四川大學

本科生毕业论文（设计）

题　　目　椭圆曲线与阿贝尔簇

学　　院　物理学院

专　　业　物理学（基地班）

学生姓名　梁嘉诚

学　　号　2018141223010 年级　2018 级

指导教师　杨海棠，朱一飞

教务处制表

二〇二二年五月十七日

椭圆曲线与阿贝尔簇

物理学院

学生: 梁嘉诚　　指导教师: 杨海棠，朱一飞

[摘要]　本文将介绍算术几何中经常出现的几个对象——形式群、椭圆曲线和阿贝尔簇。我们首先介绍形式环以及如何从光滑群簇自然地得到一个形式群。其次，我们用相对有效 Cartier 除子的技术证明任何椭圆曲线都有自然的群簇结构。然后，我们介绍群概形的一些基本性质，代数群的 étale-local 分解和群概形作用下的商概形。在最后一章我们介绍阿贝尔簇，我们将看到椭圆曲线正是 $\dim = 1$ 的阿贝尔簇，并且任何阿贝尔簇是自动交换的、光滑的和射影的。此外，我们将看到给定基点的阿贝尔簇上的群结构是唯一的。最后，我们将研究阿贝尔簇之间的 isogeny。

[主题词] 代数几何，算术几何，椭圆曲线，阿贝尔簇，特征 p

Elliptic Curves and Abelian Varieties

College of Physics

Student: Jiacheng Liang Adviser: Haitang Yang, Yifei Zhu

[**Abstract**] This article will provide an introduction to formal groups, elliptic curves and abelian varieties, which are major objects appearing in arithmetic geometry. We first introduce formal rings and how to get a natural formal group from a smooth group variety. Second we prove that any elliptic curve admits a natural structure of group variety by a technical method of relative effective Cartier divisor. After that, we introduce some basic properties of group scheme, étale-local decomposition of algebraic groups and the quotient scheme by an action of group scheme. In the last chapter we introduce abelian varieties, we will see that elliptic curves are exactly abelian varieties of dim = 1 and that any abelian variety is automatically commutative, smooth and projective. In addition we will see that the group structure is unique on an abelian variety given a basepoint. Finally we will study isogenies between abelian varieties.

[**Key Words**] Algebraic geometry, Arithmetic geometry, Elliptic curve, Abelian variety, characteristic p

目录

1. Formal groups

1.1 Linearly topological rings

Before the introduction of formal groups, we need some preliminary knowledge of linear topological rings. In the category of linear topological rings ([1] chap 4), we have an excellent framework to deal with the completion.

Definition 1.1. *A filtration of ideals $\mathfrak{I}$ in R is a non-empty collection of ideals of R such that $\forall I, J \in \mathfrak{I}$, $\exists I' \in \mathfrak{I}$, $I' \subset I \cap J$.*

Lemma 1.2. *Given a filtration of ideals $\mathfrak{I}$ in R, then*

(i) $\{a + I | a \in R, I \in \mathfrak{I}\}$ forms a topological basis in R, and we call it the topology induced by $\mathfrak{I}$.

(ii) The topology induced by $\mathfrak{I}$ makes R become a topological ring.

Proof: *Omitted.*

□

Definition 1.3. *A linearly topological ring R is a topological ring such that the topology induced by the filtrtion of open ideals in R is the same as its topology.*

Proposition 1.4. *A topological ring induced by a filtration of ideals is a linearly topological ring (note this is not a completely trivial statement).*

Example 1.5. *The linear topology induced by $\{I^n | n \geq 1\}$ for an ideal $I \in R$ is called I-adic topology. Note if $I = 0$, then this topology is discrete.*

Let us denote LRings to be the category of linearly topological rings with continuous ring maps.

Proposition 1.6. *Let R, S and T be linearly topological rings, and let $R \to S$ and $R \to T$ be continuous homomorphisms. We then give $S \otimes_R T$ the linear topology defined by the ideals $I \otimes T + S \otimes J$, where I runs over open ideals in S and J runs over open ideals in T. This is easily seen to be the pushout of S and T under R in* LRings*. We conclude* LRings *has finite colimits since the initial object ($\mathbb{Z}$ with the discrete topology) and all pushouts exist in it.*

Proposition 1.7.

(i) Let $\{R_i \mid i \in \mathcal{J}\}$ be a family of objects in LRings*, and write $R = \prod_i R_i$. We give this ring the product topology, then it is the same as the linearly topology defined by the ideals of the form $\prod_i J_i$, where J_i is open in R_i and $J_i = R_i$ for almost all i. So it is easy to check $R = \prod_i R_i$ is the product in* LRings*.*

(ii) Given following morphisms in LRings

$$B \overset{f}{\underset{g}{\rightrightarrows}} C$$

then the subring $a = \{b \in B | f(b) = g(b)\}$ *with the linear topology by filtration*

$$\{J = I \cap B | I \text{ open in } B\}$$

is the equalizer in LRings.

(iii) So we conclude LRings *has any limit.*

Now we start to introduce the completion of linearly topological rings

Definition 1.8. *Let* R *be a linearly topological ring. The completion of* R *is the ring* $\widehat{R} = \lim_{\leftarrow I} R/I$*, where* I *runs over the open ideals in* R*. There is an evident map* $R \to \widehat{R}$*, and the composite* $R \to \widehat{R} \to R/I$ *is surjective so we have* $R/I = \widehat{R}/\bar{I}$ *for some ideal* $\bar{I} \subset \widehat{R}$*. These ideals form a filtered system, so we can give* $\widehat{R}$ *the linear topology for which they are a base of neighbourhoods of zero.*

It is easy to check that $\widehat{\widehat{R}} = \widehat{R}$*. We say that* R *is complete, or that it is a formal ring, if* $R = \widehat{R}$*. Thus* $\widehat{R}$ *is always a formal ring. We write* FRings *for the category of formal rings.*

Remark 1.9. *It is important to notice that the completion* $\widehat{R}$ *from an* I*-adic topology is not always the same as the* $I\widehat{R}$*-adic topology on* $\widehat{R}$ *! But it is the case when* I *is finitely generated, see [2] Algebra 96.3.*

Proposition 1.10.

(i) A linearly topological ring with the discrete topology is always complete.

(ii) Let R, S *and* T *be in* FRings*, and let* $R \to S$ *and* $R \to T$ *be continuous homomorphisms, then* $\widehat{S \otimes_R T}$ *is easily seen to be the pushout of* S *and* T *under* R *in FLings. We conclude* FRings *has finite colimits since the initial object (* $\mathbb{Z}$ *with the discrete topology) and all pushouts exist in it.*

(iii) Any limit in FRings *exists and could be created in* LRings.

Definition 1.11. *Let* $(R, \mathfrak{m})$ *be a local ring, we have a natural linear topology in* R *by the* $\mathfrak{m}$*-adic topology. So we get a functor:* LocalRings $\longrightarrow$ LRings*. In fact this functor is fully faithful because of the following lemma, and base on that we will always treat local rings as linearly topological rings.*

Lemma 1.12. *Let $A, B \in$ LRings. Suppose their linear topology is induced by filtrations $\mathfrak{A}$ and $\mathfrak{B}$ respectively. Let $f : A \longrightarrow B$ be a ring homomorphism. Then f is continuous if and only if $\forall J \in \mathfrak{B}$ there exists $I \in \mathfrak{A}$ such that $f(I) \subset J$.*

Proposition 1.13 ([2] Algebra chap 96,97)**.** *Let $(R, \mathfrak{m})$ be a Noetherian local ring, then*

(i) $(\widehat{R}, \mathfrak{m}\widehat{R})$ is still Noetherian local, and $\widehat{\mathfrak{m}} = \lim_{\leftarrow n} \mathfrak{m}/\mathfrak{m}^n \simeq \mathfrak{m}\widehat{R}$.

(ii) $(R, \mathfrak{m})$ is regular if and only if $(\widehat{R}, \widehat{\mathfrak{m}})$ is.

(iii) The topology on the completion $\widehat{R}$ is the same as the $\widehat{\mathfrak{m}}$-adic topology on it, by 1.9.

Remark 1.14. *(i) If a local ring $(R, \mathfrak{m})$ is not Noetherian, then $(\widehat{R}, \mathfrak{m}\widehat{R})$ is not necessarily local.*
(ii) When we consider the opposite category FRings^{op} *we usually write an object to be* $\mathrm{Spf}(R)$ *instead of R.*

Definition 1.15. *A formal group scheme F over a ring R is a group object in R-FRings^{op}. A formal group G of dim n over a ring R is a commutative formal group scheme such that $G \cong \mathrm{Spf}\, R[[x_1, ..., x_n]]$.*

1.2 Formal completion of pointed k-schemes

Definition 1.16. *For a k-scheme X with a rational point $e \in X(k)$ we call it a pointed k-scheme. The formal completion $\widehat{X}$ of X "along" e is defined to be the complete linearly topological ring* $\mathrm{Spf}(\widehat{\mathcal{O}_{X,e}})$*, the completion of $\mathcal{O}_{X,e}$ by $\mathfrak{m}$-adic topology. This induces a functor $Sch_k^* \xrightarrow{\widehat{(-)}} k$-$\mathrm{FRings}^{op}$ where the left one is the category of pointed k-schemes.*

Lemma 1.17. *For a pointed k-scheme (X, e), if* $\mathrm{Spec}(A) \subset X$ *is an affine neighborhood of e. Let $\mathfrak{m} \subset A$ be the maximal ideal corresponding to e, then by $A/\mathfrak{m}^n = A_{\mathfrak{m}}/\mathfrak{m}^n$ we have $\widehat{X} = \widehat{\mathcal{O}_{X,e}} \cong \widehat{A}$ where the right one is the $\mathfrak{m}$-adic completion of A.*

Theorem 1.18. *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.*

Proof: Because any finite limit is a combination of pullbacks and terminal object, we only need to show that $\widehat{(-)}$ preserves pullbacks and terminal object. The terminal object is easy to check. For the case of pullbacks, given a pullback diagram in Sch_k^* (note that the pullback in it is the same as the ordinary fiber product of schemes),

$$\begin{array}{ccc} X \times_Z Y & \longrightarrow & Y \\ \downarrow{\scriptstyle p} & & \downarrow \\ X & \longrightarrow & Z \end{array}$$

we take neighbouhoods of basepoints $\mathrm{Spec}(R) \subset Z, \mathrm{Spec}(A) \subset X, \mathrm{Spec}(B) \subset Y, \mathrm{Spec}(A \otimes_R B) \subset X \times_Z Y$. We write corresponding maximal ideals of basepoints $e_X, e_Y, e_{X\times_Z Y}$ to be $\mathfrak{m}_1, \mathfrak{m}_2, \mathfrak{m}$ respectively. It is easy to see the basepoint $e_{X\times_Z Y}$ corresponds to $A \otimes_R B \to k \otimes_R k = k \otimes_k k$, so actually $\mathfrak{m} = \mathfrak{m}_1 \otimes_R B + A \otimes_R \mathfrak{m}_2$. By the lemma above and the description of pushout of formal rings, the natural

$$\widehat{A}\widehat{\otimes}_{\widehat{R}}\widehat{B} \to \widehat{A \otimes_R B}$$

is isomorphic, then so is

$$\widehat{\mathcal{O}_{Y,e}}\widehat{\otimes}_{\widehat{\mathcal{O}_{Z,e}}}\widehat{\mathcal{O}_{X,e}} \to \widehat{\mathcal{O}_{X\times_Z Y,e}}$$

□

It is easy to check following 2 useful propositions.

Proposition 1.19. *(i) If $k \to F$ is a field extension, then for any $(X, e) \in Sch_k^*$ we have natural isomorphism $\widehat{\mathcal{O}_{X,e}}\widehat{\otimes}_k F \to \widehat{\mathcal{O}_{X_F,e_F}}$.*
(ii) If k is a field of $char(k) = p > 0$ and $(X, e) \in Sch_k^*$, then $\widehat{\mathcal{O}_{X,e}} \to \widehat{\mathcal{O}_{X,e}}$ induced by absolute Frobenius $F : X \to X$ is absolute Frobenius on $\widehat{\mathcal{O}_{X,e}}$, and $\widehat{\mathcal{O}_{X,e}}\widehat{\otimes}_{k,Frob}k \to \widehat{\mathcal{O}_{X,e}}$ induced by relative Frobenius $F : X \to X^{(p/k)}$ is the formal relative Frobenius on $\widehat{\mathcal{O}_{X,e}}$.

By Cohen structure theorem, we will see that a smooth group k-scheme of dim n can induce a formal group over k of dim n.

Theorem 1.20 (Cohen)**.** *Let $(R, \mathfrak{m})$ be a Noetherian complete local ring. Assume R is regular. If k is a field and $k \to R$ is a ring map inducing an isomorphism $k \to R/\mathfrak{m}$, then R is isomorphic as a k-algebra to a power series ring over k.*

Proof: We pick $f_1, \ldots, f_d \in \mathfrak{m}$ which map to a basis of $\mathfrak{m}/\mathfrak{m}^2$ and we consider the continuous k-algebra map $k[[x_1, \ldots, x_d]] \to R$ sending x_i to f_i. As both source and target are $(x_1, \ldots, x_d)$-adically complete, this map is surjective by [2]Algebra 96.1. On the other hand, it has to be injective because otherwise the dimension of R would be $< d$ by [2]Algebra 60.13.

□

Theorem 1.21. *If G is a smooth group k-scheme of dim n, then $\widehat{G}$ is a formal group over k of dim n.*

Proof: We know "smooth" implies "regular", so $\widehat{\mathcal{O}_{G,e}}$ is a complete regular local ring of dim n. Then by the theorem above we win.

□

2. Elliptic curves

Definition 2.1.

(i) If k is a field then by a variety over k we mean a k-scheme of finite type. A variety of equidimension 1 (resp. 2, resp. $n > 3$) is called a curve(resp. surface, resp. n-fold).

(ii) 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.

Recall that a k-scheme is said to be geometrically integral if for some algebraically closed field K containing k the scheme X_K is irreducible and reduced. By [2] Algebra 42-47, if this holds for some algebraically closed over field K then X_F is integral for every field F containing k.

It is well-known that an elliptic curve has a natural group law(i.e. a group k-scheme structure). In this chapter our goal is to prove that

1. $Div^{+,1}_{C/k}(-)$ is representable by (C, Δ).
2. The natural transformations $Div^{+,1}_{C/k}(-) \to Pic^1_{C/k}(-) \to Pic^0_{C/k}(-)$ are isomorphic for an elliptic curve.

and then by Yoneda lemma we get a natural abelian group k-scheme structure on C from the abelian group structure of $Pic^0_{C/k}(-)$. These symbols will be explained below.

However the steps above are tricky. Let us begin with some technical preliminaries about the relative Cartier effective divisor.

2.1 Relative effective Cartier divisors

Definition 2.2. *Let S be an arbitrary scheme, and let X be an S-scheme. By a relative effective Cartier divisor D on X/S we mean a closed subscheme $D \subset X$ such that*

(i) the ideal sheaf $I(D) \subset \mathcal{O}_X$ is an invertible $\mathcal{O}_X$-module, i.e. it is a locally free $\mathcal{O}_X$-module of rank 1.

(ii) D is flat over S .

For the convenience, we abbreviate the "relative effective Cartier divisor" to be RECD.

Proposition 2.3.

(i) If D_1, D_2 are RECDs on X/S, then so is $D_1 + D_2$.

(ii) Given the following pullback diagram of schemes,

$$\begin{array}{ccc} X' & \longrightarrow & S' \\ \downarrow{\scriptstyle p} & & \downarrow \\ X & \longrightarrow & S \end{array}$$

if D is a RECD on X/S, then $D \times_X X'$ is a RECD on X'/S'.

Proof:

(i) It suffices to show $D_1 + D_2$ is still flat over S. The problem is local on the X, so we can assume $X = \mathrm{Spec}(B), S = \mathrm{Spec}(A)$. This translates into the following algebra fact: Let $A \to B$ be a ring map and $h_1, h_2 \in B$. Assume the h_i are nonzerodivisors and that B/h_iB is flat over A. Then h_1h_2 is a nonzerodivisor and B/h_1h_2B is flat over A. The reason is that we have a short exact sequence

$$0 \to B/h_1B \to B/h_1h_2B \to B/h_2B \to 0$$

where the first arrow is given by multiplication by h_2. Since the outer two are flat modules over A, so is the middle one.

(ii) In the case, the flatness of $D' = D \times_X X'$ over S' automatically holds, so it suffices to show D' is an effective Cartier divisor on X'. The problem is local on X', so we can assume $X = \mathrm{Spec}(B), S = \mathrm{Spec}(A), S' = \mathrm{Spec}(A')$. We translate this as follows into algebra. Let $A \to B$ be a ring map and $h \in B$. Assume h is a nonzerodivisor and that B/hB is flat over A. Then

$$0 \to B \xrightarrow{h} B \to B/hB \to 0$$

is a short exact sequence of A-modules with B/hB flat over A. Then this sequence remains exact on tensoring over A with any module, in particular with any A-algebra A'.

□

Given a We write $Div^+_{X/S}(T)$ to be the set of RECDs on $X \times_S T/T$. By the proposition above this is a well-defined functor $Sch_S \to Sets$ (actually to $CommutativeMonoids$) for any morphism of scheme $X \to S$.

Lemma 2.4. *Let $R \to S$ be a ring map. Let M be an S-module. Assume that $R \to S$ is flat of finite presentation. If*

$$(R \to S) = \mathrm{colim}_{\lambda \in \Lambda} (R_\lambda \to S_\lambda)$$

is written as a directed colimit such that $R_\mu \otimes_{R_\lambda} S_\lambda \to S_\mu$ are isomorphisms for $\mu \geq \lambda$ and that $R_\lambda \to S_\lambda$ is of finite presentation, then for all sufficiently large λ the S_λ is flat over R_λ. (See [2] Algebra 168.1.(3)).

Proposition 2.5. *Let $\varphi : X \to S$ be a flat morphism which is locally of finite presentation. Let $D \subset X$ be a closed subscheme. If $D \longrightarrow S$ is flat locally of finite presentation as well and that all fibres $D_s \subset X_s$ are effective Cartier divisors, then D is a RECD on X/S.*

Proof: It suffices to show D is an effective Cartier divisor on X. The problem is local on X, so we can assume $X = \mathrm{Spec}(A), S = \mathrm{Spec}(R), D = \mathrm{Spec}(A/I)$.

For any $x = \mathfrak{q} \in \mathrm{Spec}(A)$, we write $s = \varphi(x) = \mathfrak{p}$. The assumption means that we may assume $I(A_\mathfrak{q} \otimes_R \kappa(\mathfrak{p}))$ is generated by a single element f which is a nonzerodivisor in $A_\mathfrak{q} \otimes_R \kappa(\mathfrak{p})$. By 2.4, there exist $R' \subset R, A', I'$ such that R' is noetherian, A' and A'/I' are flat of finite presentation over R' and that

$$A = A' \otimes_{R'} R, \quad A/I = A'/I' \otimes_{R'} R, \quad f \in I'(A'_{\mathfrak{q}'} \otimes_{R'} \kappa(\mathfrak{p}')) = I'_{\mathfrak{q}'} \otimes_{R'} \kappa(\mathfrak{p}')$$

For the short exact sequence

$$0 \to I'_{\mathfrak{q}'} \to A'_{\mathfrak{q}'} \to (A'/I')_{\mathfrak{q}'} \to 0$$

since the right two are flat $R'_{\mathfrak{p}'}$ modules, so is the left one. We get

$$0 \to I'_{\mathfrak{q}'} \otimes_{R'_{\mathfrak{p}'}} \kappa(\mathfrak{p}') \to A'_{\mathfrak{q}'} \otimes_{R'_{\mathfrak{p}'}} \kappa(\mathfrak{p}') \to (A'/I')_{\mathfrak{q}'} \otimes_{R'_{\mathfrak{p}'}} \kappa(\mathfrak{p}') \to 0$$

The left one $I'_{\mathfrak{q}'} \otimes_{R'_{\mathfrak{p}'}} \kappa(\mathfrak{p}')$ is generated by a single nonzerodivisor, then so is $I'_{\mathfrak{q}'}$ by Nakayama lemma. Since $\mathrm{Spec}(A'/I') \to \mathrm{Spec}(A')$ is a closed immersion of Noetherian schemes, so $I'_{g'}$ is generated by a single nonzerodivisor for a neighborhood $D(g')$ of $\mathfrak{q}'$. This implies $\mathrm{Spec}(A/I) \to \mathrm{Spec}(A)$ is an effective divisor on $D(g)$ where g is the image of g'.

□

Proposition 2.6. *Let $X \to S$ be a smooth morphism of schemes of relative dimension 1. Let $D \subset X$ be a closed subscheme. Consider the following conditions*

(i) $D \to S$ is finite locally free(i.e. finite+flat+locally of finite presentation).

(ii) D is a relative effective Cartier divisor on X/S.

We always have the implication

$$(i) \Rightarrow (ii)$$

If $X \to S$ is proper, then the converse is true.

Proof: Assume (i) holds. By 2.5, we can reduce to the case $S = \mathrm{Spec}(k)$ with k a field. Let $x \in X$ be a closed point. As X is smooth of relative dimension 1 over k and we see that $\mathcal{O}_{X,x}$ is a regular local ring of dimension 1. Thus $\mathcal{O}_{X,x}$ is a discrete valuation ring and hence a PID. It follows that for any $x \in D$, $\mathcal{O}_{D,x}$ is a quotient of $\mathcal{O}_{X,x}$ by a nonzerodivisor because $dim\, \mathcal{O}_{D,x} = 0$. By the noetherianess of X, D is an effective Cartier divisor of X.

Assume $X \to S$ is proper and that (ii) holds, then $D \to S$ is proper as well. Since a proper locally quasi-finite morphism is finite, so $D \to S$ a finite locally free morphism.

□

Proposition 2.7. *Let $f : X \to S$ be a proper, smooth morphism of schemes of relative dimension 1. Let $D_1, D_2 \subset X$ be closed subschemes finite locally free of degrees d_1, d_2 over S. Then $D_1 + D_2$ is finite locally free of degree $d_1 + d_2$ over S.*

Proof: We know any Cartier divisor on a curve can be associated a degree

$$\deg_k D := \sum_x \mathrm{mult}_x(D)[k(x) : k]$$

where x runs through the closed points (see [3] 7.3.1). We claim

$$\deg_{k(s)}(D_s) = \dim_{k(s)}(f_*D)_s \otimes_{\mathcal{O}_{S,s}} k(s)$$

for any RECD $g : D \to X$ on X/S, and then by the additional property of $\deg_{k(s)}(-)$ we win. The claim is right because we have the formula $\deg_{k(s)} D_s = \dim_{k_{(s)}} H^0(D_s, \mathcal{O}_{D_s})$ (see [3] 7.3.5). Then by the finiteness of D over S, we have $s^* g_* \mathcal{O}_D = g'_* \mathcal{O}_{D_s}$ (see [2] Coherent 5.1), which implies $\dim_{k(s)}(f_*D)_s \otimes_{\mathcal{O}_{S,s}} k(s) = \dim_{k_{(s)}} H^0(D_s, \mathcal{O}_{D_s})$.

□

Remark 2.8. *Actually, with the same hypothesis above, from*

$$\deg_{k(s)}(D_s) = \dim_{k(s)}(f_*D)_s \otimes_{\mathcal{O}_{S,s}} k(s)$$

we conclude that a relative effective Cartier divisor D on X/S is finite locally free of degrees d if and only if $\forall s \in S$, $\deg_{k(s)}(D_s) = d$.

Let $f : X \to S$ be a proper, smooth morphism of schemes of relative dimension 1. Given $n \geq 0$, we write $Div^{+,n}_{X/S}(T)$ to be the set of RECDs on $X \times_S T/T$ such that corresponding closed subschemes are finite locally free of degrees n over T, where T is a S-scheme. This is a well-defined functor $Sch_S \to Sets$ by the previous statement.

Proposition 2.9. *(i) Let $f : X \to S$ be a separated morphism, then any section $s : S \to X$ of f is a closed immersion.*

(ii) Let $f : X \to S$ be a proper, smooth morphism of schemes of relative dimension 1, then $Div^{+,1}_{X/S}(-)$ is representable by (X, Δ).

Proof:

(i) By the pullback diagram it is easy to see.

$$\begin{array}{ccc} S & \longrightarrow & X \\ \downarrow & & \Big\downarrow{\scriptstyle \Delta} \\ X & \xrightarrow{(id,e)} & X \times_S X \end{array}$$

(ii) First, by 2.5 $X \xrightarrow{\Delta} X \times_S X$ is a RECD on X/S of degree 1. Now we need to prove $\mathrm{Hom}_S(T, X) \to Div^{+,1}_{X/S}(T)$ induced by Δ is an isomorphism for any S-scheme T.
For the surjectivity, given $D \in Div^{+,1}_{X/S}(T)$ we see $D \to T$ is finite locally free of degree 1, which must be an isomorphism. So D is from a section $T \to X \times_S T$.
For the injectivity, we need to check if two sections $e_1, e_2 : T \to X \times_S T$ are the same closed subschemes of $X \times_S T$, then $e_1 = e_2$. This is easy.

□

Proposition 2.10. *Let $f : X \to S$ be a flat morphism between Noetherian schemes and let $D \subset X$ be a locally principle closed subscheme such that for each $s \in S$, $D_s \subset X_s$ is an effective Cartier divisor. Then $D \to S$ is flat.*

Proof: Let $x \in D \subset X$ with $s = f(x)$. We need to show that $\mathcal{O}_{D,x}$ is a flat $\mathcal{O}_{S,s}-$ module. By the local criterion for flatness, this is equivalent to the vanishing of $\mathrm{Tor}_1\, \mathcal{O}_{S,s}\,(k(s), \mathcal{O}_{D,x})$. Consider the long exact sequence associated to the ideal sequence

$$0 \to \mathcal{I}_{D,x} \to \mathcal{O}_{X,x} \to \mathcal{O}_{D,x} \to 0$$

We have

$$0 = \mathrm{Tor}_1^{\mathcal{O}_{S,s}}\,(k(s), \mathcal{O}_{X,x}) \to \mathrm{Tor}_1^{\mathcal{O}_{S,s}}\,(k(s), \mathcal{O}_{D,x}) \to \mathcal{I}_{D,x} \otimes k(s) \to \mathcal{O}_{X,x} \otimes k(s) = \mathcal{O}_{X_s,x}$$

Since the first term is zero by flatness of $X \to S$, the required vanishing would follow from injectivity of the last map. To see this injectivity, let $r \in \mathcal{O}_{X_s,x}$ be a regular element cutting out D_s at $x \in X_s$ and let $f_x \in \mathcal{O}_{X,x}$ be a principle generated element of $\mathcal{I}_x$. Then r and $\bar{f_x}$ generate the same ideal $I_{D_s,x}$ in $\mathcal{O}_{X,x} \otimes k(s)$, so r and $\bar{f_x}$ are the same up to a unit by the fact that r is a regular element. Now multiplication by f_x induces a map $\mathcal{O}_{X,x} \otimes k(s) \overset{f_x \otimes 1}{\to} \mathcal{O}_{X,x} \otimes k(s)$ which is injective with image $I_{D_s,x}$. Thus we have an injective map which factors as

$$\mathcal{O}_{X,x} \otimes k(s) \overset{f_x \otimes 1}{\to} \mathcal{I}_{D,x} \otimes k(s) \to \mathcal{O}_{X,x} \otimes k(s)$$

where the first map is a surjection and so the required map is an injection.

□

2.2 The group structure on elliptic curves

Now we begin to prove there exist a natural (commutative) group scheme structure on an elliptic curve. Actually, we will see this structure is unique in the next chapter about abelian varieties.

Definition 2.11. *Let $f : X \to S$ be a morphism of schemes, we define relative Picard group $Pic(X/S) = Pic(X)/f^*Pic(S)$. It is easy to check $Pic_{X/S}(T) = Pic(X \times_S T/T)$ is a functor $Sch_S \to Abel$.*

We know for any proper integral curve C over a field k, there is natural degree map $Pic(C) \to \mathbb{Z}$ by following diagram.

$$\begin{array}{ccccccc} K(C)^* & \longrightarrow & Div(C) & \longrightarrow & Pic(C) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Deg}_k} & \swarrow & & & \\ & & \mathbb{Z} & & & & \end{array}$$

Remark 2.12. *So for a proper and geometrically integral curve C over k and $n \in \mathbb{Z}$, we can define a subfunctor $Pic^n_{C/k}(T) \subset Pic_{C/k}(T)$ to be the set of $[\mathcal{L}] \in Pic_{C/k}(T)$ such that $\forall t \in T$, $\mathrm{Deg}_{k(t)} \mathcal{L}_t = n$. Note that if there exsits $\mathcal{L} \in Pic(C)$ such that $\mathrm{Deg}_k \mathcal{L}_0 = 1$, then $Pic^m_{C/k}(-)$ and $Pic^n_{C/k}(-)$ are naturally isomorphic by tensoring $\pi_1^* \mathcal{L}_0^{\otimes m-n}$.*

Proposition 2.13. *Let C be a smooth proper and geometrically integral curve over k. We can define a natural transformation $Div^{+,n}_{C/k}(-) \to Pic^n_{C/k}(-)$ by $D \mapsto [\mathcal{L}(D)]$ when $n \geq 0$ because of 2.8.*

Theorem 2.14 (Grauert). *Let $f : X \to Y$ be a proper morphism of locally noetherian schemes and let $\mathcal{F}$ be a coherent $\mathcal{O}_X$-module flat over Y. If Y is reduced and the function*

$$y \mapsto \dim_{k(y)} H^i\left(X_y, \mathcal{F}_y\right)$$

is locally constant on Y for some i, then $R^i f_*\mathcal{F}$ is locally free and the canonical homomorphism

$$\left(R^i f_*\mathcal{F}\right)_y \otimes_{\mathcal{O}_{Y,y}} k(y) \to H^i\left(X_y, \mathcal{F}_y\right)$$

is an isomorphism for any $y \in Y$.

Theorem 2.15 (Cohomology and Base Change). *(see [4] III, 12.11)*
Let $f : X \to Y$ be a proper morphism of locally noetherian schemes, and let $\mathcal{F}$ be a coherent sheaf on X, flat over Y. Then:

1. *Let y be a point of Y, if the natural map*

$$\varphi^i(y) : R^i f_*(\mathcal{F}) \otimes k(y) \to H^i\left(X_y, \mathcal{F}_y\right)$$

   is surjective, then it is an isomorphism.

2. *Assume that for any $y \in Y$, $\varphi^i(y)$ is surjective. Then the following conditions are equivalent:*
   (a) For any $y \in Y$, $\varphi^{i-1}(y)$ is surjective;
   (b) $R^i f_*(\mathcal{F})$ is locally free of finite rank.

Theorem 2.16 (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 reduced k-scheme of finite type T.*
(Actually this is true for any k-scheme T, but in the general case the proof is much harder. Note it is enough to get the group k-scheme structure of C if we can prove the case above.)

Proof: We write X to be the $C \times_k T$. For the surjectivity, given $[\mathcal{M}] \in Pic^1_{C/k}(T) = Pic^1(X/T)$, by Riemann–Roch theorem we have

$$\dim_{k(t)} H^0\left(X_t, \mathcal{M}_t\right) = 1$$

$$\dim_{k(t)} H^1\left(X_t, \mathcal{M}_t\right) = 0$$

Since $p : X \to T$ is a proper morphism, and $\mathcal{M}$ is flat over T, we can apply the theorem of cohomology and base change 2.15. Looking first at $R^1 p_*(\mathcal{M})$, since the cohomology along the fibres is 0 , the map $\varphi^1(t)$ in 2.15 is automatically surjective, hence an isomorphism,

so we conclude that $R^1p_*(\mathcal{M})$ is 0. In particular, it is locally free, so we deduce from part (ii) of the theorem that $\varphi^0(t)$ is also surjective. Therefore, it is an isomorphism, and since $\varphi^{-1}(t)$ is always surjective, we see that $p_*(\mathcal{M})$ is locally free of rank 1 .

Now replacing $\mathcal{M}$ by $\mathcal{M}\otimes p^*p_*(\mathcal{M})^\vee$ in $Pic^0(X/T)$, we may then assume that $p_*(\mathcal{M}) \cong \mathcal{O}_T$. The section $1 \in \Gamma(T, \mathcal{O}_T)$ gives a section $s \in \Gamma(X, \mathcal{M})$ (i.e a map of $\mathcal{O}_X$-module $s : O_X \to \mathcal{M}$). We claim s defines an effective Cartier divisor $Z \subseteq X$.

Taking the dual of s we get a morphism $s^\vee : \mathcal{M}^\vee \to \mathcal{O}_X$, and then taking the image we get a locally principle ideal sheaf of $\mathcal{O}_X$ and hence get a locally principle closed subscheme $Z \subset X$. First, we claim $Z \to T$ is flat. By $\mathcal{O}_T \xrightarrow{\cong} p_*(\mathcal{M})$ we have $O_{k(t)} \xrightarrow{\cong} t^*p_*\mathcal{M}$. $\forall t \in T$, consider the following diagram.

$$\begin{array}{ccc} \mathcal{O}_{k(t)} & \xrightarrow{\cong} & t^*p_*\mathcal{M} \\ & \searrow & \downarrow \cong \\ & & p'_*t'^*\mathcal{M} \end{array}$$

By the theorem of cohomology and base change 2.15, the vertical arrow is isomorphic and so is the left arrow. That means $\mathcal{O}_{k(t)} \to p'_*t'^*\mathcal{M}$ is a non-zero map, and hence so are $\mathcal{O}_{X_t} \to \mathcal{M}_t$ and $\mathcal{M}_t^\vee \to \mathcal{O}_{X_t}$. Therefore $Z_t \subset X_t$ is not isomorphic(i.e non-trivial closed subscheme). But any nontrivial closed immersion to $X_t = C \times_k k(t)$ is an effective Cartier divisor, so $Z \to T$ is flat by 2.10. Then $Z \to X$ is a RECD on X/T and $s^\vee : \mathcal{M}^\vee \to \mathcal{O}_X$ is injective by 2.5. It is easy to see $Z \in Div^{+,1}_{C/k}(T)$ and $Z \mapsto [\mathcal{M}]$. (Note that we have not used the reduceness of T through proving the surjectivity.)

For the injectivity. Let $D_1, D_2 \in Div^{+,1}_{C/k}(T)$ such that $\mathcal{L}(D_1) = \mathcal{L}(D_2) \otimes p^*(\mathcal{N})$ for some $\mathcal{N} \in Pic(T)$. For any $t \in T$, pulling back to X_t we have $\mathcal{L}(D_{1t}) = \mathcal{L}(D_{2t})$. We claim $D_{1t} = D_{2t}$. Since $\mathcal{L}(D_{1t}) = \mathcal{L}(D_{2t})$ we have $D_{1t} = D_{2t} + div(f)$ for some $f \in K(X_t)^*$. By the fact $\mathcal{L}_X(D)(X) = \{f \in \mathcal{K}_X^*(X) | \operatorname{div}(f) + D \geq 0\} \cup \{0\}$ when D is a Cartier divisor on an integral scheme X, we conclude $1 \in \mathcal{L}(D_{1t})(X_t)$ and $1 \in \mathcal{L}(D_{2t})(X_t)$ when we consider them as sub $\mathcal{O}_{X_t}$-modules of $\mathcal{K}_{X_t}$ with $1 \in \mathcal{K}^*_{X_t}(X_t) = K(X_t)^*$. However, Riemann–Roch theorem shows that $\dim_{k(t)} H^0\left(X_t, \mathcal{L}(D_{1t})\right) = 1 = \dim_{k(t)} H^0\left(X_t, \mathcal{L}(D_{2t})\right)$, which implies $k(t) = \mathcal{O}_{X_t}(X_t) = \mathcal{L}(D_{1t})(X_t) = \mathcal{L}(D_{2t})(X_t) \subset K(X_t)$, and hence $f \in \mathcal{O}_{X_t}(X_t)$, $D_{1t} = D_{2t}$. So D_1, D_2 are closed subschemes of X having the same underlying spaces. By 2.9, both D_1 and D_2 are isomorphic to T, hence D_1, D_2 are reduced closed subschemes of X having the same underlying spaces, which means $D_1 = D_2$.

□

Corollary 2.17. *Let (C, e) be an elliptic curve over a field k, then $Pic^0_{C/k}(-)$ is representable by C with $\mathcal{L}(\Delta) \otimes \pi_1^* \mathcal{L}(-e)$ on $C \times_k C$, which induces a natural commutative group k-scheme structure on C with the zero map e.*

Proof: By 2.12 2.16, we conclude $Pic^0_{C/k}(-)$ is representable by C with $\mathcal{L}(\Delta) \otimes \pi_1^* \mathcal{L}(-e)$ as a functor

$$\text{Reduced finite type } Sch_k \to Sets$$

Note the left category does not necessarily have any finite product, but it has terminal object $\mathrm{Spec}(k)$, and $C \times_k C$ is reduced because C is geometrically integral. So we can still get a natural commutative group k-scheme structure from the representability.

□

3. Group schemes and algebraic groups

We have known that the elliptic curve is group k-scheme. Now we take some effort on the property of group scheme over general base scheme.

3.1 Basic properties of group schemes

Definition 3.1. *(i) 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:*

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

and

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

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

(ii) 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 $m = m \circ s : G \times_S G \to G$.

(iii) 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 $f \circ i_1 = i_2 \circ f$.)

Remark 3.2. *In practice it will usually either be understood what m, i and e are, or it will be unnecessary to make them explicit; in such case we will simply speak about "a group scheme G over S " without further specification. (In fact, we already did so in parts (ii) and (iii) of the definition.)*

If G is a group scheme over S and if $S' \to S$ is a morphism of schemes, then the pull-back $G' := G \times_S S'$ inherits the structure of an S'-group scheme. In particular, if $s \in S$ then the fibre $G_s := G \times_S \mathrm{Spec}(k(s))$ is a group scheme over the residue field $k(s)$.

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 usually called "multiplication by* n *".*

Example 3.3. *1. The additive group. Let* S *be a base scheme. The additive group over* S*, denoted* $\mathbb{G}_{a,S}$*, corresponds to the functor which associates to an* S*-scheme* T *the additive group* $\Gamma(T, O_T)$*. For simplicity, let us assume that* $S = \mathrm{Spec}(R)$ *is affine. Then* $\mathbb{G}_{a,S}$ *is represented by the affine* S*-scheme* $\mathbb{A}^1_S = \mathrm{Spec}(R[x])$*. The structure of a group scheme is given, on rings, by the following homomorphisms:*

2. The multiplicative group. This group scheme, denoted $\mathbb{G}_{m,S}$*, represents the functor which associates to an* S*-scheme* T *the multiplicative group* $\Gamma(T, O_T)^*$ *of invertible elements of* $\Gamma(T, O_T)$*. As a scheme,* $\mathbb{G}_m = \mathrm{Spec}\left(O_S[x, x^{-1}]\right)$*. The structure of a group scheme is defined by the homomorphisms given by*
$x \mapsto x \otimes x$ *defining the multiplication;*
$x \mapsto x^{-1}$ *defining the inverse;*
$x \mapsto 1$ *defining the identity element.*

3. n*-th Roots of unity. Given a positive integer* n*, we have an* S*-group scheme* $\mu_{n,S}$ *which associates to an* S*-scheme* T *the subgroup of* $\mathbb{G}_m(T)$ *of elements whose order divides* n*. The* O_S*-algebra defining this group scheme is* $O_S[x, x^{-1}]/(x^n - 1)$ *with the group law given as in Example 2. Put differently,* $\mu_{n,S}$ *is a closed subgroup scheme of* $\mathbb{G}_{m,S}$*.*

4. p^n*-th Roots of zero. Let* p *be a prime number and suppose that* $\mathrm{char}(S) = p$*. Consider the closed subscheme* $\alpha_{p^n,S} \subset \mathbb{G}_{a,S}$ *defined by the ideal* $\left(x^{p^n}\right)$*; so* $\alpha_{p^n,S} := \mathrm{Spec}\left(O_S[x]/\left(x^{p^n}\right)\right)$*. As is not hard to verify, this is in fact a closed subgroup scheme of* $\mathbb{G}_{a,S}$*. If* $S = \mathrm{Spec}(k)$ *for a field* k *of characteristic* p *then geometrically* $\alpha_{p^n,k}$ *is just a "fat point" (a point together with its* $(p^n - 1)$ *st infinitesimal neighbourhood); but as a group scheme it has an interesting structure. If* T *is an* S*-scheme then* $\alpha_{p^n}(T) = \left\{ f \in \Gamma(T, O_T) \mid f^{p^n} = 0 \right\}$*, with group structure given by addition.*

5. Constant group schemes. Let M *be an arbitrary (abstract) group. Let* $M_S := S^{(M)}$*, the disjoint union of copies of* S *indexed by the set* M*. The group structure on* M *clearly induces the structure of a group functor on* M_S *(multiplication of functions), so that* M_S *becomes a group scheme. And it is easy to check that* $(M_S, G(S))$ *induces adjoint pairs* $Grp \rightleftharpoons Grp(Sch_S)$ *and* $AbGrp \rightleftharpoons AbGrp(Sch_S)$*.*

Proposition 3.4. *(i) Let $f : Y \to X$ be a separated morphism of schemes. If $s : X \to Y$ is a section of f then s is a closed immersion.*

(ii) An S-group scheme G is separated if and only if the unit section e is a closed immersion.

Proof: (i) we can check following diagram is cartesian diagram, then by the separateness it is done.

$$\begin{array}{ccc} X & \xrightarrow{s} & Y \\ {\scriptstyle s}\downarrow & & \downarrow{\scriptstyle \Delta} \\ Y & \xrightarrow[id_Y \times (s \circ f)]{} & Y \times_X Y \end{array}$$

(ii) Suppose the unit section e is a closed immersion. By the following cartesian diagram we win.

$$\begin{array}{ccc} G & \xrightarrow{\pi} & S \\ {\scriptstyle \Delta}\downarrow & & \downarrow{\scriptstyle e} \\ G \times_S G & \xrightarrow[m \circ (id_G \times i)]{} & G \end{array}$$

□

Remark 3.5. *Particularly, any group k-scheme is separated.*

Now we introduce an important lemma about differentials on the group scheme.

Lemma 3.6. *Let (G, m, e, i) be a group scheme over the scheme S. Denote $f : G \to S$ the structure morphism. Then there exist canonical isomorphisms*

$$\Omega_{G/S} \cong f^* e^* \Omega_{G/S}$$

In particular, if S is the spectrum of a field, then $\Omega_{G/S}$ is a free $\mathcal{O}_G$-module.

Proof: By Morphisms, Lemma 32.10 we have

$$\Omega_{G \times_S G/G} = \pi_1^* \Omega_{G/S}$$

where on the left hand side we view $G \times_S G$ as a scheme over G using π_2. Let $\tau : G \times_S G \to G \times_S G$ be the "shearing map" given by $(g, h) \mapsto (m(g, h), h)$ on points. This map is an automorphism of $G \times_S G$ viewed as a scheme over G via the projection π_2. Combining these two remarks we obtain an isomorphism

$$\tau^* \pi_1^* \Omega_{G/S} \to \pi_1^* \Omega_{G/S}$$

Since $\pi_1 \circ \tau = m$ this can be rewritten as an isomorphism

$$m^*\Omega_{G/S} \to \pi_1^*\Omega_{G/S}$$

Pulling back this isomorphism by $(e \circ f, \mathrm{id}_G) : G \to G \times_S G$ and using that $m \circ (e \circ f, \mathrm{id}_G) = \mathrm{id}_G$ and $\mathrm{pr}_0 \circ (e \circ f, \mathrm{id}_G) = e \circ f$ we obtain an isomorphism

$$\Omega_{G/S} \to f^*e^*\Omega_{G/S}$$

as desired. If S is the spectrum of a field, then any $\mathcal{O}_S$-module on S is free and the final statement follows.

□

Lemma 3.7 ([2] Variety 25.2)**.** *Let k be a field. Let X be a scheme over k. Assume (1) X is locally of finite type over k, (2) $\Omega_{X/k}$ is locally free, (3) X is reduced, and (4) k is perfect. Then the structure morphism $X \to \mathrm{Spec}(k)$ is smooth.*

Proof: Let $x \in X$ be a point. As X is locally Noetherian (see [2]Morphisms, Lemma 15.6 there are finitely many irreducible components $X_1, \ldots, X_n$ passing through x (see [2]Properties, Lemma 5.5 and [2]Topology, Lemma 9.2). Let $\eta_i \in X_i$ be the generic point. As X is reduced we have $\mathcal{O}_{X,\eta_i} = \kappa(\eta_i)$, see [2]Algebra, Lemma 25.1. Moreover, $\kappa(\eta_i)$ is a finitely generated field extension of the perfect field k hence separably generated over k (see [2]Algebra, Section 42). It follows that $\Omega_{X/k,\eta_i} = \Omega_{\kappa(\eta_i)/k}$ is free of rank the transcendence degree of $\kappa(\eta_i)$ over k. By [2]Morphisms, Lemma 28.1 we conclude that $\dim_{\eta_i}(X_i) = \mathrm{rank}_{\eta_i}\left(\Omega_{X/k}\right)$. Since $x \in X_1 \cap \ldots \cap X_n$ we see that

$$\mathrm{rank}_x\left(\Omega_{X/k}\right) = \mathrm{rank}_{\eta_i}\left(\Omega_{X/k}\right) = \dim\left(X_i\right).$$

Therefore $\dim_x(X) = \mathrm{rank}_x\left(\Omega_{X/k}\right)$, see [2]Algebra, Lemma 114.5. It follows that $X \to \mathrm{Spec}(k)$ is smooth at x for example by [2]Algebra, Lemma 140.3.

□

Definition 3.8. *Let k be a field. An (locally) algebraic group is s a group scheme over k which is of (locally) finite type over k.*

Corollary 3.9. *Let G be a locally algebraic group over a field k. If $G \otimes_k K$ is reduced for some perfect field K containing k, then G is smooth over k. In particular, any geometrically reduced locally algebraic group over k is smooth.*

We close this subsection with a useful proposition.

Proposition 3.10. *Let G be a commutative group scheme which is finite locally free over* $\mathrm{Spec}(R)$ *of order n for some ring R. Then n kills G, i.e., the multiplication by n map $[n] : G \to G$ is the zero map.*

Proof: See [5] 3.3.

□

3.2 Connected components of algebraic groups

Let G be a group scheme over a field k. By 3.4, G is separated over k. The image of the identity section is a single closed point $e = e_G$.

Assume in addition that G is a locally algebraic group over k. Then the scheme G is locally noetherian, hence locally connected. If we write G^0 for the connected component of G containing e, it follows that G^0 is an open and closed subscheme of G. We call G^0 the identity component of G.

Proposition 3.11. *(i) The identity component G^0 of a locally algebraic group G over k is geometrically connected. And for any field extension $k \subset K$, we have $(G^0)_K = (G_K)^0$.*
(ii) The identity component G^0 of a locally algebraic group G over k is an open and closed subgroup k-scheme of G.

Proof: (i) More generally, we show that if X is a connected k-scheme, that has a rational point $x \in X(k)$ then X is geometrically connected, see [2] Variety 7.14. For the second statement, $(G^0)_K$ is a open and closed connected subscheme of $(G_K)^0$ containing e_K, so it must be $(G_K)^0$.
(ii) By [2]Variety 7.4 we see $G^0 \times_k G^0$ is connected open subscheme of $G \times_k G$ containing 0×0, so $G^0 \times_k G^0 \to G \times_k G \to G$ factors through G^0. Similarly, $G^0 \xrightarrow{i} G$ factors through G^0. So we conclude that G^0 is an open and closed subgroup k-scheme of G.

□

If X is a topological space then $\pi_0(X)$ denotes the set of connected components of X. The purpose of the following section is to discuss a scheme-theoretic analogue of this for schemes that are of finite type over a field k. To avoid confusion we shall use the notation π_0 in the topological context and ω_0 for the scheme-theoretic analogue.

If X/k is of finite type then $\omega_0(X)$ will be an étale k-scheme, and $X \mapsto \omega_0(X)$ is a covariant functor. Furthermore, if G is a algebraic group over k, then $\omega_0(G)$ inherits a natural structure of a group scheme; it is called the component group (scheme) of G.

Let us recall that an étale morphism of schemes $f : X \to Y$ is locally formal étale and locally of finite presentation; see [2]Algebra 143.

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, (see [6]) and Galois theory tells us that $L \mapsto \mathrm{Gal}\,(k_s/L)$ gives a bijection between the field extensions of k inside k_s and the closed subgroups of Γ_k. Finite extensions of k correspond to open subgroups of Γ_k. A reference is [7], Sect. 4.1.

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. Hence 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

$$\mathrm{Et}_{/k} \xrightarrow{\mathrm{eq}} \Gamma_k\text{-sets}\ .$$

write a Γ_k-set Y as a union of orbits, say $Y = \bigsqcup_{\alpha\in I} (\Gamma_k \cdot y_\alpha)$, let $k \subset L_\alpha$ be the finite field extension (inside k_s) corresponding to the open subgroup $\mathrm{Stab}\,(y_\alpha) \subset \Gamma_k$, and associate to Y the k-scheme $\mathrm{L}_{\alpha\in I}\,\mathrm{Spec}\,(L_\alpha)$. Up to isomorphism of k-schemes this does not depend on the chosen base points of the Γ_k-orbits, and it gives a quasi-inverse to the functor $X \mapsto X\,(k_s)$. Note that $X(k_s)$ is finite if and only if X is finite over k.

This equivalence of categories induces an equivalence between the corresponding categories of (commutative) group objects. This gives the following result.

Proposition 3.12. *Let $k \subset k_s$ and $\Gamma_k = \mathrm{Gal}\,(k_s/k)$ be as above. Associating to an étale (commutative) k-group scheme G the (commutative) group $G\,(k_s)$ with its natural Γ_k-action gives an equivalence of categories*

$$\left(\begin{array}{c}\textit{(finite) étale}\\ \textit{(commutative)}k\textit{-group schemes}\end{array}\right) \xrightarrow{eq} (finite)(commutative)\Gamma_k\textit{-groups},$$

where by a Γ_k-group we mean an (abstract) group equipped with a continuous left action of Γ_k by group automorphisms.

Now we turn to the main theorem of this subsection.

Lemma 3.13. *(i) Let k be a field. Let X be a scheme over k. Let A be a k-algebra. Let*

$V \subset X_A$ be a quasi-compact open. Then there exists a finitely generated k subalgebra $A' \subset A$ and a quasi-compact open $V' \subset X_{A'}$ such that $V = V'_A$.

(ii) Let $\bar{k}/k$ be a (possibly infinite) Galois extension. Let X be a scheme over k. Let $\bar{T} \subset X_{\bar{k}}$ have the following properties
(1) $\bar{T}$ is a closed subset of $X_{\bar{k}}$,
(2) for every $\sigma \in \mathrm{Gal}(\bar{k}/k)$ we have $\sigma(\bar{T}) = \bar{T}$. Then there exists a closed subset $T \subset X$ whose inverse image in $X_{\bar{k}}$ is $\bar{T}$.

(iii) Let $X \to Y$ be an open surjective map of spaces. If for any $y \in Y$, $f^{-1}(y)$ is connected, then $\pi_0(X) \to \pi_0(Y)$ is bijective.

Proof: (i) Let $U_1, \ldots, U_n$ be finitely many affine opens of X such that $V \subset \bigcup U_{i,A}$. Say $U_i = \mathrm{Spec}\,(R_i)$. Since V is quasi-compact we can find finitely many $f_{ij} \in R_i \otimes_k A, j = 1, \ldots, n_i$ such that $V = \bigcup_i \bigcup_{j=1,\ldots,n_i} D\,(f_{ij})$ where $D\,(f_{ij}) \subset U_{i,A}$ is the corresponding standard open. (We do not claim that $V \cap U_{i,A}$ is the union of the $D\,(f_{ij})\,, j = 1, \ldots, n_i.$) It is clear that we can find a finitely generated k-subalgebra $A' \subset A$ such that f_{ij} is the image of some $f'_{ij} \in R_i \otimes_k A'$. Set $V' = \bigcup D\left(f'_{ij}\right)$ which is a quasi-compact open of $X_{A'}$. Denote $\pi : X_A \to X_{A'}$ the canonical morphism. We have $\pi(V) \subset V'$ as $\pi\left(D\left(f_{ij}\right)\right) \subset D\left(f'_{ij}\right)$. If $x \in X_A$ with $\pi(x) \in V'$, then $\pi(x) \in D\left(f'_{ij}\right)$ for some i, j and we see that $x \in D\left(f_{ij}\right)$ as f'_{ij} maps to $f_{ij.}$. Thus we see that $V = \pi^{-1}\left(V'\right)$ as desired.
(ii) This lemma immediately reduces to the case where $X = \mathrm{Spec}(A)$ is affine. In this case, let $\bar{I} \subset A \otimes_k \bar{k}$ be the radical ideal corresponding to $\bar{T}$. Assumption (2) implies that $\sigma(\bar{I}) = \bar{I}$ for all $\sigma \in \mathrm{Gal}(\bar{k}/k)$. Pick $x \in \bar{I}$. There exists a finite Galois extension k'/k contained in $\bar{k}$ such that $x \in A \otimes_k k'$. Set $G = \mathrm{Gal}\,(k'/k)$. Set

$$P(T) = \prod_{\sigma \in G} (T - \sigma(x)) \in \left(A \otimes_k k'\right)[T]$$

It is clear that $P(T)$ is monic and is actually an element of $\left(A \otimes_k k'\right)^G [T] = A[T]$ (by basic Galois theory). Moreover, if we write $P(T) = T^d + a_1 T^{d-1} + \ldots + a_0$ the we see that $a_i \in I := A \cap \bar{I}$. By [2]Algebra, Lemma 38.5 we see that x is contained in the radical of $I\left(A \otimes_k \bar{k}\right)$. Hence $\bar{I}$ is the radical of $I\left(A \otimes_k \bar{k}\right)$ and setting $T = V(I)$ is a solution.
(iii) Let $T \subset Y$ be a connected component. Note that T is closed. The lemma follows if we show that $f^{-1}(T)$ is connected because any connected subset of X maps into a connected component of Y. Suppose that $f^{-1}(T) = Z_1 \sqcup Z_2$ with Z_1, Z_2 closed. For any $t \in T$ we see that $f^{-1}(\{t\}) = Z_1 \cap f^{-1}(\{t\}) \sqcup Z_2 \cap f^{-1}(\{t\})$. By (1) we see $f^{-1}(\{t\})$ is connected we conclude that either $f^{-1}(\{t\}) \subset Z_1$ or $f^{-1}(\{t\}) \subset Z_2$. In other words $T = T_1 \sqcup T_2$ with

$f^{-1}(T_i) = Z_i$. By (2) we conclude that T_i is closed in Y. Hence either $T_1 = \emptyset$ or $T_2 = \emptyset$ as desired.

□

Proposition 3.14. *(i) If X is a k-scheme of finite type, then $\pi_0(X_{k_s})$ is a continuous Γ_k-set.*

(ii) If X is a finite étale k-scheme, then we have a natural isomorphism $X(k_s) \to \pi_0(X_{k_s})$ of Γ_k-sets.

(iii) If X is a k-scheme of finite type, then $\pi_0(X_{k_s})/\Gamma_k \to \pi_0(X)$ is bijective.

(iv) If X, Y are k-schemes of finite type, then $\pi_0(X_{k_s} \times_{k_s} Y_{k_s}) \to \pi_0(X_{k_s}) \times \pi_0(Y_{k_s})$ is bijective.

(v) If X is a k-scheme of finite type, Y is a finite étale k-scheme, then the image of the injection $\mathrm{Hom}_k(X, Y) \to \mathrm{Hom}_{k_s}(X_{k_s}, Y_{k_s})$ consists of k_s-morphisms such that following diagram (of k-morphisms) is commutative for any $g \in \Gamma_k$.

$$\begin{array}{ccc} X_{k_s} & \xrightarrow{f_s} & Y_{k_s} \\ \downarrow{\scriptstyle g} & & {\scriptstyle g}\downarrow \\ X_{k_s} & \xrightarrow{f_s} & Y_{k_s} \end{array}$$

Proof:

(i) Given a connected component Z of X_{k_s}. By (i) of 3.13, taking $A = k_s$ and $V = Z$ we see that $Stab(Z)$ contains an open subgroup and hence is open.

(ii) We know $X(k_s) = X_{k_s}(k_s)$. However, X_{k_s} is finite copies of $\mathrm{Spec}(k_s)$, so it is clear that $X_{k_s}(k_s) \cong \pi_0(X_{k_s})$. By the following diagram, this isomorphism preserves Γ_k-action.

$$\begin{array}{ccc} \mathrm{Spec}(k_s) & \xrightarrow{\varphi} & X_{k_s} \\ \downarrow{\scriptstyle g} & & {\scriptstyle g}\downarrow \\ \mathrm{Spec}(k_s) & \xrightarrow{g.\varphi} & X_{k_s} \end{array}$$

(iii) The surjection is clear. For the injection, let Z be a connected component of X. If $p^{-1}(Z)$ contains 2 orbits under Γ_k-action, we get a contradiction by (ii) of 3.13.

(iv) Since $X \times_k Y \to Y$ is universally open, it is easy to check $\pi_0(X_{k_s} \times_{k_s} Y_{k_s}) \to \pi_0(X_{k_s}) \times \pi_0(Y_{k_s})$ is bijective by (iii) of 3.13.

(v) It is easy to reduce to the affine case since Y is affine. Then using Galois decent we win.

□

Theorem 3.15. *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.

Proof: (i) We can define $\omega_0(X)$ to be a (unique) finite étale k-scheme such that $\omega_0(X)(k_s) \cong \pi_0(X_{k_s})$ as Γ_k-sets by (i) of 3.14. Let us consider the following diagram.

$$\begin{array}{ccccc} \mathrm{Hom}_k(X,Y) & \longrightarrow & \mathrm{Hom}_{\Gamma_k - Sets}(\pi_0(X_{k_s}), \pi_0(Y_{k_s})) & \xrightarrow{\simeq} & \mathrm{Hom}_k(\omega_0(X), Y) \\ \downarrow & & \downarrow & & \\ \mathrm{Hom}_{k_s}(X_{k_s}, Y_{k_s}) & \xrightarrow{\simeq} & \mathrm{Hom}_{Sets}(\pi_0(X_{k_s}), \pi_0(Y_{k_s})) & & \end{array}$$

By (v) of 3.14, we conclude two vertical arrows have the same image, so the first horizontal arrow is bijective. Now we get that $\omega_0 : \mathrm{FT}_{/k} \rightleftharpoons fi\,\mathrm{ET}_{/k} : U$ is an adjoint pair. By (ii) of 3.14 we have natural isomorphism $\omega_0 \circ U(Y) \cong Y$ for any finite étale k-scheme Y.
(ii) We know $X \to \omega_0(X)$ is induced by the identity map of $\pi_0(X_{k_s}) \to \pi_0(\omega_0(X)_{k_s})$. By (iii) of 3.14 we have $\pi_0(X) \to \pi_0(\omega_0(X))$ is bijective. However $\omega_0(X)$ is a finite disjoint of spectra of fields, the statement must hold.

□

Remark 3.16. *By (iv) of 3.14, ω_0 and U preserve finite products. So this adjoint pair can extend to the corresponding (commutative) group objects.*

3.3 FPPF quotients

Consider an action of an S-group scheme G on an S-scheme X. In general there is not a simple procedure to construct a "good" quotient of X by G in the category $\mathrm{Sch}_{/S}$. Of course we have the notion of a categorical quotient, but this is only a "best possible approximation in the given category", and its definition gives no clues about whether there exists a categorical quotient and, if so, how to describe it. Most approaches to the formation of quotients follow the same pattern:

(a) replace the category $\mathrm{Sch}_{/S}$ of S-schemes by some "bigger" category, in which the formation of quotients is easier;
(b) form the quotient $Y := X/G$ in this bigger category;
(c) study under which assumptions the quotient Y is (representable by) a scheme.
Thus, for instance, in context of geometric quotients the "bigger" category is the category of locally ringed spaces over S. (In $\mathrm{LRS}_{/S}$ any colimit exists and is created in $\mathrm{RS}_{/S}$, see [8] I. §1. 1.6.)

We shall use some notions that are explained in more detail in [9]. Let S be a scheme. We write $(S)_{\mathrm{FPPF}}$ for the big fppf site of S, i.e., the category $\mathrm{Sch}_{/S}$ of S-schemes equipped with the fppf topology. We write $\mathrm{FPPF}(S)$ for the category of sheaves on $(S)_{\mathrm{FPPF}}$.

The fppf topology is coarser than the canonical topology; this means that for every S scheme X the presheaf $h_X = \mathrm{Hom}_S(-, X)$ is a sheaf on $(S)_{\mathrm{FPPF}}$ (see [9] 4.1.2). Via $X \mapsto h_X$ we can identify $\mathrm{Sch}_{/S}$ with a full subcategory of $\mathrm{FPPF}(S)$. We shall usually simply write X for h_X.

Denote by $\mathrm{ShGr}_{/S}$ and $\mathrm{ShAb}_{/S}$ the categories of sheaves of groups, respectively sheaves of abelian groups, on $(S)_{\mathrm{FPPF}}$. The category $\mathrm{ShAb}_{/S}$ is abelian. Unless specified otherwise, we shall from now on view the category of S-group schemes as a full subcategory of $\mathrm{ShGr}_{/S}$.

Remark 3.17. *(i) We may meet the set-theoretic problems since* $\mathrm{ShGr}_{/S}$ *and* $\mathrm{ShAb}_{/S}$ *are not necessarily locally small categories, but in our context there will be no problem if we use the framework of Grothendieck universe.*

(ii) Not all presheaves on any cite can be sheafificated, for example, there exists a presheaf on the fpqc site which admits no fpqc sheafification, see [10]. However any presheaf on the fppf site admits a fppf sheafification since any scheme X has a small basis of fppf covering: taking all affine fppf coverings of all affine open subschemes of X.

Definition 3.18. *(i) Let G be an S-group scheme acting, by $\rho : G \times_S X \to X$, on an S-scheme X. We write $(X/G)_{fppf}$, or simply X/G, for the fppf sheaf associated to the presheaf*

$$T \mapsto X(T)/G(T).$$

If X/G is representable by a scheme Y then we refer to Y (or to the quotient morphism $q : X \to Y$) as the fppf quotient of X by G.

We often say that "an fppf quotient exists" if $(X/G)_{\mathrm{fppf}}$ is representable by a scheme. Note that the sheaf X/G is a categorical quotient of X by G in $\mathrm{FPPF}(S)$, so we are indeed forming the quotient in a "bigger" category. Note further that if $(X/G)_{\mathrm{fppf}}$ is representable by

a scheme Y then by the Yoneda lemma we have a quotient morphism of schemes $q : X \to Y$.

(ii) Given an action ρ as in (i), we define the "graph morphism"

$$\Psi = \Psi_\rho := (\rho, \mathrm{pr}_2) : G \times_S X \longrightarrow X \times_S X;$$

on points this is given by $(g, x) \mapsto (g \cdot x, x)$. The action ρ is said to be free if Ψ is a monomorphism of schemes.

As we are mainly interested in the formation of quotients of a group scheme by a subgroup scheme, we shall mostly restrict our discussion of fppf quotients to the case that the action is free.

Remark 3.19. *The formation of fppf quotients is compatible with base change. To explain this in more detail, suppose $j : S' \to S$ is a morphism of schemes. Then j gives rise to an inverse image functor $j^* : \mathrm{FPPF}(S) \to \mathrm{FPPF}(S')$ which preserves colimits. Concretely, if $f : T \to S'$ is an S'-scheme then $j \circ f : T \to S$ is an S-scheme, and if F is an fppf sheaf on S then we have $j^*F(f : T \to S') = F(j \circ f : T \to S)$. In particular, on representable sheaves j^* is simply given by base-change: $j^*X = X \times_S S'$. Writing $X' = X \times_S S'$ and $G' = G \times_S S'$, we conclude that $j^*(X/G) = (X'/G')$ as sheaves on $(S')_{FPPF.}$. Hence if $q : X \to Y$ is an fppf quotient over S then $Y' := Y \times_S S'$ is an fppf quotient of X' by G'. Put differently:* ***An fppf quotient, if it exists, is automatically a universal fppf quotient.***

Proposition 3.20. *(i) Let G be an S-group scheme acting freely on an S-scheme X. Suppose the fppf sheaf $(X/G)_{\mathrm{fppf}}$ is representable by a scheme Y. Write $q : X \to Y$ for the canonical morphism. Then the morphism $\Psi : G \times_S X \to X \times_Y X$ is an isomorphism. This gives a commutative diagram with cartesian squares*

$$\begin{array}{ccccc} G \times_S X & \xrightarrow{\sim} & X \times_Y X & \xrightarrow{\pi_1} & X \\ \downarrow{\scriptstyle \pi_2} & & \downarrow{\scriptstyle \pi_2} & & \downarrow{\scriptstyle q} \\ X & = & X & \xrightarrow[q]{} & Y \end{array}$$

(ii) If furthermore $G \to S$ is flat and locally of finite presentation, then $q : X \to Y$ is fppf covering.

Proof: (i) Since the action is free, we see that the image of the injection $h_G \times h_X \to h_X \times h_X$ is exactly the equivalent relation. By calculation of sheafification, $\Psi : h_G \times h_X \to h_X \times_{h_Y} h_X$ is an isomorphism of fppf sheaves. By the Yoneda lemma, Ψ is then also an

isomorphism of schemes.
(ii) Let $W = Y$. Let $W \to Y$ be the identity morphism. We find

$$W \times_Y X \cong W \times_{X,\pi_1} (X \times_Y X) \cong W \times_{X,\pi_2} (X \times_Y X) \cong W \times_{X,\pi_2} (G \times_S X)$$

as W-schemes, so $W \times_Y X \to W$ is fppf. That is exactly what we want.

□

Definition 3.21. *Let $\mathcal{P}$ be a subcategory of schemes containing all isomorphisms. Let $\tau \in \{fpqc, fppf, smooth, étale, Zariski\}$. We say $\mathcal{P}$ is τ local on the base, or τ local on the target, or local on the base for the τ-topology if following conditions hold.*
(i) $\mathcal{P}$ is stable under base change;
(ii) For any τ-covering $\{Y_i \to Y\}_{i\in I}$ and any morphism of schemes $f : X \to Y$ we have $f \in \mathcal{P} \Leftrightarrow$ each $Y_i \times_Y X \to Y_i \in \mathcal{P}$.

Remark 3.22. *Many properties that play a role in algebraic geometry are fppf local on the target. More precisely, it follows from the results in [2] Decent, that this holds for the property $\mathcal{P}$ of a morphism of schemes of being quasi-compact, surjective, flat, (locally) of finite type, locally of finite presentation, smooth, étale, universally closed, separated, universally open, proper, universally injective, isomorphism, affine, integral, finite, finite locally free of degree $r (r \geq 0)$. For more details, see [2] Decent.*

Corollary 3.23. *Let $\mathcal{P}$ be a property of morphisms of schemes which is local on the target for the fppf topology. Let G be a fppf S-group scheme. If $q : X \to Y$ is an fppf quotient of X under the free action of an S-group scheme G, then*

$$\pi : G \to S \in \mathcal{P} \Rightarrow \pi_2 : G \times_S X \to X \in \mathcal{P} \Leftrightarrow q : X \to Y \in \mathcal{P}$$

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

Proof: Clear, as $q : X \to Y$ is an fppf covering and $G \times_S X \xrightarrow{\sim} X \times_Y X$.

□

In the applications we shall see that this is a most useful result. After all, it tells us that an fppf quotient morphism $q : X \to Y$ inherits many properties from the structural morphism $\pi : G \to S$.
Now we turn to the main theorem of this subsection that the category $\boldsymbol{C}_k$ of commutative algebraic groups over a field k is an abelian category.

Lemma 3.24. *If $f : G_1 \to G_2$ is a monomorphism in $\boldsymbol{C}_k$, then the fppf quotient sheaf G_2/G_1 is representable by a k-scheme, for the details of this see [11] SGA 3, Exp* $\mathrm{VI_A}$*, Thm. 3.2.*
Since "locally of finite type" is fppf-local on the source (see [2] Decent 27), G_2/G_1 is of finite type over k.

Theorem 3.25. *$\boldsymbol{C}_k$ is an abelian category.*

Proof: We know that $\mathrm{ShAb}_{/k}$ is a (big) abelian category, and that $h : \boldsymbol{C}_k \to \mathrm{ShAb}_{/k}$ is a fully faithful embedding. So it suffices to show that $\boldsymbol{C}_k$ has kernels and cokernels and that h preserves kernels and cokernels. Clearly $\boldsymbol{C}_k$ is an additive subcategory, and h preserves kernels.
For cokernel, Let $f : G_1 \to G_2$ be a morphism in $\boldsymbol{C}_k$. In the category $\mathrm{ShAb}_{/k}$ we can form the fppf quotient $q_1 : G_1 \to G_1/\operatorname{Ker}(f)$ by the lemma. Let $\bar{G}_1 := G_1/\operatorname{Ker}(f)$, and let $\bar{f} : \bar{G}_1 \to G_2$ be the homomorphism induced by f. Note that $\bar{f}$ is a monomorphism since the corresponding morphism of fppf sheaves is a monomorphism. But the natural map of sheaves $h(G_2)/h(G_1) \to h(G_2)/h(\bar{G}_1)$ is an isomorphism, so it follows that the fppf quotient G_2/G_1 exists again by the lemma. In particular, we conclude that $\boldsymbol{C}_k$ has cokernels which are all preserved by h.

□

Remark 3.26. *(i) In the construction of kernels and cokernels, we can easily see that monomorphisms in $\boldsymbol{C}_k$ are exactly closed subgroup k-schemes, and that epimorhisms in $\boldsymbol{C}_k$ are exactly fppf homomorphisms.*
(ii) If $k \to F$ is a field extension, then $\boldsymbol{C}_k \to \boldsymbol{C}_F$ is an exact functor by the description of (mono)epimorphisms in $\boldsymbol{C}_k$.

Definition 3.27. *Let G be a finite group scheme over a field k. We say that G is*
- étale if the structural morphism $G \to \operatorname{Spec}(k)$ is étale;
- local if G is connected.

Lemma 3.28. *Let G_1 and G_2 be finite group schemes over a field k, with G_1 étale and G_2 local. Then the only homomorphisms $G_1 \to G_2$ and $G_2 \to G_1$ are the trivial ones.*

Proof: Without loss of generality we may assume that $k = \bar{k}$. Then $G_{2,\,\mathrm{red}} \subset G_2$ is a connected étale subgroup scheme; hence $G_{2,\,\mathrm{red}} \cong \operatorname{Spec}(k)$. Now note that any homomorphism $G_1 \to G_2$ factors through $G_{2,\mathrm{red}}$. Similarly, any homomorphism $G_2 \to G_1$ factors through $G_1^0 \cong \operatorname{Spec}(k)$.

□

Now we introduce local-étale sequence of a commutative algebraic group over a field k.

Theorem 3.29. *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 $G \cong G^0 \times \omega_0(G)$.

Proof: Consider the homomorphism $q : G \to \omega_0(G)$ as in 3.15. As shown there, q is faithfully flat, and the kernel of q is precisely the identity component G^0. Hence we have the exact sequence above.

Let us now assume that k is perfect and G is finite. Then $G_{\mathrm{red}} \subset G$ is a closed subgroup scheme which by 3.9 is étale over k. We claim that the composition $G_{\mathrm{red}} \hookrightarrow G \to \omega_0(G)$ is an isomorphism. To see this we may assume that $k = \bar{k}$. But then G, as a scheme, is a finite disjoint union of copies of G^0. If there are n components then G_{red} and $\omega_0(G)$ are both isomorphic to the disjoint union of n copies of $\mathrm{Spec}(k)$, and it is clear that $G_{\mathrm{red}} \to \omega_0(G)$ is an isomorphism of group schemes. The inverse of this isomorphism gives a natural splitting.

□

Proposition 3.30. *If $0 \longrightarrow G_1 \longrightarrow G_2 \longrightarrow G_3 \longrightarrow 0$ is an exact sequence of finite k-schemes in $\boldsymbol{C}_k$ then* $\mathrm{rank}\,(G_2) = \mathrm{rank}\,(G_1) \cdot \mathrm{rank}\,(G_3)$.

Proof: Immediate from the fact that "finite locally free of degree $r (r \geq 0)$" is local on the target for the fppf topology, as this implies that $G_2 \to G_3$ is finite locally free of degree $\mathrm{rank}\,(G_1)$ by 3.23.

□

4. Abelian varieties

The elliptic curve is the first example of the abelian variety. In the view of the stable homotopy theory the abelian variety is less important than the elliptic curve because it does not seem that the higher dimensional formal group could be realized in the stable homotopy theory. But before we deal with the elliptic curve it is profitable to know some powerful theories about the abelian variety. The main reference of this chapter is [12, 13].

Definition 4.1. *An abelian variety (X, m, i, e) is a group scheme over k which is also a proper, geometrically integral variety over k.*

Remark 4.2. *Note that we have not required the group scheme is commutative in the definition of the abelian variety, because in the following content we will see that it automatically holds. And we will see some elegant statements in the abelian variety due to a property usually called by "rigidity", which means the triviality in the fiber can imply the triviality in the whole scheme.*

4.1 Basic properties of abelian varieties

We have seen any elliptic curve over k is an abelian variety of dim 1 in the chapter 2. Now we claim that the converse is true too.

Proposition 4.3. *Any abelian variety C of dim 1 over k is an elliptic curve.*

Proof: It suffices to show that $g(C) = 1$. By 3.9 C is smooth, we have $\omega_C \cong \Omega_{C/k}$. Using 3.6 we conclude that $\Omega_{C/k}$ is a finite direct sum of $\mathcal{O}_C$, which must have $\Omega_{C/k} \cong \mathcal{O}_C$ because $\Omega_{C/k}$ is invertible. Finally, we get $g = l(K_C) = \dim_k H^0\left(C, \Omega_{C/k}\right) = \dim_k H^0\left(C, \mathcal{O}_C\right) = 1$.

□

Now, we introduce "Rigidity lemma" mentioned at the beginning of this chapter.

Lemma 4.4. *Let k be a field, let X be a proper geometrically integral k-scheme and let Y be an affine k-scheme. Then every morphism $X \to Y$ of k-schemes factors through a k-valued point of Y .*

Proof: By the fact $\Gamma(X, \mathcal{O}_X) = k$ it is easy to see.

□

Lemma 4.5 (Rigidity lemma [14])**.** *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 $p_2 : X \times Y \to Y$.

Proof:

Let $x \in X(k)$, viewed as a morphism Spec $k \to X$, and consider the morphisms f and $g := f \circ (x \times \mathrm{id}_Y) \circ p_2$ from $X \times Y$ to Z. It suffices to show that $f = g$ or, equivalently, that the subscheme $\mathrm{Eq}(f, g)$ of $X \times Y$, where these morphisms coincide, is equal to $X \times Y$. Let $U \subset Z$ be an open affine neighborhood of z. Because X is proper over k, the projection $p_2 : X\times Y \to Y$ is closed. By hypothesis $p_2^{-1}(y) \subseteq f^{-1}(U)$, and therefore there exists an open neighborhood V of y in Y such that $p_2^{-1}(V) \subseteq f^{-1}(U)$ (by closed map). Let $y' \in V$. Then the restriction of f to $X\times_k \mathrm{Spec}\,\kappa(y') \subset X\times Y$ yields a morphism $X\otimes_k \kappa(y') \to U\otimes_k \kappa(y')$ of $\kappa(y')$-schemes, which factors through a $\kappa(y')$-valued point by 4.4. This shows that $\mathrm{Eq}(f, g)$ contains all points of $X \times V$, and hence contains the dense open subset $X \times V$. Moreover $\mathrm{Eq}(f, g)$ is closed because Z is separated. Because $X \times Y$ is reduced, $\mathrm{Eq}(f, g) = X \times Y$.

□

Theorem 4.6. *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.*

Proof: Set $y := i_Y(f(e_X))$, and define $h := t_y \circ f$. By construction we have $h(e_X) = e_Y$. Consider the composite morphism

$$g := \left(X \times X \xrightarrow{(h\circ m_X)\times(i_Y\circ m_Y\circ(h\times h))} Y \times Y \xrightarrow{m_Y} Y\right).$$

(To understand what this morphism does: if we use the additive notation for the group structures on X and Y then g is given on points by $g(x, x') = h(x + x') - h(x') - h(x)$.) We have

$$g(\{e_X\} \times X) = g(X \times \{e_X\}) = \{e_Y\}$$

By the Rigidity Lemma this implies that g factors both through the first and through the second projection $X \times X \to X$, hence g equals the constant map with value e_Y. This means that $h \circ m_X = m_Y \circ (h \times h)$, i.e., h is a homomorphism.

□

Corollary 4.7. *(i) 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.*

(ii) 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.

Proof:

(i) If (X, m, i, e) and (X, n, j, e) are abelian varieties then m and n are equal when restricted to $X \times \{e\}$ and $\{e\} \times X$. Applying (1.12) to $m \circ (m, i \circ n) : X \times X \to X$, which is constant when restricted to $X \times \{e\}$ and $\{e\} \times X$, we get $m = n$. This readily implies that $i = j$ too because the inverse map is unique if it exists.

(ii) By the previous proposition, the map $i : X \to X$ is a homomorphism. This is equivalent that the group structure is abelian.

□

Remark 4.8. *From now on we shall mostly use the additive notation for abelian varieties, writing $x+y$ for $m(x, y)$, writing $-x$ for $i(x)$, and 0 for e. Since abelian varieties are abelian as group varieties, we no longer have to distinguish between left and right translations. Also we can add homomorphisms: given two homomorphisms of abelian varieties $f, g : X \to Y$, we define $f + g$ to be the composition*

$$f + g := m_Y \circ (f, g) : X \longrightarrow Y \times Y \longrightarrow Y,$$

and we set $-f := f \circ i_X = i_Y \circ f$. This makes the set $\mathrm{Hom}_{\mathrm{AV}}(X, Y)$ of homomorphisms of X to Y into an abelian group.

As we have seen, also the set $\mathrm{Hom}_{Sch/k}(X, Y) = Y(X)$ of X-valued points of Y has a natural structure of an abelian group. By Theorem 4.6, $\mathrm{Hom}_{\mathrm{AV}}(X, Y)$ is just the subgroup of $\mathrm{Hom}_{Sch/k}(X, Y)$ consisting of those morphisms $f : X \to Y$ such that $f(0_X) = 0_Y$, and $\mathrm{Hom}_{Sch/k}(X, Y) = \mathrm{Hom}_{\mathrm{AV}}(X, Y) \times Y(k)$ as groups. We shall adopt the convention that $\mathrm{Hom}(X, Y)$ stands for $\mathrm{Hom}_{\mathrm{AV}}(X, Y)$. If there is a risk of confusion we shall indicate what we mean by a subscript "AV" or "Sch/k".

4.2 Line bundles on abelian varieties

Now we claim another result that can be thought of as a rigidity property of line bundles in abelian varieties, which is powerful in the theory of abelian varieties.

Lemma 4.9. *A line bundle $\mathcal{M}$ on a proper geometrically integral variety X over a field k is trivial iff we have $H^0(X, \mathcal{M}) \neq 0$ and $H^0(X, \mathcal{M}^{-1}) \neq 0$.*

Proof: One direction is easy because $H^0(X, \mathcal{M}) = H^0(X, \mathcal{M}^{-1}) = k \neq 0$ if $\mathcal{M}$ is trivial. For another direction, by integrality, we can choose a Cartier divisor D such that $\mathcal{L}(D) = \mathcal{M}$. Then the hypothesis implies there are $f_1, f_2 \in K(X)^*$ such that (following ≥ 0 means effective)

$$div(f_1) + D \geq 0,\ div(f_2) - D \geq 0$$

Taking the sum we get $div(f_1 f_2) \geq 0$, which implies $f_1 f_2 \in \mathcal{O}_X^* = k^*$. So $div(f_1) + div(f_2) = 0$. We write $f = f_1$, then we have both $div(f) + D \geq 0$ and $-div(f) - D \geq 0$. Hence $div(f) + D = 0$ and $\mathcal{L}(D)$ is trivial.

□

Lemma 4.10. *Given a morphism of schemes $X \to Y$. Assume $\mathcal{O}_Y \xrightarrow{\sim} f_*\mathcal{O}_X$. Then the functor $\mathcal{N} \mapsto f^*\mathcal{N}$ is fully faithful from the category $\mathcal{C}$ of locally free sheaves of finite rank on Y to that on X. The essential image is formed by the sheaves $\mathcal{M}$ on X such that*

(i) the image $f_*\mathcal{M}$ is in $\mathcal{C}$ and

(ii) the natural map $f^*f_*\mathcal{M} \to \mathcal{M}$ is an isomorphism.

Proof:

For any $\mathcal{N}$ in $\mathcal{C}$, there is a string of three natural isomorphisms

$$\mathcal{N} \xrightarrow{\sim} \mathcal{N} \otimes f_*O_X \xrightarrow{\sim} \mathcal{N} \otimes f_*f^*\mathcal{O}_Y \xrightarrow{\sim} f_*f^*\mathcal{N}.$$

The first isomorphism arises by tensor product with the comorphism of f; this comorphism is an isomorphism by hypothesis. The second isomorphism arises from the identification $\mathcal{O}_X = f^*\mathcal{O}_Y$. The third arises from the projection formula.

For any $\mathcal{N}'$ in $\mathcal{C}$, also $\mathrm{Hom}\,(\mathcal{N}, \mathcal{N}')$ is in $\mathcal{C}$. Hence, it yields an isomorphism

$$\mathcal{H}om\,(\mathcal{N}, \mathcal{N}') \xrightarrow{\sim} f_*f^*\mathcal{H}om\,(\mathcal{N}, \mathcal{N}')\,.$$

Now, since $\mathcal{N}$ and $\mathcal{N}'$ are locally free of finite rank, the natural map

$$f^*\mathcal{H}om\,(\mathcal{N}, \mathcal{N}') \to \mathcal{H}om\,(f^*\mathcal{N}, f^*\mathcal{N}')$$

is an isomorphism locally, so globally. Hence there is an isomorphism of groups

$$\mathrm{Hom}\,(\mathcal{N}, \mathcal{N}') \xrightarrow{\sim} \mathrm{Hom}\,(f^*\mathcal{N}, f^*\mathcal{N}')\,.$$

In other words, $\mathcal{N} \mapsto f^*\mathcal{N}$ is fully-faithful. Finally, the essential image consists of the sheaves $\mathcal{M}$ that are isomorphic to those of the form $f^*\mathcal{N}$ for some $\mathcal{N}$ in $\mathcal{C}$. Given such an

$\mathcal{M}$ and $\mathcal{N}$, there is an isomorphism $f_*\mathcal{M} \simeq \mathcal{N}$ owing to (2.7.1). Hence $f_*\mathcal{M}$ is in $\mathcal{C}$, and $f^*f_*\mathcal{M} \to \mathcal{M}$ is an isomorphism locally, so globally; thus (i) and (ii) hold. Conversely, if (i) and (ii) hold, then $\mathcal{M}$ is, by definition, in the essential image.

□

Lemma 4.11. *Suppose $f : X \to Y$ is a proper flat morphism of locally Noetherian schemes, whose fibers satisfy $\dim_{k(y)} H^0\left(X_y, \mathcal{O}_{X_y}\right) = 1$. (Important remark: this is satisfied if f has geometrically connected and geometrically reduced fibers) Then f satisfies that $\mathcal{O}_Y \longrightarrow f_*\mathcal{O}_X$ is isomorphic.*

Proof: Consider

$$\mathcal{O}_Y \otimes k(y) \longrightarrow (f_*\mathcal{O}_X) \otimes k(y) \xrightarrow{\phi_y^0} H^0\left(X_y, \mathcal{O}_{X_y}\right) \cong k(y)$$

The composition is surjective, hence ϕ_{y}^0 is surjective, hence it is an isomorphism by the Cohomology and Base Change Theorem 2.15. Then by the Cohomology and Base Change Theorem 2.15(ii), $f_*\mathcal{O}_X$ is locally free, thus of rank 1 . Use Nakayama's Lemma to show that a map of invertible sheaves $\mathcal{O}_Y \to f_*\mathcal{O}_X$ that is an isomorphism on fibers is necessarily an isomorphism of sheaves.

□

Proposition 4.12. *Let $f : X \to Y$ be a morphism, $L \in Pic(X)$. Let $\mathcal{P}(L, f)$ be a property on the pair (L, f). We call $Z \subset Y$ a $\mathcal{P}$-maximal closed subscheme of (L, f) if for any Y-scheme T such that $\mathcal{P}(L_T, f_T)$ holds T can factor through Z. (Note if Z exists then it is unique.)*

Assume a pair (L, f) satisfies that

(i) For any Y-scheme T, if $\mathcal{P}(L_T, f_T)$ holds, then for any open $U \subset T$ we have $\mathcal{P}(L_T|_{f^{-1}(U)}, f_T|_{f^{-1}(U)})$ holds.

(ii) For any Y-scheme T, if there exists an open covering $\{U_\alpha\}$ of T such that $\mathcal{P}(L_T|_\alpha, f_T|_\alpha)$ holds for all α, then $\mathcal{P}(L_T, f_T)$ holds.

Then

(i) Given a Y-scheme T, if Z is $\mathcal{P}$-maximal closed subscheme of (L_T, f_T), then so is $Z|_U \subset U$ for any open $U \subset T$.

(ii) Given a Y-scheme T, suppose there exists an open covering $\{U_\alpha\}$ of T and a collection $\{Z_\alpha\}$ such that for any α, $Z_\alpha \subset U_\alpha$ is a $\mathcal{P}$-maximal closed subscheme. Then $\mathcal{P}$-maximal closed subscheme Z of (L_T, f_T) exists and Z satisfies $Z \cap U_\alpha = Z_\alpha$.

Proof: It is easy to check.

□

Proposition 4.13. *Suppose $f : X \to Y$ is a proper flat morphism of locally Noetherian schemes, whose fibers are geometrically integral, $L \in Pic(X)$, then there exists a unique closed subscheme structure on Z such that L_Z is pulled back from Z, and Z is universal with this property amongst all Y-schemes.*

Proof: We define $\mathcal{P}(L, f)$ to be "$L \in f^*Pic(Y)$". By the two previous lemmas, we can show that $\mathcal{P}(L, f)$ is equivalent to "f_*L is invertible and $f^*f_*L \to L$ is isomorphic" for (L, f) here. So it is easy to see $\mathcal{P}$ satisfies the two assumptions of 4.12. Hence we can assume $Y = \mathrm{Spec}(A)$. For more details, see [15] Chap 10.

□

Theorem 4.14 (The Seesaw Theorem)**.** *Let $f : X \to S$ be a proper flat morphism between locally Noetherian schemes with geometrically integral fibres. If $L \in \mathrm{Pic}(X)$ is a line bundle on X, then*

(i) the set $Z := \{s \in S : L_s \text{ is trivial }\}$ is closed in S;

(ii) $L_{Z_{\mathrm{red}}}$ is pulled back from Z_{red}, where Z_{red} denotes the unique reduced subscheme structure on Z;

(iii) The underlying space of the maximal closed subscheme $Z(L)$ such that $L_{Z(L)}$ is pulled back from $Z(L)$ is equal to Z.

Proof: For (i), as the fibres of f are geometrically integral, Lemma 4.9 implies that Z can be rewritten as

$$Z = \left\{s \in S : H^0\left(X_s, L_s\right) \neq 0\right\} \cap \left\{s \in S : H^0\left(X_s, L_s^{-1}\right) \neq 0\right\}.$$

Both sets above are closed by the semicontinuity theorem (indeed, they are both the locus where the global sections of a certain line bundle has dimension ≥ 1), hence Z is closed.

For (ii), replace S with Z_{red} in order to assume that L_s is trivial for all $s \in S$ and that S is reduced. If $M = f_*L$, then we claim that M is a line bundle on S. This problem is local on S, so we may assume that $S = \mathrm{Spec}(A)$. By 2.14, it follows that M is a vector bundle and $M \otimes_A \kappa(s) \simeq H^0\left(X_s, L_s\right) = H^0\left(X_s, \mathcal{O}_{X_s}\right) = \kappa(s)$, where the final equality follows from the hypothesis that the map f is proper with geometrically integral fibres. Therefore, M is of rank 1, as required.

Moreover, we claim that the counit map $f^*(M) = f^*f_*L \to L$ is an isomorphism. The problem is local on S, so assume $S = \mathrm{Spec}(A)$. If one restricts the counit map to the fibre above $s \in S$, then one gets an isomorphism because L_s is trivial and $M \otimes_A \kappa(s) \xrightarrow{\simeq} H^0(X_s, L_s)$ is an isomorphism. Thus, $f^*(M) \to L$ is an isomorphism on each fibre X_s, and it is therefore an isomorphism by Nakayama's lemma.

(iii) is directly from (ii) and the maximal property of $Z(L)$.

□

Remark 4.15. *What does the Seesaw Theorem have to do with seesaws? Consider the main case of interest: when $X = S \times T$ for two proper geometrically integral varieties S and T over a field k, and $f : X \to S$ is the first projection. Theorem* 6.3 *then implies that if $L_{\{s\}\times T}$ is trivial for all $s \in S$, then L is pulled back from S.*

Theorem 4.16 (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.*

Proof: We follow the proof given by Mumford in [15] §10. We view L as a family of line bundles on $X \times Y$ parametrized by Z. Let Z' be the maximal closed subscheme of Z over which L is trivial, as discussed above. We have $z \in Z'$. We shall show that $Z' = Z$ by showing that Z' is an open subscheme and using the connectedness of Z. Let ζ be a point of Z'. Write $\mathfrak{m}$ for the maximal ideal of the local ring $O_{Z,\zeta}$ and $I \subset O_{Z,\zeta}$ for the ideal defining (the germ of) Z'. We have to show that $I = (0)$. Suppose not. By Krull's Theorem (here we use that Z is locally noetherian) we have $\cap_n \mathfrak{m}^n = (0)$, hence there exists a positive integer n such that $I \subset \mathfrak{m}^n, I \not\subset \mathfrak{m}^{n+1}$. Put $a_1 = (I, \mathfrak{m}^{n+1})$, and choose an ideal a_2 with

$$\mathfrak{m}^{n+1} \subset a_2 \subset \left(I, \mathfrak{m}^{n+1}\right) = a_1 \quad \text{and} \quad \dim_{k(\zeta)}(a_1/a_2) = 1.$$

(Note that such ideals exist.) Let $Z_i \subset \mathrm{Spec}\,(O_{Z,\zeta})$ be the closed subscheme defined by the ideal $a_i (i = 1, 2)$. We will show that the restriction of L to $X \times Y \times Z_2$ is trivial. This implies that Z_2 is contained in Z', which is a contradiction, since $I \not\subset a_2$.

Write L_i for the restriction of L to $X \times Y \times Z_i$. By construction, L_1 is trivial; choose a trivializing global section s. The inclusion $Z_1 \hookrightarrow Z_2$ induces a restriction map $\Gamma(L_2) \to \Gamma(L_1)$. We claim: L_2 is trivial if and only if s can be lifted to a global section of L_2. To see this, suppose first that we have a lift s'. The schemes $X \times Y \times Z_1$ and $X \times Y \times Z_2$ have

the same underlying point sets. If $s'(P) = 0$ for some point P then also $s(P) = 0$, but this contradicts the assumption that s is a trivialization of L_1. Hence s' is nowhere zero, and since L_2 is locally free of rank 1 this implies that s' trivializes L_2. Conversely, if L_2 is trivial then the restriction map $\Gamma(L_2) \to \Gamma(L_1)$ is just $\Gamma(O_{Z_2}) \to \Gamma(O_{Z_1})$ and this is surjective.

The obstruction for lifting s to a global section of L_2 is an element $\xi \in H^1(X \times Y, O_{X\times Y})$. We know that the restrictions of L_2 to $\{x\} \times Y \times Z_2$ and to $X \times \{y\} \times Z_2$ are trivial. Writing $i_1 = (\mathrm{id}_X, y) : X \hookrightarrow X \times Y$ and $i_2 = (x, \mathrm{id}_Y) : Y \hookrightarrow X \times Y$, this means that ξ has trivial image under $i_1^* : H^1(X \times Y, O_{X\times Y}) \to H^1(X, O_X)$ and under $i_2^* : H^1(X \times Y, O_{X\times Y}) \to H^1(Y, O_Y)$. But the map (i_1^*, i_2^*) gives a (Künneth) isomorphism

$$H^1(X \times Y, O_{X\times Y}) \xrightarrow{\sim} H^1(X, O_X) \oplus H^1(Y, O_Y)$$

hence $\xi = 0$ and s can be lifted.

□

Theorem 4.17 (Theorem of the Cube)**.** *Let L be a line bundle on X. Then the line bundle*

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

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

Proof: Restriction of $\Theta(L)$ to $\{0\} \times X \times X$ gives the bundle

$$m^* L \otimes p_2^* L^{-1} \otimes p_3^* L^{-1} \otimes m^* L^{-1} \otimes O_{X\times X} \otimes p_2^* L \otimes p_3^* L$$

which is obviously trivial. Similarly for $X \times \{0\} \times X$ and $X \times X \times \{0\}$. By 4.16 the result follows.

□

Corollary 4.18. *Let Y be a scheme and let X be an abelian variety. For every triple f, g, h of morphisms $Y \to X$ and for every line bundle L on X, 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.

Proof: Consider $(f, g, h) : Y \to X \times X \times X$ and use 4.17.

□

Another important corollary is the following.

Corollary 4.19 (Theorem of the Square)**.** *Let X be an abelian variety and let L be a line bundle on X. Then for all $x, y \in X(k)$,*

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

Proof: In the first formulation, this is immediate from 4.17 by taking for f the identity on X and for g and h the constant maps with images x and y.

□

Corollary 4.20. *Let L be a line bundle on an abelian variety X. Let $\mathrm{Pic}(X)$ be the group of isomorphism classes of line bundles on X. Then the map $\varphi_L : X(k) \to \mathrm{Pic}(X)$ given by $x \mapsto [t_x^* L \otimes L^{-1}]$ is a homomorphism.*

Corollary 4.21. *For every line bundle L on an abelian variety X and every $n \in \mathbb{Z}$ we have*

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

Proof: Set $f = n, g = 1$, and $h = -1$. Applying 4.17, one finds that

$$[n]^* L \otimes [n+1]^* L^{-1} \otimes [n-1]^* L^{-1} \otimes [n]^* L \otimes L \otimes [-1]^* L$$

is trivial, i.e.,

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

The assertion now follows by induction, starting from the cases $n = -1, 0, 1$.

□

Now we can prove abelian varieties are projective.

Lemma 4.22. *If A is an abelian variety over an algebraically closed k and $L = \mathcal{O}_A(D)$ for an effective Cartier divisor $D \subseteq A$, then $L^{\otimes 2}$ is globally-generated.*

Proof: Fix $a \in A(k)$. We must show that there exists an effective divisor $E \in |2D|$ such that $a \notin E$. Consider the dense open subset $U := (A - D) + a$ of A. Then, $U \cap [-1]^* U$ is also a dense open subset of A, because A is irreducible. Pick $b \in U \cap [-1]^* U$ and notice that
- as $b \in U, b + a \in A - D$;
- as $b \in [-1]^* U, -b \in U$ and hence $a - b \in A - D$.

Thus, $a \notin b+D$ and $a \notin -b+D$; in particular, $a \notin t_{-b}(D) \cup t_b(D)$. If $E := t_b(D) + t_{-b}(D)$, then E is an effective divisor on A and it is linearly equivalent to $2D$ by 4.19.

□

Lemma 4.23. *Let $f : X \to Y$ be a k-morphism between k-schemes of finite type over a field k. If for any closed point $x \in X$ the fiber $X_{f(x)}$ is a finite set then f is quasi-finite.*

Proof: See [14] 10.97.

□

Lemma 4.24. *If $A \to B$ is a faithfully flat map between Noetherian rings. Assume X is a proper A-scheme with $\mathcal{L} \in Pic(X)$, then $\mathcal{L}_B$ is ample on X_B if and only if $\mathcal{L}$ is ample on X.*

Proof: It is directly from the equivalent definition ([3] 5.3.6) of ample bundles by cohomology, and flat base change theorem.

□

Lemma 4.25. *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 $\varphi : X \times F_x \to Y$ obtained by restricting $f \circ m$ to $X \times F_x$. Clearly $\varphi(\{0\} \times F_x) = \{f(x)\}$. Since F_x is complete and connected, the 4.5 implies that φ maps the fibres $\{z\} \times F_x$ to a point. In particular, we find that $f(y - x + F_x) = f(y)$ for all $x, y \in X(k)$. Putting $y = z, x = 0$ gives $z + F_0 \subseteq F_z$; putting $y = 0, x = z$ gives $-z + F_z \subseteq F_0$. This shows that $F_z = z + F_0$.

To see that F_0 is a subgroup scheme of X we take a geometric point $a \in F_0(k)$. Then obviously $F_a = F_0$ so that $a + F_0 = F_a = F_0$. Since F_0 is reduced, it follows that F_0 is a subgroup scheme of X. By 3.9 it is smooth, then an abelian subvariety since it is integral [2] Variety 25.10.

□

Lemma 4.26. *If X is a Noetherian regular separated scheme, $U \subset X$ is dense affine open, then there exists an effective Cartier divisor $D \subset X$ with $U = X - D$.*

Proof: See [2] Divisor 16.6.

□

Theorem 4.27. *If X is an abelian variety over a field k, then X is projective over k.*

Proof: If $U \subseteq X$ is a non-empty affine open then $D := X - U$ is an effective Cartier divisor by last Lemma. Set $L = \mathcal{O}_X(D)$, then we claim that $L_{\bar{k}}$ is ample, which implies L is ample by 4.24. By 4.22 $L_{\bar{k}}^{\otimes 2}$ is globally-generated, so if we choose a $\bar{k}$-basis of its global section there is a morphism $f : X \to \mathbf{P}_{\bar{k}}^m$ such that $f^*\mathcal{O}_{\mathbf{P}_{\bar{k}}^m}(1) = L_{\bar{k}}^{\otimes 2}$. As any section of $L_{\bar{k}}^{\otimes 2}$ is pulled back from a section of $\mathcal{O}_{\mathbf{P}_{\bar{k}}^m}(1)$, there exists a hyperplane $H \subseteq \mathbf{P}_{\bar{k}}^m$ such that $f^{-1}(H) = 2D_{\bar{k}}$ using regular sections of effective Cartier divisors. For any closed point $x \in \mathbf{P}_{\bar{k}}^m - H$, $f^{-1}(x) \subseteq X_{\bar{k}} - D_{\bar{k}} = U_{\bar{k}}$ (moreover, there exists such an x with $f^{-1}(x)$ is non-empty, because f is defined by a complete linear system). If $f^{-1}(x)$ is non-empty, then since $U_{\bar{k}}$ is affine and $f^{-1}(x)$ is proper, it follows that $f^{-1}(x)$ is finite; Proposition 4.25 and 4.23 then implies that f is quasi-finite. By Zariski's main theorem, f is finite, and hence $L_{\bar{k}}$ is ample, since $L_{\bar{k}}^{\otimes 2}$ is the pullback of the ample line bundle $\mathcal{O}_{\mathbf{P}_{\bar{k}}^m}(1)$ by the finite map f.

□

4.3 Isogenies of abelian varieties

In this section we define the notion of an isogeny, which is an important class of homomorphisms between abelian varieties.

Remark 4.28. *Note that for a Category $\mathcal{C}$, if it has any finite limit, then so is the $AbGrp(\mathcal{C})$ and any finite limit in $AbGrp(\mathcal{C})$ is created in $\mathcal{C}$. So for any homomorphism of groups S-schemes $f : X \to Y$ over a base scheme S, the fiber of 0 is a closed subgroup scheme of X and we write it as* $\mathrm{Ker}(f)$.

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 4.29. *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.*

Proof: It suffices to show that Y is proper and geometrically integral over k. For the properness, it is immediately from [3] 3.3.16. Also, Y is geometrically irreducible since $X_{\bar{k}} \to Y_{\bar{k}}$ is surjective. Finally, since $f_{\bar{k}}$ is flat, we see $\mathcal{O}_{Y_{\bar{k}},f(x)} \to \mathcal{O}_{X_{\bar{k}},x}$ is injective for any $x \in X_{\bar{k}}$. Therefore we conclude that Y is geometrically reduced.

□

Lemma 4.30.

(i) Let $R \to S$ be a local homomorphism of Noetherian local rings. Assume that R is regular, S Cohen-Macaulay, and $\dim(S) = \dim(R) + \dim(S/\mathfrak{m}_R S)$. *Then $R \to S$ is flat.*

(ii) Let $f : R \to S$ be a morphism of finite type between noetherian rings, with R integral. Then there is a non-zero $f \in R$ such that S_f is a free R_f-module.

Proof: A proof of (i) can be found in [2], Algebra 128.1. For (ii) we refer to [2], Algebra 118.1.

□

Proposition 4.31. *Let $f : X \to Y$ be a homomorphism of abelian varieties. Then the following conditions are equivalent:*

(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.

Proof: Let us first assume that (b) holds. As $f_{\bar{k}}$ is proper it is quasi-finite at 0. So it is flat at 0 by (i) of the lemma. Because all rational fibres are translates of $\mathrm{Ker}(f_{\bar{k}})$ it follows that $f_{\bar{k}}$ is flat, and so is f. Therefore, for any $z \in X$, we have

$$\dim \mathcal{O}_{X_y,x} = \dim \mathcal{O}_{X,x} - \dim \mathcal{O}_{Y,y} = \mathrm{tr.deg}_k(k(y)) - \mathrm{tr.deg}_k(k(x)) \leq 0$$

It must be 0 because the left is non-negative. So f is quasi-finite and hence finite. It means $f(X)$ is closed and open in Y. Hence f is surjective. This shows that (a) and (c) hold.

Next suppose that (a) holds. By (ii) of the lemma, $f_{\bar{k}}$ is flat over a non-empty open subset $U \subseteq X$. As all rational fibres of $f_{\bar{k}}$ are translates of $\mathrm{Ker}(f_{\bar{k}})$, $f_{\bar{k}}$ is flat. By the same argument we have f is finite. So (a) implies (b).

Finally, it is easy to check (c) implies (a).

□

Definition 4.32. *A homomorphism $f : X \to Y$ of abelian varieties is called an isogeny if f satisfies the three equivalent conditions (a), (b) and (c) in 4.31. The degree of an isogeny f is the degree of the function field extension* $\deg(f) = [K(X) : K(Y)]$. *(Note that we have a homomorphism $K(Y) \to K(X)$, since an isogeny is surjective and hence dominant.)*

Remark 4.33. *Let $f : X \to Y$ be an isogeny. Computing this rank at the generic point of Y, respectively the closed point $0 \in Y$, gives*

$$\deg(f) = \mathrm{rank}_{O_Y}(f_* O_X) = \dim_k \Gamma(\mathrm{Ker}(f))$$

If $f : X \to Y$ and $g : Y \to Z$ are isogenies then so is $g \circ f$, and $\deg(g \circ f) = \deg(g) \cdot \deg(f)$.

Lemma 4.34. *Let $f : W \to X$ and $h : Y \to Z$ be isogenies of abelian varieties over k. If g_1, $g_2 : X \to Y$ are homomorphisms such that $h \circ g_1 \circ f = h \circ g_2 \circ f$ then $g_1 = g_2$.*

Proof: Suppose $h \circ g_1 \circ f = h \circ g_2 \circ f$. Because f is faithfully flat, it is an epimorphism of schemes, so it follows that $h \circ g_1 = h \circ g_2$. Hence $g_1 - g_2$ maps X into the finite group scheme $\mathrm{Ker}(h)$. As X is connected and reduced, $g_1 - g_2$ factors through $\mathrm{Ker}(h)^0_{\mathrm{red}}$, which is trivial.

□

This means any isogeny is both monomorphism and epimorphism in AV_k. Next we introduce a special class of isogenies.

Lemma 4.35. *(see [2]Algebra 140.9) Let $R \to S$ be an injective finite type ring map with R and S Noetherian domains. Then $R \to S$ is smooth at $\mathfrak{q} = (0)$ if the induced extension L/K of fraction fields is finite separable.*

Proposition 4.36. *Let $f : X \to Y$ be an isogeny. The following conditions are equivalent.*

(a) The function field $K(X)$ is a separable field extension of $K(Y)$;

(b) f is an étale morphism;

(c) $\mathrm{Ker}(f)$ *is an étale group scheme.*

Proof: It is clear that (b) implies (a) and (c).

Suppose that (a) holds. By the lemma above $f_{\bar{k}}$ is smooth at a neighborhood of the generic point ξ of X. So by translating to all closed points of $X_{\bar{k}}$ we conclude $f_{\bar{k}}$ is smooth and so is f. Then $\Omega_f = 0$ because X is connected, Ω_f is locally free of finite rank and $\Omega_{f,\xi} = 0$. So f is étale. This means (a) implies (b).

Suppose that (c) holds we have $\Omega_{f_{\bar{k}},0} = 0$ by Nakayama lemma. Then by translating to all closed points of $X_{\bar{k}}$ we conclude $\Omega_{f_{\bar{k}}} = 0$ and hence $\Omega_f = 0$. Taking the stalk of the ξ we have $\Omega_{K(X)/K(Y)} = \Omega_{f,\xi} = 0$, which means $K(X)|K(Y)$ is separable.

□

Definition 4.37. *An isogeny $f : X \to Y$ is called separable if it satisfies the three equivalent conditions above. It is called a (purely) inseparable isogeny if it satisfies three equivalent conditions above.*

Definition 4.38. *Let $f : X \to S$ be a morphism of schemes. We say that f is universally injective if and only if for any morphism of schemes $S' \to S$ the base change $f' : X_{S'} \to S'$ is injective (on underlying topological spaces).*

Lemma 4.39. *(see [2] Morphism 10.2) Let $f : X \to S$ be a morphism of schemes. The following are equivalent:*

(i) For every field K the induced map $\mathrm{Mor}(\mathrm{Spec}(K), X) \to \mathrm{Mor}(\mathrm{Spec}(K), S)$ is injective.

(ii) The morphism f is universally injective.

(iii) The morphism f is injective, and for every $x \in X$ the field extension $k(x)|k(f(x))$ is purely inseparable.

(iv) The diagonal morphism $\Delta_{X/S} : X \longrightarrow X \times_S X$ is surjective.

Proposition 4.40. *Let $f : X \to Y$ be an isogeny of abelian varieties. The following conditions are equivalent.*

(a) The function field $K(X)$ is a purely inseparable field extension of $K(Y)$;

(b) f is a universally injective morphism;

(c) $\mathrm{Ker}(f)$ is a connected group scheme.

Proof: Assume (a) holds. We can factor f as a composition of two isogenies: $X \to X/\mathrm{Ker}(f)^0 \to Y$. The kernel of the second isogeny is $\mathrm{Ker}(f)/\mathrm{Ker}(f)^0$, which is étale. (See also 3.29) Using 4.36 it follows that (c) holds.

That (b) implies (a) is immediate from property (ii) in 4.39, applied to the generic point of X.

Finally suppose that (c) holds. Let $k \subset K$ be a field extension. Let A be the affine algebra of N and write $A_K = A \otimes_k K$. If $y : \mathrm{spec}(K) \to Y$ is a K-valued point then the scheme-theoretic fibre $f^{-1}(y) := X \times_{Y,y} \mathrm{Spec}(K)$ is isomorphic to $N_K = \mathrm{Spec}\,(A_K)$ by translation. As A_K has finite K-dimension it is an artinian ring. Any artinian ring is a product of artinian local rings; this corresponds to the decomposition of $f^{-1}(y)$ as a union of connected components. But we know from (i) of (3.17) that N_K is a connected scheme. Hence A_K is artinian local and $|f^{-1}(y)|$ consists of a single point. This shows that f satisfies condition (i) of 4.39 and therefore $K(Y) \to K(X)$ is purely inseparable.

□

Proposition 4.41. *Every isogeny $f : X \to Y$ can be factorized as $f = h \circ g$, where $g : X \to Z$ is an inseparable isogeny and $h : Z \to Y$ is a separable isogeny. This factorization is unique up to isomorphism, in the sense that if $f = h' \circ g' : X \to Z' \to Y$ is a second such factorization then there is an isomorphism $\alpha : Z \xrightarrow{\sim} Z'$ with $g' = \alpha \circ g$ and $h = h' \circ \alpha$.*

Proof: Immediate from the above and 3.29.

□

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

Theorem 4.42. *For $n \neq 0$, the morphism $[n]_X$ is an isogeny. If $g = \dim(X)$, we have $\deg([n]_X) = n^{2g}$. If $(\mathrm{char}(k), n) = 1$ then $[n]_X$ is separable.*

Proof: Choose an ample and symmetric line bundle L on X. (Recall that L is said to be symmetric if $(-1)^*L \cong L$, and note that if L is ample then $L \otimes (-1)^*L$ is ample and symmetric.) By 4.21 we know that $n_X^*L \cong L^{\otimes n^2}$. The restiction of n_X^*L to $\mathrm{Ker}([n])$ is a trivial bundle which is ample. (Here we use that $n \neq 0$.) This implies that $\mathrm{Ker}(f)$ must be finite, hence $[n]_X$ is an isogeny. To compute the degree we use intersection theory of line bundles on projective varieties. Choose an ample and symmetric line bundle L on X. Then $\deg([n]_X) \cdot (L)^g = ([n]_X^*L)^g$. But $[n]_X^*L$ is $L^{\otimes n^2}$, so $([n]_X^*L)^g = n^{2g} \cdot (L)^g$, and we find that $\deg([n]_X) = n^{2g}$.

If $\mathrm{char}(k) = 0$ then the last assertion is trivial. If $\mathrm{char}(k) = p > 0$ with $p \nmid n$ then also p does not divide $n^{2g} = [K(X_1) : K(X_2)]$, the field extension $K(X_2) \subset K(X_1)$ given by f is separable.

□

Proposition 4.43. *Let X be an abelian variety of dim $g > 0$. Then for an integer $n \neq 0$, $[n]_X$ is separable if and only if $(\mathrm{char}(k), n) = 1$.*

Proof: We only need to prove the "only if" part. Assume that $[n]$ is separable. Therefore $[n]$ is etale and we conclude $T_{X,e} \xrightarrow{n} T_{X,e}$ is isomorphic, so we must have $p \nmid n$ otherwise the multiplication by n on g-dimensional k-linear space $T_{X,e}$ is 0, contradiction.

□

Proposition 4.44. *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 $n \cdot Q = P$.*

Proof: By the algebraically closed assumption, $X(k)$ is the same as closed points on X. The previous theorem that $[n]$ is an isogeny implies $[n]^{-1}(P)$ is a non empty closed set of X for any closed point $P \in X$. Then the statement is directly from the Jacobson property on X.

□

Corollary 4.45. *If* $(\mathrm{char}(k), n) = 1$ *then* $X[n](k_s) = X[n](\bar{k}) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.

Proof: We know that $X[n]$ is an étale group scheme of rank n^{2g}. Hence $X[n](k_s) = X[n](\bar{k})$ is an abelian group of order n^{2g}, killed by n. Further, for every prime divisor l^m of n the subgroup of elements killed by l^m is just $X[l^m](k_s)$ and has order l^{2g}. It now readily follows from the structure theorem for finite abelian groups that we must have $X[n](k_s) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.

□

Proposition 4.46. *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* $f \circ g = [d]_Y$.

Proof: If $\deg(f) = d$ then $\mathrm{Ker}(f)$ is a finite group scheme of rank d and is therefore annihilated by multiplication by d; see 3.10. It follows that $[d]_X$ factors as

$$[d]_X = (X \xrightarrow{f} Y \xrightarrow{g} X)$$

for some isogeny $g : Y \to X$. Then $g \circ [d]_Y = [d]_X \circ g = (g \circ f) \circ g = g \circ (f \circ g)$, and by Lemma 4.34 it follows that $f \circ g = [d]_Y$.

□

Corollary 4.47. *The relation* $X \sim_k Y$ *is an equivalence relation on the set of isomorphic class of abelian varieties over* k. *(Isomorphic class of abelian varieties over* k *is a set since any abelian variety is projective over* k.*)*

4.4 Frobenius and p-rank of abelian varieties

Throughout this subsection, we assume all base schemes are of characteristic $p > 0$. For any S-scheme of $p = 0$, we have a natural transformation $F_{X/S} : X \to X^{(p/S)}$ called the relative Frobenius morphism. Actually, if X is a group S-scheme, then $F_{X/S}$ is a homomor-

phism by the following diagram.

$$\begin{array}{ccc} X \times_S X & = & X \times_S X \\ \downarrow & & \downarrow \\ X^{(p/S)} \times_S X^{(p/S)} & \xrightarrow{\simeq} & (X \times_S X)^{(p/S)} \end{array}$$

For more details, see [3] 3.2.4.

Proposition 4.48. *Let X be a g-dimensional abelian variety over a field k with* $\mathrm{char}(k) = p > 0$. *Then the relative Frobenius homomorphism $F_{X/k} : X \to X^{(p)}$ is a purely inseparable isogeny of degree p^g.*

Proof: Write $X[F] := \mathrm{Ker}\left(F_{X/k}\right)$. On underlying topological spaces, the absolute Frobenius $\mathrm{Frob}_X : X \to X$ is the identity. It follows that the topological space underlying $X[F]$ is the singleton $\{e\}$, which must be finite over k by Noetherian normalization, hence $F_{X/k}$ is an isogeny.

Let now $U = \mathrm{Spec}(A)$ be an affine open neigbourhood of e in X such that e corresponds to the maximal ideal $\mathfrak{m} \subset A$. Write $\hat{A}$ for the $\mathfrak{m}$-adic completion of A. Without loss of generality we may assume that $x_1, \ldots, x_g$ form a basis of $\mathfrak{m}/\mathfrak{m}^2 = T^{\vee}_{X,e}$. The structure theory for complete regular local rings tells us that there is an isomorphism

$$k[[t_1, \ldots, t_g]] \xrightarrow{\sim} \hat{A}$$

sending t_i to x_i, see 1.20. Since $X[F]$ is a spectrum of artin local ring, by 1.19 we find that

$$\begin{aligned} X[F] \cong \widehat{X[F]} &\cong \widehat{X}[\widehat{F}] \\ &\cong k[[t_1, \ldots, t_g]] / \left(t_1^p, \ldots, t_g^p\right) \\ &\cong k\left[t_1, \ldots, t_g\right] / \left(t_1^p, \ldots, t_g^p\right). \end{aligned}$$

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

□

Our next goal is to define the Verschiebung isogeny for abelian varieties in characteristic p. In fact, under a suitable assumption the Verschiebung can be defined for arbitrary commutative group schemes over a basis S with $char(S) = p$; we shall give the construction in this generality. First we need some preparations.

Let M be an R-module with $char(R) = p$. The symmetrization operator is the R-module

homomorphism

$$N : M^{\otimes p} \to \left(M^{\otimes p}\right)^{S_p}$$
$$m_1 \otimes \ldots \otimes m_p \mapsto \sum_{\sigma \in S_p} m_{\sigma(1)} \otimes \ldots \otimes m_{\sigma(p)}$$

The map

$$\varphi_M : M \otimes_{R,\,\mathrm{Frob}} R \to \left(M^{\otimes p}\right)^{S_p} / \operatorname{im}(N)$$
$$m \otimes \lambda \mapsto \lambda \cdot m \otimes \ldots \otimes m$$

is a natural additive transformation because

$$(a+b) \otimes \ldots \otimes (a+b) = a \otimes \ldots \otimes a + b \otimes \ldots \otimes b + \sum_{i=1}^{p-1} \frac{1}{i!(p-i)!} N(\underbrace{a \otimes \ldots \otimes a}_{i} \otimes \underbrace{b \otimes \ldots \otimes b}_{p-i}).$$

Both sides of φ_M are compatible with direct sums (the mixed terms of the right hand side are in the image of N), and with filtered direct limits. For $M = R$ we get

$$N\left(a_1 \otimes \ldots \otimes a_p\right) = p! \cdot \prod_i a_i = 0$$

and thus φ_M is an isomorphism in this case. It follows that φ_M is even an isomorphism for all modules M which are filtered inductive direct limits of free R-modules. These are exactly the flat R-modules by a theorem of Lazard. For flat R-modules M of finite rank we may also argue Zariski-local, where M becomes free.

Now we treat N and φ_M in the case of M equal to an R-algebra A. The image of N is an ideal and φ_M is an R-algebra map. Let

$$\mathrm{pr} : A^{\otimes p} \to \mathrm{Sym}^p(A)$$

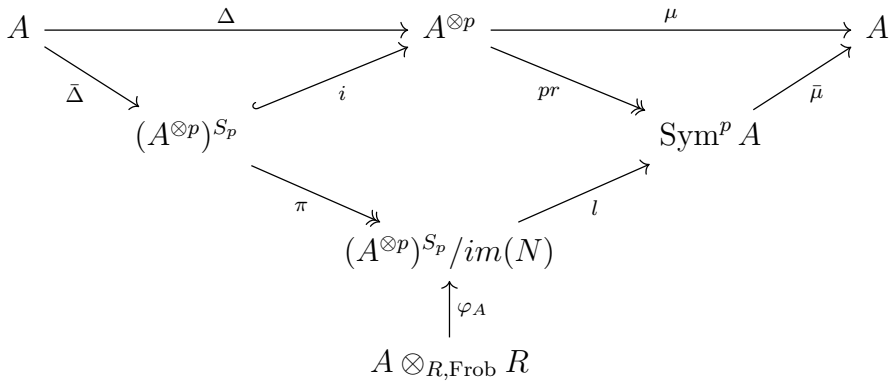
denote the quotient map of the S_p-coinvariants. Then we compute

$$\mathrm{pr} \circ N\left(a_1 \otimes \ldots \otimes a_p\right) = p! \cdot \mathrm{pr}\left(a_1 \otimes \ldots \otimes a_p\right) = 0$$

and so for a commutative and cocommutative Hopf algebra A we get the following commu-

tative diagram of R-algebra maps.

diagram 1



The top row is the map which induces the multiplication by p map $[p] : G \to G$ on the associated affine group $G = \mathrm{Spec}(A)$. The right edge leads to

$$\bar{\mu} \circ \iota \circ \varphi_A : A^{(p)} \to A$$
$$a \otimes \lambda \mapsto \lambda \cdot a \otimes \ldots \otimes a \mapsto \mathrm{pr}(\lambda \cdot a \otimes \ldots \otimes a) \mapsto \lambda \cdot a^p$$

which is easily identified with the relative Frobenius $F_{G/R} : G \to G^{(p)}$. For A representing a flat R-group G the left edge leads to the Verschiebung $V_{G/R} : G^{(p)} \to G$ by

$$V_G^* = (\varphi_A)^{-1} \circ \pi \circ \bar{\Delta} : A \to A^{(p)}.$$

Because φ_A is natural with respect to maps of R-algebras and tensor products, we get

$$V_{G \times G/R} \circ \Delta = \left(V_{G/R} \times V_{G/R}\right) \circ \Delta = \Delta^{(p)} \circ V_{G/R}$$

and the Verschiebung turns out to be a group homomorphism.

We now globalize these constructions. For this, consider a base scheme S of characteristic p and an S-scheme $q : X \to S$ where q is affine. We know that the category of affine S-schemes (warning: "affine" here means structure morphism $X \to S$ is affine) is equivalent to the category of commutative quasi-coherent $\mathcal{O}_S$-algebras. So we can replace R into $\mathcal{O}_S$, A into a flat commutative quasi-coherent $\mathcal{O}_S$-algebra $\mathcal{A}$ in the construction above. With this definition we get immediately the following proposition.

Proposition 4.49. *Let S be a scheme with $\mathrm{char}(S) = p > 0$. Let G be a flat affine commutative S-group scheme, then there is a natural homomorphism $V_{G/S} : G^{(p/S)} \to G$*

satisfying

$$V_{G/S} \circ F_{G/S} = [p]_G : G \longrightarrow G$$

Proof: The statement follows from the affine case on diagram 1 above.

□

Proposition 4.50. *(i) Let X be an abelian variety over a field k with* $\mathrm{char}(k) = p > 0$*, then there exist a unique homomorhism $V_{X/k} : X^{(p)} \to X$ such that $V_{X/k} \circ F_{X/k} = [p]_X : X \longrightarrow X$, which is called Verschiebung of an abelian variety.*
(ii) If $f : X \to Y$ is an isogeny of abelian varieties, then $f \circ V_X = V_Y \circ f^{(p)}$

Proof: The uniqueness is clear by 4.34. For the existence, consider following diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X[F] & \longrightarrow & X & \xrightarrow{F} & X^{(p)} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle [p]} & & \downarrow{\scriptstyle [p]} & \swarrow & & & \\ & & X[F] & \longrightarrow & X & & & & \end{array}$$

It suffices to show that $[p]_{X[F]} = 0$. Note $X[F]$ is clearly flat affine over k, so we have natural Verschiebung on it. Now consider following diagram.

$$\begin{array}{ccc} X & \xrightarrow{F_X} & X^{(p)} \\ \uparrow & & \uparrow \\ X[F] & \xrightarrow{F_{X[F]}} & X[F]^{(p)} \\ & \searrow^{[p]} & \downarrow{\scriptstyle V} \\ & & X[F] \end{array}$$

It is easy to show that $F_{X[F]} = 0$, hence $[p]_{X[F]} = 0$.
(ii) It is directly from the commutativity of $[p]$ and the fact that the relative Frobenius of an abelian variety is an epimorphism.

□

Now we introduce one of the most important invariant of abelian varieties.

Theorem 4.51. *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*

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

Proof: Without the generalization we can assume $k = \bar{k}$. We proceed by induction on m. Consider first the case $m = 1$: we have seen that the map $[p] : X \to X$ factors over the relative Frobenius $\mathrm{Frob}_{X/k}$ as

$$X \overset{\mathrm{Frob}_{X/k}}{\longrightarrow} X^{(p)} \overset{V}{\longrightarrow} X.$$

As $\mathrm{Frob}_{X/k}$ is a homeomorphism, there is a bijection between the p-torsion k-points $X[p](k) = [p]^{-1}(e)(k)$ and the k-points $V^{-1}(e)(k)$. Since $\deg([p]) = p^{2g}$ and $\deg\left(\mathrm{Frob}_{X/k}\right) = p^g$, we must have $\deg V = p^g$; in particular, the cardinality of $X[p](k)$ is bounded above by $\#V^{-1}(e)(k) \leq p^g$ (indeed, the degree is the size of the schemetheoretic fibre, which is at least the degree of the set-theoretic fibre). However, $X[p](k)$ is a p-torsion abelian group, and thus there exists $0 \leq i \leq g$ such that $X[p](k) \simeq (\mathbb{Z}/p\mathbb{Z})^i$.

If $m > 1$, we can use that $[p^m] : X \to X$ is surjective by 4.31 (and hence that $X(k)$ is divisible) to construct a short exact sequence

$$0 \longrightarrow X[p](k) \longrightarrow X\left[p^m\right](k) \overset{[p]}{\longrightarrow} X\left[p^{m-1}\right](k) \longrightarrow 0.$$

By induction on m, we have isomorphisms $X[p](k) \simeq (\mathbb{Z}/p\mathbb{Z})^i$ and $X\left[p^{m-1}\right](k) \simeq (\mathbb{Z}/p^{m-1}\mathbb{Z})^i$, so

$$\#X\left[p^m\right](k) = \#\left(\mathbb{Z}/p\mathbb{Z}\right)^i \times \#\left(\mathbb{Z}/p^{m-1}\mathbb{Z}\right)^i = \#\left(\mathbb{Z}/p^m\mathbb{Z}\right)^i,$$

i.e. $X\left[p^m\right](k)$ has the correct cardinality. Now, observe that $\mathrm{Ker}(p)$ of $p : X\left[p^m\right](k) \to X\left[p^m\right](k)$ is exactly $X[p](k) \simeq (\mathbb{Z}/p\mathbb{Z})^i$, so $X\left[p^m\right](k)$ must be $(\mathbb{Z}/p^m\mathbb{Z})^i$ by the structure theorem for finite abelian groups.

□

Remark 4.52. *(i) Let X be an abelian variety of p-rank $f > 0$ over a non-perfect field k, and let $k \subset k_s \subset \bar{k}$ be respectively a separable closure and an algebraic closure of k. Then we have natural injective maps $X\left[p^m\right](k_s) \to X\left[p^m\right](\bar{k})$, but these are not, in general, isomorphisms. In other words, in order to see all p^{mf} distinct physical points of order p^m, in general we need an inseparable extension of the ground field.*
(ii) 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 $f(X) = f\left(X_K\right)$. To see this we may assume that k and K are both algebraically closed. Since k is algebraically closed, any connected component $Z \subset X[p]$ is a geometrically connected finite open sub k-scheme. This implies that Z_K is a single point. So $X_K[p](K)$ has the same cardinality as $X[p](k)$, indeed $f(X) = f\left(X_K\right)$.
(iii) $f\left(X_1 \times X_2\right) = f\left(X_1\right) + f\left(X_2\right)$ for abelian varieties X_1 and X_2 over k.

Proposition 4.53. *If $h : X \to Y$ is an isogeny of abelian varieties over a field k, then $f(X) = f(Y)$.*

Proof: Assume $\deg(g) = d$. Consider following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Ker}(h) & \longrightarrow & X & \longrightarrow & Y & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & K_{h,m} & \longrightarrow & X[p^m] & \longrightarrow & Y[p^m] & & \end{array}$$

We have $\#K_{h,m}(\bar{k}) \leq \mathrm{rank}_k(K_{h,m}) \leq \mathrm{rank}_k(\mathrm{Ker}(h)) = d$. Then by the exact sequence

$$0 \to K_{h,m}(\bar{k}) \to X[p^m](\bar{k}) \to Y[p^m](\bar{k})$$

we get $p^{mf(X)} \leq d \cdot p^{mf(Y)}$. Taking m large enough, it follows that $f(X) \leq f(Y)$. As $X \sim Y$ is a symmetric relation, we conclude that $f(X) = f(Y)$.

□

An elliptic curve X is said to be ordinary if $f(X) = 1$ and supersingular if $f(X) = 0$. We end this paper with following beautiful theorems about p-rank of elliptic curves. [16]

Theorem 4.54. *Let C be an elliptic curve over a field k. Then $ht(\hat{C}) = 1$ or $ht(\hat{C}) = 2$.*

Proof: We know that $C[p] = \mathrm{Spec}\, R$ for a finite k-algebra R of rank p^2. The (formal) group scheme $\widehat{C[p]}$ is represented by $\lim R/\mathfrak{m}^j$ where $\mathfrak{m}$ corresponds $0 \in C[p]$. As R is Artinian, we have $\mathfrak{m}^N = \mathfrak{m}^{N+1} = \cdots$ for some $N > 0$ and thus $\lim R/\mathfrak{m}^j \cong R/\mathfrak{m}^N$. Note that $\mathrm{Spec}\, R/\mathfrak{m}^N = \mathrm{Spf}\, R/\mathfrak{m}^N$ as $\mathfrak{m}^N$ is already open ideal.

If one chooses a coordinate on $\widehat{C}$, one obtains a formal group law F over k. By 1.18 we know that $k[[x]]\widehat{/[p]_F}(x)$ represents the p-torsion $\hat{C}[p]$, we obtain $k[[x]]\widehat{/[p]_F}(x) \cong R/\mathfrak{m}^N$ is a finite k-module, so $[p]_F(x) \neq 0$ and $h = ht(F) < \infty$. Therefore we have

$$k[[x]]\widehat{/[p]_F}(x) \simeq \lim k[x]/(\overline{[p]_F(x)}_j + x^j) \simeq k[x]/(\overline{[p]_F(x)}_{p^h+1} + x^{p^h+1})$$

where $\overline{[p]_F(x)}_j$ means the first j terms of $[p]_F(x)$. Thus,

$$p^{\mathrm{height}(F)} = \dim_k k[x]/(\overline{[p]_F(x)}_{p^h+1} + x^{p^h+1}) = \dim_k k[[x]]\widehat{/[p]_F}(x) = \dim_k R/\mathfrak{m}^N \leq \dim_k R = p^2.$$

□

Theorem 4.55. *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 $ht(\hat{C}) + f(C) = 2$.

Proof: Suppose (i) holds, then $C[p]$ is connected and hence geometrically connected by 3.11. But $C[p]$ is geometrically connected is equivalent to $C[p](\bar{k}) = 0$, so (i) is equivalent to (ii).

Suppose (ii) holds, then $C[p] = \mathrm{Spec}(R)$ is artinian local. Therefore $\mathfrak{m}^N = 0$ and

$$p^{\mathrm{height}(F)} = \dim_k R/\mathfrak{m}^N = \dim_k R = p^2$$

So we get (ii) implies (iii).

Suppose (iii) holds, then

$$p^{\mathrm{height}(F)} = \dim_k R/\mathfrak{m}^N = p^2 = \dim_k R$$

So $\mathfrak{m}^N$ must be 0, which implies $(R, \mathfrak{m})$ is artinian local and $C[p]$ is connected. We get (iii) implies (ii).

□

参考文献

[1] Strickland N P. Formal schemes and formal groups [J]. Contemporary Mathematics. 1999, 239: 263–352. 1.1

[2] Stacks Project Authors T. *Stacks Project* [J]. 2018. 1.9, 1.13, 1.2, ii, 2.4, 2.1, 3.7, 3.1, 3.2, 3.2, 3.22, 3.24, 4.1, 4.1, 4.3, 4.35, 4.39

[3] Liu Q, et al. Algebraic geometry and arithmetic curves [M]. Oxford University Press on Demand, 2002. 2.1, 4.1, 4.3, 4.4

[4] Hartshorne R. Algebraic geometry [M]. Springer Science & Business Media, 2013. 2.15

[5] Stix J. A course on finite flat group schemes and p-divisible groups [J]. preprint. 2009. 3.1

[6] Ribes L, Zalesskii P. Profinite groups [M]. Springer, 2000. 3.2

[7] Neukirch J. Algebraic number theory [M]. Springer Science & Business Media, 2013. 3.2

[8] Gabriel, Demazure. Groupes algébriques [M]. Springer, 1970. 3.3

[9] Olsson M. Algebraic spaces and stacks [M]. American Mathematical Soc., 2016. 3.3

[10] Waterhouse W. Basically bounded functors and flat sheaves [J]. Pacific Journal of Mathematics. 1975, 57 (2): 597–610. ii

[11] Michel, Grothendieck. Séminaire de Géométrie Algébrique du Bois Marie [M]. Berlin; New York: Springer-Verlag, 1970. 3.24

[12] Edixhoven B, Van der Geer G, Moonen B. Abelian varieties [J]. Preprint. 2012: 331. 4

[13] Bhatt B. MATH 731: Topics in Algebraic Geometry I–Abelian Varieties [J]. Notes by Matt Stevenson. 2017. 4

[14] Görtz U, Wedhorn T. Algebraic Geometry I: Schemes [M]. Springer, 2010. 4.5, 4.1

[15] Mumford D, Ramanujam C P, Manin J I. Abelian varieties [M]. Oxford university press Oxford, 1974. 4.1, 4.1

[16] Meier L. From Elliptic Genera to Topological Modular Forms [J]. 2022. 4.4

声明

本人声明所呈交的学位论文是本人在导师指导下进行的研究工作及取得的研究成果。据我所知，除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得四川大学或其他教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示谢意。

本学位论文成果是本人在四川大学读书期间在导师指导下取得的，论文成果归四川大学所有，特此声明。

作者签名: _____ 导师签名: _____

日　　期: _____ 日　　期: _____

Acknowledgement

There are many people to whom I owe a debt of thanks for their support over the last year. First, I would like to sincerely acknowledge my supervisor Yifei Zhu for suggesting I study elliptic curves and patiently guiding me through the mathematics involved. He always found adequate time to oversee my studies and to share his knowledge and expertise with me. I would like to thank classmates in mathematics departments of Sichuan University and SUSTech(Southern University of Science and Technology) for their dedication and time in academic exchanges with me. Finally, I would like to thank my family and friends for encouraging me over the last year.