ABELIAN VARIETIES

BRIAN CONRAD
LECTURE NOTES BY TONY FENG

CONTENTS

Disclaimer 3

1. Basic theory 4
   1.1. Group schemes 4
   1.2. Complex tori 5
   1.3. Link between complex abelian varieties and complex tori 6
   1.4. The Mordell-Weil Theorem 7
   1.5. Commutativity 8
   1.6. Torsion 10
   1.7. Rigidity 12

2. The Picard functor 15
   2.1. Overview 15
   2.2. Rigidification 15
   2.3. Representability 18
   2.4. Properties of Pic_{X/k} 19

3. Line bundles on abelian varieties 23
   3.1. Some fundamental tools 23
   3.2. The \( \phi \) construction 24
   3.3. The Poincaré bundle 27
   3.4. Projectivity of abelian varieties 28

4. Torsion 34
   4.1. Multiplication by \( n \) 34
   4.2. Structure of the torsion subgroup 37

5. The dual abelian variety 42
   5.1. Smoothness 42
   5.2. Characterization of \( \phi_L \) 43
   5.3. The Néron-Severi group 47

6. Descent 49
   6.1. Motivation 49
   6.2. fpqc descent 50

7. More on the dual abelian variety 56
   7.1. Dual morphisms 56
   7.2. Cohomology of the Poincaré bundle 57
   7.3. Dual isogenies 60

1
DISCLAIMER

This document consists of lecture notes that I “live-TExed” from a course given by Brian Conrad at Stanford University in the Spring quarter of 2015.

I have taken the liberty of somewhat editing the notes. The most significant change is my incorporation of exercises, which were originally written up in separate problem sets by Professor Conrad. With the aid of Alessandro Maria Masullo (whose enthusiasm sparked our endeavor) I have also included solutions at the end. While all errors found here should be attributed to me, I emphasize that this last section is in particular entirely distinct from Professor Conrad's lectures, and is thus particularly prone to mistakes.

A few more remarks are in order. Two substitute lectures were delivered by Akshay Venkatesh and Zhiwei Yun. I also missed two lectures, and am grateful to Ho Chung Siu and David Sherman for providing me with notes to fill in the gaps.
1. Basic theory

1.1. Group schemes.

Definition 1.1.1. Let \( S \) be a scheme. An \( S \)-group (or group scheme over \( S \)) is a group object in the category of \( S \)-schemes. In other words, it is an \( S \)-scheme \( G \) equipped with an \( S \)-map \( m : G \times_S G \to G \) (multiplication), an \( S \) map \( i : G \to G \) (inversion), and a section \( e : S \to G \) such that the usual group axiom diagrams commute:

1. (Associativity)

\[
\begin{array}{ccc}
G \times G \times G & \xrightarrow{1 \times m} & G \times G \\
\downarrow{m \times 1} & & \downarrow{m} \\
G \times G & \xrightarrow{m} & G
\end{array}
\]

2. (Identity)

\[
\begin{array}{ccc}
G \times S & \xrightarrow{1 \times e} & G \times G \\
\downarrow{e \times 1} & & \downarrow{m} \\
G \times G & \xrightarrow{m} & G
\end{array}
\]

3. (Inverse)

\[
\begin{array}{ccc}
G & \xrightarrow{i} & G \\
i, 1 & & \downarrow{m} \\
G \times G & & S \\
e & & \downarrow{e} \\
& & G
\end{array}
\]

Remark 1.1.2. By Yoneda's Lemma, an equivalent definition is to endow \( G(S') = \text{Hom}(S',G) \) with a group structure functorially in \( S \)-schemes \( S' \).

Exercise 1.1.3. Using the Yoneda interpretation, show that if \( G, H \) are \( S \)-groups and \( f : G \to H \) is an \( S \)-scheme map that respects the multiplication morphisms, then it automatically respects the inversion map and identity section. Carry over all other trivialities from the beginnings of group theory (such as uniqueness of identity section). Can you do all this by writing huge diagrams and avoiding Yoneda?

Exercise 1.1.4. Let \( f : G \to H \) be a homomorphism of \( S \)-groups. The fiber product \( f^{-1}(e_H) = G \times_{H,e_H} S \) is the scheme-theoretic kernel of \( f \), denoted \( \ker f \). Prove that it is a subscheme of \( G \) whose \( S' \)-points (for an \( S \)-scheme \( S' \)) is the subgroup \( \ker(G(S') \to H(S')) \). The situation for cokernels is far more delicate, much like for quotient sheaves.

The fact that this is a subscheme is not entirely trivial, as sections need not be closed embeddings in general! (Consider the affine line with the doubled origin mapping to the affine line by crushing the two origins.)
Exercise 1.1.5. For each of the following group-valued functors on the category of schemes, write down a representing affine scheme and the multiplication, inversion, and identity maps at the level of coordinate rings:

- \( G_a(S) = \Gamma(S, \mathcal{O}_S) \)
- \( GL_n(S) = \Gamma(S, \mathcal{O}_S) \)
- \( \mu_m = \ker(t^m : GL_1 \to GL_1) \)
- For a finite group \( G \), do the same for the functor of locally constant \( G \)-valued functions (called the constant \( Z \)-group associated to \( G \)).

Definition 1.1.6. An abelian variety over a field \( k \) is a smooth, connected, proper group scheme \( X / k \) in other words, there are morphisms \( m : X \times X \to X \), \( e \in X(k) \), \( i : X \to X \) satisfying the usual group axioms.

From the functor of points perspective, this is equivalent to \( R \mapsto X(R) \) being a group functor on \( k \)-algebras.

Remark 1.1.7. The group axioms may be checked on \( k \)-points. This is sometimes a useful technical fact.

Example 1.1.8. In dimension 1, an abelian variety is an elliptic curve (a genus 1 curve with a rational point \( e \in X(k) \)).

Exercise 1.1.9. Let \( G \) be a group scheme locally of finite type over a field \( k \), with \( m : G \times G \to G \) the multiplication. Prove that the tangent map

\[
\frac{d}{d\lambda} m(e, \lambda e) : T_e G \to T_e G
\]

is addition.

1.2. Complex tori.

Definition 1.2.1. A complex torus is a connected, compact, complex Lie group.

These are the analytic analogues of complex abelian varieties.

Example 1.2.2. If \( V \cong \mathbb{C}^g \) and \( \Lambda \subset V \) is a lattice (a discrete, cocompact group), then \( V/\Lambda \) is a complex torus.

Example 1.2.3. Let \( C \) be a connected, compact Riemann surface. Then \( C \cong X_{\text{an}} \), where \( X \) is a smooth, projective, connected curve over \( \mathbb{C} \) (i.e. “comes from” algebraic geometry).

We want to construct a natural complex torus from \( C \). The space of holomorphic one-forms \( \Omega^1(C) \) is a \( g \)-dimensional vector space. Then we have an inclusion \( H_1(C, \mathbb{Z}) \cong \mathbb{Z}^{2g} \), and there is a natural map \( H_1(C, \mathbb{Z}) \to \Omega^1(C)^* \) via integration along cycles.

Exercise 1.2.4. Show that the image of \( H_1(C, \mathbb{Z}) \) in \( \Omega^1(C)^* \) is a lattice.

Although it is not necessary, you may use the fact from Hodge theory that \( \Omega^1(C) \oplus \Omega^1(C)^* \to \Omega^1(C)^* \) via integration along cycles.

If we pick bases \( \{w_j\} \) for \( \Omega^1(C)^* \) and \( \{\sigma_i\} \) for \( H_1(C, \mathbb{Z}) \), then \( (\int_{\sigma_i} \omega_j) \) is a \( 2g \times g \) matrix, called the period matrix.

Definition 1.2.5. The analytic Jacobian of \( C \) is \( J_C = \Omega^1(C)^*/H_1(C, \mathbb{Z}) \), a \( g \)-dimensional complex torus.
Remark 1.2.6. Notice that $J_C$ is covariant in $C$. Namely, a map $f: C' \to C$ induces $\Omega(C')^* \to \Omega(C)^*$ and $f_*: H_1(C', \mathbb{Z}) \to H_1(C, \mathbb{Z})$. One can check that the diagram

$$
\begin{array}{ccc}
\Omega(C') & \to & H_1(C', \mathbb{Z}) \\
\downarrow & & \downarrow \\
\Omega(C) & \to & H_1(C, \mathbb{Z})
\end{array}
$$

is commutative, hence we obtain an induced map on analytic Jacobians.

If $g > 0$, then there is an almost canonical way of embedding $C$ in $J_C$. For a basepoint $c_0 \in C$, we have a map $\iota_{c_0}: C \to J_C$ sending $c \mapsto \int_{c_0}^c (\mod H_1(C, \mathbb{Z}))$. However, the integral depends on the choice of path. Since we are integrating a holomorphic differential, it is unaffected by homotopy, so the integral is well-defined modulo integrals along loops.

Exercise 1.2.7. If $g > 0$, then prove that the map of sets $\iota_{c_0}: C \to J_C$ is complex-analytic and has smooth image over which $C$ is a finite analytic covering space. Deduce that $i_{c_0}$ is a closed embedding when $g > 1$, and prove that $i_{c_0}$ is an isomorphism when $g = 1$ by identifying $H_1(i_{c_0}, \mathbb{Z})$ with the identity map when $g = 1$.

This is a powerful tool for studying curves using knowledge of complex tori. We would like to replicate this in algebraic geometry over $\mathbb{C}$, and then over general fields.

Before we discuss the algebraic theory, we remark on the ubiquity of this construction.

Theorem 1.2.8. Every complex torus $A$ is commutative (contrast with the real case!) and $\exp_A: T_0(A) \to A$ is surjective homomorphism with kernel $\Lambda_A \subset T_0(A)$ a lattice. Hence $A \cong T_0(A)/\Lambda_A$.

Proof. See p. 1-2 of [Mum08]. The key is to study the adjoint representation of $A$ acting on $T_0(A)$. Associating $a \mapsto d c_a(e)$ gives a holomorphic map $A \to \text{GL}(T_0(A))$, which must be constant (by the maximum principle).

Next time we’ll adapt this idea to prove that abelian varieties are commutative. In characteristic $p$, for example, the tangent space is not so well-behaved, so one has to look at higher-order data too. But even in these algebraic cases, the theory is guided by the analytic analogy.

1.3. Link between complex abelian varieties and complex tori.

Theorem 1.3.1 (GAGA). There is a functor from proper $\mathbb{C}$-schemes to compact Hausdorff $\mathbb{C}$-analytic spaces $X \to X^a$ which is fully faithful.

Furthermore, many properties are equivalent on both sides: smoothness, connectedness, etc. The category of abelian varieties over $\mathbb{C}$ sits fully faithfully in the category of complex tori:

$$
\left\{ \text{abelian varieties of dimension } g \right\} \hookrightarrow \left\{ \text{complex tori of dimension } g \right\}.
$$

For $g = 1$ the two coincide, but for $g \geq 2$ the right hand side is much bigger. In this way, the one-dimensional case is quite misleading. However, it turns out that many of the nice properties of algebraic tori carry over to general complex tori.
As mentioned already, there is an equivalence of categories

\[
\text{\{smooth projective connected algebraic curves \}/}_C \leftrightarrow \text{\{connected compact Riemann surfaces\}}.
\]

So one might ask: can we create an algebraic analogue of the Jacobian variety? More precisely, given a smooth, projective, connected algebraic curve \(X\), can we build an abelian variety \(J_X\) of dimension \(g\) with 

\[T_0(J_X) \cong \Omega^1(X)^*\]

and (for some \(x_0 \in X(\mathbb{C})\)) an inclusion 

\[\iota_{x_0}: X \to J_X\] 

whose analytification recovers 

\[\mathbb{C} \to J_{\mathbb{C}}, \text{ where } \mathbb{C} = X^\text{an}\] 

Moreover, can we generalize this to arbitrary fields?

The answer is yes, using the Picard functor, as we shall see.

**Remark 1.3.2.** The smoothness is crucial; if \(X\) is not smooth then \(\text{Pic}_{X/k}\) still exists, but (its connected component) need not give an abelian variety; for example, it may even be affine.

**Exercise 1.3.3.** Let \(K\) be a field. An algebraic torus over \(k\) is a smooth affine \(k\)-group scheme \(T\) such that 

\[T_{\bar{k}} \cong \text{GL}_n^k\] 

as \(k\)-groups for some \(n \geq 0\).

(i) Explain how the \(\mathbb{R}\)-group 

\[G = \{x^2 + y^2 = 1\}\] 

is naturally a 1-dimensional algebraic torus over \(\mathbb{R}\), with \(G_{\mathbb{C}} \cong \text{GL}_1\) defined by \((x, y) \mapsto x + iy\) with \(x, y\) viewed over \(\mathbb{C}\), not \(\mathbb{R}\). Describe the inverse isomorphism. (This example explainst he reason for the name “algebraic torus”.)

(ii) Generalize to any separable quadratic extension of fields \(K/k\) in place of \(\mathbb{C}/\mathbb{R}\).

1.4. **The Mordell-Weil Theorem.** Poincaré originally conjectured that the rational points of any elliptic curve over \(\mathbb{Q}\) were a finitely generated abelian group. Mordell proved this, and conjectured a generalization: for \(k\) a number field and \(X\) a smooth, geometrically connected, proper curve over \(k\) of genus \(g \geq 2\), \(X(k)\) is always finite.

Weil had an insight into why this might be true. Assume that such a curve \(X\) has a rational point (otherwise there’s nothing to prove!). If we can build a map \(X \to J_X\) over \(k\), analogous to the embedding of a curve in its Jacobian, then we would have \(X(k) = J_X(k) \cap X(\mathbb{C})\). Weil wondered if it could be true that a combination of \(J_X(k)\) being “small” and \(X(\mathbb{C})\) being “small” in \(J_X(\mathbb{C})\) would force this intersection to be finite. So Weil’s strategy had two steps:

1. (Arithmetic step) Show that if \(A\) is an abelian variety over \(k\) a global field, then \(A(k)\) is finitely generated. This was Weil’s thesis, now called the Mordell-Weil theorem.

2. (Analytic step) Show (if it’s even true) that if \(C\) is a connected compact Riemann surface of genus at least 2, and \(\Gamma \subset J_C\) is a finitely generated subgroup, then \(C \cap \Gamma\) is finite.

Eventually, Faltings solved the Mordell conjecture in a different way. He deduced the conclusion of the analytic step from this, and to date this is the only known proof of the analytic step.
Remark 1.4.1. The analytic step can be viewed as a statement in algebraic geometry over finitely generated fields, since the relevant subgroup involves only finitely many complex numbers. Faltings’ proof is via induction on the transcendence degree (the algebraic case is the Mordell conjecture).

1.5. Commutativity. Earlier we saw that all complex tori are commutative (Theorem 1.2.8). The proof involved two ingredients:

1. consider the adjoint representation and observe that the matrix entries are holomorphic functions on a compact Lie group hence constant, and
2. then use the fact that a map of Lie groups is determined by the map of Lie algebras.

This second fact is completely false for varieties over a characteristic $p$ field. For example, the Frobenius morphism $x \mapsto x^p$ is non-zero but has derivative 0. Nonetheless, we want to generalize the result.

**Theorem 1.5.1.** Let $A$ be an abelian variety over $k$ a field. Then $A$ is commutative.

**Proof.** We want to prove that the two maps

$$
\begin{array}{ccc}
A \times A & \xrightarrow{m} & A \\
\text{flip} & & \\
& \downarrow & \\
A \times A & \xrightarrow{m} & 
\end{array}
$$

are equal.

**Exercise 1.5.2.** Prove that if $X, Y$ are $k$-schemes and $K/k$ is a field extension, then two maps $f, g : X \to Y$ are equal if and only if $f_K = g_K$. This is not trivial!

By the exercise, we can reduce to the case where $k$ is algebraically closed. The advantage of this is that we gain lots of rational points! (In the argument that we will eventually make, this will turn out to be unnecessary. However, it is a useful trick.) So choose $a \in A(k)$. We want to show that the map $c_a : A \to A$ sending $x \mapsto axa^{-1}$ is the identity map.

In the classical case, we proved this by studying the effect on the tangent space. Here that’s not enough, because of the failure of a map to be determined by its derivative, but since $A$ is irreducible it’s suffices to show that $c_a$ induces the identity map on $k(A)$, or even on $\mathcal{O}_{A,e}$.

Now the point is that we can inject the local ring into its completion: $\mathcal{O}_{A,e} \hookrightarrow \hat{\mathcal{O}}_{A,e}$ (the injectivity is by the Krull intersection theorem). So it’s enough to show that $c_a^\ast : \mathcal{O}_{A,e}/m_e^N \to \mathcal{O}_{A,e}/m_e^N$ is the identity map for all $N \geq 1$. For $N = 1$, this is just the derivative map. For $N > 1$, we get what the geometers would call spaces of “higher jets”. This is the generalization of the idea of checking the first-order behavior.

So we have a map $A(k) \to \text{GL}(\mathcal{O}_{A,e}/m_e^N)$ sending $a \mapsto c_a^\ast$. (Note that when $N = 2$, this is almost the tangent space; it’s really a slight enlargement of the cotangent space, so that is almost the special case of the adjoint representation.) Now, the matrix entries
are functions on $A(k)$, and $A$ is a proper variety. We would like to say that this forces the matrix entries to be constant on $A(k)^N$, so $\rho_N = \text{Id}$.

Why isn't this a complete proof already? Because we need to check that $\rho_N$ is algebraic, i.e. that there exists a $k$-morphism $A \to \text{GL}(V)$ recovering $\rho_N$ on $k$-points.

There are a few ways of dealing with this. In principle, one might try to bring out affine charts, but that's hard because the group law is not easily described in these terms. The slick way is to upgrade the construction of $\rho_N$ to work functorially on $R$-valued points, for all $k$-algebras $R$. (Of course, we mean functoriality in $R$). Then we can use the Yoneda Lemma to get argue that this comes from an algebraic morphism.

Exercise 1.5.3. If $X, Y$ are $S$-schemes and $h_X = \text{Hom}_S(-, X), h_Y = \text{Hom}_S(-, Y)$ then Yoneda's lemma says that

$$\text{Hom}_S(X, Y) \cong \text{Hom}_{-\text{Sch}}(h_X, h_Y).$$

In the category of $S = \text{Spec} R$ schemes, we can get away with less: show that if we restrict the functors to the category of affine $R$-schemes (so the functors may fail to be representable if $X, Y$ are not affine) then a natural transformation between the restricted functors still arises from a unique $R$-scheme map $X \to Y$.

In other words, an $R$-scheme map $X \to Y$ amounts to a map of sets $X(R') \to Y(R')$ for $R$-algebras $R'$ functorially in $R'$.

Therefore, an $R$-functorial construction is enough to obtain an algebraic morphism. So now we are looking for an $R$-functorial construction that recovers

$$A(k) \to \text{GL}(\mathcal{O}_{A,e}/\mathfrak{m}_e^N)$$

for $R = k$. For a $k$-algebra $R$, $a \in A(R)$, we define $c_a : A_R \to A_R$ by $x \mapsto axa^{-1}$. (What this really means is that if $R'$ is an $R$-algebra, $A(R') \to A(R')$ sends $x \mapsto a_{R'}xa_{R'}^{-1}$.) This carries $e_R$ to $e_R$, so it preserves the section $\text{Spec} R \xrightarrow{e} A_R$ (which is the base change of $\text{Spec} k \xrightarrow{e} A$).

Note that you can think of $\mathcal{O}_{A,e}/\mathfrak{m}_e^N \to \mathcal{O}_A/\mathfrak{I}_e^N$, where $\mathfrak{I}_e$ is the ideal sheaf of $e$. The map $c_a$ preserves $\mathfrak{I}_e$, and hence also the structure sheaf of $\mathcal{O}_R$. We claim that $\mathfrak{I}_{e_R} = \mathfrak{I}_e \otimes_k R$. Indeed, $\mathfrak{I}_e$ is defined by the short exact sequence

$$0 \to \mathfrak{I}_e \to \mathcal{O}_A \to k(e) \to 0$$

and tensoring with $R$ gives the short exact sequence

$$0 \to \mathfrak{I}_{e_R} \otimes R \to \mathcal{O}_{A_R} \to R(e) \to 0.$$
We’ve established that \( c_a : A_R \to A_R \) preserves \( \mathscr I_N \), the ideal sheaf of the \( N \)th infinitesimal neighborhood of the identity. Letting \( V_N = \mathcal O_{A_k} / \mathfrak m_N^N \), we have that \( c_a \) induces an \( R \)-algebra automorphism of the coordinate ring \( V_{N+1} \otimes_k R \), obtained from the action on the underlying scheme. The map \( A(R) \to GL_R(V_{N+1} \otimes_k R) \) sending \( a \to c_a \) is functorial in \( R \) (check it!).

Informally, \( GL_R(V_{N+1} \otimes_k R) = "GL(V_{N+1})"(R) \) where “\( GL(V_{N+1}) \)” means the \( k \)-group scheme \( GL(V_{N+1}) \). This gives an algebraic map \( A \to GL(V_{N+1}) \) as required. Now the punchline is that \( A \to GL(V_{N+1}) \) is a map from a proper scheme to an affine scheme, hence constant.

\[
\square
\]

**Exercise 1.5.4.** Let \( V \) be a locally free module of finite rank \( n > 0 \) over a commutative ring \( R \). Consider the functor on \( R \)-algebras defined by \( R' \to Aut_{R'}(V \otimes_R R') \). Prove in two ways that this is represented by an affine \( R \)-group \( GL(V) \) that is Zariski-locally (on \( Spec R \)) isomorphic to \( GL_n \):

1. Work Zariski-locally on \( Spec R \) and construct the group scheme by gluing,
2. Let \( S \) be the symmetric algebra of the dual module \( \text{End}(V)^* = V^* \otimes V \). Identify \( \det : \text{End}(V) \to R \) with a canonical element in \( S \) that is homogeneous of degree \( n \). Prove that \( \text{Spec}(S[1/\det]) \) does the job.

1.6. **Torsion.** First let’s consider the familiar case of a complex torus \( A \) over \( \mathbb C \). In this case \( A \cong V / \Lambda \), so

\[
A[N] = \{ a \in A \mid Na = 0 \} = \frac{1}{n} \Lambda / \Lambda \cong \Lambda / N\Lambda \cong (\mathbb Z / N) \mathbb Z^g.
\]

**Remark 1.6.1.** The latter can be identified with \( H_1(A, \mathbb Z / n\mathbb Z) \).

If \( N \mid N' \), then there is also the natural inclusion \( A[N] \hookrightarrow A[N'] \). The corresponding map \( \Lambda / N\Lambda \to \Lambda / N'\Lambda \) is “multiplication by \( N / N' \),” which is a bit weird. It is more natural to consider the following construction, due to Tate. If \( N' = dN \), then multiplication by \( d \) induces a map \( A[N'] \to A[N] \). The corresponding map \( \Lambda / N\Lambda \to \Lambda / N'\Lambda \) is then the natural reduction map.

\[
\begin{array}{ccc}
\frac{1}{N'} \Lambda / \Lambda & \xrightarrow{\times d} & \frac{1}{N} \Lambda / \Lambda \\
N' \downarrow & & N \downarrow \\
\Lambda / N' \Lambda & \xrightarrow{\text{reduction}} & \Lambda / N\Lambda.
\end{array}
\]

Therefore,

\[
\lim_{n \geq 0} \ell^n \cong \lim_{n \to \ell^n} \Lambda / \ell^n \Lambda \cong \mathbb Z / \ell \otimes \mathbb Z \cong H_1(A, \mathbb Z / \ell).
\]

We define the \( \ell \)-adic Tate module of \( A \) to be \( T_1(A) = H_1(A, \mathbb Z / \ell) \). It is a free \( \mathbb Z / \ell \)-module of rank \( 2g \). The key point is that it is a functorial in \( A \). Now, although \( H_1(A, \mathbb Z) \) cannot be cooked up in the algebraic setting, \( H_1(A, \mathbb Z / \ell) \) can and is useful over arbitrary fields!

**Remark 1.6.2.** Why “can’t” we construct an interesting integral cohomology group \( H_1(A, \mathbb Z) \), which recovers \( H_1(A, \mathbb Z / \ell) \) by change of coefficients? Here is an argument of Serre. If you
had a functorial assignment of a lattice to an abelian variety, then in particular the endomorphism ring of the abelian variety would act on this lattice. But in characteristic $p$, one can have a quaternion algebra as the endomorphism ring, which couldn’t act on a 2-dimensional lattice.

Now we turn out attention to the algebraic theory. Two questions present themselves:

1. For an abelian variety $A/k$ of dimension $g$, what can we say about $A(\overline{k})[N]$ (in particular, is it $(\mathbb{Z}/N\mathbb{Z})^g$?
2. What if $\text{char } k \mid N$?

In particular, if $A/\mathbb{Q}$, then we should expect that $A(\mathbb{Q})[N] = A(\mathbb{C})[N]$.

**Toy case.** Let’s actually just think first about $\mathbb{G}_m = \text{GL}_1$. Then $\mathbb{G}_m(\mathbb{K})[N] = \{x \in \mathbb{K} \mid x^N = 1\}$. There are two possibilities:

$$\mathbb{G}_m(\mathbb{K})[N] = \begin{cases} N \text{ solutions, cyclic} & \text{ch}(k) \nmid N, \\ \text{fewer solutions, cyclic} & \text{ch}(k) \mid N \end{cases}$$

This is analogous to what happens for abelian varieties. This was classically “understood” for elliptic curves:

$$E(\mathbb{K})[\ell] = \begin{cases} (\mathbb{Z}/\ell\mathbb{Z})^2 & \ell \neq \text{char } k \\ \mathbb{Z}/\ell \text{ or } \{0\}, & \ell = \text{char } k \end{cases}$$

**Notation.** Henceforth we adopt the convention that $p \neq \ell$ denote distinct primes, and $q$ is a power of $p$.

**Definition 1.6.3.** We denote by $[N] : A \to A$ the multiplication by $N$ map, $a \mapsto N \cdot a$. We set $A[N] := \ker([N]) = [N]^{-1}(0)$, the scheme-theoretic fiber.

In general, if $f : G \to H$ then $f^{-1}(e_H) \subset G$ represents the functor $R \mapsto \ker(G(R) \to H(R))$.

So $[N]^{-1}(0)$ represents the functor $R \mapsto \{a \in A(R) \mid N \cdot a = 0 \in A(R)\}$. We’ll see later that $A[N]$ is $k$-finite, and $\dim_k O_{A[N]} = N^2g$. However, there might not be so many geometric points; there could be nilpotent stuff contributing to the dimension but not to physical points. So the idea that the “order” of torsion is $N^2g$ is retained in a useful way, but the structure can be subtle depending on whether or not the characteristic divides $N$.

**Example 1.6.4.** The map $\mathbb{G}_m \xrightarrow{t^N} \mathbb{G}_m$ has kernel $\text{Spec } k[t]/(t^N - 1)$. If the characteristic is $p$ and $N = p$, then this is $k[x]/(x^p)$ where $x = t - 1$, so you see that you get a fat point.

On the other hand, the map $x^p : \mathbb{G}_a \to \mathbb{G}_a$ has kernel $k[x]/(x^p)$. The kernels have the same scheme structure, but the group laws are completely different! (So they are not the same group scheme).

Over $\mathbb{C}$, the torsion points of a complex torus are dense. We will see eventually that an analogous statement is true for abelian varieties: if $A$ is an abelian variety over $\mathbb{K} = \overline{k}$, then $\{A[\ell^n]\}_{n \geq 1}$ is dense in $A$ for any fixed prime $\ell \neq \text{char } k$. 


1.7. **Rigidity.** The goal of this section is to prove that any morphism \( f: A \to A' \) sending \( e_A \mapsto e_{A'} \) is automatically a homomorphism. To prove this we need the **rigidity theorem.**

By Yoneda, it suffices to show that \( f \) respect products (inversion then follows for free). In other words, we want to show that the map

\[
A \times A \to A'
\]

\[
(a_1, a_2) \mapsto f(a_1 a_2 f(a_1)^{-1} f(a_2)^{-1}
\]

is actually the constant map \( (a_1, a_2) \mapsto e := e_A \).

The rigidity theorem asserts that in some circumstances, a map from a product constant on a slice factors through the projection. Obviously \( A \times e \to e' := e_{A'} \) and \( e \times A \to e' \), so that’s why it is useful here.

**Theorem 1.7.1** (Rigidity). Let \( X, Y \) be geometrically integral schemes of finite type over \( k \), and \( Z \) a separated \( k \)-scheme. (In all our applications, everything will be an abelian variety.) Let \( f: X \times Y \to Z \) be a morphism, and assume furthermore that

1. \( X \) is proper, and
2. for some algebraically closed field \( K/k \), there exists \( y_0 \in Y(K) \) such that \( f_{y_0}: X_K \to Z_K \) is a constant map to \( z_0 \in Z(K) \).

Then \( f \) is independent of \( X \), i.e. there exists a unique \( k \)-map \( g: Y \to Z \) such that \( f(x, y) = g \).

\[
\begin{array}{ccc}
X \times Y & \xrightarrow{f} & Z \\
\downarrow & & \downarrow \cong \ \\
Y & \xrightarrow{g} & Z
\end{array}
\]

**Remark 1.7.2.** The intuitive meaning here is that for proper \( X \), constant maps \( X \to Z \) have no non-constant deformation. Indeed, we can view \( f \) as part of a \( Y \)-map \( X \times Y \to Z \times Y \) sending \( (x, y) \mapsto (f(x, y), y) \). Intuitively, this is a family of maps \( X \to Z \) indexed by \( Y \). The rigidity theorem says that if \( X \) is proper, and one map is constant then they all are.

**Example 1.7.3.** Properness is crucial. If \( X = Y = Z = \mathbb{A}^1 \) and \( f(x, c) = cx \) then \( f_0 \) is constant, but the theorem is false. (It appears that you can extend this map to \( X = Z = \mathbb{P}^1 \), but if you think carefully about it then you’ll realize that you can’t.)

**Proof.** We use the theory of descent. There are several steps:

1. **Uniqueness.** We argue that \( g \), if it exists, must be unique. This is trivial, as the projection map \( X \times Y \to Y \) is surjective.
2. **Descent.** We argue that if \( g \) exists after base change to some finite Galois extension, then it is defined over \( k \). Suppose \( k'/k \) is a finite Galois extension, and that such a \( g \) exists for \( f_{k'} \), i.e. \( f_{k'}: X_{k'} \times Y_{k'} \to Z_{k'} \) factors through \( g \). But then for any \( \sigma \in \text{Gal}(k'/k) \), we have \( \sigma^* f_{k'} = f_{k'} \), so \( \sigma^* g = g \) by the uniqueness. Galois descent then implies that \( g \) is defined over \( k \).
3. **Existence of rational points.** We want to show that there exists a Galois extension \( k'/k \) such that \( X(k') \neq \emptyset \). It suffices to show that \( X(k) \neq \emptyset \).

**Lemma 1.7.4.** If \( X \) is a geometrically reduced \( k \)-scheme of finite type over \( k = k^s \), then \( X(k) \neq \emptyset \).
**Proof.** We assume that $X$ is geometrically integral; this is a minor relaxation. The idea is to produce a dense open subset isomorphic to some affine hypersurface in $\mathbb{A}^n$.

Since $k = k^s$, $X_k \rightarrow X$ is a homeomorphism (totally inseparable morphisms are homeomorphisms). Therefore, if $k(X)$ is the function field of $X$ then we have (by the bijection between open sets)

$$k(X_\overline{k}) = \mathcal{O}_{X_\overline{k}, \eta} = \overline{k} \otimes_k \mathcal{O}_{X, \eta} = \overline{k} \otimes_k k(X).$$

This shows that $k(X)/k$ is separable (see §26 of [Mat89]). Equivalently, $k(X)/k$ has a separating transcendence basis, i.e.

$$k(X) = k(t_1, \ldots, t_n)[t_{n+1}]/(f)$$

where $f$ is a monic irreducible polynomial with coefficients in $k(t_1, \ldots, t_n)$. By removing any denominators, we may assume that $f \in k[t_1, \ldots, t_{n+1}]$ separable in $t_{n+1}$. So there is a dense open subset of $X$ isomorphic to a dense open subset $U'$ of $\{ f = 0 \} \subset \mathbb{A}^{n+1}$. We reduce to showing that $U'$ has a rational point.

Consider the projection map $\pi: U' \rightarrow \mathbb{A}^n$ to the first $n$ coordinates. There is a dense open subset $V' \subset \mathbb{A}^n$ such that $f(v', t_{n+1})$ is separable for $v' \in V'$ (we can take those points such that $\text{disc}_{t_{n+1}}(f) \neq 0$). Then taking any $v'_0 \in V'(k)$, we have that $f(v'_0, t_{n+1}) = 0$ can be solved in $t_{n+1}$ to obtain a rational point of $U'(k)$.

(4) **Existence of $g$.** By the previous part, we can pass to some Galois extension $k'/k$ to assume that $X(k) \neq \emptyset$. Having constructed some $x_0 \in X(k)$, we want to define $g(y) = f(x_0, y)$. We want to assume that $f(x, y) = g(y)$.

To check this, we may extend the base further if necessary, we may assume that $y_0 \in Y(k)$. By assumption $f(X \times \{ y_0 \})$ is crushed to $z_0$. If $U$ is some affine neighborhood of $z_0$, then $f^{-1}(U)$ is open in $X \times Y$ and contains $X \times \{ y_0 \}$.

Since the projection map $X \times Y \rightarrow Y$ is proper, the complement of $f^{-1}(U)$ maps to a closed set in $Y$. Therefore, there is an open set $V \subset Y$ such that $X \times V \subset f^{-1}(U)$. Since $U$ is affine and $X$ is proper, each fiber of $X \times V \rightarrow V$ is crushed to a point, so $f(x_0, y) = g(y)$ on $X \times V$, which is dense in $X \times Y$. As $Z$ is separated, the locus where the two maps agree is closed, hence all of $X \times Y$.

**Corollary 1.7.5.** Let $A, A'$ be abelian varieties over $k$. Then any pointed map $f(A, e) \rightarrow (A', e')$ is a homomorphism.

**Proof.** Consider the map $h: A \times A 

\rightarrow A'$ given by

$$(a_1, a_2) \mapsto f(a_1a_2)f(a_2)^{-1}f(a_1)^{-1}.$$
This gives another proof of:

**Corollary 1.7.6.** Abelian varieties are commutative.

*Proof.* Apply Corollary 1.7.5 to \( \text{inv} : A \to A \).

**Corollary 1.7.7.** For an abelian variety \( A \), the multiplication map \( m : A \times A \to A \) is determined by \( e \in A(k) \).

*Proof.* If \( m' \) is another such, consider the identity map \( \text{Id} : (A, m, e) \to (A, m', e) \). This is automatically a homomorphism by Corollary 1.7.5.

**Remark 1.7.8.** That’s interesting, but is it ever important in practice? The point is that it allows you to do deformation theory arguments cleanly, because you don’t have to keep track of the group law, associativity, etc. In some situations it is convenient to know that we only have to keep track of the geometry and not the group law.

Here are some more exercises related to descent.

**Exercise 1.7.9.** Let \( X \) and \( Y \) be schemes of finite type over a field \( k \), \( K/k \) an extension, and \( \{ K_i \} \) a directed system of subfields of \( K \) containing \( k \) such that \( \lim_{\to} K_i = K \). Show that any \( K \)-map \( X_K \to Y_K \) descends uniquely to a \( K_i \)-map \( X_{K_i} \to Y_{K_i} \) for some \( i \).

**Exercise 1.7.10.** Let \( f : X \to Y \) be a \( k \)-map. Prove that \( f \) has property \( P \) if and only if \( f_K \) does, where \( P \) is: affine, finite, quasi-finite, closed immersion, surjective, isomorphism, separated, proper, flat.

**Exercise 1.7.11.** Suppose that \( K/k \) is a finite Galois extension. Prove that a \( K \)-map \( F : X_K \to Y_K \) descends to a \( k \)-map \( f : X \to Y \) if and only if \( F \) is equivariant for the natural action by \( \text{Gal}(K/k) \) on \( X_K \) and \( Y_K \) (over \( k! \)). This is Galois descent for morphisms.
2. THE PICARD FUNCTOR

2.1. Overview. To study line bundles on an abelian variety, we digress to discuss Picard schemes over $k$. (See §9 of [FGI+05], which rests on the theory of Hilbert schemes developed in §5.) Here our approach deviates from that of [Mum08], where Mumford directly develops a theory of Picard schemes for abelian varieties.

Setup. $X$ is a geometrically reduced, geometrically connected proper $k$-scheme (e.g. an abelian variety).

Goal. We want to classify “families of line bundles on $X$,” by which we mean line bundles $L$ on $X \times_k S$ where $S$ is some $k$-scheme. Informally, you can think of a line bundle $L$ on $X \times_k S$ as a family of line bundles $\{L_s = L|_{X_s}\}_{s \in S}$.

Now, there is a basic problem you encounter when you try to study line bundles, which is that they have non-trivial automorphisms coming from units: any $L$ admits an action of $\Gamma(X_S, \mathcal{O}_X^\times) \supset \Gamma(S, \mathcal{O}_S^\times)$. The problem with automorphisms is that they make it difficult to pass from local situations to global situations because there is ambiguity in gluing local calculations.

2.2. Rigidification.

Lemma 2.2.1. Let $X/k$ be a connected, reduced, proper scheme and let $f_S: X_S \to S$ be the projection map. Then $\mathcal{O}_S = f_{S*}(\mathcal{O}_{X_S})$.

Proof. Consider the base-change diagram

$$
\begin{array}{ccc}
X_S & \longrightarrow & X \\
| & f | & | \\
S & \longrightarrow & \text{Spec } k \\
\downarrow f_S & & \downarrow f \\
S & \longrightarrow & \text{Spec } k \\
\end{array}
$$

By flat base change for quasicoherent sheaves,

$$f_{S*}(\mathcal{O}_{X_S}) \cong \mathcal{O}_S \otimes_k \Gamma(X, \mathcal{O}_X).$$

(For a quasicompact separated map, pushforward commutes with flat base change). Since $k \hookrightarrow \Gamma(X, \mathcal{O}_X)$ is an equality by the assumptions on $X$, we are done.

Exercise 2.2.2. Show that this implies $\mathcal{O}_S^\times = f_{S*}(\mathcal{O}_{X_S}^\times)$, hence by taking global sections $\Gamma(S, \mathcal{O}_S^\times) = \Gamma(X_S, \mathcal{O}_{X_S}^\times)$.

To handle the problem of units, we’re going to use a trick of Grothendieck’s called rigidification. Since abelian varieties have an identity section, we can add the datum of a rational point. This is a bad move to make in general, because even the existence of rational points may be a question of interest, so view it as a provisional solution that is harmless in the case of abelian varieties.

From now on, we assume that we are given $e \in X(k)$. 

Definition 2.2.3. A trivialization of \( \mathcal{L} \) (on \( X_S \)) along \( e \) (“along \( e_S \)”) is an isomorphism \( \iota: e_S^*(\mathcal{L}) \cong \mathcal{O}_S \).

Example 2.2.4. If \( S = \text{Spec } k \), this is just a basis of the \( k \)-line \( \mathcal{L}(e) := \mathcal{L}|_e \).

Remark 2.2.5. If \( \iota \) exists, then by Exercise 2.2.2 any two such \( \iota, \iota' \) are uniquely related by an element of \( \Gamma(S, \mathcal{O}_S) \).

Given \( \mathcal{L} \) on \( X_S \), it is obvious that such an \( \iota \) exists Zariski-locally on \( S \) (this is just the definition of local triviality of a line bundle). The ambiguity in specifying \( \iota \) is in the units.

Definition 2.2.6. An isomorphism \( (\mathcal{L}, \iota) \cong (\mathcal{L}', \iota') \) on \( X_S \) is an isomorphism \( \theta: \mathcal{L} \cong \mathcal{L}' \) preserving the trivialization, i.e.

\[
\begin{array}{ccc}
\mathcal{L} & \xrightarrow{e_S^*(\theta)} & \mathcal{L}' \\
\iota & \cong & \iota' \\
\mathcal{O}_S & \xrightarrow{e_S^*} & \mathcal{O}_S
\end{array}
\]

Lemma 2.2.7. We have \( \text{Aut}(\mathcal{L}, \iota) = \{1\} \).

Proof. This follows from \( \text{Aut}(\mathcal{L}) = \Gamma(S, \mathcal{O}_S) \) (by Exercise 2.2.2) and the fact that \( \Gamma(S, \mathcal{O}_S) \) acts simply transitively on all possible \( \iota \) for \( \mathcal{L} \).

Said differently, we know that any automorphism of \( \mathcal{L} \) is multiplication by a unit on \( S \), which is therefore detected by the induced automorphism of \( e_S^* \mathcal{L} \). But the composition

\[
\Gamma(S, \mathcal{O}_S) \to \Gamma(X_S, \mathcal{O}_X) \xrightarrow{e^*_S} \Gamma(S, \mathcal{O}_S)
\]

is the identity map, so if \( \iota = \iota' \) then this unit must be 1. So you can think of the trivialization as capturing all the ambiguity in the automorphisms of \( \mathcal{L} \).

You might complain that you are really interested in line bundles, not the rigidified line bundles, but that is assuaged by the following fact.

Proposition 2.2.8. The projection map

\[
\{(\mathcal{L}, \iota) \text{ on } X\}/ \cong \text{Pic}(X) = \{\mathcal{L} \text{ on } X\}/ \cong
\]

is bijective.

Proof. Surjectivity is simply the statement that \( \text{Pic}(\text{Spec } k) = 1 \), so we can always find some trivialization \( \iota \).

The interesting part is injectivity. You can check that this map is a homomorphism, where the group structure on the right hand side is tensor product of line bundles and
sections. Suppose we have two rigidified bundles \((\mathcal{L}, \iota), (\mathcal{L}', \iota')\) and an isomorphism 
\(\theta: \mathcal{L} \cong \mathcal{L}'\). Then \(\theta\) carries \(\iota \rightarrow u \iota'\) where \(u \in \Gamma(S, \mathcal{O}_S^*)\). Replacing \(\theta\) with \(u^{-1} \cdot \theta\) induces an isomorphism \((\mathcal{L}, \iota) \cong (\mathcal{L}', \iota')\).

Given \(\mathcal{L}\) on \(X_S\), consider the following modification:
\[
\mathcal{L} \mapsto \mathcal{L} \otimes f_s^*(e_s^* \mathcal{L})^{-1}. 
\]
where as before, \(e_S: S \rightarrow X_S\) is a section of \(f_S: X_S \rightarrow S\).

Applying \(e_S^*(-)\) to the above, we obtain
\[
e_S^*(\mathcal{L} \otimes f_s^*(e_s^* \mathcal{L})^{-1}) \cong e_S^* \mathcal{L} \otimes e_S^* f_s^*(e_s^* \mathcal{L})^{-1} \cong e_S^* \mathcal{L} \otimes (e_S^* \mathcal{L})^{-1} \cong \mathcal{O}_S.
\]
This is a canonical trivialization of \(e_S^*(\mathcal{L} \otimes f_s^*(e_s^* \mathcal{L})^{-1})\), denoted by \(\text{can}\), giving \(\mathcal{L} \otimes f_s^*(e_s^* \mathcal{L})^{-1}\) a canonical rigidified structure.

**Exercise 2.2.9.** Check that given \(\iota\) a trivialization of \(e_s^* \mathcal{L}\), the induced isomorphism
\[
e_S^*(\mathcal{L} \otimes f_s^*(e_s^* \mathcal{L})^{-1})) \cong e_S^*(\mathcal{L} \otimes \mathcal{O}_{X_S}) \cong \mathcal{O}_S
\]
is \(\iota\).

**Remark 2.2.10.** Given \((\mathcal{L}, \iota)\) and \((\mathcal{L}', \iota')\) on \(X_S\), if there exists a Zariski cover \([S_a]\) of \(S\) such that they are isomorphic when restricted to \(X_{S_a}\), then they are isomorphic on \(X_S\). Why? Just use the uniqueness of such isomorphisms (i.e. triviality of automorphisms), when they exist, to patch them.

**Definition 2.2.11.** We define the Picard functor \(\text{Pic}_{X/k, e}\) to be the functor taking
\[
S \mapsto \{(\mathcal{L}, \iota) \text{ on } X_S\}/\cong,
\]
which is a commutative group with identity \((\mathcal{O}_{X_S}, 1)\) under \(\otimes\).

The preceding remark shows that this is a Zariski sheaf on any \(S\). That would fail without the rigidification! This is certainly necessary for the functor to have any hope of being representable.

We claim that the functor is in some sense independent of \(e\). (In fact, Grothendieck gave a direct definition that made no reference to a rational point \(e\), and made sense even if there was no \(e\).) Namely, if \(e' \in X(k)\) is another point, we give an isomorphism
\[
\text{Pic}_{X/k, e}(S) \cong \text{Pic}_{X/k, e'}(S)
\]
sending \((\mathcal{L}, \iota) \mapsto (\mathcal{L} \otimes f_S^*(e_S^* \mathcal{L})^{-1} \otimes f_S^*(e_S)^* \mathcal{L}, \text{can} \otimes \iota)\).

**Proposition 2.2.12.** The map \(\text{Pic}_{X/k, e}(S) \cong \text{Pic}(X_S)/f_S^*(\text{Pic} S)\) sending \((\mathcal{L}, \iota) \mapsto \mathcal{L}\) is an isomorphism respecting the above identification.
Proof. That the map is a homomorphism is obvious. Surjectivity follows from the observation that $L \otimes f^*_S(e_S)^*L^{-1}$ admits a trivialization. Injectivity follows from the observation made earlier: any isomorphism $L \cong L'$ is induced by a unit $u \in \Gamma(S, O_S^*)$, and this $u$ can be uniquely chosen to take any $e_S$-trivialization $\iota$ to any other trivialization $\iota'$.

Exercise 2.2.13. Check the claimed compatibility with change of basepoint. □

There should be a canonical inverse; what is it? You can take

$L \mapsto (L \otimes f^*_S e^*_S L^{-1}, \text{can}).$

You might complain that this changes the line bundle, but notice that it only changes it by $f^*_S e^*_S L^{-1}$, which comes from $\text{Pic.S}$. The point is that if you’re willing to ignore $f^*_S(\text{Pic.S})$, then you have extra room to work with.

2.3. Representability. We now study the representability of $\text{Pic}_{X/k, e}$. This means that there is a scheme $\mathcal{M}$ and an isomorphism

$$\xi : \text{Pic}_{X/k, e} \cong \text{Hom}_k(-, \mathcal{M}).$$

Remark 2.3.1. Although it is common to say that “$\mathcal{M}$ represents the functor,” Grothendieck emphasized that a space alone cannot represent a functor; it is $\mathcal{M}$ plus the data of this isomorphism $\xi$ represents the functor.

Unraveling the proof of Yoneda, one sees that evaluating $\xi$ on $\mathcal{M}$ and choosing $\text{Id}_\mathcal{M}$ on the left side gives a distinguished rigidified line bundle $(\mathcal{P}, \theta) \in \text{Pic}_{X/k, e}(\mathcal{M})$, which is the “universal line bundle.” Then for any $(\mathcal{L}, \iota)$ on $X_S \to S$, there exists a unique map $S \to \mathcal{M}$ pulling back the universal bundle to $(\mathcal{L}, \iota)$:

$$\begin{array}{ccc}
X_S & \longrightarrow & X_{\mathcal{M}} \\
\downarrow & & \downarrow \\
S & \underset{\varphi}{\longrightarrow} & \mathcal{M},
\end{array}$$

i.e. $\varphi^*\mathcal{P} \cong \mathcal{L}$ over $X_S$ carrying $\varphi^*\theta$ to $\iota$. Here the isomorphism is unique, because there are no automorphisms after rigidification, so it does not have to be included as part of the data.

In conclusion, the representability amounts to the existence of $\mathcal{M}$ plus a universal family over $\mathcal{M}$, with this universal property.

Remark 2.3.2. If we didn’t make these rigidification, then things would be extremely difficult to work with, because there is ambiguity in this isomorphism with the pullback.

More generally, this discussion applies to any contravariant, set-valued functor $F$. For any field extension $K/k$, we have

$$\mathcal{M}(K) = \text{Pic}_{X/k, e}(K) = \text{Pic}(X_K)$$

because $\text{Pic}(K) = 0$ (see Proposition 2.2.12). In any “local” situation, we can drop the rigidification. In particular, $\mathcal{M}(\kappa) = \text{Pic}(X_{\kappa})$.
Grothendieck realized that it would be difficult to construct a universal line bundle directly. His insight was to work instead with divisors, a much more geometric object, and then quotient out by extraneous data.

**Theorem 2.3.3** (Grothendieck/Oort-Murre/Artin). Let $X$ be a geometrically reduced, geometrically connected, proper $k$-scheme. If $X(k) \neq \emptyset$, then $\text{Pic}_{X/k,e}$ is represented by a locally finite type $k$-scheme $\text{Pic}_{X/k,e}$ (for any $e \in X(k)$).

**Proof.** The proof requires a good deal of technical machinery (which is irrelevant to the theory of abelian varieties), so we will omit it. Instead, we just make some remarks on the construction.

Grothendieck proved this for $X$ projective and geometrically integral. We will show that abelian varieties are projective, without using this machinery, so this is sufficient for our applications. Oort-Murre proved the general result, and Artin proved an even more general result for abelian schemes.

Grothendieck explicitly constructs $\text{Pic}_{X/k}$ as a countable union of quasi-projective schemes. Line bundles have discrete invariants, like the degree, and these invariants describe distinct components.

Most references prove representability for functors like Pic, Hilb, etc. “just” on the category of locally noetherian schemes over a given locally noetherian base (or often even just on the category of schemes of finite type over a given noetherian base). That is always where the real work lies, but there are standard ways to show, under mild conditions on the functor inspired by Grothendieck’s functorial locally finitely presented criterion from EGA IV 3.14, that a representing object on that category also represents the functor on the category of all schemes over the base. (It is not necessary to establish the methods in the proof of the locally noetherian case, such as base change theorems for coherent cohomology, in the non-noetherian case, but rather to formally show that the final conclusion automatically holds more generally when known in the locally noetherian case.)

As a beginner one might not want to worry about that too much, though the cost of saying “locally noetherian” everywhere is that you have to make sure whenever you take fiber products that at least one of the two structure maps is (essentially) locally finite type (or else you’ll lose the noetherian condition). With experience one begins to appreciate that it is better to prove a result on the category of all schemes when can be done without too much effort from the locally noetherian case. (EGA develops very clean methods to carry out such bootstrap procedures, applicable for instance to Pic.)

2.4. **Properties of $\text{Pic}_{X/k}$.** To start, observe that $\text{Pic}_{X/k}$ is automatically a group scheme, as it represents a group-valued functor. Moreover, it comes out of Grothendieck’s construction that $\text{Pic}_{X/k}$ is locally of finite type.

**Exercise 2.4.1.** Let $X$ be a scheme locally of finite type over $k$.

(i) If $X(k) \neq \emptyset$ and $X$ is connected, then prove that $X$ is geometrically connected over $k$.

(ii) Assume that $k$ is algebraically closed and $X$ is a group scheme over $k$. Prove that $X_{\text{red}}$ is smooth, and deduce that if $X$ is connected and $U$ and $V$ are non-empty
open subschemes then the multiplication map $U \times V \to X$ is surjective. Deduce that for general $k$, if $X$ is a (locally finite type) group scheme over $k$ then it is connected if and only if it is geometrically irreducible over $k$, and that such $X$ are of finite type (i.e. quasicompact) over $k$.

**Remark 2.4.2.** In particular, if $A$ is an abelian variety over $k$ and $k'/k$ is an extension field, then $A \otimes_k k'$ is also an abelian variety. This is a useful result!

In particular, this shows that if $G$ is a group scheme locally finite type over $k$, then $G^0$ is geometrically irreducible and finite type (hence quasicompact).

**Remark 2.4.3.** It can really happen in more general circumstances that you end up with (natural) moduli spaces that are connected, but not quasicompact (so not of finite type).

In fact, $\text{Pic}_{X/k}$ is also separated because of:

**Lemma 2.4.4.** If $G$ is a group scheme over a field $k$, then $G$ is separated.

**Proof.** Consider the diagonal map composed with $(x, y) \mapsto xy^{-1}$.

$$
\begin{array}{ccc}
G & \xrightarrow{\Delta} & G \times G \\
\downarrow & & \downarrow \\
G & \xrightarrow{e} & G
\end{array}
$$

This realized the diagonal map as a base-change of the identity section, which is automatically a closed immersion (this is what fails over a general base).

This is non-trivial; if we weren’t working over a field, then it would not necessarily be true!

So the identity component $\text{Pic}^0_{X/k}$ is a separated $k$-group of finite type.

**Example 2.4.5.** When $X$ is not smooth, $\text{Pic}^0_{X/k}$ can be non-proper. For example, if $X$ is the nodal cubic then $\text{Pic}^0_{X/k} \cong \mathbb{G}_m$ (see 9.2/8 in [BLR90]). Intuitively, the Picard group is parametrized by slopes of lines, with two slopes missing.

In general, it’s hard to characterize $\text{Pic}^0_{X/k}(K) \subset \text{Pic}(X_K)$. In Exercise 2.4.7 you’ll show that for a curve this is just the set of line bundles of degree 0. Roughly speaking, the identity component on a disjoint union of curves consists of bundles which are “degree 0” on each.

**Compatibility with base change.** If $K/k$ is smooth, then $(\text{Pic}_{X/k}, (\mathcal{P}, \theta))_K$ is $(\text{Pic}_{X_K/K}, (\text{universal}))$ i.e. it represents $\text{Pic}_{X/K,e}$ on the category of $K$-schemes. This follows from some general nonsense. The crucial observation is the identification

$$
\text{Hom}_K(-, M)_{\text{Sch}/K} \cong \text{Hom}_K(-, M_K),
$$
which just follows from the universal property of the fibered product: if \( T \) is over \( \text{Spec} \; K \) and admits a map to \( M \) over \( k \), then there is a unique \( K \)-map \( T \rightarrow M_k \) inducing them.

So the point is that the “base change of the functor” is the same functor.

**Exercise 2.4.6.** Let \( X \) be a proper and geometrically integral scheme over \( k \). Assume that \( X(k) \neq \emptyset \) and choose \( e \in X(k) \). The identity component \( \text{Pic}^0_{X/k} \) is a \( k \)-scheme of finite type by Exercise [2.4.1](#).

1. Prove that if \( X \) is smooth and projective over \( k \) then \( \text{Pic}^0_{X/k} \) satisfies the valuative criterion for properness (so \( \text{Pic}^0_{X/k} \) is a proper \( k \)-scheme).
2. By computing with points valued in the dual numbers, and using Cech theory in degree 1, construct a natural \( k \)-linear isomorphism \( H^1(X, \mathcal{O}_X) \cong T_0(\text{Pic}^0_{X/k}) \).
3. If \( X \) is smooth with dimension 1, prove that \( \text{Pic}^0_{X/k} \) satisfies the infinitesimal smoothness criterion (for schemes locally of finite type over \( k \)). Deduce that \( \text{Pic}^0_{X/k} \) is an abelian variety of dimension equal to the genus of \( X \).

By Exercise [2.4.6](#) we have isomorphisms of \( k \)-vector spaces

\[
T_0(\text{Pic}^0_{X/k}) = T_0(\text{Pic}_X) = \ker(\text{Pic}_{X/k}(k[e]) \rightarrow \text{Pic}_{X/k}(k)) \cong H^1(X, \mathcal{O}_X).
\]

There’s a general theorem saying that the representing space, if it exists, must be locally of finite type. If \( X \) were not proper, then \( H^1(X, \mathcal{O}_X) \) could be infinite-dimensional, so you see a priori that a representing space can’t exist.

**Exercise 2.4.7.** Let \( X \) be a smooth, proper, and geometrically connected curve of genus \( g \) over a field \( k \) such that \( X(k) \neq \emptyset \), and let \( P = \text{Pic}_{X/k} \) be its Picard scheme. By Exercise [2.4.6](#) the \( k \)-group scheme \( P \) is smooth of dimension \( h^1(X, \mathcal{O}_X) = g \) over \( k \) and \( P^0 \) is proper, so \( P^0 \) is an abelian variety of dimension \( g \). In this exercise we identify \( P^0(k) \) as a subgroup of \( P(k) = \text{Pic}(X) \) parametrizing line bundles of degree 0.

1. For any \( k \)-scheme \( S \) and section \( x \in X(S) = \text{X}_S(S) \), prove that the quasi-coherent ideal sheaf of the closed subscheme \( x : S \rightarrow X_S \) is an invertible sheaf whose local generators are nowhere zero divisors on \( \mathcal{O}_{X_S} \).
2. For a coherent sheaf \( \mathcal{F} \) on a proper \( k \)-scheme \( Y \), recall that the **Euler characteristic** \( \chi(\mathcal{F}) \) is defined to be \( \sum (-1)^i h^i(Y, \mathcal{F}) \). For an invertible sheaf \( \mathcal{L} \) on \( X \), prove that \( \chi(\mathcal{L}^n) = d_{\mathcal{L}} \cdot n + (1 - g) \) for an integer \( d_{\mathcal{L}} \); we call this integer the **degree of \( \mathcal{L} \)**.

Likewise, for a Weil divisor \( D = \sum n_i x_i \) on our curve \( X \), define \( \text{deg} D = \sum n_i [k(x_i) : k] \). Prove that both notions of degree are invariant under extension of the ground field, and that they coincide when \( Y = X \) and \( \mathcal{L} \cong \mathcal{O}_X(D) \).
Choose \( e \in X(k) \), and define \( X^g \to P \) by defining \( X(S)^g \to P(S) = \text{Pic}(X_S) / \text{Pic}(S) \) for any \( k \)-scheme \( S \) to be
\[
(x_1, \ldots, x_g) \mapsto \mathcal{O}_{X_S}(x_1) \otimes \ldots \otimes \mathcal{O}_{X_S}(x_g) \otimes \mathcal{O}_{X_S}(e)^{\otimes (-g)}.
\]
This map carries \((e, \ldots, e)\) to \( 0 \in P^0(k) \), so by connectedness of \( X^g \) this map factors through a map \( X^g \to P^0 \) between proper \( k \)-schemes. Using the Riemann-Roch theorem for \( X^k \), prove that this latter map on \( k \)-points hits exactly the line bundles on \( X^k \) of degree 0 (don’t ignore the case \( g = 0 \)).

(4) It is a general fact (proved in [Mum08] Ch. II, §5) that the Euler characteristic is locally constant for a flat coherent sheaf relative to a proper morphism of locally noetherian schemes. Deduce that there is a well-defined map of \( k \)-group schemes from \( P \) to the constant group \( \mathbb{Z} \) over \( \text{Spec} \ k \) assigning to any point of \( P(S) \) the locally constant function given by the fiberwise degree of the line bundle. Using that \( \mathbb{Z} \) as a \( k \)-scheme contains no nontrivial \( k \)-proper subgroups, prove that for any field \( K \), \( P^0(K) \) is the subgroup of degree 0 line bundles in \( \text{Pic}(X_K) \). (This depends crucially on the hypothesis that \( X(k) \neq \emptyset \); Grothendieck gave a way to define \( P = \text{Pic}_{X/k} \) without such a hypothesis on \( X \), and then \( P^0(k) \) can fail to have this concrete description when \( \text{Br}(k) \neq 1 \).)

**Smoothness.** \( \text{Pic}_{X/k} \) is smooth over \( k \) if \( \dim \text{Pic}_{X/k} = \dim T_0(\text{Pic}_{X/k}) \). (This is equivalent to \( \text{Pic}^0_{X/k} \) being \( k \)-smooth, since you can check this over \( \overline{k} \), and then you can translate using the abundance of rational points.) When is this true?

In §11 of [Mum08], Mumford proves Cartier’s Theorem that any locally finite type group scheme over \( k \) is smooth if \( \text{char} k = 0 \). In characteristic \( p \), there are already counterexamples for \( X \) a smooth, projective surface, where \( \text{Pic}_{X/k} \) is not smooth. This is the content of Mumford’s “Curves on an algebraic surface.”

There’s a miracle we’ll see later: for \( X \) an abelian variety, \( \text{Pic}_{X/k} \) is always smooth, even in positive characteristic. Here the infinitesimal smoothness criterion doesn’t work, and one has to use a more geometric construction.

**Exercise 2.4.8.** Let \( X \) be a smooth, proper, geometrically connected curve of genus \( g > 0 \) over a field \( k \), and assume that \( X(k) \neq \emptyset \). Choose \( x_0 \in X(k) \). Prove that \( X \to \text{Pic}_{X/k} \) defined on \( R \)-point (for a \( k \)-algebra \( R \)) by \( x \to \mathcal{O}(x) \otimes \mathcal{O}((x_0)_R) \) (where \( \mathcal{O}(x) := \mathcal{I}(x)^{-1} \) for the invertible ideal \( \mathcal{I}(x) \) of \( x \): \( \text{Spec}(R) \to X_R \) is a proper monomorphism, hence a closed immersion. Thus, the choice of \( x_0 \) defines a closed immersion of \( X \) into the abelian variety \( \text{Pic}_{X/k}^0 \) of dimension \( g \).
3. Line Bundles on Abelian Varieties

3.1. Some fundamental tools.

**Theorem 3.1.1** (Seesaw Theorem). Let $X$ be a proper scheme over $k$, which is geometrically reduced and geometrically connected. Let $X$ be a $k$-scheme and $L$ a line bundle on $X \times Y$. There exists a closed subscheme $Y_1 \hookrightarrow Y$ such that

\[ X_S \longrightarrow X \times Y \]
\[ \downarrow \quad \downarrow \]
\[ S \quad f \quad \downarrow \]
\[ \downarrow \quad \downarrow \]
\[ Y \]

has the property that $(\text{Id}_X \times f)^*L$ comes from $S$ if and only if $f$ factors through $Y_1$.

**Example 3.1.2.** Taking $S = \text{Spec } \overline{k}$, we see that $Y_1(k) = \{ y \in Y(\overline{k})|L_{X_y} \sim = \mathcal{O}_{Y_z} \}$.

**Exercise 3.1.3.** Let $\phi : Z \to S$ be a proper flat surjective map of schemes, with $S$ locally noetherian, and assume that the geometric fibers of $\phi$ are reduced and connected. $\mathcal{N}$ be a line bundle on $Z$. Prove that $\mathcal{N} \cong \phi^*\mathcal{M}$ for a line bundle $\mathcal{M}$ on $S$ if and only if $\phi_\mathcal{N}$ is invertible and the natural map $\phi^*\phi_\mathcal{N} \to \mathcal{N}$ is an isomorphism (in which case $\mathcal{M} \cong \phi_\mathcal{L}$). Deduce that in such cases, the formation of $\phi_\mathcal{L}$ commutes with any base change on $S$.

**Proof of Theorem 3.1.1**. Note that these conditions are insensitive to fpqc base change on $S$. Because of this, by Galois descent it’s enough to build $Y_1$ after finite Galois extension, so we may assume that $X(k) \neq \emptyset$. This is unnecessary in practice because we will only use the Seesaw Theorem when there is a rational point anyway.

Without loss of generality we may assume that we have $e \in X(k)$. It is harmless to replace $\mathcal{L}$ with $\mathcal{L} \otimes p_2^*(e^*\mathcal{L})^{-1}$, as this doesn’t affect the question of whether or not $\mathcal{L}$ is pulled back from $S$. So we have reduced to the case where we have a trivialization $\iota : \mathcal{O}_Y \cong e^*_\mathcal{L}$.

Then the data $(\mathcal{L}, \iota)$ is equivalent to a map $Y \xrightarrow{j} \text{Pic}_{X/k,e}$. By functoriality, the pullback of $(\mathcal{L}, \iota)$ to $X_S$ corresponds to the map $S \to Y \to \text{Pic}_{X/k,e}$ so we see that this line bundles come from $S$ if and only if the composite map is constant, i.e. $f$ factors through $Y_1 := j^{-1}(0)$.

If $X$ is an abelian variety, then $\text{Pic}_{X/k,e}^0$ is also an abelian variety, called the dual abelian variety. The upcoming result is fundamental to discussing the relationship between line bundles and the group law, which is needed to understand the dual abelian variety.

**Theorem 3.1.4** (Theorem of the Cube). Let $Z$ be separated and finite type over $k$, and $X, Y$ be proper schemes over $k$. Assume that $X, Z$ is geometrically integral, and $Y$ is geometrically reduced and connected. Let $x_0 \in X(k), y_0 \in Y(k), z_0 \in Z(k)$. Suppose $\mathcal{L}$ is a line bundle on $X \times Y \times Z$ such that $\mathcal{L}_{x_0} := \mathcal{L}|_{x_0 \times Y \times Z} \cong \mathcal{O}_{Y \times Z}$, and $\mathcal{L}_{y_0}, \mathcal{L}_{z_0}$ are also trivial. Then $\mathcal{L} \cong \mathcal{O}_{X \times Y \times Z}$.
Abelian Varieties
Math 249C, 2015

Proof. Since $\mathcal{L}_{m}$ is trivial, $\mathcal{L}$ is classified by a map $X \times Z \to \text{Pic}_{Y/k}$, and we want this to be the 0 map. (The Picard scheme exists because $Y$ is proper, and it is separated and locally of finite type.) The geometric hypotheses on $X \times Z$ are precisely those needed in order to apply the rigidity theorem, and we have that $X \times \{z_0\} \to 0$ because $\mathcal{L}_{z_0} \cong \mathcal{O}_{X \times Z}$. So $\varphi(x, z) = \varphi(x_0, z)$ for any $z$. But this is 0 because $\mathcal{L}_{z_0}$ is trivial on $Y \times Z$. 

**Theorem 3.1.5** ("Cubical structure on $\mathcal{L}$ on $A/k$."") Let $A$ be an abelian variety over $k$ and $\mathcal{L}$ invertible on $A$. For $S$ a $k$-scheme, $a_1, a_2, a_3 \in A(S)$ the line bundle

$$(a_1 + a_2 + a_3)^* \mathcal{L} \otimes (a_1 + a_2)^* \mathcal{L}^{-1} \otimes (a_1 + a_3)^* \mathcal{L}^{-1} \otimes (a_2 + a_3)^* \mathcal{L}^{-1}$$

$$\otimes a_1^* \mathcal{L} \otimes a_2^* \mathcal{L} \otimes a_3^* \mathcal{L} \otimes (e^* \mathcal{L})^{-1}_{S}$$

on $S$ is canonically trivial.

Proof. The proof we’re about to give does not use the fact that $k$ is a field (so it applies in a relative situation as well), as long as we include this last $(e^* \mathcal{L})^{-1}_{S}$ factor. This is trivial in the case of abelian varieties, because $e^* \mathcal{L}$ is a line bundle on $\text{Spec } k$.

It suffices to establish the universal case $T = A \times A \times A$ and $a_i = \text{pr}_i: T \to A$, because any $(a_i)$ is canonically a pullback of this one one, via

$$\xymatrix{ S \ar[r]^{(a_1, a_2, a_3)} & T \ar[d]^{\text{pr}_i} \ar[l]_{a_i} \ar[ld]_{} }$$

In this universal case, we have:

$$a_1 + a_2 + a_3 = m: A^3 \to A$$

$$a_1 + a_j = m_{ij}: A^2 \to A, \quad i \neq j \quad \text{i.e. } (x_1, x_2, x_3) \mapsto x_i + x_j$$

$$a_i = \text{pr}_i: A^3 \to A.$$ 

So the line bundle of interest is $\mathcal{M} = m^* \mathcal{L} \otimes m_{12}^* \mathcal{L}^{-1} \otimes m_{13}^* \mathcal{L}^{-1} \otimes m_{23}^* \mathcal{L}^{-1} \otimes \text{pr}_1^* \mathcal{L} \otimes \text{pr}_2^* \mathcal{L} \otimes \text{pr}_3^* \mathcal{L} \otimes (0^* \mathcal{L})^{-1}_{A}$ on $A \times A \times A$.

We want a canonical isomorphism $\mathcal{M} \cong \mathcal{O}_{A \times A \times A}$. If this isomorphism exists, then it is unique up to $k^*$. If we pull this back along the identity then we get $0^* \mathcal{M} \cong k \cong 1$, so if there is some isomorphism $\xi$ then we can normalize it by demanding that $0^* \xi = 1$.

By the theorem of the cube, it is enough to show that $M$ has trivial restriction to $\{0\} \times A \times A$. By symmetry, it suffices to treat $\{0\} \times A \times A$. Here you get

$$\mathcal{M}|_{\{0\} \times A \times A} \cong \mu^* \mathcal{L} \otimes q_1^* \mathcal{L}^{-1} \otimes q_2^* \mathcal{L}^{-1} \otimes \mu^* \mathcal{L}^{-1} \otimes (0^* \mathcal{L})_{A \times A} \otimes q_1^* \mathcal{L} \otimes q_2^* \mathcal{L} \otimes (0^* \mathcal{L})^{-1}_{A \times A}$$

where $\mu, q_1, q_2$ are the multiplication and projection maps $A \times A \to A$. Evidently this is canonically isomorphic to $\mathcal{O}_{A \times A}$. 

3.2. The $\phi$ construction. For $x \in A(S)$, let $t_x: A_S \to A_S$ be the translation map sending $y \mapsto x + y$.

**Definition 3.2.1.** Given a line bundle $\mathcal{L}$ on $A$, we define a map

$$\phi_{\mathcal{L}}: A \to \text{Pic}^0_{A/k}$$
Proposition 3.2.7. \( \phi \) descent datum on \( L \) cause of the lack of uniqueness, a descent datum on \( A \) \( K \) have Galois descent situations where \( L \) translating fact, it is a special kind of isogeny called a \( 3.2.5 \) is indeed the case.

We'll soon show that \( \phi \) is a homomorphism (for this, we may assume that \( k = \overline{K} \) and treat the \( k \)-points).

Example 3.2.2. If \( K \) is a field and \( \mathcal{L} \cong \mathcal{O}(D) \), then \( \phi \) sends \( x \in A(K) \) to \( t_{-x}(D_K) - D_K \in \text{Pic}^0(X_K) \). The content of this being a homomorphism is that it is multiplicative in \( x \in A(K) \). (Pulling back a divisor via translation by \( x \) correspondings to translation by \( -x \).)

Note the minus sign: it means that this is the negative of the usual isomorphism (e.g. from Silverman’s book).

Corollary 3.2.3 (Theorem of the square). The map \( \phi \) is a homomorphism, i.e. for any \( k \)-scheme \( T \) and \( x, y \in A(T) \), we have canonical isomorphisms

\[
t^*_x(L_T) \otimes L_T \cong t^*_y(L_T) \otimes (x, y)^*(m^* \mathcal{L} \otimes p_1^* \mathcal{L}^{-1} \otimes p_2^* \mathcal{L}^{-1} \otimes (e^* \mathcal{L})_A)|_{A_T}
\]

Remark 3.2.4. This is a relative version of the usual Theorem of the Square.

We will call the line bundle \( A(\mathcal{L}) := m^* \mathcal{L} \otimes p_1^* \mathcal{L}^{-1} \otimes p_2^* \mathcal{L}^{-1} \otimes (e^* \mathcal{L})_A \) the Mumford construction (this may be non-standard notation). If \( T = \text{Spec} \ K \), which is all we need in order to prove the homomorphism property, then we can ignore it, and it implies that

\[
t^*_x(L_K) \otimes L_K^{-1} \cong (t^*_x(L_K) \otimes L_K^{-1}) \otimes (t^*_y(L_K) \otimes L_K^{-1}).
\]

Proof. Let \([x]\) be the composition \( S := A_T \rightarrow T \xrightarrow{\phi} A \). Apply the Theorem of the Cube 3.1.5 to \( S = A_T \), with \( a_1 = p_1, a_2 = [x], a_3 = [y] \):

\[
(p_1 + [x] + [y])^* \mathcal{L} \otimes p_1^* \mathcal{L} \otimes x^* \mathcal{L} \otimes y^* \mathcal{L} \cong (x + y)^* \mathcal{L} \otimes (p_1 + x)^* \mathcal{L} \otimes (p_1 + y)^* \mathcal{L} \otimes e^* \mathcal{L}_A^{-1}
\]

You can check that \( A_T \xrightarrow{I} A_T \rightarrow A \in A(A_T) \) is \( \text{pr}_1 + [x] \) and \([x] + [y] = [x + y]\) in \( A(S) \).

Therefore, the above equation simplifies as

\[
t^*_x(L_T) \otimes L_T \otimes x^* \mathcal{L}_T \otimes y^* \mathcal{L}_T \cong t^*_x(L_T) \otimes t^*_y(L_T) \otimes e^* \mathcal{L}_A^{-1}.
\]

Rearranging this gives exactly what we wanted. \( \square \)

How can we produce interesting line bundles on \( A \)? If we knew that \( A \) were projective, then we could use geometry to get divisors, hence line bundles. We'll prove later that this is indeed the case.

Remark 3.2.5. We’ll eventually see that if \( \mathcal{L} \) is ample, \( \phi : A \rightarrow \text{Pic}^0_{A/k} \) is an isogeny. In fact, it is a special kind of isogeny called a polarization.

Remark 3.2.6. The map \( \phi \) does not “remember” \( \mathcal{L} \). For instance, \( \phi \) is unaffected by translating \( \mathcal{L} \). However, the map \( \phi \) turns out to be “more important” than \( \mathcal{L} \). You can have Galois descent situations where \( K/k \) is finite Galois, and \( \mathcal{L} \) on \( A \) such that \( \phi \) descends to \( A \rightarrow \text{Pic}^0_{A/k} \) but \( \mathcal{L} \) does not descend to \( A \), for Brauer group reasons. (Because of the lack of uniqueness, a descent datum on \( \phi \) doesn’t necessarily determine a descent datum on \( \mathcal{L} \).)

Proposition 3.2.7. \( \phi(-x) = \phi^{-1}(x) \) as maps \( A \rightarrow \text{Pic}^0_{A/k} =: \widehat{A} \).
Proof. There are two ways of doing this. We could do it functorially, but since it’s just a question of equality of two maps we can also check it on geometric points.

For \( x \in A(k) \), we want \( t^*_x(L) \otimes L^{-1} \cong t^*_x(L^{-1}) \otimes L \), which is equivalent to \( t^*_x L \otimes t^*_x L \cong L \otimes L \). By the Theorem of the Square, the left hand side is precisely
\[
t^*_{x+y}(L) \otimes L \cong L \otimes L.
\]
\[\square\]

Remark 3.2.8. In particular, this means that \( \phi_L \) looks “similar” (e.g. is an isogeny) to \( \phi_{L^{-1}} \), and in particular is similar whether \( L \) is ample or anti-ample.

Proposition 3.2.9. We have \( \phi_L \otimes L = \phi_L + \phi_L \).

Proof. Just compute on points: for \( x \in A \), the left hand side is \( t^*_x(L) \otimes L^{-1} \), and the right hand side is \( t^*_x L \otimes L^{-1} \otimes t^*_x L \otimes L^{-1} \).
\[\square\]

We defined \( L \rightarrow \phi_L \) for \( L \) on \( A \). However, we can make an analogous definition for abelian schemes: for \( L \) on \( A_S \), we can define a map
\[ \phi_L : A_S \rightarrow (\text{Pic}_{A/k})_S \]
sending \( x \rightarrow t^*_x(L) \otimes L^{-1} \), and this factors through \( (\text{Pic}_{A/k})_S \). In addition, this is even a homomorphism (by the Theorem of the Square in a relative setting). This lies slightly beyond our setup. One can prove the Theorem of the Cube for a line bundle \( L \) on \( A_S \) (not pulled back from \( A \)) and thereby make a morphism
\[ \text{Pic}_{A/k} \rightarrow \text{Hom}(A, \text{Pic}_{A/k}) \]
sending “\( L \rightarrow \phi_L \).” So \( \phi_L \) is not only a homomorphism, but “varies nicely” with \( L \).

Theorem 3.2.10. For \( x \in A(k) \), \( \phi_{t^*_x L} = \phi_L \) for \( L \) on \( A \).

Proof. We can check the equality on \( \overline{k} \)-points, so assume \( k = \overline{k} \). The claim is equivalent to
\[ \phi_{t^*_x L}(y) = \phi_L(y). \]
This in turn is equivalent to
\[ t^*_y(t^*_x L) \otimes t^*_x L^{-1} = t^*_y L \otimes L^{-1} \]
i.e. \( t^*_x L \otimes L \cong t^*_x L \otimes t^*_y L \). But that is precisely the Theorem of the Square.
\[\square\]

Remark 3.2.11. In the relative setting of abelian schemes, one proves a rigidification theorem that equality of maps can be checked on fibers, and hence a lot of the theory can be bootstrapped from the case of abelian varieties.

Another Proof. We have a map \( A \rightarrow \text{Hom}(A, \text{Pic}_{A/k}) \). It turns out that this latter scheme is étale over \( k \) (satisfies the infinitesimal criterion), hence just a bunch of points. This maps \( x \in A(T) \) to \( \phi_{t^*_x(L,T)}(A) \) on \( A_T \), hence \( e \rightarrow L \). A map from connected to étale over \( k \) must be constant!
\[\square\]
Remark 3.2.12. This second proof illuminates the geometric content of the theorem, which is that the Hom scheme is discrete. For instance, if $E$ is an elliptic curve then $\text{Hom}(E, E)$ is the constant scheme $\mathbb{Z}$.

Definition 3.2.13. If $L$ is a line bundle on $A$, then we define

$$K(L) := \ker \phi_L = \phi_{L^{-1}}(0).$$

Finiteness properties of $K(L)$ detect ampleness in certain cases (but note that Proposition 3.2.7 implies that $K(L^{-1}) = K(L)$, so ampleness cannot be detected by the kernel in general).

Remark 3.2.14. Note that $K(L) = A \iff \phi_L = 0 \iff t^*_x L \cong L$ for all $x \in A(k)$.

Later we’ll see that this happens exactly when $L \in \text{Pic}^0_A(k) \subset \text{Pic} A/k$. For curves $X$, the identity component of $\text{Pic}$ is characterized by having degree 0. For an abelian variety, $\text{Pic}^0 A/k$ is characterized by the triviality of $\phi_L$.

3.3. The Poincaré bundle. On $A \times \text{Pic}^0 A/k$, we have the restriction $(\mathcal{P}_A, \theta)$ of the universal line bundle on $A \times \text{Pic} A/k = \text{Pic} A/k$, where

$$\theta : \mathcal{P}_A|_{A \times \text{Pic}^0 A/k} \cong \mathcal{O}_{\text{Pic}^0 A/k}.$$

Then $\mathcal{P}_A|_{A \times [0]} \cong \mathcal{O}_A$, as it corresponds to the classifying map

$$A \times A \to A \times \text{Pic} A/k \to \text{Pic} A/k.$$

This isomorphism has a $k^\times$ ambiguity, but we can make it canonical by requiring that on $(0,0)$ (i.e. Spec $k$) it agrees with the restriction of $\theta$.

The Poincaré bundle is the key to a symmetric relationship between an abelian variety and its dual, analogous to the evaluation pairing between a vector space and its dual.

The universal property of the Poincaré bundle $\mathcal{P}_A$ over $A \times \text{Pic}^0 A/k$ is that a map $f : T \to \text{Pic}^0 A/k$ is equivalent to a $p_2$-trivialized line bundle $W$ on $A \times T$, where $f(t) = W_t \in \text{Pic}^0 A/k$ on $A_t$. Therefore, $\phi_L$ is determined by the line bundle

$$\theta(L) := (1 \times \phi_L)^*(\mathcal{P}_A)$$

on $A \times A$. Informally, $\theta(L)|_{A \times [x]} = t^*_x (L^*_K) \otimes L^{-1}_K$ for $x \in A(k)$. We would like to have a nice “global” description of this bundle.

Proposition 3.3.1. We have a canonical isomorphism

$$(1 \otimes \phi_L)^*(\mathcal{P}_A) \cong \Lambda(L) := m^*(L) \otimes p_1^*(L^{-1}) \otimes p_2^*(L^{-1})$$

as $e \times 1_A$-trivialized line bundles.
Remark 3.3.2. The isomorphism is unique up to units from the base $k^*$. This is made canonical by demanding that pulling back via $e \times 1_A$ identifies the canonical trivializations. The definition of $\mathcal{P}_A$ includes a trivialization of $(1 \times \phi_\mathcal{L})(\mathcal{P}_A)$ after pulling back to via $e \times 1_A$, and pulling back the right hand side by $e \times 1_A$ gives $\mathcal{L} \otimes (e^*\mathcal{L}^{-1})_A \otimes \mathcal{L}^{-1}$ which has a canonical isomorphism with $\mathcal{O}_A$.

Proof. We invoke the Seesaw Theorem, which says that it is enough to check an isomorphism on $\{e\} \times A$ and $A \times \{x\}$ for all $x \in A(K)$ where $K$ is any algebraically closed field, which we may take to be $\overline{k}$.

To see why this follows from the Seesaw Theorem, first note that by taking the difference of the two line bundles, it suffices to check that $\mathcal{L}$ on $A \times S$ is trivial if and only if $\mathcal{L}$ is trivial on $\{e\} \times S$ and $A \times \{x\}$ for all $x \in S(K)$. By the Seesaw theorem, the second condition implies that $\mathcal{L}$ is pulled back from a line bundle on $S$, and the first condition guarantees that this is the trivial bundle. We remark that it is not much harder to prove this fact directly, essentially by tracing out the argument in the Seesaw Theorem. The first condition says that $\mathcal{L}$ is classified by a map $S \to \text{Pic}^0_{A/k}$. The second says that all geometric points of $S$ map to $0 \in \text{Pic}^0_{A/k}$, hence the map $S \to \text{Pic}^0_{A/k}$ is the trivial map.

On $\{e\} \times A$, the left hand side is trivial because $\mathcal{P}_A$ is $e \times 1_A$-trivialized. On the right hand side, we get $\mathcal{L} \otimes (e^*\mathcal{L})^{-1}_A \otimes \mathcal{L}^{-1} \cong \mathcal{O}_A$.

On $A \times \{x\}$, the left side is $\theta(\mathcal{L})|_{A \times \{x\}} = t^*_x \mathcal{L}_K \otimes \mathcal{L}_K^{-1}$. On the right hand side, we get $\mathcal{L}_K \otimes \mathcal{L}_K^{-1} \otimes (x^*\mathcal{L})^{-1}_A$. Again, these are identified because $x^*\mathcal{L}$ is trivial. □

We'll shortly use properties of $\phi_\mathcal{L}$ to produce ample line bundles on abelian varieties.

3.4. Projectivity of abelian varieties. We now want to prove that abelian varieties are projective, i.e. that they possess ample line bundles. First, we digress to discuss a question concerning using Weil divisors versus line bundles. Why not work with Weil divisors instead of line bundles, since they are much more concrete? Line bundles are an "intrinsically" object, while Weil divisors are more like a crutch for computation. Since linearly equivalent divisors correspond to the same line bundle, they are less suited for descent arguments (for example). Also, they don't generalize to the case where the base is not a field. Now, they do have their merits, but the line bundle formalism does too.

Theorem 3.4.1. Any abelian variety $A/k$ is projective.

Proof. Let $X$ be a proper $k$-scheme. If $X_\overline{k}$ is projective over $\overline{k}$, then so is $X/k$.

Remark 3.4.2. It is even enough that $X_K$ is projective over $K$ for some $K/k$.

Proof. The goal is to build an ample line bundle $\mathcal{L}$ on $X$. To do this, choose a projective embedding $\bar{j} : X_\overline{k} \hookrightarrow \mathbb{P}^n_{\overline{k}}$. As this involves only a finite amount of data, and $\overline{k} = \lim_{\text{finite}} k$, Exercise 1.7.9 implies that $\bar{j}$ descends to $X_K \hookrightarrow \mathbb{P}^n_k$ for some finite, normal $K/k$. 

28
Now we can split this extension as a purely inseparable extension of a Galois extension:

\[
\begin{array}{c}
K_0 \\
\text{purely inseparable} \\
K \\
\text{Galois} \\
k
\end{array}
\]

So it suffices to descend projectivity in the two cases: \( K/k \) purely inseparable (obviously only interesting in positive characteristic) or Galois.

Let's first dispose of the purely inseparable case. The trick is to use Frobenius. If you write \( K/k \) as a tower of primitive extensions, then there exists some \( e > 0 \) such that \( f^p \in k \) for all \( f \in K \). The upshot of that is as follows. If \( \pi: X_K \to X \) is the projection, and \( \mathcal{L} \) is ample on \( X_K \), then the transition functions of \( \mathcal{L} \) are invertible functions on certain open subset of \( X_K \). If you raise these transition functions to the \( p^e \)th power, you still get an ample line bundle, but you can get them to be defined over \( k \).

Let us try to rigorously (and intrinsically) formulate this argument. We have a natural map \( i: \mathcal{O}_X \hookrightarrow \mathcal{O}_{X_K} \), and \( t \mapsto t^{p^e} \) gives a map \( \pi_* \mathcal{O}_{X_K}^* \to \mathcal{O}_X^* \) (as you can check locally over affines in \( X \)). Therefore, \( i: \mathcal{O}_X^* \hookrightarrow \pi_*(\mathcal{O}_{X_K}^*) \) has cokernel killed by \( p^e \). Now here is the key point: the line bundle \( \mathcal{L} \) on \( X_K \) is trivialized by an affine open cover coming from \( X \). Indeed, for all \( x \in X \) the ring \((\pi_* \mathcal{O}_{X_K} \) is semi-local (i.e. has finitely many maximal ideals), and we have the following lemma:

**Lemma 3.4.4.** Any semi-local ring \( R \) has trivial Picard group.

**Proof.** Let \( m_1, \ldots, m_n \) be the maximal ideals of \( R \), and \( M \) be a locally free module over \( R \). For each \( m_i \), \( M/m_iM \) is an \( n \)-dimensional vector space over \( R/m_i \). Let \( m_{i_1}, \ldots, m_{i_n} \) be generators in \( M/m_iM \) for each \( i \).

We claim that there exist \( x_j, j = 1, \ldots, n \) such that \( x_j \equiv m_{i_j} \) (mod \( m_i \)) for each \( i \). This is just the Chinese Remainder Theorem.

Then the map \( R^n \to M \) sending \( e_j \to x_j \) is surjective modulo \( m_i \), hence localizes to a surjective map \( R^n_{m_i} \to M_{m_i} \) for each \( i \) by Nakayama's Lemma, hence is surjective. \( \square \)

This is a general phenomenon. For any finite flat map, a line bundle upstairs trivializes Zariski locally downstairs (although this is trivial to see in the inseparable case, since the map is also a homeomorphism). In other words, by spreading out there is an open cover \( \{ U_a \} \) of \( X \) such that \( \mathcal{L} \) is trivial on \( p_1^{-1}(U_a) \). This implies that \( \text{Pic}(X_K) = H^1(X, \pi_* \mathcal{O}_{X_K}^*) \) (which is not true by general nonsense because \( \pi_* \mathcal{O}_{X_K}^* \) is not quasicoherent), hence the cokernel of the map \( H^1(X, \Omega_X^e) \to H^1(X, \pi_* \mathcal{O}_{X_K}^*) \), which may be identified with the natural map \( \text{Pic}(X) \to \text{Pic}(X_K) \), has cokernel killed by \( p^e \). The upshot is that \( \mathcal{L}^{p^e} \cong \mathcal{N}_K \) for some line bundle \( \mathcal{N} \) on \( X \).

Since the line bundle \( \mathcal{N} \) on \( X \) pulls back to an ample line bundle on \( X_K \), \( \mathcal{N} \) is ample on \( X \) because ampleness descends. There are various ways to see this; perhaps the cleanest
Abelian Varieties

Math 249C, 2015

is Serre’s criterion: \( \mathcal{N} \) is ample if and only if for any coherent sheaf \( \mathcal{F} \) on \( X \), we have
\[
H^i(X, \mathcal{F} \otimes \mathcal{N}^{\otimes m}) = 0 \quad \text{for} \quad m \gg 0.
\]
But by flat base change,
\[
H^i(X, \mathcal{F} \otimes \mathcal{N}^{\otimes m}) = H^i(X_K, \mathcal{F}_K \otimes \mathcal{N}_K^{\otimes m})
\]
and this vanishes for \( m \gg 0 \) by Serre’s vanishing criterion.

Now we can move on to the Galois case, so suppose \( K/k \) is Galois with Galois group \( \Gamma \). Given \( L \) on \( X_K \), we define \( M = \bigotimes_{\gamma \in \Gamma} \gamma^*(L) \), which has the effect of taking the norm on transition functions. This is ample, as each \( \gamma^*L \cong L \) by the isomorphism \( \gamma: X_K \cong X_K \), and a tensor product of ample line bundles is ample.

Once again, the finite flatness of the map implies that there is a Zariski-local trivialization over \( X \), so \( \mathcal{N} = \text{Nm}_{X_K/X}(L) \) is a line bundle on \( X \) such that \( \mathcal{N}_K \cong M \).

Remark 3.4.5. A generalization of this is that the norm takes an ample line bundle to an ample line bundle under a finite faithfully map of schemes proper over a noetherian ring.

This shows that for the purposes of proving Theorem 3.4.1 it suffices to work over an algebraically closed field. So now we can restrict our attention to an abelian variety \( A \) over an algebraically closed field \( k = \overline{k} \). We have to produce a line bundle on \( A \) which is ample, but how?

We construct the divisor of the line bundle. Let \( U \subset A \) an affine open neighborhood of \( e \). We note that \( A \) is noetherian, normal, and separated. It is a general fact that in this situation, \( D := (A - U)_{\text{red}} \) is of pure codimension 1.

Exercise 3.4.6. Let \( Y \) be a normal, locally noetherian separated scheme, and \( U \) a dense affine open in \( Y \). Prove that \( Y - U \) has pure codimension 1 in the sense that its generic points have codimension 1 in \( Y \).

We want to show that \( D \) is ample, or rather that \( \mathcal{O}_A(D) \) is ample. We’re going to prove this by considering the stabilizer of \( D \) under translation.

Lemma 3.4.7. The group \( \{ x \in A(\overline{k}) \mid t_x^*(D_{\overline{k}}) = D_{\overline{k}} \text{ topologically} \} \) is finite.

Proof. Without loss of generality, \( k = \overline{k} \) and \( D = D_{\overline{k}} \) is reduced. First we show that the stabilizer of \( D \) is a Zariski-closed subgroup of \( A \) (which is geometrically obvious). Note that \( t_x^*D = D \iff t_x^*(D) \subset D \), by some combinatorics of accounting for the components and their dimensions. This is the same as \( x + d \in D \) for all \( d \in D(k) \), i.e. \( x \in \bigcap_{d \in D(k)} (-d + D) \), which is closed.

But if \( t_x \) preserves \( D \), then it also preserves \( U = A \setminus D \), hence \( x \in U \) since \( e \in U \). So this Zariski-closed subgroup (which is proper, being closed in \( A \)) lies in an affine chart, hence is finite.

This turns out to be the key to ampleness. We’ll now state four conditions on a divisor on an abelian variety, which we’ll prove are equivalent. The first is finiteness of the
Proposition 3.4.8. If $D \subset A/k = \mathcal{O}$ is an effective reduced Weil divisor and $\mathcal{L} = \mathcal{O}(D) = \mathcal{O}_D^{-1}$, then the following are equivalent:

1. \{$x \in A(\mathcal{O}) \mid t^*_x(D_F) = D_F$\} is finite
2. $\mathcal{K}(\mathcal{L}) = \{x \in A \mid t^*_x \mathcal{L} \cong \mathcal{L}\}$ is finite,
3. $\mathcal{L}^{\otimes 2}$ has no basepoints (i.e. $\mathcal{O}_A \otimes \Gamma(\mathcal{L}^{\otimes 2}) \rightarrow \mathcal{L}^{\otimes 2}$ and $A \rightarrow \mathbb{P}(\Gamma(\mathcal{L}^{\otimes 2}))$ is finite.

(Since everything here is proper, this is the same as quasifinite, i.e. doesn’t contract curves.)

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

Remark 3.4.9. (2) obviously implies (1), since $t^*_x(D_F) = D_F$ obviously implies $t^*_x \mathcal{L} \cong \mathcal{L}$ (and seems much stronger), but the two are actually equivalent in this setting.

Proof. We’re going to show that $(3) \implies (4) \implies (2) \implies (1) \implies (3)$. The last step is the most geometric (no basepoints is easy, but the quasifiniteness is not).

$(3) \implies (4)$. For the finite map $\varphi : A \rightarrow \mathbb{P}(\Gamma(\mathcal{L}^{\otimes 2}))$, we have $\varphi^*(\mathcal{O}_1) \cong \mathcal{L}^{\otimes 2}$. But under a finite morphism, the pullback of an ample line bundle is ample (for example by Serre’s cohomological criterion, and the fact that $H^i(A, \mathcal{F}) = H^i(\mathbb{P}(\Gamma(\mathcal{L}^{\otimes 2})), \varphi_* \mathcal{F})$ since $\varphi$ is finite.

$(4) \implies (2)$. Let $B = (\ker \phi \mathcal{L}_\text{red})^0$, which is an abelian subvariety of $A$ (which we want to show is trivial). By design, for all $b \in B(k)$ the map $\phi_{\mathcal{L}_b} : A \rightarrow \text{Pic}_{A/k}$ is trivial, so $t^*_b \mathcal{L} \cong \mathcal{L}$. Therefore, the pullback bundle $\mathcal{L}_B$ on $B$ has the property that $\phi_{\mathcal{L}_B} = 0$, and $\mathcal{L}_B$ is ample by hypothesis (since it is the restricton of an ample line bundle on $A$ via $B \hookrightarrow A$). This reduces to the following lemma:

Lemma 3.4.10. If $A$ is a non-zero abelian variety and $\mathcal{L}$ is an ample line bundle on $A$, then $\phi_{\mathcal{L}} \neq 0$.

Proof. To prove this, we’ll use the earlier result relating $\phi_{\mathcal{L}}$ and the Mumford construction:

$$(1 \times \phi_{\mathcal{L}})^*(\mathcal{P}_A) \cong \mathcal{N}(\mathcal{L}) = m^* \mathcal{L} \otimes p^*_1 \mathcal{L}^{-1} \otimes p^*_2 \mathcal{L}^{-1}.$$ 

By hypothesis, the left hand side is trivial on $A \times A$, so let’s see what happens to the right hand side. Restricting to the anti-diagonal, we get

$$(\mathcal{O}_A \cong (e^* \mathcal{L}) \otimes \mathcal{L}^{-1} \otimes ([-1]^* \mathcal{L})^{-1})$$

where $[-1]^* \mathcal{L}$ is ample, since $[-1]$ is an automorphism. Inverting the isomorphism, we see that the trivial line bundle is ample. This is impossible if $A \neq 0$, since we could restrict to a closed curve and then look at the degree. (Another way to see this is that it would imply the trivial line bundle were very ample, but its global sections consists only of constants by properness.) 

As mentioned, $(2) \implies (1)$ is trivial.
Finally we show (1) $\implies$ (3). We want to show that if $D \subset A$ is an effective divisor with \{x \in A(k) \mid t_x^*(D) = D\} finite, then:

1. $\mathcal{L}^{\otimes 2}$ (which is isomorphic to $\mathcal{O}_A(2D)$) has no base points, i.e. $\mathcal{O}_A \otimes \Gamma(\mathcal{L}^{\otimes 2}) \rightarrow \mathcal{L}^{\otimes 2}$, which in turn is equivalent to the condition that for all $x \in A(k)$, there exists some $s \in \Gamma(\mathcal{L}^{\otimes 2})$ such that $s(x) \neq 0$ in $\mathcal{L}(X)^{\otimes 2}$.

2. The map $f: A \rightarrow \mathcal{P}(\Gamma(\mathcal{L}^{\otimes 2}))$ sending $a \mapsto (\Gamma(\mathcal{L}^{\otimes 2}) \rightarrow \mathcal{L}(a)^{\otimes 2})$ is finite (i.e. doesn't contract any irreducible curve $C \subset X$).

We'll use the Theorem of the Square. In a sentence, it is useful here because it allows us to produce many effective divisors linearly equivalent to $\mathcal{O}(2D)$.

(1) is equivalent to the statement that for any $a \in A(k)$, there exists some effective $D' \sim 2D$ such that $a \notin \text{supp}(D')$ (i.e. “$a \notin D'$”). The Theorem of the Square implies that for all $x \in A(k)$, $(t_x^*)^*(D) + (t_x^*)^*(D) \sim 2D$ (the sum is as divisors, while translation is in the group law of $A$). So we just need to produce some $s$ such that $a \notin (t_x^*)^*(D)$ and $t_x^*(D)$. This is equivalent to $a \notin t_x^*(D)$ and $t_x^*(D)$, i.e. $\pm x + a \notin D$, i.e. $\pm x \notin a + D = t_a^*(D)$. But $t_a^*(D)$ is irreducible of codimension 1, so certainly there exist $x \notin \pm t_a^*(D)$. We see that this holds for any effective $D$.

For (2), suppose to the contrary that some irreducible closed curve $C \subset A$ lies in the fiber of $f$. But the fibers are exactly the effective divisors in the equivalence class of $2D$, so for every effective $D' \sim 2D$, either $C \subset |D'|$ or $C \cap |D'| = \emptyset$ (since $C$ lies in exactly one fiber). Again considering $D' = (t_x^*)^*(D) + (t_x^*)^*(D)$, we have that for all $x \in A$, either $C$ is disjoint from $(t_x^*)^*(D)$ or $C \subset (t_x^*)^*(D)$ or $(t_x^*)^*(D)$. We want to produce some $x$ that violates this property.

Lemma 3.4.12 below will imply that since the stabilizer of $D$ is finite, we are in the second case for all $x$, i.e. $C \subset (t_x^*)^*(D)$ for all $x \in A(k)$. This means that for any fixed $c_0 \in C$, $x + c_0$ or $-x + c_0 \in D$, so $x \in \pm c_0 + D$, which is clearly impossible.

\begin{lemma}
3.4.11. Suppose that $\Delta \subset A$ is an irreducible effective divisor. If $C$ is disjoint from $\Delta$, then $\Delta$ is preserved by $t_{x-y}$ for all $x, y \in C$.
\end{lemma}

\begin{proof}
Let $\mathcal{L} = \mathcal{O}(\Delta)$, so $\mathcal{L}|_C \cong \mathcal{O}_C$. Consider $t_a^*(\mathcal{L})|_C$ for $a \in A(k)$. We claim that $\deg t_a^*(\mathcal{L})|_C$ is independent of $a$, hence equal to 0 for all $a$. Informally, this is because we have a family of line bundles on $C$ parametrized by a connected space, and the degree is a “discrete” invariant.

Formally, $m^*(\mathcal{L})|_{A \times C}$ is a line bundle on $A \times C \rightarrow A$. On the $a$-fiber, we get $t_a^*(\mathcal{L})|_C$.

Now $A \times C \rightarrow A$ is a proper flat map, and it is a general fact that if $X \rightarrow S$ is a proper map to a connected, Noetherian base and $\mathcal{F}$ is coherent and $S$-flat, then $\chi(\mathcal{F}_s)$ is independent of $s \in S$. As a special case, for a line bundles $\mathcal{N}$ on a scheme $X$ flat over $S$, $\chi(\mathcal{N}_{S}^{\otimes n})$ is independent of $s$. But for a curve, this is a polynomial in $n$ whose linear coefficient reads off the degree of the line bundle (note the importance of being able to vary $n$ in this argument).

Geometrically, $t_a^*(\mathcal{L}) = \mathcal{O}(t_{-a}(\Delta))$ so $t_{-a}(\Delta)|_C$ has degree 0 for all $a \in A$. If $C \cap t_{-a}(\Delta)$ were non-empty and finite, then $\mathcal{O}(t_{-a}(\Delta))|_C \cong \mathcal{O}_C(C \cap t_{-a}(\Delta))$ would have positive degree. The upshot is:

32
Recall that we wanted to show that $t_{x-y}(\Delta) = \Delta$ for all $x, y \in C$, which is equivalent to $t_x(\Delta) \subset t_y(\Delta)$ for all $x, y \in C$. We deduce this by applying the observation above to a judicious choice of $a$.

For any $z \in \Delta$, choose $a = y - z$. Then $t_{y-z}(\Delta) \ni y - z + z = y$, hence $C \subset t_{z-y}(\Delta)$.

Then for any $x \in C$, we have $x - y + z \in \Delta$, i.e. $x + z \in t_y(\Delta)$, which says that $t_x(\Delta) \subset t_y(\Delta)$, which is what we wanted.

□

Lemma 3.4.12. Assume that $\{x \in A \mid t^*_x(D) = D\}$ is finite. For an irreducible closed curve $C \subset A$, and all $x \in A$, we have $C \cap (t^*_x(D) + t^*_x(D)) \neq \emptyset$.

Proof. Let $D = \sum_{i} n_i D_i$. Assume that for some $x_0$ that $C$ is disjoint from $t^*_x(D) + t^*_x(D)$, so $C$ is disjoint from $t^*_{x_0}(D_i)$ for all $i$.

By Lemma 3.4.11 for all $i$, $t^*_{x_0}(D_i)$ is preserved by $t^*_{x-y}$ for all $x, y \in C$. Then taking $\sum n_i D_i$, we have that $t^*_{x-y \pm x_0}(D) = D$ for all $x, y \in C$, which contradicts the finiteness hypothesis.

□
4. TORSION

4.1. Multiplication by $n$. We now study the torsion structure of abelian varieties. The first step is to examine the multiplication-by-$n$ map

$$[n]: A \to A.$$ 

**Theorem 4.1.1.** $[n]: A \to A$ is finite flat surjection.

**Remark 4.1.2.** Later we’ll see that $[n]$ has degree $n^{2 \dim A}$.

**Proof.** It is enough to show that $\ker([n])$ is finite. Assuming this, we immediately deduce that $[n]$ is quasi-finite, and by dimension considerations, the image must be dominant. Since $[n]$ is also proper, because $A$ is, it is finite and surjective. Therefore, if we grant the finiteness of $\ker([n])$ then for all $a \in A(k)$ we see that

$$\dim \mathcal{O}_{A,a} = \dim \mathcal{O}_{A,[n](a)} + \dim \mathcal{O}_{[n]^{-1}(a), a} - 0.$$

Then to obtain flatness, we can invoke the Miracle Flatness theorem:

**Theorem 4.1.3** (Miracle Flatness). Suppose $f: A \to B$ is a local map of local noetherian rings such that

$$\dim B = \dim A + \dim(B/f(m_A)B),$$

and $A$ is regular and $B$ is Cohen-Macaulay. Then $f$ is automatically flat.

**Proof.** See Matsumura’s *Commutative Ring Theory*, §23.1.

So why is the kernel finite? There’s an easy case: if $ch k \nmid n$, then $\text{Lie}([n]) = n: T_e(A) \to T_e(A)$ TONY: [ref: homework exercise], which induces an isomorphism. That implies that $[n]$ is étale at $e$. Thus $[n]^{-1}(0)$ is finite type plus étale at $e$, hence finite.

One might try to use this observation at $n$ away from $p$ to deduce the result for $p$. However, we don’t know the degree of $[n]$ - for all we know, these could all be isomorphisms.

Let $Z = A[n]$ (automatically proper). We want to show it’s affine, as that (together with properness) implies finiteness. To get at this, we need to study $[n]^* \mathcal{L}$ for ample $\mathcal{L}$. This will come out of the following digression.

**Theorem 4.1.4.** We have

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

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

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

**Remark 4.1.5.** In the complex-analytic setting, where line bundles are described by linear algebraic data (Apple-Humbold Theorem?) then this becomes very concrete.
Proof. Note that the second two lines follow straightforwardly from the first.

For $n = 0, 1$, the result is trivial. The strategy is to induct up and then down: we show that if it's true for $n$ and $n + 1$, then it's true for $n + 2$ (hence the result for all positive $n$), and if it's true for $n + 1, n + 2$ then it's true for $n$ (hence the result for all negative $n$).

Apply the Theorem of the Cube with $a_1 = [n + 2], a_2 = [1] = \text{Id}, a_3 = [-1] = -\text{Id}$ for $A(S), S = A$. Then

$$a_1 + a_2 + a_3 = [n + 1]$$
$$a_1 + a_2 = [n + 2]$$
$$a_1 + a_3 = [n]$$
$$a_2 + a_3 = [0]$$

and the Theorem of the Cube says

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

Rearranging so that there are only positive exponents, we have

$$[n + 2]^* \mathcal{L} \otimes [n + 1]^* \mathcal{L} \otimes [n]^* \mathcal{L} \cong \mathcal{L} \otimes [−1]^* \mathcal{L}.$$

Exercise 4.1.6. Check that this relation is enough to conclude the result.

Now we apply the theorem to an ample line bundle $\mathcal{L}$ on $A$, and pull back to $Z = A[n]$, obtaining

$$\mathcal{O}_Z \cong \mathcal{L}_Z^{[n + 2]^\mathcal{L}} \otimes ([−1]^* \mathcal{L})^{[n]^\mathcal{L}}$$

where $\mathcal{L}_Z, ([−1]^* \mathcal{L})_Z = [−1]^* (\mathcal{L}_Z)$ are ample on $Z$. Since $n \neq 0$, at least one of the exponents is actually positive, so we find that $\mathcal{O}_Z$ is ample.

Exercise 4.1.7. Show that if $Z$ is a proper (projective) scheme over an affine and $\mathcal{O}_Z$ is ample, then $Z$ is finite.

Proof. Serre’s vanishing theorem implies that twisting by $\mathcal{O}_Z$ eventually kills the higher cohomology of coherent sheaves, but this twisting does nothing, so the result follows from Serre’s criterion for affineness. Alternatively, $\mathcal{O}_Z$ would then be very ample, hence $H^0(Z, \mathcal{O}_Z)$ would give an embedding of $Z$ into $\mathbb{P}^n_{\text{Spec } A}$, but by properness $H^0(Z, \mathcal{O}_Z)$ is finite over $A$.

Digression on ampleness. There are several possible definitions of ample.

1. The “correct” one is in EGA II, which we won’t give. It looks frightening at first, but after some familiarity you realize that it is quite elegant.
2. The second is that $\mathcal{L}$ is the pullback of $\mathcal{O}(1)$ under some immersion into $\mathbb{P}^n_A$.
3. The third definition is that tensoring kills higher cohomology of coherent sheaves.

The second and third are equivalent for proper $X$ over $A$. The first two are equivalent for $X$ separated of finite type over $A$.
Remark 4.1.8. Ample symmetric line bundles $\mathcal{L}$ correspond to positive-definite quadratic forms. Away from characteristic 2, quadratic forms are related to symmetric bilinear forms.

We want to compute $\deg([n])$ (for $n \neq 0$), but what does this mean anyway? We know that $[n] : A \to A$ is finite flat and $A$ is connected and noetherian, so there is a common degree of all fibers are geometric points. Note that it is the same as $\deg([−n])$ since $[−n] = [n] \circ [−1]$, and $[−1]$ is an isomorphism. This means that without loss of generality, we may assume that $n > 0$.

Example 4.1.9. If $\text{ch} k \nmid n$, then $T_e(A[n]) = \ker(T_0(A) \to T_0(A))$. This kernel is 0 if $\text{char} k \nmid n$, so $A[n]_{\overline{k}}$ is a finite constant $\overline{k}$-scheme (by Nakayama's Lemma, and the homogeneity). Therefore, in this case $A[n]_{\overline{k}} = \coprod_{\deg([n])} \text{Spec}(\overline{k})$, i.e. $\#A(\overline{k})[n] = \deg([n])$.

(This is very interesting for $A = \text{Pic}^0_{X/k}$ for $X$ a smooth projective curve.)

Theorem 4.1.10. If $A$ is an abelian variety of dimension $g$, then $\deg([n]) = n^{2g}$.

The outline is as follows. First we clarify a notion of degree of line bundles on projective varieties, then we show that under pullback by a finite map the degree is multiplied by the degree of the map.

Choose an ample line bundle $\mathcal{L}$ on $A$, and replace $\mathcal{L}$ with $\mathcal{L} \otimes [−1]^*\mathcal{L}$ so $\mathcal{L} \cong [−1]^*\mathcal{L}$ (so $\mathcal{L}$ is symmetric). Then

$$[n]^*\mathcal{L} \cong \mathcal{L}^{n^{2g}} \otimes ([−1]^*\mathcal{L})^{n^{2g}} \cong \mathcal{L}^{n^2}.$$ 

Now we want to compute the “degree” of both sides. This is the rate of growth of Euler characteristic of its powers, namely this is a polynomial in $n$ and its leading coefficient is what we call the degree.

Definition 4.1.11. Let $X/k$ be a proper scheme and $\mathcal{N}$ a line bundle on $X$. Let $\mathcal{F}$ be a coherent sheaf on $X$ (typically $\mathcal{O}_X$, but there is purpose to this generality). Then we consider $\chi(\mathcal{F} \otimes \mathcal{N}^\otimes r)$. This turns out to be a “numeric polynomial” $r$ of degree $\leq g \dim X$. (Numeric polynomial in $r$ means that it’s a polynomial in $r$ whose values are integers; such things are integral linear combinations of binomial coefficients.) This has the form

$$\frac{d_{\mathcal{F}}(\mathcal{F})}{g!} r^g + \text{(lower-order terms)} \text{ for } d_{\mathcal{F}}(\mathcal{F}) \in \mathbb{Z}$$

(basically because when expressed in binomial coefficient form, the leading-order term is $\binom{g+r}{r}$). When $\mathcal{F} = \mathcal{O}_X$, we call $d_{\mathcal{F}}(\mathcal{O}_X)$ the degree of $\mathcal{N}$, i.e.

$$\chi(\mathcal{N}^\otimes r) = \frac{\deg \mathcal{N}}{g!} r^g + \ldots$$

Reference: EGA III, 2.5.3.

Note that if we replace $\mathcal{N}$ by a positive power, then that goes into the $r$, and hence pops out into the constant term, i.e. for $e \in \mathbb{Z}$,

$$\deg(\mathcal{N}^e) = e^g \deg(\mathcal{N}).$$
It is a fact that if $\mathcal{N}$ ample, then $\deg \mathcal{N} > 0$. One way to see this is that by raising to a large power, we can assume that $\mathcal{N}$ is very ample. Then the degree is the usual notion, i.e. the number of intersection points with a generic codimension $g$ linear subspace. [EGA IV$_2$, 5.3]

Applying this in our situation, we find that $\deg ([n]^* \mathcal{L}) = (n^2)^g \deg \mathcal{L} = n^{2g} \deg \mathcal{L} \neq 0$.

It remains to show that $\deg ([n]^* \mathcal{L}) = (\deg [n]) \cdot (\deg \mathcal{L})$. This is a completely different question: how does the degree behave under finite flat pullback?

**Proposition 4.1.12.** Let $f : X' \to X$ be a finite flat map, with $X$ proper and integral. Let $d = \deg f$. Then for all invertible $\mathcal{L}$ on $X$,

$$\deg (f^* \mathcal{L}) = d \cdot \deg (\mathcal{L}).$$

**Proof.** This is matter of studying $\chi ((f^* \mathcal{L}^{\otimes r})) = \chi (f^*(\mathcal{L}^{\otimes r}))$. Since cohomology is preserved under a finite flat map this is the same as $\chi (f_*(\mathcal{O}_{X'} \otimes \mathcal{L}^{\otimes r}))$ (by the projection formula). Here $\mathcal{F} = f_*(\mathcal{O}_{X'})$ is a vector bundle on $X$ of rank $d$.

So we want to show that $\deg (\mathcal{F} \otimes \mathcal{L}^{\otimes r}) = \rank (\mathcal{F}) \deg (\mathcal{L})$. More generally, we can assert this for $\mathcal{F} \in \text{Coh}(X)$ where $\rank (\mathcal{F}) := \dim \mathcal{F}_n$:

$$\chi (\mathcal{F} \otimes \mathcal{L}^{\otimes r}) = \frac{\rank (\mathcal{F}) \cdot \deg (\mathcal{L})}{g!} r^g + \ldots.$$  

To prove this, we apply Grothendieck’s “unscrewing” technique. Let $\mathcal{C} \subset \text{Coh}(X)$ be the subcategory of all coherent $\mathcal{F}$ satisfying this equation. The key observation is that this behaves well in short exact sequences, because $\chi$ is additive in short exact sequences: namely if

$$0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}'' \to 0$$

is short-exact, then $\mathcal{F}', \mathcal{F}'' \in \mathcal{C} \implies \mathcal{F} \in \mathcal{C}$. Grothendieck’s unscrewing lemma (EGA III, 3.1.2) says: if $\mathcal{C}$ is an exact (meaning closed in short exact sequences, as above) full subcategory of $\text{Coh}(X)$, then $\mathcal{C} = \text{Coh}(X)$ provided that for all all irreducible, reduced, closed subschemes $Y \subset X$ there exists $\mathcal{G}_Y \in \mathcal{C}$ with $\text{supp} (\mathcal{G}_Y) = Y$ with $\rank (\mathcal{G}_Y) = 1$ (e.g. $\mathcal{G}_Y = \mathcal{O}_Y$). [The proof is some sort of filtration argument.]

Applying this above: for $Y = X$ this is the definition of degree, and for $Y \subsetneq X$ both sides are 0. \qed

4.2. **Structure of the torsion subgroup.** Now we investigate the structure of $A(E)[n] = A[n](E)$.

**Lemma 4.2.1.** Let $G \to S$ be a commutative group scheme killed by $n \neq 0$. Suppose $n = ab$ where $\gcd (a, b) = 1$. Then

$$G[a] \times G[b] \xrightarrow{\text{inclusion}} G$$

is an isomorphism.
Proposition 4.2.3. If $\mathcal{O}_C$ completes the proof, by the “functor of points” perspective.

Remark 4.2.2. If $k \not\mid \chi$ then $k$ has characteristic $p$, then torsion may have fewer geometric points.

$\kappa$ is a field extension of $\mathbb{U}$ using denominators) that the geometric fibers have size $\ell^2$, i.e.

$$\mathcal{O}_{G[a]} \otimes \mathcal{O}_{G[b]} = \mathcal{O}_G$$

exhibits $\mathcal{O}_{G[a]} \otimes \mathcal{O}_S \cong \mathcal{O}_{G[a]}$ as a direct summand of a projective. ☀️ TONY: [turn into exercise]

Proof. $G(T)$ is a $\mathbb{Z}/n\mathbb{Z}$-module, so $G(T) = G(T)(a) \times G(T)(b)$ via $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ (this is just a fact about all $\mathbb{Z}/n\mathbb{Z}$ modules, and $G(T)(a) \times G(T)(b) \cong G[a] \times G[b](T)$. That completes the proof, by the “functor of points” perspective. $\square$

Proposition 4.2.4. If $\text{ch } k \not\mid n$ then $A[n](\bar{k}) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.

Proof. By the lemma, we may assume that $n = \ell^e$ where $\ell \neq \text{ch } k$ and $e \geq 1$. We are claiming that $A[\ell^e](\bar{k}) \cong (\mathbb{Z}/\ell^e\mathbb{Z})^{2g}$ and the “multiplication by $\ell$” map $A[\ell](\bar{k}) \to A[\ell^{e-1}](\bar{k})$ makes the following diagram commute:

$$
\begin{array}{ccc}
A[\ell^e](\bar{k}) & \cong & (\mathbb{Z}/\ell^e\mathbb{Z})^{2g} \\
\downarrow & & \downarrow \text{reduction} \\
A[\ell^{e-1}](\bar{k}) & \cong & (\mathbb{Z}/\ell^{e-1}\mathbb{Z})^{2g}.
\end{array}
$$

We saw, in the course of the proof that $[\ell]$ is finite flat, that it is surjective. Therefore, we have a short exact sequence

$$0 \to A[\ell](\bar{k}) \to A[\ell^e](\bar{k}) \to A[\ell^{e-1}](\bar{k}) \to 0.$$ 

Any finite abelian group killed by $\ell^e$, i.e. a finite $\mathbb{Z}/\ell^e\mathbb{Z}$-module, with the property that multiplication by $\ell$ surjects onto the $\ell^{e-1}$-torsion, forces $A[\ell^e](\bar{k})$ to be free over $\mathbb{Z}/\ell^e$. So we know what we want up to knowing that $\dim_{\mathbb{F}_p} A[\ell](\bar{k}) = 2g$ (the base case).

So far everything has just been pure group theory, and in particular the discussion applies to any $\ell$. It only remains to show that $[\ell]: A \to A$ of degree $\ell^{2g}$ is separable on function fields, as that would imply (exercise, using the primitive element theorem and chasing denominators) that the geometric fibers have size $\ell^{2g}$ over some dense open subset of the target. Then the homogeneity implies that all geometric fibers are the “same,” in particular have size $\ell^{2g}$ (we wanted this for $[\ell]^{-1}(0) = A[\ell]$). But we know that $[\ell]^*$ induces a field extension of $k(A)$ of degree $\ell^{2g}$, which is not divisible by $\text{ch } k$, so it’s separable.

What if $\ell = p = \text{ch } k$? We expect, even from the theory of elliptic curves, that the torsion may have fewer geometric points.

Proposition 4.2.4. If $k$ has characteristic $p$, then $\dim_{\mathbb{F}_p} A[p](\bar{k}) \leq g$. (So $A[p](\bar{k}) \cong (\mathbb{Z}/p\mathbb{Z})^i$ for $i \leq g$.)

General setup: let $f: X \to Y$ be a finite surjection between varieties over $\bar{k}$. Then there exists a dense open subset $U \subset Y$ such that for all $u \in U(k)$, $\#X_u(k) = \deg_i(f)$. 

38
Exercise 4.2.5. Prove this. Write \( k(X)/K/k(Y) \), use denominators to spread out.

We want \( \deg_i([p]_A) \mid \deg([p]_A) = p^{2g} \) to be \( p^i \) for \( i \leq g \), i.e. we want \( p^g \mid \deg_i([p]_A) \). So we have to build a large inseparable field subextension inside the induced field extension. The general intuition (and “correct argument”) is that for a general commutative group scheme, multiplication by \( p \) always factors through Frobenius:

\[
A \xrightarrow{[p]} A \\
\text{Frob}_A \downarrow \quad \downarrow \\
A(p)
\]

and \( \text{Frob}_A \) has degree \( p^g \) because \( A \) is (by smoothness) Zariski-locally étale over \( \mathbb{A}^g \).

We’ll use a different argument. Without loss of generality we can assume that \( k = k \).

We’ll show instead that the field extension induced by \( [p]^* \) factors through \( k(A) \subset k(A)^p \subset k(A) \)

where the second inclusion has degree \( p^g \) by using a separating transcending basis of \( k(A)/k \) (which always exist over a perfect field), and is evidently purely inseparable.

Exercise 4.2.6. Work this out.

In our case, why does \( [p] \) factor through this subfield?

**Proposition 4.2.7.** \( d : k(A) \to \Omega^1_{k(A)/k} \) has as kernel exactly \( k(A)^p \).

**Proof.** HW4.

**Remark 4.2.8.** This clearly requires \( k \) being perfect, since any element of \( k \) is obviously killed by \( d \).

The goal is to show that \( d([p]^*f) = [p]^*df = 0 \). Even better, we claim that the map \( [p] : A \to A \) induces \( \Omega^1_{A/k} \to [p]_*\Omega^1_{A/k} \) is the 0 map. What is it about the group scheme that allows us to get a handle on multiplication by \( p \)? The key is that the sheaf of invariant one-forms has a basis at the tangent space (as with Lie groups), where we know that \( [p] \) induces the 0 map.

**Definition 4.2.9.** Let \( \ell_g : G \to G \) denote the left-multiplication map \( \ell_g(x) = g \cdot x \). We say that \( \omega \in \Omega^1_{G/k} \) is left-invariant if \( \ell^*_g \omega = \omega \) for all \( g \in G(T) \). We denote the sheaf of left-invariant one-forms on \( G \) by \( \Omega^1_{G/k} \).

**Theorem 4.2.10.** Let \( G \) be a group scheme locally of finite type over \( k \) and \( g = T_eG \). Then there exists a canonical isomorphism \( \mathcal{O}_G \otimes g^* \cong \Omega^1_{G/k} \) via \( g^* \).

**Exercise 4.2.11.** (HW4) Prove this identification.

For smooth \( G \), the left-invariance can be checked on \( T = \text{Spec} \overline{k} \).

**Remark 4.2.12.** It is easy to show that the map \( \Omega^1_{G/k} \to g^* \) is injective. The surjectivity is harder. See BLR, *Néron Models*. The smoothness is not even necessary!
Proof. See HW4. One separately proves that \( \mathcal{O}_G \otimes_k \Omega_{G/k}^{1,\ell} \xrightarrow{\sim} \Omega_{G/k}^{1,\ell} \) is an isomorphism, and the map \( \mathcal{O}_G \otimes_k \Omega_{G/k}^{1,\ell} \xrightarrow{\sim} \mathcal{O}_G \otimes \mathfrak{g}^* \) is an isomorphism. 

By the Theorem and dualizing \( \mathfrak{g}^* \), it suffices to show that \( T_{\ell}(p) : T_{\ell}(A) \to T_{\ell}(A) \) is 0. But of course, this effect is multiplication by \( p \) (this is true for any commutative group scheme) - “the derivative of multiplication is addition.” This is 0 since \( p = \text{ch} \, k \).

This is sufficient to show that \( [p] \) factors through \( \text{Frob}_{A/k} \). In general, suppose \( f : G \to H \) is a dominant rational map. Then we get a “rational homomorphism”

\[
G \times G \xrightarrow{f \times f} H \times H \\
\downarrow \quad \downarrow \\
G \xrightarrow{f} H
\]

(In general, you cannot compose rational maps, but since they are dominant in this case we can compose them.) It is a general fact that a rational homomorphism is defined everywhere. Over an algebraically closed field, you have enough rational points to perform translations (but caution that the topology on the product is not the product topology). Then, you use faithfully flat descent to get the general case.

For prime \( \ell \),

\[
T_{\ell}(A) = \lim_{n} A[\ell^n](T) \cong \begin{cases} 
\mathbb{Z}_\ell^{2g} & \ell \neq \text{ch} \, k, \\
\mathbb{Z}_\ell^i & \ell = \text{ch}(k).
\end{cases}
\]

Let \( V_{\ell}(A) = T_{\ell}(A)[\frac{1}{\ell}] \). If \( \ell \neq \text{ch} \, k \), then our argument shows that \( T_{\ell}(A[\ell^n]) = 0 \), so \( A[\ell^n]_{\Gamma} = \text{Spec } \overline{k} \), which is equivalent to \( \mathcal{O}(A[\ell^n]) \otimes_k \overline{k} \cong \overline{k}^{\mathbb{Z}_{\ell^{2g}}} \), which is equivalent to \( \mathcal{O}(A[\ell^n]) \) being a product of finite separable extension over \( k \), i.e. \( A[\ell^n] \) is étale over \( k \). Thus we see that \( A[\ell^n](\overline{k}) = A[\ell^n](k_{s}) \).

So \( T_{\ell}(A) = \lim_{n} A[\ell^n](k_{s}) \), which admits a continuous action of \( \text{Gal}(k_{s}/k) \) (continuous because every point is defined over some finite separable extension). This is the analogue of \( H_{1}(A, \mathbb{Z}_{\ell}) \) for \( k = \mathbb{C} \). We’ll study the map

\[
\mathbb{Z}_{\ell} \otimes \text{Hom}_{k}(A, B) \to \text{Hom}_{\mathbb{Z}[\text{Gal}]}(T_{\ell}(A), T_{\ell}(B))
\]

in order to control \( \text{Hom}_{k}(A, B) \) and \( \mathbb{Q} \otimes \text{End}_{k}(A) \).

Remark 4.2.13. If we know that \( \mathbb{Z}_{\ell} \otimes \mathbb{Z} \text{Hom}(A, B) \to \text{Hom}(T_{\ell}A, T_{\ell}B) \) is injective (which is true), then the isomorphism \( \mathbb{Z}_{\ell} \otimes \text{Hom}(A, B) \cong \mathbb{Z}_{\ell} \otimes \mathbb{Z} \text{Hom}(A, B)_{(\ell)} \) shows that \( \text{Hom}(A, B)_{(\ell)} \) is \( \mathbb{Z}_{\ell} \)-finite for \( \ell \neq \text{ch} \, k \), by an exercise of chasing elementary tensors (which has a highbrow interpretation as fpqc descent).

This does not formally imply that \( \text{Hom}(A, B) \) is \( \mathbb{Z} \)-finite. For instance, one can take \( M = \sum_{\ell \neq 7, 13} \frac{1}{p} \mathbb{Z} \subset \mathbb{Q} \), as \( M_{(\ell)} \) is \( \mathbb{Z}_{\ell} \)-finite for all \( \ell \) (if \( \ell \neq 7, 13 \), then \( M_{(\ell)} \equiv \frac{1}{\ell} \mathbb{Z}_{\ell} \), while if \( \ell = 7, 13 \) then we just get \( \mathbb{Z}_{\ell} \)).

To get that \( \text{Hom}(A, B) \) is \( \mathbb{Z} \)-finite, we’ll need some “positivity” input via ample line bundles (using duality). For this, we need the theory of the dual abelian variety. In the special case of elliptic curves, Silverman uses this positive property in the form that the degree is the composition of an isogeny with its dual isogeny, which depends critically on the fact that the dual is canonically isomorphic.
Remark 4.2.14. \( \text{Hom}(A, B) \) is torsion-free. Indeed, suppose \( A \overset{f}{\to} B \overset{[n]_B}{\to} B \) is trivial. But this also factors as

\[
\begin{array}{ccc}
A & \overset{f}{\to} & B \\
\downarrow{[n]_A} & & \downarrow{[n]_B} \\
A & \overset{f}{\to} & B
\end{array}
\]

and we know that \([n]_A\) is surjective, so the composition is 0 if and only if \( f \) is 0.
5. The Dual Abelian Variety

5.1. Smoothness. We need to do two things:

(1) Understand properties of \( \text{Pic}^0_{A/k} =: \tilde{A} \). (Now that we know \( A \) is projective, which didn't require results from the theory of Picard schemes, we can "just" use Grothendieck's results for projective varieties.)

(2) Understand properties of the map \( \phi_\mathcal{L}: A \to \text{Pic}^0_{A/k} \) sending \( x \to t_x^* (\mathcal{L}) \otimes \mathcal{L}^{-1} \), especially for ample \( \mathcal{L} \). These are "polarizations."

For (1), since \( A \) is smooth, projective, and geometrically integral then one knows by HW1 that \( \text{Pic}^0_{A/k} \) is proper and geometrically irreducible. (In general, the Picard scheme is locally of finite type, and the homework exercise says that the identity component is geometrically integral. In this case, that is a little silly because Grothendieck's construction exhibits the Picard scheme as locally of finite type.) We don't yet know about smoothness or dimension. This is a serious concern, because the Picard scheme can be non-reduced in general, but we will see that for abelian varieties it is always smooth of dimension \( g = \dim A \).

We are not going to use the infinitesimal criterion for smoothness, because we don't know enough about abelian varieties to make an argument along those lines.

So we are instead going to study \( T_0(\text{Pic}^0_{A/k}) = T_0(\text{Pic}_{A/k}) \cong H^1(A, \mathcal{O}_A) \) (last equality by HW1). Choose \( \mathcal{L} \) ample of the form \( \mathcal{O}_A(D) \) for an effective \( D \), and consider \( \Phi_\mathcal{L}: A \to \text{Pic}^0_{A/k} \subset \text{Pic}_{A/k} \) (because \( A \) is connected and \( \phi_\mathcal{L} \) sends the identity to the trivial). We know that \( \phi_\mathcal{L} \) has finite fibers from before (because \( \ker \phi_\mathcal{L} \) is finite, equivalently \( \ker \phi_\mathcal{L} \circ [n] = \phi_\mathcal{L} \circ n \) is finite for \( n > 0 \)). (So actually this is true for any ample \( \mathcal{L} \), not just ones corresponding to effective divisors).

Therefore, \( \dim \text{Pic}^0_{A/k} \geq g \) (think over \( k = \overline{k} \) if you like). So for smoothness, it suffices to show that \( \dim H^1(A, \mathcal{O}_A) \leq g \). This would also automatically imply that \( \dim \text{Pic}^0_{A/k} = g \), and \( \phi_\mathcal{L} \) is finite surjective, hence finite flat (by generic flatness plus homogeneity, e.g. Miracle Flatness).

Mumford takes a rather indirect approach to this calculation. We'll describe another method, which is more sophisticated but also more conceptual.

**Proposition 5.1.1.** \( \dim H^1(A, \mathcal{O}_A) \leq g \).

**Proof.** The strategy will be to reduce this to a structure theorem of Borel. Borel was studying the structure of the cohomology ring of compact Lie groups, which has a graded Hopf algebra structure. The point is that the "reason" for this doesn't require gritty computation with Koszul complexes (as Mumford carries out).

Let \( R = \bigoplus_i H^i(A, \mathcal{O}_A) \). This is \( \mathbb{Z}_{\geq 0} \)-graded, and \( R^i = 0 \) for \( i > g \). This has an anti-commutative cup product \( R \otimes_k R \to R \) sending \( R^i \otimes R^j \to R^{i+j} \), \( a \otimes b \to a \sim b \) with \( (b \sim a) = (-1)^{|i|} a \sim b \). Furthermore, \( R^0 = k \), and we can say something about the top piece \( R^g = H^g(A, \mathcal{O}_A) \). Recall that \( \Omega^1_{A/R} \cong \mathcal{O}_A \otimes \text{Lie}(A)^* \), so \( \Omega^g_{A/k} \cong \mathcal{O}_A \) (non-canonically). So \( R^g = H^g(A, \Omega^g_{A/k}) \), which we know is 1-dimensional over \( k \) by Serre duality. Also, the cup product \( R^i \times R^{g-i} \to R^g \) is a perfect pairing, by Serre duality (because the canonical bundle is trivial).
Abelian Varieties

So far we haven’t used the group structure of $A$. Now we have

$$A \Rightarrow A \times A \overset{m}{\rightarrow} A$$

where the inclusions are along the identity elements, $a \rightarrow (a, 0)$ and $a \rightarrow (0, a)$. This induces

$$H^\bullet(A, \mathcal{O}_A) \overset{\cong}{\rightarrow} H^\bullet(O_A \times A)$$

Hence, we have a Künneth formula for $H^\bullet(O_A \times A)$. In general, if $X, Y$ are over Spec $k$ (where $k$ is a commutative ring) and $\mathcal{F}, \mathcal{G}$ are sheaves on $X, Y$ then we have a map

$$H^\bullet(X \times \text{Spec } k, p^*_1 \mathcal{F} \otimes p^*_2 \mathcal{G}) \overset{\sim}{\leftarrow} H^\bullet(X, \mathcal{F}) \otimes_k H^\bullet(Y, \mathcal{G})$$

and this is an isomorphism when everything is flat over $k$ (the sheaves and their cohomology), which is a Čech theory computation.

Applying this above, we have

$$R \cong R \otimes R_\mu \leftarrow R$$

(tensor product as graded associative $k$-algebras) where the two left maps use that the identity section splits off $R = k \oplus (-), 0$, and are projection to the $k$ factor follows by multiplication.

This satisfies $\mu(x) = x \otimes 1 + 1 \otimes x + (\text{higher degree terms})$ for homogeneous $x$, and $\mu$ is a $k$-algebra map (giving $R$ the structure of a hopf algebra) with a “co-inverse.” A hopf algebra is basically what you get from the coordinate ring of an affine group scheme.

**Theorem 5.1.2** (Borel). For “any such $R$,”

$$\dim R^1 \leq g$$

and equality holds if and only if $\bigwedge^\bullet(R^1) \overset{\sim}{\rightarrow} R$.

**Proof.** Without loss of generality, $k = \overline{k}$. Over perfect $k$, Borel proved a general structure theorem for Hopf algebras over $k$. See Lemma 15.2 of Milne’s AV plus handout. □

**Remark** 5.1.3. We get the bonus fact that $\bigwedge^\bullet(R^1) \cong R$, which Mumford proves directly. This is analogous to how complex tori are products of $S^1$.

**Definition** 5.1.4. If $A$ is an abelian variety over $k$, we define the **dual abelian variety** $A^\vee := \hat{A} := \text{Pic}^0_{A/k}$.

5.2. **Characterization of $\phi_{\mathcal{L}}$.** When $\mathcal{L}$ is ample, $\phi_{\mathcal{L}}: A \rightarrow \hat{A}$ is an isogeny (a finite flat surjective homomorphism).

**Corollary 5.2.1.** For ample $\mathcal{N}$ on $A$, $\mathcal{M} \in \text{Pic}(A) = \text{Pic}_{A/k}(k)$ lies in $\text{Pic}^0_{A/k}(k)$ if and only if $\mathcal{M} \cong t^*_x(\mathcal{N}) \otimes \mathcal{N}^{-1} \cong \phi_{\mathcal{N}}(x)$ for some $x \in A(\overline{k})$.

**Proof.** $\phi_{\mathcal{N}}: A \rightarrow \text{Pic}_{A/k}$ has image $\text{Pic}^0_{A/k}$. (We’re using the Nullstellensatz that surjective is equivalent to surjective on $\bar{k}$-points.) We emphasize that $x$ may not necessarily be found over $k$. □

This description is a little vague; we will want to give a better one in a moment.
Corollary 5.2.2. If $\mathcal{M} \in \text{Pic}^0_{A/k}(k)$, then $\phi_\mathcal{M} = 0$.

Proof. Without loss of generality $k = \bar{k}$. Then $\mathcal{M} \cong t_x^* \mathcal{N} \otimes \mathcal{N}^{-1}$ for ample $\mathcal{N}$ on $A$, so

$$\phi_\mathcal{M}(y) = t_y^*(\mathcal{M}) \otimes \mathcal{M}^{-1}$$

$$= t_x^* \mathcal{N} \otimes t_{x+y}^* \mathcal{N}^{-1} \otimes t_y^* \mathcal{N}^{-1} \otimes \mathcal{N}$$

$$= 0_A$$

by the Theorem of the Square. $\square$

There is an alternative geometric proof of this on the homework. Next time, we'll prove the converse. You should think about this as follows. We have a map $\text{Pic}_{A/k} \rightarrow \text{Hom}(A, \widehat{A})$ sending $\mathcal{M} \rightarrow \phi_\mathcal{M}$, and the latter is étale, hence (intuitively) discrete. That intuitively means that $\phi_\mathcal{M}$ is a “discrete” invariant of $\mathcal{M}$.

On $A \times \widehat{A}$, we have the Poincaré bundle $\mathcal{P}_A$ pulled back from the universal bundle on $A \times \text{Pic}_{A/k,e}$. This is equipped with an $(e \times 1)$-trivialization by the rigidification construction, and a $(1 \times \widehat{e})$-trivialization by definition of $\widehat{e}$ corresponding to the trivial bundle of $\text{Pic}_{A/k,e}$, which is unique after normalizing so that it is compatible with the first trivialization with respect to $(e, \widehat{e})$.

There is a symmetric relationship between $A$ and its dual. Namely, we have a flip isomorphism $\sigma : \widehat{A} \times A \cong A \times \widehat{A}$. Then $\sigma^*(\mathcal{P}_A)$ is line bundle on $\widehat{A} \times A$, and by the universal property of $\text{Pic}_{A/k}$ this corresponds to a map $A \xrightarrow{\pi} \text{Pic}_{A/k} = \widehat{A}$ sending $e \rightarrow 0$. We will show that this is an isomorphism.

More generally, a line bundle on $X \times Y$ ($X, Y$ abelian varieties) gives maps $X \rightarrow \widehat{Y}$ and $Y \rightarrow \widehat{X}$.

We want to emphasize that the relationship between an abelian variety and its dual is analogous to the relationship between a vector space and its dual, and the Poincaré line bundle is analogous to the dual pairing.

It is not true that Pic “commutes” with products. This works well on the identity component, though (homework). Roughly speaking, Pic has “quadratic” behavior, which isn’t seen at the identity component. In the analytic theory, Pic is related to $H^2$.

Theorem 5.2.3. If $\phi_{\mathcal{X}} = 0$, then $\mathcal{L}_{\mathcal{X}} \cong \phi_{\mathcal{X}}(x)$ for some $x \in A(k)$. In other words, $\mathcal{L} \rightarrow \phi_{\mathcal{X}}$ induces

$$\text{Pic}_{A/k}(\bar{k}) / \text{Pic}^0_{A/k}(\bar{k}) \rightarrow \text{Hom}_{A}(A, \widehat{A}).$$

In other words, $\phi_{\mathcal{X}}$ detects whether or not you can “continuously deform” one line bundle to another, i.e. how you can move around in the moduli space of line bundles.

Proof. We may assume without loss of generality that $k = \bar{k}$. Let’s put $\{ t_x^* \mathcal{N} \otimes \mathcal{N}^{-1} \otimes \mathcal{L}^{-1} \}_{x \in A(k)}$ into a “family” over $A$, i.e. a line bundle $\mathcal{X}$ on $A \times A$ such that $\mathcal{X}|_{\{x\} \times A} \cong t_x^* \mathcal{N} \otimes \mathcal{N}^{-1} \otimes \mathcal{L}^{-1}$, and we get a contradiction if these are all non-trivial.

To construct this $\mathcal{X}$, set $\mathcal{X} := \Lambda(\mathcal{N}) \otimes \mathcal{pr}_1^*(\mathcal{L}^{-1})$ (recall the Mumford construction $\Lambda(N) = m^*N \otimes \mathcal{pr}_1^*N^{-1} \otimes \mathcal{pr}_2^*N^{-1}$). Pulling back to $\{x\} \times A$ turn $m^*$ into $t_x^*$, kills $\mathcal{pr}_1$, turns $\mathcal{pr}_2$ into $\text{Id}^*$, so we see that we indeed get $t_x^*N \otimes \mathcal{N}^{-1} \otimes \mathcal{L}^{-1}$.

So we study $H^1(A \times A, \mathcal{X})$ using the Leray spectral sequence for

$$(p_1, p_2) : A \times A \Rightarrow A.$$
Assume $\mathcal{X}|_{[a] \times A} \not\cong \mathcal{O}_A$ for all $a \in A(k)$; we'll deduce that $H^j(A \times A, \mathcal{X}) = 0$ for all $j$ (using $\phi_Z = 0$), and then get a contradiction from this.

The spectral sequence relates $H^j(A \times A, \mathcal{X})$ to the cohomology of $A$ with coefficients in the fibers, which we know. Now, observe that the $\phi$-construction applied to $\mathcal{X}$ is trivial because it's always trivial applied to $\iota_{A,\mathcal{X}}^* N \otimes N^{-1}$, and it kills $\mathcal{L}$ by hypothesis.

We have $H^j(A, R^j \mathbb{P}_{1,\mathcal{X}} \mathcal{X}) \Rightarrow H^{j+1}(A \times A, \mathcal{X})$. We'll show that $R^j \mathbb{P}_{1,\mathcal{X}} \mathcal{X} = 0$ for all $j$. By cohomology and base change, it suffices to show that $H^j(A, \mathcal{X}|_{[a] \times A}) = 0$ for all $j, a \in A(k)$ (under a flat map, with surjective hypotheses onto fibral cohomologies, one has nice isomorphism results - look it up). So we have $\mathcal{M} \cong t_0^* N \otimes N^{-1} \otimes L^{-1}$ is non-trivial by assumption, but $\phi_{\mathcal{M}} = \phi_{\mathcal{M}^{-1}} = -\phi_{\mathcal{L}} = 0$ by hypothesis.

We're going to prove that a non-trivial line bundle whose $\phi$ vanishes has vanishing higher cohomology. By the way, this is all motivated by knowledge of the vanishing of cohomology of line bundles in the analytic setting.

**Lemma 5.2.4.** If $\mathcal{M} \not\cong \mathcal{O}_A$ and $\phi_{\mathcal{M}} = 0$, then $H^j(A, \mathcal{M}) = 0$ for all $j$.

**Proof.** Use induction on $j \geq 0$. We'll prove it directly for $j = 0$, then bootstrap.

Let's first make a general observation, which has nothing to do with a specific $j$. The fact that $\phi_{\mathcal{M}} = 0$ has the following consequence: $\Lambda(\mathcal{M}) = m^* \mathcal{M} \otimes \mathbb{P}^!_1 \mathcal{M}^{-1} \otimes \mathbb{P}^!_2 \mathcal{M}^{-1}$ is isomorphic to $(1 \times \phi_{\mathcal{M}})^* \mathbb{P}_A$ (we saw this a long time ago), under the map $A \times A \xrightarrow{1 \times \phi_{\mathcal{M}}} A \times \hat{A}$. So if $\phi_{\mathcal{M}}$ is trivial, then $\Lambda(\mathcal{M})$ is trivial, so

$$m^* \mathcal{M} \cong \mathbb{P}^!_1 \mathcal{M} \otimes \mathbb{P}^!_2 \mathcal{M}.$$  \hspace{1cm} (1)

For $(f, g) \in (A \times A)(S) = A(S) \times A(S)$, pulling back $[1]$ along $(f, g): S \to A \times A$ gives

$$(f + g)^* \mathcal{M} \cong f^* \mathcal{M} \otimes g^* \mathcal{M}.$$  

Remark: it's instructive to work out how this plays out in terms of the analytic theory. As a consequence, we get that $[n]^* \mathcal{M} \cong \mathcal{M}^n$ for all $n \in \mathbb{Z}$. In particular, for such an $\mathcal{M}$, we have

$$[-1]^* \mathcal{M} \cong \mathcal{M}^{-1}.$$  

Now let's start running the induction.

$j = 0$. Assume there exists a non-zero $s \in \mathcal{M}(A)$, i.e. a map $\mathcal{O}_A \xrightarrow{s \neq 0} \mathcal{M}$ (an injection of invertible sheaves), which dualizing gives $\mathcal{O}_A \hookrightarrow \mathcal{M}^{-1}$, which is an invertible ideal sheaf (an injection, not a surjection - think lattices). This gives $\mathcal{M}^{-1} = \mathcal{L}_D$, so $\mathcal{M} \cong \mathcal{L}_D = \mathcal{O}_A(D)$. (This is the correspondence between invertible sheaves plus sections and effective Cartier divisors.)

The relation $[-1]^* \mathcal{M} \cong \mathcal{M}^{-1}$ implies that $\mathcal{O}_A([-1]^* D) \cong \mathcal{O}_A(-D)$, so $[-1]^* D + D$ is an effective Weil divisor $\sim 0$. That implies $[-1]^* D + D = 0$, so $D = 0$, so $\mathcal{M}$ is trivial, but this contradicts the hypotheses.

$j > 0$. Now for the magic: we relate the higher cohomology groups to the lower ones. Assume $H^i(A, M) = 0$ for all $i < j$. We consider the following trick of Mumford: factor the
Abelian Varieties  
Math 249C, 2015

identity map as
\[ \text{Id}: A \xrightarrow{i_1} A \times A \xrightarrow{m} A \]
which induces
\[ H^i(A, \mathcal{M}) \leftarrow H^i(A \times A, m^* M) \xrightarrow{m^*} H^i(A, \mathcal{M}). \]
It suffices to show that the middle guy is 0. Now we use the general observation \([\mathbb{I}]:\)
\[ m^* \mathcal{M} \cong \text{pr}_1^* \mathcal{M} \otimes \text{pr}_2^* \mathcal{M} (= \mathcal{M} \boxtimes \mathcal{M}) \]
so
\[ H^j(m^* \mathcal{M}) \cong H^j(\text{pr}_1^* \mathcal{M} \otimes \text{pr}_2^* M). \]
Now we can apply Künneth, because everything is flat, to get that this is
\[ \bigoplus_{i+i'=j} H^i(A, \mathcal{M}) \otimes_k H^{i'}(A, \mathcal{M}). \]
But either \(i\) or \(i' < j\), so by induction hypothesis this all vanishes.

\[ \square \]

Remark 5.2.5. So the upshot is that for any non-trivial line bundle whose \(\phi\) vanishes, all
the cohomology vanishes.

For line bundles without vanishing \(\phi\), there is something called “index theory” in
which exactly one index doesn’t vanish. It has some analogies with the Borel-Weil-Bott
theorem for line bundles on \(G/B\).

This shows (using cohomology and base change for \(\text{pr}_1\)) that \(R^j(\text{pr}_1)_*(\mathcal{X}) = 0\) on \(A\), so
the Leray spectral sequence implies that \(H^j(A \times A, \mathcal{X}) = 0\) for all \(j\) (assuming \(\mathcal{L} \neq \phi_\mathcal{X}(x)\)
for all \(x \in A(k)\), in order to guarantee that all fibers were non-trivial).

Now let’s study the spectral sequence for other projection:
\[ H^i(A, (R^j \text{pr}_2)_*(\mathcal{X})) \implies H^{i+j}(A \times A, \mathcal{X}) = 0. \]
We have \(\mathcal{X}|_{A \times A} \cong \phi_\mathcal{X}(a)\), as \(\mathcal{X} = \Lambda(\mathcal{X}) \otimes \text{pr}_2^* \mathcal{L}^{-1}\). This has “vanishing \(\phi\)” (by theorem
of the square, from last time). At any \(a\) for which this is non-zero, i.e. \(a \notin \ker \phi_\mathcal{X}\), then
the Lemma applies again to give vanishing of fibral cohomology: \(H^j(\text{pr}_2^{-1}(a), \mathcal{X}) = 0\) for all \(j\). Therefore, by cohomology and base change the stalk of the higher direct images at
such points vanishes: \(R^j(\text{pr}_2)_*(\mathcal{X})a = 0\) for all \(j\) when \(a \notin \ker \phi_\mathcal{X}\).

But almost all points lie outside \(\ker \phi_\mathcal{X}\), since the latter is finite by \(\mathcal{X}\) being ample. Coheren sheaves \(R^j(\text{pr}_2)_*(\mathcal{X})\) on \(A\) vanishes on \(A – \ker \phi_\mathcal{X}\), hence has support contained in
the finite \(k\)-scheme \(\ker \phi_\mathcal{X}\). These “come from” \(k\)-finite subschemes of \(A\), i.e. their
annihilator ideals cut out some thickening of \(\ker \phi_\mathcal{X}\). Therefore, \(H^j(A, R^j(\text{pr}_2)_*(\mathcal{X})) = 0\) for all \(i > 0\), as it’s a coherent sheaf supported on a finite set of closed points.

So the Leray spectral sequence here has a single non-vanishing row, in that row you have
\(H^0(A, R^j \text{pr}_{2*} \mathcal{X}) = \ast R^j \text{pr}_{2*} \mathcal{X}\). The conclusion is that \(R^j(\text{pr}_2)_*(\mathcal{X}) = 0\) for all \(j\). Why
is this interesting? You always have vanishing of fibral cohomology in large degree. The
local freeness of higher direct images implies some relation with lower degrees, so you
get 0 everywhere.

By descending induction, \(H^j(A, \mathcal{X}|_{\mathcal{X}_0}) = 0\) (using local freeness, plus the cohomology/base change result needed to get this) for all \(a, j \geq 0\). Take \(j = 0, a = 0\). Then this
tells us that \(H^0(A, \mathcal{O}_A) = 0\). But this is ridiculous.

\[ \square \]
5.3. The Néron-Severi group. We’ve finally finished the proof that \( \mathcal{L} \in \operatorname{Pic}^0_{X/k}(k) \) if and only if \( \phi_{\mathcal{L}} : A \to \tilde{A} \) vanishes. For a \( k \)-scheme \( X \), geometrically connected and geometrically reduced, \( \operatorname{Pic}_{X/k} \) exists as locally finite type \( k \)-group scheme.

Definition 5.3.1. We define the Neron-Severi group

\[
\operatorname{NS}(X) = \frac{\operatorname{Pic}_{X/k}(\overline{k})}{\operatorname{Pic}^0_{X/k}(\overline{k})},
\]

which is the same as \( \operatorname{NS}(X_{\overline{k}}) \) because Picard schemes commute with base change.

Equivalently, \( \operatorname{NS}(X) \) is the group of line bundles on \( X_{\overline{k}} \) up to algebraic equivalence. That is, \( \mathcal{L}_1 \) and \( \mathcal{L}_2 \) on \( X_{\overline{k}} \) are algebraically equivalent if there exists a connected \( \overline{k} \)-scheme \( S \) and geometric points \( s_1, s_2 \in S(\overline{k}) \) and a line bundle \( \mathcal{N} \) on \( X \times_k S \) such that \( \mathcal{N}_{s_i} = (\mathcal{L}_i)_{\overline{k}} \). That this condition is equivalent to \( \mathcal{L}_1 \) and \( \mathcal{L}_2 \) lying in the same connected component of \( \operatorname{Pic}_{X/k}(\overline{k}) \) is because any line bundle \( \mathcal{N} \) on \( X \times_k S \) is classified (up to twist from a line bundle coming from the base) by a map to the Picard group.

Now we discuss some important results concerning the Néron-Severi group of \( X \). First, the Néron-Lang Theorem of the Base says that \( \operatorname{NS}(X_{\overline{k}}) \) is finitely generated over \( \mathbb{Z} \). This tells us that there is a finite torsion subgroup.

Then one might ask, can we characterize the torsion bundles? It is a theorem that the line bundles representing torsion in \( \operatorname{NS}(X_{\overline{k}}) \) are precisely those which are “invisible” from the perspective of intersection theory. More precisely, \( \mathcal{L} \) on \( X_{\overline{k}} \) is numerically equivalent to 0 (a weaker notion than algebraic equivalence) if for all integral curves \( C \subset X_{\overline{k}} \), the intersection number \( \langle C, \mathcal{L} \rangle = \deg \mathcal{L}|_C = 0 \).

We summarize these results, which appear in SGA 6.

Theorem 5.3.2 (Exp. XIII of SGA 6). We have the following results:

1. (Néron-Lang Theorem of the Base) \( \operatorname{NS}(X_{\overline{k}}) \) is finitely generated over \( \mathbb{Z} \) (Theorem 5.1).
2. If \( \operatorname{Pic}^\tau_{X/k} \) is the clopen subscheme of \( \operatorname{Pic}_{X/k} \) that is the pre-image over \( \overline{k} \) of \( \operatorname{NS}(X)_{\text{tors}} \), then \( \operatorname{Pic}^\tau_{X/k}(\overline{k}) \) consists exactly of those \( \mathcal{L} \) on \( X_{\overline{k}} \) that are numerically equivalent to 0 (Theorem 4.6).

Remark 5.3.3. What’s going on in the analytic case? You have an exponential sequence

\[
0 \to \mathbb{Z}(1) \to \mathcal{O}_X \xrightarrow{\exp} \mathcal{O}_X^\times \to 1
\]

whose associated long exact sequence gives

\[
0 \to H^1(X, \mathcal{O}_X)/H^1(X, \mathbb{Z}(1)) \to H^1(\mathcal{O}_X^\times) = \operatorname{Pic}(X) \xrightarrow{\eta} H^2(X, \mathbb{Z}(1)) \to \ldots
\]
and $H^1(X, \mathcal{O}_X)/H^1(X, \mathbb{Z}(1)) \cong \text{Pic}^0(X)$. This realizes an embedding

$$\text{Pic}(X)/\text{Pic}^0(X) \hookrightarrow H^2(X, \mathbb{Z}(1)).$$

In general, you can try to do an $\ell$-adic version of this, using étale cohomology, but it’s a little puzzling.

In SGA6, they prove a remarkable result that for abelian schemes, the locus where the rank/torsion of the NS group is bounded is nice (e.g. constructible). In contrast, the locus where the rank or torsion is equal to some specified thing can be really nasty, reflecting the fact that the fibral components of the Picard scheme jump around like crazy.

Anyway, in the special case of abelian varieties we have an embedding $\text{NS}(A) \hookrightarrow \text{Hom}_k(A_k, A_k^\vee)$ sending $[\mathcal{L}] \mapsto \phi_{\mathcal{L}}$. Since $\text{Hom}_k(A_k, A_k^\vee)$ is torsion-free, $\text{NS}(A)$ is torsion-free.

To establish our goal result on the $\mathbb{Z}$-finiteness of $\text{Hom}_k(A, B)$, we need two ingredients:

1. Properties of $A \rightarrow \tilde{A}$. (For instance, if $f, g: A \rightarrow B$ then we get $\tilde{f}, \tilde{g}: \tilde{A} \rightarrow \tilde{B}$, and one could ask if $(f + g)\wedge = \tilde{f} + \tilde{g}$. The answer is yes. You might think that this is obvious, but in the analytic theory, if you look at the induced map on the full Picard scheme, it’s basically $\wedge^2$, which is not linear. Indeed, the analytic theory clarifies that the Neron-Severi group is something like a quadratic functor. So there is really something non-trivial here.)

2. A robust theory of isogenies, e.g. forming a quotient $A/G$ for $G \subset A$ a finite $k$-group scheme. This is tricky in characteristic $p$, if you have weird things like $\alpha_p, \mu_p$. 

48
6. **Descent**

We make somewhat of a digression in order to discuss the general technique of _faithfully flat descent._

6.1. **Motivation.** For example, we want to say something like

\[ 0 \to A[n] \to A \overset{\text{[n]}}{\to} A \to 0 \text{ is a short exact sequence} \]

even if \( \text{ch } n \mid k \). As another example, we want to make sense of saying that if \( f : A \to X \) is “\( A[n] \)-invariant” then it factors as

\[
\begin{array}{ccc}
A & \overset{[n]}{\longrightarrow} & A \\
\downarrow^{f} & & \downarrow^{\exists f} \\
X & \to & X
\end{array}
\]

Here one can witness the power of Grothendieck’s theory of schemes. Old-fashioned methods (e.g. Weil) encountered significant difficulty in dealing with inseparability issues, because of the lack of technology for infinitesimal methods.

The best reference for this material is §6.1 of _Néron models._

The idea is that we want to unify in a single formalism:

1. gluing in topology,
2. quotient constructions (by group actions),
3. Galois descent,
4. everything else.

To set this up, let’s think about gluing constructions in topology. Suppose \( X \) is a topological space, \( \{ U_i \} \) an open cover of \( X \), and over each \( U_i \) we’re given data that we want to “glue” into a “global structure” over \( X \), such as sheaves, or topological spaces \( Y_i \to U_i \), or maps of stuff “over \( U_i \).” Classically, this is expressed via cocycle conditions on triple overlaps for gluing data over double overlaps.

We begin by rephrasing this classical setup. Let \( U = \bigsqcup_{i \in I} U_i \to X \). What is \( U \times_X U \)? It’s not hard to see that this is

\[ U \times_X U = \coprod_{(i,j) \in I \times I} U_i \cap U_j. \]

Note that here we allow \( i = j \) and \( (i, j) \) and \( (j, i) \). The map sends \( x_{ij} \mapsto (x_{ij} \in U_i, x_{ij} \in U_j) \).

For triple overlaps, \( U \times_X U \times_X U = \coprod_{(i,j,k) \in I^3} U_i \cap U_j \cap U_k \) and we have two maps

\[
\begin{array}{ccc}
U \times_X U & \overset{p_1}{\longrightarrow} & U \\
\downarrow^{p_2} & & \downarrow^{U_i} \\
U & \to & U
\end{array}
\]

where \( p_1 \) includes \( U_{ij} \) in \( U_i \) and \( p_2 \) includes \( U_{ij} \) to \( U_j \).
Similarly, we have three maps

\[ U \times_X U \times_X U \xrightarrow{p_1} U \]

\[ U \times_X U \times_X U \xrightarrow{p_2} U \]

\[ U \times_X U \times_X U \xrightarrow{p_3} U \]

sending \( U_{i j k} \mapsto U_i, U_j, U_k \) (respectively) and also maps

\[ p_{i j}: U \times_X U \times_X U \to U \times_X U \]

sending \( U_{i j k} \mapsto U_i \cap U_k \), etc.

Ultimately, we want to reformulate the classical gluing (i.e. cocycle data) in terms of \( U \times_X U \) and \( U \times_X U \times_X U \). In this case the map \( U \to X \) is a local homeomorphism, but the goal is to apply such ideas to \( U \to X \) which are “far” from being a local homeomorphism. If \( U \to X \) is replaced by \( U' \to S \), we still want to be able to “descend” structure from \( S' \) to \( S \). For instance, \( S' \to S \) could be

- \( \text{Spec } k' \to \text{Spec } k \), or
- \( \text{Spec } R' \to \text{Spec } R \) (where \( R \) is local noetherian), or
- \( \text{Spec } K' \to \text{Spec } k \) for \( K'/k \) finite Galois,

and variations on this.

The question is, for what class of maps on \( S' \to S \) can we do this? We want

1. base-change to induce a faithful functor \( S \to \textbf{Sch} \to S' \to \textbf{Sch} \) or \( S \to \textbf{QCoh} \to S' \to \textbf{QCoh} \), etc. and
2. to be able to describe the essential image.

In classical Galois descent, this would be isomorphism on the \( K \) objects with their Galois twists, which are coherent with respect to each other. What we want is to figure out to what extra data needs to be defined “upstairs,” playing the role of this gluing, is needed to descend downstairs.

### 6.2. fpqc descent

Grothendieck’s key discovery was that if \( S' \to S \) is fpqc (faithfully flat, quasicompact) then \( S \to \textbf{Sch} \) embeds fully faithfully into \( (S' \to \textbf{Sch} \) with “descent data”).

**Example 6.2.1.** If \( K/k \) is Galois with group \( G \), then \( K \otimes_k K \cong \prod_{g \in G} K \) sending \( a \otimes b \mapsto (g(a)b) \). This matches up with the disjoint union situation: \( S' \times_S S = \bigsqcup_{g \in G} S' \).

Let \( S' \to S \) be a fpqc map. This means that for \( U \cong \text{Spec } A \subset S \), the pre-image \( U' \) is quasicompact, i.e. covered by finitely many affines \( U'_i = \text{Spec } A'_i \). So \( U' \) admits a surjection from \( \bigsqcup_{i \in I} U'_i = \text{Spec } (\prod_{i \in I} A'_i) \). Then the composite map \( \text{Spec } (\prod_{i \in I} A'_i) \to \text{Spec } A \) is a surjective, flat map of affines, which is equivalent to the usual commutative-algebraic notion of faithfully flat modules. So we see that the quasicompactness is a trick to reduce to an affine situation.

**Example 6.2.2.** In Hartshorne’s book, there is an exercise called “schemes over \( \mathbb{R} \)” which tries to encode the data of a scheme over \( \mathbb{R} \) as a scheme over \( \mathbb{C} \) plus some stuff about complex conjugation. This is a baby case of the general framework that we want to set up.
Let \( \mathcal{F}' \) be a quasicoherent sheaf on \( S' \), (e.g. if \( \mathcal{F}' \) is a quasicoherent \( \mathcal{O}_{S'} \)-algebra then this is the “same” as an \( S' \)-affine scheme). We ask: what “extra structure” on \( \mathcal{F}' \) encodes a quasicoherent sheaf \( \mathcal{F} \) on \( S \) and the data of an isomorphism \( f^* \mathcal{F} \cong \mathcal{F}' \)?

**Example 6.2.3.** In the case of a Galois covering, e.g. \( S' = \text{Spec } K' \) and \( S = \text{Spec } K \) with \( K'/K \) a finite Galois extension with group \( G \), this extra structure should be something like a \( G \)-action.

**Example 6.2.4.** If \( S' = \bigcup S_i \) where \( \{S_i\} \) is an open cover of \( S \) by quasicompact opens, so \( \mathcal{F}' = \{ \mathcal{F}'_i \text{ quasicoherent on } S'_i \} \) and the “extra structure” should be classical gluing data.

As motivation, suppose \( \mathcal{F} \) is a quasicoherent sheaf on \( S \) and \( \mathcal{F}' = f^* \mathcal{F} \). Then what extra structure does \( \mathcal{F}' \) have? Let \( S'' = S' \times_S S' \) and \( S''' = S' \times_S S' \times_S S' \). We have two projections

\[
\begin{array}{ccc}
S'' & \xrightarrow{p_1} & S' \\
\downarrow p_2 & & \downarrow f \\
S & & S
\end{array}
\]

with the composites \( f \circ p_1 = f \circ p_2 \) being the same (by definition of the fibered product). So we get

\[
\theta: p_1^* \mathcal{F}' = p_1^* f^* \mathcal{F} = (f \circ p_1)^* \mathcal{F} = (f \circ p_2)^* \mathcal{F} = p_2^* \mathcal{F}'
\]

as \( \mathcal{O}_{S''} \)-modules (i.e. over \( S'' \)).

**Example 6.2.5.** Let’s see what this is really doing in the affine setting. In the affine case,

\[
\begin{array}{ccc}
S'' & \xrightarrow{p_1} & S' \\
\downarrow p_2 & & \downarrow f \\
S & & S
\end{array}
\]

\[
\begin{array}{ccc}
R'' & \xleftarrow{p_2} & R' \\
\downarrow p_1 & & \downarrow f'
\end{array}
\]

and \( \mathcal{F}' \hookrightarrow M' \), a module over \( R' \). Then \( p_1^* \mathcal{F}' \hookrightarrow M' \otimes_{R'} p_1^* (R' \otimes_R R') \cong M' \otimes_R R' \), so \( \theta \) corresponds to an isomorphism

\[
\theta^*: M' \otimes_R R' \cong R' \otimes_R M' \text{ as } R'' = R' \otimes_R R' \text{-modules}.
\]

**Example 6.2.6.** In the case of a Zariski-open covering, we have \( S' = \bigcup S'_i \) and \( \mathcal{F}' \hookrightarrow \{ \mathcal{F}'_i \text{ on } S'_i \} \) and \( S'' = \bigsqcup_{i,j} S'_i \cap S'_j \). We have two maps \( p_1, p_2: S'' \twoheadrightarrow S' \) as discussed previously. Then \( p_1^* \mathcal{F}' = \{ \mathcal{F}'_i|_{S'_i} \}_{i,j} \) and \( p_2^* \mathcal{F}' = \{ \mathcal{F}'_j|_{S'_j} \}_{i,j} \). So

\[
\theta \leftarrow \theta_{ij}: \mathcal{F}'_i|_{S'_i} \sim \mathcal{F}'_j|_{S'_j} \text{ for all } (i, j).
\]

The upshot is that to give \( \mathcal{F} \) on \( S \) and \( \alpha: \mathcal{F}' \cong f^* \mathcal{F} \) is the same as “gluing” \( \{ \mathcal{F}'_i \} \) by transition functions \( \theta_{ij} \). As we know from the classical theory, we should also have a “cocycle condition” on triple overlaps.
Abelian Varieties

As we saw in the preceding example, the data of a isomorphism $\theta$ is not quite enough, even in the classical situation of gluing on an open cover. So let’s go back and ask, does the isomorphism $\theta: p_1^* F' \sim p_2^* F$ arising from an $F'$ obtained from $(F, \alpha)$ have any special property? For this Zariski open covering, we saw that the answer is yes: there is a triple overlap condition. In the Galois setting, there is also an associativity/consistency condition corresponding to that in the definition of action.

Motivated by this, we look on $S''$, which admits three maps $q_{ij}: S'' \to S'$. On $S''$ we have the isomorphism $\theta: p_1^* F' \sim p_2^* F'$, pulling back across the three maps gives six bundles, and three isomorphisms, so we get a hexagon and the condition is that this hexagon “commutes.”

Let’s first consider pulling back $\theta$ by $q_{12}$:

$$q_{12}^* p_1^* F' \xrightarrow{q_{12}^*(\theta)} q_{12}^* p_2^* F'. $$

Now, $p_1 \circ q_{12} = p_1 \circ q_{13}$, so we have canonically

$$q_{12}^* p_1^* F' = q_{13}^* p_1^* F'. $$

This fits together as

Next, pulling back $\theta$ by $q_{13}$ gives $q_{13}^* p_1^* F' \xrightarrow{q_{13}^*(\theta)} q_{13}^* p_2^* F'$, and then we have again canonically $q_{13}^* p_2^* F' = q_{23}^* p_2^* F'$, so the diagram extends to

Continuing the same argument, we obtain a commutative hexagon

$$q_{12}^* p_1^* F' \xrightarrow{q_{12}^*(\theta)} q_{12}^* p_2^* F'$

$$q_{13}^* p_1^* F' \xrightarrow{q_{13}^*(\theta)} q_{13}^* p_2^* F'$

$$q_{23}^* p_1^* F' \xrightarrow{q_{23}^*(\theta)} q_{23}^* p_2^* F'$$

$$q_{13}^* p_2^* F' \xrightarrow{q_{13}^*(\theta)} q_{13}^* p_2^* F'$$

$$q_{23}^* p_2^* F' \xrightarrow{q_{23}^*(\theta)} q_{23}^* p_2^* F'$$

(2)
Definition 6.2.7. Given $\mathcal{F}'$ on $S'$ (quasicoherent), a descent datum on $\mathcal{F}'$ with respect to $f: S' \to S$ is an isomorphism $\theta: p_1^* \mathcal{F}' \cong p_2^* \mathcal{F}'$ such that the hexagon \(\Box\) commutes.

Such pairs $(\mathcal{F}', \theta)$ for fixed $S' \to S$ form a category in an evident manner: a morphism $(\mathcal{F}', \theta) \to (\mathcal{G}', \psi)$ is $h: \mathcal{F}' \to \mathcal{G}'$ such that $p_1^*(h)$ and $p_2^*(h)$ are compatible via $\theta, \psi$. We denote this category by $\text{QCoh}(S'/S)$. So we have constructed a functor $\text{Coh}(S) \to \text{QCoh}(S'/S)$ taking $\mathcal{F} \mapsto (f^* \mathcal{F}', \theta_{\mathcal{F}})$.

Theorem 6.2.8 (Grothendieck). This is an equivalence of categories.

The key to the proof is the affine case: if $R \to R'$ is faithfully flat and $(M', \theta)$ is a descent datum over $R'$, then you have to produce some $M$ over $R$. There is one natural guess:

$$M = \{ m' \in M' \mid \theta'(m' \otimes 1) = 1 \otimes m' \} \subset M'$$

For this to work, one has to know that if $M' = M \otimes_R R'$, then

$$M = \{ m' \in M \otimes_R R' \mid \theta'(m' \otimes 1) = 1 \otimes m' \text{ in } (M \otimes R) R' \cong R' \otimes_R (M \otimes R') \}$$

This is resolved using a brilliant trick involving faithful flatness: see §6.1, Theorem 4 of Néron Models.

That settles the case of sheaves. The real “beef” is the case geometric objects, which is much harder. You win for schemes that are affine over the base, because that’s equivalent to the data of a sheaf of algebras.

Geometric objects. Suppose $X' \to S'$ is an arbitrary scheme and $f: S' \to S$ is fpqc.

Definition 6.2.9. A descent datum on $X'$ with respect to $f$ is

$$\theta: X' \times_S S' \sim \to S' \times_S X'$$

such that the analogue of the hexagon \(\Box\) commutes.

As before, the descent datum pairs $(X', \theta)$ form a category $(S'/S) \to \text{Sch}$.

Example 6.2.10. If $X' = X \times_S S'$, then there is an evident isomorphism

$$\theta_X: (X \times_S S') \times_S S' \sim \to S' \times_S (X \times_S S')$$

coming from the equality $f \circ p_1 = f \circ p_2$. This is not merely the “flip” isomorphism, because it has to be a morphism over $S' \times_S S'$!

Theorem 6.2.11. The functor $S \to \text{Sch} \to (S'/S) \to \text{Sch}$ is fully faithful.

So if a map upstairs respects the identifications of the descent datum, then it comes from a map downstairs.

However, the essential surjectivity is a nightmare. Call $(X', \theta)$ effective if it is in the essential image, i.e. it comes from some $X$ downstairs. It’s very hard to identify the effective descent data in general. In some cases it’s easier: for relative affine morphisms,
all descent data are effective (since it reduces to descending a quasicoherent sheaf). For projective morphisms, you also get a coordinate ring, which is enough leverage to get effective descent data.

**Remark 6.2.12.** If $X'$ is equipped with an $S'$-ample line bundle $\mathcal{L}'$ and $X' \to S'$ is quasi-compact and separated, and $\mathcal{L}'$ is equipped with its own descent datum over $\theta: p_1^*\mathcal{L}' \cong p_2^*\mathcal{L}$, then $(X', \theta)$ is effective.

**Proof.** §6.1 of *Néron Models*, Theorem 6 and proof plus Theorem 7 (for effectivity). 

**Example 6.2.13.** The relation with Zariski gluing and Galois descent are examples A, B in *Néron Models*, §6.2.

Without $\mathcal{L}'$, you need algebraic spaces. Part of the purpose of the theory of algebraic spaces is to give a broader framework for effectivity results without needing such assumptions. Next, we’ll want to give a variant of this with a group action included.

In the same proof, one finds:

**Theorem 6.2.14.** Representable functors $\text{Hom}_S(-, Z)$ are fpqc sheaves. In other words, if

\[
\begin{array}{ccc}
T'' = T' \times_S T' & \xrightarrow{p_1} & T' \\
p_2 & \xrightarrow{\text{fpqc}} & T \\
\downarrow & & \downarrow \quad \text{fpqc} \\
S & & Z
\end{array}
\]

then the diagram of sets

\[
Z(T) \xhookrightarrow{\sim} Z(T') \xhookrightarrow{\sim} Z(T'')
\]

is exact.

\[\blacksquare\blacksquare\blacksquare\text{ TONY: [adjoint for } S\text{-points]}\]

**Example 6.2.15.** In the Galois case, this amounts to equivariance for the Galois action.

**Key case.** If $G \xrightarrow{f} H$ is a fpqc map of $S$-group schemes (e.g. a surjection of smooth groups of finite type over $k$) and $K = \ker f = f^{-1}(e_H) \subset G$, then

\[
\begin{array}{ccc}
K \times_S G & \xrightarrow{\text{Yoneda}} & G \times_H G \\
p_1 & \swarrow & \searrow p_2 \\
& f & \\
& \downarrow & \\
& H &
\end{array}
\]

where the first map is $(k, g) \mapsto (k \cdot g, g)$. The composition with the two projections are $(k \cdot g, g) \mapsto k \cdot g$ and $(k \cdot g, g) \mapsto g$, which are the action and projection maps. So this is telling us that $z: G \to Z$ factors (uniquely) through $f$ if and only if $z$ is invariant under the left $K$-action on $G$, i.e. "$H$ serves as a quotient $G/K$ for the fpqc topology."

**Example 6.2.16.** Apply the above to $\text{SL}_n \to \text{PGL}_n$ over Spec $\mathbb{Z}$. Here $\ker f = \mu_n$, so the upshot is that a $\mu_n$-invariant map $\text{SL}_n \to Z$ factors uniquely through $f$ (even though usually $\text{SL}_n(R) \to \text{PGL}_n(R)$ is not surjective).
Example 6.2.17. We’ll want to apply this to “$A/A[n] \to A$” for an abelian variety $A/k$ and $n \in \mathbb{Z} - \{0\}$. See Homework 6. The machinery of descent allows us to make sense of this in the difficult case where $\text{ch } k \mid n$.

Remark 6.2.18. If $H$ is not given, then the problem of building a quotient is very difficult. Over a field $k$, for any abelian variety $A$ and a finite subgroup scheme $K$ one can always build $A/K$ using a trick by Deligne. In general, it is quite subtle. The quotient constructions always exist as \textit{algebraic spaces}.
7. MORE ON THE DUAL ABELIAN VARIETY

7.1. Dual morphisms. Let \( f : A \to B \) be a map of abelian varieties. Then we get a dual map \( \hat{f} : \hat{B} \to \hat{A} \) restricted from the pullback map \( \text{Pic}_{B/k} f^* \to \text{Pic}_{A/k} \) corresponding under the functor of points perspective to \( L' \in \text{Pic}_{B/k} f^*(T) \to f^*_T L' \). Recall that for \( k = \mathbb{C} \), we have a natural (in \( A \)) isomorphism

\[
\hat{A}^{an} \cong H^1(A, \mathcal{O}_A)/H^1(A(\mathbb{C}), \mathbb{Z}(1))
\]

where \( \mathbb{Z}(1) = 2\pi i \mathbb{Z} = \ker(\exp : \mathbb{C} \to \mathbb{C}^\times) \).

Theorem 7.1.1. Let \( f, g : A \to B \) be two morphisms of abelian varieties. Then \( (f + g)^\vee = \hat{f} + \hat{g} \) as maps \( \hat{B} \to \hat{A} \).

Remark 7.1.2. As we mentioned before, this is false on Pic, e.g. for \( k = \mathbb{C} \) we saw that \( \text{Pic}_0 \hat{B} \to H^2(A(\mathbb{C}), \mathbb{Z}(1)) = \bigwedge^2(H^1(\mathbb{Z})) \).

So there really is a subtlety here: Picard is somehow a “quadratic” functor but its identity component behaves linearly.

Proof. Without loss of generality, we can assume that \( k = \overline{k} \) and compare on \( k \)-points. So we want that for \( \mathcal{M} \in \text{Pic}_{A/k}^0(k) \) (i.e. \( \phi_{\mathcal{M}} = 0 \)),

\[
(f + g)^* \mathcal{M} \cong f^* \mathcal{M} \otimes g^* \mathcal{M} \quad \text{in Pic}(A).
\]

Note that we can ignore the trivializations, since as long as one has a trivialization, then the other has a unique compatible trivialization.

The left hand side is the pullback under \( (f, g) : A \to B \times B \) of \( m^*_B \mathcal{M} \). The right hand side is pullback under \( (f, g) \) of \( p^*_B \mathcal{M} \otimes p^*_B \mathcal{M} \). That these are isomorphic on \( B \times B \) was an earlier consequence of the Theorem of the Square.

Here we crucially used that \( \mathcal{M} \in \text{Pic}_{B/k}^0(k) \implies \phi_{\mathcal{M}} = 0 \) (the hard direction of the equivalence!).

The analytic case is enlightening. There is a linear piece and a quadratic piece, and on \( \text{Pic}^0 \) the quadratic piece vanishes. □

Corollary 7.1.3. We have \( [n]_{\hat{A}} = [n]_A \). (This is false on \( \text{Pic} / \text{Pic}^0 \) !)

With this basic relationship finally established, we can ask some more fundamental questions about the relationship between a morphism and its dual.

(1) Suppose \( f : A \to B \) is an isogeny of degree \( d > 0 \). Is \( \hat{f} : \hat{B} \to \hat{A} \) also an isogeny of degree \( d \)? The “isogeny” part is easy: once we set up the machinery, we’ll see that being an isogeny is equivalent to being a factor of \( [n]_A \). Therefore, the dual also has this property by Corollary 7.1.3. But what about the degree?

Example 7.1.4. For \( k = \mathbb{C} \), one can see this via the analytic model. It amounts to the assertion that if \( T : L \to L' \) has degree \( d \) for finite free \( \mathbb{Z} \)-modules \( L, L' \), then the dual map \( L^* \to (L')^* \): \( T^* \) also has degree \( d \).
The idea of proof is as follows: check that \( \tilde{f} \) is an isogeny via factoring some \([n]\), and verify that \( \text{deg}(f) = \#\ker f \) (in the sense of finite group schemes, namely \( \dim_{\mathcal{O}} \)), and then verify that that this is the same as \( \#\ker \tilde{f} \) by verifying that \( \ker f \) and \( \ker \tilde{f} \) are “Cartier dual.”

(2) Is the map \( \iota_A A \sim \widehat{\mathbb{A}} \) an isomorphism? Recall that this was constructed via the Poincaré bundle \( \mathcal{P}_A \) on \( A \times \widehat{A} \), giving \( \sigma^*(\mathcal{P}_A) \) on \( \widehat{A} \times A \), giving \( A \to \text{Pic}_{\widehat{A}/k, \sigma} \), which factors through \( (\widehat{A})^\wedge \) defining \( \iota_A \).

More generally, given a line bundle \( \mathcal{L} \) on \( A \times B \) with (compatible) trivializations along \( \{e\} \times B \) and \( A \times \{e'\} \), you can ask when the maps \( A \to \widehat{B} \) and \( B \to \widehat{A} \) are isomorphisms. This will involve the *Euler characteristic* of \( \mathcal{L} \):

\[
\chi(\mathcal{L}) = \sum_{l} (-1)^l h^l(A \times B, \mathcal{L}).
\]

This motvies us to compute \( \chi(\mathcal{P}_A) \). That will be quite a lengthy calculation.

### 7.2. Cohomology of the Poincaré bundle.

**Theorem 7.2.1.** \( H^n(A \times \widehat{A}, \mathcal{P}_A) = \begin{cases} 0 & n \neq g, \\ 1 & n = g. \end{cases} \)

**Proof.** Consider \( A \times \widehat{A} \xrightarrow{\pi} \widehat{A} \). We will use the Leray spectral sequence, which relates the total cohomology to the cohomology of the fibers. For this, we had better know the fibral line bundles. Tautologically,

\[
\mathcal{P}_A|_{\pi^{-1}(\mathcal{L})} \cong \mathcal{L}
\]

(the restriction of the universal bundle to the point of \( \widehat{A} \) corresponding to \( \mathcal{L} \) is \( \mathcal{L} \).) So

\[
E_2^{i,j} = H^i(\widehat{A}, R^j \pi_* \mathcal{P}_A) \Rightarrow H^{i+j}(A \times \widehat{A}, \mathcal{P}_A).
\]

We claim that \( R^j \pi_* \mathcal{P}_A \) is supported on \( \hat{0} \) for all \( j \). Why? By cohomology and base change, it’s enough to show that \( H^j(A, \mathcal{P}|_{A \times \{\hat{a}\}}) \) for all \( j \) for all \( \hat{a} \in \widehat{A}(k) \setminus \{0\} \). (See earlier argument.) Now, by the definition of \( \widehat{A} \), \( \mathcal{P}|_{A \times \{\hat{a}\}} = \hat{a} \). So it is enough to show that \( H^j(A, \mathcal{M}) = 0 \) for all \( \mathcal{M} \in \text{Pic}_{A/k}(k) \) such that \( \mathcal{M} \not\cong \mathcal{O}_A \). But we already this!

Now \( R^j \pi_* \mathcal{P}_A \) is a coherent sheaf on \( \widehat{A} \), which vanishes over \( \widehat{A} \setminus \{0\} \), so it’s “really” a coherent sheaf on an infinitesimal closed subscheme \( Z_j \subset \widehat{A} \) supported at \( 0 \). So \( H^j(\widehat{A}, R^j \pi_* \mathcal{P}_A) \) vanishes for \( i > 0 \), and the only possibly non-zero row is on \( i = 0 \). So the spectral sequence degenerates, hence

\[
H^n(A \times \widehat{A}, \mathcal{P}_A) = (R^n \pi_* \mathcal{P}_A)_0.
\]

This is \( k \)-finite, and 0 for \( n > g \) by the Theorem on formal functions because the infinitesimal fibers have dimension \( g \). ☻☻☻ TONY: [inquiry] It remains to show that this is 0 for \( n < g \) and 1-dimensional for \( n = g \).
Let $R = \mathcal{O}_{\hat{A}, 0}$, which is a regular local ring. Consider the base change

$$
\begin{array}{ccc}
A_R & \longrightarrow & A \times \hat{A} \\
\downarrow & & \downarrow \pi \\
\text{Spec } R & \longrightarrow & \hat{A}
\end{array}
$$

By cohomology and base change (for flat maps),

$$R^j \pi_*(\mathcal{P}_A)_{\hat{A}} = H^j(A_R, (\mathcal{P}_A)_{\hat{A}}).$$

By generalities on the cohomology of coherent sheaves on proper $R$-schemes, the right hand side is finite over $R$. In fact, since $H^j(A \times \hat{A}, \mathcal{P}_A)$ is finite-dimensional over $k$, the above is even finite dimensional over $k$. ♠♠♠ TONY: [what? not used later]

We can calculate this using the alternating Cech complex. Let $C^*$ be the alternating Cech complex for $(\mathcal{P}_A)_{\hat{A}}$ on $A_R$, which a bounded complex of flat $R$-modules

$$C^*: 0 \rightarrow C^0 \rightarrow \ldots \rightarrow C^N \rightarrow 0$$

such that $H^j(C^*)$ are all $R$-finite. ♠♠♠ TONY: [what about this alternating guy?]

Now there is a beautiful trick due to Mumford: given a bounded complex of modules whose cohomology is finite, there exists a finite flat complex which computes the same cohomology even after base change. (See Chapter II, §5, 2nd Theorem of Mumford or CH III, §12.3 of Hartshorne.) More precisely, studying cohomology and base change shows that there exists a bounded complex of finite free $R$-modules

$$K^*: 0 \rightarrow K^0 \rightarrow K^1 \rightarrow \ldots \rightarrow K^N \rightarrow 0$$

and $K^* \rightarrow C^*$ such that for all $R$-modules $M$,

$$H^j(K^* \otimes M) \sim H^j(C^* \otimes_R M)$$

for all $j$.

The idea of the construction is not hard to guess. The top homology is finitely generated, so you pick some free thing mapping to it. Then you keep going downwards, and at a certain point you’ve gone too far, so you truncate. Note that Mumford takes $M$ to be an $R$-algebra in his construction, but it isn’t necessary.

Now we have a bounded complex $K^*$ of finite free $R$-modules with the property that $H^j(K^*)$ are all $k$-finite and vanish for $j > g = \dim R$. We claim that whenever we’re in this kind of situation, and $R$ is “nice” enough (e.g. regular), then the homologies automatically vanish in dimension below $g$ as well. For the one-dimensionality, we’re going to use the universality of the Poincaré bundle relative to $\hat{A}$ as a moduli scheme (i.e. using infinitesimal bases).

**Lemma 7.2.2.** Let $R$ be Cohen-Macaulay (e.g. regular) local ring of dimension $g \geq 0$. Let $K^*$ be a bounded complex of finite free $R$-modules

$$0 \rightarrow K^0 \rightarrow \ldots \rightarrow K^N \rightarrow 0$$

such that all the $H^j(K^*)$ have finite $R$-length. Then $H^j(K^*) = 0$ for all $j < g$.
Proof. We induct on $g$. The case $g = 0$ is empty. Suppose $g > 0$ and pick $x \in \mathfrak{m}_R$ a non-zerodivisor (so $\overline{R} = R/(x)$ is Cohen-Macaulay of dimension $g - 1$). Then

$$0 \rightarrow R \xrightarrow{x} R \rightarrow \overline{R} \rightarrow 0$$

is exact, and since $K^\bullet$ is finite free

$$0 \rightarrow K^\bullet \xrightarrow{x} K^\bullet \rightarrow \overline{K}^\bullet \rightarrow 0$$

is exact, so we get a long exact sequence in cohomology,

$$\cdots \rightarrow H^{j-1}( \overline{K}^\bullet ) \xrightarrow{\delta} H^j(K^\bullet) \xrightarrow{x} H^j(K^\bullet) \rightarrow H^j(\overline{K}^\bullet) \xrightarrow{\delta} \cdots$$

so $H^j(\overline{K}^\bullet)$ all have finite length. Therefore, we can apply induction to $\overline{K}^\bullet$ viewed over $R$ (which is Cohen-Macaulay of dimension $g - 1$) to get that $H^j(\overline{K}^\bullet) = 0$ for $j < g - 1$. For $j < g$ (so $j - 1 < g - 1$), $H^{j-1}(\overline{K}^\bullet) = 0$, so $x$-multiplication on $H^j(K^\bullet)$ is injective. But $H^j(K^\bullet)$ has finite $R$-length, so it is killed by $m_R^N$ for $N \gg 0$, hence by $x^N$. That shows that $H^j(K^\bullet) = 0$.

\[ \square \]

Remark 7.2.3. Here we only needed flatness, not finiteness, so we didn’t need the $K^\bullet$.

From this, we conclude that the Čech complex was exact in degrees below $g$.

$$0 \rightarrow K^0 \rightarrow \cdots \rightarrow K^g \rightarrow K^{g+1} \rightarrow \cdots \rightarrow K^N \rightarrow 0$$

Suppose $N > g$. Then $\ker(K^{N-1} \rightarrow K^N)$ is finite and $R$-flat, as kernel of a surjective map of flats (hence finite free) and its formation commutes with any tensor over $R$, we can drop $K^n$ by replacing $K^{n-1}$ with this kernel.

Thus without loss of generality, we may assume that $N = g$. That is, we have a finite free resolution of $H^g(K^\bullet) = R^g \pi_s(\mathcal{A}_0)$:

$$0 \rightarrow K^0 \rightarrow \cdots \rightarrow K^g \rightarrow R^g \pi_s(\mathcal{A}_0) \rightarrow 0$$

and we want to know that $R^g \pi_s(\mathcal{A}_0)$ has length 1. Applying $\Hom_R(-, R)$, we get

$$0 \rightarrow \overline{K}^0 \rightarrow \cdots \rightarrow \overline{K}^g \rightarrow 0$$

whose homology computes $\Ext^*(R^g \pi_s(\mathcal{A}_0)_0, R)$. But $R^g \pi_s(\mathcal{A}_0)_0$ has finite length, so the $\Ext$ groups also have finite length ♠♠♠ TONY: [something to check here], and then we can apply the Lemma again! That tells us that this is exact in low degrees. Let $M$ be the final homology group, $\Ext_R^g(R^g \pi_s(\mathcal{A}_0)_0, R)$, which has finite length, so we have another finite free resolution

$$0 \rightarrow \overline{K}^g \rightarrow \cdots \rightarrow \overline{K}^0 \rightarrow \overline{M} \rightarrow 0.$$ 

So $R^g \pi_s(\mathcal{A}_0)_0 = \Ext_R^g(M, R)$. To show that it is one-dimensional, we’re going to analyze $M$.

It is a general fact that for Gorenstein (e.g. regular) local rings of dimension $g$ that $\Ext^g_R(\text{residue field}, R)$ is 1-dimensional (this is a manifestation of local duality for Gorenstein rings). So it’s enough to show that $M$ is 1-dimensional over $k$. 

59
We know that $M$ is finitely generated over $R$, and we claim that it is generated by a single element. Indeed, $M$ is the cokernel of a map of finite free modules $M = \text{coker}(\hat{K}^1 \to \hat{K}^0)$, so $$M/m = \text{coker}((K^1 \mod m)^* \to (K^0 \mod m)^*)$$ since tensoring is right exact, and dualizing commutes with everything for free modules. But this is the same as $\text{ker}(K^0 \otimes R/m \to K^1 \otimes R/m)$, which is $$H^0(K^* \otimes R/m) = H^0(A, \mathcal{P}_{A|A \times \text{Spec}(R/m)}) = k.$$ By Nakayama’s lemma, $M$ is principally generated, so $M = R/J$. It remains to check that $J = m$.

For any $m$-primary $J' \subset R$, $$\text{Hom}(M, R/J') = \text{ker}((K^0 \mod J') \to K^1 \mod J')$$ $$\cong H^0(C^* \mod J')$$ $$= H^0(A \times \text{Spec}(R/J'), \mathcal{P}_{A|A \times \text{Spec}(R/J')}).$$ Let’s apply this to both $J' = J$ and $m$. We get

$$\text{Hom}(M, R/J) \sim \Gamma(A \times \text{Spec } R/J, \mathcal{P}_{A})$$

$$\text{Hom}(M, R/m) \sim \Gamma(A, \mathcal{O}_{A})$$

The left hand side is trivially surjective, so the right hand side is surjective. That shows that the generating section of $\Gamma(A, \mathcal{O}_{A})$ lifts, so $\mathcal{P}_{A|A \times \text{Spec}(R/J)} \cong \mathcal{O}$ (i.e. is trivial!). Now, by the universal property of $\mathcal{P}_{A}$, it follows that the induced inclusion of the infinitesimal point $\text{Spec}(R/J) \to \hat{A}$ factors through the inclusion $\text{Spec}(R/m) \to \hat{A}$, so $J = m$. \hfill \Box

**Corollary 7.2.4.** $\chi(\mathcal{P}_{A}) = (-1)^g$.

### 7.3. Dual isogenies.

**Corollary 7.3.1.** If $f: A \to B$ is an isogeny of degree $d$ (see HW6), then $\hat{f}: \hat{B} \to \hat{A}$ is an isogeny of degree $d$.

**Proof.** For $n > 0$ killing the finite $k$-group scheme $\ker f$, we have $A[n] \supset \ker f$ (see HW6). That induces

$$A \xrightarrow{[n]_A} A$$

and dualizing everything gives

$$\hat{A} \xrightarrow{[n]_A=[n]_{\hat{A}}} \hat{A}$$
so \( \hat{f} : \hat{B} \to \hat{A} \) is surjective, but the dimensions are the same. By flatness considerations (e.g. Miracle Flatness theorem, surjective homomorphism of smooth groups over a field is automatically flat, or better yet generic flatness plus the group structure), \( \dim(\ker \hat{f}) = 0 \), i.e. \( \hat{f} \) is quasi-finite, and proper, hence finite, so \( \hat{f} \) is an isogeny. TONY: [didn’t really need miracle flatness?]

What about the degree? HW5 implies that

\[
\begin{array}{ccc}
A \times \hat{B} & \xrightarrow{1 \times \hat{f}} & A \times \hat{A} \\
\downarrow f \times 1 & & \downarrow f \times 1 \\
B \times \hat{B} & & B \times \hat{B}
\end{array}
\]

pulls back \( \mathcal{L} \cong (1 \times \hat{f})^* \mathcal{P}_A \cong (f \times 1)^* \mathcal{P}_B \) (This is basically just theorem of the square). But \( f \times 1 \) and \( 1 \times \hat{f} \) are finite flat surjections of degrees \( d \) and \( \hat{d} \) respectively. We want to check that these are the same. The idea is to compare these using the Euler characteristic. The effect on Euler characteristic on pullback via a finite flat map is to multiply by degree. Formally, if \( \varphi : X \to Y \) is a finite flat surjection of degree \( m \) between proper \( k \)-schemes, then

\[\chi(\varphi^* \mathcal{L}) = m \chi(\mathcal{L}).\]

The point is that \( \chi(\varphi^* \mathcal{L}) = \chi(\varphi_* \mathcal{L} \otimes \mathcal{O}_X) \), and \( \varphi_* \mathcal{O}_X \) is a rank \( m \) vector bundle.

Applying this above, we get that

\[\hat{d} \chi(\mathcal{P}_B) = \chi(Q) = d \chi(\mathcal{P}_A).\]

\[\square\]

**Theorem 7.3.2.** Let \( A, B \) be abelian varieties of dimension \( g > 0 \) and \( \mathcal{L} \) a line bundle on \( A \times B \) such that \( \mathcal{L}|_{A \times \{0\}}, \mathcal{L}|_{\{0\} \times B} \) are trivial, so that \( \mathcal{L} \) corresponds to a homomorphism \( f = f_\mathcal{L} : A \to \hat{B} \). (The fact that \( \mathcal{L} \) trivializes on \( A \times \{0\} \) gives a map to \( \hat{B} \), and the fact that \( \mathcal{L} \) trivializes on \( \{0\} \times B \) implies that it sends 0 to 0.) Then the following are equivalent:

1. \( |\chi(\mathcal{L})| = 1 \)
2. \( f_\mathcal{L} : A \to \hat{B} \) or \( f'_\mathcal{L} : B \to \hat{A} \) is an isomorphism,
3. both \( f_\mathcal{L} \) and \( f'_\mathcal{L} \) are isomorphisms.

**Example 7.3.3.** If \( B = \hat{A}, \mathcal{L} = \mathcal{P}_A \) then \( f'_\mathcal{L} = \text{Id}_{\hat{A}} \), \( f_\mathcal{L} = \iota_A \) so the theorem implies the “double duality” result.

**Proof.** Since \( \sigma : B \times A \isom A \times B \) satisfies \( \chi(\sigma^* \mathcal{L}) \cong \chi(\mathcal{L}) \), the content is to show that \( |\chi(\mathcal{L})| = 1 \iff f_\mathcal{L} \) is an isomorphism.

One direction is easy. Suppose \( f_\mathcal{L} \) is an isomorphism. Then \( (1 \times f_\mathcal{L})^* (\mathcal{P}_B) = \mathcal{L} \) (by definition of \( f_\mathcal{L} \)). Since \( 1 \times f_\mathcal{L} : A \times B \isom B \times \hat{B} \), we have \( \chi(\mathcal{L}) = \chi(\mathcal{P}_B) = \pm 1 \).

In the other direction, the idea is that if \( f_\mathcal{L} \) isn’t an isomorphism, it factors through some non-trivial isogeny, which imposes some divisibility condition on \( \chi(\mathcal{L}) \).

So suppose that \( |\chi(\mathcal{L})| = 1 \), so \( \chi(\mathcal{L}) \in \mathbb{Z} \) is not divisible by any prime. We want \( f_\mathcal{L} : A \to \hat{B} \) to be an isomorphism. Since \( \dim A = \dim B \), \( f_\mathcal{L} \) is an isomorphism if and
only if \( \ker(f_\varpi) = 1 \) as a scheme. This result is because the degree of an isogeny coincides with the degree of the kernel.

**Exercise 7.3.4.** Check this. Basically a computation for quotients in the fppf topology.

Suppose \( K := \ker(f_\varpi) \neq 1 \). We seek a contradiction. By HW5, \( K^0_{\text{red}} \) is an abelian subvariety. (At this point we could assume that \( k = \overline{k} \), but it is not necessary. Over a perfect field, this is obvious. But over an imperfect field, we can make affine, connected group schemes whose underlying reduced scheme is not a subgroup scheme.) If \( K \) is not finite, then \( K^0_{\text{red}}[\ell] \neq 0 \) for some prime \( \ell \), which we may assume is not \( \text{char} \ k \). Therefore, \( K \) always contains a finite closed \( k \)-subgroup scheme \( H \neq 1 \). Now we factor

\[
\begin{array}{ccc}
A & \xrightarrow{f_\varpi} & \hat{B} \\
\downarrow{g} & & \downarrow{} \\
A/H & & \end{array}
\]

and \( g \) is an isogeny of degree \( \#H > 1 \). Then \( \chi(\varpi) = \chi((f_\varpi \times 1)^* \mathcal{P}_B) = \chi(g^*(\mathcal{L})) = (\deg g) \chi(\mathcal{L}) \).

\[\blacktriangleleft\blacktriangleleft \text{ TONY: [change notation]} \blacktriangleleft\blacktriangleleft\]

\[\square\]

### 7.4. Symmetric morphisms

Now that we know double duality is an isomorphism, it makes sense to consider the notion of a “symmetric” map \( A \to \hat{A} \).

**Parallels with linear algebra.** Recall that if \( V, W \) are finite-dimensional over \( k \), then

\[
\begin{array}{c}
\text{Bilinear maps} \quad V \times W \xrightarrow{B} k \\
\leftrightarrow \quad \text{linear maps} \quad V \xrightarrow{T} W^* \\
\text{eval} \quad v \mapsto B(v, -)
\end{array}
\]

For \( T: V \to W^* \), the dual map \( V^* \xleftarrow{T^*} W^{**} \sim W \) corresponds to \( w \mapsto B(-, w) \).

If \( W = V \), then \( V \times V \xrightarrow{B} k \) is symmetric if and only if \( V \xrightarrow{T_L} V^* \) is symmetric in the sense of double duality. Our starting point for abelian varieties is analogous to this.

**Remark 7.4.1.** The connection with linear algebra in the analytic theory of abelian varieties over \( \mathbb{C} \) is much more direct.

**Remark 7.4.2.** There is a theory of \( \mathbb{G}_m \)-biextensions” that gives a geometric construction mimicking this.

For any bilinear form \( B: V \times V \to k \) with induced linear map \( T_B \), the composition

\[
V \xrightarrow{(1, T_B)} V \times V^* \xrightarrow{\text{eval}} k
\]

recovers \( B \). So the evaluation map \( V \times V^* \to k \) is analogous to the Poincaré bundle.

**Definition 7.4.3.** A homomorphism \( f: A \to \hat{A} \) is symmetric if \( f = \hat{f} \circ \iota_A \):

\[
\hat{A} \xleftarrow{\hat{f}} \hat{A} \xleftarrow{\iota_A} A.
\]

**Proposition 7.4.4.** For \( \mathcal{L} \) on \( A \), \( \phi_\mathcal{L}: A \to \hat{A} \) is symmetric.
Remark 7.4.5. Over an algebraically closed field, all symmetric homomorphisms are obtained by this construction. (It’s in Mumford’s book.) Now we know that \( \phi_L \) doesn’t recover \( L \). We emphasize that if \( k \) is not algebraically closed, then you can have symmetric homomorphisms not defined by some \( \phi_L \) for \( L \) defined over that field.

The correspondence \( L \leftarrow \phi_L \) is analogous to the relationship between a quadratic form over \( \mathbb{Z} \) and a symmetric bilinear form over \( \mathbb{Z} \).

Proof. We want to know if

\[
\begin{array}{c}
A \\ \downarrow_{\iota_A} \\
\widehat{A} \\
\phi_L \downarrow \\
\widehat{\widehat{A}}
\end{array}
\]

is equal to \( \phi_L \). Equivalently, we want to show that \( \phi_L \circ \iota_A^{-1} : \widehat{\widehat{A}} \to \widehat{A} \) is equal to \( \phi_L \). In general, for \( f : A \to B \), with associated diagram

\[
\begin{array}{ccc}
A \times B & \xrightarrow{1 \times f} & A \times \widehat{A} \\
\downarrow f \times 1 & & \downarrow \\
B \times \widehat{B}
\end{array}
\]

we know that

\[
(1 \times f)^* \mathcal{P}_A \cong (f \times 1)^* \mathcal{P}_B.
\]

As the maps here are classified by their pullback of the Poincaré bundle, it is equivalent to show that

\[
(1 \times (\phi_L \circ \iota_A^{-1}))^* \mathcal{P}_A \cong (\phi_L \times \iota_A)^* \mathcal{P}_A.
\]

By functoriality, the left hand side is \( (1 \times \iota_A^{-1})^* (1 \times \phi_L)^* \mathcal{P}_A \), so we want

\[
(1 \times \phi_L)^* \mathcal{P}_A \cong (1 \times \phi_L \times 1)^* \mathcal{P}_A
\]

\[
\cong (\phi_L \times 1)^* (1 \times \iota_A)^* \mathcal{P}_A
\]

(double duality) \( \iff \cong (\phi_L \times 1)^* \sigma^* \mathcal{P}_A \)

where \( \sigma : \widehat{\widehat{A}} \times A \cong A \times \widehat{\widehat{A}} \).

\[
\begin{array}{cc}
A \times \widehat{\widehat{A}} & \\
\downarrow 1 \times \iota_A^{-1} & \\
A \times A \\
\downarrow \phi_L \times 1 & \\
A \times A \\
\downarrow \Sigma & \\
A \times A
\end{array}
\]

which is \( (\phi_L \times 1)^* \sigma^* \mathcal{P}_A = (1 \times \phi_L)^* \mathcal{P}_A \).
7.5. **Ampleness.** Although $\phi_\mathcal{L}$ only “knows” $\mathcal{L}$ up to $\text{Pic}^0_{A/k} = \hat{A}$, we will see that in some sense $\phi_\mathcal{L}$ can detect if $\mathcal{L}$ is ample or not!

**Remark 7.5.1.** The Nakai-Moishezon criterion says that for geometrically integral, projective $k$-schemes $X$, $\mathcal{L}$ is ample if and only if it has positive degree on every curve over $\overline{k}$. In such a situation, ampleness of a line bundle on $X$ depends only on the class of $\mathcal{L}$ in the Nerón-Severi group $(\text{Pic}_X/k)/\text{Pic}^0_X/k)$, hence ampleness is insensitive to moving in connected families.

**An analogy.** Recall the analogy we made last time, which is made precise by the complex analytic theory: $L \mapsto \phi_\mathcal{L}$ is analogous to the association

$$n\text{ symmetric bilinear form }B_q: L \times L \to \mathbb{Z}$$

sending

$$((\ell, \ell')) \mapsto q(\ell + \ell') - q(\ell) - q(\ell').$$

But given $B: L \times L \to \mathbb{Z}$, if you try to recover $Q_B = B|_{\text{diag}}: \ell \mapsto B(\ell, \ell)$ then you get back $Q_B(n) = 2q$. So you see that you don’t quite recover $q$, as there is an ambiguity of 2, although over $\mathbb{Z}$ you can just divide by 2.

In the abelian variety case, we can try to recover $\mathcal{L}$ by pulling back the Poincaré bundle via

$$(1, \phi_\mathcal{L}) \circ \Delta_{A/k}: A \to A \times \hat{A}$$

to get $(\Delta_{A/k})^*(1 \times \phi_\mathcal{L})^*\mathcal{P}_A$. Now the bundle $(1 \times \phi_\mathcal{L})^*\mathcal{P}_A$ on $A \times A$ is our old friend $\Lambda(\mathcal{L}) = m^*\mathcal{L} \otimes p_1^*\mathcal{L}^{-1} \otimes p_2^*\mathcal{L}^{-1}$. So when we restrict to the diagonal, we get $[2]^*\mathcal{L} \otimes \mathcal{L}^{-2}$.

**Lemma 7.5.2.** For $n \in \mathbb{Z}$ and $\mathcal{L}$ a line bundle on $A$,

$$[n]^*\mathcal{L} \cong \mathcal{L} \otimes \mathcal{L}^{-n} \quad (\text{mod } \text{Pic}^0_{A/k}).$$

In other words, the effect of $[n]_A$ on $\text{NS}(A_{\overline{k}})$ is multiplication by $n^2$.

**Example 7.5.3.** For $n = 2$, this tells us that $[2]^*\mathcal{L} \cong \mathcal{L}^4$ (mod $\text{Pic}^0_{A/k}$), so

$$([2]^*\mathcal{L} \otimes \mathcal{L}^{-2}) \cong \mathcal{L}^6 \quad (\text{mod } \text{Pic}^0_{A/k}).$$

Once we prove that ampleness is insensitive under tensoring with stuff in $\text{Pic}^0$, we see that we can recover $\mathcal{L} \otimes \mathcal{L}^2$ up to something from $\text{Pic}^0$ from $\phi_\mathcal{L}$. Since $\mathcal{L} \otimes \mathcal{L}^2$ is ample if and only if $\mathcal{L}$ is, we win.

**Proof.** We showed some time ago that

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

So we want to show that $\mathcal{L} \otimes [-1]^*\mathcal{L}^{-1} \in \text{Pic}^0$, or equivalently (since we saw that being in $\text{Pic}^0$ is the same as being killed by the $\phi$-construction) that

$$\phi_\mathcal{L} = \phi_{[-1]^*\mathcal{L}}$$ as maps $A \to \hat{A}$. 


So we may assume without loss of generality that $k = \overline{k}$ and compute on $x \in A(k)$:

$$t^*_x \mathcal{L} \otimes \mathcal{L}^{-1} \cong t^*_x (-1)^* \mathcal{L} \otimes (-1)^*(\mathcal{L}^{-1})$$

$$\cong (-1)^*(t^{-1}_x \mathcal{L} \otimes (-1)^* \mathcal{L}^{-1})$$

$$\cong (-1)^* \varphi(-x).$$

But $\varphi(-x) \in \hat{A}$, and $(-1)^* \varphi(-x) = (-1) \varphi(-x)$ and we know that $[n]_A = [n]_{\widehat{A}}$, so this is $\varphi(x)$ (since $\varphi$ is a homomorphism). 

□

**Proposition 7.5.4.** For any line bundles $\mathcal{L}, \mathcal{N}$ on $A$ with $\mathcal{N} \in \text{Pic}^0_{\text{A}/k}(k)$, $\mathcal{L}$ is ample if and only if $\mathcal{L} \otimes \mathcal{N}$ is ample, i.e. ampleness depends only on $[\mathcal{L}]$ in $\text{NS}(A)$.

**Remark 7.5.5.** This shows that $\mathcal{L}$ is ample if and only if $(1, \varphi_{\mathcal{L}})^* \mathcal{O}_A$ is ample.

**Proof.** It suffices to prove the forward direction that if $\mathcal{L}$ ample, then $\mathcal{L} \otimes \mathcal{N}$ is ample, since the other can be obtained by tensoring with $\mathcal{N}^{-1}$.

Recall that ampleness is insensitive to ground field extension, so we may and do assume that $k$ is algebraically closed. Then we know that $\varphi_{\mathcal{L}} : A(k) \to \hat{A}(k)$ is surjective (which needs the assumption on the ground field!), so $\mathcal{N} = \varphi_{\mathcal{L}}(x) = t^*_x \mathcal{L} \otimes \mathcal{L}^{-1}$ for some $x \in A(k)$, so $\mathcal{L} \otimes \mathcal{N} \cong t^*_x \mathcal{L}$, and $t_x$ is an automorphism hence preserves ampleness. □

---

I will be become the dealer.


---

So although $\varphi_{\mathcal{L}}$ doesn’t recover $\mathcal{L}$, it does recover the ampleness. This is important for the theory of polarizations. You don’t see this in the theory of elliptic curves, because they coincide with the multiplication by $n$ maps.

### 7.6. Endomorphisms.

Let $X, Y$ be abelian varieties over $k$. We now study $\text{Hom}_k(X, Y)$. In particular, we want to show that it is $\mathbb{Z}$-finite. Since $\text{Hom}_k(X, Y) \hookrightarrow \text{Hom}_{\overline{k}}(\overline{X}, \overline{Y})$, it suffices for this purpose to work over $k = \overline{k}$. This affords the advantage of giving us lots of torsion points.

Here is a useful trick. If $X, Y$ are abelian varieties, we have $\text{End}(X \times Y) = \text{End}(X) \oplus \text{Hom}(X, Y) \oplus \text{Hom}(Y, X) \oplus \text{End}(Y)$. Therefore, the $\mathbb{Z}$-finiteness of $\text{Hom}(X, Y)$ follows from showing that for $\text{End}_k(A)$. The advantage of $\text{End}_k(A) \otimes \mathbb{Z} \mathbb{Q}$ is that it has a multiplicative structure making it an associative $\mathbb{Q}$-algebra. We know that this is torsion-free, so

$$\text{End}_k(A) \hookrightarrow \text{End}_k(A) \otimes \mathbb{Z} \mathbb{Q}.$$ 

Why working rationally makes things nicer can be seen from the analogy between $\mathbb{Z}$-lattice representations of a finite group $\Gamma$ versus finite-dimensional $\mathbb{Q}$-linear representations of $\Gamma$ - on the right hand side we have isotypic decomposition, semisimplicity, etc.

Analogous to the semiplicity, abelian subvarieties of $A$ will split off in $\text{End}_k(A) \otimes \mathbb{Z} \mathbb{Q}$. Indeed, in HW6 Exercise 1 we define $\text{Hom}_k^0(A, B) := \text{Hom}_k(A, B) \otimes \mathbb{Q}$, the isogeny category of abelian varieties over $k$, and you check that a usual map $f : A \to B$ becomes an
isomorphism in the isogeny category if and only if $f$ is an isogeny. Remark: the objects are abelian varieties, but there are no points because points are not functorial. We claim that this category is semi-simple.

**Theorem 7.6.1** (Poincaré reducibility). For $A' \hookrightarrow A$ an abelian subvariety over $k$, there exists an abelian subvariety $A'' \hookrightarrow A$ over $K$ such that $A' \times A'' \rightarrow A$ is an isogeny.

In the analogy, you try to construct a projector. Here, we use a map to the dual as a proxy for a symmetric invariant bilinear form, and try to make the analogous argument, constructing $A'$ as a kind of orthogonal complement.

**Remark 7.6.2.** This is false for $\mathbb{C}$-analytic tori.

**Proof.** Choose an ample line bundle $\mathcal{L}$ on $A$. Quite generally for $f: B \rightarrow A$ we have

$$\hat{f} \circ \phi_{\mathcal{L}} \circ f = \phi_{f^* \mathcal{L}},$$

i.e. the diagram commutes

$$\begin{array}{ccc}
B & \xrightarrow{f} & A \\
\phi_{f^* \mathcal{L}} & \downarrow & \phi_{\mathcal{L}} \\
B & \leftarrow & \hat{A}
\end{array}$$

Applying this to $B = A'$, we have

$$\begin{array}{ccc}
A' & \xrightarrow{i} & A \\
\phi_{i^* \mathcal{L}} & \downarrow & \phi_{\mathcal{L}} \\
\hat{A'} & \leftarrow & \hat{A}
\end{array}$$

Then consider $\ker(\hat{f} \circ \phi_{\mathcal{L}})$. By homework, $\ker(\hat{f} \circ \phi_{\mathcal{L}})_{\text{red}}$ is an abelian variety (especially a smooth $k$-subgroup scheme) ♠♠♠ **TONY:** [this fixes a gap in Milne’s article]. What can we say about $A'' \cap A'$? It lies in $\ker \phi_{i^* \mathcal{L}}$ which is finite. So we just need to know that $\dim A'' \geq \dim A - \dim A'$.

The point is that $\phi_{\mathcal{L}}$ is finite surjective, so its presence doesn't really affect the dimension. So

$$\dim A'' = \dim \ker \hat{f} \geq \dim \hat{A} - \dim \hat{A}' = \dim A - \dim A',$$

which is what we wanted. □

**Definition 7.6.3.** We say that $A$ is $k$-simple if it is non-zero and has no non-zero proper abelian subvarieties over $k$.

**Exercise 7.6.4.** HW7 shows that $k$-simple does not imply $\overline{k}$-simple.

**Notation.** If $A, B$ are abelian varieties over $k$, then there exists an isogeny $A \rightarrow B$ if and only if there exists an isogeny $B \rightarrow A$ (all over $k$). We write $A \sim B$.

Last time we saw that if $A' \hookrightarrow A$ is an abelian subvariety, then there is an “isogeny complement” $A'' \hookrightarrow A$ such that $A' \times A'' \rightarrow A$ is an isogeny. This shows that

$$A \sim \prod A_i^{e_i}$$

with each $A_i$ simple, pairwise non-isogeneous over $k$. 
If $B$ is $k$-simple, then
\[
\text{Hom}_k^0(B, A) \cong \prod_i \text{Hom}_k^0(B, A_i)^{e_i}
\]
because we’ve just seen that the isogeny category is semisimple (think Schur’s Lemma in representation theory). But for $k$-simple $B, B'$ any non-zero element in $\text{Hom}_k^0(B, B')$ is an isogeny! Therefore, at most one of the above is non-zero. So this is
\[
\text{Hom}_k^0(B, A) \cong \begin{cases} 
0 & B \not\sim A_i \text{ for all } i, \\
\text{End}_k^0(A_{i_0})^{e_{i_0}} & B \sim A_{i_0}
\end{cases}
\]
and $\text{End}_k^0(A_{i_0})^{e_{i_0}}$ is a division algebra (again think Schur’s Lemma). Therefore, $\{A_i\}$ is unique up to $k$-isogeny and the $e_i$ are also unique. We can say phrase this as follows.
\[
\sum_{f: A_{i_0} \sim A} f(A_{i_0}) \subset A
\]
is intrinsic to $A$, and called the “$A_{i_0}$-isotypic piece,” of dimension $e_{i_0}A_{i_0}$. Again, think to the representation theory of finite groups.

**Remark 7.6.5.** If $B, B' \subset A$ are abelian subvarieties and there exists a commutative diagram
\[
\begin{array}{ccc}
B & \sim & B' \\
\downarrow & & \downarrow \\
A & & \\
\end{array}
\]
in the isogeny category, then $B = B'$ inside $A$. This is basically the fact that multiplication by $n$ is surjective.

**Exercise 7.6.6.** Prove it.

This is analogous to lattice representations of finite groups. Rationally you get a direct sum decomposition, and on the lattice level you don’t get this but you get something off by finite index.

Now let’s study $\text{Hom}_k(A, B)$. We have $k$-simple decompositions
\[
A \sim \prod A_i^{e_i}, \quad B \sim \prod B_j^{f_j}.
\]
Tensoring with $\mathbb{Q}$, we get
\[
\text{Hom}_k^0(A, B) = \prod_{i,j} \text{Hom}_k(A_i, B_j)^{e_i f_j}.
\]
Now $\text{Hom}_k(A_i, B_j)^{e_i f_j}$ vanishes unless $A_i \sim B_j$. Therefore, $L := \text{Hom}_k(A, B)$ and $L' := \prod_{i,j} \text{Hom}_k(A_i, B_j)^{e_i f_j}$ fit into a diagram of the form
\[
\begin{array}{ccc}
L & \longrightarrow & L' \\
\downarrow & & \downarrow \\
& n & \end{array}
\]
Thus for \( \mathbb{Z} \)-finiteness, it's enough to study the case where \( A, B \) are \( k \)-simple and isogenous over \( k \). By the same game comparing \( \text{Hom}(A, B) \) and \( \text{Hom}(A, A) \), we can reduce to studying \( \text{Hom}(A, A) \).

**Remark 7.6.7.** Once the \( \mathbb{Z} \)-finiteness is settled, \( \text{End}^{0}_k(A) \) is a finite-dimensional division algebra over \( \mathbb{Q} \). Therefore, its center \( Z \) is a number field. What kind of number field? (We know from elliptic curves that you can only get \( \mathbb{Q} \), or a quadratic imaginary field.) Such \( Z \) and the class of \( \text{End}^{0}_k(A) \in \text{Br}(Z) \) are very restricted, see §21 of Mumford AV for \( k = \overline{k} \).

The presence of the polarization forces \( Z \) to be totally real or a CM field.

**Theorem 7.6.8.** For \( A, B \) abelian varieties over \( k \),
\[
\text{Hom}_k^\ell(A, B) \rightarrow \text{Hom}_{\mathbb{Z}_\ell^\ell}(T_\ell A, T_\ell B) \subset \text{Hom}_{\mathbb{Z}_\ell}(T_\ell A, T_\ell B).
\]

**Remark 7.6.9.**
(1) This gives a very crude upper bound on the \( \mathbb{Z} \)-rank:
\[
\text{rank}_{\mathbb{Z}} \text{Hom}_k(A, B) \leq 4 \dim A \cdot \dim B.
\]
If \( \text{ch} k = 0 \), then one can do better using the \( \mathbb{C} \)-analytic theory and then using the Lefschetz principle to reduce to this case.

(2) There is a version for \( \ell = p \) using \( p \)-divisible groups in place of Tate modules. But actually there is a way of making a uniform statement even of the \( \ell \)-adic Tate module in terms of \( \ell \)-divisible groups (but this is much better to do after knowing the \( \mathbb{Z} \)-finiteness).

(3) The Tate conjecture is that the injection is an isomorphism for \( k \) finitely generated over its prime field. This was proved by Tate for finite fields, Zahrin for positive characteristic, and Faltings in characteristic 0. The first two are also true for \( \ell = p \), but not easy to find in the literature. See the book of Conrad and Oort.

(4) One might wonder if this injectivity of \( \mathbb{Z}_\ell \) for many \( \ell \) gives the result automatically for purely group-theoretic reasons. If you take \( M \) to be the subset of rational numbers with squarefree denominator, but \( M \otimes \mathbb{Z}_\ell = \frac{1}{\ell} \mathbb{Z}_\ell \) is \( \mathbb{Z}_\ell \)-finite for all \( \ell \).

**Proof.** Without loss of generality, \( k = \overline{k} \) and \( A = B \) is \( k \)-simple. Now we study the ring \( \text{End}_k A \). Then we have a multiplicative map
\[
\text{deg}: \text{End}_k A \rightarrow \mathbb{Z}
\]
sending \( f \) to 0 if it is 0, and \( \text{deg} f \) otherwise. Noting
\[
\text{deg}(n f) = \text{deg}([n]) \text{deg}(f) = n^{2g} \text{deg} f,
\]
we see that \( \text{deg} \) extends uniquely to a function homogeneous of degree \( 2g \)
\[
\text{deg}: \text{End}^{0}_k(A) = \text{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Q} \rightarrow \mathbb{Q}
\]
sending \( \frac{1}{m} f \rightarrow \frac{1}{m^{2g}} \text{deg} f \).

We claim that \( \text{deg} \) is a “polynomial function” on this vector space, but since we don’t yet know that \( \text{End}^{0}_k(A) \) is finite dimensional, we have to phrase this carefully.

**Definition 7.6.10.** Let \( W \) be a vector space over an infinite field \( F \). A function \( f: W \rightarrow F \) is polynomial if it is given by a polynomial in linear coordinates on every finite-dimensional subspace. The obvious definition is made for “homogeneous polynomial of degree \( d \).”
Proposition 7.6.11. As defined above, \( \text{deg}: \text{End}_k^0(A) \rightarrow \mathbb{Q} \) is polynomial (hence automatically homogeneous of degree \( 2g \)).

Proof. We'll study degree by relating it to Euler characteristics of line bundles.

By HW7, it's enough to treat, it is always enough to check on 2-dimensional subspaces. (The one-dimensional case is already clear by homogeneity.) By homogeneity, we can study

\[ n \rightarrow \text{deg}(n \phi + \psi) \]

for fixed \( \phi, \psi \in \text{End}(A) \). We want to prove that this is in \( \mathbb{Q}[n] \).

We know that one way to interpret the degree is from its effect on the Euler characteristic:

\[ \text{deg}(n \phi + \psi) = \frac{\chi((n \phi + \psi)^* \mathcal{L})}{\chi(\mathcal{L})} \]

such that \( \chi(\mathcal{L}) \neq 0 \).

for ample \( \mathcal{L} \) such that \( \chi(\mathcal{L}) \neq 0 \). Here we're using that \( n \phi + \psi \) is an isogeny (finite flat) if non-zero. The condition \( \chi(\mathcal{L}) \neq 0 \) is easily achieved for some \( \mathcal{L} \) - in fact there is a Riemann-Roch theorem for abelian varieties (see Mumford) which says that \( \text{deg} \phi \mathcal{L} = \chi(\mathcal{L})^2 \).

By the cubical structure theorem for \( n \phi + \psi, \phi, \psi \in A(A), \mathcal{L}_{(n)} = (n \phi + \psi)^* \mathcal{L} \) satisfies

\[ \mathcal{L}_{(n+2)} = \mathcal{L}_{(n+1)}^2 \otimes \mathcal{L}_{(n)}^{-1} \otimes \underbrace{(2 \phi)^* \mathcal{L} \otimes \phi^* \mathcal{L}^{-2}}_{\text{fixed part}}. \]

By up/down induction,

\[ \mathcal{L}_{(n)} = N_{1}^{n(n-1)/2} \otimes N_{2}^n \otimes N_{3} \]

where \( N_{2} = \mathcal{L}_{(1)} \otimes \mathcal{L}_{(2)}, N_{1} = \mathcal{L}_{(2)}^{-1} \otimes \mathcal{L}_{(1)}^{-1} \).

Now, it's a general fact called the Snapper Theorem that on any projective scheme,

\[ \chi(\mathcal{L}_{1}^{n_1} \otimes \ldots \otimes \mathcal{L}_{r}^{n_r}) \in \mathbb{Q}[n_1, \ldots, n_r]. \]

Exercise 7.6.12. Prove this by slicing.

Last time we showed that \( \text{deg}: \text{End}_k^0(A) \rightarrow \mathbb{Q} \) (where \( A \) is \( k \)-simple, needed to ensure that every non-zero endomorphism has a degree, since it's an isogeny) is non-zero away from 0, and \( \mathbb{Z} \)-valued on \( \text{End}_k(A) \), and it is a homogeneous polynomial of degree \( 2g \).

At this point, we can more or less emulate the proof for elliptic curves.

Claim. For \( \mathbb{Z} \)-finite \( M \subset \text{End}_k(A) \), \( \mathbb{Q} M \cap \text{End}_k(A) \) is \( \mathbb{Z} \)-finite.

Granting this claim, we can conclude as follows.

1. The injectivity of \( \mathbb{Z}_\ell \otimes \text{End}_k(A) \rightarrow \text{End}_{\mathbb{Z}_\ell}(T_\ell A) \) is goes exactly as for elliptic curves: consider a hypothetical elementary of the kernel, write as a finite sum of elementary tensors, which only involves a \( \mathbb{Z} \)-finite part of this, and then argue by contradiction.

Exercise 7.6.13. Do it.
(2) By step 1, $\mathbb{Q}_\ell \otimes_{\mathbb{Q}} \text{End}_0^k(A) \hookrightarrow \text{End}_{\mathbb{Q}_\ell}(V(\ell)) \ (V(\ell) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)$ which is finite-dimensional over $\mathbb{Q}_\ell$. So $\text{End}_0^k(A)$ is finite-dimensional over $\mathbb{Q}$.

(By faithfully flat descent from the completion, we can conclude that $\text{End}_k(A) \otimes \mathbb{Z}_\ell(\ell)$ is $\mathbb{Z}_\ell(\ell)$-finite.)

(3) We can pick a $\mathbb{Z}$-finite $M \subset \text{End}_k(A)$ such that $\mathbb{Q} \otimes M = \text{End}_0^k(A)$. Then we use this $M$ in the claim, since $\mathbb{Q}M = \text{End}_0^k(A)$.

Proof of the claim: look at the real vector space $V = \mathbb{R} \otimes_{\mathbb{Q}} \mathbb{Q}M = \mathbb{R} \otimes_{\mathbb{Z}} M$. (At this moment, we only know that $\text{End}_0^k(A)$ is a torsion-free abelian group of finite rank.) Since this a finite-dimensional $\mathbb{R}$-vector space, polynomial functions on $\text{End}_0^k(A)$ extend uniquely to polynomial functions on $V$ by density. If we look at $\mathbb{Q}M \text{End}_k(A) \hookrightarrow V \xrightarrow{\deg} \mathbb{R}$ meets $\{\{\deg < 1\}\}$ (an open set around 0) in $\{0\}$. Therefore, the additive subgroup $\text{End}_k(A) \cap \mathbb{Q}M$ is discrete, hence $\mathbb{Z}$-finite.

♠♠♠ TONY: [reorganize the proof with injectivity first, and then prove directly the case we care about?]

□
8. The Weil Pairing

There are two more general topics:

1. **Weil pairings** \((-,-)_{A,n} : A[n] \times \hat{A}[n] \to \mu_n\) for \(n \neq 0\), which is bi-additive and identifies each with the Cartier dual of the other:

   \[
   \hat{A}[n] \to \text{Hom}_{\text{grp}}(A[n], \mu_n) = \text{Hom}_{\text{grp}}(A[n], \mathbb{G}_m)
   \]

2. **Polarizations**: symmetric isogenies \(\phi : A \to \hat{A}\) such that \((1, \phi)^* \mathcal{P}_A\) is ample on \(A\).
   (Over \(\overline{k}\), these are exactly \(\phi_{\text{c}}\) for ample \(\mathcal{L}\).)

Using such \(\phi\), we get

\[
(\cdot, -)_{\phi,n} : A[n] \times A[n] \xrightarrow{1 \times \phi} A[n] \times \hat{A}[n] \to \mu_n.
\]

**Remark 8.0.14.** In the elliptic curve case there is always a canonical \(\phi\), so the pairing is usually phrased at the level of \(E[n] \times E[n]\).

In fact, there is a unique polarization of degree \(n^2\),

\[
E \to E \xrightarrow{\text{canonical} / \pm} \hat{E}.
\]

The degree of a polarization is always a perfect square. In geometric terms, it has to do with \(\chi(\mathcal{L})\) being a square. In other terms, it has to do with the dimension of a symplectic space being even.

Let’s address (1): first quick review of Cartier duality (HW7).

8.1. **Cartier duality.** Suppose \(G\) is a finite locally free commutative group scheme over \(S\) (any scheme), i.e. \(\pi_* \mathcal{O}_G\) is a locally free \(\mathcal{O}_S\)-module of finite rank. Then the **Cartier dual** of \(G\) is the group scheme \(\mathbb{D}(G)\) whose functor of points takes \(T \to S\) to \(\text{Hom}_{S-\text{Grp}}(G_T, \mathbb{G}_m)\).

We emphasize that this is **not** \(\text{Hom}(G(T), \mathbb{G}_m(T))\); the latter is not well-behaved.

On the homework, you show that \(\mathbb{D}(G)\) is (represented by) another such group scheme, with structure sheaf

\[
\pi_* (\mathcal{O}_{\mathbb{D}(G)}) = \text{Hom}_{\mathcal{O}_S}(\pi_* \mathcal{O}_G, \mathcal{O}_S).
\]

**Example 8.1.1.**

\[
\mathbb{D}(\mu_n) = \text{Hom}_{S-\text{Grp}}(\mu_n, \mathbb{G}_m) = \text{Hom}_{S-\text{Grp}}(\mu_n, \mu_n) \cong (\mathbb{Z}/n\mathbb{Z})_S
\]

where the rightmost map sends \(j \mapsto (t \mapsto t^j)\).

There is an obvious pairing \(G \times_S \mathbb{D}(G) \to \mathbb{G}_m\), and this induces

\[
G \xrightarrow{\cong} \text{Hom}(\mathbb{D}(G), \mathbb{G}_m) \cong \mathbb{D}\mathbb{D}G.
\]

**Example 8.1.2.** \(\mathbb{D}(\alpha_p) = \alpha_p\). You can check this over \(\mathbb{F}_p\). Of course, this has no geometric points, which is good because over a field there are no non-zero maps from \(\alpha_p\) to \(\mathbb{G}_m\).

So what’s the canonical pairing

\[
\alpha_p \times \alpha_p \to \mathbb{G}_m^2
\]

It’s a truncated exponential [see Shatz article]. As you go to \(\alpha_p^2\) etc you have to use Artin-Hasse exponentiation, and it gets complicated quickly.
The question we want to focus on:

How are $A[n]$ and $\hat{A}[n]$ put in duality?

Of course, we will want to know also about functoriality, interplay between $m$ and $n$, etc. but let’s just focus on this for now.

Recall that $[n]_A = ([n]_A)^\vee$.

More generally, if $f : A \to B$ is an isogeny, then we want to put $\ker f$ and $\ker \hat{f}$ in duality. Special cases of interest will be $B = \hat{A}, A, \ldots$

**Theorem 8.1.3.** There is a natural duality pairing

$$\ker f \times \ker \hat{f} \to \mathbb{G}_m$$

(i.e. the associated map $\ker \hat{f} \to \mathbb{D}(\ker f)$ is an isomorphism).

**Warning** (to be addressed in HW9). How is $(-,-) : \ker \hat{f} \times \ker f \to \mathbb{G}_m$ related to $(-,-)_f$ via $f = \hat{f}$? They agree up to flip and sign.

**Proof.** We want to know if

$$(\ker \hat{f})(T) \cong \text{Hom}_{T-\text{Grp}}(\ker(f_T), \mathbb{G}_m, T)$$

naturally in $T$. By definition, the left hand side is

$$\ker(\text{Pic}^0_{B/k,e}(T) \xrightarrow{f_T} \text{Pic}^0_{A/k,e}(T)).$$

We claim that this kernel is the same if we drop the restriction to the identity component, because we will want to do some descent theory argument for which checking such issues will be a pain. Obviously replacing the target has no effect on the kernel, but we claim that the above is the same as

$$\ker(\text{Pic}_{B/k,e}(T) \xrightarrow{f_T} \text{Pic}_{A/k,e}(T)).$$

Since this is a Zariski-local statement, we can assume that $T$ is local. (The problem is topological: we want to say that if a $T$-valued point becomes trivial after pulling back, then it was in the identity component.) So without loss of generality for this purpose, we may assume that $T = \text{Spec} K$ (and we can even assume that $K$ is algebraically closed). The point is that $f^*$ is an isogeny, hence invertible up to $\mathbb{Z} - \{0\}$, and $\text{NS}(A_K)$ is torsion-free and $\text{NS}(A_K)^G \to \text{NS}(B_K)^G$ is an isomorphism (using that the effect of $[n]$ on $\text{NS}(A_K)$ is multiplication by $n^2$. So there is no kernel in Neron-Severi group.

So we see that

$$(\ker \hat{f})(T) = \left\{ (\mathcal{L}, i) \text{ on } B_T \mid f_T^\ast \mathcal{L} \cong i_{\ast} \mathcal{O}_T \right\}.$$

The initial isomorphism is ambiguous up to $\mathcal{O}(T)^\ast$, and this is normalized by the condition $i \mapsto 1$. 

72
Since the two identity sections are compatible, i.e. the diagram

\[ \begin{array}{ccc}
B_T & \xrightarrow{f_T} & \mathcal{L} \\
\downarrow & & \downarrow \\
A_T & \xrightarrow{e_T} & T
\end{array} \]

commutes, the above is actually the same as

\[(\ker f(T)) = \{ \mathcal{L} \text{ on } B_T \ | \ f_T^* \mathcal{L} \cong \mathcal{O}_{A_T} \} / \cong\]

because the ambiguity of the unit is taken care of by demanding that its pullback via \( e_T \) agrees with the original given trivialization.

So \( B = A / \ker f \). In order to study \( A \to A/G \) and \( \mathbb{D}G \) over a scheme \( T \), we want to relate the descent problem with a homomorphism \( G \to \mathbb{G}_m \).

Last time we saw that \( G = \ker f \implies f : A \to B \) is identified with \( A \to A/G \) (with \( G \) acting freely by left translation on \( A \)). We saw that \( \ker f(T) = \ker(\text{Pic}(B_T) \to \text{Pic}(A_T)) \). We want to identify this with \( \text{Hom}_{T-\text{Grp}}(G_T, \mathbb{G}_m, T) \) naturally in \( T \).

We've reduced to the following.

**Setup.** Let \( f : X \to S \) be proper and flat and finitely presented, with reduced and connected geometric fibers. (This implies that \( f^* \mathcal{O}_X \xleftarrow{\sim} \mathcal{O}_S \) universally.) Suppose that we are given \( G \to S \) a finite locally free commutative \( S \)-group with an action of \( G \) on \( X \) over \( S \) that is free, i.e. \( G(T) \) acts freely on \( S(T) \) for all \( T \), or equivalently the action map \( G \times_S X \to X \times_S X \) is a monomorphism. Suppose furthermore that there exists \( X \to Y \) a finite locally free surjection representing \( X/G \) - see HW6 - (hence the same for \( X_T \to Y_T \) for all \( T \to S \); think to \( A \to B \)).

**Proposition 8.1.4.** With the setup above, for all \( T \to S \)

\[ \ker(\text{Pic}(Y_T) \to \text{Pic}(X_T)) \cong \text{Hom}_{T-\text{Grp}}(G_T, \mathbb{G}_m, T) \]

naturally in \( T \).

**Proof.** We'll see that this is basically an exercise in descent theory. The role of \( \mathbb{G}_m \) is secretly that \( f_* \mathbb{G}_m, X = \mathbb{G}_m, S \).

“Without loss of generality,” \( T = S \). What we mean is that we're just going to do \( T = S \) for notational easy, but you have to check that what follows is compatible with base change.

“I'm waiting for the delivery. I'm getting very tense.”

Now, \( \ker(\text{Pic}(Y) \to \text{Pic}(X)) \) consists of descents of \( \mathcal{O}_X \) to a line bundle on \( Y \), up to isomorphism. It's going to save some grief that there are no non-trivial coboundaries. So
Abelian Varieties

we have

\[ X \times_Y X \xrightarrow{(g \times g)} G \times_S X \]

By descent theory, \( \ker(\text{Pic}(Y) \to \text{Pic}(X)) \) is equal to

\[ \{ p^* \mathcal{O}_X \cong p_2^* \mathcal{O}_X \text{ satisfying cocycle condition as } \mathcal{O}_{X \times X}\text{-modules}\} \]

What about coboundaries? Since we're dealing with linear maps, you can check that the 1-coboundaries are just trivial, using \( f_\ast \mathbb{G}_{m,X} = \mathbb{G}_{m,S} \). So the data above is the same as a unit on \( G \times X \) satisfying a cocycle, expressed in terms of the action. For such a unit \( u \), for any \( T \) and \( g \in G(T) \), \( u(g, -) \) is a unit on \( X_T \) by pullback:

\[ X_T \xrightarrow{(g, \text{id})} G_T \times X_T \]

pulling back \( u_T \leftarrow \ker(\text{Pic}(Y) \to \text{Pic}(X)) \). If you unravel the cocycle condition here, then you see that is exactly matches up with \( G_T \to \mathbb{G}_m(X_T) \) sending \( g \mapsto u(g) \) being a homomorphism.

\textit{Exercise 8.1.5.} Check this.

8.2. **Explicit description of the Weil pairing.** We would like a more explicit description \((\ker f) \times (\ker \hat{f}) \to \mathbb{G}_m \) for an isogeny \( f : A \to B \), because we want to know compatibility, etc. for how these fit together in an abelian variety (e.g. formation of the Tate module). Choose \( \hat{b} \in \ker \hat{f}(T) \) and \( a \in \ker f(T) \). We want to describe \( \langle a, \hat{b} \rangle \in \mathbb{G}_m(T) \). Well, \( \hat{b} \) corresponds to a line bundle \( \mathcal{L} \) on \( B_T \) such that \( f_T^\ast \varphi : \mathcal{L} \cong \mathcal{O}_{A_T} \) with trivialization \( \sigma \mapsto 1 \).

There is a distinguished choice of trivialization, imposed by demanding that the trivialization pulled back via \( e_B \) agrees with this.

Since \( a \in \ker f \), translation by \( a \) is invisible to \( B \), i.e. the following diagram commutes

\[ \begin{array}{ccc}
A_T & \xrightarrow{f_T} & A_T \\
\downarrow t_a & & \downarrow f_T \\
B_T & & B_T
\end{array} \]

which provides a canonical isomorphism

\[ t_a^\ast f_T^\ast \mathcal{L} \cong f_T^\ast \mathcal{L} \]

But the trivializations \( t_a^\ast(\sigma) \) and \( \sigma \) are (probably) not the same - this corresponds to the horrible \( f_T^\ast \frac{f(x - a)}{x} \) formulas you might remember from elliptic curves. So there is some unit \( \langle a, \hat{b} \rangle_F \in \mathbb{G}_m(A_T) = \mathbb{G}_m(T) \) such that \( t_a^\ast(\sigma) = \langle a, \hat{b} \rangle_f \sigma \) and you check that this is the unit furnished by our construction above.

\textit{Exercise 8.2.1.} Check it.
Remark 8.2.2. For $k = \bar{k}$ and $ch k \nmid n$, then early in §20 Ch. IV, Mumford translates the construction into the more classical language of divisors and rational functions for $f = [n]_A$. This gives reciprocal of the “Silverman formula” because $t_a^* “is”$ translation by $-a$.

Now we want to know about the functoriality of $\langle -, - \rangle_{A,n} : A[n] \times A[n] \to \mu_n$ with respect to $A$ and $n$.

To address the first point, let $h : A' \to A$ be any homomorphism. We claim that the following diagram “commutes”:

$$
\begin{array}{ccc}
A'[n] \times \hat{A}[n] & \xrightarrow{(-,-)_{A',n}} & \mu_n \\
\downarrow h & & \downarrow \hat{h} \\
A[n] \times \hat{A}[n] & \xrightarrow{(-,-)_{A,n}} & \\
\end{array}
$$

i.e. for $a' \in A'[n](T), \hat{a} \in \hat{A}[n](T)$,

$$
\langle h(a'), \hat{a} \rangle_{A,n} = \langle a', \hat{h}(\hat{a}) \rangle_{A',n} \in \mu_n(T).
$$

Let’s check this by using the explicit description. Again, for sanity’s sake we will check this only over $S$ - the interested reader can check that our calculations are valid after base-changing to any $T$, i.e. adding a subscript of $T$ everywhere. Then $\hat{a} \leftrightarrow \mathcal{L}$ on $A$ equipped with $\sigma : [n]_A^* \mathcal{L} \cong \mathcal{O}_A$, and $h^* \mathcal{L} \leftrightarrow \hat{h}(\hat{a})$ satisfies

$$
[n]_A^* (h^* \mathcal{L}) = h^*([n]_A^* \mathcal{L}) \cong \mathcal{O}_{A'}.
$$

Let’s first calculate $\langle a', \hat{h}(\hat{a}) \rangle_{A',n}$. The general formula is $t_a^* (f^* \mathcal{L}) \cong f_a^* \mathcal{L}$, so we are comparing

$$
t_a^*([n]_A^* h^* \mathcal{L}) \cong [n]_{A'}^* h^* \mathcal{L}
$$

which takes $t_a^* (h^*(\sigma)) \to \langle a', \hat{h}(\hat{a}) \rangle_{A',n} h^* \sigma$ by the explicit formula. We’re going to put this into a big commutative diagram and follow around to get the other expression. We start off with

$$
\begin{array}{ccc}
[n]_A^* h^* \mathcal{L} & \xrightarrow{t_a^*} & [n]_{A'}^* h^* \mathcal{L} \\
\downarrow & & \downarrow \\
t_a^*([n]_A^* h^* \mathcal{L}) & \xrightarrow{t_a^*} & t_a^*([n]_{A'}^* h^* \mathcal{L}) \\
\end{array}
$$
which is induced by moving multiplication by \(n\) past the homomorphism \(h\). Next we move translation past the homomorphism, using the commutativity of the diagram

\[
\begin{array}{c}
A' \\
\downarrow h \\
A
\end{array} \quad \begin{array}{c}
t_{a'} \\
\downarrow h \quad \quad t_{h(a')}
\end{array}
\]

since \(h(a' + x') = h(a') + h(x')\).

\[
[n]_{A'}^* h^* \mathbb{L} = t_{a'}^*([n]_{A'}^* h^* \mathbb{L}) = t_{h(a')}^* h^*(t_{a'}^*([n]_{A'}^* h^* \mathbb{L})) = h^*(t_{h(a')}^*([n]_{A'}^* h^* \mathbb{L}))
\]

Following the trivialization through this commutative diagram, we get

\[
\langle a', h(\hat{a}) \rangle_{A', n} h^* \sigma = t_{a'}^*(h^*(\sigma)) = \langle h(a'), \hat{a} \rangle h^* \sigma = t_{h(a')}^*(h^*(\sigma)) = h^*(t_{h(a')}^*(\sigma))
\]

What about the change in \(n\)? We want to pass to \(\text{lim}^{−\infty}_{−}\) on \(\langle −, − \rangle_{A, A'}\) to get a \(\mathbb{Z}_\ell\)-pairing

\[
T_\ell A \times T_\ell \hat{A} \to \mathbb{Z}_\ell(1).
\]

(at least for \(\ell \neq \text{ch } k\).) Now, \(\mathbb{Z}_\ell(1) = \lim_{\mu_{\ell^n}}\mu_{\ell^n}\) using

\[
\mu_{\ell^{n+1}} \xrightarrow{\ell_{\text{act}}^{-1}} \mu_{\ell^n}.
\]

For this compatibility, you need:

**Proposition 8.2.3.** For \(m, n \geq 1\), the diagram commutes:

\[
\begin{array}{c}
A[\ell^m] \times \hat{A}[\ell^m] \\
\downarrow (m, m) \\
A[\ell^n] \times \hat{A}[\ell^n]
\end{array} \quad \begin{array}{c}
\mu_{\ell^m,n} \\
\downarrow \ell^m \\
\mu_{\ell^n,n}
\end{array}
\]

**Proof.** See handout.

On HW9, you’ll show that the \(\ell\)-adic pairings of \(A\) and \(\hat{A}\) are negative via double duality.
Corollary 8.2.4. For $f: A \to A$ any homomorphism, $T_\ell(f)$ is adjoint to $T_\ell(\hat{f})$ under these perfect pairings.

Here is a disorienting special case: if $f: A \to \hat{A}$, then we get a pairing

$$e_{f,\ell}\!: T_\ell(A) \times T_\ell(A) \xrightarrow{1\times f} T_\ell A \times T_\ell \hat{A} \to \mathbb{Z}_\ell(1).$$

On HW9 you should that $f$ is symmetric if and only if $e_f$ is skew-symmetric. When we study symmetric $f$ (polarizations), we will get skew-symmetric pairings. For $f$ an isogeny, $e_{f,\ell}$ is perfect if and only if $\ell \nmid \deg f$ (because we get an isomorphism on the Tate module - no $\ell$ in the kernel).
9. THE MORDELL-WEIL THEOREM

9.1. Overview. The goal is to prove the Mordell-Weil Theorem:

Theorem 9.1.1 (Mordell-Weil). Let $K$ be a global field and $A$ an abelian variety over $K$. Then $A(K)$ is finitely generated.

The proof has three parts:

1. Cohomological step. ("weak Mordell-Weil Theorem") One first shows that $A(K)/mA(K)$ is finite for some $m \geq 2$. This is deduced from finiteness properties of "$S$-integral" Galois cohomology for $m$-torsion modules, when $\text{ch} k \nmid m$. This doesn't require any deep results, just the usual finiteness theorems for ideal class groups and unit groups. This step is done by injecting $A(K)/mA(K)$ into a finite $H^1$ group.

Remark 9.1.2. Finding actual generators for $A(K)/mA(K)$ is the challenging part, because you have to construct points.

2. Geometric step (Weil-Tate heights) There is a canonical "height pairing"

\[ \langle -,- \rangle_{A,k} : A(\bar{K}) \times \hat{A}(\bar{K}) \to \mathbb{R} \]

Moreover, for any polarization $\phi : A \to \hat{A}$ for which $(1, \phi)^\ast \mathcal{P}_A =: \mathcal{L}_\phi$ is symmetric (i.e. $\mathcal{L} \cong [-1]^\ast \mathcal{L}$), the pullback pairing

\[ \langle -,- \rangle_\phi = \langle -,- \rangle_{A,k} \circ (1 \times \phi) : A(\bar{K}) \times A(\bar{K}) \to \mathbb{R} \]

satisfies the following properties:

(1) $\langle -,- \rangle_\phi$ is symmetric and positive-semidefinite, i.e. $\langle a', a' \rangle_\phi \geq 0$ for all $a' \in A(\bar{K})$ and

(2) \{ $a \in A(K) \mid \langle a, a \rangle < C$ \} is finite for any $C > 0$.

Remark 9.1.3. It is easy to construct such $\phi$. For instance, we can take $\phi = \phi_{\mathcal{L}}$ for ample symmetric $\mathcal{L}$, such as $\mathcal{N} \otimes [-1]^\ast \mathcal{N}$ for ample $\mathcal{N}$. Then $(1, \phi)^\ast \mathcal{P}_A \cong \mathcal{L} \otimes \mathcal{L} \otimes \mathcal{L}$.

Remark 9.1.4. The existence of such a pairing already $A(K)_{\text{tors}}$ to be finite (which is not obvious!), since torsion is killed under the pairing by linearity and positive semidefiniteness. The construction will give for any finite extension $K'/K$,

\[ \langle -,- \rangle_{A,K'} = [K':K] \langle -,- \rangle_{A,K} \]

Because of this, there is a normalization convention: for number fields, people often use

\[ \frac{1}{[K:\mathbb{Q}]} \langle -,- \rangle_{A,K} \]

to attain invariance under finite extension. There is no analogue of this in the function field case, so we’ll not use it.
3. Functoriality For \( f : A \to B \) a \( K \)-homomorphism, the construction of \( \langle - , - \rangle_{A,K} \) gives:

\[
\begin{align*}
A(\overline{K}) & \times \hat{A}(\overline{K}) \\
\downarrow f & \downarrow \hat{f} \\
B(\overline{K}) & \times \hat{B}(\overline{K})
\end{align*}
\]

satisfying

\[
\langle f(a), b' \rangle_{B,K} = \langle a, \hat{f}(b') \rangle_{A,K}.
\]

This is reminiscent of the functoriality of the Weil pairing, though these pairings of course have nothing to do with Weil pairings (the latter are for torsion; this kills torsion). Moreover, there is no “symplectic” behavior: for \( a \in A(\overline{K}), a' \in \hat{A}(\overline{K}) \) and \( \iota_A : A \xrightarrow{\sim} \hat{A} \):

\[
\langle a', \iota_A(a) \rangle_{\hat{A},K} = \langle a, a' \rangle_{A,K}
\]

Remark 9.1.5. Weil’s original construction was of a quadratic form “up to bounded error.” Tate recognized that the pairing was properly viewed between \( A \) and \( \hat{A} \), and used a limiting process to produce an actual quadratic form.

9.2. Proof assuming weak Mordell-Weil plus heights. We will indicate how the full Mordell-Weil Theorem assuming the weak Mordell-Weil theorem and the height pairing.

Let \( L \) be an abelian group such that \( L/nL \) is finite for some \( n \geq 2 \) and there exists a bilinear form

\[
\langle - , - \rangle : L \times L \to \mathbb{R}
\]

such that

1. \( \langle \ell, \ell \rangle \geq 0 \) for all \( \ell \in L \) and
2. \( \{ \ell \in L | \langle \ell, \ell \rangle < C \} \) is finite for all \( C > 0 \).

We claim that in this general situation, \( L \) is finitely generated.

In practice, for computational purposes one doesn’t work with Tate’s slick bilinear form, but something coarser which is computable. The second part is easily made effective; the hard part is producing generators of \( L/nL \).

Proof. Choose representatives \( \{ \ell_1, \ldots , \ell_m \} \subset L \) representatives of \( L/nL \). Define \( ||\ell|| = \sqrt{\langle \ell, \ell \rangle} \geq 0 \). Choose \( C > \max_j ||\ell_j|| \).

The point is that if something in \( L \) has norm considerably larger than \( C \), then we can subtract off some \( \ell_j \) to make it smaller. Then we can show that the set of things in a small ball (which is finite) together with these generate \( L \).

Lemma 9.2.1. If \( ||\ell|| \geq 2C \), then \( ||\ell - \ell_j|| \leq \frac{5}{4}||\ell|| \) for all \( j \).

Proof. We have

\[
||\ell - \ell_j||^2 = \langle \ell - \ell_j, \ell - \ell_j \rangle
= \langle \ell, \ell \rangle - 2\langle \ell, \ell_j \rangle + \langle \ell_j, \ell_j \rangle
\]

79
and positive-semidefiniteness ensures that Cauchy-Schwarz is still true, so \langle \ell, \ell \rangle \leq 2|\langle \ell, \ell \rangle|.

Putting this above gives

\[
||\ell - \ell_j||^2 \leq ||\ell||^2 + ||\ell_j|| \cdot (||\ell_j|| + 2||\ell||).
\]

Since by assumption \( ||\ell|| \geq 2C \geq 2||\ell_j|| \), we have \( ||\ell_j|| \leq \frac{1}{2}||\ell|| \), so the above is

\[
||\ell - \ell_j||^2 \leq ||\ell||^2 + \frac{1}{2}||\ell||(2||\ell|| + \frac{1}{2}||\ell||)
= ||\ell||^2(1 + 5/4)
= \frac{9}{4}||\ell||^2.
\]

Taking square roots, we obtain

\[
||\ell - \ell_j|| \leq \frac{3}{2}||\ell||.
\]

□

We're going to use this as follows. We claim that \( L \) is generated by \{\ell_j\} and \( L \cap (\text{ball of radius } 2C) \), the latter being finite of course. Choose \( \ell \in L \), with \( ||\ell|| \geq 2C \). We have \( \ell \equiv \ell_j \mod nL \) for some \( j \). Then \( \ell - \ell_j = n\ell' \) for some \( \ell' \in L \) with \( n \geq 2 \). Then by the Lemma,

\[
n||\ell'|| = ||\ell - \ell_j|| \leq \frac{3}{2}||\ell||
\]

so \( ||\ell'|| \leq \frac{3}{2n}||\ell|| \). Iterating, we can keep subtracting off \( \ell_j \) until we reach something lying in the desired ball.

□

9.3. The weak Mordell-Weil Theorem. The goal of this section is to prove:

Theorem 9.3.1 (Weak Mordell-Weil Theorem). For \( n \geq 2 \) such that \( \text{ch } k \nmid n \), \( A(K)/nA(K) \) is finite.

The rough outline is to inject this group into some Galois cohomology group, which we then prove is finite. The difficulty of explicitly computing Galois cohomology is what makes it hard to make this effective.

Remark 9.3.2. \( A[n] \) is a finite commutative étale group scheme over \( k \) (which is equivalent to the data of a finite discrete Gal(\( K_s/K \))-module, by taking the \( K_s \)-points) so there exists a finite Galois extension \( K'/K \) such that \( A_{K'/k}[n] \) is "split": meaning \( A[n](K_s) = A[n](K') \). (If \( A \) is principally polarized, then there exists \( \zeta_n \in (K')^* \), obtained from pairing generators for the \( n \)-torsion.)

We will see that if the \( n \)-torsion is split over the ground field, then certain cohomological computations are simpler. Since \( A(K) \hookrightarrow A(K') \), for the purpose of proving Mordell-Weil (not Weak Mordell-Weil, since it is unclear if \( A(K)/nA(K) \hookrightarrow A(K')/nA(K') \)), we can replace \( K \) with \( K' \) without loss of generality. However, this is something we don't want to do in practice. For this reason, we'll try to carry out as much of this proof as possible over the ground field, but in the end we'll cave in and make a field extension.

We now begin the proof. We have an exact sequence of \( K \)-groups

\[ 0 \to A[n] \to A \xrightarrow{n} A \to 0 \]
where $n$ is a finite étale surjection, since $\text{ch } k \nmid n$. We claim that taking $K_s$-points gives a short exact sequence

$$0 \rightarrow A[n](K_s) \rightarrow A(K_s) \xrightarrow{n} A(K_s) \rightarrow 0. \quad (3)$$

The non-trivial point is surjectivity. For $a \in A(K_s)$,

$$\begin{array}{ccc}
E & \longrightarrow & \text{Spec } K_S \\
\downarrow & & \downarrow \\
A & \xrightarrow{n} & A
\end{array}$$

Since $E \rightarrow \text{Spec } K_s$ is a base change of a finite étale cover, it is itself a finite étale cover of a separably closed field, so it must have $K_s$-points.

The above is even a short exact sequence of discrete $\Gamma = \text{Gal}(K_s/K)$-modules, since any point shows up over a finite extension, hence is stabilized by a big a open subgroup.

Now we consider applying $H^\bullet(\Gamma, -)$ to (3):

$$\begin{array}{ccc}
0 & \longrightarrow & A[n](K) \\
& & \blacksquare \delta \longrightarrow \\
& & A(K) \xrightarrow{n} A(K) \longrightarrow H^1(K, A[n]) \longrightarrow \ldots
\end{array}$$

This gives an injection $A(K)/nA(K) \hookrightarrow H^1(K, A[n])$ (with the latter meaning $H^1(\Gamma, A[n](K_s))$ or $H^1_{\text{ét}}(\text{Spec } K, A[n])$, with $A[n]$ regarded as an étale sheaf on Spec $K$). Unfortunately, this Galois cohomology group is very large. For example, if $A[n]$ were split over $K$ then we would have $\zeta_n \in K^\times$ and $A[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g} \cong \mu_n^{2g}$. So in that case we would have

$$H^1(K, A[n]) = H^1(K, \mu_n^{2g}) = (K^\times/(K^\times)^n)^{2g},$$

which is of course enormous.

This tells us that the space $H^1(K, A[n])$ is enormous, and we need to find some conditions on the image of $A(K)/nA(K)$ that cut down the space of possibilities. So we need to somehow use the fact that $A(K)$ is the $K$-points of a proper $K$-scheme. It will turn out that $\delta(A(K)) \subset H^1(K, A[n])$ satisfies very stringent unramifiedness conditions. This has the effect of allowing us to replace $K$ by $\mathcal{O}_S$. Then finiteness then follows from the $S$-unit theorem.

Ok, so we have some smooth, proper, geometrically connected commutative group $A \rightarrow \text{Spec } K = \lim_{\longrightarrow} \mathcal{O}_{K,S}$. We would like to spread this out to some model defined over $\mathcal{O}_{K,S}$, while keeping these nice geometric properties.

There's a general principle in algebraic geometry that if you are given a “reasonable” algebro-geometric situation over a direct limit of rings (“reasonable” meaning some nice conditions on the morphisms, such as we have here) then the whole thing should spread out, i.e. be the pullback of something that has the same properties at a finite stage. In its easiest guises this is a matter of “clearing denominators” but here it’s much less obvious because we want to keep things like the group structure, geometric connectedness, flatness, etc. - it is not clear how to capture flatness in equations, for example. This is developed in generality in EGA IV$_3$ – IV$_4$ §8, §9, §11, etc.
In this case, we don’t really need the full generality. For instance, we can create a flat model by spreading out an affine subset and then taking the projective closure. This will be flat because over a Dedekind base, flatness is equivalent to the being torsion-free. However, it is worthwhile to know that this is a special case of a general phenomenon. Anyway, we get an abelian scheme $A \rightarrow \text{Spec } \mathcal{O}_{K,S} =: U$, which is a Dedekind domain.

Because $\mathcal{O}_{K,S}$ is Dedekind, the “valuative criterion over a Dedekind base” implies that we can choose $A(K) = A(U)$ (deduce it from the usual DVR version by denominator chasing).

**Exercise 9.3.3.** Do this. You can spread out any point over some open set, but why can you get all the points over a single $U$? Something to do with inverting the remaining denominators.

Without loss of generality, $n \in \mathcal{O}_{K,S}^\times$, i.e. $n \in \mathbb{G}_m(U)$.

**Remark 9.3.4.** (1) In actual computations, you would want to control $S$ very precisely. For this, you would use the theory of Néron models.

(2) Step 0 of Néron models is that $A$ is the “Néron model” of its generic fiber $A - \text{ see 1.412 in [BLR]. Such } A \text{ is uniquely functorial in } A$.

Now we claim that this $U$-group diagram is exact:

$$0 \rightarrow A[n] \rightarrow A \rightarrow 0$$

Only the surjectivity is substantial. But this can be checked on closed points, since everything is finite type over $U$, and we showed that earlier.

We claim that $[n]_{\mathcal{O}}$ is finite étale over $U$, hence $\mathcal{O}[n]$ is finite étale. To see this, recall that the “fibral criterion” says that étale is equivalent to flat and étale on geometric fibers. Since $[n]_{\mathcal{O}}$ is a map between flat schemes over $U$, it is itself flat ♠♠♠ TONY: [??? Use miracle flatness, or constancy of fibral Hilbert polynomials], and the geometric fibers are the $n$-torsion subgroups of abelian varieties, which are étale since $\text{ch } k \nmid n$. Finally, since $[n]_{\mathcal{O}}$ is proper, it is finite (proper plus quasifinite implies finite).

Recall that we say a $\Gamma$-module $M$ is unramified at $u \in \text{Spec } \mathcal{O}_K$ if the inertia subgroup $I_u$ at $u$ acts trivially on $M$.

**Corollary 9.3.5.** With the running assumptions, $A[n]$ is unramified at all closed points $u \in U$.

**Proof.** It suffices to show that if $\mathcal{G}$ is any finite étale group over a discrete valuation ring $R$, then $\mathcal{G}$ has unramified generic fiber. To prove this, we can pass to the completion $\hat{R}$, so we may assume without loss of generality that $R$ is complete.

The key tool is Hensel’s Lemma. If $\mathcal{G} = \text{Spec } B$, then by assumption $R \rightarrow B$ is finite étale. This means that we can lift solutions of equations in $B$ (mod $m_R$) to $B$ (using that $R$, hence also $B$, is $m_R$-adically complete).

We claim that if $R \rightarrow R'$ is a finite unramified extension whose residue field splits $\mathcal{G}_0$, then $\mathcal{G}_R \cong \left[ \text{Spec } R', \text{Frac}(R') \right]$ is an unramified finite extension of $K$ splitting $\mathcal{G}_K$. This is because the special fiber of $\mathcal{G}_R$ is a constant group scheme over the residue field (i.e.
a product of copies of the residue field), and by Hensel’s Lemma we can lift the idempotents splitting it to ones inducing a splitting of \( g_{R'} \), which splitting must be complete for rank reasons.

This shows that \( K(A[n]) \) lies in unramified extensions of the completions \( \overline{K}_u \) for all closed \( u \in U \), which is precisely the meaning of the lemma.

Alright, so we have \( \mathcal{O}(U)/n.A(K) \hookrightarrow H^1(K, A[n]) \), with \( A[n] \) unramified outside \( S \) and \( #A[n] \) an \( S \)-unit. We’ll use the integral structure to put some strong conditions on the image, cutting it down to something finite.

**Lemma 9.3.6.** The image of \( A(K)/n.A(K) \hookrightarrow H^1(K, A[n]) \) consists of classes unramified outside \( S \), i.e. \( \xi|_{I_u} \in H^1(I_u, A[n]) \) is trivial for all closed points \( u \in U \) (i.e. not in \( S \)).

We give two proofs: one using more machinery, which we feel better captures the “moral reason” behind the lemma, and one which is more elementary.

**First proof.** We have an exact sequence of sheaves on \( U_{et} \):

\[
0 \to \mathcal{O}[n] \to \mathcal{O} \xrightarrow{n} \mathcal{O} \to 0
\]

so passing to cohomology gives an inclusion \( \mathcal{O}(U)/n.\mathcal{O}(U) \hookrightarrow H^1_{et}(U, \mathcal{O}[n]) \). There is a restriction map \( H^1_{et}(U, \mathcal{O}[n]) \to H^1(K, A[n]) \), and the image of \( A(K)/n.A(K) \) in \( H^1(K, A[n]) \) coincides with the image of \( \mathcal{O}(U)/n.\mathcal{O}(U) \) under the composite map - this is the key point of spreading out to an integral structure!

Now, \( \mathcal{O}[n] \) restricts to an étale sheaf on \( O^{sh}_{U, u} \). The composite map \( H^1_{et}(U, \mathcal{O}[n]) \to H^1(K, A[n]) \to H^1(I_u, A[n]) \) factors through \( H^1_{et}(O^{sh}_{U, u}, \mathcal{O}[n]) \) since the inertia group at \( u \) is the étale fundamental group of the strict Henselization at \( u \), so we have the commutative diagram

\[
\begin{array}{ccc}
H^1_{et}(U, \mathcal{O}[n]) & \longrightarrow & H^1_{et}(O^{sh}_{U, u}, \mathcal{O}[n]) \\
& \downarrow & \downarrow \\
H^1(K, A[n]) & \longrightarrow & H^1(I_u, A[n])
\end{array}
\]

but \( H^1_{et}(O^{sh}_{U, u}, A[n]) = 0 \) because the spectrum of a henselian ring is cohomologically trivial. This argument highlights that the “moral” reason for the unramifiedness is that the map to inertial cohomology factors through something which is itself cohomologically trivial.

**Second proof.** For \( a \in A(K)/n.A(K) \), we can view the image \( \xi_a \) of \( a \) in \( H^1(K, A[n]) \) as an obstruction to \( n \)-divisibility. We are claiming that the restriction of this obstruction class to \( I_u \) vanishes. But that restriction is itself the obstruction class for \( a \) to be \( n \)-divisible when regarded as an element of \( A(F_u)/n.A(F_u) \), where \( F_u = K^{unr}_u = \text{Frac}(O^{sh}_{U, u}) \). Therefore it suffices to show that \( [n]: A(F_u) \to A(F_u) \) is surjective.

Let \( R = O^{sh}_{U, u} \). Then we know that \( A(F_u) = \mathcal{O}(R) \) functorially, so it suffices to show that \( [n]_\mathcal{O}: \mathcal{O}(R) \to \mathcal{O}(R) \) is surjective. Going back to the Kummer sequence, suppose
we have an $R$-point of $A$ and consider its base-change via multiplication by $n$:

$$\begin{array}{c}
\mathcal{A} \\
\downarrow \\
\mathcal{A}[n] \\
\downarrow \\
\mathcal{E} \longrightarrow \text{Spec } R
\end{array}$$

Since we know that $\mathcal{A}[n] \longrightarrow \mathcal{A}$ is finite étale cover, so is the base-change morphism $\mathcal{E} \rightarrow \text{Spec } R$. But $\text{Spec } R$ is strictly henselian, so any finite étale cover is split over $R$: the special fiber is split (as the residue field is separably closed), and then you lift idempotents. (This is an integral version of the argument we gave for surjectivity over the separable closure.) Therefore, there exists some element $a' \in \mathcal{E}(R)$ lying over $a$, which gives an $R$-point $a'$ of $A$ such that $na' = a$. □

So we’ve reduced to a general fact:

**Theorem 9.3.7.** Let $K$ be a global field, and $S$ a finite set of places of $K$ containing the archimedean places. If $M$ is a finite, discrete $\Gamma = \text{Gal}(K_s/K)$-module such that $\#M$ is an $S$-unit and $M$ is unramified outside $S$, then

$$H^1_S(K, M) := \{ \xi \in H^1(K, M) \mid \xi \text{ unramified outside } S \}$$

is finite.

**Example 9.3.8.** Taking $M = \mu_n$, and assuming that $K \supset \mu_n$, we have

$$H^1_S(K, M) \cong \mathcal{O}_K^\times / (\mathcal{O}_K^\times)^n.$$  

**Example 9.3.9.** If $p \mid M$, then we can cook up counterexamples. Let $K$ be a field of characteristic $p$. The Artin-Scheier sequence is

$$0 \rightarrow \mathbb{F}_p \rightarrow \mathbb{G}_a \xrightarrow{x \rightarrow x^p} \mathbb{G}_a \rightarrow 0.$$  

By (additive) Hilbert’s Theorem 90, $H^1(\mathbb{G}_a) = 0$. Then $H^1_S(\Gamma, \mathbb{F}_p) = K/\mathcal{O}(K)$. The unramified part outside $S$ is parametrized by $\mathcal{O}_K^\times / \mathcal{O}(\mathcal{O}_K^\times)$, which is infinite: $x^p - x = f(t)$ is unramified outside the zeros of $f$. In particular, we see that we can find a counterexample with $K = \mathbb{F}_p(t)$.

**Proof.** At this point, we will cave in and extend scalars on $K$. That will allow us to assume that the Galois module structure is trivial, and then we’ll deduce it from an $S$-unit theorem (applied to an appropriate extension). We’re going to employ a trick involving inflation-restriction. This is “ad-hoc” in the sense that it only works for $H^1$.

Let $K'/K$ be a finite Galois extension splitting $M$, i.e. such that $\Gamma' := \Gamma_{K'}$ acts trivially on $M$. Note that for the purpose of the proving the theorem, we may increase $S$, as that only “increases” the subgroup of cohomology unramified outside $S$. So we may assume that $K' \supset \mu_n$ for $n = \#M$ (or the exponent of $M$), since throwing in $n$th roots of unity introduces ramification only at the primes dividing $n$, which we may assume lie in $S$.

Let $S' \subset K'$ be the places over $S$. So we have an isomorphism as $\Gamma'$-modules

$$M \cong \prod_{d_i \in \mathcal{O}_K^\times, S'} (\mathbb{Z}/d_i \mathbb{Z}) \cong \prod \mathbb{Z}/d_i.$$

84
with the last equality following from the fact that $K'$ contains $\mu_n$. By inflation restriction, we have the exact sequence

$$0 \to H^1(K'/K, M = M') \xrightarrow{\text{Inf}} H^1(K, M) \xrightarrow{\text{Res}} H^1(K', M).$$

The group $H^1(K'/K, M = M')$, since $M$ and $\text{Gal}(K'/K)$ are both finite. Under the restriction map $H^1(K, M) \xrightarrow{\text{Res}} H^1(K', M)$, the subgroup $H^1_{\S}(K, M) \subset H^1(K, M)$ maps to $H^1_{\S}(K', M)$ since the restriction of this map to the inertia group $I_\nu$ is the corresponding restriction map on the inertial Galois cohomology. So it’s enough to show that $H^1_{\S}(K', M)$ is finite. But

$$H^1_{\S}(K', M) \cong \prod H^1_{\S}(K', \mu_{d_i})$$

so it suffices to show that each factor $H^1_{\S}(K', \mu_{d_i})$ is finite.

Renaming $K = K'$ and $S = S'$, we want to show that $H^1_{\S}(K, \mu_n)$ is finite for any $n \in \mathcal{O}_K^\times$. We have $\mu_n \subset K^\times$, so by Kummer theory we have an isomorphism

$$K^\times/(K^\times)^n \cong H^1(K, \mu_n)$$

$$[c] \mapsto \xi_c := K(\sqrt[n]{c})/K$$

The crucial question to understand here: when is $\xi_c$ going to be unramified? We claim that $\xi_c$ is unramified at $v \nmid \infty$ if and only if the extension $K(\sqrt[n]{c})/K$ is unramified at $v$.

Exercise 9.3.10. Prove it.

Now there are two approaches we could take at this point. First, we could use the Kummer sequence for $\mathcal{O}_{K,S}$ for the étale topology. However, we’re going to do something more hands-on. We can increase $S$ further so that $h_{k,S} = \text{Pic}(\mathcal{O}_{K,S}) = 1$ (adjoin elements killing a finite set of primes representing the nontrivial elements in the class group). The only way such an extension can be unramified at $v$ when $h_{k,S} = 1$ and $v \notin S$ is that is if $n \mid \text{ord}_v(c)$, again noting that $n \notin S$ (and using the unique prime factorization).

Exercise 9.3.11. Prove it.

So now we have

$$H^1_{\S}(K, \mu_n) \cong \mathcal{O}^\times_{K,S}/(\mathcal{O}^\times_{K,S})^n$$

which is finite by the $S$-unit theorem.
10. Heights

10.1. Naïve Heights. The idea of Weil’s height machine is to define some measure of “size” for points in projective space over a global field, and then to study how the height of points of an abelian variety, embedded by some very ample line bundle, interact with the group structure.

Example 10.1.1. A point \( x \in \mathbb{P}^n(\mathbb{Q}) = \mathbb{P}^n(\mathbb{Z}) \) can be represented by \( x = [x_0, \ldots, x_n] \) with \( \gcd\{x_i\} = 1 \), unique up to \( \mathbb{Z}^\times = \{\pm 1\} \). A natural attempt is to define

\[
\text{ht}(x) := \max \{\log |x_i|_\infty\}.\]

Clearly there are only many rational points with height less than some given constant.

For \( \mathbb{P}^n(\mathbb{F}_q(t)) = \mathbb{P}^n(\mathbb{F}_q[t]) \), any \( x \) can be represented by \( x = [f_0, \ldots, f_n] \) with \( f_i \in \mathbb{F}_q[t] \) and \( \gcd\{f_i\} = 1 \), unique up to \( \mathbb{F}_q[t]^\times = \mathbb{F}_q^\times \). Then we can again attempt to define

\[
\text{ht}(x) := \max \{\log ||f_i||_{\infty} := \deg(f_i) \cdot \log q\}.
\]

There are a couple of drawbacks to this definition:

1. It’s not clear how to extend this to \( \mathbb{P}^n(K) \) for a general global field \( K \),
2. It is not \( \text{PGL}_{n+1}(K) \)-invariant.

Weil’s insight was that although this height isn’t invariant under change of coordinates, it is “invariant up to bounded functions.” So the theory of heights is a theory of functions up to bounded functions.

Definition 10.1.2. Let \( \Sigma_K \) denote the set of all places of \( K \) (finite and infinite). The standard height function \( h_{K,n} : \mathbb{P}^n(K) \to \mathbb{R} \) is defined by

\[
[t_0, \ldots, t_n] \mapsto \frac{1}{[K' : K]} \sum_{v' \in \Sigma_{K'}} \max_i \{\log ||t_i||_{v'}\}
\]

where \( K' \supseteq K(t_0, \ldots, t_n) \) is some finite extension of \( K \) and \( ||t||_{v'} \) is the normalized absolute value on \( K_{v'} \) (i.e. \( ||\pi_{v'}||_{v'} = q_{v'}^{-1} \)).

For this to be well-defined, we should check a couple of properties:

1. given \( K' \), it is unaffected by \( (K')^\times \) scaling, and
2. it is independent of \( K' \).

For (1), suppose we make change of variables \( t_i \mapsto ct_i \) for some \( c \in (K')^\times \). Then the formula changes by adding

\[
\frac{1}{[K' : K]} \sum_{v' \in \Sigma_{K'}} \log ||c||_{v'} = 0 \text{ by the product formula.}
\]

This shows that without loss of generality, we may assume that \( t_i = 1 \), so each max is non-negative, and hence \( h_{K,n} \geq 0 \).

Next, let’s check invariance under change of field. This is just a matter of understanding how the normalized absolute value changes under field extension. Suppose \( K''/K' \)}
is a finite extension, so for \( t_i \in K' \) (not all 0):

\[
\frac{1}{[K'' : K']} \sum_{\nu''} \max_i \log ||t_i||_{\nu''} = \frac{1}{[K' : K]} \sum_{\nu'} \left( \frac{1}{[K'' : K']} \sum_{\nu''|\nu'} \max_i \log ||t_i||_{\nu''} \right)
\]

Now, the point of the normalized absolute value is that \( ||t_i||_{\nu''} = ||t_i||_{\nu''|\nu''} \). This is obviously true for an unramified extension, and for a totally ramified extension the residue field size doesn’t change, but the uniformizer does, so it’s true in that case too. So the above is equal to

\[
= \frac{1}{[K' : K]} \sum_{\nu'} \left( \frac{1}{[K'' : K']} \sum_{\nu''|\nu'} \max_i \log ||t_i||_{\nu''} \right) \frac{1}{[K'' : K']} \sum_{\nu''|\nu'} \left[ K''_{\nu''} : K'_{\nu'} \right]
\]

\[
= \frac{1}{[K' : K]} \sum_{\nu'} \max_i \log ||t_i||_{\nu'} \frac{1}{[K'' : K']} \sum_{\nu''|\nu'} \left[ K''_{\nu''} : K'_{\nu'} \right]
\]

\[
= \frac{1}{[K' : K]} \sum_{\nu'} \max_i \log ||t_i||_{\nu'}
\]

**Example 10.1.3.** Let’s see how this plays out for \( K' = K = \mathbb{Q} \): if \( t = [t_i] \in \mathbb{P}^n(\mathbb{Q}) = \mathbb{P}^n(\mathbb{Z}) \) with \( t_i \in \mathbb{Z} \) with \( \gcd\{t_i\} = 1 \), then for all finite \( p \) we have \( |t_i|_p \leq 1 \) but for any given \( p \) at least one \( |t_i|_p = 1 \). So actually, \( \max_i \log |t_i|_p = 0 \) for all \( p \): the non-archimedean places contribute nothing, so \( h_{K,n} \) agrees with the naïve attempt.

From the definition it is clear that \( h_{K,n} \) is \( \text{Aut}(\overline{K}/K) \)-invariant, so \( h_{K,n} \) is a well-defined function on the set of closed points of \( \mathbb{P}^n_\overline{K} \). The problem with this is that the set of closed points do not form a group (while \( A(\overline{K}) \) does).

**Remark 10.1.4.** If \( K_1/K \) is a finite extension, then you can check that

\[
h_{K,n} = [K_1 : K] h_{K,n}.
\]

This isn't important for the finiteness statements we are interested in at the moment. Over a number field, you can get rid of this by renormalizing the height function by the degree over \( \mathbb{Q} \), but as this doesn't work for function fields we'll avoid it.

**Exercise 10.1.5.** On HW10, we'll show that \( h_{K,n} \) is \( \text{PGL}_{n+1}(K) \)-invariant on \( \mathbb{P}^n(\overline{K}) \) “modulo \( O(1) \).”

The main theorem we'll prove is the following estimate.

**Theorem 10.1.6.** For any \( C > 0 \) and \( d \in \mathbb{Z}^+ \),

\[
\{ \xi \in \mathbb{P}^n(\overline{K}) \mid [K(\xi) : K] \leq d, h_{K,n}(\xi) \leq C \} \text{ is finite.}
\]
We’ll reduce this to the case of rational points over $\mathbb{Q}$ or $\mathbb{F}_q(t)$ by some norm argument, at the cost of a large constant factor. What’s actually going on is Weil restriction: a point over a quadratic field is a rational point on the Weil restriction.

**Example 10.1.7.** The preservation of projectivity under Weil restriction is non-trivial. Try doing it for $\mathbb{P}^1$ over a primitive field extension!

**Remark 10.1.8.** We’ll typically apply this to some fixed $K$, but the statement seems stronger— it is a statement for all $K$. (Though the proof shows that only finitely many number fields can actually show up.)

**Proof.** We’ll eventually reduce to the (easy!) case $K = \mathbb{Q}$ or $\mathbb{F}_p(t)$ and $d = 1$, at the cost of increasing $n, C$ in an controlled way.

The first order of business is a minor technical point: we want to reduce to considering only $x$ with $K(x)/K$ separable. In general, the inseparable degree is $p^r = [K(x): K]_i \leq d$, so there are only finitely many possibilities for $r$. For each such $r$, we consider $x' = \text{Frob}^r x = [x_0^{p^r}, \ldots, x_n^{p^r}] \in \mathbb{P}^n(\overline{K})$.

Without loss of generality we may assume that $x_j \in K(x)$, by scaling one of the coordinates to be 1. Then $K(x)/K'$ is separable of degree at most $d$, and $x'$ determines $x$ (i.e. the association $x \mapsto x'$ is injective), and by the definition

$$h_{K,n}(x) = p^r h_{K,n}(x) \leq p^r C \leq d C$$

because the exponentiation is sucked out as a constant factor by the logarithms in the definition of $h_{K,n}$. So the bound in general is at most that for separable $K$ multiplied by $C$.

This shows that for the purpose of proving the theorem, we may now assume that $K(x)/K$ is separable. Choose a presentation of $K$ as a finite (separable) extension of $\mathbb{F}$ of degree $\delta$ where $\mathbb{F} = \mathbb{Q}$ or $\mathbb{F}_p(t)$. (This is possible by the theory of transcendence bases— a finite totally inseparable extension of $\mathbb{F}_q(t)$ is abstractly isomorphic to $\mathbb{F}_q(t)$.) So we have a diagram

$$\begin{array}{ccc}
K & \xrightarrow{d} & K(x) \\
\delta \downarrow & & \downarrow \\
\mathbb{F} & \to & \mathbb{F}(x).
\end{array}$$

Then $K(x)/\mathbb{F}$ is separable of degree at most $\delta \cdot d$, and we have $\overline{K} = \overline{\mathbb{F}}$, so $h_{\mathbb{F},n} = [K : \mathbb{F}]^{-1} h_{K,n}$. This reduces us to proving the result over $K = \mathbb{F}$, at the cost of increasing the bound by a uniform constant.

Without loss of generality, it suffices to study the case $[K(x) : K] = d$ since we only have to add up the finitely many contributions from the finitely many possibilities $d$. Let $x = [x_0, \ldots, x_n] \in \mathbb{P}^n(\overline{K})$ with $x_j \in K(x)$. Then consider the ring-theoretic norm

$$K(x)[T_0, \ldots, T_n] \xrightarrow{\text{Nm}} K[T_0, \ldots, T_n].$$
This is a homogeneous polynomial of degree \( d \) (in the \( x \)'s)

\[
\text{Nm}_{K(x)/K} \left( \sum x_i T_i \right) = \sum_{||I||=d} X_I(x) T_I^I.
\]

Now let’s consider the product formulation of the norm:

\[
\text{Nm}_{K(x)/K} \left( \sum x_i T_i \right) = \prod_{\sigma: K(x) \to K_s} \left( \sum \sigma(x_i) T_i \right) =: \sum X_I(x) T_I^I.
\]

If you think about what this looks like, you’ll see that \( X_I(x) \) is defined over \( K \), since every coefficient is a product over the embeddings \( \sigma \) of something.

Let \( N(n, d) = \left( \frac{n + d}{d} \right) - 1 \), which one less than \( \# \{ I: ||I|| = d \} \), i.e. the projective dimension of the space of polynomials in \( x_0, \ldots, x_n \) of degree \( d \). The norm map can be interpreted as giving a morphism

\[
\left\{ x \in \mathbb{P}^{n}(\bar{K}) \mid K(x)/K \text{ separable, degree } d \right\} \to \left\{ \xi \in \mathbb{P}^{N(n,d)}(K) \mid h_{K,N}(\xi) \leq ??? \right\}
\]

sending \( x \to (X_I(x)) \). The key point is that the size of the fibers is at most \( d \) (actually, it’s exactly \( d \)). Indeed, \( \sum_{||I||=d} X_I(x) T_I^I \) determines the product of the linear factors involved in the norm, up to scaling factors. But that is in fact rigidified by normalizing the product, because it tells you the coefficient of each \( T_i^d \), which is \( \text{Nm}(x_i) \). Then the only ambiguity is in the “order” of the linear factors.

[Question: is there an interpretation of this in terms of Weil restriction?]

So it only remains to investigate the structure of \( X \) in terms of \( x \). Specifically, it suffices to bound \( h_{K,n}(X(x)) \) in terms of \( h_{K,n}(x) \). First we’ll study the non-archimedean case. Recall that the height was defined in terms of a sum of logarithms at places of an extension over which the point becomes rational. Let \( E(x) \) be the Galois closure of \( K(x) \) over \( K \). TONY: [some confusion about if this is necessary], which has degree at most \( d! \) over \( K \). We compare the terms contributing to the naïve height from \( v \in \Sigma_K \) and \( v' \in \Sigma_{E(x)} \) lying over it.

\[
\log ||X_I(x)||_v = \log ||X_I(x)||_{E(x)/K_v}^{1/[E(x):K_v]}
\]

(non-archimedean inequality) \( \implies \leq \max_i \log ||x_i||_v ||E(x):K_v||^{1/[E(x):K_v]} \leq d! \max_i \log ||x_i||_v.
\]

Summing this inequality over \( v \in \Sigma_K \) we find that

\[
h_{K,n}(X(x)) \leq d! \cdot h_{K,n}(x).
\]

For archimedean \( v \), you can’t use the non-archimedean inequality so you amplify by some function \( \mu(n, d) \) of \( n \) and \( d \). TONY: \([n+1]^{d!} \text{ should be enough}\] This completes the reduction to considering only \( K \), which should be enough.
10.2. **Intrinsic theory of heights.** This is bad for intrinsic theory. What we would like is, given an abelian variety over a global field and an ample line bundle, to attach a *coordinate-independent* height function. The coordinate-free version is a theory of "functions up to bounded functions." On HW10, you’ll show directly that $h_{K,n}$ is "$\text{PGL}_{n+1}(\overline{K})$-invariant mod $O(1)$.

For later purposes, we need more:

**Theorem 10.2.1.** Let $X$ be a proper $K$-scheme and $\mathcal{L}$ is a line bundle on $X$. If $X \xrightarrow{f} \mathbb{P}^n$ and $X \xrightarrow{g} \mathbb{P}^m$ are maps such that $f^*\mathcal{O}(1) \cong \mathcal{L} \cong g^*(\mathcal{O}(1))$, then

$$h_f = h_{K,n} \circ f : X(\overline{K}) \to \mathbb{R}$$

and

$$h_g = h_{K,m} \circ g : X(\overline{K}) \to \mathbb{R}$$

agree mod $O(1)$, i.e. $|h_f - h_g|$ is bounded on $X(\overline{K})$.

**Example 10.2.2.** If $f$ and $g$ are obtained by different choice of bases of sections of the same very ample line bundle, then this recovers the invariance under change of coordinates.

If $X = \mathbb{P}^n$, $f = \text{Id}$ and $g$ is an automorphism induced by some $\tau \in \text{PGL}_{n+1}(K)$, then this recovers the HW10 exercise. However, this example is a bit "fake" because we actually need the result in the proof.

**Example 10.2.3.** If $\mathcal{L}$ is very ample and $f : X \hookrightarrow \mathbb{P}(\Gamma(X,\mathcal{L})^*) \cong \mathbb{P}^N(\mathcal{L})$ gives the "naïve height" $h_\mathcal{L}$ on $X(\overline{K})$ (well-defined mod $O(1)$).

**Remark 10.2.4.** The theorem allows us to define "$h_\mathcal{L} : X(\overline{K}) \to \mathbb{R}$" as "functions mod $O(1)$" for any $\mathcal{L} \cong f^*\mathcal{O}(1)$.

To extend to general $\mathcal{L}$ for projective $X$, we would like to write $\mathcal{L}$ as the difference of two very ample line bundles and then subtract the heights. For this to be coherent, we need to relate $h_{\mathcal{L}_1 \otimes \mathcal{L}_2}$ and $h_{\mathcal{L}_1} + h_{\mathcal{L}_2}$ for $\mathcal{L}_1, \mathcal{L}_2$ as in the Theorem. That is basically just a matter of understanding the Segre embedding.

This more general theory of heights associated to arbitrary line bundles will allow us to study the interaction between heights and the group law, which is necessary for Mordell-Weil.

Now let us develop the theory. Let $K$ be a global field, $X$ a projective $K$-scheme, and $X \xrightarrow{f} \mathbb{P}^n_K$ a morphism, and $h_f := h_{K,n} \circ f : X(\overline{K}) \to \mathbb{R}$ the height function.

**Claim.** The height function is completely determined by the isomorphism class of $\mathcal{L} = f^*\mathcal{O}(1)$.

Once this is proved, we can speak sensibly about a well-defined "function up to bounded functions" $h_\mathcal{L} \in \{ \text{Functions } X(\overline{K}) \to \mathbb{R} \}/O(1)$, and discuss functorial properties, etc.

Notice that such $\mathcal{L}$ are generated by global sections, since $\mathcal{O}(1)$ is on $\mathbb{P}^n_K$ and we can pull back global sections along $f$. Conversely, if $\mathcal{L}$ is generated by global sections then by the universal property of $(\mathbb{P}^n_K, \mathcal{O}(1))$ there is a map $f : X \to \mathbb{P}(\Gamma(X,\mathcal{L}))$ such that $t_{\mathcal{L}} \mathcal{O}(1) \cong \mathcal{L}$.
\[ \mathcal{L}. \] From \( i_\mathcal{L} \) we can also get \( h_{i_\mathcal{L}} \). This is only determined up to a bounded function, since the map to projective space depends on a choice of basis.

A better statement of the claim in light of HW10:

**Theorem 10.2.5.** Given a projective \( K \)-scheme \( X \), a line bundle \( \mathcal{L} \) on \( X \) generated by global sections, and any \( X \xrightarrow{f} \mathbb{P}_K^n \) such that \( f^* \mathcal{O}(1) \cong \mathcal{L} \), then

\[
h_f - h_{i_\mathcal{L}}:X(\overline{K}) \to \mathbb{R} \text{ is bounded.}
\]

We will define a “canonical height” so that \( h_{i_\mathcal{L}} \) is additive in \( \mathcal{L} \). So then as any line bundle is the difference of two very ample line bundles, it suffices to define the canonical height for very ample line bundles.

**Proof.** The map \( f^*: \Gamma(\mathbb{P}^n, \mathcal{O}(1)) \to \Gamma(X, \mathcal{L}) \) might have non-zero kernel, or in equivalent geometric terms \( f(X) \) might lie in a hyperplane \( \mathbb{P}^{n-1}_K \cong H \subset \mathbb{P}^n_K \). But this is harmless, since \( h_f \) does not notice this. Thus, without loss of generality assume that \( f(X) \) is non-degenerate, i.e. it does not lie in a proper linear subspace of \( \mathbb{P}^n_K \), so that \( \Gamma(\mathbb{P}^n, \mathcal{O}(1)) \hookrightarrow \Gamma(X, \mathcal{L}) \).

**Upper bound.** We bound \( h_f \) by \( h_{i_\mathcal{L}} \) from above. Remember that again we can choose our favorite coordinates in \( \Gamma(X, \mathcal{L}) \) since that only changes \( h_{i_\mathcal{L}} \) by a bounded function, which is harmless. So let us choose coordinates \( T_0, \ldots, T_n \) for \( \Gamma(\mathbb{P}^n, \mathcal{O}(1)) \) and coordinates \( Z_0, \ldots, Z_N \) for \( \Gamma(X, \mathcal{L}) \), where \( Z_0, \ldots, Z_n \) are the pullbacks \( f^*(T_0), \ldots, f^*(T_n) \). By definition it is clear that \( h_f \leq h_{i_\mathcal{L}} \) since we are taking a maximum over more values (from \( Z_{n+1}, \ldots, Z_N \)).

**Lower bound.** Now we bound \( h_f \) by \( h_{i_\mathcal{L}} \) from below. The main point is that \( Z_0, \ldots, Z_n \in \Gamma(X, \mathcal{L}) \) have no common zero on \( X(\overline{K}) \), i.e. they generate \( (\mathcal{L}_X) \), for every \( x \in X(\overline{K}) \). That means that \( X \) is covered by the pre-images of \( D_+(Z_0), \ldots, D_+(Z_n) \).

Let \( S = K[Z_0, \ldots, Z_N]/I \subset \bigoplus_{r \geq 0} \Gamma(X, \mathcal{L}^{\otimes r}) \), the homogeneous coordinate ring for the image of \( i_\mathcal{L} : X \to \mathbb{P}_K^N \). This factorizes

\[
X \to \text{Proj } S \hookrightarrow \mathbb{P}^N.
\]

Consider \( J = (Z_0, \ldots, Z_n) \subset S \). Then \( \text{Proj}(S/J) = \text{Proj}(S) \cap \{Z_0 = \ldots = Z_n = 0\} \) as subsets of \( \mathbb{P}^n_K \), which is empty since we observed that the zero locus of \( Z_0, \ldots, Z_n \) doesn’t intersect the image of \( X \), i.e. \( \text{Proj}(S/J) = \emptyset \). By the Nullstellensatz, this is equivalent to the irrelevant ideal \( (Z_0, \ldots, Z_N) \) having nilpotent image in \( S/J \) (which is obviously equivalent to the same statement for \( Z_{n+1}, \ldots, Z_N \)). In other words, there is \( e \gg 0 \) such that \( Z_{n+1}^e, \ldots, Z_N^e \in (Z_0, \ldots, Z_n)S \).

The upshot is that for \( n+1 \leq j \leq N \),

\[
Z_j^e = \sum_{i=1}^n F_{ij} Z_j \text{ in } K[Z_0, \ldots, Z_N]/I
\]

where \( F_{ij} \in K[Z_0, \ldots, Z_n] \) is homogeneous of degree \( e-1 \). For \( x \in X(\overline{K}) \), think of the contributions one place at a time (with the non-archimedean ones first):

\[
eh_{K,\mathcal{L}} \leq (e-1)h_{K,\mathcal{L}}(x) + h_f(x) + \text{constant}
\]

91
The contribution \((e - 1)h_{K,\mathcal{L}}(x) + hf(x)\) is because the sums are replaced by a max, and each \(F_{ij}\) is also a sum. The constant is from \(\log|\text{coefficients of } F_{ij}|_v\) and \(\log n\) plus stuff from the archimedean places. This shows that
\[
h_{K,\mathcal{L}}(x) \leq hf(x) + O(1).
\]

\[\square\]

Remark 10.2.6. There is a subtlety in that this constant is supposed to be uniform for all geometric point, not just a fixed finite extension \(K' = K(x)/K\). One has to keep track of the factor \([K' : K]^{-1}\) to ensure that there really is uniform control.

Exercise 10.2.7. Do this.

Corollary 10.2.8 (Weil’s thesis). There is a unique assignment \((X, \mathcal{L}) \mapsto h_{\mathcal{L}} = h_{K,\mathcal{L}} \in \text{Fun}(X(\overline{K}), \mathbb{R})/O(1)\) satisfying:

1. \(h_{\mathcal{L} \otimes \mathcal{L}'} = h_{\mathcal{L}} + h_{\mathcal{L}'}\),
2. \((\mathbb{P}^n_K, O(1)) \mapsto h_{K,n}\), the standard height for projective space
3. (functoriality) For \(X \xrightarrow{f} X\), we have \(h_{f^*\mathcal{L}} = h_{\mathcal{L}} \circ f\).

Moreover, for \(\mathcal{L}\) generated by global sections this recovers our earlier construction.

Proof. Our construction satisfies (2) and (3) for \(\mathcal{L}\) generated by global sections. (This property is stable under (1) and (3), and satisfied by (2).) We now check (1). Given maps \(X \to \mathbb{P}^n\) and \(X \to \mathbb{P}^m\) coming from \(\mathcal{L}\) and \(\mathcal{L}'\), we can build a map for \(\mathcal{L} \otimes \mathcal{L}'\) by
\[
X \to \mathbb{P}^n \times \mathbb{P}^m \xrightarrow{\text{Segre}} \mathbb{P}^{(n+1)(m+1)-1}, [t_i], [u_j] \mapsto [t_i u_j]
\]
Then (1) follows from \(\log|ab| = \log|a| + \log|b|\).

In general, for any \(\mathcal{L}\) on \(X\) and ample \(\mathcal{N}\), both \(\mathcal{N} \otimes \mathcal{N} =: \mathcal{N}'\) are very ample for \(n \gg 0\), so \(\mathcal{L}\) can be expressed as the difference of very ample line bundles \(\mathcal{L} = \mathcal{N}_1 \otimes (\mathcal{N}_2)^{-1}\) with both \(\mathcal{N}_1\) and \(\mathcal{N}_2\) very ample.

Exercise 10.2.9. Check that we can uniquely extend our construction via \(h_{\mathcal{L}} = h_{\mathcal{N}_1} - h_{\mathcal{N}_2}\).

\[\square\]

For \(K\) a global field and \(X/K\) a projective variety, \(\mathcal{L}\) a line bundle on \(X\), we’ve discussed assigning a height function
\[
h_{\mathcal{L}} : X(\overline{K}) \to \mathbb{R}
\]
such that

1. When \(X = \mathbb{P}^n\) and \(\mathcal{L} = O(1)\), then \(h_{\mathcal{L}}\) is the standard height,
2. for \(\varphi : Y \to X\) then \(h_{\varphi^*\mathcal{L}} \sim h_{\mathcal{L}} \circ \varphi\) where \(h \sim h'\) if \(|h - h'|\) is bounded, \(\spadesuit\spadesuit\spadesuit\) TONY: [introduce this equivalence relation earlier]
3. \(h_{\mathcal{L}_1 + \mathcal{L}_2} \sim h_{\mathcal{L}_1} + h_{\mathcal{L}_2}\).

Theorem 10.2.10. (1) \(h_{\mathcal{L}}\) is bounded below on \((X - B)(\overline{K})\) where \(B\) is the base locus of \(\mathcal{L}\) (i.e. \(x \in B\) when every \(x \in \Gamma(X, \mathcal{L})\) vanishes at \(x\)).

(2) If \(\mathcal{L}\) is ample, then \(|\{x \in X(L), [L : K] \leq n \text{ and } h_{\mathcal{L}}(x) \leq B\}| < \infty\).
(3) If $\mathcal{L}$ is ample and $\mathcal{M} \in \text{Pic}_0^0 X/K$, then
\[ \lim_{x \in X(K), h_{\mathcal{L}}(x) \to \infty} \frac{h_{\mathcal{M}}(x)}{h_{\mathcal{L}}(x)} = 0. \]

The content of the third part is that $h_{\mathcal{M}+\mathcal{L}}$ and $h_{\mathcal{L}}$ are “basically the same.” (They might differ by more than a bounded amount, but at least their ratio goes to 1.)

**Proof.** (1) is in a Handout.

(2) Replacing $\mathcal{L}$ by $\mathcal{L} \otimes N$, we can reduce to the case where $\mathcal{L}$ is very ample, and then to $X = \mathbb{P}^n$ and $\mathcal{L} = \mathcal{O}(1)$. We’ve already done this (Northcott’s Theorem).

(3) For any $\mathcal{M}' \in \text{Pic}_0^0$, $\mathcal{L} - \mathcal{M}'$ is ample - this follows from the cohomological criterion. In particular, $\mathcal{L} - 1000 \mathcal{M}$ is ample. By (1), $h_{\mathcal{L} - 1000 \mathcal{M}}$ is bounded below so $h_{\mathcal{L} - 1000} \mathcal{M} \geq C$, so $h_{\mathcal{M}} \leq \frac{h_{\mathcal{L} - C}}{1000}$. Apply the same reasoning for $\mathcal{M}' - 1$, we get happy. 

**Theorem 10.2.11.** If $A$ is an abelian variety and $\mathcal{L}$ is a line bundle on $A$, then
\[ h_{\mathcal{L}}(x+y+z) - h_{\mathcal{L}}(x+y) - h_{\mathcal{L}}(x+z) - h_{\mathcal{L}}(y+z) + h_{\mathcal{L}}(x) + h_{\mathcal{L}}(y) + h_{\mathcal{L}}(z) \sim 0 \]
\[ i.e. \ h_{\mathcal{L}} \text{ is an approximately “quadratic function” on } A(K) \text{ (the second difference is almost a constant).} \]

Next time you’ll see an observation of Tate: for basically trivial reasons, there exists a unique quadratic function $h_{\mathcal{L}} \sim h_{\mathcal{L}'}$.

**Proof.** The Theorem of the Cube gives the same relation for line bundles on $A \times A \times A$. Compute the height of $x,y,z$. 

**Remark 10.2.12.** The quadratic height is something like $ax^2 + bx + c$ - it has a genuine linear term.

10.3. **Intersection theory picture.** Let $K$ be a function field. The nice properties of heights over function fields come from viewing the height as an intersection pairing. You can then set up the intersection theory in a way that works well for both number fields and function fields.

Let $K = \mathbb{F}_q(C)$ for $C$ a projective smooth curve. For $X/K$, choose a proper model $\mathcal{X} \to C$. We’ll be fuzzy on the technical conditions necessary - perhaps projective and flat. By properness, $X(K) = \mathcal{X}(C)$. The line bundle $\mathcal{L}$ on $X/K$ corresponds to some divisor $D$ on $X$, and $h_{\mathcal{L}}(x)$ is meant to be the intersection number of $x(C)$ and $D$. More intrinsically, this is deg$_C(x^*\mathcal{L})$. It’s nice to have this intrinsic formulation, rather than “difference of very ample line bundles.”

[Reference: Serre’s “Lectures on Mordell-Weil”]

Suppose $\mathcal{L} \in \mathcal{O}(D)$. We’ll define a local height $h_{D,v} : X(K) - D(K_v) \to \mathbb{R}$ (which intuitively counts intersection above $v$) such that if $D' = D + (f)$, then
\[ h_{D',v} \sim h_{D,v} + \log |f|_v \]
and then we define a global height function
\[ h_{\mathcal{L}}(x) = \sum_v h_{D,v}(x). \]
The $h_{D,v}$ measures the intersection of $x$ and $D$ above $v$. By the product formula, the global height is then well-defined.

The function $h_{D,v}$ has the following property which characterizes it up to $O(1)$: for each $x \in \text{supp}(D)$, let $\varphi$ be a local equation defining $D$. Then $h_{D,v} + \log|\varphi|$ extends to a continuous function on an open neighborhood of $x$. In other words, $h_{D,v}$ has a logarithmic singularity along $D$. This characterizes $h_{D,v}$ up to $O(1)$, because the difference extends to a continuous function on $X(\overline{K})$, which is compact and hence bounded. Moreover, if $h_{D,v}$ is a local height for $D$ then $h_{D,v} - \log|f|$ is a local height for $D + (f)$.

**Example 10.3.1.** Let $X = \mathbb{P}^n$, $D$ be the divisor at infinity $\{x_n = 0\}$. Then $h_{D,v} = \max(\log|x_0/x_n|_v, \log|x_1/x_n|_v, \ldots)$ is a local height, because it blows up logarithmically.

Since the second property is true for $\mathbb{P}^n$, it’s true for everything.

Suppose we have an effective (for simplicity) divisor $D$, $\mathcal{L} = O(D)$, and $s \in \Gamma^0(X, \mathcal{L})$. If we choose an integral model $\mathcal{X}, \mathcal{L} \to \text{Spec } \mathcal{O}_X[1/S]$; $s \in \Gamma^0(X, \mathcal{L})$ (say proper and smooth), then we get a local height for each $v \notin S$. For $x \in X(K_v)$, we get a section $x : \text{Spec } \mathcal{O}_v \to \mathcal{X}$. Then $x^*\mathcal{L}$ is a line bundle on $\mathcal{O}_v$, and $x^*s \in \Gamma(\text{Spec } \mathcal{O}_v, x^*\mathcal{L})$. Define $h_{D,v}(x)$ to be the valuation of $x^*s$ in the rank one $\mathcal{O}_v$-module $\Gamma(\text{Spec } \mathcal{O}_v, x^*\mathcal{L})$ (choosing an identification $\Gamma(\text{Spec } \mathcal{O}_v, x^*\mathcal{L}) \cong \mathcal{O}_v$). So this gives a canonical choice of local height for almost all places.

**Integral points on elliptic curves.** Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve. Let $\mathcal{L} = O(\infty)$. If $p, q \in E(\mathbb{Q})$ are integral, then we claim that $h(p - q) \geq \min(h(p), h(q)) + C$. This says that any two integral points are very far apart in the Mordell-Weil lattice. Since the height is the logarithm, this says that the coordinates grow double exponentially.

(There is a similar story for rational points on curves of genus $\geq 2$.)

**Proof.** Let $D = \infty$. Then

$$h(p - q) \geq h_{D,\infty}(p - q)$$

just by the construction of the global height. Now, $h_{D,\infty}(p - q)$ measures how close on a logarithmic scale $p - q$ is from $\infty$, so

$$h_{D,\infty}(p - q) \geq \min(h_{D,\infty}(p), h_{D,\infty}(q)) + C.$$ 

On the other hand, integrality means that $h_{D,\infty}(p) = h(p) + O(1)$, because $p$ being integral means that $p$ doesn’t intersect $\infty$ above any finite place. Putting these inequalities together, you get the result. In words, the integral points repel. \hfill \Box

10.4. **Tate’s canonical height.** Let $A/K$ be an abelian variety and $\mathcal{L}$ a line bundle on $A$. We’ve defined a height function

$$h_{\mathcal{L},K} : A(\overline{K}) \to \mathbb{R}$$

which is well-defined up to $O(1)$. Now we want to construct a canonical representative $h_{K,\mathcal{L}} \sim h_{K,\mathcal{L}} : A(\overline{K}) \to \mathbb{R}$ which is a “quadratic function.”

**Theorem 10.4.1** (Tate). Let $\Gamma$ be an abelian group and $h : \Gamma \to \mathbb{R}$ be a function satisfying

$$h(x_1 + x_2 + x_3) - h(x_1 + x_2) - h(x_3 + x_1) - h(x_2 + x_3) + h(x_1) + h(x_2) + h(x_3) \sim 0.$$ 

94
Then there exists a unique symmetric bilinear form \( b: \Gamma \times \Gamma \to \mathbb{R} \) and a linear function \( \ell: \Gamma \to \mathbb{R} \) such that

\[
h(x) \sim \frac{1}{2} b(x, x) + \ell(x).
\]

We apply this to \( \Gamma = A(K) \to \mathbb{R} \). The Theorem of the Cube easily implies that \( h_{K,L} \) satisfies the hypothesis. Interpret the function as a function on \( A(K) \times A(K) \times A(K) \). That is a height function for the abelian variety \( A^3 \) with respect a line bundle which is trivial by the Theorem of the Cube: 

\[
M = m_{123}^* \mathcal{L} \otimes m_{12}^* \mathcal{L}^{-1} \otimes m_{23}^* \mathcal{L}^{-1} \otimes m_{31}^* \mathcal{L}^{-1} \otimes \mathcal{L}^1 \otimes \mathcal{L}^1 \otimes \mathcal{L}^1 \cong \mathcal{O}_{A^3}.
\]

Thus, by the theorem we obtain \( b_{K,L}: A(K) \times A(K) \to \mathbb{R} \) and \( \ell_{K,L}: A(K) \to \mathbb{R} \) such that

\[
h_{K,L} \sim \frac{1}{2} b_{K,L} + \ell_{K,L}.
\]

**Definition 10.4.2.** We define the Tate canonical height function

\[
\hat{h}_{K,L}(x) = \frac{1}{2} b_{K,L}(x, x) + \ell_{K,L}(x).
\]

By the preceding discussion, \( \hat{h}_{K,L} - h_{K,L} = O(1) \) on \( A(K) \).

We now turn to the proof of Tate's theorem. Actually, we can generalize it.

**Definition 10.4.3.** If \( h: \Gamma \to \mathbb{R} \) is any function, then we define the “polarization” \( P_r h: \Gamma^r \to \mathbb{R} \) by

\[
P_r h(x_1, \ldots, x_r) = \frac{1}{r} \sum_{I \subseteq \{1,2,\ldots,r\}} (-1)^{r-\# I} h(x_I)
\]

where \( x_I = \sum_{i \in I} x_i \).

For \( r = 2 \), this is basically the expression that appeared in Theorem 10.4.1 except that we include the empty set with the convention that \( x_\emptyset = 0 \). This is called a polarization because it generalizes the notion of polarization of quadratic form, whereby one obtains a bilinear form.

We now discuss the reverse direction.

**Definition 10.4.4.** Let \( A: \Gamma^r \to \mathbb{R} \) be multilinear and symmetric. Then define \( \Delta_r A: \Gamma \to \mathbb{R} \) by

\[
\Delta_r A(x) = A(x, \ldots, x).
\]

This generalizes the process from bilinear forms to quadratic forms.

Reformulating the condition of linearity symmetry, \( A \) can be viewed as an element of \( \text{Hom}(S_r(\Gamma), \mathbb{R}) \), where \( S_r(\Gamma) = (\Gamma \otimes \mathbb{Z} \cdots \otimes \mathbb{Z})_{S_r} \) (the coinvariants under the symmetric group).

**Proposition 10.4.5.** The set of \( h: \Gamma \to \mathbb{R} \) such that \( P_r h = 0 \) is isomorphic to \( \bigoplus_{j=0}^{r-1} \text{Hom}(S_j \Gamma, \mathbb{R}) \):

\[
\{ h: \Gamma \to \mathbb{R} \mid P_r h = 0 \} \sim \bigoplus_{j=0}^{r-1} \text{Hom}(S_j \Gamma, \mathbb{R}).
\]
This map from right to left takes

\[(A_0, A_1, \ldots, A_{r-1}) \mapsto h(x) := A_0 + A_1(x) + A_2(x, x) + \ldots + A_{r-1}(x, \ldots, x).\]

It’s easy to see that \(P_r\) kills this function. (Check it!) Less obvious is that anything killed by \(P_r\) actually comes from this construction. We’ll prove this in a bit, but we first state a generalization of Tate’s theorem.

**Theorem 10.4.6.** The set of \(h: \Gamma \to \mathbb{R}\) such that \(P_r h \sim 0\) is isomorphic to \(\bigoplus_{j=1}^{r-1} \text{Hom}(S_j \Gamma, \mathbb{R}):\)

\[\{h: \Gamma \to \mathbb{R} \mid P_r h \sim 0\}/O(1) \sim \bigoplus_{j=1}^{r-1} \text{Hom}(S_j \Gamma, \mathbb{R}).\]

**Proof of Proposition.** This follows easily from formal properties of \(P_r\) and \(\Delta_r\).

1. If \(A \in \text{Hom}(S_r(\Gamma), \mathbb{R})\), then \(P_r \Delta_r A = A\). Also, \(P_r \Delta_r A = 0\) if \(r' > r\).

2. We want to see how far \(P_{r-1} h\) is from being linear, so we consider

\[(P_{r-1} h)(x_0 + x_1, x_2, \ldots, x_r) - (P_{r-1} h)(x_0, x_2, \ldots) - (P_{r-1} h)(x_1, x_2, \ldots).\]

Then this is exactly equal to \(P_r h(x_0, x_1, \ldots)\).

**Exercise 10.4.7.** Check these properties.

Now we prove the result. Since \(P_r h = 0\), the second property implies that \(P_{r-1} h\) is multilinear and symmetric, i.e. can be viewed in \(\text{Hom}(S_{r-1} \Gamma, \mathbb{R})\). So we consider consider \(h' = h - \Delta_{r-1} P_{r-1} h\) as a “first-order approximation.” Then

\[P_{r-1} h' = P_{r-1} h - P_{r-1}(\Delta_{r-1} P_{r-1} h) = 0\]

because \(P_{r-1} \Delta_{r-1} = \text{Id}\). Define \(A_{r-1} := P_{r-1} h\), so

\[h = \Delta_{r-1} A_{r-1} + h', \quad \text{where } P_{r-1} h' = 0.\]

The result then follows by induction. \(\square\)

**Proof of Theorem.** We prove only surjectivity (the hard part). Suppose \(P_r h \sim 0\). The idea is similar: consider \(P_{r-1} h\). Since \(P_r h\) is not exactly 0, \(P_{r-1} h\) is not exactly multilinear. But it’s “asymptotically” multilinear: the difference

\[(P_{r-1} h)(x_0 + x_1, x_2, \ldots, x_r) - (P_{r-1} h)(x_0, x_2, \ldots) - (P_{r-1} h)(x_1, x_2, \ldots) \sim 0.\]

Now Tate’s idea is to take a limiting process. Define

\[A_{r-1}(x_1, x_2, \ldots, x_{r-1}) = \lim_{N \to \infty} \frac{P_{r-1} h(2^N x_1, \ldots, 2^N x_{r-1})}{2^N(r-1)}.\]

We need to justify that this limit exists. Write \(2^N x_1 = 2^{N-1} x_1 + 2^{N-1} x_1\), so

\[|P_{r-1} h(2^N x_1, x_2, \ldots, x_{r-1}) - 2^{r-1} P_{r-1} h(2^{N-1} x_1, x_2, \ldots, x_{r-1})| \leq C.\]

Iterating this for all the coordinates, we obtain

\[|P_{r-1} h(2^N x_1, \ldots, 2^N x_{r-1}) - 2^{r-1} P_{r-1} h(2^{N-1} x_1, \ldots, 2^N x_{r-1})| \leq 2^{r-1} \cdot C.\]

Dividing by \(2^N(r-1)\), we get a bound

\[|P_{r-1} h(2^N x_1, \ldots, 2^N x_{r-1}) - 2^{r-1} P_{r-1} h(2^{N-1} x_1, \ldots, 2^{N-1} x_{r-1})| \leq \frac{2^r \cdot C}{2^N(r-1)}\]
and that shows that the limit exists (since this forms a Cauchy sequence).

This produces \( A_{r-1} \in \text{Hom}(S_{r-1} \Gamma, \mathbb{R}) \). If \( h' = h - \Delta_{r-1} A_{r-1} \), then
\[
P_{r-1} h' = P_{r-1} h - P_{r-1} \Delta_{r-1} A_{r-1} \\
= P_{r-1} h - A_{r-1} \\
\sim 0.
\]

Then we proceed by induction, reducing to the base case \( P_1 h \sim 0 \iff h \sim 0 \). But that's a tautology. \( \square \)

**Properties.** We fix the global field \( K \) and consider varying \( \mathcal{L} \).

1. (Additive) \( \tilde{h}_{\mathcal{L}} \circ \phi_{\mathcal{L}, \mathcal{L}} = \tilde{h}_{\mathcal{L}} + \tilde{h}_{\mathcal{L}} \).
2. (Functoriality) If \( f: A \to B \) is a homomorphism of abelian varieties, then \( \tilde{h}_{\mathcal{L}} \circ f = \tilde{h}_{f^{*} \mathcal{L}} \).
3. (Symmetry) If \( \mathcal{L} \) is symmetric, i.e. \( \mathcal{L} \cong [-1]^{*} \mathcal{L} \), then \( \tilde{h}_{\mathcal{L}} \) is even, so the linear part vanishes. We denote \( \tilde{h}_{\mathcal{L}}(x) = \frac{1}{2} \langle x, x \rangle_{\mathcal{L}} \). (Similarly, if it's antisymmetric then \( h_{\mathcal{L}} \) is linear, but that's less useful.)
4. (Positivity) If \( \mathcal{L} \) is ample and symmetric, then \( \tilde{h}_{\mathcal{L}}(x) \geq 0 \).
5. (Boundedness) \[
\{ x \in A(K) \mid [K(x):K] \leq d, \tilde{h}_{\mathcal{L}}(x) \leq C \}
\]
is a finite set (this follows immediately from the analogous statement for \( h_{\mathcal{L}} \)).

On a general abelian variety, there is no canonical choice of line bundle. However, there is one situation in which we do have a canonical line bundle: on \( A \times A^{\vee} \) we have the Poincaré line bundle \( \mathcal{P}_{A} \). Then we have a the canonical height function
\[
\tilde{h}_{A \times A^{\vee}, \mathcal{P}_{A}}: A(K) \times A^{\vee}(K) \to \mathbb{R}.
\]
This is the Néron-Tate bilinear pairing. Any \( \mathcal{L} \) on \( A \) gives \( \phi_{\mathcal{L}}: A \to A^{\vee} \) sending \( x \mapsto t_{x}^{*} \mathcal{L} \otimes \mathcal{L}^{-1} \). For \( x \in A(K) \),
\[
\langle x, \phi_{\mathcal{L}}(x) \rangle_{NT} = \langle x, x \rangle_{\mathcal{L}}.
\]

**Theorem 10.4.8.** If \( \mathcal{L} \) is ample and symmetric then \( x \mapsto \frac{1}{2} \langle x, x \rangle_{\mathcal{L}} =: \tilde{h}_{\mathcal{L}}(x) \) is positive-definite.

This is an important fact. While the properties are used in the proof of Mordell-Weil, the proof of this theorem uses that fact. The idea is that for any finite extension \( K'/K \), and we consider \( A(K')_{\mathbb{R}} \), then \( \tilde{h} \) is a positive-definite form on this space. We may as well rename \( K' = K \). This is a finite-dimensional \( \mathbb{R} \)-vector space with a quadratic form, having the property that the set of lattice points with bounded height, \( \{ x \in A(K) \mid \tilde{h}_{\mathcal{L}}(x) \leq C \} \) is finite. A theorem of Minkowski on quadratic forms implies that this quadratic form is positive-definite.
11. Selected Solutions

I thank Alessandro Maria Masullo for contributing solutions.

11.1. Exercises from §1.

Solution to Exercise 1.1.3 By Yoneda, this follows from the analogous group-theoretic fact, which is straightforward. For instance, if \( f \) is not trivial, then let \( g \in G \) be such that \( f(g) \neq e_H \). Then \( f(e_G g) = f(e_G) f(g) = f(g) \), so \( f(e_G) = e_H \). Other basic group-theoretic facts, such as uniqueness of the identity, follow similarly.

These properties can be checked by diagram, with some effort. We illustrate how to show that any map respecting multiplication respects inversions. By assumption, the diagram

\[
\begin{array}{ccc}
G \times G & \xrightarrow{f \times f} & H \times H \\
m & \downarrow{m} & \downarrow{m} \\
G & \xrightarrow{f} & H
\end{array}
\]

commutes. We insert the diagram defining the identity morphism for \( G \):

\[
\begin{array}{ccc}
G \times S & \xrightarrow{f \times 1} & H \times S \\
1 \times e_G & \downarrow{1 \times f(e_G)} & \downarrow{1 \times e_G} \\
G \times G & \xrightarrow{f \times f} & H \times H \\
m & \downarrow{m} & \downarrow{m} \\
G & \xrightarrow{f} & H
\end{array}
\]

This shows that \( f(e_G) \) has the defining property of \( e_H \).

Solution to Exercise 1.1.4 We study the functor of points:

\[
\begin{array}{ccc}
S' & \xrightarrow{G \times_{H} S} & S \\
& \downarrow{f} & \downarrow{} \\
G & \xrightarrow{f} & H
\end{array}
\]

for an \( S \)-scheme \( S' \), the universal property of the fibered product says that

\[
\ker f(S') = \{ \alpha \in G(S') \mid f(\alpha) = e_H \in H(S') \}
\]

\[= \ker(G(S') \to H(S')).\]

Solution to Exercise 1.1.5 The group schemes under consideration are all base changed from group schemes over \( \mathbb{Z} \), so it suffices to describe the latter. They are affine group schemes, so it suffices to describe the corresponding ring maps.
• For $G_a$, we have $R = \mathbb{Z}[t]$, with the multiplication map $R \rightarrow R \otimes R$ being $t \mapsto 1 \otimes t + t \otimes 1$, inversion being $t \mapsto -t$, and the identity being $t \mapsto 0$.

• For $GL_n$, we have $R = \mathbb{Z}[\{x_{ij}\}]_{1 \leq i,j \leq n}$ with the multiplication map being $x_{ij} \mapsto \sum_k x_{ik} \otimes x_{kj}$, inversion being defined by the corresponding entries of the inverse matrix, and the identity being $x_{ij} \mapsto \delta_{ij}$.

• For $\mu_m$, we have $R = \mathbb{Z}[t][t^m - 1]$ with the multiplication map being $t \mapsto t \otimes t$, inversion being $t \mapsto t^{-1}$, and the identity being $t \mapsto 1$.

• For a finite group $G$, we have $R = \bigoplus_{g \in G} \mathbb{Z}e_g$ with the multiplication map being $e_g \mapsto \sum_{hk=g} e_h \otimes e_k$, the inverse map being $e_g \mapsto e_g^{-1}$, and the identity map being $e_g \mapsto \delta_{eg}$.

Solution to Exercise 1.1.9 Consider the composition $G \times \text{Spec } k \rightarrow G \times G \rightarrow G$ which is the identity map. The induced maps on tangent spaces are $T_e G \rightarrow T_e G \oplus T_e G \xrightarrow{d \text{m}_{(e,e)}} T_e G$.

This shows that the map $T_e G \oplus T_e G \xrightarrow{d \text{m}_{(e,e)}} T_e G$ sends $(x,0) \mapsto x$. Similarly, it sends $(0,y) \mapsto y$. By linearity, it is the addition map $(x,y) \mapsto x + y$.

Solution to Exercise 1.2.4 If the image of $H_1(X,\mathbb{Z})$ is not a lattice, then it lies in some real hyperplane. We can assume that it is cut out by the linear functional $\text{Rep } \omega = 0$ for some non-zero $\omega \in \Omega^1(C)$. Then all the periods of $\text{Rep } \omega$ vanish, so integrating $\omega$ gives a harmonic function on $C$, which must be constant. But that implies that $\omega = 0$.

Alternate solution to Exercise 1.2.4 Here is another solution assuming the Hodge theory result $\Omega(C) \oplus \overline{\Omega}(C) \rightarrow H^1(C,\mathbb{C})$.

Suppose $\gamma \in H_1(C,\mathbb{R}) = H_1(C,\mathbb{Z}) \oplus \mathbb{R}$ has vanishing image in $\Omega^1(C)^*$. If not, then we can find $\lambda_1,\ldots,\lambda_2 \in \mathbb{R}$ and a cycle $\gamma \in H_1(C,\mathbb{Z})$ such that $\sum_i \lambda_i \int_\gamma \omega = 0$ for all $\omega \in \Omega(C)$.

Then we also have $\sum_i \lambda_i \int_\gamma \overline{\omega} = \sum_i \overline{\lambda_i} \int_\gamma \omega = 0$ for all $\omega \in \Omega(C)$.

But this contradicts the assumption that $\Omega \oplus \overline{\Omega}$ spans $H^1(C,\mathbb{C}) \cong H^1(C,\mathbb{R}) \otimes \mathbb{C}$.
**Solution to Exercise 1.2.7.** Choose a basis \((\omega_1, \ldots, \omega_g)\) of \(\Omega^1(C)\). In local on \(C\) we have \(\omega_j = f_j(z)\,dz\) where \(f_j\) is holomorphic, the map \(i_{c_0}\) is locally given by

\[
c \mapsto \left( \int_{x_0}^{c} \omega_1, \ldots, \int_{x_0}^{c} \omega_g \right)
\]

for some basepoint \(x_0\). This is evidently holomorphic, with derivative at \(c\) being \((f_1(c), \ldots, f_g(c))\) at \(c\). Since the canonical bundle is base-point free, this is non-vanishing.

By compactness of \(C\), \(i_{c_0}\) and non-vanishing of the differential, \(C\) is a local homeomorphism onto its image (so its image is smooth.) This combined with the fact that \(i_{c_0}\) is a proper map implies that it is an analytic covering map (so this image also has the structure of a Riemann surface).

We claim that \(i_{c_0}\) must have genus at least \(g\). Indeed, the vector space spanned by the holomorphic forms \(dz_1, \ldots, dz_g\) on \(J_C\) pull back isomorphically to \(\Omega^1(C)\), but factor through \(\Omega^1(i_{c_0})(C)\).

By Riemann-Hurwitz \(i_{c_0}(C)\) has genus at most \(g\), hence exactly \(g\) when combined with the previous paragraph. If \(g \geq 2\), then Riemann-Hurwitz implies that there are no non-trivial covers of a genus \(g\) Riemann surface by another genus \(g\) Riemann surface, so \(i_{c_0}\) is injective, hence an embedding.

When \(g = 1\), we can determine the degree of the covering map from its effect on \(H_1\). In fact, we claim that \(i_{c_0}\) induces an isomorphism \(H^1(C, \mathbb{Z}) \to H^1(J(C), \mathbb{Z})\) for all \(C\) of genus at least \(1\). Indeed, the image of a cycle in \(H^1(C, \mathbb{Z})\) is the cycle obtained by integrating a basis of \(\Omega^1(C)\), but by definition the homology of \(J(C)\) is generated by these periods.

Here is an easy proof of injectivity assuming the Abel-Jacobi theorem. Suppose that there exist \(c, c'\) such that

\[
\int_{c}^{c'} \omega_j \in \ker i_{c_0}.
\]

By the Abel-Jacobi theorem, \((c' - c)\) lies in the kernel of the Abel-Jacobi map hence is a principal divisor. But that implies that there is a meromorphic function of degree 1 on \(C\), which is only possible if \(g = 0\).

\(\square\)

**Solution to 1.3.3.**

1. We have \(\mathcal{O}_C = \mathbb{R}[x,y]/(x^2 + y^2 - 1)\). Base-changing to \(\mathbb{C}\), we find that

\[
\mathbb{C} \otimes_{\mathbb{R}} \mathcal{O}_C \cong \mathbb{C}[x,y]/(x^2 + y^2 - 1)
\]

\[
= \mathbb{C}[x,y]/((x + iy)(x - iy) - 1)
\]

\[
\cong \mathbb{C}[u,v]/(uv - 1)
\]

with the change of variables \(u = x + iy\), \(v = x - iy\). This suggests how to define the algebraic group structure on \(\mathcal{O}_C\) in terms of that on \(GL_1/\mathbb{C}\), which we leave as a (sub)exercise.

2. Any separable quadratic extension \(K/k\) can be written as \(K = k[x]/(x^2 = ax + \beta)\) (we need this level of generality if \(\text{ch } k = 2\)). Then we claim that there is an affine \(k\)-group, informally described as "elements of \(K\) of norm 1," which is a torus not "split"
over \( k \). Indeed, if \( a + bx \in k \) then we have
\[
\text{Nm}(a + bx) = \det \begin{pmatrix} a & b\beta \\ b & a + b\alpha \end{pmatrix} = a^2 + ab\alpha - b^2\beta.
\]
Therefore, the \( k \)-group scheme \( G \) has
\[
\mathcal{O}_G = k[a, b]/(a^2 + ab\alpha - b^2\beta - 1).
\]
Upon base-change to \( K \), we can write
\[
\mathcal{O}_G \otimes_k K = k[a, b]/((a + bx)(a + b(a - x)) - 1) \\
\cong k[u, v]/(uv - 1).
\]
We note that the last isomorphism follows from the invertibility of the change-of-basis matrix
\[
\begin{pmatrix}
1 & 1 \\
x & a - x
\end{pmatrix}
\]
since \( x \neq a - x \) by the separability hypothesis. \( \square \)

Solution to 1.5.3 We reduce the problem to Yoneda’s Lemma by showing that a natural transformation of the functors \( h_X \xrightarrow{T} h_Y \) restricted to affine \( R \)-schemes is equivalent to a natural transformation on the full category of \( R \)-schemes. It is easy to see that any extending natural transformation is unique, since every scheme admits an open cover by affine subschemes, and a map is determined by its restriction to the open cover.

In the other direction, suppose \( Z \) is any \( R \)-scheme. For a map \( Z \to X \), we want to produce a functorial map \( Z \to Y \). Choose an affine cover \( \{U_i\} \) for \( Z \). Then a map \( Z \to X \) amounts to maps \( U_i \to X \) agreeing on overlaps. Covering the intersections \( U_i \cap U_j \) by affine schemes \( V_{ijk} \), we have a coequalizer sequence
\[
0 \to \text{Hom}_R(Z, X) \to \prod_i \text{Hom}_R(U_i, X) \rightrightarrows \prod_{i,j} \text{Hom}_R(V_{ijk}, X).
\]
In particular, we have \( \{f_i: U_i \to X\} \in \text{Hom}_R(U_i, X) \) by restricting \( f \), which are closed since they come from a global morphism. Then their images under \( T \) form a closed cycle of \( \prod_i \text{Hom}_R(U_i, Y) \), which thus glue to a morphism \( Z \to Y \). It is easy to see that this is independent of the choice of cover, by the uniqueness of all the constructions. \( \square \)

Solution to 1.5.4 (1) We can choose \( f_1, \ldots, f_n \) generating \( R \) such that \( \theta_i: V_{fi} \cong R^n_{fi} \) is free. On the intersections, we have
\[
\tau_{ij}: R^n_{f_if_j} \xrightarrow{\theta_i^{-1}} V_{fi} \xrightarrow{\theta_j} R^n_{f_if_j}.
\]
Then conjugation by \( \tau_{ij} \) defines a gluing \( \text{GL}_n(R_{f_if_j}) \cong \text{GL}_n(R_{f_if_j}) \). This evidently satisfies the cocycle condition, so we can use it to glue \( \text{GL}_n(R_{fi}) \to \text{Spec} R_{fi} \), creating a group scheme \( X \) over \( R \). We claim that this represents.

For any \( R \)-algebra \( R' \), we want to identify \( X(R') \) with \( \text{Aut}(V \otimes_R R') \). A morphism \( \text{Spec} R' \to X \) over \( R \) is equivalent to the data of morphisms \( \text{Spec} R'_{fi} \to X_{fi} \) over \( R_{fi} \) agreeing on overlaps. But since \( V_{fi} \) is free, that is equivalent to automorphisms of \( V_{fi} \) with the gluing condition that the induced automorphisms agree on \( V_{fi,fj} \), i.e. the two compositions
to $\text{GL}_n(f_j, f_j)$ agree. One checks that this is precisely agrees with the gluing data given above.

(2) Let $R'$ be an $R$-algebra. We want to identify an $R$-morphism $\text{Spec } R' \to \text{Spec } S[1/\det]$ with an automorphism of $V \otimes_R R'$. Such a homomorphism is equivalent to an $R$-algebra homomorphism $S[1/\det] \to R'$, which is the same as an $R$-algebra homomorphism $S \to R'$ sending $\det$ to a unit. We first interpret the meaning of an $R$-algebra homomorphism $S \to R'$.

By the universal property of the symmetric algebra, that is equivalent to the data of an $R$-module homomorphism $\text{End}(V^*) \to R'$. Now, $\text{Hom}_R(\text{End}(V)^*, R') \cong \text{Hom}_R(V^* \otimes V, R')$.

Thus we have $\text{Hom}_{R-\text{alg}}(S, R') \cong \text{Hom}_{R'}(V_{R'}, V_{R'})$. It only remains to track that the invertibility of the image of the determinant corresponds to the invertibility of the endomorphism of $V_{R'}$. This is left to the reader. $\square$

Solution to 1.7.9. (1) Since $X$ and $Y$ are of finite type over $k$, we may pick a finite affine open cover of $Y$, and cover then cover each pre-image by finitely many affine open subsets of $X$. Then a morphism $X \to Y$ is specified by finitely many ring homomorphisms of rings, each finitely generated over $k$, which are described by finitely many coefficients. Each coefficient exists in $K$ and hence some $K_i$, so all of them exist in some $K_i$ as the system is directed. The fact that the morphisms are compatible, hence glue, can be checked after extending coefficients to $K$, so is automatic. $\square$

Solution 1.7.10. We proceed in order.

Affine. Since the property of being an affine morphism is local on the target, and base change commutes with base change, we may replace $Y$ with an affine scheme and reduce to showing: $X$ is affine if and only if $X_K$ is affine. If $X \cong \text{Spec } A$ is affine, then $X_K \cong \text{Spec } (A \otimes_k K)$ is again affine.

The converse is deeper. We use Serre’s criterion for affineness: all quasicoherent sheaves have vanishing higher cohomology.

If $\mathcal{F}$ is a quasicoherent sheaf on $X$, then we have

$$H^i(X, \mathcal{F}) \otimes_k K \cong H^i(X_K, \mathcal{F}_K).$$
Thus we see that if $X_k$ is affine then so is $X$.

**Finite.** Since the property of being a finite morphism is local on the target, and we have already established that affineness of $f$ and $f_k$ are equivalent, we are reduced to showing: if $A \to B$ is a morphism of $k$ algebras, then $B$ is finite over $A$ (as a module) if and only if $B \otimes_k K$ is finite over $A \otimes_k K$. The forward direction is obvious from the right exactness of the tensor product.

Conversely, suppose $B \otimes_k K$ is finite over $A \otimes_k K$. Pick finitely many elements of $B \otimes_k K$ generating it. These elements are defined over some finite extension $K_i/k$, so we reduce to the case where $K/k$ is finite. But then $A \otimes_k K$ is finite over $A$, so $B \otimes_k K$ is finite over $k$, hence certainly $B$ is as well.

**Quasifinite.** Recall that quasifinite is finite type plus finite fibers. We check each of these separately. Since they are local on the target, we may suppose that $Y = \text{Spec } B$ is affine.

Suppose that $f$ is finite type. Then we can cover $X$ by finitely many affines, whose ring of functions are finitely generated over $B$. Then their base changes have the same property over $B \otimes_k K$, so $f_k$ is finite type. Now suppose that $f_k$ is finite type. Then $X_k$ can be covered by finitely many affine open subsets, which we can take to be $(U_i)_K$ for affine open $U_i \cong \text{Spec } A_i \subset X$, so the morphism is quasicompact. Furthermore, $\text{Spec } A_i \otimes_k K$ is finitely generated over $B$, meaning that there is a surjective ring map

$$B[x_1, \ldots, x_n] \otimes_k K \to A_i \otimes_k K.$$ Again, this map is defined over a finite extension so we may assume that $K/k$ is finite. Then the left hand side is a finitely generated $B$-algebra, and $A_i \to A_i \otimes_k K$, so we have that $A_i$ is a finitely generated $B$-algebra.

**Closed immersion.** Since the property is local on the target, we reduce to $Y$ being affine. Since we have already established that $f$ is affine if and only if $f_k$ is, we may reduce to $X$ being affine. Then the assertion is that a ring homomorphism $B \to A$ is surjective if and only if $B \otimes_k K \to A \otimes_k K$. One direction is true by the general properties of the tensor product, and the other follows from faithful flatness of $K/k$.

**Surjective.** The diagram

$$\begin{array}{ccc}
X_K & \xrightarrow{f_k} & Y_K \\
\downarrow & & \downarrow \\
X & \xrightarrow{f} & Y
\end{array}$$

shows that $f$ is surjective if $f_k$ is. In the other direction, it is a general fact that the base change of a surjective morphism is surjective. Indeed, if $Z \to Y$, then the fiber over $p \in Z$
is the fibered product of $p$ with the fiber over its image in $Y$:

\[
\begin{array}{cccccc}
p \times_Y X & \longrightarrow & Z \times_Y X & \longrightarrow & X \\
p & \downarrow & & \downarrow f & \downarrow Y \\
p & \longrightarrow & Z & \longrightarrow & Y
\end{array}
\]

The result follows from the fact that the fibered product of two non-empty schemes over a point is non-empty (for instance, it receives a map from the fibered product of two points, and the tensor product of two field extensions of $k$ is non-zero).

**Isomorphism.** Reducing to $Y$ and $X$ affine as above, this follows immediately from faithful flatness.

**Separated.** $X \to Y$ is separated if and only if the diagonal $X \leftarrow X \times_Y X$ is a closed embedding. The base change of $\Delta$ to $K$ is the diagonal morphism for $X_K \to Y_K$, so this follows from the equivalence of closed immersions.

**Proper.** One direction is obvious as the base-change of a proper morphism is proper. For the other direction, first note that since properness is local on the base, we may assume that $Y$ is affine (in particular, separated). Then a version of Chow’s Lemma says that there exists a quasiprojective morphism $X' \to Y$ factoring through a surjection to $X$:

\[
\begin{array}{cccc}
X' & \longrightarrow & X \\
& \text{quasi-projective} & \downarrow \\
& & Y
\end{array}
\]

In fact, we can take $X'$ to be a blowup of $X$. ♠♠♠ TONY: [see http://math.columbia.edu/~de-jong/wordpress/?p=2790. Can I find a proper citation?] Now, $X \to Y$ is proper if and only if $X' \to Y$ is proper, so we have reduced to the case where $Y$ is affine and $X \to Y$ is quasiprojective, i.e. we have embeddings

\[
\begin{array}{cccc}
X^\text{open} & \longrightarrow & Z^\text{closed} & \longrightarrow \mathbb{P}^n_Y \\
& \downarrow & & \downarrow \\
& Y & \longrightarrow &
\end{array}
\]

Then we have similarly

\[
\begin{array}{cccc}
X_K^\text{open} & \longrightarrow & Z_K^\text{closed} & \longrightarrow \mathbb{P}^n_{Y_K} \\
& \downarrow & & \downarrow \\
& Y_K & \longrightarrow &
\end{array}
\]

We thus reduce to showing that if $f_K : X_K \to Y_K$ is quasiprojective (and $Y$ is affine), then $f : X \to Y$ is quasiprojective. As $X_K \to Y_K$ is proper, $X_K \hookrightarrow Z_K$ is also closed, hence an isomorphism. Therefore $X \hookrightarrow Z$ is also an isomorphism.
Flat. We want to show that for each \( x \in X \), the morphism \( \partial_{Y,f(x)} \rightarrow \partial_{X,x} \) is flat if and only if \( \partial_{Y,f(x)} \otimes_k K \rightarrow \partial_{X,x} \otimes_k K \) is flat. But that is immediate from \( K \) being faithfully flat over \( k \).

\[ \square \]

Solution to 1.7.11 Abusing notation, we denote by \( \pi \) the projection maps \( X_K \rightarrow X \) and \( Y_K \rightarrow Y \). Choose an affine open cover \( V_i \cong \text{Spec} \; B_i \) for \( Y \). Then the \((V_i)_K\) cover \( Y_K \), \( U'_i := f^{-1}((V_i)_K) \) cover \( X_K \). As \( V_i \) is stable under \( \text{Gal}(K/k) \), so is \( U'_i \). Since finitely presented flat maps are open, \( U_i := \pi(U'_i) \subset X \) is open. As the fibers are acted on transitively by \( \text{Gal}(K/k) \) and \( U'_i \) is stable by \( \text{Gal}(K/k) \), we in fact have that \( U'_i = (U_i)_K \).

The morphism \( U'_i \rightarrow (V_i)_K \) corresponds to a ring homomorphism

\[ B_i \otimes_k K \rightarrow \Gamma(U'_i, \partial_{X_K}) \cong \Gamma(U_i, \partial_X) \otimes_k K \]

(the latter isomorphism following, for instance, from the fact that we can choose a cover of \( U'_i \) coming from a cover of \( U_i \)). This homomorphism is \( \text{Gal}(K/k) \)-equivariant, so taking invariants shows that it sends \( B_i \rightarrow \Gamma(U_i, \partial_X) \). That defines morphisms \( U_i \rightarrow V_i \) for all \( i \), which agree on overlaps since they do after faithfully flat base change. That shows that \( f_K \) is the base change of some \( f : X \rightarrow Y \).

\[ \square \]

11.2. Exercises from §2.

Solution to Exercise 2.4.1 (i) We first reduce to showing that \( X_K \) is connected for all finite \( K/k \). Indeed, if \( X_K \) is disconnected, then we can choose closed points in distinct components, which will be defined over some finite extension \( K/k \) and witness the disconnectedness of \( X_K \).

But then \( X_K \rightarrow X \) is open because it is flat and finitely presented, and also closed because it is the base change of the integral map \( \text{Spec} \; K \rightarrow \text{Spec} \; k \), so if \( X_K \) is disconnected then so is \( X \).

(ii) Since \( X_{\text{red}} \) is reduced by definition, it is generically smooth (for completeness, we include a proof at the end). Let \( m : X \rightarrow X \) denote the multiplication map and \( m_x = m(x,\mathbf{-}) : X \rightarrow X \). If \( U \) is an open neighborhood of \( X \) such that \( U \rightarrow X \) is smooth, and \( \overline{x} \in X \) then as \( m_x \) is an isomorphism, the composition

\[ m_x^{-1}(U) \overset{m_x}{\rightarrow} U \rightarrow k \]

is also smooth. But the translates of \( U \) cover \( X \), and smoothness is local on the source, so \( X \rightarrow k \) is smooth.

If \( X \) is a connected group scheme, then \( X \) geometrically connected and smooth over \( k \), hence geometrically irreducible, hence irreducible. If \( g \in X \), then \( g(U \cap V) \neq \emptyset \), so \( g \) is in the image of \( m(U \times V) \). Taking \( U \) and \( V \) to be quasicompact (e.g. affine), we find that \( X \) is quasicompact. The converse is obvious.

\[ \square \]

Now we finish the loose end:
Abelian Varieties Math 249C, 2015

**Proposition 11.2.1.** Let $A/k$ be a finite type reduced $k$-algebra. Then there exists a non-empty open subset $U \subset \text{Spec } A$ such that $U \to k$ is smooth.

**Proof.** After localizing, we may assume that $A$ is an integral domain. We may also reduce to the case $k=k$, since smoothness is preserved by base change and descends over fpqc covers. Write $A=k[x_1,\ldots,x_n]/(F_1,\ldots,F_m)$ and $K=\text{Frac}(A)$.

Let $r$ be the rank of the Jacobian matrix $(\frac{\partial F_i}{\partial x_j})_{1\leq i,j \leq r}$ in $K$. After re-ordering, we may assume that $(\frac{\partial F_i}{\partial x_j})_{1\leq i,j \leq r}$ has non-zero determinant in $K$. By localizing, we may assume that the determinant is even a unit in $A$.

Now we claim that $k[x_{r+1},\ldots,x_n] \subset A$ is a polynomial ring. If this is established, then the result follows immediately from the Jacobian criterion. So we focus on proving the claim. If it is not true, then there is a non-constant polynomial $F(x_{r+1},\ldots,x_n) \in I$.

We may assume that $F$ has minimal degree among all such polynomials. Since the gradient of $F$ cannot be in the span of the $F_i$ for $i \leq r$ (as its partials with respect to the first $r$ variables vanish), its gradient must be 0. But this is only possible if $k$ has characteristic $p$ and $F(x_{r+1},\ldots,x_n) = \bar{F}(x_{r+1}^p,\ldots,x_n^p)$. By assumption, $\bar{F} \notin I$, but $\bar{F}^p = F \in I$, contradicting the hypothesis of reducedness of $A$. \qed

**Solution to Exercise 2.4.6** (i) The valuative criterion asks that for any diagram

\[
\begin{array}{ccc}
\text{Spec } K & \longrightarrow & \text{Pic} X/k \\
\downarrow & & \downarrow \\
\text{Spec } R & \longrightarrow & \text{Spec } k
\end{array}
\]

where $R$ is a discrete valuation ring and $K$ its fraction field, there exists a unique lift $\text{Spec } R \to \text{Pic} X/k$ making the diagram commute.

In terms of the functor-of-points description of $\text{Pic} X/k$, this means that we have to show: given a discrete valuation ring $R$ which is a $k$-algebra, and a line bundle $L$ on $\text{Spec } K \times X$ together with a chosen trivialization $e^*_K L \cong K$, that there exists a unique line bundle $\mathcal{L}$ on $\text{Spec } R \times X$ and a trivialization $e^*_R \mathcal{L} \cong R$ extending $e_K$. Actually, since $R$ is local we automatically know that $e^*_R \mathcal{L} \cong R$, and the only ambiguity in the trivialization is $R^\times$. Therefore, we always have $\text{Pic} X/k(R) = \text{Pic}(X_R)$ as groups.

Since $X \to k$ is smooth, $\text{Spec } R \times X \to \text{Spec } R$ is smooth. Then $X$ is regular, being smooth over a regular base, so we can invoke the bijection between line bundles and Weil divisors on a regular scheme. The line bundle $L$ corresponds to a Weil divisor $D_L$ on $X_K \subset X_R$. We let $D_{\mathcal{L}}$ be the (scheme-theoretic) closure of $D_L$ in $X_R$. In other words, we form the closure of the divisor by taking the closure of each codimension-one points. Then if $\mathcal{L}$ is the line bundle corresponding to $D_{\mathcal{L}}$, we obviously have that $\mathcal{L}$ extends $L$.  

106
(ii) The tangent space $T_0(\text{Pic}_{X/k})$ is parametrized by morphisms

$$\begin{array}{ccc}
\text{Spec } k[\epsilon]/\epsilon^2 & \longrightarrow & \text{Pic}_{X/k} \\
\downarrow & & \downarrow \\
\text{Spec } k & \longrightarrow & 0
\end{array}$$

Unwinding the definition of the Picard scheme, we see that this corresponds to first-order deformations of the trivial line bundle on $X$, i.e. line bundles on $X_{\epsilon} := X \times_k k[\epsilon]/\epsilon^2$ whose restriction to $X_0 \cong X \subset X_{\epsilon}$ is trivial.

We can describe such bundles in terms of the usual transition functions. Given an affine open cover of $X$, say $\{U_a = \text{Spec } A_a\}$, we have an affine open cover of $X_{\epsilon}$ by $\{U_{\alpha}^{\epsilon} := \text{Spec } A_{\alpha}[\epsilon]/\epsilon^2\}$. A line bundle on $X_{\epsilon}$ is then described by transition functions on $U_{\epsilon}^{\alpha\beta}$ satisfying the cocycle condition. Since we have assumed that the line bundle is trivial on $X$, we may assume that the transition functions take the form $1 + g_{\alpha\beta} \epsilon$. The cocycle condition then reads

$$(1 + g_{\alpha\beta} \epsilon)(1 + g_{\beta\gamma} \epsilon) = 1 + g_{\alpha\gamma} \epsilon.$$ 

This is equivalent to (using $\epsilon^2 = 0$)

$$g_{\alpha\beta} + g_{\beta\gamma} = g_{\alpha\gamma}.$$ 

That, of course, is the cocycle condition for $\mathcal{O}_X$. It only remains to determine the redundancy in this description. This comes from choosing different local trivializations. Any two trivializations $f_{\alpha}^{\epsilon}, f_{\alpha}'^{\epsilon}$ on $U_{\alpha}^{\epsilon}$ which lift the same trivialization on $U_{\alpha}$ differ by $1 + h_{\alpha}$ for some $h_{\alpha} \in A_{\alpha}$. Therefore, the trivial deformations are described by the cocycles of the form $(g_{\alpha\beta}) = (h_{\alpha} - h_{\beta})$, which are precisely the Čech coboundaries for $\mathcal{O}_X$.

(iii) Since smoothness descends via fpqc morphisms, we may assume that $k$ is algebraically closed. We use the following form of the infinitesimal smoothness criterion: if $A \to A_0$ is a surjection of artin local rings over $k$, then

$$\text{Pic}_{X/k}(A) \to \text{Pic}_{X/k}(A_0).$$

By our remarks in (i), this morphism may be identified with $\text{Pic}(X_A) \to \text{Pic}(X_{A_0})$. Let $m$ be the maximal ideal of $A$, so the residue field is $k$. By induction on the length of $I := \ker(A \to A_0)$ we may assume that $mI = 0$. Then tensoring the short exact sequence

$$0 \to I \to A \to A_0 \to 0$$

with $\mathcal{O}_X$ over $k$, we obtain a short exact sequence of sheaves

$$0 \to I \otimes_A \mathcal{O}_{X_A} \to \mathcal{O}_{X_A} \to A_0 \otimes_A \mathcal{O}_{X_A} \to 0$$

Note that $I \otimes_A \mathcal{O}_{X_A} \cong \mathcal{O}_{X_A}$ since $I$ kills $m$ by assumption, and $A_0 \otimes_A \mathcal{O}_{X_A} \cong A_0 \otimes_k \mathcal{O}_{X_A} \cong \mathcal{O}_{X_{A_0}}$.

Since $I$ is nilpotent, the induced morphism on unit groups is exact:

$$0 \to I \otimes_A \mathcal{O}_{X_A} \xrightarrow{\iota - 1 + s} \mathcal{O}_{X_A}^* \to (\mathcal{O}_{X_{A_0}})^* \to 0$$
Abelian Varieties

The long exact sequence in cohomology then reads

$$\cdots \rightarrow \text{Pic}(X_A) \rightarrow \text{Pic}(X_{\mathcal{A}}) \rightarrow H^2(X_A, I \otimes \mathcal{O}_{X_A}) \rightarrow \cdots$$

But since $X_A$ is a curve over $A$, $H^2(X_A, I \otimes \mathcal{O}_{X_A}) = I \otimes H^2(X_A, \mathcal{O}_{X_A})$ vanishes. 

**Solution to Exercise 2.4.7** (1)

(2) By the assumptions on $X$, the line bundle $\mathcal{L}$ corresponds to a Weil divisor $D$ on $X$. We have a short exact sequence

$$0 \rightarrow \mathcal{O}(-D) \rightarrow \mathcal{O}_X \rightarrow i_* \mathcal{O}_D \rightarrow 0$$

where if $D = \sum n_i x_i$, then $i_* \mathcal{O}_D = \prod \mathcal{O}_{x_i}$. Tensoring with $\mathcal{L}^n \cong \mathcal{O}(nD)$, we have the short exact sequence

$$0 \rightarrow \mathcal{O}((n-1)D) \rightarrow \mathcal{O}(D) \rightarrow i_* \mathcal{O}_D \rightarrow 0$$

(the last term unchanged because $\mathcal{L}$ is locally trivial). By the additivity of the Euler characteristic in short exact sequences, we have

$$\chi(\mathcal{L}^n) - \chi(\mathcal{L}^{n-1}) = \chi(i_* \mathcal{O}_D).$$

This shows that $\chi(\mathcal{L}^n)$ is linear. For $n = 0$, we see that $\chi(\mathcal{O}) = 1 - g$ essentially by the definition of $g$, giving

$$\chi(\mathcal{L}^n) = \chi(i_* \mathcal{O}_D)n + 1 - g.$$ 

It remains to show that $\chi(i_* \mathcal{O}_D) = \sum n_i [k(x_i) : k]$, but this is evident from the fact that stalks have no higher cohomology.

Since cohomology commutes with field extension, the first notion of degree is evidently invariant under ground field extension. Since this agrees with the other notion, that proves that it is also invariant under ground field extension, but that is easy to see directly: $\dim_k k(x_i) = \dim_k k(x_i) \otimes_k K$.

(3) It is obvious that the map on $\overline{k}$-points lands in the set of line bundles having degree 0. Conversely, let $\mathcal{L}$ be on a line bundle on $X$ of degree 0. Then we know that $\mathcal{L} \cong \mathcal{O}(D)$ for some Weil divisor $D$ on $X$, and we want to show that $D$ is linearly equivalent to a divisor of the form $\sum_{i=1}^g x_i - g \cdot e$, i.e. that $D + g \cdot e$ is effective. This follows as long as $\mathcal{O}(D + g \cdot e)$ is effective, which is immediate from Riemann-Roch.

(4) By (3) we know that $P_0(K)$ contains all the degree 0 line bundles on $X_K$. On the other hand, the image of $P_0(K)$ in the constant scheme $\mathbb{Z}$ must be 0, so all line bundles in $P_0(K)$ have degree 0.

**Solution to Exercise 2.4.8** Being a morphism of proper varieties over $k$, this map is automatically proper. We check that it is universally injective.

First we claim that for any $k$-algebra $R$, and any $x \in X(R)$, the canonical inclusion

$$R \hookrightarrow H^0(X_R, \mathcal{O}_{X_R}(x))$$

108
is an isomorphism. We only need to check that it is surjective, and for that it suffices to show that it is surjective on stalks. By Nakayama’s Lemma, surjectivity on stalks follows from surjectivity on fibers. If \( \kappa(p) := R_p/p \) denotes the residue field at \( p \in \text{Spec } R \), we have

\[
H^0(X_R, \mathcal{O}_{X_R}(x))_p \otimes \kappa(p) \cong H^0(X_{R(p)}, \mathcal{O}_{X_R(p)})
\]

and we now that the natural inclusion of \( \kappa(p) \) in this cohomology group is an isomorphism, e.g. by Riemann-Roch. ♠♠♠TONY: [need to cite proper base change theorem for above]

Now suppose that \( \mathcal{O}_{X_R}(x) \cong \mathcal{O}_{X_R}(x') \). Consider the inclusion

\[
\mathcal{O}_{X_R}(x) \otimes \mathcal{O}_{X_R}(x')^{-1} \hookrightarrow \mathcal{O}_{X_R}(x).
\]

This is an isomorphism away from \( x' \), so the cokernel is supported at \( x' \), and in fact its annihilator is \( \mathcal{I}_{x'} = \mathcal{O}_{x'} \). But it must be an \( \mathcal{R}^x \)-multiple of the canonical inclusion of the trivial bundle, hence is also an isomorphism away from \( x \), so its cokernel is supported at \( x \), and its annihilator is \( \mathcal{I}_{x} = \mathcal{O}(-x) \). But by the analogous reasoning, the annihilator is also \( \mathcal{I}_{x} \). Thus we have an equality \( \mathcal{I}_{x} = \mathcal{I}_{x'} \), hence \( x = x' \).

\[ \square \]

11.3. Exercises from §3.

Exercise 11.3.1. Let \( X \) be a scheme over a field \( k \), and assume that \( X(k) \) is dense in \( X \) (e.g. \( k = k_s \) with \( X \) geometrically reduced and locally of finite type). Prove that \( X(k) \) is “relatively schematically dense” in \( X \) in the following sense: for any \( k \)-scheme \( S \), if a closed subscheme \( Z \) of \( X_S \) contains all sections in \( X_S(S) = X(S) \) arising from \( X(k) \) then \( Z = X_S \).

Solution to Exercise 11.3.1 We consider the subset \( Y \subset X \) defined by

\[
Y = \{ x \in X : x \times S \subset Z \}.
\]

Since \( Z \) contains all sections base changed from rational points of \( X \), we have \( Y \supset X(k) \). If we can show that \( Y \) is a closed subset of \( X \), then we will be done by the assumption that \( X(k) \) is scheme-theoretically dense. But this is clear, since the condition that \( x \times S \subset Z \) is the condition that \( \mathcal{I}_Z \) vanishes on \( x \times S \), which is a closed condition. \[ \square \]

Exercise 11.3.2. Let \( X \rightarrow S \) be a map of schemes and \( Z \subset Z' \) a containment of \( S \)-flat closed subschemes whose associated ideal sheaves are locally finitely generated. If \( Z_s = Z'_s \) inside of \( X_s \) for all \( s \in S \) then prove that \( Z = Z' \) inside of \( X \).

Solution to Exercise 11.3.2 Replacing \( X \) by \( Z \), we have only to show that if \( Z_s = X_s \) for all \( s \in S \) then \( Z = X \). Since this question is local on the source and target, we may assume that everything is affine: say \( S = \text{Spec } A \), \( X = \text{Spec } B \) equipped with a ring homomorphism \( A \rightarrow B \), and the ideal of \( Z \) in \( X \) is \( I \).

Consider the short exact sequence

\[
0 \rightarrow I \rightarrow B/I \rightarrow 0.
\]

By hypothesis, for all primes \( p \in A \) we have that \( B \otimes A_p/p \rightarrow (B/I) \otimes A_p/p \) is an isomorphism. Tensoring with the entire short exact sequence by \( A_p/p \), we have a long exact
Since $B/I$ is flat over $A$, we have $\text{Tor}_1^A(B, A_p/p) = 0$. Combining this with the preceding observation, we find that $I \otimes A_p/p = 0$ for all $p \in A$. By Nakayama’s Lemma $I \otimes A_p = 0$ for all $p \in A$, so $I = 0$.

Solution to Exercise 3.1.3 If $\mathcal{N} \cong \phi^* \mathcal{M}$, then we show that $\phi_* \mathcal{N} \cong \mathcal{M}$. The isomorphism uses the fact that $\phi_* \mathcal{O}_X = \mathcal{O}_S$ (applied Zariski-locally on $S$) by Lemma 2.2.1 and the projection formula:

$$\phi_*(\phi^* \mathcal{M}) \cong \mathcal{M} \otimes \mathcal{O}_X \cong \mathcal{M} \otimes \phi_* \mathcal{O}_X \cong \mathcal{M} \otimes \mathcal{O}_S \cong \mathcal{M}.$$ 

So for $\mathcal{N}$ to be pullbacked back from $S$, we must have $\phi_* \mathcal{N}$ be a line bundle and $\phi^* \phi_*(\mathcal{N}) \cong \mathcal{N}$. These two conditions are obviously also sufficient.

Solution to Exercise 3.4.6 Otherwise, one could take an affine open neighborhood $W$ of a generic point of $D$ having codimension at least 2 in $A$. Then every regular function on $U \cap W$ (which is still affine thanks to the separatedness hypothesis) extends to a regular function on $W$ by “algebraic Hartog’s Theorem,” implying that $U = W$, a contradiction.

References

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, Néron models, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990. MR 1045822 (91i:14034)

