$ be a point of Z. If L is a line bundle on $X \times Y \times Z$ whose restriction to $\{x\} \times Y \times Z$, to $X \times \{y\} \times Z$ and to $X \times Y \times \{z\}$ is trivial then L is trivial.

Theorem (Theorem of the Cube)

Let X be an abelian variety over k. Let L be a line bundle on X. Then the line bundle

$$\Theta(L) := \bigotimes_{I \subset \{1,2,3\}} p_I^* L^{\otimes (-1)^{1+\#I}}$$
$$= p_{123}^* L \otimes p_{12}^* L^{-1} \otimes p_{13}^* L^{-1} \otimes p_{23}^* L^{-1} \otimes p_1^* L \otimes p_2^* L \otimes p_3^* L$$

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

Corollary

For every line bundle L on an abelian variety X and every $n \in \mathbb{Z}$ we have

$$[n]^* L \cong L^{n(n+1)/2} \otimes [-1]^* L^{n(n-1)/2}.$$

Theorem (Theorem of the Cube)

Let X be an abelian variety over k. Let L be a line bundle on X. Then the line bundle

$$\Theta(L) := \bigotimes_{I \subset \{1,2,3\}} p_I^* L^{\otimes (-1)^{1+\#I}}$$
$$= p_{123}^* L \otimes p_{12}^* L^{-1} \otimes p_{13}^* L^{-1} \otimes p_{23}^* L^{-1} \otimes p_1^* L \otimes p_2^* L \otimes p_3^* L$$

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

Corollary

For every line bundle L on an abelian variety X and every $n \in \mathbb{Z}$ we have

$$[n]^* L \cong L^{n(n+1)/2} \otimes [-1]^* L^{n(n-1)/2}.$$

Isogenies between abelian varieties

Definition

Let $f : X \to Y$ be a homomorphism of abelian varieties. A homomorphism $f : X \to Y$ of abelian varieties is called an isogeny if f satisfies following equivalent conditions:

(a) f is surjective and $\dim(X) = \dim(Y)$;

(b) $\mathrm{Ker}(f)$ is a finite group scheme and $\dim(X) = \dim(Y)$;

(c) f is a finite, flat and surjective morphism.

Definition

A homomorphism $f : X \to Y$ of abelian varieties is called an isogeny if f satisfies the three equivalent conditions (a), (b) and (c) above. The degree of an isogeny f is the degree of the function field extension $\deg(f) = [K(X) : K(Y)]$. We can prove a formula $\deg(f) = \mathrm{rank}_{O_Y}(f_* O_X) = \mathrm{rank}(\mathrm{Ker}(f))$.

We call an isogeny to be separable (resp. inseparable) if and only if $K(X)|K(Y)$ is a separable (resp. inseparable) extension.

Isogenies between abelian varieties

Definition

Let $f : X \to Y$ be a homomorphism of abelian varieties. A homomorphism $f : X \to Y$ of abelian varieties is called an isogeny if f satisfies following equivalent conditions:

(a) f is surjective and $\dim(X) = \dim(Y)$;

(b) $\mathrm{Ker}(f)$ is a finite group scheme and $\dim(X) = \dim(Y)$;

(c) f is a finite, flat and surjective morphism.

Definition

A homomorphism $f : X \to Y$ of abelian varieties is called an isogeny if f satisfies the three equivalent conditions (a), (b) and (c) above. The degree of an isogeny f is the degree of the function field extension $\deg(f) = [K(X) : K(Y)]$. We can prove a formula $\deg(f) = \mathrm{rank}_{O_Y}(f_* O_X) = \mathrm{rank}(\mathrm{Ker}(f))$.

We call an isogeny to be separable (resp. inseparable) if and only if $K(X)|K(Y)$ is a separable (resp. inseparable) extension.

Isogenies between abelian varieties

An important example of an isogeny is the multiplication $[n]_X : X \to X$ by an integer $n \neq 0$. We write $X[n] := \mathrm{Ker}\left([n]_X\right) \subset X$.

Theorem

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

Proposition

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

If $(\mathrm{char}(k), n) = 1$ then $X[n]\left(k_s\right) = X[n](\bar{k}) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.

Isogenies between abelian varieties

An important example of an isogeny is the multiplication $[n]_X : X \to X$ by an integer $n \neq 0$. We write $X[n] := \mathrm{Ker}\left([n]_X\right) \subset X$.

Theorem

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

Proposition

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

If $(\mathrm{char}(k), n) = 1$ then $X[n]\left(k_s\right) = X[n](\bar{k}) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.

Isogenies between abelian varieties

An important example of an isogeny is the multiplication $[n]_X : X \to X$ by an integer $n \neq 0$. We write $X[n] := \mathrm{Ker}\left([n]_X\right) \subset X$.

Theorem

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

Proposition

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

If $(\mathrm{char}(k), n) = 1$ then $X[n]\left(k_s\right) = X[n](\bar{k}) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.

p-rank of an abelian variety of char(p)>0

Now we consider abelian varieties over a field of characteristic $p > 0$.

Theorem

If X is an abelian variety of dimension g over field k of characteristic p, then there is a unique integer $0 \leq i \leq g$, $i = f(X)$ called the p-rank of X, such that

$$X[p^m](\bar{k}) = (\mathbb{Z}/p^m\mathbb{Z})^i.$$

Proposition

If $h : X \to Y$ is an isogeny of abelian varieties over a field k, then $f(X) = f(Y)$.

Remark

The p-rank does not depend on the ground field. More precisely, if $k \subset K$ is a field extension and X is an abelian variety over k then $f(X) = f(X_K)$.

p-rank of an abelian variety of char(p)>0

Now we consider abelian varieties over a field of characteristic $p > 0$.

Theorem

If X is an abelian variety of dimension g over field k of characteristic p, then there is a unique integer $0 \leq i \leq g$, $i = f(X)$ called the p-rank of X, such that

$$X\left[p^m\right](\bar{k}) = \left(\mathbb{Z}/p^m\mathbb{Z}\right)^i.$$

Proposition

If $h : X \to Y$ is an isogeny of abelian varieties over a field k, then $f(X) = f(Y)$.

Remark

The p-rank does not depend on the ground field. More precisely, if $k \subset K$ is a field extension and X is an abelian variety over k then $f(X) = f\left(X_K\right)$.

p-rank of an abelian variety of char(p)>0

Now we consider abelian varieties over a field of characteristic $p > 0$.

Theorem

If X is an abelian variety of dimension g over field k of characteristic p, then there is a unique integer $0 \leq i \leq g$, $i = f(X)$ called the p-rank of X, such that

$$X\left[p^m\right](\bar{k}) = \left(\mathbb{Z}/p^m\mathbb{Z}\right)^i.$$

Proposition

If $h : X \to Y$ is an isogeny of abelian varieties over a field k, then $f(X) = f(Y)$.

Remark

The p-rank does not depend on the ground field. More precisely, if $k \subset K$ is a field extension and X is an abelian variety over k then $f(X) = f\left(X_K\right)$.

Formal completion of pointed k-schemes

Definition

For a k-scheme X with a rational point $e \in X(k)$. The formal completion $\widehat{X}$ of X "along" e is defined to be the complete linearly topological ring $\mathrm{Spf}(\widehat{\mathcal{O}_{X,e}})$. This induces a functor $Sch_k^* \xrightarrow{\widehat{(-)}} k\text{-FRings}^{op}$ where the left one is the category of pointed k-schemes.

Theorem

The functor $\widehat{(-)}$ preserves finite limits. Particularly, it preserves finite products and hence preserves (commutative) Monoid objects, (commutative) Group objects. So it takes group k-schemes to formal group k-schemes.

This theorem tells us an interesting basic fact: a formal group scheme can be obtained naturally by formal completion of a smooth group variety.

Formal completion of pointed k-schemes

Definition

For a k-scheme X with a rational point $e \in X(k)$. The formal completion $\widehat{X}$ of X "along" e is defined to be the complete linearly topological ring $\mathrm{Spf}(\widehat{\mathcal{O}_{X,e}})$. This induces a functor $Sch_k^* \xrightarrow{\widehat{(-)}} k\text{-FRings}^{op}$ where the left one is the category of pointed k-schemes.

Theorem

The functor $\widehat{(-)}$ preserves finite limits. Particularly, it preserves finite products and hence preserves (commutative) Monoid objects, (commutative) Group objects. So it takes group k-schemes to formal group k-schemes.

This theorem tells us an interesting basic fact: a formal group scheme can be obtained naturally by formal completion of a smooth group variety.

Definition

An elliptic curve X is said to be ordinary if $f(X) = 1$ and supersingular if $f(X) = 0$.

We end with following beautiful theorems of the correspondence p-rank of elliptic curves and the height of its formal completion.

Theorem

Let C be an elliptic curve over a field k. Then $ht(\hat{C}) = 1$ or $ht(\hat{C}) = 2$.

Theorem

Let C be an elliptic curve over a field k. Then following conditions are equivalent
(i) $[p]_C$ is a purely inseparable isogeny;
(ii) C is supersingular;
(iii) $ht(\hat{C}) = 2$.
Particularly, by the last theorem we have $ht(\hat{C}) + f(C) = 2$.

Definition

An elliptic curve X is said to be ordinary if $f(X) = 1$ and supersingular if $f(X) = 0$.

We end with following beautiful theorems of the correspondence p-rank of elliptic curves and the height of its formal completion.

Theorem

Let C be an elliptic curve over a field k. Then $ht(\hat{C}) = 1$ or $ht(\hat{C}) = 2$.

Theorem

Let C be an elliptic curve over a field k. Then following conditions are equivalent
(i) $[p]_C$ is a purely inseparable isogeny;
(ii) C is supersingular;
(iii) $ht(\hat{C}) = 2$.
Particularly, by the last theorem we have $ht(\hat{C}) + f(C) = 2$.

Definition

An elliptic curve X is said to be ordinary if $f(X) = 1$ and supersingular if $f(X) = 0$.

We end with following beautiful theorems of the correspondence p-rank of elliptic curves and the height of its formal completion.

Theorem

Let C be an elliptic curve over a field k. Then $ht(\hat{C}) = 1$ or $ht(\hat{C}) = 2$.

Theorem

Let C be an elliptic curve over a field k. Then following conditions are equivalent
(i) $[p]_C$ is a purely inseparable isogeny;
(ii) C is supersingular;
(iii) $ht(\hat{C}) = 2$.
Particularly, by the last theorem we have $ht(\hat{C}) + f(C) = 2$.

THANK YOU!