UNIVERSITÄT
HEIDELBERG
ZUKUNFT
SEIT 1386

Bachelor's Thesis

Computing simple factors of certain Jacobian varieties over finite fields

by *Tim Holzschuh*

supervised by
Prof. Dr. Gebhard Böckle

Abstract

We give a detailed exposition of some basic results concerning abelian varieties (over arbitrary fields), including proofs of the Theorem of the Cube, the Theorem of the Square and the infamous Poincaré Splitting Theorem.
We then continue by stating results over *finite* fields, which we finally apply to describe an algorithm that is capable of explicitly computing the decomposition of an abelian variety into its simple factors for Jacobian varieties associated to curves corresponding to certain Carlitz-cyclotomic function fields.

Zusammenfassung

Wir präsentieren eine detaillierte Einführung in einige grundlegende Resultate über Abelsche Varietäten (über beliebigen Körpern), inklusive vollständiger Beweise des Theorems des Kubus, des Quadrats und des berühmten Reduzibilitätssatzes von Poincaré.
Danach erwähnen wir Resultate im Fall *endlicher* Körper und nutzen diese letztendlich, um einen Algorithmus zu beschreiben mit dem man die Zerlegung einer Abelschen Varietät in ihre einfachen Faktoren für Jacobische Varietäten assoziiert zu Kurven, die zu bestimmten Carlitz-zyklotomischen Körpererweiterungen korrespondieren, berechnen kann.

Contents

1 Introduction

The theory of *abelian varieties* is of fundamental importance in modern mathematics.
Abelian varieties are higher-dimensional generalizations of *elliptic curves*, which are of essential interest in a vast amount of questions regarding *arithmetic*, to begin with. Then there is *Chevalley's structure theorem* telling us that any *algebraic group* G defined over a perfect field k fits inside a short exact sequence

$$1 \longrightarrow H \longrightarrow G \longrightarrow A \longrightarrow 1$$

with H a *linear algebraic group* and A an *abelian variety*, suggesting a way of studying general algebraic groups by means of studying the linear and projective part of the theory separately.
Last but not least they also are a crucial tool in studying algebraic curves C through their *Jacobian* $\mathcal{J}$, which is an abelian variety classifying degree zero line bundles living on C - which we will talk about again later.
The content of this bachelor's thesis can be roughly separated into two parts. There is a theoretical part trying to investigate long-known fundamental results on abelian varieties in general. We start off with a quick survey on the theory of general *group schemes* trying to emphasize the *functorial point of view* and fixing some basic notions and ideas the presence of which is ubiquitous in the upcoming theory.
The subsequent four chapters then all are devoted to studying *abelian varieties* over arbitrary ground fields. In chapter 4 we explain why abelian varieties are *abelian*, a result which is not as obvious as the mere name might suggest.
We take some time to investigate *line bundles* on abelian varieties and prove – among other things – the renowned theorems of the *cube* and of the *square*.
The notion of *isogeny* and basic properties of it are introduced in chapter 5. Identifying abelian varieties *up to isogeny* results in a classification task that is properly coarser than that of identifying isomorphic abelian varieties only. However, the former task seems much more feasible than the latter and *isogenous* abelian varieties still share interesting properties.
Chapter 6 gives a rather incomplete introduction to the study of *picard schemes*, in particular of the *dual* X^t of an abelian variety X, introduces *polarizations*, the overall importance of which should certainly *not* be measured by the amount of time spent studying them in this particular thesis, and finishes off with shortly introducing the notion of *Jacobian varieties*.
Then, we finally are able to study *endomorphisms* of abelian varieties, resulting in the proof of the main result of the theoretical part of this thesis, namely the *Poincaré Splitting Theorem* 7.1 which roughly states that *any* abelian variety admits a *unique* decomposition into *simple* abelian subvarieties *up to isogeny*.
As it was the authors personal aim to get a basic understanding of the theory of abelian varieties in the first place, we try to give lots of complete proofs regarding abelian varieties and group schemes. We freely use the language of *schemes* and related results though and make extensive use of existing literature, especially the well-known *stacks project*.

The second part of this bachelor thesis has a more *algorithmic* flavor. As already mentioned, one important application of abelian varieties is to the theory of curves C by means of studying their *Jacobian variety* $\mathcal{J}$. The Poincaré Splitting Theorem tells us that $\mathcal{J}$ can – at least up to isogeny – be decomposed into simple factors, that are easier to study as the name suggests already. It gives us no direct clue on how to *effectively determine* such a decomposition though.
We try to address this question in the second part for *certain curves* defined over *finite* fields. A famous theorem by *Taira Honda* and *John T. Tate* gives a much more delicate understanding of the structure theory of abelian varieties over *finite fields*. This theorem together with results of *Steven Galovich* and *Michael Rosen* allows us to develop a computer algorithm (implemented in MAGMA) that is able to compute a set of *complete invariants* of the simple factors of Jacobians associated to curves that arise as special *Carlitz-cyclotomic* field extensions of function fields.

Acknowledgements

First of all I would like to sincerely thank my advisor *Prof. Dr. Gebhard Böckle*. Not only did he suggest this exciting topic to me, but he also answered all kinds of questions of mine very patiently and explained to me many things I struggled to understand throughout my whole period of studying mathematics.
He continuously supported me in my studies and I benefited greatly from his deep understanding of mathematics in general and of algebraic and arithmetic geometry in particular.

I would furthermore like to express my deep gratitude towards my family, especially my parents *Stefan* and *Heike* not only for always encouraging me in my studies, but also for their unconditional love and their constant effort of trying to restrain me from doing too much mathematics and too few other things.

I would also like to thank *Matthias Hauck* for being a great teacher, who motivated me to become a mathematician.

Last but not least I would like to thank all of my friends, especially *Raphael Senghaas*, *Manuel Hoff* and *Lukas Heger* for their invaluable support by proofreading this thesis, their warm friendship and their endurance when it comes to discussing mathematics with me.

Finally, I would like to dedicate this thesis to my departed grandfather *Hans Gerhart* for playing a major role in the development of my curiosity, for being an incomparable role model and for giving all the warm love and support a young child could hope for.

2 Preliminaries

Conventions and Notations

Category theory

Let $\mathcal{C}$ be a category. The *dual* of $\mathcal{C}$ is denoted by $\mathcal{C}^{op}$.
Given two objects X, Y of $\mathcal{C}$ we will denote the set of morphisms $X \longrightarrow Y$ by $\mathrm{Mor}_{\mathcal{C}}(X, Y)$ or also $\mathcal{C}(X, Y)$.
If $\mathcal{C}$ is an additive category, we will often write $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ instead of $\mathrm{Mor}_{\mathcal{C}}(X, Y)$.

Given an object $S \in \mathcal{C}$ we denote by $\mathcal{C}_{/S}$ the category of objects above S. That is: An object in $\mathcal{C}_{/S}$ is given by a morphism $A \longrightarrow S$ in $\mathcal{C}$. A morphism from $A \longrightarrow S$ to $B \longrightarrow S$ is given by a commutative triangle

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr] & & B \arrow[dl] \\ & S & \end{tikzcd}$$

in $\mathcal{C}$.
Consequently, we will denote the category of objects beneath S by $\mathcal{C}^{S/}$, it is given as the dual of the category $\mathcal{C}_{/S}$.
Given categories $\mathcal{C}_\circ$ and $\mathcal{C}_\bullet$, the category of functors $\mathcal{C}_\circ \longrightarrow \mathcal{C}_\bullet$ will be denoted by $[\mathcal{C}_\circ, \mathcal{C}_\bullet]$.
Sch, Set, Grp, CRng denote the categories of *schemes*, *sets*, *groups* and *commutative unital rings* respectively.
Furthermore, given a commutative ring A we will denote by Alg_A the category $\mathsf{CRng}^{A/}$, i.e. the category of A-*algebras*.

A subspace Y of a topological space X is called *very dense* if for any open $U \subseteq X$ one has that $Y \cap U$ is dense in U.

Schemes

If $x \in X$, we will denote by $\mathcal{O}_{X,x}$ the *local ring* of X at x, by $\mathfrak{m}_{X,x}$ the unique *maximal ideal* of $\mathcal{O}_{X,x}$ and by $\kappa_X(x)$ the *residue field* of X at x, i.e. $\kappa_X(x) = \mathcal{O}_{X,x} \,/\, \mathfrak{m}_{X,x}$.
Furthermore we will often suppress X from the notation and simply write $\mathcal{O}_x$, $\mathfrak{m}_x$ and $\kappa(x)$ respectively.
Sometimes, we will denote the ring of global sections $\Gamma(X, \mathcal{O}_X)$ of a scheme X by Γ_X.

If X is integral, we will denote the function field of X by $\kappa(X)$, that is: $\kappa(X) = \mathcal{O}_{X,\eta}$ where η is the generic point of X.

A morphism $X \xrightarrow{f} Y$ of schemes is *surjective*, if the underlying map of sets is surjective.

If $X \longrightarrow S$ is a scheme$_{/S}$ and $S' \longrightarrow S$ is any morphism, we often denote by $X_{S'}$ the S'-scheme obtained by base change of X along $S' \longrightarrow S$, i.e. $X_{S'} \overset{\mathrm{def}}{=} X \times_S S'$ viewed as an S'-scheme via the canonical projection. If $X \xrightarrow{f} Y$ is a morphism over S we consequently denote by $f_{S'}$ the morphism $X_{S'} \xrightarrow{f \times_S \mathrm{id}_{S'}} Y_{S'}$.
Note that $f_{S'}$ is a morphism over S'.

Using the Yoneda lemma, we will frequently identify a scheme X over S with its functor of points $X(\cdot) : \mathsf{Sch}_{/S}^{op} \to \mathsf{Set}$ given by $T \mapsto \mathsf{Sch}_{/S}(T, X)$ and $(f : T \to T') \mapsto (g \mapsto g \circ f)$.
We may sometimes write $X_S(\cdot)$, $X_{/S}(\cdot)$ if we want to stress that we are considering points of X *above* S. This should not introduce any confusions as $X \times_S S \cong X$ as schemes$_{/S}$.

The category of *quasi-coherent* sheaves on X is denoted by $\mathsf{QCoh}(X)$.
A *rank n vector bundle* on a scheme X is a locally free $\mathcal{O}_X$-module of rank n. A rank 1 vector bundle is also called *line bundle*.
Let k be a field. By *k-variety* (or *variety$_{/k}$*) we mean separated k-scheme of finite type that is geometrically integral (e.g. X_K is integral for some algebraically closed field K containing k).
A k-variety V is called *complete* if the structure morphism $V \longrightarrow \operatorname{Spec} k$ is proper.

Some generalities used frequently

Now that we have fixed notations and standing conventions, we would like to collect some facts, that will be used more or less frequently in the following chapters. Most of these are collected from [Vakil].

Yoneda Lemma 2.1.
Let $\mathcal{C}$ be a category, $X \in \mathcal{C}$ and $\mathcal{C}^{op} \xrightarrow{F} \mathsf{Set}$ a presheaf on $\mathcal{C}$. Then one has a bijection

$$[\mathcal{C}^{op}, \mathsf{Set}](\mathcal{C}(\cdot, X), F) \longrightarrow F(X), \eta \mapsto \eta_X(\mathrm{id}_X)$$

natural in X and F. The inverse is given explicitly by $F(X) \ni a \mapsto (\eta_Y : f \mapsto F(f)(a))$.

Lemma 2.2.
Let S be a scheme. The category $\mathsf{Sch}_{/S}$ admits equalizers. Given any two morphisms$_{/S}$ $X \underset{g}{\overset{f}{\rightrightarrows}} Y$, the canonical morphism $\mathrm{Eq}(f, g) \longrightarrow X$ is an embedding, and a closed embedding if Y is separated$_{/S}$.

Proof. Follows formally from the fact that $\mathsf{Sch}_{/S}$ admits fiber products and finite products. More concretely, $\mathrm{Eq}(f, g)$ is given via the following cartesian diagram:

$$\begin{tikzcd}
\mathrm{Eq}(f,g) \arrow[r] \arrow[d, "i"'] \arrow[dr, phantom, "\lrcorner", very near start] & Y \arrow[d, "\Delta"] \\
X \arrow[r, "f \times_S g"] & Y \times_S Y
\end{tikzcd}$$

as one can check on points for example. Hence i is seen to be an embedding by base change, and it is a closed embedding if Y is separated. □

Lemma 2.3.
Let $\mathcal{C}_\circ$ be a category admitting equalizers and $\mathcal{C}_\circ \xrightarrow{F} \mathcal{C}_\bullet$ a *conservative* functor commuting with equalizers. Then F is *faithful.*

Proof. Let $f, g \in \mathcal{C}_\circ(X, Y)$. Then

$$\begin{aligned} F(f) = F(g) &\iff \mathrm{Eq}(F(f), F(g)) = F(\mathrm{Eq}(f, g)) \text{ is an isomorphism} \\ &\iff \mathrm{Eq}(f, g) \text{ is an isomorphism} \\ &\iff f = g. \end{aligned} \tag{2.1}$$

Hence for any $X, Y \in \mathcal{C}_\circ$ one has that $\mathcal{C}_\circ(X, Y) \xrightarrow{F_{X,Y}} \mathcal{C}_\bullet(FX, FY)$ is injective, i.e. F is faithful. □

Remark 2.4.
Note that Lemma 2.3 is applicable when $\mathcal{C}_\circ$ and $\mathcal{C}_\bullet$ are abelian and when F is *left-exact.*

As a useful application of Lemma 2.3, we obtain the following immediate

Corollary 2.5.
Let $X \xrightarrow{f} Y$ be a *faithfully flat* morphism of schemes.
Then the pullback functor $f^* : \mathsf{QCoh}(Y) \longrightarrow \mathsf{QCoh}(X)$ is faithful.

Proof. f^* is *conservative*, as the property of being an isomorphism of sheaves is a stalk-local property and as

$$f^*(\mathcal{F})_x = \mathcal{F}_{f(x)} \otimes_{\mathcal{O}_{Y,f(x)}} \mathcal{O}_{X,x},$$

i.e. the statement reduces to the fact that $(- \otimes_A M)$ is conservative when M is faithfully flat$_{/A}$.
Flatness of f implies *exactness* of f^*, implying *faithfulness* of f^* in virtue of Remark 2.4. □

Reduced-to-Separated Theorem 2.6.
Two morphisms$_{/S}$ $U \underset{g}{\overset{f}{\rightrightarrows}} Z$ from a reduced scheme U to a separated scheme Z agreeing on a dense open subset of U are equal.

Proof. $\mathrm{Eq}(f,g)$ is closed in U, hence equals U topologically, as it contains a dense open subset of U by the assumption.
As U is assumed to be reduced, we obtain that $\mathrm{Eq}(f,g) = U$, i.e. $f = g$. □

Cancellation Theorem 2.7.
Let $\mathcal{P}$ be a class of morphisms that is stable under composition and base change. Suppose

$$\begin{tikzcd}
X \arrow[rr, "f"] \arrow[dr, "h"'] & & Y \arrow[dl, "g"] \\
& Z &
\end{tikzcd}$$

is a commutative triangle of schemes.
Suppose further that $Y \xrightarrow{\Delta_g} Y \times_Z Y$ and $X \xrightarrow{h} Z$ are in $\mathcal{P}$. Then f is in $\mathcal{P}$ as well. In particular:

(i) Suppose that embeddings are in $\mathcal{P}$. If $h \in \mathcal{P}$, then $f \in \mathcal{P}$.
(ii) Suppose that closed embeddings are in $\mathcal{P}$. If $h \in \mathcal{P}$ and if g is separated, then $f \in \mathcal{P}$.
(iii) Suppose that quasicompact morphisms are in $\mathcal{P}$. If $h \in \mathcal{P}$ and if g is quasi-separated, then $f \in \mathcal{P}$.

Proof. One uses that

$$\begin{tikzcd}
X \arrow[r, "\Gamma_f"] \arrow[d, "f"'] \arrow[dr, phantom, "\lrcorner", very near start] & X \times_Z Y \arrow[d, "f_Y"] \\
Y \arrow[r, "\Delta_g"] & Y \times_Z Y
\end{tikzcd}$$

is cartesian, as can be easily checked on points.
Here Γ_f denotes the *graph morphism*, i.e. Γ_f is the unique morphism$_{/Z}$ such that $\mathrm{pr}_1 \circ \Gamma_f = \mathrm{id}_X$ and $\mathrm{pr}_2 \circ \Gamma_f = f$.
As $\Delta_g \in \mathcal{P}$, so is Γ_f, as $\mathcal{P}$ is stable under base change. pr_2 also is in $\mathcal{P}$, as it is the base change of h along g and as $h \in \mathcal{P}$:

$$\begin{tikzcd}
X \times_Z Y \arrow[r, "\mathrm{pr}_2"] \arrow[d, "\mathrm{pr}_1"'] \arrow[dr, phantom, "\lrcorner", very near start] & Y \arrow[d, "g"] \\
X \arrow[r, "h"] & Z
\end{tikzcd}$$

Hence we see that $f = \mathrm{pr}_2 \circ \Gamma_f \in \mathcal{P}$ as we assumed $\mathcal{P}$ to be stable under composition.
Assertions (i)-(iii) follow immediately. □

Proposition 2.8.
If X is a connected, reduced and proper scheme over an algebraically closed field $k = \bar{k}$, then $\Gamma(X, \mathcal{O}_X) = k$.

Proof. [Vakil, Paragraph 10.3.7] □

Proposition 2.9 (Equality of morphisms$_{/k}$ descends).

Let $K \mid k$ be a field extension. Suppose $X \overset{f}{\underset{g}{\rightrightarrows}} Y$ are morphisms of schemes$_{/k}$. Then equality $f_K = g_K$ after extending the base to K *descends* to k, i.e. $f = g$ to begin with.

Proof. [Vakil, Exercise 9.2.I.] □

Lemma 2.10.

Let $X \xrightarrow{f} Y$ be a morphism$_{/S}$, $S' \longrightarrow S$ a quasi-compact and faithfully flat morphism and $Z \xhookrightarrow{i} Y$ an embedding. Denote the respective base changes along $S' \longrightarrow S$ by $(\cdot)'$.
Then f factorizes over i as soon as f' factorizes over i'.

Proof. We claim that f factorizes over i if and only if $f^{-1}(Z) \overset{\text{def}}{=} X \times_Y Z \cong_{/X} X$:
If $f = i \circ f_|$, then $f^{-1}(Z) \cong (i \circ f_|)^{-1}(Z) \cong f_|^{-1}(\underbrace{i^{-1}(Z)}_{=Z \times_Y Z}) = f_|^{-1}(Z) = X \times_Z Z \cong X$.
Suppose $X \cong_{/X} X \times_Y Z$ on the other hand. One then has a cartesian diagram

$$\begin{tikzcd} X \times_Y Z \arrow[r, "\mathrm{pr}_Z"] \arrow[d, "\cong"'] \arrow[dr, phantom, "\lrcorner", very near start] & Z \arrow[d, "i"] \\ X \arrow[r, "f"] & Y \end{tikzcd}$$

showing that f factorizes over i.

Hence the assumption implies that $(X \times_Y Z)_K \cong X_K \times_{Y_K} Z_K \cong_{/X_K} X_K$ which implies $X \times_Y Z \cong X$ as base changing along quasi-compact faithfully flat morphisms is *conservative* [EGA-IV, Proposition (2.7.1)]. The claim thus follows. □

Remark.

Lemma 2.10 in particular applies to the case $S' = \operatorname{Spec} K \longrightarrow \operatorname{Spec} k = S$ for arbitrary field extensions $K \mid k$.

Proposition 2.11.

Let X be a scheme locally of finite type$_{/k}$. Then the set of closed points of X lies *very dense* in X.

Proof. A proof is given in [GW, Proposition 3.35]. □

Lemma 2.12.

Suppose X is a topological space such that Y is a *very dense* subspace. Then X is *quasi-compact* if and only if Y is *quasi-compact*.

Proof. We show that $\bigcup_i U_i$ is an open cover of X if and only if $\bigcup_i (U_i \cap Y)$ is an open cover of Y. The claim is then an immediate consequence.
The *only if* part is trivial. Suppose $\bigcup_i (U_i \cap Y)$ is any open cover of Y. Then $X \cap Y = Y = \bigcup_i (U_i \cap Y) = (\bigcup_i U_i) \cap Y$ implies that $X = \bigcup_i U_i$ as Y being very dense in X means that $U \mapsto U \cap Y$ defines a bijection of open sets of X and Y respectively. □

3 Group schemes

We start off by introducing basic results on the theory of general group schemes.
Throughout this chapter we will fix a base scheme S and usually work in the category of schemes$_{/S}$.
The basic reference used to study this material is [AV].

Basic definitions

Definition 3.1 (Group scheme over S).

(i) A *group scheme over* S is a scheme$_{/S}$ G, together with a functor $\mathsf{Sch}^{op}_{/S} \xrightarrow{\bar{G}} \mathsf{Grp}$ and a fixed natural isomorphism $V \circ \bar{G}(\cdot) \xrightarrow{\cong} G(\cdot)$, where V denotes the forgetful functor $\mathsf{Grp} \to \mathsf{Set}$:

$$\begin{tikzcd}
\mathsf{Sch}^{op}_{/S} \arrow[rr, bend left, "G(\cdot)"] \arrow[dr, "\bar{G}(\cdot)"'] & {} \arrow[d, Rightarrow, "\cong"'] & \mathsf{Set} \\
& \mathsf{Grp} \arrow[ur, "V"'] &
\end{tikzcd}$$

If G and G' are group schemes over S, then a morphism $G \longrightarrow G'$ of S-schemes is called *S-homomorphism*, if for any S-scheme T the induced map $G(T) \longrightarrow G'(T), (T \to G) \mapsto (T \to G \to G')$ of T-valued points is a group homomorphism. We obtain the category $\mathsf{GSch}_{/S}$ of group schemes over S.

(ii) G is called *commutative* (or *abelian*), if $G(T)$ is an abelian group for any S-scheme T.

Notation.
We sometimes write *group scheme*$_{/S}$ (or even plainly *group scheme*, if S is to be understood from the context) instead of group scheme over S. Analogously, we sometimes write *homomorphism*$_{/S}$ or plainly *homomorphism* instead of S-homomorphism or homomorphism over S.

Remark 3.2.
Let G be a group scheme$_{/S}$. If T is any scheme$_{/S}$, the group structure on $G(T)$ gives rise to mappings

$$G(T) \times G(T) \xrightarrow{m_T} G(T),\ (g,h) \longmapsto g \cdot h,\ \ G(T) \xrightarrow{i_T} G(T),\ g \longmapsto g^{-1} \text{ and } \ 0 \xrightarrow{e_T} G(T)$$

which are the components of natural transformations $G(\cdot) \times G(\cdot) \xrightarrow{m} G(\cdot)$, $G(\cdot) \xrightarrow{i} G(\cdot)$ and $S(\cdot) \xrightarrow{e} G(\cdot)$ respectively. As $\mathsf{Sch}_{/S}$ admits finite products these transformations correspond to morphisms $G \times_S G \xrightarrow{m} G$, $G \xrightarrow{i} G$ and $S \xrightarrow{e} G$ over S, called *multiplication*, *inversion* and *unit section* respectively, of schemes$_{/S}$ by the Yoneda lemma. A group scheme$_{/S}$ G as defined above is equivalent to the data (G, m, i, e) satisfying some commutative diagrams (corresponding to the different group axioms).

A homomorphism $G \xrightarrow{f} G'$ turns out to be the same thing as a morphism $G \xrightarrow{f} G'$ of schemes$_{/S}$ such that

$$m_{G'} \circ (f \times f) = f \circ m_G \tag{3.1}$$

as morphism $G \times_S G \longrightarrow G'$.

If $G \xrightarrow{f} G'$ is a homomorphism, one has $f \circ i_G = i_{G'} \circ f$ and $f(e_G) = e_{G'}$ by the Yoneda lemma 2.1.

G is commutative if and only if $m \circ t = m$, where $G \times_S G \xrightarrow{t} G \times_S G$ corresponds to the natural transformation with components $G(T) \times G(T) \longrightarrow G(T) \times G(T),\ (g,h) \longmapsto (h,g)$.

If G is a group scheme$_{/S}$ and $S' \longrightarrow S$ is any morphism, then the base change $G_{S'} \longrightarrow S'$ is a group scheme$_{/S'}$ as $G_{S'}(T \to S') \cong G(T \to S' \to S)$ naturally in T, by the universal property of the fiber product.
In particular, if $s \in S$, then the fiber G_s is a group scheme$_{/\kappa(s)}$.

Definition 3.3 (Subgroup schemes).
Let G be a group scheme$_{/S}$. A subscheme (resp. an open subscheme, resp. a closed subscheme) $H \hookrightarrow G$ is called *subgroup scheme*$_{/S}$ (resp. *open subgroup scheme*$_{/S}$, resp. *closed subgroup scheme*$_{/S}$) if $H(T) \leq G(T)$ is a subgroup for any scheme$_{/S}$ T. A subgroup scheme $H \hookrightarrow G$ is said to be *normal* in G if $H(T)$ is a normal subgroup of $G(T)$ for every scheme$_{/S}$ T.

Definition 3.4 (Kernel).
The *kernel* of a homomorphism $G \xrightarrow{f} G'$ of group schemes$_{/S}$ is a tuple $(\ker f, j)$ consisting of a scheme$_{/S}$ $\ker f$ representing the functor $\mathsf{Sch}^{op}_{/S} \to \mathsf{Set}, T \mapsto \ker(G(T) \to G'(T))$, and the morphism $j : \ker f \to G$ corresponding to the transformation that is determined by the inclusions $\ker(G(T) \to G'(T)) \hookrightarrow G(T)$.
More explicitly, $\ker f$ is given as the base change of f along $e : S \to G'$, i.e.

$$\begin{tikzcd}
\ker f \arrow[r, "j"] \arrow[d] \arrow[dr, phantom, "\lrcorner", very near start] & G \arrow[d, "f"] \\
S \arrow[r, "e"] & G'
\end{tikzcd}$$

is a cartesian diagram: $(S\times_{G'}G)(T) \cong S(T)\times_{G'(T)}G(T) = \{(0,g) \in 0\times G \mid f(g) = 0\} \cong \ker(G(T) \xrightarrow{f} G'(T))$, naturally in T.

Definition 3.5 ($[n]$and n-torsion).
If G is a group scheme$_{/S}$ and $n \in \mathbb{Z}$ is an integer we denote by $G \xrightarrow{[n]_G} G$ the morphism corresponding to the transformation with components $G(T) \to G(T), g \mapsto g^n$. $[n]_G$ factors as:

$$\begin{tikzcd}
G \arrow[rr, "{[n]_G}"] \arrow[dr, "\Delta^n"'] & & G \\
& G^n \arrow[ur, "m^n"'] &
\end{tikzcd}$$

Here m^n is the morphism$_{/S}$ corresponding to the transformation with components $G^n(T) \to G(T), (g_1, ..., g_n) \mapsto g_1 \cdot ... \cdot g_n$ and Δ^n is the unique morphism$_{/S}$ such that $\mathrm{pr}_k \circ \Delta^n = \mathrm{id}_G$ for all k if $n > 0$ and the unique morphism$_{/S}$ such that $\mathrm{pr}_k \circ \Delta^n = i_G$ for all k if $n < 0$ denoting by $G^n \xrightarrow{\mathrm{pr}_i} G$ the canonical projection to the i-th factor.
If G is commutative, one calls $[n]_G$ *multiplication by n*. In this case $[n]_G$ is a homomorphism$_{/S}$, as $g \mapsto g^n$ is a homomorphism of groups and $G[n] \overset{\text{def}}{=} \ker[n]_G$ is called the *n-torsion of G*.

Example 3.6 (Multiplicative group).
We denote by $\mathbb{G}_{m,S}$ the group scheme$_{/S}$ representing the functor $\mathsf{Sch}^{op}_{/S} \to \mathsf{Set}, T \mapsto \Gamma(T, \mathcal{O}_T)^\times$, i.e. the composition of the forgetful functor $\mathsf{Grp} \to \mathsf{Set}$ with the unit group functor $\mathsf{CRng} \to \mathsf{Grp}$ and the global section functor $\mathsf{Sch}^{op}_{/S} \to \mathsf{CRng}$.

$\mathbb{G}_{m,S}$ is given more explicitly as the base change $\mathbb{G}_{m,\mathbb{Z}} \times S$, where $\mathbb{G}_{m,\mathbb{Z}} \overset{\text{def}}{=} \operatorname{Spec} \mathbb{Z}[X^{\pm 1}]$.
Indeed, for an arbitrary scheme T one has

$$\mathbb{G}_{m,\mathbb{Z}}(T) \cong \mathsf{CRng}(\mathbb{Z}[X^{\pm 1}], \Gamma_T) \cong \{\varphi \in \mathsf{CRng}(\mathbb{Z}[X], \Gamma_T) \mid \varphi(X) \in \Gamma_T^\times\} \cong \Gamma_T^\times$$

hence by the universal property of the base change

$$(\mathbb{G}_{m,S})_{/S}(T) \cong \mathbb{G}_{m,\mathbb{Z}}(T) \times S_{/S}(T) \cong \mathbb{G}_{m,\mathbb{Z}}(T) \cong \Gamma_T^\times.$$

The claim thus follows by Yoneda, as both computations are natural in the variable T.

Group schemes$_{/S}$

Lemma 3.7.

(i) If $Y \xrightarrow{f} X$ is a morphism of schemes and $X \xrightarrow{s} Y$ is a section of f, then s is an embedding. If f is separated, s is a closed embedding.

(ii) If $X \xrightarrow{s} Y$ is a section of $Y \xrightarrow{f} X$ as in (i), then s maps closed points to closed points.

Proof.

(i) The diagram

$$\begin{tikzcd} X \arrow[r, "s"] \arrow[d, "s"'] \arrow[dr, phantom, "\lrcorner", very near start] & Y \arrow[d, "\Delta_f"] \\ Y \arrow[r, "(\mathrm{id}\times s\circ f)"'] & Y\times_X Y \end{tikzcd}$$

is cartesian, as the following computation on T-valued points shows: $(Y \times_{(Y\times_X Y)} Y)(T) = \{(y,y') \in Y(T)\times Y(T) \mid (y, s(f(y))) = (y',y')\} \cong \{y \in Y(T) \mid s(f(y)) = y\} \cong X(T)$ where the last bijection is given via $y \longmapsto f(y)$ with inverse $x \longmapsto s(x)$, naturally in T.

(ii) Let x be a closed point of X. Consider the following commutative diagram:

$$\begin{tikzcd} \{x\} \arrow[r, hook] \arrow[dr, dashed, "\exists! s_|"'] \arrow[ddr, bend right, "\mathrm{id}"'] & X \arrow[dr, bend left, "s"] & \\ & f^{-1}(x) \arrow[r, hook, "cl."] \arrow[d, "f_|"'] \arrow[dr, phantom, "\lrcorner", very near start] & Y \arrow[d, "f"] \\ & \{x\} \arrow[r, hook, "cl."] & X \end{tikzcd}$$

As $f_| \circ s_| = \mathrm{id}$, $s_|$ is a section of $f_|$. Furthermore, $f^{-1}(x) \hookrightarrow Y$ is a closed embedding as base change of a closed embedding. We thus only need to show that $s_|(x)$ is closed in $f^{-1}(x)$.

Because being closed is a local property, it suffices to show that $s_|(x)$ is closed in every *affine* open $U \subseteq f^{-1}(x)$ that contains $s_|(x)$. $s_|$ will factorize over $U \hookrightarrow f^{-1}(x)$ as $s_|(x) \in U$. We henceforth may assume $f^{-1}(x)$ to be affine. In this case $f^{-1}(x) \xrightarrow{f_|} \{x\}$ is a morphism between affine schemes, hence is separated. Therefore $s_|$ is a closed embedding by (i), thus $s_|(x)$ is closed in $f^{-1}(x)$ and we are done.

□

Proposition 3.8.

(i) A group scheme$_{/S}$ G is separated if and only if the unit section $S \xrightarrow{e} G$ is a closed embedding.

(ii) If S is a discrete scheme (e.g., $S = \operatorname{Spec} k$ for some field k), then every group scheme$_{/S}$ is separated.

Proof.

(i) If $G \longrightarrow S$ is separated, $S \xrightarrow{e} G$ is a closed embedding by Lemma 3.7(i).
For the other direction we will show that the following diagram is cartesian:

$$\begin{tikzcd} G \arrow[r] \arrow[d, "\Delta_{G/S}"'] \arrow[dr, phantom, "\lrcorner", very near start] & S \arrow[d, hook, "e"] \\ G\times_S G \arrow[r, "m\circ(\mathrm{id}_G\times i)"] & G \end{tikzcd}$$

We compute on points:

$$\begin{aligned}((G \times_S G) \times_G S)(T) &\cong (G(T) \times_{S(T)} G(T)) \times_{G(T)} S(T) \\ &\cong \{(g, g', 0) \in G(T) \times G(T) \times S(T) \mid g \cdot (g')^{-1} = 0\} \\ &\cong \{(g, g) \in G(T) \times G(T) \mid g \in G(T)\} \\ &\cong G(T)\end{aligned} \tag{3.2}$$

naturally in T. Hence $\Delta_{G/S}$ is a closed embedding by base change, so $G \longrightarrow S$ is separated.

(ii) In virtue of (i), it suffices to show that the unit section $S \xrightarrow{e} G$ is a closed embedding. As S is discrete, $G = \bigcup_{s \in S} \pi^{-1}(s)$ is an open cover of G, where we denoted the structure morphism $G \longrightarrow S$ by π. Because being a closed embedding is a property that is local on the target, we are done if we can show that $\{s\} \xrightarrow{e_|} \pi^{-1}(s)$ is a closed embedding $(e^{-1}(\pi^{-1}(s)) = \{s\})$. In fact, $e_|$ is a section of $\pi^{-1}(s) \xrightarrow{\pi_|} \{s\}$. Therefore $e_|$ maps closed points to closed points by Lemma 3.7(ii) and thus indeed is a closed embedding as claimed.

□

Remark 3.9.
If $G \xrightarrow{f} G'$ is a homomorphism of group schemes$_{/S}$, where G' is separated over S, then by 3.8(i) $\ker f$ is a closed subgroup scheme of G, as closed embeddings are stable under base change.

Definition 3.10.
Suppose G is a group scheme$_{/S}$ and $g \in G(T)$ is any T-valued point.
The *right translation* t_g along g (resp. *left translation* ${}_gt$ along g) is the morphism $G_T \longrightarrow G_T$ given on points by $t_g(T') : G_T(T') \to G_T(T'), h \mapsto hg_{T'}$ (resp. ${}_gt(T') : G_T(T') \to G_T(T'), h \mapsto g_{T'}h$) for any scheme$_{/T}$ T', where $T' \xrightarrow{g_{T'}} G_T$ denotes the unique morphism$_{/T}$ depicted in the following diagram

$$\begin{tikzcd}
T' \arrow[r] \arrow[dr, dashed, "g_{T'}", "\exists!"'] \arrow[ddr, bend right] & T \arrow[dr, bend left, "g"] & \\
& G_T \arrow[r, "\mathrm{pr}_G"] \arrow[d, "\mathrm{pr}_T"'] \arrow[dr, phantom, "\lrcorner", very near start] & G \arrow[d] \\
& T \arrow[r] & S
\end{tikzcd}$$

Note that $t_{g'} \circ t_g = t_{gg'}$ and ${}_{g'}t \circ_g t =_{g'g} t$ as these identities certainly hold on points.

Remark 3.11 (Universal translations).
Choosing $G = T, g = \mathrm{id}_G \in G(G)$ in Definition 3.10 above, one obtains the so called *universal (right/left) translation* $G \times_S G \overset{\tau}{\underset{\tau'}{\rightrightarrows}} G \times_S G$ given on points by $(g_1, g_2) \xmapsto{\tau} (g_1 g_2, g_2)$ and $(g_1, g_2) \xmapsto{\tau'} (g_2 g_1, g_2)$ respectively.
τ, τ' are *universal* in the sense that given any T-valued point $g \in G(T)$ one has that t_g (resp. ${}_gt$) is given as the base change of τ (resp. τ') along $G_T = G \times_S T \xrightarrow{\mathrm{id}_G \times g} G \times_S G$, i.e. the diagram

$$\begin{tikzcd}
G_T \arrow[r] \arrow[d, "t_g"'] \arrow[dr, phantom, "\lrcorner", very near start] & G \times_S G \arrow[d, "\tau"'] \\
G_T \arrow[r, "\mathrm{id}_G \times g"] & G \times_S G
\end{tikzcd}$$

is cartesian by the Yoneda lemma as follows:

We have the functor $F : \mathsf{Sch}_{/S}^{op} \to \mathsf{Set}$ given on objects by $F(T \to S) \overset{\text{def}}{=} \mathsf{Sch}_{/T}(G_T, G_T)$ and on a morphism $T' \xrightarrow{f} T$ by the following diagram:

$$\begin{tikzcd}
G \times_S T' \arrow[r] \arrow[d, "f^*(g)"'] \arrow[dr, phantom, "\lrcorner", very near start] & G \times_S T \arrow[d, "g"] \\
G \times_S T' \arrow[r, "\mathrm{id}_G \times f"] & G \times_S T
\end{tikzcd}$$

where we wrote $f^* \overset{\text{def}}{=} F(f)$. The construction of Definition 3.10 now yields a natural transformation $t : G(\cdot) \to F$ with components $t_T(g) \overset{\text{def}}{=} t_g \in \mathsf{Sch}_{/T}(G_T, G_T)$, and the explicit bijection from the Yoneda lemma states that in this situation one has

$$t_g = t_T(g) = F(g)(\underbrace{t_G(\mathrm{id}_G)}_{=\tau}) = F(g)(\tau) = g^*(\tau)$$

as claimed. A similar argument shows the analogous statement about τ'.

We now show how one can apply translation morphisms to transport local information on a group scheme from one point to another.
For this, let $G \xrightarrow{\pi} S$ be a group scheme with unit section $S \xrightarrow{e} G$. We write $\omega_{G/S} \overset{\text{def}}{=} e^*\Omega^1_{G/S}$, where $\Omega^1_{G/S}$ denotes the sheaf of relative *Kähler differentials.*

Proposition 3.12.
Let $G \xrightarrow{\pi} S$ be a group scheme. Then there is a canonical isomorphism $\pi^*\omega_{G/S} \xrightarrow{\sim} \Omega^1_{G/S}$.

Proof. View $G \times_S G$ as a group scheme$_{/G}$ via the projection pr_2 onto the second factor. Then the universal translation τ is an automorphism of $G \times_S G$ over G, so that there is a natural isomorphism (see for example [Stacks, 01UV])

$$\tau^*\Omega^1_{G\times_S G/G} \xrightarrow{\sim} \Omega^1_{G\times_S G/G} \tag{3.3}$$

As $G \times_S G_{/G}$ is the pullback of $G_{/S}$ along pr_1, one furthermore has that $\Omega^1_{G\times_S G/G} \cong \mathrm{pr}_1^* \Omega^1_{G/S}$ as sheaves of differentials behave well with respect to base change.
Using $\tau = m \times_S \mathrm{pr}_2$ we can rewrite (3.3) as

$$m^*\Omega^1_{G/S} \xrightarrow{\sim} \mathrm{pr}_1^* \Omega^1_{G/S} .$$

Pulling back along $G \xrightarrow{(e\circ\pi)\times_S \mathrm{id}_G} G \times_S G$ results in the isomorphism

$$\Omega^1_{G/S} \xrightarrow{\sim} \pi^* e^* \Omega^1_{G/S} = \pi^*\omega_{G/S}$$

as claimed. □

Group schemes$_{/k}$

We conclude this introduction to the theory of group schemes by giving special emphasis to the case $S = \operatorname{Spec} k$ for a field k.

The following lemma is another example of how one can use the group structure to *transport* (local) properties of points on a group scheme to each other:

Lemma 3.13.
Let G be a locally of finite type group scheme$_{/k}$. Then G is *equidimensional* and $\dim G = \dim_g G$ for any $g \in G$.

Proof. We first show that $\dim_g G = \dim_{g'} G$ for any $g, g' \in G$. Using the fact that $\dim_{g_K} G_K = \dim_g G$ for any field extension $K \mid k$ and any point g_K lying above g we may assume g and g' to be k-rational. In this case $t_{g^{-1}g'}$ is an automorphism$_{/k}$ with $g \longmapsto g'$; so $\dim_g G = \dim_{g'} G$ in particular.
Observing $\dim G \overset{\text{def}}{=} \sup_{g \in G} \dim_g G$ thus concludes the proof.
A slightly enhanced version of this statement can be found in [Stacks, 045X]. □

Another useful result on group schemes$_{/k}$ is given in the following

Lemma 3.14.
Let G be a group scheme$_{/k}$ where k denotes a *perfect* field. Then the reduced underlying scheme $G_{\text{red}} \hookrightarrow G$ is a closed subgroup scheme.

Proof. We will use the characterization of group schemes in terms of explicit morphisms at the level of schemes$_{/k}$. This way, a group scheme is given by three morphisms m, i and e making certain natural diagrams commutative. As $(\cdot)_{\text{red}}$ is a functor, it induces morphisms on the reduced underlying closed subscheme and sends commutative diagrams to commutative diagrams.
Note that the universal property of the reduction implies that $(\cdot)_{\text{red}}$ is right adjoint to the inclusion functor $\mathsf{Sch}^{\text{red}} \hookrightarrow \mathsf{Sch}$, where $\mathsf{Sch}^{\text{red}}$ denotes the full subcategory of Sch with objects the *reduced* schemes. Hence $(\cdot)_{\text{red}}$ commutes with (fiber) products. As $\mathsf{Sch}^{\text{red}}$ is a *full* subcategory of Sch it suffices to show that the product $G_{\text{red}} \times_k G_{\text{red}}$ in the category of all schemes is itself reduced, to conclude that it is right product in the category of reduced schemes already - i.e. that $(G \times_k G)_{\text{red}} = G_{\text{red}} \times_k G_{\text{red}}$.
It therefore suffices to show that $G_{\text{red}} \times_k G_{\text{red}}$ is reduced to complete the proof in virtue of the functoriality of $(\cdot)_{\text{red}}$. Hence the result follows from the fact that being reduced is equivalent to being *geometrically* reduced for schemes over a *perfect* field k and the fact that the product of geometrically reduced schemes$_{/k}$ stays reduced - see for example [Stacks, 020I] and [Stacks, 035Z].
□

Definition 3.15.
Suppose G is group scheme$_{/k}$. Then G is separated over k by Proposition 3.8(ii) and the image of the identity section consists of a single point $e = e_G$.
If furthermore G is assumed to be locally noetherian, it is locally connected (see for example [Stacks, 04MF]).
We write G^0 for the connected component of G containing e in this case (note that G^0 is open, since G is locally connected (see [Stacks, 04ME])). G^0 is called *identity component* of G and it follows that it is an open subscheme of G.

Proposition 3.16.
Let G be a group scheme, locally of finite type$_{/k}$. The following are equivalent:

(i) G_K is reduced for some *perfect* field $K \mid k$.
(ii) G_K is reduced at the *origin* for some *perfect* field $K \mid k$.
(iii) G is smooth$_{/k}$.
(iv) G^0 is smooth$_{/k}$.
(v) G is smooth$_{/k}$ at the origin.

Proof. That (iii) implies (iv) and (v) and that (i) implies (ii) is trivial.
For (iii) implies (ii) use that smoothness is stable under base change and implies regularity, hence being integral and thus reduced, at stalks.
(v) implies (iii) is an immediate consequence of Proposition 3.12 by observing that $\omega_{G/k}$ is nothing but the *cotangent space* at the identity element and using the characterization of *smoothness* of morphisms via the sheaf of relative Kähler differentials (see for example [Vakil, Theorem 25.2.2]).
(ii) implies (i) follows from the fact that (ii) implies that G is *geometrically* reduced at the origin (compare [Stacks, 020I]), so that one can base change to $\overline{k}$ and then use translation to conclude that G is reduced at all *closed* points and hence reduced at every point as the set of closed points lies very dense in G by Proposition 2.11.
It thus only remains to show that (i) implies (iii).
As (i) implies that G is *geometrically* reduced and as smoothness of schemes *locally of finite type*$_{/k}$ can be checked over arbitrary field extensions (see [GW, Theorem 6.28]), we may assume $k = \overline{k}$ from this point on.
As the set $G(k)$ of closed points of G lies *very dense* in G in this situation according to Proposition 2.11 and as the smooth locus $\mathrm{sm}(G/k)$ of $G_{/k}$ is always open, it suffices to check smoothness at all closed points.
As furthermore k is now *perfect* and as G is a *reduced* scheme locally of finite type$_{/k}$, one knows that the smooth locus sm(G/k) is dense ([GW, Theorem 6.19]) and hence contains a closed point.
We then obtain $G(k) \subseteq \mathrm{sm}(G/k)$ as G is a *homogeneous space* on its closed points $G(k)$ via translation.
Hence $\mathrm{sm}(G/k) = G$ as claimed. □

Proposition 3.17.
Let G be a group scheme, locally of finite type$_{/k}$.
Then G^0 is an open and closed subgroup scheme of G which is *geometrically irreducible* and *of finite type*$_{/k}$. In particular $(G_K)^0 = (G^0)_K$ for any field extension $K \mid k$.

Remark.
A more general result can be found in [AV, (3.17) Proposition] proving that *every* connected component of G as above is *irreducible*.

Proof. One knows that any *connected* scheme$_{/k}$ admitting a k-rational point is geometrically connected (see for example [Stacks, 04KV]). This in particular implies that $(G^0)_K = (G_K)^0$:
Since $(G^0)_K$ is connected and contains the identity it is certainly contained in $(G_K)^0$. But we already know that G^0 is open and closed, hence $(G^0)_K$ is as well, which implies $(G^0)_K = (G_K)^0$ as claimed.
We may thus assume $k = \overline{k}$ from this point on. As k is now a perfect field, we may apply Lemma 3.14 to furthermore assume G^0 to be reduced [note that the underlying topological space does not change when passing to the reduced underlying scheme].
Hence, using Proposition 3.16, we see that G^0 is smooth$_{/k}$, in particular *regular*.
Suppose now that G^0 were reducible. As G^0 is locally connected it follows that all irreducible components of G^0 are *open* as cited in Definition 3.15 already. Hence connectedness of G^0 shows that there exist distinct irreducible components $C_\circ \neq C_\bullet$ with non-empty intersection. Let $g \in C_\circ \cap C_\bullet$. Then $\mathcal{O}_{G,g}$ cannot be an integral domain, as it contains at least two distinct minimal prime ideals. This contradicts the fact that $\mathcal{O}_{G,g}$ is regular hence an integral domain by [Stacks, 00NP]. So G^0 is irreducible as claimed.
It remains to show that G^0 is *quasi-compact*.
Note that, as G^0 is locally of finite type$_{/k}$, the set of closed points of G^0, i.e. $G^0(k)$ as k is algebraically closed, is *very dense* in G^0 (again by Proposition 2.11).
It therefore suffices to show that $G^0(k)$ is quasi-compact in virtue of Lemma 2.12.
Take any non-empty affine open part $U \subseteq G^0$. $U(k)$ lies dense in $G^0(k)$, as $G^0(k)$ is irreducible. Hence for every $g \in G(k)$ one has that $g^{-1}U(k) \cap U(k) \neq \emptyset$. Hence the map $U(k) \times U(k) \longrightarrow G^0(k)$ given by multiplication is *surjective* and *continuous*, so that $G^0(k)$ is quasi-compact as $U(k) \times U(k)$ is [use Lemma 2.12 again]. □

4 Abelian varieties

Let k denote a field and fix an algebraic closure $\bar{k}$ of k.
We still mostly follow [AV]. In the proof of Theorem 4.13, we also took a look at [Mumford, §10] and the proof of the Rigidity lemma 4.3 was taken from [Vakil, Lemma 10.3.12].

Generalities

Definition 4.1 (Abelian variety).
A *group variety*$_{/k}$ is a group scheme$_{/k}$ G, such that G is a variety$_{/k}$.
An *abelian variety*$_{/k}$ is group variety$_{/k}$ that is complete as a variety$_{/k}$.
We obtain the category $\mathsf{AV}_{/k}$ of abelian varieties$_{/k}$ as the full subcategory of $\mathsf{GSch}_{/k}$ with abelian varieties$_{/k}$ as objects.

As immediate consequence of Proposition 3.16 we obtain the following useful

Corollary 4.2.
Any group variety $X \longrightarrow \operatorname{Spec} k$ is smooth$_{/k}$.

Before investigating the nature of *abelian varieties*, we first proof a useful result on general *complete varieties*, which has strong implications on the geometry of *abelian varieties* in particular, the

Rigidity Lemma 4.3.
Let X, Y and Z be varieties$_{/k}$, X complete such that X admits a k-rational point $p \in X(k)$. If $X \times_k Y \xrightarrow{f} Z$ is a morphism such that, for some $q \in Y$, the fiber $X \times_k \{q\} = \mathrm{pr}_Y^{-1}(q)$ is mapped to a single point $r \in Z$, then f factors as

$$\begin{tikzcd}
X \times_k Y \arrow[rr, "f"] \arrow[dr, "\mathrm{pr}_Y"'] & & Z \\
& Y \arrow[ur, dashed, "\exists\varphi"'] &
\end{tikzcd}$$

Proof. Define $X \times_k Y \xrightarrow{g} Z$ by $g(x, y) = f(p, y)$, i.e. $g = f \circ \sigma_p \circ \mathrm{pr}_Y$. Here $Y \xrightarrow{\sigma_p} X \times_k Y$ denotes the pullback of $\operatorname{Spec} k \xrightarrow{p} X$ along $X \times_k Y \xrightarrow{\mathrm{pr}_X} X$, where we identified $Y = Y \times_k k = Y \times_k (X \times_X k) = (Y \times_k X) \times_X k$.
We show that $f = g$, by which we are done via $\varphi \overset{\text{def}}{=} f \circ \sigma_p$:

$$\varphi \circ \mathrm{pr}_Y = f \circ \sigma_p \circ \mathrm{pr}_Y \overset{\text{def}}{=} g = f.$$

As equality of morphisms of schemes$_{/k}$ can be checked after extension of the base field by Proposition 2.9, we may assume $k = \bar{k}$ from here on.
It furthermore suffices to show that equality holds on a non-empty open subset of $X \times_k Y$ by the Reduced-To-Separated theorem 2.6.
Now let $r \in U = \operatorname{Spec} B \subseteq Z$ be an open, affine subscheme of Z. Then $f^{-1}(Z \setminus U)$ is closed in $X \times_k Y$ and hence $A \overset{\text{def}}{=} \mathrm{pr}_Y(f^{-1}(Z \setminus U))$ is closed in Y because X is proper$_{/k}$ and properness is stable under base change. Note that $q \in Y \setminus A$, as $f(X \times_k \{q\}) \subseteq U$.
Let $V \overset{\text{def}}{=} Y \setminus A$. We will prove that $f_{|} \overset{\text{def}}{=} f_{|\mathrm{pr}_Y^{-1}(V)} = g_{|\mathrm{pr}_Y^{-1} V} \overset{\text{def}}{=} g_{|}$. As we are working over an algebraically closed field, it suffices to check equality on all *closed points* of $\mathrm{pr}_Y^{-1}(V)$. Let $y \in V(k)$ be any closed point.
If we show that $f(X \times_k \{y\})$ consists of a single point of Z, we see that

$$f(X \times_k \{y\}) = \{f(p, y)\} \overset{\text{def}}{=} g(X \times_k \{y\})$$

which implies $f_| = g_|$, as $X \times_k \{y\}$ contains all closed points of $\mathrm{pr}_Y^{-1}(V)$ for varying $y \in V(k)$ – note that the closed points of $\mathrm{pr}_Y^{-1}(V)$ are exactly the points $\mathrm{pr}_Y^{-1}(V)(k) = \{(x, y) \in (X \times_k Y)(k) = X(k) \times Y(k) \mid y \in V\}$.
To see that $f(X \times_k \{y\})$ consists of a single point, note that $X \times_k \{y\} \cong X$ is $\mathrm{proper}_{/k}$ and connected, hence $\Gamma_{X\times_k\{y\}} = k$ by Proposition 2.8, so that $f_{|X\times_k\{y\}}$ factors as:

$$\begin{tikzcd}
X \times_k \{y\} \arrow[rr, "f_|"] \arrow[dr] & & U = \operatorname{Spec} B \\
& \underbrace{\operatorname{Spec} k}_{=\operatorname{Spec}\Gamma_{X\times_k\{y\}}} \arrow[ur] &
\end{tikzcd}$$

which concludes the proof. □

As an easy consequence of the Rigidity Lemma 4.3, we see that arbitrary morphisms of $\mathrm{schemes}_{/k}$ between abelian varieties are not very far from being *homomorphisms*:

Proposition 4.4.
Let X and Y be abelian varieties and $f \in \mathsf{Sch}_{/k}(X, Y)$. Then f factors as

$$\begin{tikzcd}
X \arrow[rr, "f"] \arrow[dr, dashed, "\exists! h"'] & & Y \\
& Y \arrow[ur, "t_{f(e_X)}"'] &
\end{tikzcd}$$

where $h \in \mathsf{AV}_{/k}(X, Y)$ is a homomorphism and $t_{f(e_X)}$ is the translation morphism defined in 3.10.

Proof. Set $y \overset{\text{def}}{=} i_Y(f(e_X))$ and let $h \overset{\text{def}}{=} t_y \circ f$ [note that h has to be defined this way, i.e. is unique], so that we have

$$h(e_X) = t_y(f(e_X)) = e_Y.$$

Consider the morphism $X \times_k X \xrightarrow{g} Y$ given on points by $g(x, x') = h(x \cdot x') \cdot h(x')^{-1} \cdot h(x)^{-1}$, i.e. given by

$$X \times_k X \xrightarrow{(h\circ m_X)\times_k(i_Y \circ m_Y \circ (h\times_k h))} Y \times_k Y \xrightarrow{m_Y} Y \ .$$

We then have

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

as one readily checks using the description on points. Hence g factorizes through the first and the second projection $X \times_k X \longrightarrow X$ by the Rigidity lemma 4.3, i.e. g is a map with constant value e_Y.
Evaluation on points shows that $h(x \cdot x') \cdot h(x')^{-1} \cdot h(x)^{-1} = g(x, x') = g(e_X, e_X) = e_Y$, i.e. $h(x \cdot x') = h(x) \cdot h(x')$, so that h is seen to be a $\mathrm{homomorphism}_{/k}$. The calculation

$$t_{f(e_X)} \circ h = t_{f(e_X)} \circ t_{i_Y(f(e_X))} \circ f = t_{e_Y} \circ f = f$$

concludes the proof. □

Corollary 4.5 (*Abelian* varieties are *abelian*).

(i) If X is a variety$_{/k}$ and $e \in X(k)$, then there is at most one way to endow X with the structure of an abelian variety$_{/k}$ such that e is the identity section of X.

(ii) If X is an abelian variety$_{/k}$, then X is commutative as a group scheme$_{/k}$.

Proof.

(i) If (X, m, i, e) and (X, m', i', e) are abelian varieties, then m and m' certainly equal on $X \times_k \{e\}$ and $\{e\} \times_k X$. As $m \circ (m \times_k i \circ m')$ is constant on $X \times_k \{e\}$ and $\{e\} \times_k X$, we see that $m \circ (m \times_k i \circ m')$ is constant with value e according to the Rigidity Lemma 4.3. Hence $m = m'$, which readily implies $i = i'$ as well.

(ii) As $i(e_X) = e_X$, Proposition 4.4 states that i is a homomorphism, which implies that the group structure is abelian.

□

Given the fact, that abelian varieties are commutative we shall introduce the

Notation.
$x + y \overset{\text{def}}{=} m(x, y) = m \circ (x \times y)$, $-x \overset{\text{def}}{=} i(x)$ and $0 \overset{\text{def}}{=} e$, where $x, y \in X(T)$ are points.
If $f, g \in \mathsf{AV}_{/k}(X, Y)$, then $f + g \overset{\text{def}}{=} m_Y \circ (f \times g) \in \mathsf{AV}_{/k}(X, Y)$, $-f \overset{\text{def}}{=} f \circ i_X \underset{3.2}{=} i_Y \circ f \in \mathsf{AV}_{/k}(X, Y)$.

Remark 4.6.
These constructions endow $\mathsf{AV}_{/k}(X, Y)$ with the structure of an abelian group.
Note that $\mathsf{Sch}_{/k}(X, Y) \overset{\text{def}}{=} Y(X)$ carries the structure of an abstract group by definition and that $\mathsf{AV}_{/k}(X, Y) \leq \mathsf{Sch}_{/k}(X, Y)$ is the subgroup of morphisms $X \xrightarrow{f} Y$ satisfying $f(e_X) = e_Y$ according to Proposition 4.4. One has $\mathsf{Sch}_{/k}(X, Y) \cong \mathsf{AV}_{/k}(X, Y) \times Y(k)$ as abstract groups, again in virtue of Proposition 4.4.

As it will become important when studying *endomorphisms* of abelian varieties later on, we will prove the following

Proposition 4.7.
Let $f \in \mathsf{AV}_{/k}(X, Y)$ be a homomorphism of abelian varieties$_{/k}$. Then the (scheme-theoretic) image of f is an abelian variety$_{/k}$ again.

Proof. Define $Z \hookrightarrow Y$ to be the *scheme-theoretic image* of f. As every morphism of schemes between abelian varieties$_{/k}$ is proper, f is *universally closed*, so that Z is nothing but the closed subset $f(X)$ equipped with the unique reduced scheme-structure induced by Y. Hence Z is seen to be a finite type, separated, integral and closed subscheme of Y, i.e. a proper subvariety of Y.

We show that Z is a subgroup scheme$_{/k}$, for which it suffices to show that $Z \times Z \xrightarrow{m_|} Y$ factorizes over Z. Hence Lemma 2.10 implies that we may assume $k = \bar{k}$ from this point on. Note that Z behaves well with respect to base extension, i.e. the scheme-theoretic image of f_K is given by Z_K, as we are base changing along a *flat* morphism [Stacks, 081I]. As $(Z \times Z)(k) = Z(k) \times Z(k)$ is very dense in $Z \times Z$ by Proposition 2.11, it suffices to show that m carries $Z(k) \times Z(k)$ into Z by continuity of m. But this follows from f being a *homomorphism* and the fact that $Z(k) = f(X(k))$: given $z_\circ = f(x_\circ)$ and $z_\bullet = f(x_\bullet)$ in $Z(k)$, one simply has $z_\circ \cdot z_\bullet = f(x_\circ) \cdot f(x_\bullet) = f(x_\circ \cdot x_\bullet) \in f(X(k)) = Z(k) \subseteq Z$.
We thus see that Z is a subgroup scheme$_{/k}$ when k does not necessarily equal $\bar{k}$ already. It follows that Z is *geometrically* irreducible in virtue of Proposition 3.17 and *geometrically* reduced in virtue of Proposition 3.16.
We therefore conclude that Z is a *proper subgroup-variety*, i.e. an abelian subvariety, of Y as claimed. □

We finish the section on generalities of the theory of abelian varieties with the following crucial

Theorem 4.8.
Let X be an abelian variety$_{/k}$. If $Y \hookrightarrow X$ is a closed subgroup scheme, then the connected component $Y^0 \subseteq Y$ is an open and closed subgroup scheme of Y that is geometrically irreducible. The reduced underlying scheme $Y^0_{\text{red}} \hookrightarrow X$ is an abelian subvariety of X.

Proof. We will restrict ourselves to explaining the strategy of the proof; a complete proof is presented in [AV, (5.31) Proposition]. $Y^0 \subseteq Y$ is an open, closed and geometrically irreducible subgroup scheme by Proposition 3.17(i).
One proves that Y^0_{red} is *geometrically reduced*. The result then follows:
Indeed, as is explained in the proof of Lemma 3.14 it suffices to see that $Y^0_{\text{red}} \times_k Y^0_{\text{red}}$ is itself reduced. Hence we conclude that Y^0_{red} is a closed subgroup scheme as the product of geometrically reduced schemes is reduced - again: [Stacks, 035Z].
Now Y^0_{red} is seen to be a *geometrically integral* subgroup scheme of X, hence an abelian subvariety.
One proves that Y^0_{red} is geometrically reduced for char $k = 0$ and char $k = p > 0$ separately. When char $k = 0$ one uses *Cartier's theorem* [AV, (3.20) Theorem], which states that group schemes locally of finite type over a field k of characteristic 0 are reduced, to conclude that Y is reduced. Since k is perfect, this implies that Y is smooth$_{/k}$ (see for example [Vakil, 12.2.10 Smoothness-Regularity Comparison Theorem]), hence Y^0 is smooth$_{/k}$ as well by Proposition 3.17$(ii)(c)$ and thus reduced by 3.17$(ii)(a)$.
The argument for k a field of positive characteristic is slightly more involved and is based on the fact that the p^n-torsion $\{X[p^n]\}_{n\in\mathbb{N}}$ of an abelian variety X lies (scheme-theoretically) *dense* in X. □

Line bundles on abelian varieties (I)

Recall that given any scheme X, the isomorphism classes of line bundles $\mathcal{L}$ on X form an abelian group Pic X, the so called *Picard group* of X.
The group operation is given by $([\mathcal{L}_\circ], [\mathcal{L}_\bullet]) \mapsto [\mathcal{L}_\circ \otimes \mathcal{L}_\bullet]$, the neutral element is $[\mathcal{O}_X]$ and the inverse of $[\mathcal{L}]$ is given by $[\mathcal{L}^\vee]$ where $\mathcal{L}^\vee \overset{\text{def}}{=} \mathcal{H}om_{\mathcal{O}_X}(\mathcal{L}, \mathcal{O}_X)$ is the *dual* of $\mathcal{L}$.
Even better, this construction yields a functor $\operatorname{Pic} : \mathsf{Sch}^{op} \longrightarrow \mathsf{Ab}$ via

$$(X \to Y) \mapsto ([\mathcal{L}]_Y \mapsto [(X \to Y)^* \mathcal{L}]_X)$$

In order to state some of the following results more concisely, we start this section by introducing the following

Notation 4.9.

(i) Suppose X, Y and Z are schemes$_{/S}$, $Z \xrightarrow{i} Y$ is a morphism$_{/S}$ and $\mathcal{L}$ is a line bundle on $X \times_S Y$.
Then we will call $\mathcal{L}$ *trivial along* i if $(\mathrm{id}_X \times_S i)^* \mathcal{L} \cong \mathrm{pr}_Z^* \mathcal{L}'$ for a line bundle $\mathcal{L}'$ on Z.
If $Y_0 \hookrightarrow Y$ is a subscheme, we will say that $\mathcal{L}$ is *trivial on* Y_0, if it is trivial along $Y_0 \hookrightarrow Y$ and similarly for subschemes $X_0 \hookrightarrow X$.

(ii) If X is an abelian variety$_{/k}$, $n \in \mathbb{N}$ and $I = \{i_1, ..., i_k\} \subseteq \{1, ..., n\}$, then we write $p_I \overset{\text{def}}{=} p_{i_1,...,i_k} \overset{\text{def}}{=} X^n \longrightarrow X$ for the morphism given on points by $(x_1, ..., x_n) \longmapsto x_{i_1} + ... + x_{i_k}$.

(iii) If X is a scheme$_{/S}$, $\mathcal{L}$ is a line bundle on X and $S' \longrightarrow S$ is any morphism, we denote by $\mathcal{L}_{S'}$ the pullback of $\mathcal{L}$ along the projection $X_{S'} \longrightarrow X$.

We will use the following theorem without proof:

Fact 4.10.
Let X be a complete variety$_{/k}$, let Y be a scheme$_{/k}$ and let $\mathcal{L}$ be a line bundle on $X \times_k Y$. Then there exists a *closed* subscheme $Y_0 \hookrightarrow Y$ which is the maximal subscheme of Y, over which $\mathcal{L}$ is trivial:

(i) $\mathcal{L}_{|X\times Y_0} = \mathrm{pr}_{Y_0}^* \mathcal{L}_0$ for a line bundle $\mathcal{L}_0$ on Y_0.

(ii) if $Z \xrightarrow{\varphi} Y$ is any morphism such that $\mathcal{L}$ is trivial along φ, then φ factors through $Y_0 \hookrightarrow Y$.

Proof. [AV, (2.4) Proposition], which in turn references [Mumford, §10]. □

Lemma 4.11.
Let X be a geometrically integral, proper scheme$_{/k}$ and $\mathcal{L}$ a line bundle on X. Then $\mathcal{L}$ is trivial if and only if $\Gamma(X, \mathcal{L}) \neq 0 \neq \Gamma(X, \mathcal{L}^\vee)$.

Proof. If $\mathcal{L}$ is trivial we have that $\Gamma(X, \mathcal{L}) \cong \Gamma_X \cong \Gamma(X, \mathcal{L}^\vee)$ and $\Gamma_X \neq 0$, as $X \neq \emptyset$.
Suppose now that there exist nontrivial sections $\Gamma(X, \mathcal{L}) \ni s \neq 0 \neq s^\vee \in \Gamma(X, \mathcal{L}^\vee)$. These sections induce morphisms $\mathcal{O}_X \xrightarrow{s} \mathcal{L}$ and $\mathcal{L} \xrightarrow{s^\vee} \mathcal{O}_X$, both of which are non-zero. Hence the composition $\mathcal{O}_X \xrightarrow{s} \mathcal{L} \xrightarrow{s^\vee} \mathcal{O}_X$ is a non-zero endomorphism: As $s \neq 0 \neq s^\vee$ we have that $s_\eta \neq 0 \neq s^\vee_\eta$, where η denotes the generic point of X. Hence $s^\vee_\eta \circ s_\eta \neq 0$ as a composition of two non-zero homomorphisms of vector spaces$_{/\kappa(X)}$.

Suppose that $\mathcal{O}_X \xrightarrow{s} \mathcal{L} \xrightarrow{s^\vee} \mathcal{O}_X$ is an isomorphism. Then the induced map $\mathcal{O}_x \xrightarrow{s} \mathcal{L}_x$ on stalks is certainly injective. The $\kappa(x)$-linear map $\kappa(x) \xrightarrow{s} \mathcal{L}(x) \xrightarrow{s^\vee} \kappa(x)$ induced on *fibers* is an isomorphism as well, hence $\kappa(x) \xrightarrow{s} \mathcal{L}(x)$ is *injective*, hence also *surjective* as $\dim_{\kappa(x)} \mathcal{L}(x) = 1$. It follows that $\mathcal{O}_x \xrightarrow{s_x} \mathcal{L}_x$ is *surjective on stalks* already by Nakayama, hence an isomorphism as claimed.
It thus suffices to show that $\mathcal{O}_X \xrightarrow{s} \mathcal{L} \xrightarrow{s^\vee} \mathcal{O}_X$ is an isomorphism.
To see this first note that it suffices to check this in the case where $k = \bar{k}$ is algebraically closed:
As $\operatorname{Spec} \bar{k} \longrightarrow \operatorname{Spec} k$ is faithfully flat, so is $X_{\bar{k}} \xrightarrow{\mathrm{pr}} X$ by base change. Hence pulling back quasi-coherent sheaves along pr is *faithful* and *conservative* as shown in Corollary 2.5, in particular pulling back non-trivial morphisms results in non-trivial morphisms.
When $k = \bar{k}$, one knows $\Gamma(X, \mathcal{O}_X) = k$ by Proposition 2.8, so that any non-trivial endomorphism $\mathcal{O}_X \longrightarrow \mathcal{O}_X$ is given via multiplication with an element $\lambda \in k^\times$, i.e. is an isomorphism.
Thus $s^\vee \circ s$ is an isomorphism, which concludes the proof. □

Corollary 4.12.
Let X be a geometrically integral, proper scheme$_{/k}$, $\mathcal{L}$ a line bundle on X and $K \mid k$ any field extension. Then $\mathcal{L}$ is trivial if and only if $\mathcal{L}_K$ is trivial.

Proof. If $\Gamma(X_K, \mathcal{L}_K) \neq 0 \neq \Gamma(X_K, \mathcal{L}_K^\vee)$, then certainly $\Gamma(X, \mathcal{L}) \neq 0 \neq \Gamma(X, \mathcal{L}^\vee)$ by identifying sections of $\mathcal{L}$ with morphisms $\mathcal{O}_X \longrightarrow \mathcal{L}$ and in virtue of the faithfulness of the functor $(X_K \xrightarrow{\mathrm{pr}} X)^* : \mathsf{QCoh}(X) \longrightarrow \mathsf{QCoh}(X_K)$ as described in Corollary 2.5. The result is thus an immediate consequence of Lemma 4.11. □

The following theorem is a rather technical, but very important general result on complete varieties. Its importance will become clear later on, when we will be able to put its immediate corollaries to full use.

Theorem 4.13.
Let X,Y and Z be complete varieties$_{/k}$. Take points $x \in X, y \in Y, z \in Z$. If $\mathcal{L}$ is a line bundle on $X \times Y \times Z$ such that the restrictions $\mathcal{L}_{|\{x\}\times Y \times Z}$, $\mathcal{L}_{|X \times \{y\} \times Z}$ and $\mathcal{L}_{|X\times Y \times \{z\}}$ are all trivial, then $\mathcal{L}$ is trivial.

Proof. We first reduce to the case where x, y and z are k-rational points [i.e. $x \in X(k), y \in Y(k), z \in Z(k)$]:
As $X \times Y \times Z$ is again a complete variety$_{/k}$, $\mathcal{L}$ is trivial on $X \times Y \times Z$ if and only if $\mathcal{L}' \overset{\text{def}}{=} \mathcal{L}_K$ is trivial on $(X \times_k Y \times_k Z)_K = X_K \times_K Y_K \times_K Z_K$ for any field extension $K \,|\, \kappa(x), \kappa(y), \kappa(z) \,|\, k$ in virtue of Corollary 4.12.
We obtain a K-rational point x' of X_K by the following commutative diagram:

$$\begin{tikzcd}
\operatorname{Spec} K \arrow[rrd, bend left] \arrow[rd, dashed, "\exists!"] \arrow[rdd, dashed, "x'"'] \arrow[rddd, bend right, "\mathrm{id}"'] & & \\
& \{x\}_K \arrow[r] \arrow[d, "x_K"'] \arrow[rd, phantom, "\lrcorner"] & \{x\} \arrow[d, "x"] \\
& X_K \arrow[r] \arrow[d] \arrow[rd, phantom, "\lrcorner"] & X \arrow[d] \\
& \operatorname{Spec} K \arrow[r] & \operatorname{Spec} k
\end{tikzcd}$$

and similarly for y' and z'. We claim that $\mathcal{L}'_{|\{x'\}\times Y_K \times Z_K}$, $\mathcal{L}'_{|X_K \times \{y'\} \times Z_K}$ and $\mathcal{L}'_{|X_K \times Y_K \times \{z'\}}$ are all trivial again, which will conclude the reduction to k-rational points x, y and z.
We will show this only for x', as the proof for y' and z' is entirely analogous. We know that

$$\mathcal{L}'_{|\{x'\}\times Y_K \times Z_K} = (x' \times \mathrm{id}_{Y_K \times Z_K})^* \operatorname{pr}^*_{X\times Y\times Z} \mathcal{L} = (\operatorname{pr}_{X\times Y \times Z} \circ (x' \times \mathrm{id}_{Y_K \times Z_K}))^* \mathcal{L}$$

where $\operatorname{pr}_{X\times Y \times Z}$ denotes the natural projection $X_K \times Y_K \times Z_K \longrightarrow X \times Y \times Z$.
A fairly straightforward diagram chase shows that

$$x' \times \mathrm{id}_{Y_K \times Z_K} \circ \operatorname{pr}_{X \times Y \times Z} = x \circ \varphi \times \operatorname{pr}_{Y\times Z}$$

where $\operatorname{pr}_{Y\times Z}$ is the natural projection $Y_K \times Z_K \longrightarrow Y \times Z$ and where φ denotes the natural morphism $\operatorname{Spec} K \longrightarrow \{x\}$.
We therefore obtain that

$$\mathcal{L}'_{|\{x'\}\times Y_K \times Z_K} = (x \circ \varphi \times \operatorname{pr}_{Y\times Z})^* \mathcal{L} = ((x \times \mathrm{id}_{Y \times Z}) \circ (\varphi \times \operatorname{pr}_{Y \times Z}))^* \mathcal{L} = (\varphi \times \operatorname{pr}_{Y\times Z})^* \underbrace{(x \times \mathrm{id}_{Y\times Z})^* \mathcal{L}}_{=\mathcal{L}_{|\{x\}\times Y \times Z}}$$

is trivial as a pullback of the trivial bundle $\mathcal{L}_{|\{x\}\times Y \times Z}$.
Hence we may now assume x, y and z to be k-rational points. We can view $\mathcal{L}$ as a family of line bundles on $X \times Y$ via the projection $X \times Y \times Z \xrightarrow{\text{pr}} Z$. Let Z' be the maximal closed subscheme of Z over which $\mathcal{L}$ is trivial as in Theorem 4.10. Then $z \in Z'$: $(\mathrm{id}_{X\times Y} \times z)^* \mathcal{L} = \mathcal{L}|_{X \times Y \times \{z\}}$ is trivial by assumption, hence $\operatorname{Spec} k \xrightarrow{z} Z$ factors through Z' by the universal property of Z' (here we use that z is k-rational). We will show that $Z = Z'$ by showing that Z' is an open subscheme of Z (here we use that Z is connected). Let $\zeta \in Z'$ be any point of Z'. Set $\mathcal{O}_\zeta \overset{\text{def}}{=} \mathcal{O}_{Z,\zeta}$ and $\mathcal{O}'_\zeta \overset{\text{def}}{=} \mathcal{O}_{Z',\zeta}$ to simplify notation. We then know that $\mathcal{O}'_\zeta = \mathcal{O}_\zeta / I_\zeta$ for some ideal I_ζ of $\mathcal{O}_\zeta$. Since Z is locally noetherian, it suffices to show that $I_\zeta = 0$:
Choose some affine open $\zeta \in \operatorname{Spec} A \subseteq Z$ with A noetherian and ζ corresponding to the prime ideal $\mathfrak{p}$ of A. Then $\mathcal{O}_\zeta = A_\mathfrak{p}$ and Z' locally looks like A/I for some ideal I of A. $I_\zeta = 0$ translates to the fact that the localized ideal $I_\mathfrak{p}$ is zero. Since A is noetherian, $I = (f_1, ..., f_n)_A$ is finitely generated.
$I_\mathfrak{p} = 0$ means that for every $i \in I$ there exists an $x \in A \setminus \mathfrak{p}$ such that $x \cdot i = 0$. There in particular exist elements $x_1, ..., x_n \in A \setminus \mathfrak{p}$ such that $x_i \cdot f_i = 0$. Then for $x \overset{\text{def}}{=} \prod_i x_i \in A \setminus \mathfrak{p}$, it readily follows that $I_x = 0$. Hence $\operatorname{Spec}(A_x / I_x) = \operatorname{Spec} A_x$ is an open subscheme of Z contained in Z' containing ζ.
We have reduced the problem to showing that $I_\zeta = 0$.

Since Z is locally noetherian, we obtain that $\bigcap_n \mathfrak{m}_\zeta^n = 0$ by Krull's intersection theorem. If I_ζ were not zero, we would therefore find a positive integer $n \in \mathbb{N}$ such that $I_\zeta \subseteq \mathfrak{m}^n$ but $I_\zeta \not\subseteq \mathfrak{m}^{n+1}$. Put $\mathfrak{a}_0 \overset{\text{def}}{=} I_\zeta$, $\mathfrak{a}_1 \overset{\text{def}}{=} (I_\zeta, \mathfrak{m}^{n+1})$ and choose some ideal $\mathfrak{a}_2$ satisfying

$$\mathfrak{m}^{n+1} \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_1 \text{ and } \dim_{\kappa(\zeta)} \mathfrak{a}_1 / \mathfrak{a}_2 = 1$$

so that $\mathfrak{a}_1 = (\mathfrak{a}_2, r)$ for some element $r \in \mathcal{O}_\zeta$. Let $Z_i \overset{\text{def}}{=} \operatorname{Spec} \mathcal{O}_\zeta / \mathfrak{a}_i$ and $\mathcal{L}_i \overset{\text{def}}{=} \mathcal{L}_{|X\times Y\times Z_i}$ for $i \in \{0,1,2\}$ respectively (i.e. $\mathcal{O}_{Z_0} = \mathcal{O}'_\zeta$ and $\mathcal{L}_i = (\mathrm{id}_{X\times Y} \times (Z_i \longrightarrow Z))^* \mathcal{L}$).

We will show that $\mathcal{L}_2$ is trivial. We may assume $\zeta \in Z(k)$ again, as $\mathcal{L}_2$ is trivial if and only if $(\mathcal{L}_2)_{\kappa(\zeta)}$ is. $\mathcal{L}_1$ is trivial by construction - choose any trivializing global section $s \in \Gamma(\mathcal{L}_1)$. The inclusion $Z_1 \hookrightarrow Z_2$ induces a restriction $\Gamma(\mathcal{L}_2) \xrightarrow{\text{res}} \Gamma(\mathcal{L}_1)$ (note that Z_0, Z_1 and Z_2 share the same underlying topological space $\{\zeta\}$). Then $\mathcal{L}_2$ is trivial if and only if s lifts to a section $s' \in \Gamma(\mathcal{L}_2)$:

If we have a lift s' of s, then $s'(P) = 0$ for some point $P \in |Z_i|$ implies $s(P) = 0$, which would contradict the fact that s trivializes $\mathcal{L}_1$. Hence s' has no zeros, and thus trivializes $\mathcal{L}_2$ (since $\mathcal{L}_2$ is locally free of rank 1).

If on the other hand $\mathcal{L}_2$ is trivial, the restriction map is given by $\Gamma(\mathcal{O}_{Z_2}) \xrightarrow{\text{res}} \Gamma(\mathcal{O}_{Z_1})$ which is surjective.

We have hence reduced the problem to lifting global sections, i.e. to calculating cohomology:

We have an exact sequence

$$0 \longrightarrow \mathcal{O}_{Z_0} \xrightarrow{\cdot r} \mathcal{O}_{Z_2} \xrightarrow{\text{res}} \mathcal{O}_{Z_1} \longrightarrow 0$$

on $X \times Y \times \{\zeta\}$, which yields the exact sequence

$$0 \longrightarrow \mathcal{L}_0 \xrightarrow{\cdot r} \mathcal{L}_2 \xrightarrow{\text{res}} \mathcal{L}_1 \longrightarrow 0\ .$$

Hence the obstruction of lifting $s \in \mathrm{H}^0(\mathcal{L}_1) = \Gamma(\mathcal{L}_1)$ to $\Gamma(\mathcal{L}_2)$ is an element $\xi \in \mathrm{H}^1(X\times Y\times\{\zeta\}, \mathcal{O}_{X\times Y\times\{\zeta\}}) = \mathrm{H}^1(X \times Y, \mathcal{O}_{X\times Y})$, where the last equation holds since $\zeta \in Z(k)$. We know that the restrictions of $\mathcal{L}_2$ to $\{x\} \times Y \times Z_2$ and $X \times \{y\} \times Z_2$ are trivial.

Writing $i_1 \overset{\text{def}}{=} \mathrm{id}_X \times y : X \hookrightarrow X \times Y$ and $i_2 \overset{\text{def}}{=} x \times \mathrm{id}_Y : Y \hookrightarrow X \times Y$, this means that ξ is in the kernel of $i_1^* : \mathrm{H}^1(X \times Y, \mathcal{O}_{X\times Y}) \longrightarrow \mathrm{H}^1(X, \mathcal{O}_X)$ and $i_2^* : \mathrm{H}^1(X \times Y) \longrightarrow \mathrm{H}^1(Y, \mathcal{O}_Y)$ (note that we used the k-rationality of x and y to define i_1 and i_2).

As the map $i_1^* \times i_2^* : \mathrm{H}^1(X \times Y, \mathcal{O}_{X\times Y}) \xrightarrow{\sim} \mathrm{H}^1(X, \mathcal{O}_X) \times \mathrm{H}^1(Y, \mathcal{O}_Y)$ determines a Künneth isomorphism (here we use $\Gamma(X\ \mathcal{O}_X) = k = \Gamma(Y, \mathcal{O}_Y)$, i.e. Proposition 2.8, again), we see that $\zeta = 0$. Hence $\mathcal{L}_2$ is trivial, so that $Z_2 \longrightarrow Z$ factorizes through Z', which contradicts $I \not\subseteq \mathfrak{a}_2$.

□

For the remaining part of this section X will denote an abelian variety$_{/k}$ and $\mathcal{L}$ a line bundle on X.

Theorem 4.14 (Theorem of the Cube).
The line bundle

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

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

Proof. Restricting $\Theta(\mathcal{L})$ to $\{0\} \times X \times X$ yields the bundle

$$m^* \mathcal{L} \otimes p_2^* \mathcal{L}^{-1} \otimes p_3^* \mathcal{L}^{-1} \otimes m^* \mathcal{L}^{-1} \otimes \mathcal{O}_{X \times X} \otimes p_2^* \mathcal{L} \otimes p_3^* \mathcal{L}$$

which obviously is trivial. One easily verifies that the restriction of $\Theta(\mathcal{L})$ to $X \times \{0\} \times X$ and $X \times X \times \{0\}$ is trivial as well, hence the result follows in virtue of Theorem 4.13. □

Corollary 4.15.
Let Y be a scheme and let X be an abelian variety$_{/k}$. For every triple f, g, h of morphisms $Y \longrightarrow X$ and for every line bundle $\mathcal{L}$ on X, the bundle

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

on Y is trivial.

Proof. Use Theorem 4.14 and pull back along $Y \xrightarrow{f \times g \times h} X \times X \times X$. □

Theorem 4.16 (Theorem of the Square).
Let $\mathcal{L}$ be a line bundle on X. Let T be a scheme$_{/k}$ and write $\mathcal{L}_T$ for the pullback of $\mathcal{L}$ along the canonical projection $X_T \xrightarrow{\mathrm{pr}_X} X$. Then

$$t_{x+y}^*\mathcal{L}_T \otimes \mathcal{L}_T \cong t_x^*\mathcal{L}_T \otimes t_y^*\mathcal{L}_T \otimes \mathrm{pr}_T^*((x+y)^*\mathcal{L} \otimes x^*\mathcal{L}^{-1} \otimes y^*\mathcal{L}^{-1})$$

for all $x, y \in X(T)$. Choosing $T = k$ we in particular see that

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

Proof. Let $f = \mathrm{pr}_X : X_T \longrightarrow X, g = x \circ \mathrm{pr}_T$ and $h = y \circ \mathrm{pr}_T$. Then

$$f + g = \mathrm{pr}_X \circ t_x, f + h = \mathrm{pr}_X \circ t_y, g + h = (x+y) \circ \mathrm{pr}_T$$

and

$$f + g + h = \mathrm{pr}_X \circ t_{x+y}.$$

Now apply Corollary 4.15. □

As a consequence of the Theorem of the Square we obtain the immediate

Corollary 4.17.
Let $\mathcal{L}$ be a line bundle on X. Let $\operatorname{Pic} X$ be the picard group of X. Then the map $X(k) \xrightarrow{\varphi_{\mathcal{L}}} \operatorname{Pic} X$ given by $x \longmapsto [t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}]$ is a homomorphism of groups.

Once we will have established some more framework, the homomorphisms $\varphi_{\mathcal{L}}$ for *ample* line bundles $\mathcal{L}$ will form the prototype of so-called *polarizations*, which play an overall important role in the theory of abelian varieties.

Corollary 4.18.
Let $\mathcal{L}$ be any line bundle on an abelian variety X. Then

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

Proof. One has that

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

is trivial by letting $f = n, g = 1, h = -1$ in Corollary 4.15. Hence we have that

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

The result now follows by induction, starting from $n = -1, 0, 1$. □

Remark 4.19.
Note that Corollary 4.18 implies $n^* \mathcal{L} \cong \mathcal{L}^{\otimes n^2}$ for line bundles $\mathcal{L}$ satisfying $(-1)^* \mathcal{L} \cong \mathcal{L}$, which we will call *symmetric* line bundles from this point on.

As we will use the notion of *ampleness* when studying polarizations, we will take a quick detour to recall some basic definitions and results on *(very) ample line bundles*. We will not give any proofs, but give the relevant references instead.

Ample line bundles

Definition 4.20.
Let $(X, \mathcal{O})$ be any ringed space, $\mathcal{F}$ an $\mathcal{O}$-module on X and $(s_\lambda)_{\lambda\in\Lambda} \in \Gamma(X, \mathcal{F})^\Lambda$ a family of global sections of $\mathcal{F}$. $\mathcal{F}$ is said to be *generated by* $(s_\lambda)_\lambda$ if the morphism $\mathcal{O}^{(\Lambda)} \longrightarrow \mathcal{F}$ canonically associated to $(s_\lambda)_\lambda$ is surjective. We say that a $\mathcal{O}$-module $\mathcal{F}$ is *generated by global sections* if there exists a family $(s_\lambda)_\lambda$ of global sections generating $\mathcal{F}$.

Definition 4.21 (Ample line bundles).
Let X be a quasicompact, quasiseparated scheme. A line bundle $\mathcal{L}$ on X is called *ample* if for every quasi-coherent $\mathcal{O}_X$-module $\mathcal{F}$ of finite type there exists an integer $n_0 = n_0(\mathcal{F})$ such that $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{L}^{\otimes n}$ is generated by its global sections for all $n > n_0$.

Proposition 4.22.
Let X be qcqs and let $\mathcal{L}$ be a line bundle on X. The following are equivalent:

(i) $\mathcal{L}$ is ample.

(ii) For every quasi-coherent ideal $\mathcal{I} \subseteq \mathcal{O}_X$ of finite type there exists an integer $n \geq 1$ such that $\mathcal{I} \otimes \mathcal{L}^{\otimes n}$ is generated by its global sections.

(iii) The open subsets X_f for $f \in \Gamma(X, \mathcal{L}^{\otimes n})$ and $n > 0$ form a basis of the topology of X.

(iv) There exists $d \in \mathbb{N}$ and finitely many sections $f_i \in \Gamma(X, \mathcal{L}^{\otimes d})$ such that X_{f_i} is affine for all i and such that $X = \bigcup_i X_{f_i}$

Proof. [GW, Proposition 13.47]. □

Proposition 4.22 in turn implies the following

Proposition 4.23.
Let X be qcqs and let $\mathcal{L}_\circ$ and $\mathcal{L}_\bullet$ be line bundles on X.

(i) Let $n \in \mathbb{N}$. Then $\mathcal{L}_\circ$ is ample if and only if $\mathcal{L}_\circ^{\otimes n}$ is ample.

(ii) If $\mathcal{L}_\circ$ is ample, then there exists $n_\circ \in \mathbb{N}$ such that $\mathcal{L}_\circ^{\otimes n_\circ} \otimes \mathcal{L}_\bullet$ is ample and generated by its global sections for all $n \geq n_\circ$.

(iii) If $\mathcal{L}_\circ$ is ample and if there exists $n_\bullet \in \mathbb{N}$ such that $\mathcal{L}_\bullet^{\otimes n_\bullet}$ is generated by its global sections, then $\mathcal{L}_\circ \otimes \mathcal{L}_\bullet$ is ample.

(iv) If $\mathcal{L}_\circ$ and $\mathcal{L}_\bullet$ are ample, then $\mathcal{L}_\circ \otimes \mathcal{L}_\bullet$ is ample as well.

Proof. [GW, Proposition 13.50] □

Proposition 4.24.
Let X be qcqs and let $Z \hookrightarrow X$ be a quasi-compact embedding. Then ample line bundles of X pull back to ample line bundles on Z along $Z \hookrightarrow X$. In particular: Pulling back along *closed* embeddings preserves ampleness of line bundles.

Proof. [GW, Proposition 13.51] □

Proposition 4.25.
Let $X \xrightarrow{f} \operatorname{Spec} A$ be a morphism of schemes. Then f is *quasi-affine* if and only if $\mathcal{O}_X$ is ample on X.

Proof. Combine [Stacks, Tag 01VK] and [Stacks, Tag 0891]. □

Now that we fixed the necessary definitions and some basic properties of ampleness, we are able to continue the study of line bundles on abelian varieties:

Line bundles on abelian varieties (II)

We will go on by introducing the *Mumford line bundle* $\Lambda(\mathcal{L})$ of a line bundle $\mathcal{L}$ on an abelian variety and establish some more basic results.

Definition 4.26.
Let $\mathcal{L}$ be a line bundle on an abelian variety$_{/k}$ X. The *Mumford line bundle* $\Lambda(\mathcal{L})$ is defined via

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

and hence is a line bundle on $X \times_k X$.

Remark 4.27.
The restriction of $\Lambda(\mathcal{L})$ to a vertical fiber $\{x\} \times_k X$ as well as to a horizontal fiber $X \times_k \{x\}$ is given by $t_x^* \mathcal{L} \otimes \mathcal{L}^{-1}$. In particular, $\Lambda(\mathcal{L})$ is trivial on $\{0\} \times_k X$ and $X \times_k \{0\}$.

As it will become important at one point later on, we go on with the following

Lemma 4.28.
Let $X \xrightarrow{f} Y$ be a homomorphism of abelian varieties and let $\mathcal{L}$ be a line bundle on Y. Then

$$\Lambda(f^* \mathcal{L}) \overset{\text{can.}}{=} (f \times f)^* \Lambda(\mathcal{L})$$

Proof.

$$\begin{aligned}
(f \times f)^* \Lambda(\mathcal{L}) &\cong (f \times f)^* (m_Y^* \mathcal{L} \otimes p_{1,Y}^* \mathcal{L}^{-1} \otimes p_{2,Y}^* \mathcal{L}^{-1}) \\
&\cong (m_Y \times (f \times f))^* \mathcal{L} \otimes (p_{1,Y} \circ (f \times f))^* \mathcal{L}^{-1} \otimes (p_{2,Y} \circ (f \times f))^* \mathcal{L}^{-1} \\
&= (f \circ m_X)^* \mathcal{L} \otimes (f \circ p_{1,X})^* \mathcal{L}^{-1} \otimes (f \circ p_{2,X})^* \mathcal{L}^{-1} \qquad (4.1) \\
&\cong m_X^* (f^* \mathcal{L}) \otimes p_{1,X}^* (f^* \mathcal{L})^{-1} \otimes p_{2,X}^* (f^* \mathcal{L})^{-1} \\
&\cong \Lambda(f^* \mathcal{L})
\end{aligned}$$

where the equality holds because f is a *homomorphism* - see (3.1). □

Definition 4.29.
Let $\mathcal{L}$ be a line bundle on an abelian variety$_{/k}$ X. We define $\mathrm{K}(\mathcal{L})$ to be the maximal closed subscheme (as in Theorem 4.10) of $X \times_k X$ such that $\Lambda(\mathcal{L})|_{X \times_k \mathrm{K}(\mathcal{L})}$ is trivial over $\mathrm{K}(\mathcal{L})$, i.e. such that $\Lambda(\mathcal{L})|_{X \times_k \mathrm{K}(\mathcal{L})} \cong \mathrm{pr}_2^* \mathcal{L}'$ for a line bundle $\mathcal{L}'$ on $\mathrm{K}(\mathcal{L})$.

Remark 4.30.
Note that the universal property of $\mathrm{K}(\mathcal{L})$ implies that it behaves well with respect to base change. In particular: If $K \mid k$ is any field extension, one has $\mathrm{K}(\mathcal{L}_K) = \mathrm{K}(\mathcal{L}) \times_k K$.

Lemma 4.31.
Let T be a scheme$_{/k}$ and $x \in X(T)$ a T-valued point of X.

(i) x factors through $\mathrm{K}(\mathcal{L})$ if and only if $t_x^*\mathcal{L}_T \otimes \mathcal{L}_T^{-1}$ is trivial along $X_T \xrightarrow{\mathrm{pr}_T} T$.

(ii) If $t_x^*\mathcal{L}_T \otimes \mathcal{L}_T^{-1} \cong \mathrm{pr}_T^* \mathcal{L}'$, then $\mathcal{L}' \cong x^*\mathcal{L}$.

(iii) $\Lambda(\mathcal{L})|_{X\times_k \mathrm{K}(\mathcal{L})} \cong \mathcal{O}_{X\times_k \mathrm{K}(\mathcal{L})}$.

Proof.

(i) Denote by $X_T \xrightarrow{\mathrm{pr}_X} X$ the canonical projection as usual.

First note that $X \times_k T \xrightarrow{t_x} X \times_k T \xrightarrow{\mathrm{pr}_X} X$ equals the composition $X \times_k T \xrightarrow{\mathrm{id}_X \times_k x} X \times_k X \xrightarrow{m} X,$ as one has

$$\begin{tikzcd}
(p,1) \arrow[r, mapsto, "t_x"] \arrow[d, mapsto, "\mathrm{id}_X \times x"'] & (p+x,1) \arrow[d, mapsto, "\mathrm{pr}_X"] \\
(p,x) \arrow[r, mapsto, "m"] & p+x
\end{tikzcd}$$

on T'-valued points$_{/T}$, where we denoted by 1 the unique T'-valued point of T over T.
We therefore obtain that

$$t_x^*\,\mathcal{L}_T \cong (\mathrm{id}_X \times_k x)^* m^*\,\mathcal{L}$$

As furthermore $\mathrm{pr}_X = p_1 \circ (\mathrm{id}_X \times x) : X \times_k T \to X \times_k X \to X$, we also see $\mathcal{L}_T \cong (\mathrm{id}_X \times x)^* p_1^*\,\mathcal{L}$. Hence

$$t_x^* \otimes \mathcal{L}_T^{-1} \cong (\mathrm{id}_X \times x)^*\Lambda(\mathcal{L}) \otimes (\mathrm{id}_X \times x)^* p_2^*\,\mathcal{L} \cong (\mathrm{id}_X \times x)^*\Lambda(\mathcal{L}) \otimes \mathrm{pr}_T^*\, x^*\,\mathcal{L},$$

and we deduce the assertion of (i) by the defining property of $\mathrm{K}(\mathcal{L})$.

(ii) Let $i : T \xrightarrow{\cong} \{0\} \times T \hookrightarrow X \times T$ be the inclusion. Then

$$\mathcal{L}' \cong \underbrace{(\mathrm{pr}_T \circ i)}_{=\,\mathrm{id}_T}{}^*\,\mathcal{L}' \cong i^*\,\mathrm{pr}_T^*\,\mathcal{L}' \cong i^*(t_x^*\,\mathcal{L}_T \otimes \mathcal{L}_T^{-1}) \cong \underbrace{(\mathrm{pr}_X \circ t_x \circ i)}_{=\,x}{}^*\,\mathcal{L} \otimes \underbrace{(\mathrm{pr}_X \circ i)}_{=\,0}{}^*\,\mathcal{L}^{-1} \cong x^*\,\mathcal{L}\,.$$

(iii) Let $T = \mathrm{K}(\mathcal{L})$ and $x : \mathrm{K}(\mathcal{L}) \hookrightarrow X$ be the inclusion. The computation in (i) together with the defining property of $\mathrm{K}(\mathcal{L})$ then shows that

$$t_x^*\,\mathcal{L}_T \otimes \mathcal{L}_T^{-1} \cong \Lambda(\mathcal{L})_{|X\times \mathrm{K}(\mathcal{L})} \otimes (p_2^*\,\mathcal{L})_{|X\times\mathrm{K}(\mathcal{L})} \cong p_2^*\,\mathcal{M} \otimes p_2^*(\mathcal{L}_{|X\times\mathrm{K}(\mathcal{L})})$$

for some line bundle $\mathcal{M}$ on $\mathrm{K}(\mathcal{L})$.
As we also have that $x^*\,\mathcal{L} = \mathcal{L}_{|X\times\mathrm{K}(\mathcal{L})}$, we obtain $\mathcal{M} \cong \mathcal{O}_{\mathrm{K}(\mathcal{L})}$ in virtue of (ii).
Thus $\Lambda(\mathcal{L})_{|X\times\mathrm{K}(\mathcal{L})} \cong p_2^*\,\mathcal{O}_{\mathrm{K}(\mathcal{L})} \cong \mathcal{O}_{X\times\mathrm{K}(\mathcal{L})}$ as desired.

□

Proposition 4.32.
The subscheme $\mathrm{K}(\mathcal{L})$ is a subgroup scheme of X.

Proof. We have to show that $\mathrm{K}(\mathcal{L})(T) \subseteq X(T)$ is a subgroup for any $T \in \mathsf{Sch}_{/k}$.
Suppose $x, y \in \mathrm{K}(\mathcal{L})(T)$. We show that $x - y \in \mathrm{K}(\mathcal{L})(T)$.
Setting $\mathcal{M} \overset{\mathrm{def}}{=} (x-y)^*\,\mathcal{L} \otimes x^*\,\mathcal{L}^{-1} \otimes y^*\,\mathcal{L}^{-1}$, the Theorem of the Square implies that

$$\begin{aligned}
t_{x-y}^*\,\mathcal{L}_T \otimes \mathcal{L}_T^{-1} &\cong\ t_x^*\,\mathcal{L}_T \otimes t_{-y}^*\,\mathcal{L}_T \otimes \mathrm{pr}_T^*(\mathcal{M} \otimes \mathcal{L}^{-2}) \\
&\cong (t_x^*\,\mathcal{L}_T \otimes \mathcal{L}_T^{-1}) \otimes (t_y^*\,\mathcal{L}_T)^{-1} \otimes \mathrm{pr}_T^*(\mathcal{M} \otimes \mathcal{L}^{-1}) \\
&\cong (t_x^*\,\mathcal{L}_T \otimes \mathcal{L}_T^{-1}) \otimes (t_y^*\,\mathcal{L}_T \otimes \mathcal{L}_T^{-1})^{-1} \otimes \mathrm{pr}_T^*(\mathcal{M} \otimes \mathcal{L}^{-2}),
\end{aligned} \tag{4.2}$$

hence $x - y \in \mathrm{K}(\mathcal{L})(T)$ in virtue of Lemma 4.31(i) as $x, y \in \mathrm{K}(\mathcal{L})(T)$. □

Lemma 4.33.
If $\mathcal{L}$ is ample, then $\mathrm{K}(\mathcal{L})$ is finite.

Proof. The pullback $\mathcal{L}_{\bar{k}}$ of $\mathcal{L}$ along $X_{\bar{k}} \longrightarrow X$ is again ample by Proposition 4.24. We furthermore have $\mathrm{K}(\mathcal{L}_{\bar{k}}) = \mathrm{K}(\mathcal{L}) \times_k \bar{k}$ as remarked in 4.30. Thus, if we prove the result under the assumption that $k = \bar{k}$, we obtain that $\mathrm{K}(\mathcal{L}) \times_k \bar{k}$ is finite, and thus realize $\mathrm{K}(\mathcal{L})$ to be finite as well, as finiteness descends along *faithfully flat* base change [EGA-IV, Proposition (2.7.1)]. We thus may assume $k = \bar{k}$ from this point on. Then $Y \overset{\text{def}}{=} \mathrm{K}(\mathcal{L})^0_{\text{red}} \hookrightarrow X$ is seen to be an abelian subvariety of X by combining Proposition 3.17 (here we use $k = \bar{k}$ as we need to work over a perfect ground field) and Lemma 3.14.
Alternatively, the assertion is a special case of the stronger (and also unproven) Theorem 4.8.
The restriction $\mathcal{L}_|$ of $\mathcal{L}$ to Y is again ample by Proposition 4.24, as $Y \hookrightarrow X$ is a closed embedding. The Mumford bundle $\Lambda(\mathcal{L}_|)$ on $Y \times Y$ is now seen to be trivial in virtue of Lemma 4.31(iii). Pulling back via $(1, -1) : Y \longrightarrow Y \times Y$ gives that $\mathcal{L}_| \otimes (-1)^* \mathcal{L}_|$ is trivial on Y. But $\mathcal{L}_|$ is ample, so $(-1)^* \mathcal{L}_|$ and thus $\mathcal{L}_| \otimes (-1)^* \mathcal{L}_|$ are as well in virtue of Proposition 4.23(iv). Thus the trivial bundle $\mathcal{O}_Y$ on Y is ample, hence Y is quasi-affine by Proposition 4.25, i.e $Y \longrightarrow \operatorname{Spec} \Gamma(Y, \mathcal{O}_Y) \overset{2.8}{=} \operatorname{Spec} k$ is an open embedding $-$ Y consists of a single point. Hence $\dim Y = 0$, so that we see $\dim \mathrm{K}(\mathcal{L}) = 0$ by Lemma 3.13 and hence obtain that $\mathrm{K}(\mathcal{L})$ is *finite* as 0-dimensional schemes of finite type$_{/k}$ are finite (see [Stacks, 06LH]). □

Establishing a few more results on line bundles on abelian varieties, one can show the following very important theorem:

Theorem 4.34.
An abelian variety$_{/k}$ is projective.

Proof. A proof can be found in [AV, (2.25) Theorem]. □

Remark 4.35.
Note that Theorem 4.34 implies that every abelian variety X admits an ample line bundle:
Indeed, since we can find a (necessarily!) closed embedding of X into projective space, it suffices to show that $\mathbb{P}^n_k$ admits ample line bundles by Proposition 4.24. Observing $(\mathbb{P}^n_k)_{X_i} = D_+(X_i)$ where $X_0, \dots, X_n \in \Gamma(\mathbb{P}^n_k, \mathcal{O}_{\mathbb{P}^n}(1))$ we see that $\mathcal{O}_{\mathbb{P}^n}(1)$ is ample in virtue of Proposition 4.22(iv) as $\mathbb{P}^n_k = \bigcup_i D_+(X_i)$.

5 Isogenies

In this chapter we will introduce the notion of *isogeny*, which is of fundamental importance to the theory of abelian varieties.
We once again do not strive for a thorough and complete investigation, but for a quick introduction establishing only very basic results.
Two abelian varieties being *isogenous* to each other is a strictly weaker condition than being isomorphic. However, the conditions imposed by isogeny are still strong enough to intimately relate the geometry of isogenous abelian varieties.
We begin by recalling without proof some well-known facts from algebraic geometry:

Lemma 5.1.

(i) Let X and Y be irreducible noetherian, regular schemes with $\dim X = \dim Y$. Then quasi-finite morphisms $X \longrightarrow Y$ are flat.

(ii) Let $X \xrightarrow{f} Y$ be a morphism of finite type between noetherian schemes, with Y reduced and irreducible. Then there is a non-empty open subset $U \subseteq Y$ such that either $f^{-1}(U) = \emptyset$ or the restricted morphism $f^{-1}(U) \xrightarrow{f_|} U$ is flat.

Proof. [AV, (5.1)]. □

Lemma 5.2.
If $X \xrightarrow{f} Y$ is a *flat* morphism of varieties$_{/k}$ and $F \subseteq X$ is the fiber of f over a *closed* point of Y, then F is equidimensional and

$$\dim X = \dim Y + \dim F.$$

Proof. Special case of [Hartshorne, Chapter III: Proposition 9.5]. □

Proposition 5.3.
Let $X \xrightarrow{f} Y$ be a homomorphism of abelian varieties. The following are equivalent:

(i) f is surjective and $\dim X = \dim Y$.

(ii) $\ker f$ is a finite group scheme and $\dim X = \dim Y$.

(iii) f is finite, flat and surjective.

Proof. First note that any homomorphism $X \to Y$ of abelian varieties is *proper* by the Cancellation theorem 2.7.
Assume that (ii) holds. As f is proper and all fibers are translates of $\ker f$, it follows that f is finite - compare [Stacks, 02OG] or [Vakil, 29.6.2. Theorem] for a proof avoiding spectral sequences. Thus $f(X)$ is closed in Y of dimension equal to $\dim X = \dim Y$, i.e. f is surjective. f is flat in virtue of Lemma 5.1(i). Hence (ii) implies (i) and (iii).
Now suppose that (i) holds. Then f is flat over a non-empty open subset $V \subseteq Y$ by Lemma 5.1(ii). Hence we can apply Lemma 5.2 to obtain that $\dim \ker f = 0$, as $\dim F = 0$ holds for any fiber over a closed point in U and as $\ker f$ is a translate of any such fiber F. Hence (i) implies (ii).
We now show that (iii) implies (ii) as well. As f is flat, Lemma 5.2 implies that $\dim X = \dim Y + \dim \ker f$. Since f is finite, so is $\ker f$ by base change. Hence $\ker f$ is of finite type$_{/k}$ and consists of finitely many points only, i.e. $\dim \ker f = 0$ so that we obtain $\dim X = \dim Y$ as well. □

Remark 5.4.
As a homomorphism $X \xrightarrow{f} Y$ satisfying the conditions from Proposition 5.3 is surjective, it carries the generic point η_X of X to the generic point η_Y of Y and hence induces a function field extension $\kappa(Y) = \mathcal{O}_{Y,\eta_Y} \longrightarrow \mathcal{O}_{X,\eta_X} = \kappa(X)$.

Definition 5.5 (Isogeny).

A homomorphism $X \xrightarrow{f} Y$ of abelian varieties is called *isogeny*$_{/k}$, if f satisfies the three equivalent conditions of Proposition 5.3.
The *degree* of f, denoted by $\deg f$, is the degree of the function field extension $[\kappa(X) : \kappa(Y)]$.

Remark.
If $X \xrightarrow{f} Y$ and $Y \xrightarrow{g} Z$ are isogenies, so is $X \xrightarrow{g \circ f} Z$ and $\deg(g \circ f) = \deg g \cdot \deg f$.

Lemma 5.6.
Let $W \xrightarrow{f} X$ and $Y \xrightarrow{h} Z$ be isogenies of abelian varieties over k. If $X \underset{g_2}{\overset{g_1}{\rightrightarrows}} Y$ are homomorphisms such that $h \circ g_1 \circ f = h \circ g_2 \circ f$ then $g_1 = g_2$.

Proof. As equality of morphisms$_{/k}$ of varieties can be checked after base extension, we may assume $k = \bar{k}$.
As f is surjective and flat, it is faithfully flat, hence an epimorphism of schemes [Stacks, 02VW]. Hence $h \circ g_1 = h \circ g_2$.
Thus $g_1 - g_2$ factorizes through the finite group scheme $\ker h$. As X is connected and reduced, it even factorizes through $(\ker h)^0_{\mathrm{red}}$, which is trivial. □

Proposition 5.7.
$[n]_X$ is an isogeny$_{/k}$ for $n \neq 0$ and $\deg[n]_X = n^{2 \dim X}$.

Proof. We will only prove the first assertion, namely that $[n]_X$ is an isogeny whenever $n \neq 0$.
Note that X admits an *ample* and *symmetric* line bundle $\mathcal{L}$ (use that X admits an ample line bundle as explained in remark 4.35 and that $\mathcal{L} \otimes (-1)^* \mathcal{L}$ is symmetric for any line bundle $\mathcal{L}$).
One has that $n^* \mathcal{L} \cong \mathcal{L}^{\otimes n^2}$ according to Remark 4.19, hence $n^* \mathcal{L}$ is *ample* in virtue of Proposition 4.23 since $n \neq 0$.
Note that the restriction $(n^* \mathcal{L})_{|X[n]}$ is still ample according to Proposition 4.24.
We claim that $(n^* \mathcal{L})_{|X[n]}$ is *trivial*. To see this, recall that the diagram

$$\begin{tikzcd}
X[n] \arrow[r, "j"] \arrow[d, hook, "i"'] \arrow[dr, phantom, "\lrcorner", very near start] & \{0\} \arrow[d, hook, "e"'] \\
X \arrow[r, "{[n]}"] & X
\end{tikzcd}$$

is cartesian. It follows that

$$\begin{aligned}
(n^* \mathcal{L})_{|X[n]} &= i^* n^* \mathcal{L} \\
&\cong ([n] \circ i)^* \mathcal{L} \\
&\cong (e \circ j)^* \mathcal{L} \\
&\cong j^* e^* \mathcal{L} \\
&\cong j^* \mathcal{O}_{\{0\}} \\
&\cong \mathcal{O}_{X[n]}
\end{aligned} \tag{5.1}$$

is trivial as claimed.
$(n^* \mathcal{L})_{|X[n]}$ is thus ample *and* trivial, which implies that $X[n] = \ker[n]$ is finite (compare the proof of Lemma 4.33).
Hence $[n]$ is seen to be an isogeny as claimed. A proof for the second assertion using intersection theory on smooth varieties can be found in [AV, (5.9) Proposition]. □

As an immediate consequence of the previous statement we obtain

Corollary 5.8.
Let X be an abelian variety over an algebraically closed field $k = \overline{k}$. Then $X(k)$ is a *divisible* group, i.e. for any $P \in X(k)$ and any $n \in \mathbb{Z} \setminus \{0\}$ there exists $Q \in X(k)$ such that $n \cdot Q = P$.

If we had covered some basic results concerning the theory of *étale group schemes*, we could have also given a complete proof of

Corollary 5.9.
One has $X[n](k^s) = X[n](\overline{k}) \cong (\mathbb{Z}/n\mathbb{Z})^{2 \dim X}$ whenever $(\operatorname{char} k, n) = 1$.

Proof. [AV, (5.11) Corollary]. □

Proposition 5.10.
If $X \xrightarrow{f} Y$ is an isogeny of degree d, there exists an isogeny $Y \xrightarrow{g} X$ with $g \circ f = [d]_X$ and $f \circ g = [d]_Y$.

Remark.
The proof uses the existence of certain *quotients* under suitable assumptions. Given that this is the *only* place that we will (actively) use the existence of such quotients, we will not prove it, but just use it here to convey the idea behind the proof. Consult [AV, Chapter 4] for a detailed treatment of quotients by group schemes.

Proof. One shows that $\ker f \subseteq \ker[d]_X$ using the finiteness of $\ker f$. One then uses that $X/\ker f$ exists, that f induces an isomorphism $Y \xrightarrow{\cong} X/\ker f$ and the universal property of quotients to obtain the following commutative diagram:

$$\begin{tikzcd}
X \arrow[r, "{[d]_X}"] \arrow[d, "\pi"'] \arrow[dd, bend right=60, "f"'] & X \\
X/\ker f \arrow[ur, dotted, "\exists!"] \arrow[d, "\cong"'] & \\
Y \arrow[uur, dotted, "g"'] &
\end{tikzcd}$$

where $Y \xrightarrow{g} X$ is a morphism of group schemes, hence of abelian varieties.
The computation

$$\mathrm{id}_Y \circ (f \circ g) \circ f = f \circ (g \circ f) = f \circ [d]_X = [d]_Y \circ f = \mathrm{id}_Y \circ [d]_Y \circ f$$

shows that $f \circ g = [d]_X$ in virtue of Lemma 5.6. Proposition 5.7 now implies that g is an isogeny:
g is surjective because $g \circ f = [d]_X$ is, and $\ker g$ is finite because $\ker g = g^{-1}(0) \subseteq g^{-1}(\ker f) = \ker(f \circ g) = \ker[d]_Y$ and because $\ker[d]_Y$ is finite. □

One important aspect of Proposition 5.10 is that it implies

Corollary 5.11.
The relation

$$X \sim_k Y \overset{\text{def}}{=} \text{there exists an isogeny } X \longrightarrow Y$$

is an equivalence relation on the set of abelian varieties$_{/k}$.

Remark 5.12.
If $X \sim_k Y$, X and Y are said to be *isogenous over* k or also *isogenous*$_{/k}$. If the base field k is to be understood from the context, one often simply writes $X \sim Y$ and calls X and Y *isogenous* without referencing k.
Note that $X \sim_k Y$ implies $X_K \sim_K Y_K$ for any base extension $K \mid k$, but *not* the other way around in general.

6 Picard schemes

Picard schemes

In order to introduce the *dual* of an abelian variety, we will take a glimpse on picard schemes first. As this is rather technical and not the main concern of this thesis, we will not bother to prove most results discussed in this chapter.

Given any scheme$_{/S}$ X, we are interested in studying the contravariant functor $P_{X/S} : \mathsf{Sch}_{/S}^{op} \to \mathsf{Grp}$ given by $T \mapsto \operatorname{Pic} X_T$.
We would like $P_{X/S}$ to be representable by a group scheme - $P_{X/S}$ is not representable in *all* nontrivial cases though (that is: whenever $X \neq \emptyset$) however. There are different ways to address this problem, as is often then case when facing the problem of representability of moduli functors. As we try to mainly use the theory of picard schemes, we will not strive for maximal generality and instead just add some hypothesis to the S-scheme X and in some sense weaken the functor $P_{X/S}$, in order to obtain a representable one.
In the following, we will assume that

(i) the structure morphism $X \xrightarrow{f} S$ is quasi-compact and quasi-separated.
(ii) $f_*(\mathcal{O}_{X_T}) = \mathcal{O}_T$ for all S-schemes T.
(iii) f admits a section $S \xrightarrow{\epsilon} X$.

Note that the assumptions $(i) - (iii)$ are all satisfied in the case of our interest, i.e. abelian varieties$_{/k}$.
Indeed, the only non-trivial thing is (ii) which follows for example from [Vakil, Remark 28.1.9] using that $X \longrightarrow \operatorname{Spec} k$ is proper (by definition of an abelian variety), finitely presented (we are working over the Noetherian base Spec k, so this reduces saying that the morphism under consideration is of finite type$_{/k}$) and flat with geometrically connected and geometrically reduced fibers (again trivial by the definitions involved).

Definition 6.1.
If $\mathcal{L}$ is a line bundle on X_T for some S-scheme T, a *rigidification of* $\mathcal{L}$ *along* ϵ_T is an isomorphism $\alpha : \ \mathcal{O}_T \xrightarrow{\ \sim\ } \epsilon_T^*\mathcal{L}$, where ϵ_T denotes the section of X_T induced by ϵ via base change.

If $(\mathcal{L}_\circ, \alpha_\circ)$ and $(\mathcal{L}_\bullet, \alpha_\bullet)$ are rigidifications of $\mathcal{L}$ along ϵ_T, then by a *homomorphism* $(\mathcal{L}_\circ, \alpha_\circ) \to (\mathcal{L}_\bullet, \alpha_\bullet)$ we mean a homomorphism $\mathcal{L}_\circ \xrightarrow{\varphi} \mathcal{L}_\bullet$ of line bundles such that $\epsilon_T^*\varphi \circ \alpha_\circ = \alpha_\bullet$.

The set of isomorphism classes of line bundles on X rigidified along ϵ, denoted by $\operatorname{Pic}_\epsilon X$, again carries the structure of an abelian group:
The group structure is defined by $([(\mathcal{L}_\circ, \alpha_\circ)], [(\mathcal{L}_\bullet, \alpha_\bullet)]) \mapsto [(\mathcal{L}_\circ \otimes \mathcal{L}_\bullet, \alpha)]$, where $\alpha \overset{\text{def}}{=} \alpha_\circ \otimes \alpha_\bullet : \mathcal{O}_T \overset{\text{can.}}{=} \mathcal{O}_T \otimes_{\mathcal{O}_T} \mathcal{O}_T \to \epsilon_T^* \mathcal{L}_\circ \otimes_{\mathcal{O}_T} \epsilon_T^* \mathcal{L}_\bullet \overset{\text{can.}}{=} \epsilon_T^*(\mathcal{L}_\circ \otimes_{\mathcal{O}_T} \mathcal{L}_\bullet)$.

Given the notion of *rigidification* we are now led to study the following functor:

Definition 6.2.
The functor $P_{X/S,\epsilon} : \mathsf{Sch}_{/S}^{op} \to \mathsf{Grp}$ defined by

$$T \mapsto \operatorname{Pic}_{\epsilon_T}(X_T)$$
$$(T' \xrightarrow{\varphi} T) \mapsto P_{X/S,\epsilon}(\varphi)$$

is called *rigidified relative Picard functor*.
Here $P_{X/S,\epsilon}(\varphi)$ maps $[(\mathcal{L}, \alpha)] \in \operatorname{Pic}_\epsilon(X_T)$ to $[((\mathrm{id}_X \times \varphi)^*\mathcal{L}, (\mathrm{id}_X \times \varphi)^*\alpha)] \in \operatorname{Pic}_\epsilon(X_{T'})$.

Suppose now that $P_{X/S,\epsilon}$ is representable by an S-scheme denoted by $P_{X/S,\epsilon}$ again.
We then obtain a *universal* rigidified line bundle $(\mathcal{P},\nu)$ on $X\times_S P_{X/S,\epsilon}$ by the Yoneda lemma; the so called *Poincaré bundle* on X. Going through the explicit bijection in the Yoneda lemma as in 3.11, one checks that $(\mathcal{P},\nu)$ satisfies the following universal property:
If $(\mathcal{L},\alpha)$ is any line bundle on X_T rigidified along ϵ_T, then there exists a unique morphism $T\xrightarrow{g}P_{X/S,\epsilon}$ such that $(\mathcal{L},\alpha)\cong(\mathrm{id}_X\times g)^*(\mathcal{P},\nu)$ as rigidified line bundles on X_T.

Also note that $P_{X/S,\epsilon}$ is compatible with base change, i.e. if $P_{X/S,\epsilon}$ is represented by a scheme$_{/S}$ $\mathfrak{X}$ and if $T\longrightarrow S$ is any morphism, $P_{X_T/T,\epsilon_T}$ is represented by the base change $\mathfrak{X}_T$ of $\mathfrak{X}$ along $T\longrightarrow S$.
This in turn implies that the Poincaré bundle is compatible with base change as well:

$$\mathcal{P}_{X_T/T,\epsilon_T}=\mathrm{pr}^*_{X\times_S P_{X/S,\epsilon}}\mathcal{P}_{X/S,\epsilon}$$

where $\mathrm{pr}_{X\times_S P_{X/S,\epsilon}}\overset{\mathrm{def}}{=}X_T\times_T P_{X_T/T,\epsilon_T}\xrightarrow{\mathrm{pr}_X\times_S\mathrm{pr}_P}X\times_S P_{X/S,\epsilon}$ is the morphism induced by the two canonical projections $X_T\xrightarrow{\mathrm{pr}_X}X$ and $P_{X_T/T,\epsilon_T}\xrightarrow{\mathrm{pr}_P}P_{X/S,\epsilon}$.

Our interest in the functor $P_{X/S,\epsilon}$ comes from the fact, that $P_{X/S,\epsilon}$ indeed is representable if $S=\operatorname{Spec}k$ and $X\to S$ is proper in addition to our standing hypothesis from above. One can even show that the representing scheme $P_{X/S,\epsilon}$ is separated and locally of finite type$_{/k}$. We will not proof this claim though and just refer to [AV, (6.3)] instead.

The dual of an abelian variety

Let X be an abelian variety over $S=\operatorname{Spec}k=\{0\}$ with zero section $\{0\}\xrightarrow{e}X$.
In order to simplify notation we will denote the functor $P_{X/S,e}$ by Pic_X.

We already know that Pic_X is represented by a separated group scheme Pic_X, locally of finite type$_{/k}$.
Astonishingly, one can show that the connected component Pic^0_X of Pic_X carries the structure of an abelian variety$_{/k}$ again. In order to sketch the rough idea of how one proves that Pic^0_X is an abelian variety, we first give a new interpretation of the Mumford line bundle using Pic_X:
If $\mathcal{L}$ is a line bundle on X, one has the associated Mumford bundle $\Lambda(\mathcal{L})$ on $X\times X$. Write $X^{(1)}\overset{\mathrm{def}}{=}X\times\{0\}$ and $X^{(2)}\overset{\mathrm{def}}{=}\{0\}\times X$ to distinguish the two factors.
Note that Remark 4.27 implies that $\Lambda(\mathcal{L})$ carries a natural rigidification along $\{0\}\times X\hookrightarrow X\times X$.
Considering $\Lambda(\mathcal{L})$ as a family of line bundles on $X^{(1)}$ parametrized by $X^{(2)}$ thus results in a morphism

$$X=X^{(2)}\xrightarrow{\varphi_{\mathcal{L}}}\mathrm{Pic}_{X/k}$$

which is the unique morphism such that $(\mathrm{id}_X\times\varphi_{\mathcal{L}})^*\,\mathcal{P}=\Lambda(\mathcal{L})$.
The morphism is given on points via $x\mapsto[t_x^*\,\mathcal{L}\otimes\mathcal{L}^{-1}]$, as one can find in [Mumford, §13.].
We have seen that $\varphi_{\mathcal{L}}$ is a homomorphism in Corollary 4.17 already.
One in particular sees that $\varphi_{\mathcal{L}}$ is a morphism $X\longrightarrow\mathrm{Pic}^0_{X/k}$, as X is connected and as $\varphi_{\mathcal{L}}(0)=0$.

Theorem 6.3.
Let X be an abelian variety$_{/k}$. Then Pic^0_X is reduced, hence an abelian variety.
For every *ample* line bundle $\mathcal{L}$ on X, the homomorphism $\varphi_{\mathcal{L}} : X \to \mathrm{Pic}^0_X$ is an isogeny with kernel $\mathrm{K}(\mathcal{L})$. One has $\dim \mathrm{Pic}^0_{X/k} = \dim X = \dim_k H^1(X, \mathcal{O}_X)$.

Proof. The proof uses some results that we did not discuss at all. Hence we only present the strategy of the proof and refer to [AV, (6.18) Theorem] for the details missing.
Let $\mathcal{L}$ be an ample line bundle. It is an immediate consequence of Lemma 4.31 that $\mathrm{K}(\mathcal{L}) = \ker \varphi_{\mathcal{L}}$. As $\mathcal{L}$ is assumed to be ample, $\mathrm{K}(\mathcal{L})$ is finite in virtue of Lemma 4.33, hence $\dim \mathrm{Pic}^0_{X/k} \geq \dim X$. From here on, one proceeds as follows:
One shows that $\mathrm{Pic}^0_{X/k}$ is smooth$_{/k}$ if and only if $\dim \mathrm{Pic}^0_{X/k} = \dim_k H^1(X, \mathcal{O}_X)$ and that $H^1(X, \mathcal{O}_X)$ is isomorphic to the tangent space of $\mathrm{Pic}^0_{X/k}$ at the identity element. Furthermore one shows that $\dim_k H^1(X, \mathcal{O}_X) \leq \dim X$ using the so-called *Borel-Hopf structure theorem*. So one obtains $\dim \mathrm{Pic}^0_{X/k} \geq \dim X \geq \dim_k H^1(X, \mathcal{O}_X) = \dim \mathrm{Pic}^0_{X/k}$. Reducedness then follows in virtue of Proposition 3.16. □

We are now able to introduce the *dual* of an abelian variety:

Definition 6.4 (Dual of an abelian variety).
Given any abelian variety$_{/k}$ X, we denote the abelian variety Pic^0_X by X^t and call it the *dual* of X.
We write $\mathcal{P}_X$ or sometimes $\mathcal{P}$ for the restriction of the Poincaré bundle on $X \times \mathrm{Pic}_X$ to $X \times X^t$.
If $X \xrightarrow{f} Y$ is a homomorphism of abelian varieties$_{/k}$, we denote by $Y^t \xrightarrow{f^t} X^t$ the unique homomorphism such that

$$(\mathrm{id}_X \times f^t)^* \mathcal{P}_X \cong (f \times \mathrm{id}_{Y^t})^* \mathcal{P}_Y. \tag{6.1}$$

as line bundles on $X \times Y^t$ rigidified along $\{0\} \times Y^t \xrightarrow{e_{Y^t}} X \times Y^t$.

Remark 6.5.
Note that taking duals respects extension of the base field: $(f^t)_K = (f_K)^t$ for $K \mid k$ any field extension. Indeed:

$$\begin{aligned}
(\mathrm{id}_{X_K} \times (f^t)_K)^* \mathcal{P}_{X_K} &= ((\mathrm{id}_X \times f^t)_K)^* (\mathrm{pr}_X \times_k \mathrm{pr}_{X^t})^* \mathcal{P}_X \\
&= ((\mathrm{pr}_X \times \mathrm{pr}_{X^t}) \circ (\mathrm{id}_X \times f^t)_K)^* \mathcal{P}_X \\
&= (\mathrm{pr}_X \times \underbrace{(\mathrm{pr}_{X^t} \circ (f^t)_K)}_{= f^t \circ \mathrm{pr}_{Y^t}})^* \mathcal{P}_X \\
&= ((\mathrm{id}_X \times f^t) \circ (\mathrm{pr}_X \times \mathrm{pr}_{Y^t}))^* \mathcal{P}_X \\
&= (\mathrm{pr}_X \times \mathrm{pr}_{Y^t})^* (\mathrm{id}_X \times f^t)^* \mathcal{P}_X \\
&\overset{6.1}{=} (\mathrm{pr}_X \times \mathrm{pr}_{Y^t})^* (f \times \mathrm{id}_{Y^t})^* \mathcal{P}_Y \qquad (6.2) \\
&= ((f \times \mathrm{id}_{Y^t}) \circ (\mathrm{pr}_X \times \mathrm{pr}_{Y^t}))^* \mathcal{P}_Y \\
&= ((\underbrace{f \circ \mathrm{pr}_X}_{= \mathrm{pr}_Y \circ f_K}) \times \mathrm{pr}_{Y^t})^* \mathcal{P}_Y \\
&= ((\mathrm{pr}_Y \times \mathrm{pr}_{Y^t}) \circ (f_K \times \mathrm{id}_{Y_K}))^* \mathcal{P}_Y \\
&= (f_K \times \mathrm{id}_{Y^t_K})^* ((\mathrm{pr}_Y \times \mathrm{pr}_{Y^t})^* \mathcal{P}_Y \\
&= (f_K \times \mathrm{id}_{Y^t_K})^* \mathcal{P}_{Y_K},
\end{aligned}$$

where we used that

$$\mathrm{pr}_{\mathrm{Pic}_X}(\underbrace{\mathrm{Pic}^0_{X_K}}_{\overset{\mathrm{def}}{=} (X_K)^t}) \subseteq \mathrm{Pic}^0_X \overset{\mathrm{def}}{=} X^t$$

by continuity and the fact that it carries $0 \mapsto 0$.
Thus one has $(f^t)_K = (f_K)^t$ by uniqueness.

Polarizations

Polarizations are of crucial importance in the theory of abelian varieties in general.
As we will only use polarizations in order to proof the *Poincaré Splitting Theorem* later on, we will keep this introduction very sketchy.

Definition 6.6 (Polarization).
A *polarization* of an abelian variety$_{/k}$ X is a homomorphism $X \xrightarrow{\lambda} X^t$ such that there exists a field extension $K \mid k$ and an ample line bundle $\mathcal{L}$ on X_K with $\lambda_K = \varphi_{\mathcal{L}}$.

Remark 6.7.
Note that every abelian variety X admits a polarization as abelian varieties admit ample line bundles, as explained in Remark 4.35.

Proposition 6.8.
Let $f \in \mathsf{AV}_{/k}(X,Y)$ be a homomorphism, $\mathcal{M}$ a line bundle on Y and let $\mathcal{L} \overset{\text{def}}{=} f^* \mathcal{M}$. Then $\varphi_{\mathcal{L}}$ is given by the composition $X \xrightarrow{f} Y \xrightarrow{\varphi_{\mathcal{M}}} Y^t \xrightarrow{f^t} X^t$.

Proof. We use that $\varphi_{\mathcal{L}}$ is the ***unique*** morphism satisfying

$$(\mathrm{id}_X \times \varphi_{\mathcal{L}})^* \mathcal{P}_X = \Lambda(\mathcal{L})$$

as mentioned above. One now computes

$$\begin{aligned}(\mathrm{id}_X \times (f^t \circ \varphi_{\mathcal{M}} \circ f))^* \mathcal{P}_X &\cong (\mathrm{id}_X \times f)^* (\mathrm{id}_X \times \varphi_{\mathcal{M}})^* (\mathrm{id}_X \times f^t)^* \mathcal{P}_X \\ &\cong (\mathrm{id}_X \times f)^* (\mathrm{id}_X \times \varphi_{\mathcal{M}})^* (f \times \mathrm{id}_{Y^t})^* \mathcal{P}_Y \\ &\cong (\mathrm{id}_X \times f)^* (f \times \varphi_{\mathcal{M}})^* \mathcal{P}_Y \\ &\cong (\mathrm{id}_X \times f)^* (f \times \mathrm{id}_Y)^* (\mathrm{id}_Y \times \varphi_{\mathcal{M}})^* \mathcal{P}_Y \\ &\cong (f \times f)^* \Lambda(\mathcal{M}) \\ &\cong \Lambda(\mathcal{L})\end{aligned} \tag{6.3}$$

where the last isomorphism holds according to Lemma 4.28 as $\mathcal{L} \overset{\text{def}}{=} f^* \mathcal{M}$. □

Lemma 6.9.
Let $Y \xrightarrow{i} X \in \mathsf{AV}_{/k}(Y,X)$ be a closed embedding and let $X \xrightarrow{\lambda} X^t$ be a polarization of X.
Then $i^*(\lambda) \overset{\text{def}}{=} \; Y \xrightarrow{i^t \circ \lambda \circ i} Y^t$ is a polarization of Y.

Proof. Choose a field extension $K \mid k$ and an ample line bundle $\mathcal{L}$ on X_K satisfying $\lambda_K = \varphi_{\mathcal{L}}$.
Let $\mathcal{L}_| \overset{\text{def}}{=} i_K^* \mathcal{L}$ be the restriction of $\mathcal{L}$ onto Y_K. Then $\mathcal{L}_|$ is ample again, as pulling back line bundles along closed embeddings preserves ampleness according to Proposition 4.24.
One now computes:

$$(i^t \circ \lambda \circ i)_K = \underbrace{(i^t)_K}_{\overset{6.5}{=} (i_K)^t} \circ \underbrace{\lambda_K}_{= \varphi_{\mathcal{L}}} \circ i_K = (i_K)^t \circ \varphi_{\mathcal{L}} \circ i_K \overset{6.8}{=} \varphi_{(\mathcal{L}_|)}.$$

□

Jacobian varieties

We finish the discussion of picard schemes by shortly introducing the notion of *Jacobians* associated to curves, as the term will come up in applications later again.
By *curve* we simply mean variety of dimension 1.
Given a *proper, smooth curve*$_{/k}$ C of *genus* g one easily checks that conditions (i)-(iii) from the beginning of this chapter are satisfied, if C admits a rational point $\operatorname{Spec} k \xrightarrow{\epsilon} C$.
We know that the rigidified picard functor is representable by a scheme in this case and we denote by $\mathcal{J} \overset{\text{def}}{=} \mathcal{J}_{C/k} \overset{\text{def}}{=} \operatorname{Pic}^0_{C/k,\epsilon}$ the identity component of the representing scheme and call it the *Jacobian variety* associated to C.
As in the case of the dual of an abelian variety, one can show that $\mathcal{J}$ admits the structure of an abelian variety of dimension $\dim \mathcal{J} = g$ the genus of the curve.

Note that we assumed our curve to admit a rational point so that we were able to rigidify the picard functor. This is not strictly necessary:
One could also *sheafify* the usual picard functor $\operatorname{Pic}_{C/k}$ with respect to the fppf-site to obtain a representable functor that is isomorphic to the rigidified picard functor if the curve under consideration admits a rational point.
The scheme representing this sheafified functor will also always carry the structure of an abelian variety.

7 The endomorphism ring

Let X and Y be abelian varieties over a field k.
Recall from Remark 4.6 that if $X \overset{f}{\underset{g}{\rightrightarrows}} Y$ are homomorphisms, one can build the homomorphism $X \xrightarrow{f+g} Y$ given on points by $x \longmapsto f(x) + g(x)$, i.e.

$$\begin{tikzcd}
X \arrow[rr, "f+g"] \arrow[dr, "f\times g"'] & & Y \\
& Y \times_k Y \arrow[ur, "m_Y"'] &
\end{tikzcd}$$

is a commutative triangle$_{/k}$. This construction endows the set $\mathrm{Hom}_{\mathsf{AV}_{/k}}(X, Y)$ of homomorphism of group schemes$_{/k}$ between two abelian varieties X and Y with the structure of an abelian group.
In the case $X = Y$ one finds that $\mathrm{End}_{\mathsf{AV}_{/k}}(X) = \mathrm{Hom}_{\mathsf{AV}_{/k}}(X, X)$ carries a natural ring-structure with composition as multiplication.

Notation.
We will sometimes suppress the index $\mathsf{AV}_{/k}$ if it is to be understood from the context. So we will simply write $\mathrm{Hom}(X, Y)$, $\mathrm{End}(X)$ and so on instead of $\mathrm{Hom}_{\mathsf{AV}_{/k}}(X, Y)$ and $\mathrm{End}_{\mathsf{AV}_{/k}}(X)$ et cetera.

Poincaré Splitting Theorem

We are now finally able to give a complete proof of the

Poincaré Splitting Theorem 7.1.
Let X be an abelian variety$_{/k}$. If $Y \overset{i}{\hookrightarrow} X$ is an abelian subvariety, there exists an abelian subvariety $Z \hookrightarrow X$ such that the homomorphism $Y \times_k Z \longrightarrow X$ given on points by $(y, z) \longmapsto y + z$ is an isogeny, that is: $Y + Z = X$ and $Y \cap Z$ is finite.

In order to proof the Poincaré Splitting Theorem, we will use the following well-known fact, a proof of which can be found in [Vakil, 11.4.1. Theorem] for example:

Reminder 7.2.
Suppose $X \xrightarrow{\pi} Y$ is a morphism of irreducible k-varieties. Then there exists a nonempty open subset $V \subseteq Y$ such that the fiber $\pi^{-1}(q)$ is either of pure dimension $\dim X - \dim Y$ or empty, for all $q \in V$.

Proof. Choose any polarization $X \xrightarrow{\lambda} X^t$ and set $W \overset{\mathrm{def}}{=} \ker(X \xrightarrow{\lambda} X^t \xrightarrow{i^t} Y^t)$.
Then we know by Lemma 6.9 that $i^*\lambda = i^t \circ \lambda \circ i : Y \to Y^t$ is a polarization again, hence $Y \cap W = \ker i^*\lambda$ is *finite*.
Let $Z \overset{\mathrm{def}}{=} W^0_{\mathrm{red}}$. Thus Z is an abelian variety by Theorem 4.8.
Note that

$$\begin{tikzcd}
Y \cap Z \arrow[r] \arrow[d, hook, "cl."'] \arrow[dr, phantom, "\lrcorner", very near start] & Z \arrow[d, hook, "cl."'] \\
Y \cap W \arrow[r] & W
\end{tikzcd}$$

is cartesian. As $Z \hookrightarrow W$ is a closed embedding, so is $Z \cap Y \hookrightarrow Z \cap W$ by base change.
It follows that $Y \cap Z$ is finite as the composition of finite morphisms stays finite and as closed embeddings are finite.
Hence $(Y \cap Z) \times_k (Y \cap Z)$ also is finite as

$$\begin{tikzcd}
(Y \cap Z) \times_k (Y \cap Z) \arrow[r] \arrow[d] \arrow[dr, phantom, "\lrcorner"] & (Y \cap Z) \arrow[d] \\
(Y \cap Z) \arrow[r] & \operatorname{Spec} k
\end{tikzcd}$$

is cartesian and as finite morphisms are stable under base change and composition.
Furthermore we know that $\dim Z = \dim W^0 \overset{3.13}{=} \dim W = \dim X - \dim Y$ by Remark 7.2:
We can calculate the dimension of W after extension of the base field and thus assume k to be algebraically closed for this part. Then W is homeomorphic to the fiber above *any* closed point of Y^t via *translation*, as the set of closed points lies *very dense* in W in virtue of Proposition 2.11 - implying that the desired formula holds for the fiber above some closed point.
Since $\dim(Y \times_k Z) = \dim Y + \dim Z = \dim X$, it follows that $Y \times_k Z \longrightarrow X, (y, z) \longmapsto y + z$ is an isogeny, as $\ker(Y \times_k Z \longrightarrow X) \subseteq (Y \cap Z) \times_k (Y \cap Z)$, as easily checked on points, is finite.

□

Definition 7.3.
A non-zero abelian variety$_{/k}$ X is said to be *simple*$_{/k}$ if X has no abelian subvarieties$_{/k}$ other than 0 and X.
X is *elementary*$_{/k}$ if X is isogenous$_{/k}$ to a power of a simple$_{/k}$ abelian variety.

Lemma 7.4.
Let X and Y be two abelian varieties that are simple$_{/k}$ and let $X \xrightarrow{f} Y$ be a homomorphism. Then either $f = 0$ or f is an isogeny.

Proof. If $f \neq 0$, one has that $\ker f \hookrightarrow X$ is an abelian subvariety that is not X so that $\ker f = 0$ as X is simple.
One furthermore knows that the scheme-theoretic image of f is an abelian subvariety of Y according to Proposition 4.7. $f \neq 0$ then implies $\operatorname{im} f \neq 0$, i.e. $\operatorname{im} f = Y$ as Y is simple. We therefore obtain that f is a surjective homomorphism of abelian varieties with trivial, in particular finite, kernel, hence an isogeny by Proposition 5.3 as claimed. □

Corollary 7.5.
A non-zero abelian variety$_{/k}$ is isogenous to a product of simple$_{/k}$ abelian varieties:
There exist simple$_{/k}$ abelian varieties $Y_1, \dots, Y_n$, pairwise not isogenous$_{/k}$, and positive integers $m_1, \dots, m_n$ such that

$$X \sim_k \prod_{j=1}^{n} Y_j^{m_j}$$

and, up to permutation, the factors Y_j are unique up to isogeny$_{/k}$ and the corresponding multiplicities m_j are uniquely determined.

Proof. The existence of such a decomposition follows from the Poincaré Splitting Theorem 7.1.
The Uniqueness statement is a consequence of Lemma 7.4.

□

If $n \in \mathbb{Z}$ and $f \in \mathsf{AV}_{/k}(X, Y)$, we have that $n \cdot f = [n]_Y \circ f = f \circ [n]_X$. We know that $[n]$ is an isogeny for $n \neq 0$ by Proposition 5.7, hence in particular *surjective*. $\operatorname{Hom}(X, Y)$ therefore is *torsion-free* and we introduce the

Notation.

$$\operatorname{Hom}^0(X, Y) \overset{\text{def}}{=} \operatorname{Hom}(X, Y) \otimes_{\mathbb{Z}} \mathbb{Q} \text{ and } \operatorname{End}^0(X) \overset{\text{def}}{=} \operatorname{End}(X) \otimes_{\mathbb{Z}} \mathbb{Q}$$

$\operatorname{End}^0(X)$ hence is a $\mathbb{Q}$-algebra, which will often simply be referred to as the *endomorphism algebra* of X.

Definition 7.6.
The category of *abelian varieties*$_{/k}$ *up to isogeny* is the category $\mathbb{Q}\,\mathsf{AV}_{/k}$ with objects abelian varieties$_{/k}$ and morphisms $\mathbb{Q}\,\mathsf{AV}_{/k}(X, Y) \overset{\text{def}}{=} \operatorname{Hom}^0_{\mathsf{AV}_{/k}}(X, Y) = \mathsf{AV}_{/k}(X, Y) \otimes_{\mathbb{Z}} \mathbb{Q}$.
An isomorphism $f \in \mathbb{Q}\,\mathsf{AV}_{/k}(X, Y)$ is called *quasi-isogeny*$_{/k}$.

Remark 7.7.
One can show that $\mathbb{Q}\,\mathsf{AV}_{/k}$ is equivalent to the category obtained by *localizing* $\mathsf{AV}_{/k}$ at all *isogenies*.
Note that $f \in \mathbb{Q}\,\mathsf{AV}_{/k}(X, Y)$ is a quasi-isogeny if and only if there is some $n \in \mathbb{N}_{>0}$ such that nf is an isogeny $X \xrightarrow{nf} Y$.
Therefore two abelian varieties$_{/k}$ X and Y are isogenous$_{/k}$ if and only if they are isomorphic when considered as objects of $\mathbb{Q}\,\mathsf{AV}_{/k}$.

Corollary 7.8.
If X is simple$_{/k}$, then $\mathrm{End}^0(X)$ is a division algebra. For arbitrary X with decomposition as in Corollary 7.5, we have

$$\mathrm{End}^0(X) \cong \mathrm{M}_{m_1}(D_1) \times \ldots \times \mathrm{M}_{m_n}(D_n)$$

where we wrote $D_i \overset{\text{def}}{=} \mathrm{End}^0(Y_i)$.
In particular, $\mathrm{End}^0(X)$ is a semi-simple $\mathbb{Q}$-algebra for every abelian variety$_{/k}$ X.

Proof. We know that any non-zero endomorphism of a *simple* abelian variety is an *isogeny*, hence an isomorphism in $\mathbb{Q}\,\mathsf{AV}_{/k}$ in virtue of Lemma 7.4. Thus, whenever X is simple, $\mathrm{End}^0(X)$ is a *division algebra*.
The computation

$$\begin{aligned} \mathrm{End}^0(X) &\cong \mathrm{Hom}^0(\prod_i Y_i^{m_i}, \prod_j Y_j^{m_j}) \\ &\cong \prod_{i,j} \mathrm{Hom}^0(Y_i^{m_i}, Y_j^{m_j}) \\ &\overset{7.4}{\cong} \prod_i \mathrm{Hom}^0(Y_i^{m_i}, Y_i^{m_i}) \\ &\cong \prod_i \mathrm{M}_{m_i}(D_i) \end{aligned} \tag{7.1}$$

proves the second claim. □

The Poincaré Splitting Theorem 7.1 together with the other results of this section show us that - as long as one is willing to identify *isogenous* abelian varieties - one has a fairly good understanding of how abelian varieties behave like.
One problem however is that we do not really know how to effectively decompose (up to isogeny) a given abelian variety into its simple factors.
The second part of this bachelor thesis tries to investigate this problem in certain special cases as already stated in the introduction.
We are now leaving the *theoretical* part though and thus will not prove any more results but merely state things one *could* prove and show how we can apply those results.

Tate modules and characteristic polynomials

Definition 7.9.
Let X be an abelian variety$_{/k}$, k_s a separable closure of k, and let $l \neq \operatorname{char} k$ be a prime number.
The *Tate-l-module* of X, denoted $\mathrm{T}_l X$, is given as

$$\mathrm{T}_l X \overset{\text{def}}{=} \varprojlim \left(\{0\} \xleftarrow{l} X[l](k_s) \xleftarrow{l} X[l^2](k_s) \xleftarrow{l} X[l^3](k_s) \xleftarrow{l} \cdots\right)$$

where the notation $X[l^n]$ was introduced in 3.5 and where the transition maps are given via multiplication with l.
As $X[l^n](k_s)$ is l^n-torsion, it is a $\mathbb{Z}/l^n\,\mathbb{Z}$-module, so that $\mathrm{T}_l X$ carries a natural $\mathbb{Z}_l$-module structure.
We furthermore set

$$\mathrm{V}_l X \overset{\text{def}}{=} \mathrm{T}_l X \otimes_{\mathbb{Z}_l} \mathbb{Q}_l\,.$$

Remark 7.10.
Note that each $X[l^n](k_s)$ carries a natural *galois action* by $G_k \overset{\text{def}}{=} \mathrm{Gal}(k_s/k)$ which is compatible with the transition maps. Hence $\mathrm{T}_l X$ carries a natural G_k-action as well.

Similarly, any homomorphism $X \xrightarrow{f} Y$ sends l^n-torsion to l^n-torsion, thus induces a morphism $X[l^n](k_s) \xrightarrow{f[l^n]} Y[l^n](k_n)$ compatible with the transition maps. We thus see that f induces a $\mathbb{Z}_l$-linear morphism

$$\mathrm{T}_l f \overset{\text{def}}{=} \varprojlim_n f[l^n] : \mathrm{T}_l X \longrightarrow \mathrm{T}_l Y.$$

Theorem 7.11.
Let X and Y be abelian varieties$_{/k}$.
If char $k \neq l$ is a prime number, then the $\mathbb{Z}_l$-linear map

$$\mathrm{Hom}(X,Y) \otimes \mathbb{Z}_l \xrightarrow{\mathrm{T}_l} \mathrm{Hom}_{\mathbb{Z}_l}(\mathrm{T}_l X, \mathrm{T}_l Y)$$

given by $f \otimes c \longmapsto c \cdot \mathrm{T}_l(f)$ is injective and has a torsion-free cokernel.

Proof. [AV, (12.10) Theorem] □

Corollary 7.12.
If X and Y are abelian varieties$_{/k}$, then $\mathrm{Hom}(X,Y)$ is a free $\mathbb{Z}$-module of rank at most $4\dim(X)\dim(Y)$. In particular $\mathrm{End}^0(X)$ is a finite-dimensional semi-simple $\mathbb{Q}$-algebra of dimension at most $4\dim(X)^2$.

Proof. We already remarked that $\mathrm{Hom}(X,Y)$ is torsion-free in the above. Theorem 7.11 tells us that $\mathrm{Hom}(X,Y) \otimes \mathbb{Z}_l$ injects into $\mathrm{Hom}_{\mathbb{Z}_l}(\mathrm{T}_l X, \mathrm{T}_l Y)$, which is free over $\mathbb{Z}_l$ of rank $4\dim(X)\dim(Y)$ by Corollary 5.9. Hence $\mathrm{Hom}(X,Y)$ is a torsion-free, finitely generated module over a principal ideal domain, hence free. □

Proposition 7.13.
Let $X \xrightarrow{f} X$ be an endomorphism of an abelian variety$_{/k}$ and $\mathrm{T}_l X \xrightarrow{\mathrm{T}_l(f)} \mathrm{T}_l X$ the induced endomorphism of $\mathrm{T}_l X$ where $l \neq$ char k. The characteristic polynomial $P(t) = \det(t - \mathrm{T}_l(f))$ of $\mathrm{T}_l(f)$ is then *monic* of degree $\deg P(t) = 2 \cdot \dim X$, has *integral* coefficient and satisfies $P(f) = 0$.
$P(t)$ furthermore does *not* depent on the choice of prime $l \neq$ char k.

Proof. [AV, (12.18) Theorem]. □

Definition 7.14.
The above polynomial $P(t) = \sum_{i=0}^{2g} a_i t^i \in \mathbb{Z}[t]$ associated to an endomorphism $X \xrightarrow{f} X$ is called *characteristic polynomial* of f. One furthermore calls a_0 the *norm* of f and $-a_{g-1}$ the *trace* of f.

8 Abelian varieties over finite fields

In this section we will fix a finite field $\mathbb{F}$, an algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$ and write $p \overset{\text{def}}{=} \operatorname{char} \mathbb{F}$, $q \overset{\text{def}}{=} \# \mathbb{F}$.
We will denote by $\mathbb{F}_{q^n}$ the *unique* field extension of $\mathbb{F} = \mathbb{F}_q$ inside $\overline{\mathbb{F}}$ with q^n elements.

X and Y will denote *abelian varieties*$_{/\mathbb{F}}$ of dimension $\dim X = g_X$ and $\dim Y = g_Y$ respectively in this section if not explicitly stated otherwise.
If we only need one of the varieties stated above we will denote its dimension more simply by g.
One major technical tool in the finite field case is – as one might expect – the *geometric Frobenius*:

Definition 8.1.
Let X be any scheme$_{/\mathbb{F}}$. The morphism$_{/\mathbb{F}}$ $X \xrightarrow{\pi_X} X$ defined to be the identity on the underlying topological space and given on sections via $f \longmapsto f^q$ is called *geometric Frobenius*.
We also write $\pi_{X/\mathbb{F}}$ if we want to stress the ground field.

Remark.
Note that one has $\pi_{X_{\mathbb{F}_{q^n}}/\mathbb{F}_{q^n}} = \pi^n_{X/\mathbb{F}_q} \times_{\mathbb{F}_q} \mathbb{F}_{q^n}$.

Returning to the case of X being an abelian variety, one can show that π_X carries the origin into the origin and hence defines an endomorphism. One can even show the following

Lemma 8.2.
The geometric Frobenius $X \xrightarrow{\pi_X} X$ is an *isogeny*.

Proof. [AV, (16.2)]. □

We can thus make the

Definition 8.3.
The *characteristic polynomial of Frobenius* is given by $f_X \overset{\text{def}}{=} P_{\pi_X}$ as previously defined in 7.14.

Proposition 8.4.

(i) Every complex root $\alpha \in \mathbb{C}$ of f_X has absolute value $|\alpha| = \sqrt{q}$.

(ii) If $\alpha \in \mathbb{C}$ is a complex root of f_X then so is $\bar{\alpha} \overset{\text{def}}{=} \frac{q}{\alpha}$ and the two roots occur with the same multiplicity. If $\alpha = \pm\sqrt{q}$ occurs as a root then its multiplicity is even.

Proof. [AV, (16.4) Proposition] □

Definition 8.5.
Let X be a scheme$_{/\mathbb{F}}$ of finite type. The *(Hasse-Weil) ζ-function* of X is defined by

$$\zeta(X;t) \overset{\text{def}}{=} \exp\left(\sum_{n=1}^{\infty} \#X(\mathbb{F}_{q^n}) \cdot \frac{t^n}{n}\right) \in \mathbb{Q}[[t]]$$

Alternatively one has

$$\zeta(X;t) = \prod_{x \in |X|_{cl}} (1 - t^{\deg x})^{-1}$$

where $|X|_{cl}$ denoted the set of closed points of X and $\deg x = [\kappa(x) : \mathbb{F}]$.

Theorem 8.6.
Let $\{\alpha_1, ..., \alpha_{2g}\}$ denote the multiset of complex roots of the characteristic polynomial f_X, so that we have $f_X = \prod_{j=1}^{2g}(t-\alpha_j)$. If I is a subset of $\{1, ..., 2g\}$, define $\alpha_I \overset{\text{def}}{=} \prod_{i\in I}\alpha_i$.

(i) For any $n \in \mathbb{N}_{>0}$ we have

$$\#X(\mathbb{F}_{q^n}) = \prod_{j=1}^{2g}(1-\alpha_j^n) = \sum_{j=0}^{2g}(-1)^j \mathrm{tr}(\pi_X^n; \wedge^j V_l X),$$

where l is any prime number different from p and where $\mathrm{tr}(\pi_X^n; \wedge^j V_l X)$ denotes the trace of the automorphism $\wedge^k V_l(\pi_X^n)$ of $\wedge^k V_l$.

(ii) The ζ-function of X is given by

$$\zeta(X;t) = \prod_{j=0}^{2g} P_j^{(-1)^{j+1}} = \frac{P_1 \cdot P_3 \cdot ... \cdot P_{2g-1}}{P_0 \cdot P_2 \cdot ... \cdot P_{2g}}$$

where $P_j \in \mathbb{Z}[t]$ is the polynomial given by

$$P_j = \prod_{I\subseteq\{1,...,2g\},\#I=j}(1-t\cdot\alpha_I) = \det(\mathrm{id}-t\cdot\pi_X; \wedge^j V_l X),$$

i.e the reciprocal characteristic polynomial of $\wedge^j V_l(\pi_X)$.

(iii) The ζ-function satisfies the functional equation $\zeta(X; \frac{1}{q^g t}) = \zeta(X;t)$.

A very important result closely connected to Theorem 8.6 for the case of *Jacobians of curves* is the following

Theorem 8.7.
Let C be a *smooth, complete* curve of genus g over $\mathbb{F}$ and let $\mathcal{J}$ be the Jacobian of C. Let $\{\alpha_1, \ldots, \alpha_{2g}\}$ denote the multiset of complex roots of the characteristic polynomial f of the geometric Frobenius of $\mathcal{J}$. Then

$$\zeta(C;t) = \frac{\prod_{i=1}^{2g}(1-\alpha_i\cdot t)}{(1-t)(1-q\cdot t)}.$$

Proof. [AV, (16.11) Theorem]. □

Tate's Theorem 8.8.
Let $l \neq p = \mathrm{char}\,\mathbb{F}$ be any prime number. Then the natural map

$$\mathbb{Z}_l \otimes \mathrm{Hom}_{\mathsf{AV}_{/\mathbb{F}}}(X,Y) \longrightarrow \mathrm{Hom}_{\mathrm{Gal}(\bar{k}/k)}(\mathrm{T}_l X, \mathrm{T}_l Y)$$

is an isomorphism.

Corollary 8.9.
The following are equivalent:

(i) $X \sim_{\mathbb{F}} Y$

(ii) $\mathrm{V}_l X \cong \mathrm{V}_l Y$ as representations of $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ for some prime number $l \neq p$

(iii) $\mathrm{V}_l X \cong \mathrm{V}_l Y$ as representations of $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ for all prime numbers $l \neq p$

(iv) $f_X = f_Y$

(v) $\zeta(X;t) = \zeta(Y;t)$

(vi) $\#X(\mathbb{F}') = \#Y(\mathbb{F}')$ for all finite field extensions $\mathbb{F}' \mid \mathbb{F}$.

Abelian varieties up to isogeny

Definition 8.10.
Let q be a power of a prime number. A *q-Weil number* is an algebraic integer π such that $|\iota(\pi)| = \sqrt{q}$ for all embeddings $\mathbb{Q}[\pi] \overset{\iota}{\hookrightarrow} \mathbb{C}$. Two q-Weil numbers π and π' are called *conjugate* if they share the same minimal polynomial over $\mathbb{Q}$.

Remark.
Note that Proposition 8.4 implies that every root of f_X, in particular π_X, is a q-Weil number.

Lemma 8.11.
Let X and Y be *simple* abelian varieties$_{/\mathbb{F}}$. Then $X \sim_{\mathbb{F}} Y$ if and only if the associated q-Weil numbers π_X and π_Y are conjugate.

Theorem of Honda-Tate 8.12.
For any q-Weil number π there exists a simple abelian variety$_{/\mathbb{F}}$ X such that π_X is conjugate to π.
Furthermore, the mapping $X \longmapsto \pi_X$ gives a bijection

$$\{\text{isogeny classes of simple abelian varieties}_{/\mathbb{F}}\} \overset{\sim}{\longleftrightarrow} \{\text{conjugacy classes of } q\text{-Weil numbers}\}$$

Moreover, the inverse of this mapping associated to a q-Weil number π a simple abelian variety$_{/\mathbb{F}}$ X such that f_X is a power of the minimal polynomial of π.

Proof. [AV, (16.41) Theorem of Honda-Tate]. □

Remark 8.13.
If π is a q-Weil number with minimal polynomial f_π and associated simple abelian variety X, Tate explains in his original paper in [Tate, §1. Remarques. 2)] that $f_X = f_\pi^m$ where $m = [E : F]^{\frac{1}{2}}$. Here F is the number field $\mathbb{Q}(\pi)$ and E is the division algebra $\mathrm{End}^0(X)$.
Tate moreover explains in [Tate, §1 Théorème 1] how to compute the *invariant* in $\mathbb{Q}\,/\,\mathbb{Z}$ of E in the *Brauer group* F, namely

- $\mathrm{inv}_v E \equiv 2$ for all real places v, if existent
- $\mathrm{inv}_v E \equiv \frac{v(\pi)}{v(q)} \cdot [F_v : \mathbb{Q}_p]$ for all places v lying above p
- $\mathrm{inv}_v E \equiv 0$ for all remaining places v

Applications

The *Poincaré Splitting Theorem* suggests the following

Question.
Given an abelian variety$_{/k}$ X, can one *explicitly* determine the factors Y_j and exponents m_j of the decomposition of X into *simple* abelian subvarieties up to isogeny given by

$$X \sim_k \prod_{j=1}^{n} Y_j^{m_j} \tag{8.1}$$

as in Corollary 7.5?

We try to apply the results of the preceding section to give some *partial* answers to this question for Jacobians of curves:

Let C be a *smooth, complete* curve of genus g over $\mathbb{F}$. Then Theorem 8.7 tells us that the ζ-function of C is of the form

$$\zeta(C;t) = \frac{\prod_{i=1}^{2g}(1-\alpha_i \cdot t)}{(1-t)(1-q\cdot t)} \tag{8.2}$$

where $\{\alpha_1, \ldots, \alpha_{2g}\}$ denotes the multiset of roots of $f_{\mathcal{J}}$, $\mathcal{J}$ denoting the *Jacobian* of C.
As we are especially interested in the nominator of $\zeta(C;t)$, we write

$$\mathrm{L}(C;t) \overset{\text{def}}{=} \prod_{i=1}^{2g}(1-\alpha_i \cdot t) \tag{8.3}$$

and call $\mathrm{L}(C;t)$ the *L-Polynomial of C* in the following.

Honda-Tate theory now suggests the following

Idea. Let C be a *smooth, complete curve* of genus g over a finite field $\mathbb{F}$.
Suppose we *explicitly* knew the L-Polynomial $\mathrm{L}(C;t) \in \mathbb{Z}[t]$ of C as well as its decomposition into irreducible factors

$$\mathrm{L}(C;t) = f_1^{n_1} \cdot \ldots \cdot f_l^{n_l}.$$

We know that the roots of $\mathrm{L}(C;t)$ are reciprocals of q-Weil numbers according to Proposition 8.4 and hence determine *simple* abelian subvarieties of the Jacobian $\mathcal{J}$ in virtue of the Honda-Tate Theorem 8.12.
Two roots α_i and α_j determine the same isogeny-class if and only if they are conjugated, i.e share the same *minimal polynomial*. That is: If and only if they belong to the same irreducible factor of $f_{\mathcal{J}}$ or equivalently, if and only if α_i^{-1} and α_j^{-1} share the same irreducible factor of $\mathrm{L}(C;t)$.

We thus observe that the *simple* factors $\{Y_j\}_j$ of $\mathcal{J}$ are in bijection with the *irreducible factors* $\{f_j\}_j$ above and those f_j determine the corresponding factors up to isogeny according to Corollary 8.9.
We would also like to compute the exponents m_j of (8.1). This can be achieved using the explicit formulas given in Remark 8.13, by means of *class field theory* as we will explain later. □

We realized this idea in a first algorithm (implemented in MAGMA) that is able to compute a set of *complete invariants* of a Jacobian of a curve *given* the L-Polynomial of the curve.

In order to effectively apply this algorithm we still need to explicitly determine the L-Polynomial of curves. This is where the second algorithm of this thesis comes into play:
It is well-known that *smooth projective curves*$_{/k}$ correspond to *finitely generated field extensions $K \mid k$ of transcendence degree 1* (see for example [Stacks, 0BY1]).
Galovich and *Rosen* investigated in [GR] ζ-functions of a *special class* of such extensions over finite fields $\mathbb{F}$, namely of *Carlitz-cyclotomic field extensions*, which might be thought of as function field analogues of *Cyclotomic number fields*.
They in particular gave rather explicit formulas for computing the ζ-function of such field extensions - which coincides with the ζ-function associated to the Jacobian of the corresponding curve. The algorithm exploits these formulas to compute the ζ-functions attached to *certain* Carlitz-cyclotomic field extensions as will be explained later.
We also took a look [Shiomi] in order to implement the algorithm.

We first explain how to reconstruct the exponents m_j from the observation made in Remark 8.13.
This is based on results around *class field theory*, namely:

Lemma 8.14.
If F is a number field and A is a central, simple F-algebra, then the index of A is the least common multiple of the denominators of the local invariants $\{\mathrm{inv}_v(A \otimes_F F_v)\}_{v\in\Sigma}$, where Σ denotes the set of all places of F.

Proof. [Pierce, 18.6. Proposition]. □

Combining Lemma 8.14 with the formulas stated in Remark 8.13 thus tells us that

$$m^2 = [E : F] = \mathrm{lcm}\{b \in \mathbb{Z} \mid \exists\, v \in \Sigma : \mathrm{inv}_v E \equiv \frac{a}{b} \in \mathbb{Q}/\mathbb{Z}\}$$

and that the local invariants $\mathrm{inv}_v E$ are determined by essentially *global* arithmetic properties of the number field F - i.e. by the formulas given in Remark 8.13.
Note that the *geometric* information of how often an abelian subvariety occurs in the decomposition of a given abelian variety over a field of *positive characteristic* is encoded in global arithmetic phenomena in *characteristic zero*!
The computer algebra package MAGMA offers algorithms able to compute the desired invariants associated to the number field F, which explains how one obtains the first algorithm.

Main algorithm

We now explain how the results of Galovich and Rosen can be used to determine the ζ-function attached to certain Carlitz-cyclotomic field extensions.
We first recall basic definitions and results involved (to be found in [Rosen] for example):

Cyclotomic function fields

Let k be a field of rational functions over our fixed finite field $\mathbb{F} = \mathbb{F}_q$. Fix a generator $t \in k$ such that $k = \mathbb{F}(t)$ and let $A \overset{\text{def}}{=} \mathbb{F}[t]$. Fix an algebraic closure $\overline{k}$ of k. Then $\Lambda \overset{\text{def}}{=} \overline{k}$ becomes a A-module via the action

$$m \cdot u \overset{\text{def}}{=} m(\mathrm{Fr}_k + \phi)(u)$$

where $u \in \overline{k}, m \in A,\ \overline{k} \xrightarrow{\mathrm{Fr}_k} \overline{k}\ , u \longmapsto u^q$ is the *Frobenius* and where $\overline{k} \xrightarrow{\ \phi\ } \overline{k}\ , u \longmapsto t \cdot u$ is given via multiplication by t.
Carlitz moreover showed that the set $\Lambda[m] = \{\lambda \in \Lambda \mid m \cdot \lambda = 0\}$ of m torsion points under this action is isomorphic to $A/(m)$ as an A-module and that the field $K_m \overset{\text{def}}{=} k(\Lambda[m])$ obtained by adjoining $\Lambda[m]$ to k is an *abelian* Galois extension with Galois group $\mathrm{Gal}(k(\Lambda[m])/k) \cong (A/(m))^{\times}$. The field K_m is called *Carlitz-cyclotomic* field extension (associated to m).

One has the product decomposition of the ζ-function of the integral closure $\mathcal{O}_m \overset{\text{def}}{=} \overline{A}^{K_m}$ of A in K_m

$$\zeta(\mathcal{O}_m; s) = \prod_{\chi} \mathrm{L}(\chi\,; s)$$

where the product runs over all *primitive* Dirichlet characters of $(A/(m))^{\times}$.
It furthermore holds that

$$\mathrm{L}(\chi\,; s) = \sum_f \frac{\chi(f)}{q^{|f|\cdot s}}$$

where the sum runs over all *monic* polynomials $f \in A$ and where $|f| \overset{\text{def}}{=} \deg f$.
We try to exploit this decomposition in order to compute the ζ-function of $\mathcal{O}_m$.
We thus want to understand the primitive Dirichlet characters χ of $(A/(m))^{\times}$.
We will now *restrict* to Carlitz extensions given by $m \in A$ that is *squarefree*, as we then obtain:

Let $m = f_1 \cdot \ldots \cdot f_n$ be the factorization into the pairwise different irreducible polynomials f_i with $d_i \overset{\text{def}}{=} |f_i| = \deg f_i$. Then $A/(m) = A/(f_1 \cdot \ldots \cdot f_n) \cong \prod_i A/(f_i)$. As f_i is irreducible, $A/(f_i)$ is the field extension $\mathbb{F}_{q^{d_i}}$ of $\mathbb{F}$. We thus see that $(A/(m))^{\times} \cong (\prod_i \mathbb{F}_{q^{d_i}})^{\times} \cong \prod_i \mathbb{F}_{q^{d_i}}^{\times} \cong \prod_i \mathbb{Z}/((q^{d_i} - 1)\,\mathbb{Z})$ is a product of cyclic groups.

When restricting to squarefree m, we thus only need to effectively compute the (primitive) characters of a product of cyclic groups.
This is a rather easy combinatorial problem so that it's possible to calculate these characters in an algorithm with MAGMA.
A proof-of-concept implementation can be found at [GitHub, jacobians].
This implementation uses an action of $\mathrm{Gal}(\mathbb{Q}(\zeta_k)/\,\mathbb{Q})$ (where $k = \mathrm{lcm}\{q^{\deg f_i} - 1 | i = 1 \dots n\}$), which is given by $\sigma \curvearrowright \chi \overset{\text{def}}{=} \sigma \circ \chi$, on the set of characters to pre-decompose the L-Polynomial, which speeds up the computation time.

Experiments

Here are some examples computed with the implementation cited above.
The output consists of the following data:

- The choice of q and m
- The factorization of the L-Polynomial
- A set of complete invariants for the decomposition of $\mathcal{J}$ into simple parts according to Honda-Tate

The computations of the L-Polynomials carried out in this thesis confirm the computations done in [Troya] via a different approach that does not use the results by Galovich and Rosen.
Using the results by Galovich and Rosen yields a faster algorithm however. That is why we are able to explicitly compute examples (namely $q = 7, \deg m = 2$) the algorithm described in [Troya] did not perform well on.
The usage of Honda-Tate theory furthermore proves that the decompositions calculated describe the decomposition of the Poincaré Splitting Theorem.

Example ($q = 2, \deg m = 4$).

```
q:  2
m:  T^4 + T^3 + T^2 + T + 1
m irreducible: true
m squarefree:  true
Factorization of L:  [
    <4*T^4 + 6*T^3 + 5*T^2 + 3*T + 1, 3>,
    <16*T^8 + 16*T^7 + 8*T^6 + 10*T^5 + 11*T^4 + 5*T^3 + 2*T^2 + 2*T + 1, 1>,
    <16*T^8 + 8*T^7 + 16*T^6 + 4*T^5 + 9*T^4 + 2*T^3 + 4*T^2 + T + 1, 1>
]
Honda-Tate invariants:  [
    <4*T^4 + 6*T^3 + 5*T^2 + 3*T + 1, 3>,
    <16*T^8 + 16*T^7 + 8*T^6 + 10*T^5 + 11*T^4 + 5*T^3 + 2*T^2 + 2*T + 1, 1>,
    <16*T^8 + 8*T^7 + 16*T^6 + 4*T^5 + 9*T^4 + 2*T^3 + 4*T^2 + T + 1, 1>
]
```

Example ($q = 3, \deg m = 2$).

```
q:  3
m:  T^2 + 1
m irreducible: true
m squarefree:  true
Factorization of L:  [
    <9*T^4 - 2*T^2 + 1, 1>
]
Honda-Tate invariants:  [
    <9*T^4 - 2*T^2 + 1, 1>
]
```

Example ($q = 5, \deg m = 2$).

```
q:  5
m:  T^2 + 3
m irreducible: true
m squarefree:  true
Factorization of L:  [
    <5*T^2 - 4*T + 1, 1>,
    <25*T^4 - 8*T^2 + 1, 1>,
    <5*T^2 + 2*T + 1, 2>,
    <25*T^4 - 2*T^2 + 1, 2>
]
Honda-Tate invariants:  [
    <5*T^2 - 4*T + 1, 1>,
    <25*T^4 - 8*T^2 + 1, 1>,
    <5*T^2 + 2*T + 1, 2>,
    <25*T^4 - 2*T^2 + 1, 2>
]
```

Example ($q = 7, \deg m = 2$).

```
q:  7
m:  T^2 + T + 3
m irreducible: true
m squarefree:  true
Factorization of L:  [
    <7*T^2 - 4*T + 1, 1>,
    <7*T^2 + 4*T + 1, 3>,
    <7*T^2 - 2*T + 1, 4>,
    <2401*T^8 - 196*T^6 - 26*T^4 - 4*T^2 + 1, 1>,
    <5764801*T^16 + 1882384*T^14 + 201684*T^12 + 8624*T^10 + 422*T^8 + 176*T^6 +
        84*T^4 + 16*T^2 + 1, 1>
]
Honda-Tate invariants:  [
    <7*T^2 - 4*T + 1, 1>,
    <7*T^2 + 4*T + 1, 3>,
    <7*T^2 - 2*T + 1, 4>,
    <2401*T^8 - 196*T^6 - 26*T^4 - 4*T^2 + 1, 1>,
    <5764801*T^16 + 1882384*T^14 + 201684*T^12 + 8624*T^10 + 422*T^8 + 176*T^6 +
        84*T^4 + 16*T^2 + 1, 1>
]
```

Here is an example using *reducible* m, the computation of which took slightly longer than the other ones though.

Example ($q = 2, \deg m = 6$).

```
q:  2
m:  T^6 + T^4 + T^3 + T^2 + 1
m irreducible: false
m squarefree:  true
Factorization of L:  [
    <16*T^8 + 6*T^5 + T^4 + 3*T^3 + 1, 1>,
    <16*T^8 + 24*T^7 + 24*T^6 + 24*T^5 + 19*T^4 + 12*T^3 + 6*T^2 + 3*T + 1, 1>,
    <16*T^8 + 32*T^7 + 16*T^6 - 14*T^5 - 21*T^4 - 7*T^3 + 4*T^2 + 4*T + 1, 1>,
    <4096*T^24 + 6144*T^23 + 12288*T^22 + 12288*T^21 + 14336*T^20 + 11520*T^19 +
        10496*T^18 + 8160*T^17 + 6720*T^16 + 5568*T^15 + 4244*T^14 + 3468*T^13 +
        2357*T^12 + 1734*T^11 + 1061*T^10 + 696*T^9 + 420*T^8 + 255*T^7 +
        164*T^6 + 90*T^5 + 56*T^4 + 24*T^3 + 12*T^2 + 3*T + 1, 1>,
    <4*T^4 + 6*T^3 + 5*T^2 + 3*T + 1, 2>,
    <4096*T^24 + 8192*T^23 + 12288*T^22 + 18944*T^21 + 23552*T^20 + 25600*T^19 +
        27008*T^18 + 25984*T^17 + 23040*T^16 + 19624*T^15 + 15776*T^14 +
        11970*T^13 + 8675*T^12 + 5985*T^11 + 3944*T^10 + 2453*T^9 + 1440*T^8 +
        812*T^7 + 422*T^6 + 200*T^5 + 92*T^4 + 37*T^3 + 12*T^2 + 4*T + 1, 1>,
    <65536*T^32 + 327680*T^31 + 901120*T^30 + 1761280*T^29 + 2760704*T^28 +
        3717120*T^27 + 4490240*T^26 + 4986880*T^25 + 5164800*T^24 + 5034240*T^23
        + 4651840*T^22 + 4096480*T^21 + 3450896*T^20 + 2788880*T^19 +
        2167260*T^18 + 1621540*T^17 + 1168429*T^16 + 810770*T^15 + 541815*T^14 +
        348610*T^13 + 215681*T^12 + 128015*T^11 + 72685*T^10 + 39330*T^9 +
        20175*T^8 + 9740*T^7 + 4385*T^6 + 1815*T^5 + 674*T^4 + 215*T^3 + 55*T^2
        + 10*T + 1, 1>
]
Honda-Tate invariants:  [
    <16*T^8 + 6*T^5 + T^4 + 3*T^3 + 1, 1>,
    <16*T^8 + 24*T^7 + 24*T^6 + 24*T^5 + 19*T^4 + 12*T^3 + 6*T^2 + 3*T + 1, 1>,
    <16*T^8 + 32*T^7 + 16*T^6 - 14*T^5 - 21*T^4 - 7*T^3 + 4*T^2 + 4*T + 1, 1>,
    <4096*T^24 + 6144*T^23 + 12288*T^22 + 12288*T^21 + 14336*T^20 + 11520*T^19 +
        10496*T^18 + 8160*T^17 + 6720*T^16 + 5568*T^15 + 4244*T^14 + 3468*T^13 +
        2357*T^12 + 1734*T^11 + 1061*T^10 + 696*T^9 + 420*T^8 + 255*T^7 +
        164*T^6 + 90*T^5 + 56*T^4 + 24*T^3 + 12*T^2 + 3*T + 1, 1>,
    <4*T^4 + 6*T^3 + 5*T^2 + 3*T + 1, 2>,
    <4096*T^24 + 8192*T^23 + 12288*T^22 + 18944*T^21 + 23552*T^20 + 25600*T^19 +
        27008*T^18 + 25984*T^17 + 23040*T^16 + 19624*T^15 + 15776*T^14 +
        11970*T^13 + 8675*T^12 + 5985*T^11 + 3944*T^10 + 2453*T^9 + 1440*T^8 +
        812*T^7 + 422*T^6 + 200*T^5 + 92*T^4 + 37*T^3 + 12*T^2 + 4*T + 1, 1>,
    <65536*T^32 + 327680*T^31 + 901120*T^30 + 1761280*T^29 + 2760704*T^28 +
        3717120*T^27 + 4490240*T^26 + 4986880*T^25 + 5164800*T^24 + 5034240*T^23
        + 4651840*T^22 + 4096480*T^21 + 3450896*T^20 + 2788880*T^19 +
        2167260*T^18 + 1621540*T^17 + 1168429*T^16 + 810770*T^15 + 541815*T^14 +
        348610*T^13 + 215681*T^12 + 128015*T^11 + 72685*T^10 + 39330*T^9 +
        20175*T^8 + 9740*T^7 + 4385*T^6 + 1815*T^5 + 674*T^4 + 215*T^3 + 55*T^2
        + 10*T + 1, 1>
]
```

Bibliography

AV. B. Edixhoven, G. van der Geer, and B. Moonen. *Abelian Varieties*. 2019.

GR. S. Galovich and M. Rosen. *The Class Number of Cyclotomic Function Fields*. Journal of Number Theory. 1985.

EGA-IV. A. Grothendieck. *Éléments de géométrie algébrique: IV.Étude locale des schémas et de morphismes de schémas, Seconde partie*. Publications mathématiques de l'IHÉS. 1965.

GW. U. Görtz and T. Wedhorn. *Algebraic Geometry, Part 1: Schemes. With Examples and Exercises*. 2010.

Hartshorne. R. Hartshorne. *Algebraic Geometry*. 1977.

GitHub. T. Holzschuh. https://github.com/tholzschuh/jacobians. 2019.

Mumford. D. Mumford. *Abelian Varieties*. 2012.

Pierce. R. S. Pierce. *Associative Algebras*. 1982.

Rosen. M. Rosen. *Number Theory in Function Fields*. 2000.

Shiomi. D. Shiomi. *Ordinary cyclotomic function fields*. Journal of Number Theory. 2013.

Stacks. T. Stacks Project Authors. *Stacks Project*. `https://stacks.math.columbia.edu`. 2019.

Tate. J. T. Tate. *Classes d'isogénie des variétés abéliennes sur un corps fini*. Séminaire N. Bourbaki. 1968.

Troya. A. Troya. *The Weil conjectures for curves and the Carlitz module*. 2016.

Vakil. R. Vakil. *The Rising Sea: Foundations of Algebraic Geometry*. `http://math.stanford.edu/~vakil/216blog/index.html`. 2017.