ABELIAN VARIETIES

BRIAN CONRAD
LECTURE NOTES BY TONY FENG

CONTENTS

Note to the reader 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 11
1.7. Rigidity 12
2. The Picard functor 17
2.1. Overview 17
2.2. Rigidification 17
2.3. Representability 20
2.4. Properties of $\mathrm{Pic}_{X/k}$. 22
3. Line bundles on abelian varieties 25
3.1. Some fundamental tools 25
3.2. The ϕ construction 27
3.3. The Poincaré bundle 30
3.4. Projectivity of abelian varieties 31
4. Torsion 37
4.1. Multiplication by n 37
4.2. Structure of the torsion subgroup 41
5. The dual abelian variety 46
5.1. Smoothness 46
5.2. Characterization of $\phi_{\mathscr{L}}$ 48
5.3. The Néron–Severi group 51
6. Descent 54
6.1. Motivation 54
6.2. fpqc descent 55
7. More on the dual abelian variety 62
7.1. Dual morphisms 62
7.2. Cohomology of the Poincaré bundle 63
7.3. Dual isogenies 67

7.4. Symmetric morphisms 69
7.5. Ampleness 71
7.6. Endomorphisms 72
8. The Weil Pairing 78
8.1. Cartier duality 78
8.2. Explicit description of the Weil pairing 81
9. The Mordell–Weil Theorem 85
9.1. Overview 85
9.2. Proof assuming weak Mordell–Weil plus heights 86
9.3. The weak Mordell–Weil Theorem 87
10. Heights 93
10.1. Naïve Heights 93
10.2. Intrinsic theory of heights 97
10.3. Tate's canonical height 101
References 105

NOTE TO THE READER

This document consists of lecture notes that Tony Feng "live-TEXed" from a course given by Brian Conrad at Stanford University in the Spring quarter of 2015, which both Feng and Conrad edited afterwards.

The material in §10.3 is largely distinct from Conrad's lectures, and two substitute lectures were delivered (by Akshay Venkatesh and Zhiwei Yun) when Conrad was out of town. For two lectures missed by Feng, we are grateful to Ho Chung Siu and David Sherman for providing 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:

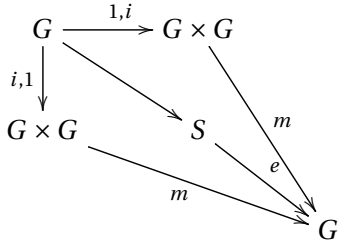
(1) (Associativity)

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

(2) (Identity)

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

(3) (Inverse)



Remark 1.1.2. By Yoneda's Lemma, it is equivalent to endow $G(S') = \mathrm{Hom}(S', G)$ 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 locally closed subscheme of G whose set of 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 (locally closed) subscheme is not entirely trivial, as sections need not be closed immersions 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 schemes, write down a representing affine scheme and the multiplication, inversion, and identity maps at the level of coordinate rings:

$$\mathbf{G}_a(S) = \Gamma(S, \mathscr{O}_S), \mathrm{GL}_n(S) = \mathrm{GL}_n(\Gamma(S, \mathscr{O}_S)), \mu_m = \ker(t^m \colon \mathrm{GL}_1 \to \mathrm{GL}_1).$$

For a finite group G, do the same for the functor of locally constant G-valued functions (called the *constant* $\mathbf{Z}$*-group* associated to G).

Definition 1.1.6. An *abelian variety* over a field k is a smooth, connected, proper k-group scheme X. In particular, there are morphisms $m \colon X \times X \to X$, $e \in X(k)$, $i \colon X \to X$ satisfying the usual group-axiom diagrams.

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

Remark 1.1.7. By smoothness, it suffices to check the group-scheme axioms for such given data on X on $\overline{k}$-points. This is sometimes a useful 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, and let the map $m \colon G \times G \to G$ be the multiplication morphism. Prove that the tangent map

$$dm_{(e,e)} \colon T_e(G) \oplus T_e(G) \to T_e(G)$$

is addition. This is very useful!

1.2. **Complex tori.**

Definition 1.2.1. A *complex torus* is a connected compact Lie group over $\mathbf{C}$.

These are the analytic analogues of abelian varieties over $\mathbf{C}$.

Example 1.2.2. If $V \simeq \mathbf{C}^g$ and $\Lambda \subset V$ is a lattice (a discrete, co-compact subgroup) then V/Λ is a complex torus.

Example 1.2.3. Let C be a connected compact Riemann surface. Then $C \simeq X^{\mathrm{an}}$, where X is a smooth proper connected curve over $\mathbf{C}$ (i.e. "comes from" algebraic geometry). We now construct a natural complex torus from C, studied by Abel and Jacobi long before the advent of the algebraic theory of abelian varieties (and in fact a big impetus for its development by Weil and others).

The space $\Omega^1(C)$ of holomorphic 1-forms on C is a g-dimensional $\mathbf{C}$=vector space. We have $H_1(C, \mathbf{Z}) \simeq \mathbf{Z}^{2g}$, and there is a natural map $H_1(C, \mathbf{Z}) \to \Omega^1(C)^*$ via integration along cycles. Here is a crucial property:

Exercise 1.2.4. Show that the image of $H_1(C, \mathbf{Z})$ in $\Omega^1(C)^*$ is a lattice. One approach is to use the fact from Hodge theory that the natural $\mathbf{C}$-linear map $\Omega^1(C) \oplus \overline{\Omega}^1(C) \to H^1(C, \mathbf{C})$ is an isomorphism. (There are proofs which do not use Hodge theory.)

If we pick bases $\{w_j\}$ for $\Omega^1(\mathbf{C})^*$ and $\{\sigma_i\}$ for $H_1(C, \mathbf{Z})$, 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 $J_C = \Omega^1(C)^*/H_1(C,\mathbf{Z})$, 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 $f_*: H_1(C',\mathbf{Z}) \to H_1(C,\mathbf{Z})$. One can check that the diagram

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

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 $\iota_{c_0}: C \to J_C$ defined by $c \mapsto \int_{c_0}^{c} \pmod{H_1(C,\mathbf{Z})}$. The integral depends on the choice of path, and integrating a holomorphic differential 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 $H_1(i_{c_0},\mathbf{Z})$ 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 $\mathbf{C}$, and then over general fields.

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

Theorem 1.2.8. *Every complex torus A is commutative (contrast with connected compact Lie groups over $\mathbf{R}$!) and the holomorphic exponential map $\exp_A: T_0(A) \to A$ is a surjective homomorphism with kernel $\Lambda_A \subset T_0(A)$ a lattice. Hence $A \simeq T_0(A)/\Lambda_A$.*

Proof. See pp. 1-2 of [Mum]. The key is to study the adjoint representation of A acting on $T_0(A)$. This map $a \mapsto \mathrm{d}c_a(e)$ (with $c_a(x) = axa^{-1}$) is a holomorphic map $A \to \mathrm{GL}(T_0(A))$ from a connected compact complex manifold into an open submanifold of a Euclidean space, so it must be constant (by the maximum principle in several complex variables). □

Next time we'll adapt this idea to prove that abelian varieties are commutative. In characteristic p, for example, the tangent space is not as useful an invariant as in the analytic theory of Lie groups, so one has to look at higher-order data. But even in these algebraic cases, the theory is guided by the analytic analogy.

1.3. **Link between complex abelian varieties and complex tori.** Here is an important fact (proved by Serre under projectivity hypotheses, from which the general case was deduced by Grothendieck using Chow's Lemma):

Theorem 1.3.1 (GAGA)**.** *The analytification functor $X \mapsto X^{\mathrm{an}}$ from proper $\mathbf{C}$-schemes to compact Hausdorff $\mathbf{C}$-analytic spaces is fully faithful.*

Many properties are equivalent on both sides: smoothness, connectedness, flatness, normality, etc. (Some such equivalences are not at all elementary to prove; for our purposes in this course the analytic theory is just a source of motivation.) The category of abelian varieties over **C** sits fully faithfully in the category of complex tori:

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

For $g = 1$ the two coincide, but for $g \geq 2$ the right side is much bigger. In this way, the 1-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

$$\left\{\begin{array}{c}\text{smooth proper connected}\\ \text{algebraic curves /}\mathbf{C}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{connected compact}\\ \text{Riemann surfaces}\end{array}\right\}.$$

So one might ask: can we create an *algebraic* analogue of the Jacobian variety? More precisely, given a smooth, proper, (geometrically) connected curve X over **C** with positive genus, can we build an abelian variety J_X of dimension g with $T_0(J_X) \simeq \Omega^1(X)^*$ and (for some $x_0 \in X(\mathbf{C})$) an inclusion $\iota_{x_0} : X \to J_X$ whose analytification recovers $C \xrightarrow{\iota_{C_0}} J_C$, where $C = X^{\mathrm{an}}$? Moreover, can we generalize this to arbitrary ground fields?

The answer is yes, using the Picard scheme $\mathrm{Pic}_{X/k}$, as we shall see.

Remark 1.3.2. The smoothness is crucial; if the curve X is not smooth then $\mathrm{Pic}_{X/k}$ still exists, but its identity component need not be an abelian variety; for example, it can even be affine (such as for X a nodal cubic).

Exercise 1.3.3. Let k be a field. An *algebraic torus* over k is a smooth affine k-group scheme T such that $T_{\overline{k}} \simeq \mathrm{GL}_1^n$ as $\overline{k}$-groups for some $n \geq 0$.

(i) Explain how the **R**-group $G = \{x^2 + y^2 = 1\}$ is naturally a 1-dimensional algebraic torus over **R**, with $G_{\mathbf{C}} \simeq \mathrm{GL}_1$ defined by $(x, y) \mapsto x + iy$ with x, y viewed over **C**, not **R**. Describe the inverse isomorphism. (This example explains the reason for the name "algebraic torus".)

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

1.4. **The Mordell–Weil Theorem.** Poincaré conjectured that the group rational points of any elliptic curve over **Q** is *finitely generated*. 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 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 $X(k) = J_X(k) \cap X(\mathbf{C})$ (upon fixing an embedding of k into **C**). Weil wondered if it could be true that a combination of $J_X(k)$ being "small" (in the sense of finite generatedness) and $X(\mathbf{C})$ being "small" in the g-dimensional complex torus $J_X(\mathbf{C})$ (as a complex submanifold of codimension $g - 1 > 0$) 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 a global field k 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 case of transcendence degree 0 being the Mordell conjecture).

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

(i) for the adjoint representation, the matrix entries are holomorphic functions on a connected compact complex manifold and hence constant;
(ii) use the fact that a map between connected Lie groups is *determined* by the map of Lie algebras.

The analogue of second fact is *false* for smooth connected group varieties over fields of characteristic $p > 0$. For example, the Frobenius morphism $x \mapsto x^p$ is a nonzero endomorphism of $\mathbf{G}_{\mathrm{a}}$ but induces 0 between Lie algebras (and likewise on $\mathbf{G}_{\mathrm{m}}$). Nonetheless, the commutativity property from the analytic theory holds in the algebraic case in all characteristics:

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

Proof. We want to prove that the two maps

$$\begin{array}{ccc} A \times A & \xrightarrow{m} & A \\ {\scriptstyle \mathrm{flip}}\downarrow & \nearrow_{m} & \\ A \times A & & \end{array}$$

are equal. We first digress to address some facts of general utility when extending the ground field:

Exercise 1.5.2. Prove that if X, Y are k-schemes and K/k is a field extension, then two maps $f, g : X \rightrightarrows Y$ are equal if and only if $f_K = g_K$. (This requires some thought since we certainly do not assume X and Y are affine.)

Exercise 1.5.3. 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_{red} is smooth, and deduce that if X is connected and U and V are nonempty 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

X is connected if and only if it is geometrically irreducible over k, and that such X are of finite type (i.e. quasi-compact) over k.

By the preceding Exercise, 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 will be used all the time without comment. By Exercise 1.5.2, to prove Theorem 1.5.1 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 conjugation morphism $c_a : A \to A$ defined by $x \mapsto a\,x\,a^{-1}$ is the identity map.

In the classical case, we proved this by studying the effect on the tangent space at the identity. Over general fields that's not enough, because of the failure of a map between smooth connected group varieties to be determined by its effect between Lie algebras. But A is irreducible and reduced, so it suffices to show that c_a induces the identity map on the function field $k(A)$, or even on the local domain $\mathscr{O}_{A,e}$.

Now inject the local ring into its completion: $\mathscr{O}_{A,e} \hookrightarrow \widehat{\mathscr{O}_{A,e}}$ (injectivity is by the Krull intersection theorem). It's enough to show that $c_a^* : \mathscr{O}_{A,e}/\mathfrak{m}_e^N \to \mathscr{O}_{A,e}/\mathfrak{m}_e^N$ is the identity map for all $N \geq 1$. For $N = 1$, this is $\mathrm{Lie}(c_a)$. 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 $\rho_N : A(k) \to \mathrm{GL}(\mathscr{O}_{A,e}/\mathfrak{m}_e^N)$ given by $a \mapsto c_a^*$. (Note that when $N = 2$, this is almost the tangent space; it's really a slight enlargment 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 $A(k)$, so $\rho_N = \mathrm{Id}$.

Why isn't this a proof? Because we need to prove ρ_N is *algebraic*; i.e., for the finite-dimensional k-vector space $V_N := \mathscr{O}_{A,e}/\mathfrak{m}_e^N$, there exists a k-morphism $A \to \mathrm{GL}(V_N)$ recovering ρ_N on k-points (see Exercise 1.5.5).

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 ρ_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 1.5.4. If X, Y are S-schemes and $h_X = \mathrm{Hom}_S(-, X)$, $h_Y = \mathrm{Hom}_S(-, Y)$ then Yoneda's lemma says that

$$\mathrm{Hom}_S(X, Y) \simeq \mathrm{Hom}_{S\text{-}\mathbf{Sch}}(h_X, h_Y).$$

In the category of schemes over $S = \mathrm{Spec}\ R$ 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 on this category 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, a construction functorial in varying k-algebras R is enough to obtain an algebraic morphism. So now we are looking for an R-functorial construction that recovers

$$A(k) \to \mathrm{GL}(\mathscr{O}_{A,e}/\mathfrak{m}_e^{N+1})$$

for $R = k$. For a k-algebra R and $a \in A(R)$, 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, $A(R') \to A(R')$ is defined by $x \mapsto a_{R'} x a_{R'}^{-1}$.) This carries e_R to e_R, so it preserves the section $\mathrm{Spec}\, R \xrightarrow{e_R} A_R$ (which is the base change of $\mathrm{Spec}\, k \xrightarrow{e} A$).

Note $\mathscr{O}_{A,e}/\mathfrak{m}_e^{N+1}$ is the stalk of the skyscraper sheaf $\mathscr{O}_A/\mathscr{I}_e^{N+1}$ at e, where $\mathscr{I}_e$ is the ideal sheaf of e. The map c_a preserves e_R, and hence also the structure sheaf of e_R. We claim that $\mathscr{I}_{e_R} = \mathscr{I}_e \otimes_k R$. Indeed, $\mathscr{I}_e$ is defined by the short exact sequence

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

and tensoring with R gives the short exact sequence

$$0 \to \mathscr{I}_{e_k} \otimes R \to \mathscr{O}_{A_R} \to R(e) \to 0.$$

The crucial point is that the ideal sheaf of a section "commutes" with base change. Indeed, on the level of an affine open around a k-point section the section induces a splitting $B = k \oplus I_e$, hence $B_R = R \oplus I_R$. (In general, a non-flat base change can have a more violent effect on a general quasi-coherent ideal sheaf not assumed to arise from a section; the problem is caused by the possible non-flatness of the associated closed subscheme over the base.)

So we have

$$\mathscr{O}_{A_R}/\mathscr{I}_{e_R}^{N+1} \simeq (\mathscr{O}_A/\mathscr{I}_e^{N+1}) \otimes_k R \simeq \mathscr{O}_{A,e}/\mathfrak{m}_e^{N+1} \otimes_k R.$$

Now we crucially use the fact that we are working over a ring, so that an infinitesimal neighborhood of the section (which is affine) is still an *affine* scheme (because this property can be checked on the reduced scheme; e.g., by Serre's cohomological criterion). Thus $\mathscr{O}_{A,e}/\mathfrak{m}_e^{N+1} \otimes_k R$ is the coordinate ring of the Nth infinitesimal neighborhood of e_R.

We've established that $c_a : A_R \to A_R$ preserves the ideal sheaf $\mathscr{I}_N$ of the Nth infinitesimal neighborhood of the identity. Letting $V_N = \mathscr{O}_{A,e}/\mathfrak{m}_e^{N+1}$, we have that c_a induces an R-algebra automorphism of the coordinate ring $V_N \otimes_k R$, obtained from the action on the underlying scheme. The map $A(R) \to \mathrm{GL}_R(V_N \otimes_k R)$ sending $a \mapsto c_a$ is *functorial* in R (check it!).

Functorially in k-algebras R, $\mathrm{GL}_R(V_N \otimes_k R)$ is the group of R-valued points of the k-group scheme $\mathrm{GL}(V_N)$. This gives an *algebraic* map $A \to \mathrm{GL}(V_N)$ as required. Now the punchline is that $A \to \mathrm{GL}(V_N)$ is a k-morphism from a smooth geometrically connected proper k-scheme to an affine scheme, hence a map onto a k-point of the target. □

Exercise 1.5.5. 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 $R' \mapsto \mathrm{Aut}_{R'}(V \otimes_R R')$. Prove in two ways that this is represented by an affine R-group $\mathrm{GL}(V)$ that is Zariski-locally (on $\mathrm{Spec}\, R$) isomorphic to GL_n:

(1) Work Zariski-locally on $\mathrm{Spec}\, R$ and construct the group scheme by gluing,

(2) Let S be the symmetric algebra o the dual module $\mathrm{End}(V)^* = V^* \otimes V$. Identify $\det\colon \mathrm{End}(V) \to R$ with a canonical element in S that is homogeneous of degree n. Prove that $\mathrm{Spec}(S[1/\det])$ does the job.

1.6. **Torsion.** First let's consider the familiar case of a complex torus A. In this case $A \simeq V/\Lambda$, so

$$A[N] := \{a \in A \mid Na = 0\} = \frac{1}{N}\Lambda/\Lambda \simeq \Lambda/N\Lambda \simeq (\mathbf{Z}/N\mathbf{Z})^{2g}.$$

Remark 1.6.1. The latter can be identified with $H_1(A, \mathbf{Z}/n\mathbf{Z})$.

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.

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

Therefore,

$$\varprojlim_{n\geq 0} A[\ell^n] \simeq \varprojlim_{n} \Lambda/\ell^n\Lambda \simeq \mathbf{Z}_\ell \otimes_{\mathbf{Z}} \Lambda \simeq H_1(A, \mathbf{Z}_\ell)$$

for prime ℓ. We define the ℓ-adic *Tate module* of A to be $T_\ell(A) = H_1(A, \mathbf{Z}_\ell)$. It is a free $\mathbf{Z}_\ell$-module of rank $2g$. The key point is that it is a *functorial* in A. Now, although $H_1(A, \mathbf{Z})$ cannot be cooked up in the *algebraic* setting, $H_1(A, \mathbf{Z}_\ell)$ can and is useful over arbitrary fields!

Remark 1.6.2. Why "can't" we algebraically construct a cohomology group $H_1(A, \mathbf{Z})$ that recovers $H_1(A, \mathbf{Z}_\ell)$ by change of coefficients? Here is an argument of Serre. If you had a functorial assignment of a rank-$2g$ lattice to an abelian variety of dimension g over a general field, then the endomorphism ring of the abelian variety would act on this lattice. But in characteristic $p > 0$ with $g = 1$ one can have an order in a quaternion algebra over $\mathbf{Q}$ as the endomorphism ring, which has no representation on a rank-2 lattice.

Now we turn to the algebraic theory over a general field k. Two questions present themselves:

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

In particular, if A is an abelian variety over $\overline{\mathbf{Q}}$ then we expect that $A(\overline{\mathbf{Q}})[N] = A(\mathbf{C})[N]$.

Toy case. Consider analogoues for $\mathbf{G}_m = \mathrm{GL}_1$. Clearly $\mathbf{G}_m(\overline{k})[N] = \{x \in \overline{k} \mid x^N = 1\}$. There are two possibilities:

$$\mathbf{G}_m(\overline{k})[N] = \begin{cases} N \text{ solutions, cyclic} & \mathrm{char}(k) \nmid N, \\ \text{fewer solutions, cyclic} & \mathrm{char}(k) \mid N; \end{cases}$$

this will be analogous to what happens for abelian varieties and was classically "understood" for elliptic curves:

$$E(\overline{k})[\ell] = \begin{cases} (\mathbf{Z}/\ell\mathbf{Z})^2, & \ell \neq \mathrm{char}\ k; \\ \mathbf{Z}/\ell\mathbf{Z} \text{ or } \{0\}, & \ell = \mathrm{char}\ k. \end{cases}$$

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 $[N]\colon A \to A$ the multiplication-by-N map defined by $a \mapsto N \cdot a$. We define $A[N] := \ker([N]) = [N]^{-1}(0)$, the *scheme-theoretic* fiber. For a homomorphism $f : G \to H$ between group schemes over a field k, the fiber $f^{-1}(e_H) \subset G$ represents the functor $R \rightsquigarrow \ker(G(R) \to H(R))$ on k-algebras.

The fiber $A[N] = [N]^{-1}(0)$ represents the functor $R \mapsto \{a \in A(R) \mid N \cdot a = 0 \in A(R)\}$, and we'll see later that $A[N]$ is k-finite and $\dim_k \mathcal{O}(A[N]) = N^{2g}$. However, there might not be so many geometric points; there could be nilpotents in the coordinate ring of $A[N]$ contributing to the dimension but not to physical points. The idea that the "order" of the N-torsion subgroup should be N^{2g} is retained in a useful way by focusing on the dimension of the coordinate ring of $A[N]$ as a k-scheme, but the structure of this group scheme will be subtle, depending on whether or not the characteristic divides N.

Example 1.6.4. The map $\mathbf{G}_m \xrightarrow{t^N} \mathbf{G}_m$ has kernel Spec $k[t]/(t^N - 1)$. If the characteristic is p and $N = p$, then this is the k-scheme $k[x]/(x^p)$ where $x = t - 1$, so it is a fat point. Likewise, the map $x^p\colon \mathbf{G}_a \to \mathbf{G}_a$ in characteristic $p > 0$ has kernel $k[x]/(x^p)$. These kernels have the same scheme structure but as *group schemes* that are *not* isomorphic (Cartier duality, to be discussed later, will provide an obstruction).

The set of torsion points of a complex torus is dense, and we will prove an analogous statement for abelian varieties: if A is an abelian variety over $k = \overline{k}$, then the union of the subgroups $\{A[\ell^n]\}_{n \geq 1}$ is Zariski-dense in A for any fixed prime $\ell \neq \mathrm{char}\ k$.

1.7. **Rigidity.** The goal of this section is to prove that for abelian varieties A and A' over a field k, any k-morphism $f : A \to A'$ satisfying $e_A \mapsto e_{A'}$ 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

$$\begin{aligned} h : A \times A &\to A' \\ (a_1, a_2) &\mapsto f(a_1 a_2) f(a_1)^{-1} f(a_2)^{-1} \end{aligned}$$

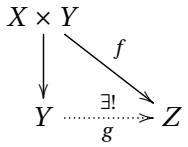
is actually the constant map $(a_1, a_2) \mapsto e := e_A$.

The rigidity theorem asserts that in some circumstances, a map from a product that is constant on one slice must factor through projection to the other factor. Obviously $h|_{A\times\{e\}}$ factors through the k-point $e' := e_{A'}$ and likewise for $h|_{\{e\}\times A}$, so we can apply:

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

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

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



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 $X \times Y \to Z \times Y$ given by $(x,y) \mapsto (f(x,y), y)$. 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 in the family is constant then they all are.

Example 1.7.3. Properness is crucial. If $X = Y = Z = \mathbf{A}^1$ and $f(x,c) = c\,x$ then f_0 is constant, but the conclusion of the theorem does not hold. (It may seem that you can extend this map to $X = Z = \mathbf{P}^1$, 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 with Y reduced.
(2) *Descent.* We argue that if g exists after base change to some finite Galois extension, then it exists 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 for any $\sigma \in \mathrm{Gal}(k'/k)$ 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 finite Galois extension k'/k such that $X(k') \neq \emptyset$. It suffices to show that $X(k_s) \neq \emptyset$. The next lemma settles this:

Lemma 1.7.4. *If X is a geometrically reduced scheme of finite type over $k = k_s$ then $X(k) \neq \emptyset$.*

Proof. The irreducible components of X are geometrically irreducible since $k = k_s$. We may assume X is irreducible by passing to an irreducible component with reduced structure (exercise: prove this is still geometrically reduced over

k). Now X is geometrically integral. The idea is to produce a dense open subscheme isomorphic to some affine hypersurface in $\mathbf{A}^n$.

Since $k = k_s$, $X_{\overline{k}} \to X$ is a homeomorphism (since $\overline{k}/k$ is purely inseparable). Letting $\eta \in X$ and $\overline{\eta} \in X_{\overline{k}}$ be the generic points, passing to stalks at such points as a limit over non-empty open sets gives the $\overline{k}$-algebra isomorphism

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

between function fields. This shows that $k(X)/k$ is *separable* (see §26 of [Mat]). Equivalently, $k(X)/k$ has a separating transcendence basis, so

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

where f is a monic irreducible polynomial over $k(t_1, \ldots, t_n)$ that remains irreducible over $\overline{k}(t_1, \ldots, t_n)$. Let $d > 0$ be the t_{n+1}-degree of f.

Let $h \in k[t_1, \ldots, t_{n+1}]$ be obtained from f by multiplying against a least common multiple of the denominators of f in the UFD $k[t_1, \ldots, t_n]$, so h is irreducible $\partial h/\partial t_{n+1} \neq 0$. The isomorphism between the function fields of X and of the hypersurface $\{h = 0\} \subset \mathbf{A}^{n+1}$ yields a dense open subset of X isomorphic to a dense open subset U' of $(h = 0)$. We reduce to showing that U' has a rational point (or more specifically that the locus of k-points in $(h = 0)$ is Zariski-dense).

Consider the projection map $\pi\colon U' \to \mathbf{A}^n$ to the first n coordinates. The discriminant $\mathrm{disc}_{t_{n+1}}(h) \in k[t_1, \ldots, t_n]$ is nonzero (since $\partial h/\partial t_{n+1} \neq 0$). Let $V' \subset \mathbf{A}^n$ be the dense open defined by the simultaenous non-vanishing of this dscriminant and of the leading t_{n+1}^d-coefficient of h. The formation of the discriminant of degree-d polynomials over commutative rings is given by a universal (albeit messy) determinant and as such is compatible with scalar extension (such as reduction modulo an ideal) with the caveat that *scalar extension might kill the leading coefficient*. The discriminant of degree-3 polynomials applied to a degree-2 polynomial (with coefficient 0 in degree 3) does not agree with the quadratic discriminant, for example!

The situation is much better with polynomials whose leading coefficient is a *unit*: for these the formation of the discriminnt iis compatible with any extension of scalars. We defined V' so that the t_{n+1}^d-coefficient of h is a unit over V', so if $v_0' \in V'(k)$ (as exists since k is infinite and V' is dense open in an affine space) then $f(v_0', t_{n+1}) \in k[t_{n+1}]$ has non-zero discriminant in k! This says that $f(v_0', t_{n+1})$ is separable over k with degree $d > 0$, so it has a solution in k since $k = k_s$. Any such solution gives a point in $U'(k)$. □

(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 $x_0 \in X(k)$, define $g(y) = f(x_0, y)$. We want to show that $f(x, y) = g(y)$.

To check this, we may extend the base field further if necessary, so we may assume that $y_0 \in Y(k)$ and k is algebraically closed. 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 the fiber $X \times \{y_0\}$. Since the projection map $X \times Y \to Y$ is proper, the complement of $f^{-1}(U)$ maps to a closed set in Y. Therefore,

its complement is an open set $V \subset Y$ such that $X \times V \subset f^{-1}(U)$. (This is a general and very useful fact about proper maps: any open neighborhood of a fiber contains the preimage of an open set around the base point of the fiber.)

Since U is affine and X is proper, each fiber of $X \times V \to V$ is crushed to a point, so $f(x,y) = f(x_0,y) = g(y)$ on $(X \times V)(k)$. As Z is separated, the scheme $(f, g \circ \mathrm{pr}_2)^{-1}(\Delta_{Z/k}) \subset X \times Y$ classifying equality for f and $g \circ \mathrm{pr}_2$ is a closed subscheme of the scheme $X \times Y$ that is reduced (!), yet this closed subscheme contains the subset $(X \times V)(k)$ that is Zariski-dense (as $k = \overline{k}$ and Y is irreducible). Hence, the scheme of equality coincides with $X \times Y$; i.e., $f = g \circ \mathrm{pr}_2$.

□

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

Proof. Consider the map $h : A \times A \to A'$ given by

$$(a_1, a_2) \mapsto f(a_1 a_2) f(a_2)^{-1} f(a_1)^{-1}.$$

This crushes $A \times \{e\}$, hence factors through the second projection. But it also crushes $\{e\} \times A$, hence factors through the first projection. So for all a_1, a_2, we have

$$h(a_1, a_2) = h(e, a_2) = h(e, e) = e'.$$

□

This gives another proof of:

Corollary 1.7.6. *Abelian varieties are commutative.*

Proof. Apply Corollary 1.7.5 to 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 $\mathrm{Id} : (A, m, e) \to (A, m', e)$. This is automatically a homomorphism by Corollary 1.7.5. □

Remark 1.7.8. The preceding corollary is curious, but is it ever important in practice? Yes! The point is that it allows us to carry out deformation theory arguments with abelian varieties without needing to keep as careful track of the group law, associativity, etc. as might seem necessary (provided one can *somehow* deformation the group law, which Grothendieck figured out how to handle by a general shearing trick). 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, very useful in practice. In each case the key point is that we do not assume the schemes of interest are affine.

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 $\varinjlim K_i = K$. 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 any of the properties: 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 actions of $\mathrm{Gal}(K/k)$ 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 [FGA, §9], which rests on the theory of Hilbert schemes developed in [FGA, §5].) Our approach deviates from that of [Mum] in which a theory of Picard schemes is developed only for abelian varieties.

Setup. Let X be a (non-empty) 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 $\mathscr{L}$ on $X \times_k S$ where S is some k-scheme. Informally, you can think of a line bundle $\mathscr{L}$ on $X \times_k S$ as a family of line bundles $\{\mathscr{L}_s = \mathscr{L}|_{X_s}\}_{s\in S}$.

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 $\mathscr{L}$ admits an action of $\Gamma(X_S, \mathscr{O}_{X_s}^\times) \supset \Gamma(S, \mathscr{O}_S^\times)$. 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 S be a k-scheme and $f_S\colon X_S \to S$ the projection map. Then $\mathscr{O}_S = f_{S*}(\mathscr{O}_{X_S})$.*

Proof. Consider the base-change diagram

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

By flat base change for quasicoherent sheaves, the natural map

$$\mathscr{O}_S \otimes_k \Gamma(X, \mathscr{O}_X) \to f_{S*}(\mathscr{O}_{X_S})$$

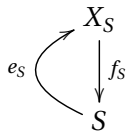
is an isomorphism. (For a quasi-compact separated map, pushforward commutes with flat base change.) Since $k \hookrightarrow \Gamma(X, \mathscr{O}_X)$ is an equality by the assumptions on X, we are done. □

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

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 incorporate the datum of a rational point into our list of running assumptions on X. This is a bad move to make in general (such as for the theory of Picard schemes for algebraic curves), because even the existence of rational points may be a question of interest. Hence, using a specified point in $X(k)$ in what follows is to be regarded as a provisional method that is harmless in the case of abelian varieties.

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

Definition 2.2.3. A *trivialization* of $\mathscr{L}$ (on X_S) along e ("along e_S") is an isomorphism $\iota\colon e_S^*(\mathscr{L}) \simeq \mathscr{O}_S$.

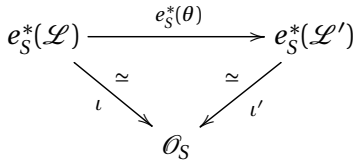


Example 2.2.4. If $S = \operatorname{Spec} k$, this is just a basis of the k-line $\mathscr{L}(e) := \mathscr{L}|_e$.

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

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

Definition 2.2.6. An *isomorphism* $(\mathscr{L}, \iota) \simeq (\mathscr{L}', \iota')$ on X_S is an isomorphism $\theta\colon \mathscr{L} \simeq \mathscr{L}'$ preserving the trivialization; i.e.,



Lemma 2.2.7. *We have* $\operatorname{Aut}(\mathscr{L}, \iota) = \{1\}$.

Proof. This follows from $\operatorname{Aut}(\mathscr{L}) = \Gamma(S, \mathscr{O}_S^\times)$ (by Exercise 2.2.2) and the fact that $\Gamma(S, \mathscr{O}_S^\times)$ acts simply transitively on all possible ι for $\mathscr{L}$.

Said differently, we know that any automorphism of $\mathscr{L}$ is multiplication by a unit from S, which is therefore detected by the induced automorphism of $e^*\mathscr{L}$. But the composition

$$\Gamma(S, \mathscr{O}_S^\times) \to \Gamma(X_S, \mathscr{O}_{X_S}^\times) \xrightarrow{e_S^*} \Gamma(S, \mathscr{O}_S^\times)$$

is the identity map, so if $\iota = \iota'$ then this unit must be 1. □

You might complain that you are really interested in line bundles, not the rigidified line bundles, but that is assuaged by the following fact that is specific to working over a field (or more generally over a local ring):

Proposition 2.2.8. *The projection map*

$$\begin{array}{c} \{(\mathscr{L}, \iota) \text{ on } X\}/\simeq \\ \downarrow \\ \operatorname{Pic}(X) = \{\mathscr{L} \text{ on } X\}/\simeq \end{array}$$

is bijective.

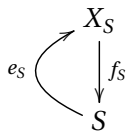
Proof. Surjectivity is simply the statement that $\mathrm{Pic}(\mathrm{Spec}\, k) = 1$, so we can always find some trivialization ι. The interesting part will be injectivity.

You can check that this map is a homomorphism, where the group structure on the source is tensor product of line bundles and sections. Suppose we have two rigidified bundles $(\mathscr{L},\iota),(\mathscr{L}',\iota')$ and an isomorphism $\theta : \mathscr{L} \simeq \mathscr{L}'$. Then θ carries ι to $u\iota'$ for some $u \in \Gamma(S, \mathscr{O}_S^\times)$. Replacing θ with $u^{-1}\cdot\theta$ induces an isomorphism $(\mathscr{L},\iota) \simeq (\mathscr{L}',\iota')$. □

Given $\mathscr{L}$ on X_S, consider the following modification:

$$\mathscr{L} \rightsquigarrow \mathscr{L} \otimes f_S^*(e_S^*\mathscr{L})^{-1}.$$

where as before, $e_S : S \to X_S$ is a section of $f_S : X_S \to S$.



Applying $e_S^*(-)$ to the above, we obtain

$$e_S^*(\mathscr{L} \otimes f_S^*(e_S^*\mathscr{L})^{-1}) \simeq e_S^*\mathscr{L} \otimes e_S^* f_S^*(e_S^*\mathscr{L})^{-1} \simeq e_S^*\mathscr{L} \otimes (e_S^*\mathscr{L})^{-1} \simeq \mathscr{O}_S.$$

This is a *canonical* trivialization of $e_S^*(\mathscr{L} \otimes f_S^*(e_S^*\mathscr{L})^{-1})$, giving $\mathscr{L} \otimes f_S^*(e_S^*\mathscr{L})^{-1}$ a canonical rigidified structure (denoted as "can")

Exercise 2.2.9. Check that given a trivialization ι of $e_S^*\mathscr{L}$, the induced isomorphism

$$e_S^*(\mathscr{L} \otimes f_S^*(e_S^*\mathscr{L})^{-1})) \simeq e_S^*(\mathscr{L} \otimes \mathscr{O}_{X_S}) \simeq \mathscr{O}_S$$

is ι.

Remark 2.2.10. Given $(\mathscr{L},\iota)$ and $(\mathscr{L}',\iota')$ on X_S, if there exists a Zariski cover $\{S_\alpha\}$ of S such that these rigidified line bundles become isomorphic over each X_{S_α} then they are isomorphic over X_S. This holds because the absence of non-trivial automorphisms of such pairs implies that the given isomorphisms over the X_{S_α}'s must coincide on overlaps and hence glue to a global isomorphism.

Definition 2.2.11. We define the *Picard functor* $\underline{\mathrm{Pic}}_{X/k,e}$ to be the functor

$$S \mapsto \{(\mathscr{L},\iota) \text{ on } X_S\}/\simeq,$$

whose values are commutative groups (with identity $(\mathscr{O}_{X_S}, 1)$ under $\otimes$).

The preceding remark shows that this is a Zariski sheaf on any S. That would fail without the rigidification! Such a sheaf property 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 have an isomorphism

$$\underline{\mathrm{Pic}}_{X/k,e}(S) \simeq \underline{\mathrm{Pic}}_{X/k,e'}(S)$$

via $(\mathscr{L},\iota) \mapsto (\mathscr{L} \otimes f_S^*(e'_S)^*\mathscr{L}^{-1} \otimes f_S^*(e_S)^*\mathscr{L}, \mathrm{can} \otimes \iota)$.

Proposition 2.2.12. *The map* $\underline{\mathrm{Pic}}_{X/k,e}(S) \to \mathrm{Pic}(X_S)/f_S^*(\mathrm{Pic}\, S)$ *given by* $(\mathscr{L},\iota) \mapsto \mathscr{L}$ *is an isomorphism respecting the above identification under change of* e.

Proof. That the map is a homomorphism is obvious. Surjectivity follows from the observation that $\mathscr{L} \otimes f_S^*(e_S)^*\mathscr{L}^{-1}$ admits a (canonical) trivialization. Injectivity follows from the earlier observation that any isomorphism $\mathscr{L} \simeq \mathscr{L}'$ is induced by a unit $u \in \Gamma(S, \mathscr{O}_S^\times)$ and this u can be *uniquely* chosen to take any e_S-trivialization ι to any other trivialization ι'.

Exercise 2.2.13. Check the claimed compatibility with change of base point.

□

There must be a canonical inverse to the preceding isomorphism; what is it? A bit of thought shows it is

$$\mathscr{L} \mapsto (\mathscr{L} \otimes f_S^* e_S^* \mathscr{L}^{-1}, \mathrm{can}).$$

You might complain that this changes the line bundle, but composition with the isomorphism in the opposite direction really does give the identity because changing by $f_S^* e_S^* \mathscr{L}^{-1}$ has no effect modulo $\mathrm{Pic}\, S$.

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

$$\xi\colon \mathrm{Hom}_k(\cdot, \mathscr{M}) \simeq \underline{\mathrm{Pic}}_{X/k,e}.$$

It is common to say "$\mathscr{M}$ represents the functor", but this is abusive. As Grothendieck emphasized in his Seminaire Bourbaki and Seminaire Cartan lectures, an object alone cannot represent a functor: it is $\mathscr{M}$ *plus* the data of this isomorphism ξ that represents the functor. The point is that, upon unraveling the proof of Yoneda, evaluating ξ on $\mathscr{M}$ and choosing $\mathrm{Id}_{\mathscr{M}}$ on the left side gives a *distinguished* rigidified line bundle $(\mathscr{P},\theta) \in \underline{\mathrm{Pic}}_{X/k,e}(\mathscr{M})$, which is the "universal line bundle." Then for any $(\mathscr{L},\iota)$ on $X_S \to S$, there exists a unique map $S \to \mathscr{M}$ pulling back the universal bundle to $(\mathscr{L},\iota)$:

$$\begin{array}{ccc} X_S & \longrightarrow & X_{\mathscr{M}} \\ {\scriptstyle f_S}\downarrow & & \downarrow \\ S & \xrightarrow[\varphi_{(\mathscr{L},\iota)}]{\exists!} & \mathscr{M}. \end{array}$$

i.e. $\varphi^*\mathscr{P} \simeq \mathscr{L}$ over X_S carrying $\varphi^*\theta$ to ι. Note that the isomorphism $\varphi^*\mathscr{P} \simeq \mathscr{L}$ is *unique* because there are no automorphisms after rigidification, so this isomorphism does not have to be specified as part of the data.

In conclusion, the representability amounts to the existence of $\mathscr{M}$ *plus* a structure over $\mathscr{M}$ with a universal property. (If we didn't make the rigidification then the situation would become rather murky due to ambiguity in the isomorphism onto the pullback line bundle.) More generally, the preceding discussion applies to any contravariant, set-valued functor F.

For any field extension K/k, we have

$$\mathscr{M}(K) = \underline{\mathrm{Pic}}_{X/k,e}(K) = \mathrm{Pic}(X_K)$$

because $\mathrm{Pic}(K) = 0$ (see Proposition 2.2.12). In any "local" situation, we can drop the rigidification. To do the hard work of building a universal structure, 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 pass to a quotient removing the effect of the choice of a divisor. The ultimate result is:

Theorem 2.3.1 (Grothendieck/Oort–Murre/Artin)**.** *Let X be a geometrically reduced, geometrically connected, proper k-scheme. If $X(k) \neq \emptyset$ then for any $e \in X(k)$ the functor $\underline{\mathrm{Pic}}_{X/k,e}$ is represented by a locally finite type k-scheme $\mathrm{Pic}_{X/k,e}$.*

Proof. The proof requires a good deal of technical machinery (which is irrelevant to setting up the rest of the theory of abelian varieties), so we will omit it and instead just make some remarks about the construction.

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

Grothendieck explicitly constructs $\mathrm{Pic}_{X/k}$ as a countable union of quasi-projective schemes. The connected components can sometimes be distinguished by evident "discrete" invariants (such as the degree of a line bundle when X is a curve), but in many cases one has little idea as to when a given line bundle on X lies in the identity component of the Picard scheme. (For abelian varieties we will obtain a concrete characterization of line bundles in the identity component.)

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 criterion for a morphism to be locally finitely presented [EGA IV_3 8.14]) 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 over a general base the methods in the *proof* of the locally noetherian case, such as base change theorems for coherent cohomology; rather, one formally shows that the final conclusion of representability automatically holds more generally when known in the locally noetherian case.)

As a beginner in algebraic geometry one might not want to worry about the restriction to the locally noetherian case, though one cost of requiring "locally noetherian" everywhere is that whenever you take fiber products that at least one of the two structure maps should be (essentially) locally finite type (or else you may 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 it can be deduced without too much effort from the locally noetherian case. (EGA develops very clean methods to carry out such bootstrap procedures, applicable for instance to Picard functors.) □

We have seen above that in a *natural* way the functor $\underline{\mathrm{Pic}}_{X/k,e}$ is independent of e; more specifically, we described the functor in terms that do not mention a choice of e (but requires $X(k) \neq \emptyset$ to be an appropriate notion): $S \rightsquigarrow \mathrm{Pic}(X_S)/\mathrm{Pic}(S)$. Thus, from

now on we shall usually write $\mathrm{Pic}_{X/k}$ to denote the Picard scheme, suppressing the mention of e (though when we need to do computations with a universal structure we will need to make a choice of e).

2.4. **Properties of** $\mathrm{Pic}_{X/k}$**.** To start, observe that $\mathrm{Pic}_{X/k}$ is automatically a group scheme, as it represents a group-valued functor. Moreover, it comes out of Grothendieck's construction that $\mathrm{Pic}_{X/k}$ is locally of finite type (though that also follows from a functorial criterion).

Exercise 1.5.3 yields that if G is a group scheme locally finite type over k then G^0 is geometrically irreducible and finite type (hence quasi-compact). But it can really happen in more general circumstances that one builds (natural) moduli schemes that are locally of finite type and connected but not quasi-compact (i.e., not of finite type).

The Picard scheme $\mathrm{Pic}_{X/k,e}$ is separated due to how it is constructed, or more conceptually because of:

Lemma 2.4.1. *If G is a group scheme over a field k, then G is separated.*

This lemma generally fails when the base is not a field.

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

$$\begin{array}{ccc} G & \xrightarrow{\Delta} & G \times G \\ \downarrow & & \downarrow{\scriptstyle (x,y)\mapsto x\,y^{-1}} \\ G & \xrightarrow{e} & G \end{array}$$

This realizes the diagonal map as a base-change of the identity section, which is a closed immersion when over a field (this fails over a more general base). □

We conclude that the identity component $\mathrm{Pic}^0_{X/k}$ is a separated k-group of finite type.

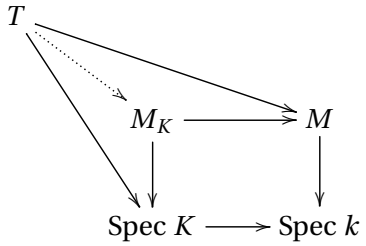
Example 2.4.2. When X is not smooth, $\mathrm{Pic}^0_{X/k}$ can be non-proper. For example, if X is the nodal cubic then $\mathrm{Pic}^0_{X/k} \simeq \mathbf{G}_m$ (see 9.2/8 in [BLR]). Intuitively, the Picard group is parametrized by slopes of lines, with two slopes missing.

In general, it's hard to characterize $\mathrm{Pic}^0_{X/k}(K) \subset \mathrm{Pic}(X_K)$. In Exercise 2.4.4 you'll show that for a curve this is just the set of line bundles of degree 0. Roughly speaking, the identity component for the Picard scheme of a geometrically connected but reducible curve classifies line bundles that are "degree 0" on each geometric irreducible component.

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

$$\mathrm{Hom}_k(-, M)|_{\mathbf{Sch}/K} \simeq \mathrm{Hom}_K(-, M_K),$$

which just follows from the universal property of the fibered product: if T is over Spec K and admits a map to M over k, then there is a unique K-map $T \to M_K$ inducing them.



So the point is that "base change of the representing object" corresponds to restriction to the subcategory over the new base.

Exercise 2.4.3. 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 $\mathrm{Pic}^0_{X/k}$ is a k-scheme of finite type by Exercise 1.5.3.

(i) Prove that if X is smooth and projective over k then $\mathrm{Pic}_{X/k}$ satisfies the valuative criterion for properness (so $\mathrm{Pic}^0_{X/k}$ is a proper k-scheme).

(ii) By computing with points valued in the dual numbers, and using Cech theory in degree 1, construct a natural k-linear isomorphism $H^1(X, \mathscr{O}_X) \simeq T_0(\mathrm{Pic}^0_{X/k}) = T_0(\mathrm{Pic}_{X/k})$.

(iii) If X is smooth with dimension 1, prove that $\mathrm{Pic}_{X/k}$ satisfies the infinitesimal smoothness criterion (for schemes locally of finite type over k). Deduce that $\mathrm{Pic}^0_{X/k}$ is an abelian variety of dimension equal to the genus of X.

By Exercise 2.4.3, we have isomorphisms of k-vector spaces

$$T_0(\mathrm{Pic}^0_{X/k}) = T_0(\mathrm{Pic}_{X/k}) = \ker(\mathrm{Pic}_{X/k}(k[\epsilon]) \to \mathrm{Pic}_{X/k}(k)) \simeq H^1(X, \mathscr{O}_X).$$

There's a general characterization in terms of the functor of points for when a scheme over a base is locally of finite presentation, and that provides a conceptual explanation for why Picard schemes must be locally of finite type over k when they exist. Note that if X is not proper then $H^1(X, \mathscr{O}_X)$ could be infinite-dimensional, so we see a priori that a Picard scheme cannot exist in such cases.

Exercise 2.4.4. 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 $P = \mathrm{Pic}_{X/k}$ be its Picard scheme. By Exercise 2.4.3 the k-group scheme P is smooth of dimension $h^1(X, \mathscr{O}_X) = g$ 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 $P(k) = \mathrm{Pic}(X)$ parametrizing line bundles of degree 0.

(1) For any k-scheme S and section $x \in X(S) = X_S(S)$, prove that the quasi-coherent ideal sheaf of the closed subscheme $x : S \hookrightarrow X_S$ is an invertible sheaf whose local generators are nowhere zero-divisors on $\mathscr{O}_{X_S}$.

(2) For a coherent sheaf $\mathscr{F}$ on a proper k-scheme Y, recall that the *Euler characteristic* $\chi(\mathscr{F})$ is defined to be $\sum (-1)^j h^j(Y, \mathscr{F})$. For an invertible sheaf $\mathscr{L}$ on X, prove that $\chi(\mathscr{L}^n) = d_{\mathscr{L}} \cdot n + (1-g)$ for an integer $d_{\mathscr{L}}$: we call this integer the *degree* of $\mathscr{L}$.

For a Weil divisor $D = \sum n_i x_i$ on our curve X, define $\deg D = \sum n_i [k(x_i) : k]$. Prove that both notions of degree are invariant under extension of the ground field, and that they coincide when $Y = X$ and $\mathscr{L} \simeq \mathscr{O}_X(D)$.

(3) Choose $e \in X(k)$, and define $X^g \to P$ by defining $X(S)^g \to P(S) = \mathrm{Pic}(X_S)/\mathrm{Pic}(S)$ for any k-scheme S to be

$$(x_1, \ldots, x_g) \mapsto \mathscr{O}_{X_S}(x_1) \otimes \ldots \otimes \mathscr{O}_{X_S}(x_g) \otimes \mathscr{O}_{X_S}(e)^{\otimes(-g)}.$$

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 $X_{\overline{k}}$, prove that this latter map on $\overline{k}$-points hits exactly the line bundles on $X_{\overline{k}}$ of degree 0 (don't ignore the case $g = 0$!).

(4) It is a general fact (proved in [Mum] 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 $\mathbf{Z}$ over $\mathrm{Spec}\ k$ assigning to any point of $P(S)$ the locally constant function given by the fiberwise degree of the line bundle. Using that $\mathbf{Z}$ as a constant 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 $\mathrm{Pic}(X_K)$. (This depends crucially on the hypothesis that $X(k) \neq \emptyset$; Grothendieck gave a way to define $P = \mathrm{Pic}_{X/k}$ without such a hypothesis on X, and then $P^0(k)$ can fail to have this concrete description when $\mathrm{Br}(k) \neq 1$.)

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

In §11 of [Mum], Mumford proves Cartier's Theorem that any locally finite type group scheme over k is smooth if $\mathrm{char}\ k = 0$. In characteristic $p > 0$, there are examples of smooth (geometrically connected) projective surfaces X with $\mathrm{Pic}_{X/k}$ not smooth. Understanding this phenomenon is the main point of Mumford's book "Lectures on curves on an algebraic surface."

Despite the general failure of smoothness of Picard schemes in positive characteristic, a miracle occurs for abelian varieties: for X an abelian variety, $\mathrm{Pic}_{X/k}$ is *always* smooth, even in positive characteristic. The infinitesimal smoothness criterion is very hard to directly verify (I don't know how to do that), and instead one uses a more geometric argument to establish its smoothness; we will address this later.

Exercise 2.4.5. 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 $X \to \mathrm{Pic}_{X/k}$ defined on R-points (for a k-algebra R) by $x \mapsto \mathscr{O}(x) \otimes \mathscr{O}((x_0)_R)$ (where $\mathscr{O}(x) := \mathscr{I}(x)^{-1}$ for the *invertible* ideal $\mathscr{I}(x)$ of $x : \mathrm{Spec}(R) \hookrightarrow X_R$) is a proper monomorphism, hence a closed immersion. Thus, the choice of x_0 defines a closed immersion of X into the abelian variety $\mathrm{Pic}^0_{X/k}$ of dimension g. The realization of X inside the abelian variety $\mathrm{Pic}^0_{X/k}$ is a powerful tool in the study of the arithmetic of curves.

3. LINE BUNDLES ON ABELIAN VARIETIES

3.1. **Some fundamental tools.**

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

$$\begin{array}{ccc} X_S & \xrightarrow{1_X \times f} & X \times Y \\ \downarrow & & \downarrow \\ S & \xrightarrow{f} & Y \end{array}$$

has the property that the line bundle $\mathscr{N} := (1_X \times f)^*\mathscr{L}$ on X_S comes from a line bundle on S if and only if f factors through Y_1.

Remark 3.1.2. Our proof of the Seesaw Theorem will use the existence of $\mathrm{Pic}_{Y/k}$ when $Y(k) \neq \emptyset$. At the start of §10 of Chapter III of [Mum], Mumford gives a direct proof of the Seesaw Theorem over algebraically closed k by a cohomological study of infinitesimal fibers, artfully hiding any appeal to the existence of Picard schemes (but with the consequence that the result may seem somewhat mysterious, whereas the proof using Picard schemes below gives a very intuitive reason for the existence of Y_1).

Before proving the Seesaw Theorem, we make some observations:

Example 3.1.3. Taking $S = \mathrm{Spec}\ \overline{k}$, necessarily

$$Y_1(\overline{k}) = \{y \in Y(\overline{k}) | \mathscr{L}_{X_y} \simeq \mathscr{O}_{X_y}\}.$$

Exercise 3.1.4. Let $\phi : Z \to S$ be a proper flat surjective map of schemes, with S locally noetherian, and assume that the geometric fibers of ϕ are reduced and connected. For a line bundle $\mathscr{N}$ on Z, prove that $\mathscr{N} \simeq \phi^*\mathscr{M}$ for a line bundle $\mathscr{M}$ on S if and only if $\phi_*\mathscr{N}$ is invertible and the natural map $\phi^*\phi_*\mathscr{N} \to \mathscr{N}$ is an isomorphism (in which case $\mathscr{M} \simeq \phi_*\mathscr{L}$). Deduce that in such cases, the formation of $\phi_*(\mathscr{L})$ commutes with any base change on S.

Proof of Theorem 3.1.1. Let $h : X_S \to S$ be the proper flat structure morphism. By Exercise 3.1.4 for locally noetherian S (and limit considerations if one wants to avoid noetherian hypotheses), $\mathscr{N}$ comes from S if and only if $h_*(\mathscr{N})$ is invertible on S and the natural map $h^*(h_*(\mathscr{N})) \to \mathscr{N}$ is an isomorphism. Whether or not these hold can be checked after applying scalar extension through by a finite Galois extension K/k, so by Galois descent for closed subschemes it suffices to build Y_1 after finite Galois extension on k. Hence, we may assume that $X(k) \neq \emptyset$. (This scalar extension is unnecessary in practice because we will only use the Seesaw Theorem when there is a rational point anyway.)

Choose $e \in X(k)$. It is harmless to replace $\mathscr{L}$ with $\mathscr{L} \otimes p_2^*(e_Y^*\mathscr{L})^{-1}$, as this doesn't affect the question of whether or not $\mathscr{L}$ is pulled back from S. So we have reduced to the case where we have a trivialization $\iota : \mathscr{O}_Y \simeq e_Y^*\mathscr{L}$.

Then the data $(\mathscr{L},\iota)$ is equivalent to a k-morphism $Y \xrightarrow{j} \mathrm{Pic}_{X/k,e}$. By functoriality, the pullback of $(\mathscr{L},\iota)$ to X_S corresponds to the map $S \to Y \to \mathrm{Pic}_{X/k,e}$ so we see that this line bundle comes 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 we shall later prove (after showing the projectivity of abelian varieties) that $\mathrm{Pic}^0_{X/k,e}$ is also an abelian variety, called the *dual abelian variety*. The next result is fundamental to the interaction between line bundles on abelian varieties and the group law, which will be needed to study the dual abelian variety.

Theorem 3.1.5 (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 $\mathscr{L}$ is a line bundle on $X \times Y \times Z$ such that $\mathscr{L}_{x_0} := \mathscr{L}|_{\{x_0\}\times Y\times Z} \simeq \mathscr{O}_{Y\times Z}$, and $\mathscr{L}_{y_0}, \mathscr{L}_{z_0}$ are also trivial. Then $\mathscr{L} \simeq \mathscr{O}_{X\times Y\times Z}$.*

Proof. Since $\mathscr{L}_{y_0}$ is trivial, $\mathscr{L}$ is classified by a map $X \times Z \to \mathrm{Pic}_{Y/k}$, and we want this to be the 0 map. (The Picard scheme exists with the expected functorial meaning because Y is proper and geometrically reduced and connected with $Y(k) \neq \emptyset$, and this Picard scheme 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 $\mathscr{L}_{z_0} \simeq \mathscr{O}_{X\times Y}$. So $\varphi(x,z) = \varphi(x_0,z)$ for any z. But the map $\varphi(x_0,z)$ is identically 0 because $\mathscr{L}_{x_0}$ is trivial on $Y \times Z$. □

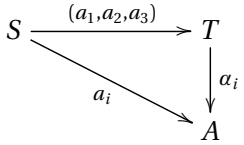
Theorem 3.1.6 ("Cubical structure on $\mathscr{L}$ on A/k")**.** *Let A be an abelian variety over k and $\mathscr{L}$ invertible on A. For S a k-scheme, $a_1, a_2, a_3 \in A(S)$ the line bundle*

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

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) because we include this final $(e^*\mathscr{L})_S^{-1}$ factor (which is trivial when k is a field).

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



In this universal case, we have

$$\alpha_1+\alpha_2+\alpha_3 = m : A^3 \to A$$
$$\alpha_i+\alpha_j = m_{ij} : A^2 \to A,\ i \neq j \quad \text{i.e. } (x_1,x_2,x_3) \mapsto x_i+x_j$$
$$\alpha_i = \mathrm{pr}_i : A^3 \to A,$$

so the line bundle of interest is

$$\mathscr{M} = m^*\mathscr{L} \otimes m_{12}^*\mathscr{L}^{-1} \otimes m_{13}^*\mathscr{L}^{-1} \otimes m_{23}^*\mathscr{L}^{-1} \otimes \mathrm{pr}_1^*\mathscr{L} \otimes \mathrm{pr}_2^*\mathscr{L} \otimes \mathrm{pr}_3^*\mathscr{L} \otimes (0^*\mathscr{L})_A^{-1}$$

on $A \times A \times A$.

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

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

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

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

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

Definition 3.2.1. Given a line bundle $\mathscr{L}$ on A, we define a map of k-schemes

$$\phi_{\mathscr{L}} : A \to \mathrm{Pic}^0_{A/k}$$

by the functorial rule $x \mapsto t_x^*\mathscr{L} \otimes \mathscr{L}^{-1}$.

Notice that this sends e to 0 (the point of $\mathrm{Pic}^0_{A/k}$ corresponding to the trivial bundle). We'll soon show that $\phi_{\mathscr{L}}$ is a homomorphism (for this, we may assume that $k = \overline{k}$ and compute with k-points).

Example 3.2.2. If K is a field and $\mathscr{L} \simeq \mathscr{O}(D)$, then $\phi_{\mathscr{L}}$ sends $x \in A(K)$ to $t_{-x}(D_K) - D_K \in \mathrm{Pic}^0(X_K)$. The content of $\phi_{\mathscr{L}}$ being a homomorphism is that this divisor is additive in $x \in A(K)$ *modulo principal divisors.*

Note that pulling back a divisor via translation by x correspondings to applying translation by $-x$ to the divisor.) The minus sign implies that this is the *negative* of the isomorphism from Silverman's book on elliptic curves (but we will see that including the sign is the "right" thing to do, and that avoiding it in the language of divisors is an unwise choice).

Corollary 3.2.3 (Theorem of the square)**.** *The map $\phi_{\mathscr{L}}$ is a homomorphism; i.e., for any k-scheme T and $x, y \in A(T)$, we have canonical isomorphisms*

$$t_{x+y}^*(\mathscr{L}_T) \otimes \mathscr{L}_T \simeq t_x^*(\mathscr{L}_T) \otimes t_y^*(\mathscr{L}_T) \otimes [(x,y)^*(m^*\mathscr{L} \otimes p_1^*\mathscr{L}^{-1} \otimes p_2^*\mathscr{L}^{-1} \otimes (e^*\mathscr{L})_A)]_{A_T}$$

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

We will call the line bundle $\Lambda(\mathscr{L}) := m^*\mathscr{L} \otimes p_1^*\mathscr{L}^{-1} \otimes p_2^*\mathscr{L}^1 \otimes (e^*\mathscr{L})_A$ the *Mumford construction* (this may be non-standard terminology). If $T = \mathrm{Spec}\, K$, which is all we need to consider to prove the homomorphism property, the Theorem of the Square asserts exactly the existence of an isomorphism

$$t_{x+y}^*(\mathscr{L}_K) \otimes \mathscr{L}_K^{-1} \simeq (t_x^*\mathscr{L}_K \otimes \mathscr{L}_K^{-1}) \otimes (t_y^*\mathscr{L}_K \otimes \mathscr{L}_K^{-1}).$$

Proof. Let $[x]$ be the composition $S := A_T \to T \xrightarrow{x} A$. Apply the Theorem of the Cube 3.1.6 to $S = A_T$, with $a_1 = p_1, a_2 = [x], a_3 = [y]$:

$$(p_1+[x]+[y])^*\mathscr{L} \otimes p_1^*\mathscr{L} \otimes x^*\mathscr{L} \otimes y^*\mathscr{L} \simeq (x+y)^*\mathscr{L} \otimes (p_1+x)^*\mathscr{L} \otimes (p_1+y)^*\mathscr{L} \otimes e^*\mathscr{L}_A^{-1}$$

You can check that $A_T \xrightarrow{t_x} A_T \to A \in A(A_T)$ is $\mathrm{pr}_1 + [x]$ and $[x]+[y] = [x+y]$ in $A(S)$. Therefore, the above isomorphism simplifies to say

$$t_{x+y}^*\mathscr{L}_T \otimes \mathscr{L}_T \otimes x^*\mathscr{L}_T \otimes y^*\mathscr{L}_T \simeq t_x^*\mathscr{L}_T \otimes t_y^*\mathscr{L}_T \otimes e^*\mathscr{L}_A^{-1}.$$

Rearranging this gives exactly what we wanted. □

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 $\mathscr{L}$ is ample then $\phi_{\mathscr{L}} : A \to \mathrm{Pic}^0_{A/k}$ is an *isogeny*. In fact, it is a special kind of isogeny to be called a *polarization*.

Remark 3.2.6. The map $\phi_{\mathscr{L}}$ does not "remember" $\mathscr{L}$. For instance, we will see that $\phi_{\mathscr{L}}$ is unaffected by translating $\mathscr{L}$ by a point in $\mathrm{Pic}^0_{A/k}(k)$. However, the map $\phi_{\mathscr{L}}$ turns out to be "more important" than $\mathscr{L}$.

For instance, when studying the Jacobian J of a smooth proper geometrically connected curve over k without a known rational point, one often finds finite Galois extensions K/k and line bundles $\mathscr{L}$ on A_K such that $\phi_{\mathscr{L}}$ descends to a k-homomorphism $A \to \mathrm{Pic}^0_{A/k}$ but $\mathscr{L}$ does *not* descend to a line bundle on A; such failure is due to obstructions in the Brauer group of k (so it is not detected for finite k, but is ubiquitious when k is a number field or even $\mathbf{R}$).

Proposition 3.2.7. *$\phi_{\mathscr{L}}(-x) = \phi_{\mathscr{L}^{-1}}(x)$ as maps $A \to \mathrm{Pic}^0_{A/k} =: \widehat{A}$.*

Proof. There are two ways of proving this. We could proceed functorially, but since it's just a question of equality of two maps we can also check it on geometric points. For $x \in A(\overline{k})$, we want $t_{-x}^*(\mathscr{L}) \otimes \mathscr{L}^{-1} \simeq t_x^*(\mathscr{L}^{-1}) \otimes \mathscr{L}$, or equivalently $t_{-x}^*\mathscr{L} \otimes t_x^*\mathscr{L} \simeq \mathscr{L} \otimes \mathscr{L}$. By the Theorem of the Square, the left side is precisely $t_{-x+x}^*(\mathscr{L}) \otimes \mathscr{L} \simeq \mathscr{L} \otimes \mathscr{L}$. □

Remark 3.2.8. We conclude that $\phi_{\mathscr{L}}$ is an isogeny if and only if $\phi_{\mathscr{L}^{-1}}$ is an isogeny, so it is an isogeny when $\mathscr{L}$ is either ample or anti-ample (see Remark 3.2.5).

Proposition 3.2.9. *We have $\phi_{\mathscr{L}_1 \otimes \mathscr{L}_2} = \phi_{\mathscr{L}_1} + \phi_{\mathscr{L}_2}$.*

Proof. For geometric points $x \in A$, $\phi_{\mathscr{L}_1 \otimes \mathscr{L}_2}(x) = t_x^*(\mathscr{L}_1 \otimes \mathscr{L}_2) \otimes \mathscr{L}_1^{-1} \otimes \mathscr{L}_2^{-1}$. Likewise the right side at x is $t_x^*\mathscr{L}_1 \otimes \mathscr{L}_1^{-1} \otimes t_x^*\mathscr{L}_2 \otimes \mathscr{L}_2^{-1}$. □

We defined $\mathscr{L} \rightsquigarrow \phi_{\mathscr{L}}$ for $\mathscr{L}$ on A. However, we can make an analogous definition for abelian schemes: for $\mathscr{L}$ on A_S, we can define a map

$$\phi_{\mathscr{L}} : A_S \to (\mathrm{Pic}_{A/k})_S$$

via $x \mapsto t_x^*(\mathscr{L}) \otimes \mathscr{L}^{-1}$, and this factors through $(\mathrm{Pic}^0_{A/k})_S$ for topological reasons on fibers over S. In addition, this is even a homomorphism (by the Theorem of the Square in a relative setting) but lies slightly beyond our setup since $\mathscr{L}$ doesn't begin life over A.

Remark 3.2.10. One can prove the Theorem of the Cube for a line bundle $\mathscr{L}$ on A_S (not pulled back from A) and thereby make a k-morphism

$$\mathrm{Pic}_{A/k} \to \underline{\mathrm{Hom}}(A, \mathrm{Pic}^0_{A/k})$$

via "$\mathscr{L} \mapsto \phi_{\mathscr{L}}$", expressing a precise sense in which $\phi_{\mathscr{L}}$ "varies nicely" with $\mathscr{L}$.

Theorem 3.2.11. *For $x \in A(k)$, $\phi_{t_x^*\mathscr{L}} = \phi_{\mathscr{L}}$ for $\mathscr{L}$ on A.*

Of course, the same holds true for any extension field K/k, $x \in A(K)$ and $\mathscr{L}$ on A_K.

Proof. It suffices to check the equality on $\overline{k}$-points, so assume $k = \overline{k}$. The claim is equivalent to

$$\phi_{t_x^*\mathscr{L}}(y) = \phi_{\mathscr{L}}(y).$$

This in turn is equivalent to

$$t_y^*(t_x^*\mathscr{L}) \otimes t_x^*\mathscr{L}^{-1} = t_y^*\mathscr{L} \otimes \mathscr{L}^{-1};$$

i.e., $t_{x+y}^*\mathscr{L} \otimes \mathscr{L} \simeq t_x^*\mathscr{L} \otimes t_y^*\mathscr{L}$. But that is precisely the Theorem of the Square. □

Remark 3.2.12. In the relative setting of abelian schemes, one proves a rigidification theorem to the effect that equality of maps can be checked on (geometric) fibers, and hence a lot of the basic relative theory of abelian schemes can be bootstrapped from the case of abelian varieties over fields.

Another Proof. Granting the existence of Hom-schemes for proper schemes over fields (as follows from Grothendieck's work under projectivity hypotheses, and exists as an algebraic space via work of Artin in general), we have a map $A \to \underline{\mathrm{Hom}}(A, \mathrm{Pic}^0_{A/k})$ carrying $x \in A(T)$ to $\phi_{t_x^*(\mathscr{L}_T)}$, so $e \mapsto \phi_{\mathscr{L}}$. It can be shown using rigidity methods for maps that the infinitesimal criterion for étaleness holds for this Hom-scheme/space, so as a map from a connected pointed k-scheme to an étale target, it must be a constant map to a k-point! □

Remark 3.2.13. This second proof illuminates the geometric content of the theorem, which is that a certain Hom-scheme/space is étale. For instance, if E is a non-CM elliptic curve then $\underline{\mathrm{Hom}}(E, E)$ is the constant scheme $\mathbf{Z}$.

Definition 3.2.14. If $\mathscr{L}$ is a line bundle on A, then we define

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

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

Remark 3.2.15. Note that

$$K(\mathscr{L}) = A \iff \phi_{\mathscr{L}} = 0 \iff t_x^*\mathscr{L}_{\overline{k}} \simeq \mathscr{L}_{\overline{k}} \text{ for all } x \in A(\overline{k}).$$

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

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

$$\theta : \mathscr{P}_A|_{\{0\}\times \mathrm{Pic}^0_{A/k}} \simeq \mathscr{O}_{\mathrm{Pic}^0_{A/k}}$$

is the universal rigidification along 0. Note that $\mathscr{P}_A|_{A\times\{0\}} \simeq \mathscr{O}_A$ by the very meaning of $0 \in \mathrm{Pic}^0_{A/k}(k)$. This isomorphism $\mathscr{P}_A|_{A\times\{0\}} \simeq \mathscr{O}_A$ has a $k^\times$-ambiguity, but we can make it canonical by requiring that on the k-point $(0,0)$ it agrees with the fiber of θ at that point.

The Poincaré bundle is the key to a symmetric relationship between A and $\mathrm{Pic}^0_{A/k}$, analogous to the evaluation pairing betwen a vector space and its dual. The universal property of the Poincaré bundle $\mathscr{P}_A$ over $A \times \mathrm{Pic}^0_{A/k}$ is that a map $f : T \to \mathrm{Pic}^0_{A/k} \subset \mathrm{Pic}_{A/k}$ is equivalent to a p_2-trivialized line bundle $\mathscr{M}$ on $A \times T$, where $f(t) = \mathscr{M}_t \in \mathrm{Pic}^0_{A/k}(k(t))$ on A_t. Therefore, $\phi_{\mathscr{L}}$ is determined by the line bundle

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

on $A \times A$. Informally, $\theta(\mathscr{L})|_{A\times\{x\}} = t_x^*(\mathscr{L}_K) \otimes \mathscr{L}_K^{-1}$ for $x \in A(K)$ (for extension fields K/k). Here is a very useful alternative description of the line bundle $\theta(\mathscr{L})$:

Proposition 3.3.1. *We have a canonical isomorphism*

$$(1 \otimes \phi_{\mathscr{L}})^*(\mathscr{P}_A) \simeq \Lambda(\mathscr{L}) := m^*(\mathscr{L}) \otimes p_1^*(\mathscr{L})^{-1} \otimes p_2^*(\mathscr{L})^{-1}$$

as $e \times 1_A$-trivialized line bundles.

Remark 3.3.2. The isomorphism is unique up to units from the base k. We remove that ambiguity by demanding that pulling back via $e \times 1_A$ respects the canonical trivializations on both sides: the definition of $\mathscr{P}_A$ includes a trivialization of $(1 \times \phi_{\mathscr{L}})^*(\mathscr{P}_A)$ after pulling back to via $e \times 1_A$, and pulling back the right side by $e \times 1_A$ gives the line bundle $\mathscr{L} \otimes (e^*\mathscr{L}^{-1})_A \otimes \mathscr{L}^{-1}$ on A that has a canonical isomorphism with $\mathscr{O}_A$.

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 a single algebraically closed field, which we may take to be $\overline{k}$.

To see why this follows from the Seesaw Theorem, for the "difference" of the two line bundles it suffices to check that if S is a geometrically reduced k-scheme (such as A) then a line bundle $\mathscr{M}$ on $A \times S$ is trivial if (and only if) it is trivial on $\{e\} \times S$ and $A \times \{x\}$ for all $x \in S(K)$. By the Seesaw theorem, the second triviality condition implies that $\mathscr{M}$ is pulled back from a line bundle on S, and the first condition guarantees that this line bundle on S is trivial. Alternatively, the first triviality condition says that $\mathscr{M}$ is classified by a map $S \to \mathrm{Pic}^0_{A/k}$, and the second says that all geometric points of S map to $0 \in \mathrm{Pic}^0_{A/k}$, hence the map $S \to \mathrm{Pic}^0_{A/k}$ is the trivial map (since S is geometrically reduced).

On $\{e\} \times A$, the left side is trivial because $\mathscr{P}_A$ is $e \times 1_A$-trivialized. On the right side, we get $\mathscr{L} \otimes (e^*\mathscr{L})_A^{-1} \otimes \mathscr{L}^{-1} \simeq \mathscr{O}_A$. On $A \times \{x\}$, the left side is $\theta(\mathscr{L})|_{A\times\{x\}} = t_x^*\mathscr{L}_K \otimes \mathscr{L}_K^{-1}$. On the right side, we get $t_x^*\mathscr{L}_K \otimes \mathscr{L}_K^{-1} \otimes (x^*\mathscr{L})_{A_K}^{-1}$. Again, these are identified because $x^*\mathscr{L}$ is trivial. □

We'll shortly use properties of $\phi_{\mathscr{L}}$ 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 better-suited to relative considerations (including descent theory), whereas Weil divisors are more like a crutch for computation. Since linearly equivalent divisors correspond to the same line bundle, they are less suitable for descent arguments (for example). Also, they don't work well beyond the theory over a field.

Theorem 3.4.1. *Any abelian variety A over a field k is projective.*

We want to reduce to the case where $k = \overline{k}$, since then we have lots of rational points to work with. That is accomplished by the following result.

Proposition 3.4.2. *For a proper k-scheme X, if $X_{\overline{k}}$ is projective over $\overline{k}$ then so is X over k.*

Remark 3.4.3. It is even enough that X_K is projective over K for *some* extension field K/k (not necessarily algebraic).

Proof. The goal is to build an ample line bundle $\mathscr{L}$ on X. To do this, choose a projective embedding $\overline{j}\colon X_{\overline{k}} \hookrightarrow \mathbf{P}^n_{\overline{k}}$. As this involves only a finite amount of data, and $\overline{k} = \varinjlim_{K/k \text{ finite}} K$, Exercise 1.7.9 implies that $\overline{j}$ descends to a closed immersion $X_K \hookrightarrow \mathbf{P}^n_K$ for some *finite, normal* K/k.

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

$$\begin{array}{c} K \\ \Big| \text{ purely inseparable} \\ K_0 \\ \Big| \text{ Galois} \\ k \end{array}$$

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 $f^{p^e} \in k$ for all $f \in K$. The upshot of that is as follows. If $\pi\colon X_K \to X$ is the projection, and $\mathscr{L}$ is a line bundle on X_K, then the transition functions of $\mathscr{L}$ are invertible functions on open subsets of X_K. If you raise these transition functions to the p^eth power, you still get gluing data for a line bundle, namely $\mathscr{L}^{p^e}$ (so ample if $\mathscr{L}$ is ample), but the transition functions arise from sections of $\mathscr{O}_X^\times \subset \pi_*(\mathscr{O}_{X_K}^\times)$ and hence this suggests that $\mathscr{L}^{p^e}$ is the pullback of a line bundle on X that we can hope to be ample.

Let us rigorously (and intrinsically) formulate this argument. We have a natural map $\iota\colon \mathscr{O}_X \hookrightarrow \pi_*\mathscr{O}_{X_K}$, and $t \mapsto t^{p^e}$ gives a map $\pi_*\mathscr{O}_{X_K}^\times \hookrightarrow \mathscr{O}_X^\times$ (as you can check locally over affines in X). Therefore, $\iota\colon \mathscr{O}_X^\times \hookrightarrow \pi_*(\mathscr{O}_{X_K}^\times)$ has cokernel killed by p^e. Now here is the key point (very useful in general settings): for any finite extension K/k (not assumed to be purely inseparable), a line bundle $\mathscr{L}$ on X_K is trivialized by an affine open cover *coming from* X. Indeed, for all $x \in X$ the ring $(\pi_*\mathscr{O}_{X_K})_x$ is *semi-local* (i.e. has finitely many maximal ideals), and we have the following lemma:

Lemma 3.4.4. *Any vector bundle M of constant fiber-rank $n > 0$ over a semi-local ring R is free.*

Proof. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$ be the maximal ideals of R, so $M/\mathfrak{m}_i M$ is an n-dimensional vector space over $R/\mathfrak{m}_i$. Let $\{m_{i1}, \ldots, m_{in}\}$ be a basis of $M/\mathfrak{m}_i M$ for each i.

We claim that for $j = 1, \ldots, n$ there exists $x_j \in M$ such that $x_j \equiv m_{ij} \pmod{\mathfrak{m}_i M}$ for each i. This is just the Chinese Remainder Theorem. The map $f : R^n \to M$ defined by $e_j \mapsto x_j$ is surjective modulo $\mathfrak{m}_i$, so it localizes to a surjective map $R^n_{\mathfrak{m}_i} \to M_{\mathfrak{m}_i}$ for each i by Nakayama's Lemma, and hence f is surjective. But M is a rank-n vector bundle, so f is an isomorphism. □

We conclude via "spreading out" from stalks on the target that for any finite flat (finitely presented) map, a line bundle upstairs trivializes Zariski-locally downstairs (although this is trivial to see in the inseparable case, since the map π is then a homeomorphism). In other words, there is an open cover $\{U_\alpha\}$ of X such that $\mathscr{L}$ is trivial on each $p_1^{-1}(U_\alpha)$. This implies that $\mathrm{Pic}(X_K) = H^1(X, \pi_*\mathscr{O}_{X_K}^\times)$ (which is *not* just general Leray nonsense because $\pi_*\mathscr{O}_{X_K}^\times$ is not quasicoherent). Thus, the cokernel of the map $H^1(X, \mathscr{O}_X^\times) \to H^1(X, \pi_*\mathscr{O}_{X_K}^\times)$ is identified with the natural map $\mathrm{Pic}(X) \to \mathrm{Pic}(X_K)$, so this latter map is killed by p^e. The upshot is that $\mathscr{L}^{p^e} \simeq \mathscr{N}_K$ for some line bundle $\mathscr{N}$ on X.

Since the line bundle $\mathscr{N}$ on X pulls back to an ample line bundle on X_K, $\mathscr{N}$ is ample on X because ampleness descends through ground field extension. There are various ways to see this; perhaps the cleanest is Serre's criterion: $\mathscr{N}$ is ample if and only if for any coherent sheaf $\mathscr{F}$ on X, any $i > 0$ and any sufficiently large m (largeness depending on $\mathscr{F}$ and i) we have

$$H^i(X, \mathscr{F} \otimes N^{\otimes m}) = 0.$$

But by flat base change,

$$H^i(X, \mathscr{F} \otimes \mathscr{N}^{\otimes m})_K = H^i(X_K, \mathscr{F}_K \otimes \mathscr{N}_K^{\otimes m})$$

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 Γ. Given $\mathscr{L}$ on X_K, we define $\mathscr{M} = \bigotimes_{\gamma \in \Gamma} \gamma^*(\mathscr{L})$; this is described as applying a ring-theoretic norm (through π) on transition functions. The line bundle $\mathscr{M}$ is ample, as each $\gamma^*\mathscr{L}$ is ample on X_K (being a pullback of the ample $\mathscr{L}$ by an automorphism of X_K over the automorphism γ of K) and a tensor product of ample line bundles is ample. There is an evident K/k-descent datum on $\mathscr{M}$, so $\mathscr{M} \simeq \mathscr{N}_K$ for a line bundle $\mathscr{N}$ on X, and ampleness of $\mathscr{M}$ on X_K is inherited by its descent $\mathscr{N}$ on X (by Serre's criterion, as above). □

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. The proof of this result from EGA II lies deeper than the preceding method which relied on the crutch of field extensions.

We conclude that for the purpose 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 desired 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* $\{x \in A(\overline{k}) \mid t_x^*(D_{\overline{k}}) = D_{\overline{k}}$ *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 $A(k)$ (which is geometrically obvious). Note that $t_x^* D = D \iff t_x^*(D) \subset D$, by finiteness of the number of irreducible components and dimensions. This condition says exactly that $x + d \in D$ 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 stabilizer 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 stabilizer (as we have here) and the last is ampleness, and the others are intermediate conditions that aren't so interesting on their own.

Proposition 3.4.8. *If $D \subset A$ is an effective reduced Weil divisor and $\mathcal{L} = \mathcal{O}(D) = \mathcal{I}_D^{-1}$, for an abelian variety A over $k = \overline{k}$. The following are equivalent:*

(1) $\{x \in A(\overline{k}) \mid t_x^*(D_{\overline{k}}) = D_{\overline{k}}\}$ *is finite;*
(2) $K(\mathcal{L}) = \{x \in A \mid t_x^* \mathcal{L} \simeq \mathcal{L}\}$ *is finite;*
(3) $\mathcal{L}^{\otimes 2}$ *has no basepoints (i.e.* $\mathcal{O}_A \otimes \Gamma(\mathcal{L}^{\otimes 2}) \twoheadrightarrow \mathcal{L}^{\otimes 2}$*) and the resulting k-morphism* $A \to \mathbf{P}(\Gamma(\mathcal{L}^{\otimes 2}))$ *is finite (equivalently quasi-finite, which is to say not contracting any curves);*
(4) $\mathcal{L}$ *is ample.*

Remark 3.4.9. (2) obviously implies (1), since $t_x^*(D_{\overline{k}}) = D_{\overline{k}}$ (equality of divisors, not just linear equivalence) obviously implies $t_x^* \mathcal{L} \simeq \mathcal{L}$ (and seems much stronger), but the two conditions are actually equivalent in this setting.

Proof. We're going to show that (3) $\Longrightarrow$ (4) $\Longrightarrow$ (2) $\Longrightarrow$ (1) $\Longrightarrow$ (3). The last step is the most geometric (no basepoints is easy, but the quasi-finiteness is not).

(3) $\Longrightarrow$ (4). For the finite map $\varphi: A \to \mathbf{P}(\Gamma(\mathscr{L}^{\otimes 2}))$, we have $\varphi^*(\mathscr{O}(1)) \simeq \mathscr{L}^{\otimes 2}$. 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 $H^i(A, \mathscr{F}) = H^i(\mathbf{P}(\Gamma(\mathscr{L}^{\otimes 2})), \varphi_*\mathscr{F})$ since φ is finite).

(4) $\Longrightarrow$ (2). The hypothesis in (4) ensures that A is projective, so Grothendieck's work on Picard schemes applies to A. In particular, $\phi_{\mathscr{L}}$ makes sense without needing to go beyond Grothendieck's existence results for Picard schemes. Let $B = (\ker \phi_{\mathscr{L}})^0_{\mathrm{red}}$, an abelian subvariety of A. Our task is exactly to show that $B = 0$.

By design, for all $b \in B(k)$ the map $\phi_{\mathscr{L}_b}: A \to \mathrm{Pic}_{A/k}$ is trivial, so $t_b^*\mathscr{L} \simeq \mathscr{L}$. Therefore, the pullback $\mathscr{L}_B$ on B has the property that $\phi_{\mathscr{L}_B} = 0$, and $\mathscr{L}_B$ is ample by hypothesis (since it is the restricton of an ample line bundle on A via $B \hookrightarrow A$). It remains to apply:

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

Proof. Since we're assuming the existence of an ample line bundle, so A is projective, Grothendieck's work on Picard schemes is applicable to $A \times A$. In particular, the Seesaw Theorem (whose proof was given using Picard schemes) applied to $A \times A$ only involves Grothendieck's existence results for Picard schemes (not the deeper results of Oort–Murre or Artin which avoid projectivity hypotheses), and the k-morphism $\phi_{\mathscr{L}}$ makes sense. We shall use the earlier result relating $\phi_{\mathscr{L}}$ and the Mumford construction:

$$(1 \times \phi_{\mathscr{L}})^*(\mathscr{P}_A) \simeq \Lambda(\mathscr{L}) = m^*\mathscr{L} \otimes p_1^*\mathscr{L}^{-1} \otimes p_2^*\mathscr{L}^{-1}$$

(see Proposition 3.3.1, whose proof rests on the Seesaw Theorem applied to $A \times A$).

Assuming $\phi_{\mathscr{L}} = 0$, we seek a contradiction. The left side is trivial on $A \times A$, so let's analyze the right side. Restricting to the anti-diagonal, we get

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

where $[-1]^*\mathscr{L}$ is ample, since $[-1]$ is an automorphism. Applying inversion to both sides, we see that the trivial line bundle is ample. The assumption that A supports an ample line bundle implies that A is projective. But $A \neq 0$, so by projectivity and slicing it A contains a curve, on which the structure sheaf is not ample (for degree reasons, or many other reasons). This is a contradiction. □

As mentioned, (2) $\Longrightarrow$ (1) is trivial.

Finally we show (1) $\Longrightarrow$ (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:

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

(ii) The morphism $f: A \to \mathbf{P}(\Gamma(\mathscr{L}^{\otimes 2}))$ defined on k-points by $a \mapsto (\Gamma(A, \mathscr{L}^{\otimes 2}) \twoheadrightarrow \mathscr{L}(a)^{\otimes 2})$ is finite, or equivalently doesn't contract any irreducible curve $C \subset A$.

To prove (i), we'll use the Theorem of the Square (resting on the Seesaw Theorem over algebraically closed fields, so see Remark 3.1.2!) to produce many effective divisors linearly equivalent to $2D$.

Assertion (i) is equivalent to the statement that for any $a \in A(k)$, there exists some effective $D' \sim 2D$ such that $a \notin \mathrm{supp}(D')$ (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, but translation is in the group law of A). So we just need to produce some x such that $a \notin t_x^*(D)$ and $a \notin t_{-x}^*(D)$. This is equivalent to $a \notin t_{-x}(D)$ and $a \notin t_x(D)$; i.e., $\pm x + a \notin D$, or equivalently $\pm x \notin -a + D = t_{-a}(D)$. 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 (ii), suppose to the contrary that some irreducible closed curve $C \subset A$ lies in a 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 $t_{\pm x}^*(D)$ 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., $C \subset t_{\pm x}^*(D)$ 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 $x \in \pm c_0 + D$ for all x, which is clearly impossible. □

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

Proof. Let $\mathscr{L} = \mathscr{O}(\Delta)$, so $\mathscr{L}|_C \simeq \mathscr{O}_C$. Consider $t_a^*(\mathscr{L})|_C$ for $a \in A(k)$. We claim that $\deg t_a^*(\mathscr{L})|_C$ 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, $m^*(\mathscr{L})|_{A \times C}$ is a line bundle on $A \times C \to A$. On the a-fiber, we get $t_a^*(\mathscr{L})|_C$. Now $A \times C \to A$ is a proper flat map, and it is a general fact that if $X \to S$ is a proper map to a connected, noetherian base and $\mathscr{F}$ is coherent and S-flat, then $\chi(\mathscr{F}_s)$ is independent of $s \in S$. As a special case, for a line bundles $\mathscr{N}$ on a scheme X proper and flat over S, $\chi(\mathscr{N}_s^{\otimes n})$ is independent of s. But for a curve, this is a polynomial in n of degree at most 1 whose linear coefficient reads off the degree of the line bundle (note the importance of being able to vary n in this argument). Hence, the degree of $t_a^*(\mathscr{L})|_C$ is independent of $a \in A(k)$ as claimed.

Geometrically, $t_a^*(\mathscr{L}) = \mathscr{O}(t_{-a}(\Delta))$ so $\mathscr{I}_{t_{-a}(\Delta)}|_C$ has degree 0 for all $a \in A$. If $C \cap t_{-a}(\Delta)$ were non-empty and finite, then $\mathscr{O}(t_{-a}(\Delta))|_C \simeq \mathscr{O}_C(C \cap t_{-a}(\Delta))$ would have positive degree, a contradiction. The upshot is that for each $a \in A(k)$, either C is disjoint from $t_{-a}(\Delta)$ or $C \subset t_{-a}(\Delta)$. 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 shall 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., $x+z \in t_y(\Delta)$. This 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. By effectivity, $D = \sum_i n_i D_i$ with $n_i > 0$ for all i. (Clearly $D \neq 0$, by the finiteness hypothesis.) Assume for some x_0 that C is *disjoint* from $t_{-x_0}^*(D) + t_{x_0}^*(D)$, so C is disjoint from $t_{\pm x_0}^*(D_i)$ for all i.

By Lemma 3.4.11, for all i, $t_{\pm x_0}^*(D_i)$ is preserved by t_{x-y}^* for all $x, y \in C$. Hence, D_i is preserved by t_{x-y}^* for all $x, y \in C$. Since $D = \sum n_i D_i$, we conclude that $t_{x-y}^*(D) = D$ for all $x, y \in C$, contradicting the finiteness hypothesis. □

We have finally proved that all abelian varieties are projective. Our proof did not require the existence of Picard schemes beyond the projective setting provided that in the proof of assertion (i) in the proof of "(1) ⇒ (3)" in Proposition 3.4.8 one appeals to a different proof of the Seesaw Theorem over algebraically closed fields (see Remark 3.1.2). Consequently, we now have the existence of $\mathrm{Pic}_{A/k}$ without needing to appeal to existence results for Picard schemes beyond Grothendieck's work in the projective case.

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

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

Theorem 4.1.1. *The map $[n]\colon A \to A$ is a 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 dense. Since $[n]$ is also proper, because A is, its image is closed and hence $[n]$ surjective. Quasi-finiteness and properness of $[n]$ would also yield finiteness of $[n]$. Therefore, if we grant the finiteness of $\ker([n])$ then for all $a \in A(k)$ we see that

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

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

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

$$\dim B = \dim A + \dim(B/f(\mathfrak{m}_A)B),$$

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? if $\mathrm{char}\, k \nmid n$ then $\mathrm{Lie}([n]) = n\colon T_e(A) \to T_e(A)$ (since $m : A \times A \to A$ induces addition on Lie algebras, as for any k-group scheme). This is an isomorphism, so the finite type k-group scheme $[n]^{-1}(0)$ has vanishing tangent space at the identity, so it is finite (and étale). If $p = \mathrm{char}(k) > 0$ then one might try to use this observation for n not divisible by p to deduce the result for n divisible by p, but we don't know the degree of $[n]$ for general n; maybe $[p]$ is an isomorphism?

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 $[n]^*\mathscr{L}$ for ample $\mathscr{L}$. This will come out of the following discussion.

Theorem 4.1.4. *We have*

$$\begin{aligned}[n]^*\mathscr{L} &\simeq \mathscr{L}^{\otimes \frac{n^2+n}{2}} \otimes ([-1]^*\mathscr{L})^{\otimes \frac{n^2-n}{2}} \\ &\simeq \mathscr{L}^{\otimes n} \otimes (\mathscr{L} \otimes [-1]^*\mathscr{L})^{\frac{n^2-n}{2}} \\ &\simeq \mathscr{L}^{\otimes n^2} (\mathscr{L} \otimes [-1]^*\mathscr{L}^{-1})^{\frac{n-n^2}{2}}.\end{aligned}$$

Remark 4.1.5. In the complex-analytic setting, where line bundles are described by linear algebraic data (Appel-Humbert Theorem), this becomes very concrete.

Proof. Note that the second and third lines are elementary. For $n = 0, 1$, the initial isomorphism 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).

For a general integer n, we apply the Theorem of the Cube with $a_1 = [n+2], a_2 = [1] = \mathrm{Id}, a_3 = [-1] = -\mathrm{Id}$ for $A(S)$ with $S = A$. Clearly

$$\begin{aligned} a_1 + a_2 + a_3 &= [n+1], \\ a_1 + a_2 &= [n+2], \\ a_1 + a_3 &= [n], \\ a_2 + a_3 &= [0], \end{aligned}$$

so the Theorem of the Cube gives

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

Rearranging so that there are only positive exponents, we have

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

for any integer n.

Exercise 4.1.6. Check that this relation is enough to conclude the result by inducting up and down in n.

□

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

$$\mathscr{O}_Z \simeq \mathscr{L}_Z^{\frac{n^2+n}{2}} \otimes ([-1]^*\mathscr{L})_Z^{\frac{n^2-n}{2}}$$

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

Rather generally, if Z is a proper (or just projective) scheme over a noetherian affine base $\mathrm{Spec}(A)$ and $\mathscr{O}_Z$ is ample, then Z is finite over the base. Indeed, Serre's vanishing theorem implies that twisting by $\mathscr{O}_Z$ eventually kills the higher cohomology of coherent sheaves, but this twisting does nothing, so the result follows from Serre's criterion for affineness and the coherence of higher direct images under proper morphisms then gives finiteness since $H^0(Z, \mathscr{O}_Z)$ is finite over A. This completes the proof that $A[n]$ is k-finite for all $n > 0$. □

Digression on ampleness. There are several possible definitions of ampleness for a line bundle $\mathscr{L}$ on a quasi-compact separated over a noetherian affine base $\mathrm{Spec}(A)$.

(1) The "correct" one is in EGA II, which we won't give. It looks frightening at first, but after some familiarity one realizes that it is quite elegant.
(2) The second is that $\mathscr{L}$ is the pullback of $\mathscr{O}(1)$ under some immersion into $\mathbf{P}^n_A$.
(3) The third 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 4.1.7. Ample symmetric line bundles $\mathscr{L}$ are to be regarded as analogous to positive-definite quadratic forms (an analogy that acquires concrete meaning in the complex-analytic theory, via the description of holomorphic line bundles on complex tori in terms of linear algebra data). Away from characteristic 2, recall that quadratic forms are closely related to symmetric bilinear forms.

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

Example 4.1.8. If $\mathrm{char}\, k \nmid n$, then $T_e(A[n]) = \ker(T_e(A) \xrightarrow{T_e([n])=n} T_e(A))$. This kernel is 0 if $\mathrm{char}\, k \nmid n$, so $A[n]_{\overline{k}}$ is a finite *constant* $\overline{k}$-scheme (by Nakayama's Lemma, and the homogeneity). Therefore, in this case $A[n]_{\overline{k}}$ is $\coprod_{\deg[n]} \mathrm{Spec}(\overline{k})$; i.e., $\#A(\overline{k})[n] = \deg([n])$. (This is very interesting for $A = \mathrm{Pic}^0_{X/k}$ for X a smooth projective curve.)

Theorem 4.1.9. *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 flat map, the degree is multiplied by the degree of the map.

Choose an ample line bundle $\mathscr{L}$ on A, and replace $\mathscr{L}$ with $\mathscr{L} \otimes [-1]^*\mathscr{L}$ so $\mathscr{L} \simeq [-1]^*\mathscr{L}$ (i.e., $\mathscr{L}$ is *symmetric*). Then

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

Now we want to compute the "degree" of both sides. This is the rate of growth of Euler characteristic of its powers: a polynomial in n whose leading coefficient encodes the degree in the following sense.

Definition 4.1.10. Let X be a proper k-scheme and $\mathscr{N}$ a line bundle on X. Let $\mathscr{F}$ be a coherent sheaf on X (typically $\mathscr{O}_X$, but there is purpose to this generality). Then we consider $\chi(\mathscr{F} \otimes \mathscr{N}^{\otimes r})$. This turns out to be a "numeric polynomial" in r of degree $\leq g \dim X$. ("Numeric polynomial in r" means that it's a polynomial in r whose values at integral values of r are integers; such things are integral linear combinations of binomial coefficients.) This has the form

$$\frac{d_{\mathscr{N}}(\mathscr{F})}{g!} r^g + (\text{lower-order terms})$$

for some $d_{\mathscr{N}}(\mathscr{F}) \in \mathbf{Z}$ (because when expressed in terms of binomial coefficients the leading-order term is $\binom{g+r}{r}$). When $\mathscr{F} = \mathscr{O}_X$, we call $d_{\mathscr{N}}(\mathscr{O}_X)$ the *degree* of $\mathscr{N}$; i.e.,

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

Reference: EGA III_1, 2.5.3.

Note that if we replace $\mathscr{N}$ by a positive power, then that is absorbed into r and hence appears in the leading coefficient; i.e., for $e \in \mathbf{Z}$,

$$\boxed{\deg(\mathscr{N}^e) = e^g \deg(\mathscr{N}).}$$

If $\mathscr{N}$ is ample then $\deg \mathscr{N} > 0$. One way to see this is that by raising to a large power, we can assume that $\mathscr{N}$ is very ample, in which case "degree" is the usual notion, namely the k-rank of the finite intersection with a generic codimension-g linear subspace. See EGA IV_2, 5.3 for an alternative argument.

Applying this in our situation, we find that

$$\deg([n]^*\mathscr{L}) = (n^2)^g \deg \mathscr{L} = n^{2g} \deg \mathscr{L} \neq 0.$$

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

Proposition 4.1.11. *Let $f : X' \to X$ be a finite map, with X proper and integral. Let d be the degree of the generic fiber. Then for all invertible $\mathscr{L}$ on X,*

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

Proof. This is matter of studying $\chi((f^*\mathscr{L})^{\otimes r}) = \chi(f^*(\mathscr{L}^{\otimes r}))$. Since cohomology interacts easily with pushforward under a finite map, this is the same as $\chi(f_*(f^*\mathscr{L}^{\otimes r})) = \chi(f_*(\mathscr{O}_{X'}) \otimes \mathscr{L}^{\otimes r})$ (by the projection formula). Here $\mathscr{F} = f_*(\mathscr{O}_{X'})$ is a coherent sheaf on X with generic stalk of rank d.

So we want to show that $\deg_{\mathscr{L}}(\mathscr{F}) = \mathrm{rank}(\mathscr{F}) \deg(\mathscr{L})$. More generally, we can assert this for $\mathscr{F} \in \mathrm{Coh}(X)$ with $\mathrm{rank}(\mathscr{F}) := \dim \mathscr{F}_\eta$ that

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

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

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

is short-exact, then $\mathscr{F}', \mathscr{F}'' \in \mathscr{C} \implies \mathscr{F} \in \mathscr{C}$. Grothendieck's unscrewing lemma (EGA III_1, 3.1.2) says: if $\mathscr{C}$ is an exact (meaning closed in short exact sequences, as above) full subcategory of $\mathbf{Coh}(X)$, then $\mathscr{C} = \mathbf{Coh}(X)$ provided that for all irreducible and reduced closed subschemes $Y \subset X$ there exists $\mathscr{G}_Y \in \mathscr{C}$ with $\mathrm{supp}(\mathscr{G}_Y) = Y$ and $\mathrm{rank}(\mathscr{G}_Y) = 1$ (e.g. $\mathscr{G}_Y = \mathscr{O}_Y$). [The proof is an elaborate filtration argument.]

To apply the unscrewing lemma, it suffices to check the hypothesis using $\mathscr{G}_Y = \mathscr{O}_Y$: for $Y = X$ this is the definition of degree, and for $Y \subsetneq X$ both sides are 0. □

Remark 4.1.12. In fact, with a bit more technique we can push through the preceding result requiring only that f is generically finite (i.e., finite over a dense open subset of X, or equivalently has finite generic fiber). This goes as follows.

Using the Leray spectral sequence

$$H^i(X, R^j f_*(\mathscr{G})) \Rightarrow H^{i+j}(X', \mathscr{G})$$

for any $\mathscr{O}_{X'}$-module $\mathscr{G}$, we see that if $\mathscr{G}$ is coherent then $\chi(\mathscr{G}) = \sum(-1)^j \chi(R^j f_*(\mathscr{G}))$. Setting $\mathscr{G}$ to be $(f^*\mathscr{L})^{\otimes r}$, we have $R^j f_*(\mathscr{G}) = R^j f_*(\mathscr{O}_{X'}) \otimes \mathscr{L}^{\otimes r}$. Thus,

$$\chi((f^*\mathscr{L})^{\otimes r}) = \sum (-1)^j \chi(R^j f_*(\mathscr{O}_{X'}) \otimes \mathscr{L}^{\otimes r}).$$

By generic finiteness, the coherent higher direct images $\mathscr{F}_j := R^j f_*(\mathscr{O}_{X'})$ have vanishing generic stalk when $j > 0$, so their rank is 0. Now we can use the result shown in the preceding proof via the unscrewing lemma to conclude that the Euler characteristics for $j > 0$ vanish and thus

$$\chi((f^*\mathscr{L})^{\otimes r}) = \chi(f_*(\mathscr{O}_{X'}) \otimes \mathscr{L}^{\otimes r}) = d\,\chi(\mathscr{L}^{\otimes r})$$

where d is the rank of the finite generic fiber of f. It follows that $\deg(f^*\mathscr{L}) = d \deg(\mathscr{L})$. In case f is not dominant, we have $d = 0$ and thus $\deg(f^*\mathscr{L}) = 0$.

4.2. **Structure of the torsion subgroup.** Now we investigate the structure of $A(K)[n] = A[n](K)$ for extension fields K/k.

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*

$$G[a] \times G[b] \xrightarrow{m} G$$

is an isomorphism.

Proof. For any S-scheme T, $G(T)$ is a $\mathbf{Z}/n\mathbf{Z}$-module. Hence, $G(T) = G(T)[a] \times G(T)[b]$ via $\mathbf{Z}/n\mathbf{Z} = \mathbf{Z}/a\mathbf{Z} \times \mathbf{Z}/b\mathbf{Z}$ (this is just a fact about all $\mathbf{Z}/n\mathbf{Z}$ modules). That completes the proof, by the "functor of points" perspective. □

Here is an interesting application of the preceding lemma. If $G \to S$ as in the lemma is finite and locally free ("$\mathscr{O}_G$ is a vector bundle over $\mathscr{O}_S$-module of finite rank"), then the same is for $G[a], G[b]$ because the identity section splits off a trivial summand of $\mathscr{O}_{G[b]}$; i.e., the isomorphism

$$\mathscr{O}_{G[a]} \otimes \underbrace{\mathscr{O}_{G[b]}}_{\mathscr{O}_S \oplus \ldots} = \mathscr{O}_G$$

exhibits $\mathscr{O}_{G[a]} \otimes \mathscr{O}_S \simeq \mathscr{O}_{G[a]}$ as a direct summand of a vector bundle, and likewise for $G[b]$. Hence, $G[a]$ and $G[b]$ are each finite locally free over S as well!

Proposition 4.2.2. *If* $\mathrm{char}\ k \nmid n$ *then* $A[n](\overline{k}) \simeq (\mathbf{Z}/n\mathbf{Z})^{2g}$.

Proof. By the lemma, we may assume that $n = \ell^e$ where $\ell \neq \mathrm{char}\ k$ and $e \geq 1$. We are claiming that $A[\ell^e](\overline{k}) \simeq (\mathbf{Z}/\ell^e\mathbf{Z})^{2g}$ and the "multiplication by ℓ" map $A[\ell^e](\overline{k}) \to A[\ell^{e-1}](\overline{k})$ for $e > 1$ makes the following diagram commute:

$$\begin{array}{ccc} A[\ell^e](\overline{k}) & \xrightarrow{\simeq} & (\mathbf{Z}/\ell^e\mathbf{Z})^{2g} \\ \Big\downarrow{\scriptstyle \ell} & & \Big\downarrow{\scriptstyle \text{reduction}} \\ A[\ell^{e-1}](\overline{k}) & \xrightarrow{\simeq} & (\mathbf{Z}/\ell^{e-1}\mathbf{Z})^{2g}. \end{array}$$

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

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

Thus, by induction $\#A[\ell^e](\overline{k}) = \#A[\ell](\overline{k})^e$. But the structure of finite abelian ℓ-groups shows that $A[\ell^e](\overline{k})$ is a quotient of $(\mathbf{Z}/\ell^e\mathbf{Z})^d$ with $\ell^d = \#A[\ell](\overline{k})$, so by cardinality reasons this quotient map is an isomorphism. So we know what we want up to proving $\dim_{\mathbf{F}_\ell} A[\ell](\overline{k}) = 2g$ (the base case).

So far everything has just been pure group theory, and in particular the discussion applies to any prime ℓ. It only remains to show that $[\ell]\colon A \to A$ of degree ℓ^{2g} is separable on function fields when $\ell \neq \mathrm{char}(k)$, as that would imply (by elementary "spreading out" from the generic fiber via denominator-chasing) that the geometric fibers have size ℓ^{2g} over some dense open subset of the target. Then homogeneity implies all geometric fibers of $[\ell]$ have the same size ℓ^{2g} (we wanted this for the fiber $[\ell]^{-1}(0) = A[\ell]$).

Since $[\ell]$-pullback on rational functions induces a field extension $k(A) \to k(A)$ of degree ℓ^{2g}, if $\ell \neq \mathrm{char}\ k$ then this is not divisible by char k and hence is separable. □

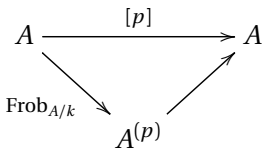
What if $\ell = p = \mathrm{char}\ k$? We expect, even from the theory of elliptic curves, that the torsion may have fewer geometric points.

Proposition 4.2.3. *If k has characteristic $p > 0$ then* $\dim_{\mathbf{F}_p} A[p](\overline{k}) \leq g$ *(so $A[p^e](\overline{k}) \simeq (\mathbf{Z}/p^e\mathbf{Z})^i$ for all $e \geq 1$ and some $i \leq g$).*

General setup: let $f\colon X \twoheadrightarrow Y$ be a finite surjection between geometrically integral k-schemes of finite type. Then there exists a dense open subset $U \subset Y$ such that for all $u \in U(\overline{k})$, $\#X_u(\overline{k}) = \deg_s(f)$.

Exercise 4.2.4. Prove this. Reduce to the case $k = \overline{k}$ and then use the tower $k(X)/K/k(Y)$ with K the separable closure of $k(Y)$ in $k(X)$. Denominator-chasing spreads out this tower over a dense open in Y with finite flat ring extensions.

We want the factor $\deg_s([p]_A)$ of $\deg([p]_A) = p^{2g}$ 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 function field extension. The general intuition (and "correct argument") is that for a general commutative group scheme, multiplication by p always factors through Frobenius:



and $\mathrm{Frob}_{A/k}$ has degree p^g because A is (by smoothness) Zariski-locally étale over the affine space $\mathbf{A}^g$.

We'll use a different argument. Without loss of generality we can assume that $k = \overline{k}$. We'll show that the field extension induced by $[p]^*$ factors as

$$\underbrace{k(A) \subset k(A)^p \subset k(A)}_{[p]^*},$$

where the second inclusion is clearly purely inseparable and has degree p^g (due to a separating transcending basis of $k(A)/k$, which always exist over a perfect field such as $k = \overline{k}$; work out the details as an exercise).

In our case, why does $[p]^*$ factor through this subfield? This rests on:

Proposition 4.2.5. *The universal differential $d\colon k(A) \to \Omega^1_{k(A)/k}$ has as kernel exactly $k(A)^p$.*

Proof. HW4. □

Remark 4.2.6. The validity of this proposition requires k to be perfect (we have arranged $k = \overline{k}$) since any element of k is killed by d.

To exploit our knowlede of the kernel of d, it suffices to prove $d([p]^* f) = 0$ for all $f \in k(A)$. Certainly $d([p]^* f) = [p]^*(df)$. Thus, it suffices to prove that the natural map of sheaves $\Omega^1_{A/k} \to [p]_*\Omega^1_{A/k}$ induced by $[p] : A \to A$ vanishes. What is it about the group scheme A that allows us to get a handle on multiplication by p? The key is that the sheaf of 1-forms is generated by global invariant 1-forms that in turn are determined by their value at the origin (as with Lie groups) yet the effect of $[p]$ between (co)tangent spaces is 0 since $p = \mathrm{char}(k)$. To carry out this ideas, we need:

Definition 4.2.7. Let G be a k-group scheme locally of finite type, and $\ell_g\colon G_T \to G_T$ the left-multiplication map $\ell_g(x) = g \cdot x$ for k-schemes T and $g \in G(T)$. We say that $\omega \in \Omega^1_{G/k}(G)$ is *left-invariant* if $\ell_g^* \omega_T = \omega_T$ for all k-schemes T and $g \in G(T)$. We denote the k-vector space of left-invariant 1-forms on G by $\Omega^{1,\ell}_{G/k}$.

Theorem 4.2.8. *Let G be a group scheme locally of finite type over k and $\mathfrak{g} = T_e G$. Then evaluation at e defines a k-linear isomorphism $\Omega^{1,\ell}_{G/k} \simeq \mathfrak{g}^*$, and the resulting map of $\mathcal{O}_G$-modules $\mathcal{O}_G \otimes \mathfrak{g}^* \to \Omega^1_{G/k}$ is an isomorphism.*

In HW4 one is led through a proof of this important fact. Note that for smooth G, the left-invariance can be checked using just $T = \mathrm{Spec}\ \overline{k}$. It is easy to show that the map $\Omega^{1,\ell}_{G/k} \to \mathfrak{g}^*$ is injective. The surjectivity is harder, and is explained in the book "Néron Models". (It is remarkable that smoothness is not necessary.)

By Theorem and dualizing $\mathfrak{g}^*$, to prove $[p]$-pullback kills the sheaf of 1-forms it suffices to show that the tangent map $T_e([p])\colon T_e(A) \to T_e(A)$ vanishes. But this effect is multiplication by p (as for any commutative group scheme, on which "the derivative of multiplication is addition';), so it vanishes on any k-vector space since $p = \mathrm{char}\ k$. This concludes the proof of Proposition 4.2.3.

Remark 4.2.9. The preceding argument gives a bit more: we claim it yields that $[p]$ factors through $\mathrm{Frob}_{A/k}$. Such a factorization is initially obtained at the level of function fields, and hence as dominant rational maps. To obtain a factorization globally, we just need to relate "dominant rational homomorphisms" between smooth group varieties to actual (dominant) homomorphisms of group varieties.

In general, suppose $f\colon G \dashrightarrow H$ is a dominant rational map between smooth group varieties. We call it a "rational homomorphism" if the diagram of dominant rational

maps

$$\begin{array}{ccc} G \times G & \overset{f\times f}{\dashrightarrow} & H \times H \\ {\scriptstyle m_G}\downarrow & & \downarrow{\scriptstyle m_H} \\ G & \dashrightarrow & H \end{array}$$

commutes. (In general we cannot compose rational maps, but in the *dominant* case we can compose them.) The general fact we want is that such a rational homomorphism is defined everywhere. Over a separably closed field there are enough rational points (by smoothness) to make the desired global homomorphism via translation by rational points. Then we can pull down the result from k_s via Galois descent.

For prime ℓ, define the ℓ-adic Tate module

$$T_\ell(A) = \varprojlim_n A[\ell^n](\overline{k}) \simeq \begin{cases} \mathbf{Z}_\ell^{2g} & \ell \neq \mathrm{char}\ k, \\ \mathbf{Z}_\ell^i,\ i \leq g & \ell = \mathrm{char}(k). \end{cases}$$

Let $V_\ell(A) = T_\ell(A)[1/\ell]$. If $\ell \neq \mathrm{char}\ k$, then our arguments above show that the finite k-group scheme $A[\ell^n]$ has vanishing tangent space at the identity point, so it is étale at the identity and hence étale everywhere (as we may prove over $\overline{k}$ via translation arguments). Thus, $A[\ell^n](\overline{k}) = A[\ell^n](k_s)$ for such ℓ, so $T_\ell(A) = \varprojlim A[\ell^n](k_s)$ when $\ell \neq \mathrm{char}\ k$. There is a natural *continuous* action of $\mathrm{Gal}(k_s/k)$ on $T_\ell(A)$ (continuous because every point in $A[\ell^n](k_s)$ is defined over some finite separable extension of k).

These Tate modules are analogues of $H_1(A, \mathbf{Z}_\ell)$ for $k = \mathbf{C}$. We'll study the map

$$\mathbf{Z}_\ell \otimes \mathrm{Hom}_k(A, B) \to \mathrm{Hom}_{\mathbf{Z}_\ell[\mathrm{Gal}]}(T_\ell(A), T_\ell(B))$$

in order to control $\mathrm{Hom}_k(A, B)$ and $\mathbf{Q} \otimes_{\mathbf{Z}} \mathrm{End}_k(A)$.

Remark 4.2.10. If we know $\mathbf{Z}_\ell \otimes_{\mathbf{Z}} \mathrm{Hom}(A, B) \to \mathrm{Hom}(T_\ell A, T_\ell B)$ is injective (which will be proved later) then the isomorphism $\mathbf{Z}_\ell \otimes_{\mathbf{Z}} \mathrm{Hom}(A, B) \simeq \mathbf{Z}_\ell \otimes_{\mathbf{Z}_{(\ell)}} \mathrm{Hom}(A, B)_{(\ell)}$ shows that $\mathrm{Hom}(A, B)_{(\ell)}$ is $\mathbf{Z}_{(\ell)}$-finite for $\ell \neq \mathrm{char}\ k$, by an exercise of chasing elementary tensors (which has a high-brow interpretation as fpqc descent).

This does not *formally* imply that $\mathrm{Hom}(A, B)$ is $\mathbf{Z}$-finite. For instance, letting $M = \sum_{p \neq 7,13} \frac{1}{p}\mathbf{Z} \subset \mathbf{Q}$, we see that $M_{(\ell)}$ is $\mathbf{Z}_{(\ell)}$-finite for all ℓ (if $\ell \neq 7, 13$, then $M_{(\ell)} \simeq \frac{1}{\ell}\mathbf{Z}_{(\ell)}$, and if $\ell = 7, 13$ then we just get $\mathbf{Z}_\ell$).

To prove that $\mathrm{Hom}(A, B)$ *is* $\mathbf{Z}$-finite, we'll therefore need to go beyond ℓ-adic considerations. The key is to use some "positivity" input via ample line bundles (and duality). For this, we require 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 an elliptic curve is naturally its own dual.

Remark 4.2.11. The additive group $\mathrm{Hom}(A,B)$ is torsion-free. Indeed, suppose $A \xrightarrow{f} B \xrightarrow{[n]_B} B$ is trivial with an integer $n \neq 0$. But this also factors as

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle [n]_A}\downarrow & & \downarrow{\scriptstyle [n]_B} \\ A & \xrightarrow{f} & B \end{array}$$

and we know that $[n]_A$ is surjective, so the vanishing of the composition holds if and only if $f = 0$.

5. The dual abelian variety

5.1. **Smoothness.** We need to do two things:

(1) Understand properties of $\mathrm{Pic}^0_{A/k} =: \widehat{A}$.
(2) Understand properties of the map $\phi_{\mathscr{L}}: A \to \mathrm{Pic}^0_{A/k}$ defined by $x \mapsto t_x^*(\mathscr{L}) \otimes \mathscr{L}^{-1}$, *especially* for ample $\mathscr{L}$. These are examples of "polarizations."

For (1), since A is smooth, projective, and geometrically integral, one knows by HW1 that $\mathrm{Pic}^0_{A/k}$ is proper and geometrically irreducible. (In general, homework exercise says that the identity component of a group scheme locally of finite type is of finite type, but that is obvious for Picard schemes since Grothendieck's construction exhibits the Picard scheme as a countably infinite disjoint union of quasi-projective schemes.) We don't yet know about its smoothness or dimension. This is a serious concern, because the Picard scheme can be non-reduced in general (even for smooth projective surfaces in positive characteristics), but we will see that for abelian varieties it is always smooth of dimension $g = \dim A$ (in every characteristic).

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. Instead, we will study $T_0(\mathrm{Pic}^0_{A/k}) = T_0(\mathrm{Pic}_{A/k}) \simeq H^1(A, \mathscr{O}_A)$ (last equality by HW1). Choose $\mathscr{L}$ ample and consider $\phi_{\mathscr{L}}: A \to \mathrm{Pic}^0_{A/k} \subset \mathrm{Pic}_{A/k}$.

We know $\phi_{\mathscr{L}}$ has finite fibers (because $\ker \phi_{\mathscr{L}}$ is finite for ample $\mathscr{L}$, as $\ker \phi_{\mathscr{L}} \circ [n] = \phi_{\mathscr{L}^n}$ and $\mathscr{L}^n = \mathscr{O}_A(D)$ for an effective D when n is large), so it is a finite morphism by properness. It follows from quasi-finiteness that $\dim \mathrm{Pic}^0_{A/k} \geq g$. So for smoothness, it suffices to show that $\dim H^1(A, \mathscr{O}_A) \leq g$. This would also automatically imply that $\dim \mathrm{Pic}^0_{A/k} = g$, and that the finite $\phi_{\mathscr{L}}$ is surjective and hence flat (by generic flatness plus homogeneity considerations over $\overline{k}$).

Mumford takes a rather indirect approach to this calculation in [Mum], using a gritty calculation with Koszul complexes. We'll describe another method, which is more sophisticated but also more conceptual.

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

Proof. The strategy is to reduce this to a structure theorem of Borel applied to the (coherent) cohomology ring of A. Borel was studying the structure of the cohomology ring of compact Lie groups, which has a graded Hopf algebra structure.

Let $R = \bigoplus_i H^i(A, \mathscr{O}_A)$. This is $\mathbf{Z}_{\geq 0}$-graded, and $R^i = 0$ for $i > g$. This has an anti-commutative cup product $R \otimes_k R \to R$ denoted $a \otimes b \mapsto a \smile b$ such that if $a \in R^i$ and $b \in R^j$ then $a \smile b \in R^{i+j}$ and $(b \smile a) = (-1)^{ij} a \smile b$. Furthermore, $R^0 = k$, and we can say something about the top piece $R^g = H^g(A, \mathscr{O}_A)$: since $\Omega^1_{A/R} \simeq \mathscr{O}_A \otimes \mathrm{Lie}(A)^*$, so $\Omega^g_{A/k} \simeq \mathscr{O}_A$ (non-canonically), we have $R^g = H^g(A, \Omega^g_{A/k})$. But that is 1-dimensional over k by Serre duality. Likewise, 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).

So far the group structure of A has been used just to verify that the tangent bundle is globally free. Now we use the group structure in a more direct manner: using the

diagram

$$A \rightrightarrows A \times A \xrightarrow{m} A$$

where the inclusions are along the identity elements ($a \mapsto (a,0)$ and $a \mapsto (0,a)$), we get a diagram

$$H^\bullet(A, \mathscr{O}_A) \leftleftarrows H^\bullet(\mathscr{O}_{A\times A}) \xleftarrow{m^*} H^\bullet(A, \mathscr{O}_A).$$

We shall combine this with the Künneth formula for $H^\bullet(\mathscr{O}_{A\times A})$: for schemes X and Y over a commutative ring k and sheaves of modules $\mathscr{F}$, $\mathscr{G}$ on X, Y respectively, cup product defines a map

$$H^\bullet(X \times_{\mathrm{Spec}\, k} Y, p_1^*\mathscr{F} \otimes p_2^*\mathscr{G}) \xleftarrow{\smile} H^\bullet(X, \mathscr{F}) \otimes_k H^\bullet(Y, \mathscr{G})$$

and by a Cech-theoretic computation this is an isomorphism when everything is flat over k (the sheaves and their cohomology). Thus, over a field k the cohomology ring of the structure sheaf on $X \times Y$ is the graded tensor product of the cohomology rings of the structure sheaves on X and Y.

Applying this to $X = Y = A$, we obtain factorizations of the identity:

$$R \leftleftarrows R \otimes R \xleftarrow{\mu} R$$

(tensor product as graded associative k-algebras) where μ is a k-algebra map giving R a structure of Hopf algebra over k and the two left maps use that $R^0 = k$. We conclude that $\mu(x) = x \otimes 1 + 1 \otimes x +$(higher degree terms) for all x. We may then conclude via the following structure theorem of Borel. □

Theorem 5.1.2 (Borel)**.** *Let R be a finite-dimensional $\mathbf{Z}_{\geq 0}$-graded associative Hopf algebra over a field k such that $R^0 = k$, $\dim R^g = 1$, and $R^j = 0$ for all $j > 0$. Assume multiplication $R^i \times R^{g-i} \to R^g$ is a perfect pairing for $0 \leq i \leq g$. Then*

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

and equality holds if and only if the natural map $\bigwedge^\bullet(R^1) \to R$ is an isomorphism.

Proof. Without loss of generality, $k = \overline{k}$. Over perfect fields Borel proved a general structure theorem for Hopf algebras that gives this result as a special case; see Lemma 15.2 in Milne's article "Abelian Varieties" (in the book *Arithmetic Geometry*) and the handout on Borel's structure theorem for details on this result. □

The preceding proof yields the additional fact that $\wedge^i(H^1(A, \mathscr{O}_A)) \to H^i(A, \mathscr{O}_A)$ via cup product is an isomorphism for all $0 \leq i \leq g$, which Mumford proves directly in [Mum]. In the analytic theory we have a much easier analogous result for cohomology with constant coefficients since a complex torus is a product of circles.

The smoothness result above allows us to finally define the dual:

Definition 5.1.3. If A is an abelian variety over k, the *dual abelian variety* $A^\vee$ is $\mathrm{Pic}^0_{A/k}$.

5.2. **Characterization of $\phi_{\mathscr{L}}$.** For ample $\mathscr{L}$, we have seen that $\phi_{\mathscr{L}}: A \to \widehat{A}$ is an isogeny (a finite flat surjective homomorphism). We can use a single ample line bundle to characterize the line bundles in the identity component of the Picard scheme (i.e., to describe the field-valued points of the dual abelian variety):

Lemma 5.2.1. *For ample $\mathscr{N}$ on A, a line bundle $\mathscr{M} \in \mathrm{Pic}(A) = \mathrm{Pic}_{A/k}(k)$ lies in $\mathrm{Pic}^0_{A/k}(k) = \widehat{A}(k)$ if and only if $\mathscr{M}_{\overline{k}} \simeq \phi_{\mathscr{N}}(x) = t_x^*(\mathscr{N}_{\overline{k}}) \otimes \mathscr{N}_{\overline{k}}^{-1}$ for some $x \in A(\overline{k})$.*

Proof. This just expresses that the map $\phi_{\mathscr{N}}: A \to \mathrm{Pic}_{A/k}$ has image $\mathrm{Pic}^0_{A/k}$ and so is surjective on $\overline{k}$-points. (We emphasize that x might *not* be found in $A(k)$.) □

Here is a more useful refinement:

Proposition 5.2.2. *If $\mathscr{M} \in \mathrm{Pic}^0_{A/k}(k)$, then $\phi_{\mathscr{M}} = 0$.*

The converse will be proved shortly, but lies deeper.

Proof. Without loss of generality $k = \overline{k}$. Let $\mathscr{N}$ be an ample line bundle on A. By the preceding lemma, $\mathscr{M} \simeq t_x^*\mathscr{N} \otimes \mathscr{N}^{-1}$ for some $x \in A(k)$, so for any $y \in A(k)$ we have as points of $\mathrm{Pic}(A)$ that

$$\begin{aligned}\phi_{\mathscr{M}}(y) &= t_y^*(\mathscr{M}) \otimes \mathscr{M}^{-1} \\ &= t_{x+y}^*\mathscr{N} \otimes t_y^*\mathscr{N}^{-1} \otimes t_x^*\mathscr{N}^{-1} \otimes \mathscr{N} \\ &= \mathscr{O}_A,\end{aligned}$$

the final equality by the Theorem of the Square. □

An alternative proof of the vanishing of $\phi_{\mathscr{M}}$ for $\mathscr{M} \in \mathrm{Pic}^0_{A/k}(k)$ is outlined on the homework, and provides illuminating geometric insight into this result. The idea is to view the construction $\mathscr{M} \mapsto \phi_{\mathscr{M}}$ as arising from a morphism of k-schemes $\mathrm{Pic}_{A/k} \to \underline{\mathrm{Hom}}(A, \widehat{A})$, where the target Hom-scheme is étale (by rigidity considerations, and the infinitesimal criterion). This expresses that $\phi_{\mathscr{M}}$ is a "discrete" invariant of $\mathscr{M}$, and more specifically the identity component $\mathrm{Pic}^0_{A/k}$ must get crushed to a single k-point under any such k-morphism (so the vanishing of $\phi_{\mathscr{O}_A}$ then does the job).

Now we prepare to prove the converse result. On $A \times \widehat{A}$, we have the Poincaré bundle $\mathscr{P}_A$ that is the restriction of the universal (rigidified) line bundle on $A \times \mathrm{Pic}_{A/k,e}$. This is equipped with an $(e \times 1)$-trivialization by the rigidification data, and it has a $(1 \times \widehat{e})$-trivialization by definition of $\widehat{e}$ corresponding to the trivial bundle of $\mathrm{Pic}_{A/k,e}$; the latter trivialization is uniquely determined upon scaling it by $k^\times$ to be compatible with the first trivialization at the point $(e, \widehat{e})$.

Using these two trivialization, a symmetric relationship between A and its dual is set up as follows. For the flip isomorphism $\sigma: \widehat{A} \times A \simeq A \times \widehat{A}$ we have that $\sigma^*(\mathscr{P}_A)$ is line bundle on $\widehat{A} \times A$ trivialized along $\widehat{e} \times 1$. Thus, by the universal property of the Picard scheme $\mathrm{Pic}_{\widehat{A}/k,\widehat{e}}$ this rigidified line bundle is classified by a map $A \to \mathrm{Pic}_{\widehat{A}/k}$ satisfying $e \mapsto 0$. This map then factors through the identity component, so it is a pointed map $\iota_A: A \to \widehat{\widehat{A}}$. Being a pointed map between abelian varieties, ι_A is a homomorphism.

More generally, for abelian varieties X and Y, a line bundle on $X \times Y$ equipped with trivializations along the identity sections of the factors (which can be arranged to be compatible at $(0,0)$) yields homomorphisms $X \to \widehat{Y}$ and $Y \to \widehat{X}$.

In §7.3 we will see that ι_A is an isomorphism, and in the homework you will show that $(\iota_A)^\wedge = i_{\widehat{A}}^{-1}$. The relationship between an abelian variety and its dual is analogous to the relationship between a finite-dimensional vector space and its dual, and the Poincaré line bundle is analogous to the evaluation pairing. This analogy will be addressed in some detail when we study the notion of "symmetric homomorphism" in §7.4.

Remark 5.2.3. Much as the formation of a dual vector space is compatible with finite direct sums, we will see in the homework that the formation of the dual abelian variety Pic^0 is compatible with direct products of abelian varieties. But beware that this compatible it is not true for the entire Picard scheme! Roughly speaking, $\mathrm{Pic}_{A/k}$ has "quadratic" behavior in A that isn't seen on the identity component. This is analogous to the fact that for $k = \mathbf{C}$, the component group of $\mathrm{Pic}_{A/\mathbf{C}}(\mathbf{C})$ is $H^2(A(\mathbf{C}), \mathbf{Z}) = \wedge^2(H^1(A(\mathbf{C}), \mathbf{Z}))$ via the analytic theory.

Theorem 5.2.4. *If $\phi_{\mathscr{L}} = 0$, then $\mathscr{L}_{\overline{k}} \simeq \phi_{\mathscr{N}}(x)$ for some $x \in A(\overline{k})$. In other words, $\mathscr{L} \mapsto \phi_{\mathscr{L}}$ induces an injective homomorphism*

$$\mathrm{Pic}_{A/k}(\overline{k})/\mathrm{Pic}^0_{A/k}(\overline{k}) \hookrightarrow \mathrm{Hom}_{\overline{k}}(A_{\overline{k}}, \widehat{A}_{\overline{k}}),$$

or equivalently a closed k-subgroup inclusion between étale k-groups

$$\mathrm{Pic}_{A/k}/\mathrm{Pic}^0_{A/k} \to \underline{\mathrm{Hom}}(A, \widehat{A}).$$

In other words, $\phi_{\mathscr{L}}$ detects whether or not you can "continuously deform" one line bundle to another; i.e., how we can move around continuously in the moduli space of line bundles on A.

Proof. We may assume without loss of generality that $k = \overline{k}$. The idea is to put the collection of line bundles $\{t_x^*\mathscr{N} \otimes \mathscr{N}^{-1} \otimes \mathscr{L}^{-1}\}_{x \in A(k)}$ into a "family" over A; i.e., to make a line bundle $\mathscr{K}$ on $A \times A$ such that $\mathscr{K}|_{\{x\} \times A} \simeq t_x^*\mathscr{N} \otimes \mathscr{N}^{-1} \otimes \mathscr{L}^{-1}$ for all x, and we will get a contradiction if these are all non-trivial.

To construct this $\mathscr{K}$, set $\mathscr{K} := \Lambda(\mathscr{N}) \otimes \mathrm{pr}_2^*\mathscr{L}^{-1}$ (recall the Mumford construction $\Lambda(N) = m^*\mathscr{N} \otimes \mathrm{pr}_1^*\mathscr{N}^{-1} \otimes \mathrm{pr}_2^*\mathscr{N}^{-1}$). Pulling back to $\{x\} \times A$ turn m^* into t_x^*, kills pr_1, turns pr_2^* into Id^*, so we see that we indeed get $t_x^*\mathscr{N} \otimes \mathscr{N}^{-1} \otimes \mathscr{L}^{-1}$.

Now we study $H^j(A \times A, \mathscr{K})$ using the Leray spectral sequences for the two maps

$$(p_1, p_2) \colon A \times A \rightrightarrows A.$$

Assume $\mathscr{K}|_{\{a\} \times A} \not\simeq \mathscr{O}_A$ for all $a \in A(k)$; we'll deduce that $H^j(A \times A, \mathscr{K}) = 0$ for all j (using $\phi_{\mathscr{L}} = 0$), and then get a contradiction from this.

We have $H^i(A, R^j \mathrm{pr}_{1*}\mathscr{K}) \implies H^{i+j}(A \times A, \mathscr{K})$. We'll show that $R^j \mathrm{pr}_{1*}\mathscr{K} = 0$ for all j. By the theorem on cohomology and base change (applicable since pr_1 is proper and flat), it suffices to show that $H^j(A, \mathscr{K}|_{\{a\} \times A}) = 0$ for all j and all $a \in A(k)$. By design $\mathscr{K}|_{\{a\} \times A} \simeq t_a^*\mathscr{N} \otimes \mathscr{N}^{-1} \otimes \mathscr{L}^{-1}$ is non-trivial by assumption, and since $\phi_{\mathscr{M}}$ is a "discrete" invariant of $\mathscr{M}$ we have $\phi_{\mathscr{K}|_{\{a\} \times A}} = \phi_{\mathscr{L}^{-1}} = -\phi_{\mathscr{L}}$, which vanishes by hypothesis on $\mathscr{L}$. We're going to prove that a non-trivial line bundle $\mathscr{M}$ for which $\phi_{\mathscr{M}} = 0$ must have

vanishing cohomology in all degrees (motivated by knowledge of the cohomology of line bundles in the analytic setting):

Lemma 5.2.5. *If $\mathscr{M} \not\simeq \mathscr{O}_A$ and $\phi_{\mathscr{M}} = 0$, then $H^j(A, \mathscr{M}) = 0$ 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. Recall that $\Lambda(\mathscr{M}) := m^*\mathscr{M} \otimes \mathrm{pr}_1^*\mathscr{M}^{-1} \otimes \mathrm{pr}_2^*\mathscr{M}^{-1}$ is isomorphic to the pullback $(1 \times \phi_{\mathscr{M}})^*\mathscr{P}_A$ under the map $A \times A \xrightarrow{1\times\phi_{\mathscr{M}}} A \times \widehat{A}$. So if $\phi_{\mathscr{M}} = 0$ then $\Lambda(\mathscr{M})$ is trivial, so

$$\boxed{m^*\mathscr{M} \simeq \mathrm{pr}_1^*\mathscr{M} \otimes \mathrm{pr}_2^*\mathscr{M}.} \tag{1}$$

For any k-scheme S and $(f, g) \in (A \times A)(S) = A(S) \times A(S)$, pulling back (1) along $(f, g)\colon S \to A \times A$ gives

$$\boxed{(f+g)^*\mathscr{M} \simeq f^*\mathscr{M} \otimes g^*\mathscr{M}.}$$

As a consequence, we get that $[n]^*\mathscr{M} \simeq \mathscr{M}^{\otimes n}$ for all $n \in \mathbf{Z}$. In particular, *for such an $\mathscr{M}$*, we have

$$\boxed{[-1]^*\mathscr{M} \simeq \mathscr{M}^{-1}.}$$

Now let's start running the induction.

$\underline{j = 0}$. Assume there exists a non-zero global section $s \in \mathscr{M}(A)$, so $\mathscr{O}_A \to \mathscr{M}$ defined locally by $f \mapsto fs$ is a nonzero map of invertible sheaves. This dualizes to a nonzero map of invertible sheaves $\mathscr{O}_A \hookleftarrow \mathscr{M}^{-1}$, so it must be an injection and so identifies $\mathscr{M}^{-1}$ with an ideal sheaf $\mathscr{I}_D$ for an effective Cartier divisor D. Thus, $\mathscr{M} \simeq \mathscr{I}_D^{-1} = \mathscr{O}_A(D)$.

The relation $[-1]^*\mathscr{M} \simeq \mathscr{M}^{-1}$ implies that $\mathscr{O}_A([-1]^*D) \simeq \mathscr{O}_A(-D)$, so $[-1]^*D + D$ is an *effective* Weil divisor linearly equivalent to 0. But a nonzero rational function whose divisor (of zeros and poles) is effective must be constant, so $[-1]^*D + D = 0$ and hence $D = 0$. Thus, $\mathscr{M}$ is trivial, a contradiction.

$\underline{j > 0}$. 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 identity map as

$$\mathrm{Id}\colon A \xrightarrow{\iota_1} A \times A \xrightarrow{m} A,$$

yielding a factorization of the identity endomorphism

$$H^j(A, \mathscr{M}) \leftarrow H^j(A \times A, m^*M) \xleftarrow{m^*} H^j(A, \mathscr{M}).$$

It suffices to show that the middle term is 0. Since $m^*\mathscr{M} \simeq \mathrm{pr}_1^*\mathscr{M} \otimes \mathrm{pr}_2^*\mathscr{M}$, we have

$$H^j(A \times A, m^*\mathscr{M}) \simeq H^j(A \times A, \mathrm{pr}_1^*\mathscr{M} \otimes \mathrm{pr}_2^*\mathscr{M})$$

and we can apply Künneth over the field k to get that this is

$$\bigoplus_{i+i'=j} H^i(A, \mathscr{M}) \otimes_k H^{i'}(A, \mathscr{M}).$$

But either $i < j$ or $i' < j$ since $j > 0$, so by induction hypothesis this entirely vanishes. □

Remark 5.2.6. The upshot is that for any non-trivial line bundle whose ϕ vanishes, *all* the cohomology vanishes. For line bundles with ϕ an isogeny, it turns out (as explained in [Mum, §16]) there is exactly one index for which the cohomology doesn't vanish. This is somewhat analogous to the Borel–Weil–Bott theorem for the cohomology of line bundles on (projective) flag varieties G/B.

Returning to our main goal, we conclude that $R^j(\mathrm{pr}_1)_*(\mathscr{K}) = 0$ on A, so the Leray spectral sequence implies that $H^j(A \times A, \mathscr{K}) = 0$ for all j. Keep in mind that this is all proceeding under the assumption that $\mathscr{L} \neq \phi_{\mathscr{N}}(x)$ for all $x \in A(k)$, to ensure that all fibers $\mathscr{K}|_{\{a\}\times A}$ are non-trivial.

Now let's study the spectral sequence for *other* projection:

$$H^i(A, (R^j \mathrm{pr}_2)_*(\mathscr{K})) \Longrightarrow H^{i+j}(A \times A, \mathscr{K}) = 0.$$

We have $\mathscr{K}|_{A\times\{a\}} \simeq \phi_{\mathscr{N}}(a)$, as $\mathscr{K} = \Lambda(\mathscr{N}) \otimes \mathrm{pr}_2^* \mathscr{L}^{-1}$. This has "vanishing ϕ" (by Theorem of the Square) due to our assumption that $\phi_{\mathscr{L}} = 0$, as we have already noted. For any a at which $\phi_{\mathscr{N}}$ is non-zero, Lemma 5.2.5 applies again to give vanishing of fibral cohomology: $H^j(\mathrm{pr}_2^{-1}(a), \mathscr{K}|_{A\times\{a\}}) = 0$ for all j. Therefore, by cohomology and base change the stalks of the higher direct images at such points vanish: $R^j(\mathrm{pr}_2)_*(\mathscr{K})_a = 0$ for all j when $a \notin \ker \phi_{\mathscr{N}}$.

But $\ker \phi_{\mathscr{N}}$ is *finite* by ampleness of $\mathscr{N}$, so the coherent sheaves $R^j(\mathrm{pr}_2)_*(\mathscr{K})$ on A vanishes on $A - \ker \phi_{\mathscr{N}}$ and thus have support contained in the finite k-scheme $\ker \phi_{\mathscr{N}}$. These coherent sheaves are then pushforwards to A from k-finite closed subschemes, so $H^i(A, R^j(\mathrm{pr}_2)_*(\mathscr{K})) = 0$ for all $i > 0$ and all j.

So the Leray spectral sequence vanishes away from the row consisting of terms

$$H^0(A, R^j \mathrm{pr}_{2*} \mathscr{K})$$

whose members are the global sections of the coherent sheaves $R^j \mathrm{pr}_{2*} \mathscr{K}$ with k-finite support, so the coherent sheaves $R^j(\mathrm{pr}_2)_* \mathscr{K}$ vanishes for all j. Why is this interesting? By the theorem on cohomology and base change, now applied to the proper flat pr_2, it follows via descending induction from larger cohomological degrees that the fibral cohomologies $H^j(A, \mathscr{K}|_{p_2^{-1}a})$ vanish for all $a \in A(k)$ and all $j \geq 0$. Taking $j = 0$ and $a = 0$ then gives that $H^0(A, \mathscr{O}_A) = 0$, which is absurd! □

5.3. **The Néron–Severi group.** We've *finally* finished the proof that a line bundle $\mathscr{L}$ on A comes from $\mathrm{Pic}^0_{A/k}(k)$ if and only if $\phi_{\mathscr{L}} : A \to \widehat{A}$ vanishes. In effect, the additive ϕ-construction is the unique "discrete invariant" of $\mathscr{L}$ (it detects when two line bundles lie in the same geometric connected component of $(\mathrm{Pic}_{A/k})_{\overline{k}}$).

To put this into a broader framework, we introduce some terminology: if X is a proper k-scheme that is geometrically connected and geometrically reduced then $\mathrm{Pic}_{X/k}$ is a k-group scheme locally of finite type, and its geometric component group has a name:

Definition 5.3.1. The *Néron–Severi group* of X is

$$\mathrm{NS}(X) = \mathrm{Pic}_{X/k}(\overline{k}) / \mathrm{Pic}^0_{X/k}(\overline{k}).$$

This is the group of geometric points of the étale k-group $\mathrm{Pic}_{X/k}/\mathrm{Pic}^0_{X/k}$ since the formation of Picard schemes commutes with extension of the ground field. In geometric terms, $\mathrm{NS}(X)$ is the group of line bundles on $X_{\overline{k}}$ up to algebraic equivalence, where $\mathscr{L}_1$ and $\mathscr{L}_2$ on $X_{\overline{k}}$ are *algebraically equivalent* if there exists a connected $\overline{k}$-scheme S, points $s_1, s_2 \in S(K)$ for an extension field $K/\overline{k}$, and a line bundle $\mathscr{N}$ on $X \times S$ such that $\mathscr{N}_{s_i} = (\mathscr{L}_i)_K$. (This is equivalent to $\mathscr{L}_1$ and $\mathscr{L}_2$ lying in the same geometric connected component of $\mathrm{Pic}_{X/k}$ is because any line bundle $\mathscr{N}$ on $X \times S$ is classified – up to twisting by a line bundle coming from S – by a $\overline{k}$-morphism $S \to \mathrm{Pic}_{X_{\overline{k}}/\overline{k}} = (\mathrm{Pic}_{X/k})_{\overline{k}}$, and such a map must land in a connected component since S is connected.)

Now for general cultural awareness (to better appreciate what we will prove for the Néron–Severi group of an abelian variety) we discuss some deep results concerning $\mathrm{NS}(X)$ for such general X. First, the Néron-Lang "Theorem of the Base" says that $\mathrm{NS}(X_{\overline{k}})$ is always *finitely generated* over $\mathbf{Z}$ (so, for example, its torsion subgroup is finite). One is then led to ask if we can characterize the torsion bundles. Those turn out to be precisely the line bundles that are "invisible" from the perspective of intersection theory: we say $\mathscr{L}$ on $X_{\overline{k}}$ is *numerically equivalent to* 0 (a weaker notion than algebraic equvalence) if for all integral curves $C \subset X_{\overline{k}}$, the intersection number $C \cdot \mathscr{L} := \deg_C(\mathscr{L}|_C)$ vanishes (see §9.1 of *Néron Models* for several definitions of degree for a line bundle on a general integral proper curve over a field, such as degree of the pullback to the normalization or the degree using a representive Weil divisor or as a coefficient of a Hilbert polynomial), and we have:

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

(1) (Theorem of the Base) $\mathrm{NS}(X_{\overline{k}})$ *is finitely generated over* $\mathbf{Z}$.

(2) If $\mathrm{Pic}^{\tau}_{X/k}$ *is the open and closed subgroup sscheme of* $\mathrm{Pic}_{X/k}$ *corresponding to* $\mathrm{NS}(X)_{\mathrm{tor}}$ *then* $\mathrm{Pic}^{\tau}_{X/k}(\overline{k})$ *consists exactly of those* $\mathscr{L}$ *on* $X_{\overline{k}}$ *that are numerically equivalent to* 0.

Part (1) in Theorem 5.1 in Exp. XIII, and part (2) in Theorem 4.6 in Exp. XIII.

Remark 5.3.3. The proofs of these results are rather deep, involving some input from étale cohomology. But there is a simple analytic explanation for the Theorem of the Base over $\mathbf{C}$: for any connected compact complex manifold X, the exponential sequence

$$0 \to \underline{\mathbf{Z}}(1) \to \mathscr{O}_X \xrightarrow{\exp} \mathscr{O}_X^{\times} \to 1$$

gives a long exact sequence

$$0 \to H^1(X, \mathscr{O}_X)/H^1(X, \underline{\mathbf{Z}}(1)) \to H^1(X, \mathscr{O}_X^{\times}) = \mathrm{Pic}(X) \xrightarrow{c_1} H^2(X, \underline{\mathbf{Z}}(1)) \to \dots$$

If $X = A(\mathbf{C})$ for an abelian variety A over $\mathbf{C}$ then $H^1(X, \mathscr{O}_X)/H^1(X, \underline{\mathbf{Z}}(1)) = \mathrm{Pic}^0_{A/\mathbf{C}}(\mathbf{C})$ as subgroups of $\mathrm{Pic}(A)$ (this is intuitively plausible, but does require a proof), so we get an embedding of groups

$$\mathrm{NS}(A) \hookrightarrow H^2(X, \underline{\mathbf{Z}}(1)).$$

This motivates using étale cohomology to analyze the algebraic case over general fields.

In SGA6, a remarkable relative version is proved: for any proper flat finitely presented morphism of schemes $X \to S$, the rank and torsion of the Néron–Severi groups are *bounded* locally on S as we vary through the geometric fibers whereas the locus where the rank or torsion subgroup are equal to some specified value are typically non-constructible (e.g., for a family of elliptic curves, the rank is affected by being CM or not). So in general the geometric fibral components of the Picard scheme jump around like crazy.

Coming back to the special case of abelian varieties, we have an embedding

$$\mathrm{NS}(A) \hookrightarrow \mathrm{Hom}_{\overline{k}}(A_{\overline{k}}, \widehat{A}_{\overline{k}})$$

given by $[\mathscr{L}] \mapsto \phi_{\mathscr{L}}$. Since $\mathrm{Hom}_{\overline{k}}(A_{\overline{k}}, \widehat{A}_{\overline{k}})$ is torsion-free, it follows that $\mathrm{NS}(A)$ is torsion-free (leading to the puzzling phrase "abelian varieties are torsion-free" that one sees in some older literature on abelian varieties, such as in the book of Lang). We will prove that this Hom-group is finitely generated, so $\mathrm{NS}(A)$ is finitely generated.

To establish the $\mathbf{Z}$-finiteness of $\mathrm{Hom}_k(A, B)$ for general abelian varieties A and B over a field k, we need two ingredients:

(1) Properties of the functor $A \rightsquigarrow \widehat{A}$. (For instance, if $f, g\colon A \rightrightarrows B$ then we get $\widehat{f}, \widehat{g}\colon \widehat{B} \rightrightarrows \widehat{A}$, and one could ask if $(f+g)^{\wedge} = \widehat{f} + \widehat{g}$. The answer is yes. You might think that this should obvious, but it *fails* for the induced map on the *full* Picard scheme, as we see in the analytic theory due to the non-additivity of the functor $\wedge^2$. The analytic theory clarifies that the Néron–Severi group is to be regarded as a "quadratic functor".)

(2) A robust theory of isogenies; e.g., forming a quotient A/G for $G \subset A$ a finite k-group scheme. This requires some extra care in characteristic $p > 0$ when G is non-étale, such as α_p, μ_p. But quotients by such subgroup schemes are an essential feature in positive characteristic; e.g., there are abelian surfaces for which the finite k-group scheme $\ker \phi_{\mathscr{L}}$ is non-étale for every ample line bundle $\mathscr{L}$.

To make good sense of quotients as needed in (2), we need to use the techniques of faithfully flat descent. Thus, our next order of business is a digression into the basic generalities of descent theory (a vast generalization of classical Galois descent).

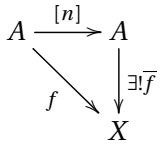
6. DESCENT

We now discuss the general technique of *faithfuly flat descent*.

6.1. **Motivation.** For example, we want to be able to attach meaning to the idea:

$$\text{“}0 \to A[n] \to A \xrightarrow{[n]} A \to 0 \text{ is a short exact sequence”}$$

even if char $k \mid n$ (so $A[n]$ is non-étale). As another example, we want to prove that if $f : A \to X$ is $A[n]$-invariant then it factors uniquely as:



The ability to make useful sense out of quotient constructions involving nasty fibers for the quotient map is one of the great triumphs of Grothendieck's theory of schemes. Earlier approaches to algebraic geometry (e.g., Weil) encountered significant difficulty in dealing with inseparability issues, in retrospect because of the lack of technology for infinitesimal methods. The best introductory reference for this material is §6.1 of the book *Néron Models*.

We want to unify into a single formalism all of the following ideas:

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

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 "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 $U = \coprod_{i \in I} U_i \to X$. 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 there is a term for $i = j$ and we have both ordered pairs (i, j) and (j, i). Under this map, a point $x \in U_i \cap U_j$ for the ordered pair (i, j) corresponds to (x_i, x_j) where x_i is x as a point in U_i and x_j is x as a point in U_j. In contrast, for the ordered pair (j, i) we would associate the point (x_j, x_i), an entirely different point in $U \times_X U$ when $i \neq j$.

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

$$U \times_X U \underset{p_2}{\overset{p_1}{\rightrightarrows}} U = \coprod U_i$$

where p_1 includes U_{ij} in U_i and p_2 includes U_{ij} to U_j.

Similarly, we have three maps

$$U \times_X U \times_X U \underset{p_3}{\overset{p_1}{\overset{\longrightarrow}{\overset{p_2}{\longrightarrow}}}} U$$

whose restrictions to U_{ijk} are the respective inclusions into U_i, U_j, U_k, and the projection

$$p_{ij} : U \times_X U \times_X U \to U \times_X U$$

restricts to U_{ijk} as the inclusion into $U_i \cap U_k$, 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 $U \xrightarrow{p} X$ which are "far" from being a local homeormophism. If $U \to X$ is replaced by $S' \to S$, we still want to be able to "descend" structure from S' to S. For instance, $S' \to S$ could be

- Spec $\overline{k} \to$ Spec k, or
- Spec $\widehat{R} \to$ Spec R (where R is local noetherian), or
- Spec $K \to$ 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 from the category of S-schemes to the category of S'-schemes, as well as between categories of quasi-coherent sheaves, and so on;
(2) describe the essential images of these functors.

In classical Galois descent for a finite Galois extension K/k, the role of "gluing" is played by isomorphisms among the Galois-twists of a given structure over K, which such isomorphisms satisfying a coherence condition analogous to the triple-overlap compatibility in topological gluing. We need to figure what extra data needs to be defined over S' playing the role of this gluing to descend to data over S.

6.2. **fpqc descent.** Grothendieck's key discovery was that if $S' \to S$ is fpqc (faithfully flat, quasi-compact) then the category of S-schemes embeds *fully faithfully* into the category of pairs consisting of an S'-scheme and a *descent datum* on it relative to $S' \to S$ (a notion we need to define, generalizing gluing as described above via fiber products).

Example 6.2.1. If K/k is Galois with group G, then $K \otimes_k K \simeq \prod_{g \in G} K$ sending $a \otimes b \mapsto (g(a)b)$. This is a special case of disjoint unions for gluing: $S' \times_S S' = \coprod_{g \in G} S'$.

Let $S' \to S$ be an fpqc map. For any affine open $U \simeq \text{Spec } A \subset S$, the pre-image $U' \subset S'$ is quasi-compact, so it is covered by finitely many affines opens $U'_i = \text{Spec } A'_i$. Thus, U' admits a surjection from the affine $\coprod_{\text{finite}} U'_i = \text{Spec}(\prod A'_i)$. The composite map $\text{Spec}(\prod A'_i) \to \text{Spec } A$ is a surjective flat map of affines, which is equivalent to the *usual* commutative-algebra notion of faithfully flatness. So we see that the quasi-compactness is a trick to make contact with an affine situation.

Example 6.2.2. In Hartshorne's algebraic geometry textbook, there is an exercise called "schemes over **R**" which encodes the data of a scheme over **R** in terms of a scheme over **C** equipped with a suitable isomorphism to its twist by complex conjugation. This is a baby case of the general framework that we shall set up, and the exercise can become quite messy if one tries to solve it without the benefit of the ideas we are about to develop.

Let $\mathscr{F}'$ be a quasicoherent sheaf on S' (if $\mathscr{F}'$ is a quasicoherent $\mathscr{O}_{S'}$-algebra then this is the "same" as an S'-affine scheme). What "extra structure" on $\mathscr{F}'$ encodes a quasicoherent sheaf $\mathscr{F}$ on S *and* the data of an isomorphism $\alpha\colon f^*\mathscr{F} \simeq \mathscr{F}'$?

Example 6.2.3. In the case $S' = \operatorname{Spec} K'$ and $S = \operatorname{Spec} K$ with K'/K a finite Galois extension with group G, this extra structure should be a G-action on a K'-vector space semi-linear over the G-action on K'.

Example 6.2.4. If $S' = \coprod S_i$ where $\{S_i\}$ is an open cover of S by quasi-compact opens with quasi-compact overlaps, $\mathscr{F}'$ amounts to the data $\{\mathscr{F}_i'$ quasicoherent on $S_i'\}$ and the "extra structure" should be classical gluing data. (One doesn't actually want to impose such quasi-compactness hypotheses to do gluing, so in the end we will want to merge fpqc-descent with usual gluing for the Zariski topology.)

As motivation, suppose $\mathscr{F}$ is a quasicoherent sheaf on S and $\mathscr{F}' = f^*\mathscr{F}$. What extra structure does $\mathscr{F}'$ have due to being a pullback? Let $S'' = S' \times_S S'$ and $S''' = S' \times_S S' \times_S S'$. We have two projections

$$S'' \underset{p_2}{\overset{p_1}{\rightrightarrows}} S' \xrightarrow{f} S$$

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

$$\theta_{\mathscr{F}}\colon p_1^*\mathscr{F}' = p_1^* f^*\mathscr{F} = (f \circ p_1)^*\mathscr{F} = (f \circ p_2)^*\mathscr{F} = p_2^*\mathscr{F}'$$

as $\mathscr{O}_{S''}$-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,

$$\begin{array}{ccccc} S'' & \underset{p_2}{\overset{p_1}{\rightrightarrows}} & S' & \xrightarrow{f} & S \\ \uparrow & & \uparrow & & \uparrow \\ R' \otimes_R R' & \underset{p_2^*}{\overset{p_1^*}{\rightleftarrows}} & R' & \xleftarrow[f^*]{} & R \end{array}$$

and $\mathscr{F}' \longleftrightarrow M'$, a module over R'. Then $p_1^*\mathscr{F}' \longleftrightarrow M' \otimes_{R', p_1^*} (R' \otimes_R R') \simeq M' \otimes_R R'$, so θ correponds to an isomorphism

$$\theta^*\colon M' \otimes_R R' \simeq R' \otimes_R M'$$

as modules over $R'' = R' \otimes_R R'$. When $M' = M \otimes_R R'$, there is an evident such isomorphism over R'' via $(m \otimes r_1') \otimes r_2' \mapsto r_1' \otimes (m \otimes r_2')$, and this corresponds to θ_M as built above.

Example 6.2.6. In the case of a Zariski-open covering, we have $S' = \coprod S_i'$ and $\mathscr{F}' \longleftrightarrow \{\mathscr{F}_i' \text{ on } S_i'\}$ and $S'' = \coprod_{i,j} S_i' \cap S_j'$. We have two maps $p_1, p_2 \colon S'' \rightrightarrows S'$ as discussed previously. Then $p_1^*\mathscr{F}' = \{\mathscr{F}_i'|_{S_{ij}'}\}_{i,j}$ and $p_2^*\mathscr{F}' = \{\mathscr{F}_j'|_{S_{ij}'}\}_{i,j}$. So

$$\theta \longleftrightarrow \theta_{ij} \colon \mathscr{F}_i'|_{S_{ij}'} \xrightarrow{\sim} \mathscr{F}_j'|_{S_{ij}'} \text{ for all } (i,j).$$

The upshot is that to give $\mathscr{F}$ on S and $\alpha \colon \mathscr{F}' \simeq f^*\mathscr{F}$ is the *same* as "gluing" $\{\mathscr{F}_i'\}$ by transition functions θ_{ij}. As we know from the classical theory, we should also have a "cocycle condition" on triple overlaps to get a meaningful gluing, and this needs to be translated into a constraint on θ.

As we saw in the preceding example, the data of a isomorphism θ 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 $\theta \colon p_1^*\mathscr{F}' \xrightarrow{\sim} p_2^*\mathscr{F}$ arising from an $\mathscr{F}'$ obtained from $(\mathscr{F}, \alpha)$ have any special property? For this Zariski open covering, we saw that there is a triple overlap condition. In the Galois setting, there is also an associativity/consistency condition corresponding to that in the definition of a group action.

Motivated by this, we look on S''', which admits three maps $q_{ij} \colon S''' \to S''$. On S'' we have the isomorphism $\theta \colon p_1^*\mathscr{F}' \xrightarrow{\sim} p_2^*\mathscr{F}'$. Pulling back across the three maps gives six bundles, and three isomorphisms, so we get a hexagon and the condition will be that this hexagon "commutes."

Let's first consider pulling back θ by q_{12}:

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

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

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

This fits together as

$$\begin{array}{ccc} & & q_{12}^*p_1^*\mathscr{F}' \xrightarrow{q_{12}^*(\theta)} q_{12}^*p_2^*\mathscr{F}' \\ & \diagup\!\diagup & \\ q_{13}^*p_1^*\mathscr{F}' & & \end{array}$$

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

$$\begin{array}{ccc} & & q_{12}^*p_1^*\mathscr{F}' \xrightarrow{q_{12}^*(\theta)} q_{12}^*p_2^*\mathscr{F}' \\ & \nearrow\!\!= & \\ q_{13}^*p_1^*\mathscr{F}' & & \\ & \searrow^{q_{13}^*(\theta)} & \\ & & q_{13}^*p_2^*\mathscr{F}' = q_{23}^*p_2^*\mathscr{F}' \end{array}$$

Continuing the same argument, we obtain a hexagon diagram

$$\begin{array}{ccccc} & & q_{12}^*p_1^*\mathscr{F}' & \xrightarrow{q_{12}^*(\theta)} & q_{12}^*p_2^*\mathscr{F}' & & \\ & \nearrow\!\!= & & & & \searrow\!\!= & \\ q_{13}^*p_1^*\mathscr{F}' & & & & & & q_{23}^*p_1^*\mathscr{F}' \\ & \searrow^{q_{13}^*(\theta)} & & & & \swarrow_{q_{23}^*(\theta)} & \\ & & q_{13}^*p_2^*\mathscr{F}' & = & q_{23}^*p_2^*\mathscr{F}' & & \end{array} \tag{2}$$

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

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

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', θ) is a descent datum over R', then we have to produce some M over R such that $(M_{R'}, \theta_M) \simeq (M', \theta)$. There is one natural guess:

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

For this to be reasonable, we should first make sure that if $M' = M \otimes_R R'$, then

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

via $m \mapsto m \otimes 1 \in M \otimes_R R'$. This is establishes using a brilliant trick involving faithful flatness: see Theorem 4 in §6.1 of *Néron Models*.

That settles the case of quasi-coherent sheaves. The real "beef" is the case geometric objects (e.g., schemes), which is *much* harder. All is fine for schemes that are affine over the base, because that's equivalent to the data of a quasi-coherent sheaf of algebras. But going beyond the (relatively) affine case is more serious. We take this up next.

Geometric objects. Suppose $X' \to S'$ is an arbitrary S'-scheme, with $f : S' \to S$ an fpqc morphism. How can we specify a descent of X' to an S-scheme? That is, we seek to specify an S-scheme X equipped with an isomorphism $X \times_S S' \simeq X'$. Using the projections $p_1, p_2 : S'' = S' \times_S S' \rightrightarrows S'$ we have:

Definition 6.2.9. A *descent datum* on X' with respect to f is an S''-isomorphism

$$\theta : \underbrace{X' \times_{S',p_1} S''}_{p_1^*(X')} \xrightarrow{\sim} \underbrace{S'' \times_{p_2,S'} X'}_{p_2^*(X')}$$

such that the analogue of the hexagon (2) commutes. This can equivalently be expressed as an isomorphism $X' \times_S S' \simeq S' \times_S X'$ over $S' \times_S S' = S''$.

The requirement that θ be an S''-morphism prevents θ from being the (useless) "flip" isomorphism over S (generally not over S''!). The pairs (X', θ) form a category, say denoted (S'/S)-**Sch**.

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

$$\begin{array}{ccc} (X \times_S S') \times_{S',p_1} S'' & \xrightarrow[\simeq]{\theta_X} & S'' \times_{p_2,S'} (X \times_S S') \\ & \searrow \quad \swarrow & \\ & S'' & \end{array}$$

coming from the equality of the composite maps $S'' \rightrightarrows S' \to S$. We emphasize that θ_X is a morphism over $S'' = S' \times_S S'$.

Theorem 6.2.11. *The functor S-***Sch** $\to (S'/S)$-**Sch** *given by $X \rightsquigarrow (X \times_S S', \theta_X)$ is fully faithful.*

In particular, if X and Y are S-schemes and an S'-morphism $X_{S'} \to Y_{S'}$ respects the descent dats, then it comes from an S-morphism $X \to Y$ that is moreover uniquely determined.

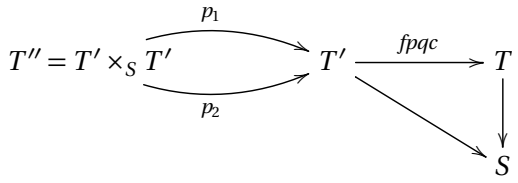
The essential surjectivity aspect of this functor is a very serious problem. Call a pair (X', θ) *effective* if it is in the essential image; i.e., it comes from some X over S. It is very hard to identify the effective descent data in general. In some cases there are affirmative results. For instance, with relative affine morphisms all descent data are effective (since this is a special case of descending a quasicoherent sheaf equipped with algebra structure).

Example 6.2.12. For quasi-projective morphisms, the homogeneous coordinate ring associated to a relatively ample line bundle can provide effectivity results *assuming* such a line bundle is compatible with the descent datum. To be precise, if $X' \to S'$ is separated and quasi-compact and we are given a line bundle $\mathscr{L}'$ on X' that is S'-ample in the sense of EGA II (over open affines in S' this is characterized by a cohomological vanishing criterion of Serre) such that $\mathscr{L}'$ is equipped with its own descent datum $\theta : p_1^*\mathscr{L}' \simeq p_2^*\mathscr{L}$ then (X', θ) is effective! This is proved in Theorems 6 and 7 of §6.1 of *Néron Models*.

Example 6.2.13. The realization of Zariski gluing and Galois descent as special cases of fpqc descent are addressed in detail in Examples A,B in §6.2 of *Néron Models*.

To go beyond Example 6.2.12, avoiding any crutch of $\mathscr{L}'$, requires going beyond schemes to algebraic spaces. Part of the purpose of the theory of algebraic spaces is to give a broader framework for effectivity results in descent theory. That is too much of a digression to discuss further in this course.

Theorem 6.2.14. *Representable functors are fpqc sheaves of sets. In other words, given an S-scheme Z and a diagram*



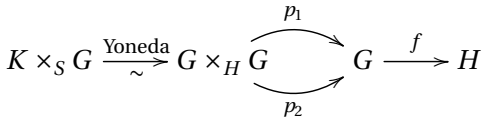
then the diagram of sets

$$Z(T) \hookrightarrow Z(T') \rightrightarrows Z(T'')$$

is exact.

Proof. This is just a special case of full faithfulness of the "descent datum" functor: if we define $Z_T = Z \times_S T$ then the set $Z(T)$ of S-maps $T \to Z$ is naturally identified with the set of T-maps $T \to Z_T$, likewise $Z(T')$ is identified with the set of T'-maps $h : T' \to Z_T \times_T T'$, and being in the equalizer of $Z(T') \rightrightarrows Z(T'')$ is the same as h being compatible with the natural descent data on its source and target relative to $T' \to T$. □

Key case. If $G \xrightarrow{f} H$ is a fpqc map of S-group schemes (e.g. a surjective homomorphism between smooth groups of finite type over $S = \mathrm{Spec}(k)$ for a field k) and if $K := \ker f = f^{-1}(e_H) \subset G$ (an fpqc S-group scheme) then



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. Thus, an S-map $z : G \to Z$ 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 6.2.15. Apply the above to $\mathrm{SL}_n \to \mathrm{PGL}_n$ over $\mathrm{Spec}\ \mathbf{Z}$. Here $\ker f = \mu_n$, so the upshot is that a μ_n-invariant map $\mathrm{SL}_n \to Z$ factors uniquely through f (even though usually $\mathrm{SL}_n(R) \to \mathrm{PGL}_n(R)$ is not surjective for rings R).

Example 6.2.16. For an abelian variety A over a field k and a nonzero integer n, we want to be able to view $[n] : A \to A$ as a quotient map modulo $A[n]$. This is developed in HW6. The machinery of descent allows us to make useful sense of this as a quotient map even when $\mathrm{char}\ k \mid n$.

If we instead given a (reasonable) S-group scheme G and a closed S-subgroup scheme $K \subset G$ that is fpqc over S and normal as a subgroup functor but H is not given then the problem of *building* a quotient G/K as an S-scheme (perhaps even without a normality hypothesis on K, which we don't want to require in practice) 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 to bootstrap from the known case "$A/A[n] = A$" (to be discussed in the homework). More generally, to perform quotient constructions over a base beyond fields (even over something as simple as a discrete valuation ring) one should use algebraic spaces, for which Artin proved deep effectivity results.

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* $\widehat{f}: \widehat{B} \to \widehat{A}$ restricted from the pullback map $\mathrm{Pic}_{B/k} \xrightarrow{f^*} \mathrm{Pic}_{A/k}$ corresponding under the functor of points perspective to $\mathscr{L} \rightsquigarrow f_T^*\mathscr{L}$ on T-valued points (for a k-scheme T). Recall that for $k = \mathbf{C}$, we have a *natural* (in A) isomorphism

$$\widehat{A}^{\mathrm{an}} \simeq H^1(A, \mathscr{O}_A)/H^1(A(\mathbf{C}), \underline{\mathbf{Z}}(1))$$

where $\mathbf{Z}(1) = 2\pi i\mathbf{Z} = \ker(\exp: \mathbf{C} \to \mathbf{C}^\times)$. Since the formation of a complex torus V/Λ is "additive" in Λ, the following result is therefore to be expected:

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

Remark 7.1.2. This is *false* on the entire Picard schemes; e.g., for $k = \mathbf{C}$ we saw that

$$\mathrm{Pic}\,/\,\mathrm{Pic}^0 \hookrightarrow H^2(A(\mathbf{C}), \underline{\mathbf{Z}}(1)) = \wedge^2(H^1(A(\mathbf{C}), \mathbf{Z}))$$

upon choosing a basis of $\mathbf{Z}(1)$, and this ambient group is not additive in the lattice. So there really is a subtlety here: the component group of the Picard scheme is a "quadratic" functor whereas its *identity component* behaves additively.

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

$$(f+g)^*\mathscr{M} = f^*\mathscr{M} \otimes g^*\mathscr{M}$$

in $\mathrm{Pic}(A)$. (Note that we can ignore the trivializations, since $\mathrm{Pic}_{A/k}(k) = \mathrm{Pic}(A)$.)

The left side is the pullback under $(f,g): A \to B \times B$ of $m_B^*\mathscr{M}$. The right side is pullback under (f,g) of $p_1^*\mathscr{M} \otimes p_2^*\mathscr{M}$. Thus, it suffices to show $m_B^*(\mathscr{M}) \simeq p_1^*(\mathscr{M}) \otimes p_2^*(\mathscr{M})$ as line bundles on $B \times B$. But such an isomorphism was established earlier via the Theorem of the Square whenever $\phi_{\mathscr{M}} = 0$, and we have proved the hard implication that $\mathscr{M} \in \mathrm{Pic}^0_{B/k}(k) \Longrightarrow \phi_{\mathscr{M}} = 0$. □

We obtain immediately the following important consequence:

Corollary 7.1.3. *We have $\widehat{[n]_A} = [n]_{\widehat{A}}$.*

Once again, the analogue on the entire Picard scheme, and even just on its component group, is false! (Indeed, the component group is a subgroup of $\mathrm{Hom}(A, \widehat{A})$ on which the combined functorial effect of $[n]_A$ and $[n]_A^\wedge = [n]_{\widehat{A}}$ is multiplication by n^2.)

Now we are in position to 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 $\widehat{f}: \widehat{B} \to \widehat{A}$ 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 factoring through $[n]_A$ for some nonzero integer n. Hence, Corollary 7.1.3 would ensure that the dual of an isogeny is an isogeny. But what about the degree?

Example 7.1.4. For $k = \mathbf{C}$, one can see preservation of degree via the analytic model for the dual. This amounts to the assertion that if $T: L \to L'$ is an index-d subgroup for finite free $\mathbf{Z}$-modules L, L' then the $\mathbf{Z}$-dual map $L^* \leftarrow (L')^* : T^*$ also has index d.

The idea of proof of equality of the degree of an isogeny f and of its dual (which we will return to later) is as follows: one shows that $\deg(f) = \#\ker f$ (order in the sense of finite k-schemes, namely k-dimension of the coordinate ring), and then verify equality with $\#\ker \widehat{f}$ by proving that $\ker f$ and $\ker \widehat{f}$ are "Cartier dual" to each other (and Cartier duality for finite commutative k-group schemes preserves order).

(2) Is the map $\iota_A A \to \widehat{\widehat{A}}$ an isomorphism? Recall that this was constructed via the Poincaré bundle $\mathscr{P}_A$ on $A \times \widehat{A}$, using $\sigma^*(\mathscr{P}_A)$ on $\widehat{A} \times A$ to define $A \to \mathrm{Pic}_{\widehat{A}/k,\widehat{e}}$ carrying e to 0 and hence factoring through $(\widehat{A})^\wedge$.

More generally, given a line bundle $\mathscr{Q}$ on $A \times B$ with (compatible) trivializations along $\{e\} \times B$ and $A \times \{e'\}$, when are the maps $A \to \widehat{B}$ and $B \to \widehat{A}$ isomorphisms? This will involve the *Euler characteristic*

$$\chi(\mathscr{Q}) = \sum_i (-1)^i h^i(A \times B, \mathscr{Q}).$$

In view of (2), our next task is to compute $\chi(\mathscr{P}_A)$. This will be quite a lengthy calculation.

7.2. **Cohomology of the Poincaré bundle.**

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

Proof. Consider the projection $A \times \widehat{A} \xrightarrow{\pi} \widehat{A}$. 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,

$$\mathscr{P}_A|_{\pi^{-1}(\mathscr{L})} \simeq \mathscr{L}$$

(the restriction of the universal bundle to the point of $\widehat{A}$ corresponding to $\mathscr{L}$ is $\mathscr{L}$.) The spectral sequence takes the form:

$$E_2^{i,j} = H^i(\widehat{A}, R^j \pi_* \mathscr{P}_A) \Longrightarrow H^{i+j}(A \times \widehat{A}, \mathscr{P}_A).$$

We claim that $R^j \pi_* \mathscr{P}_A$ is supported on $\widehat{0}$ for all j. Why? Since π is proper and flat, by cohomology and base change it's enough to show that $H^j(A, \mathscr{P}|_{A \times \{\widehat{a}\}})$ for all j and all $\widehat{a} \in \widehat{A}(\overline{k}) - \{\widehat{0}\}$. Now, by the definition of $\widehat{A}$, $\mathscr{P}|_{A \times \{\widehat{a}\}} = \widehat{a}$. So it is enough to show that $H^j(A, \mathscr{M}) = 0$ for all $\mathscr{M} \in \mathrm{Pic}^0_{A/k}(k)$ such that $\mathscr{M} \not\simeq \mathscr{O}_A$. But we already proved this!

Now $R^j \pi_* \mathscr{P}_A$ is a coherent sheaf on $\widehat{A}$, which vanishes over $\widehat{A} - \{\widehat{0}\}$, so it's "really" a coherent sheaf arising from an infinitesimal closed subscheme $Z_j \subset \widehat{A}$ supported at

$\widehat{0}$. So $H^i(\widehat{A}, R^j\pi_*\mathscr{P}_A)$ vanishes for $i > 0$, and the only possibly non-zero terms at the E_2-stage occur on the column $i = 0$. So the spectral sequence degenerates to give:

$$H^n(A \times \widehat{A}, \mathscr{P}_A) = (R^n\pi_*\mathscr{P}_A)_{\widehat{0}}.$$

This is k-finite, and 0 for $n > g$ by the Theorem on formal functions because the infinitesimal fibers have dimension g. (That is, for any proper map between noetherian schemes with fibers of dimension $\leq d$, the higher direct images of any coherent sheaf vanish beyond degree d.) It remains to show vanishing for $n < g$ and 1-dimensionality for $n = g$.

Let $R = \mathscr{O}_{\widehat{A},\widehat{0}}$; note that this is a regular local ring. Consider the base change

$$\begin{array}{ccc} A_R & \longrightarrow & A \times \widehat{A} \\ \downarrow & & \downarrow \pi \\ \operatorname{Spec} R & \xrightarrow[\text{flat}]{} & \widehat{A} \end{array}$$

By compatibility of coherent cohomology with flat base change, we have

$$R^j\pi_*(\mathscr{P}_A)_{\widehat{0}} = H^j(A_R, (\mathscr{P}_A)_{A_R}).$$

By generalities on the cohomology of coherent sheaves on proper R-schemes, the right side is *finitely generated* over R. (In fact, since we have identified the stalk at $\widehat{0}$ with $H^j(A \times \widehat{A}, \mathscr{P}_A)$, this is even finite-dimensional over k.)

We can calculate this cohomology on A_R using the *alternating Cech complex* $C^\bullet$ for $(\mathscr{P}_A)_{A_R}$ associated to a finite affine open cover of A_R (i.e., this is the Cech complex in which we fix an enumeration of the indices for the constituents of the cover and only use overlaps for strictly increasing indices, so it is a *bounded* complex):

$$C^\bullet : 0 \to C^0 \to \ldots \to C^N \to 0$$

Note that each C^j is R-flat, since A_R is R-flat and $(\mathscr{P}_A)_{A_R}$ is a line bundle on A_R, and each homology $H^j(C^\bullet)$ is R-finite.

Now there is a beautiful trick due to Mumford: given a bounded complex of flat modules over a noetherian ring such that the homologies are finitely generated, there exists a bounded complex of finite free modules which computes the same homologies and continues to work *even after* any base change. (See Chapter II, §5, 2nd Theorem of Mum or Ch. III, §12.3 of Hartshorne's textbook on algebraic geometry.) More precisely, studying cohomology and base change shows that there exists a bounded complex of *finite flat* R-modules

$$K^\bullet : 0 \to K^0 \to K^1 \to \ldots \to K^N \to 0$$

(free above the left-most term) and a map of complexes $K^\bullet \to C^\bullet$ such that for all R-modules M the natural map

$$H^j(K^\bullet \otimes M) \to H^j(C^\bullet \otimes_R M)$$

is an isomorphism for every j. The idea of the construction is not hard to guess. The top homology is finitely generated, so you pick a free module mapping to C^N that hits representatives for generators of the top homology module. Then you keep going downwards, and at a certain point you've gone too far, so you truncate. One needs some care to ensure the truncated term is flat (perhaps not free in general, but free for us since R is *local*). In [Mum] only R-algebras M are considered, but one can use any R-module M whatsoever.

Now we have a bounded complex $K^\bullet$ of finite free R-modules with the property that $H^j(K^\bullet)$ 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. To then conclude with the 1-dimensionality in degree g we're going to use the universality of the Poincaré bundle relative to $\widehat{A}$ as a moduli *scheme* (i.e. using infinitesimal considerations).

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

$$0 \to K^0 \to \ldots \to K^N \to 0$$

such that all the $H^j(K^\bullet)$ have finite R-length. Then $H^j(K^\bullet) = 0$ for all $j < g$.

Proof. We induct on g. The case $g = 0$ is empty. Suppose $g > 0$, so by the CM property we can pick $x \in \mathfrak{m}_R$ that is not a zero-divisor (so $\overline{R} = R/(x)$ is Cohen-Macaulay of dimension $g-1$). Then

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

is exact, and since each $K^\bullet$ is finite free we conclude that the diagram of complexes

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

is short exact. Note that each $\overline{K}^j$ is finite free over $\overline{R}$, since K^j is finite free over R.

Consider the long exact sequence in homology

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

It follows that every $H^j(\overline{K}^\bullet)$ has finite length. Therefore, we can apply induction to $\overline{K}^\bullet$ viewed over $\overline{R}$ (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 $j-1 < g-1$) we have $H^{j-1}(\overline{K}^\bullet) = 0$, so x-multiplication on $H^j(K^\bullet)$ is injective. But $H^j(K^\bullet)$ has finite R-length, so it is killed by $\mathfrak{m}_R^N$ for $N \gg 0$, hence by x^N. That shows that $H^j(K^\bullet) = 0$. □

Remark 7.2.3. We didn't need that each K^j is finite free in the preceding proof, just that it is R-flat. Indeed, that ensures x is not a zero-divisor on K^j and that each $\overline{K}^j$ is $\overline{R}$-flat (so the induction works). Thus, up to here we could have used $C^\bullet$ instead of $K^\bullet$.

We conclude that the Cech complex was exact in degrees away from g; more specifically, we now have:

$$\underbrace{0 \to K^0 \to \ldots}_{\text{exact by Lemma}} \to K^g \to K^{g+1} \to \underbrace{\ldots \to K^N}_{\text{exact from setup}} \to 0$$

Suppose $N > g$. Then $\ker(K^{N-1} \twoheadrightarrow K^N)$ is (finite and) R-flat, as it is the kernel of a surjective map between flat modules, and its formation commutes with any base change on R, so we can drop K^N and replacing K^{N-1} with that kernel without any harm.

Thus without loss of generality, we may assume that $N = g$, so we have built a finite free resolution of the R-module $H^g(K^\bullet) = R^g\pi_*(\mathscr{P}_A)_{\widehat{0}}$:

$$0 \to K^0 \to \ldots \to K^g \to R^g\pi_*(\mathscr{P}_A)_{\widehat{0}} \to 0$$

and it remains to prove $R^g\pi_*(\mathscr{P}_A)_{\widehat{0}}$ has length 1. Applying $\mathrm{Hom}_R(-, R)$, we get

$$0 \to \widehat{K^g} \to \ldots \to \widehat{K^0} \to 0$$

whose homology computes $\mathrm{Ext}^\bullet(R^g\pi_*(\mathscr{P}_A)_{\widehat{0}}, R)$. But $R^g\pi_*(\mathscr{P}_A)_{\widehat{0}}$ has finite R-length (it is R-finite and killed by a power of the maximal ideal), so the Ext-modules also have finite R-length. Thus, we can apply the preceding Lemma again! That tells us exactness of $\widehat{K^\bullet}$ below the top term. Letting M be the homology at the final term, namely $\mathrm{Ext}^g(R^g\pi_*(\mathscr{P}_A)_{\widehat{0}}, R)$, we have *another* finite free resolution

$$0 \to \widehat{K^g} \to \ldots \to \widehat{K^0} \to M \to 0.$$

Thus, we can compute $\mathrm{Ext}^\bullet_R(M, R)$ by applying $\mathrm{Hom}_R(\cdot, R)$ to this final resolution. That has the effect of undoing the original dualization, as each K^j is a finite free R-module, so $R^g\pi_*(\mathscr{P}_A)_{\widehat{0}} = \mathrm{Ext}^g_R(M, R)$. To show that it has length 1, we're going to analyze M.

It is a general fact that for Gorenstein (e.g. regular) local rings of dimension g that $\mathrm{Ext}^g_R(\text{residue field}, R)$ 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.

We know M is finitely generated over R, and we claim it is *non-zero* and generated by a single element. By design, M is the cokernel $\mathrm{coker}(\widehat{K}^1 \to \widehat{K}^0)$ of a map of finite free modules so

$$M/\mathfrak{m}M = \mathrm{coker}((K^1 \bmod \mathfrak{m})^* \to (K^0 \bmod \mathfrak{m})^*)$$

since tensoring is right exact, and dualizing commutes with scalar extension for finite free modules. But this is the same as $\ker(K^0 \otimes R/\mathfrak{m} \to K^1 \otimes R/\mathfrak{m})$, which is

$$H^0(K^\bullet \otimes R/\mathfrak{m}) = H^0(A, \underbrace{\mathscr{P}_A|_{A\times\{\widehat{0}\}}}_{=\mathscr{O}_A}) = k;$$

here we have used the universal property of the Poincaré bundle. By Nakayama's lemma, we conclude that M is nonzero and principally generated, so $M = R/J$ for a proper ideal J in R. This is the annihilator ideal for the finite-length M, so J is $\mathfrak{m}$-primary. It remains to check that $J \supset \mathfrak{m}$.

For *any* $\mathfrak{m}$-primary $J' \subset R$,

$$\begin{aligned}\mathrm{Hom}(M, R/J') &= \ker((K^0 \bmod J') \to K^1 \bmod J') \\ &\simeq H^0(C^\bullet \bmod J') \\ &= H^0(A \times \mathrm{Spec}(R/J'), \mathscr{P}_A|_{A\times\mathrm{Spec}(R/J')}).\end{aligned}$$

Let's apply this to *both* $J' = J$ and to $J' = \mathfrak{m}$.

We get a commutative diagram of natural maps

$$\begin{array}{ccc} \mathrm{Hom}(M, R/J) & \xrightarrow{\sim} & \Gamma(A_R \times_R \mathrm{Spec}\ R/J, \mathscr{P}_A) \\ \downarrow & & \downarrow \\ \mathrm{Hom}(M, R/\mathfrak{m}) & \xrightarrow{\sim} & \Gamma(A, \mathscr{O}_A) \end{array}$$

The left side is trivially surjective, so the right side is surjective. That shows that the generating section of $\Gamma(A, \mathscr{O}_A)$ lifts, so the line bundle $\mathscr{P}_A|_{A_R \times_R \mathrm{Spec}(R/J)}$ on the infinitesimal thickening $A_R \otimes_R R/J = A \otimes_k R/J$ of A has a global section that is nonzero in all fibers and thus is a generating section; i.e., this line bundle is trivial!

Now, by the universal property of $\mathscr{P}_A$, it follows that the infinitesimal closed immersion $\mathrm{Spec}(R/J) \to \widehat{A}$ *factors through* the inclusion $\mathrm{Spec}(R/\mathfrak{m}) \to \widehat{A}$, forcing $J \supset \mathfrak{m}$. □

As a consequence of our determination of the cohomologies of the Poincaré bundle in all degrees, we obtain:

Corollary 7.2.4. $\chi(\mathscr{P}_A) = (-1)^g$.

7.3. **Dual isogenies.** Here is an important application of our determination of the Euler characteristic of the Poincaré bundle:

Proposition 7.3.1. *If $f : A \to B$ is an isogeny of degree d then $\widehat{f} : \widehat{B} \to \widehat{A}$ is an isogeny of degree d.*

See HW6 for a general discussion of isogenies.

Proof. For $n > 0$ killing the finite k-group scheme $\ker f$ (e.g., one can always take $n = \#\ker f$ by a theorem of Deligne for finite flat commutative group schemes over any local ring, but over a field one can give a more elementary proof of Deligne's result), we have $A[n] \supset \ker f$ (see HW6). Thus, we get a factorization

$$\begin{array}{ccc} A & \xrightarrow{[n]_A} & A \\ & {\scriptstyle f}\searrow \quad \nearrow & \\ & B & \end{array}$$

and dualizing everything gives

$$\begin{array}{ccc} \widehat{A} & \xleftarrow{\widehat{[n]_A} = [n]_{\widehat{A}}} & A \\ & {\scriptstyle \widehat{f}}\nwarrow \quad \swarrow & \\ & \widehat{B} & \end{array}$$

so $\widehat{f} : \widehat{B} \to \widehat{A}$ is surjective, but the dimensions are the same. Thus, $\widehat{f}$ has 0-dimensional fibers over a dense open of the target, so all fibers are finite via translation arguments over $\overline{k}$. This implies that $\widehat{f}$ is a finite surjective map. It is also generically flat, and thus everywhere flat again by homogeneity considerations over $\overline{k}$ (as for any surjective homomorphism between smooth group varieties over a field). Thus, $\widehat{f}$ is an isogeny.

What is the degree of this finite flat map? HW5 implies that in the diagram

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

we have $\mathscr{Q} := (1\times \widehat{f})^* \mathscr{P}_A \simeq (f\times 1)^* \mathscr{P}_B$ (This is basically just Theorem of the Square). But $f \times 1$ and $1 \times \widehat{f}$ are finite flat surjections of degrees d and $\widehat{d}$ respectively. We want to check that these degrees coincide. The idea is to compare them using the Euler characteristics: we will show that the effect on Euler characteristic by pullback along a finite flat map is multiplication by the degree.

To be precise, if $\varphi : X \to Y$ is a finite flat surjection of degree m between proper k-schemes then we claim that

$$\chi(\varphi^* \mathscr{L}) = m\,\chi(\mathscr{L}).$$

for any line bundle $\mathscr{L}$ on Y. The point is that $\chi(\varphi^*\mathscr{L}) = \chi(\varphi_*\varphi^*\mathscr{L}) = \chi(\mathscr{L} \otimes \varphi_* \mathscr{O}_X)$, and $\varphi_* \mathscr{O}_X$ is a rank-m vector bundle on Y. Now we can use Proposition 4.1.11 to conclude.

Applying this above, we get that

$$\widehat{d}\,\chi(\mathscr{P}_B) = \chi(Q) = d\,\chi(\mathscr{P}_A).$$

But $\chi(\mathscr{P}_B) = (-1)^g = \chi(\mathscr{P}_A)$ is a common nonzero integer, so $\widehat{d} = d$. □

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

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

Example 7.3.3. If $B = \widehat{A}$, $\mathscr{Q} = \mathscr{P}_A$ then $f'_{\mathscr{Q}} = \mathrm{Id}_{\widehat{A}}$ and $f_{\mathscr{Q}} = \iota_A$, so the theorem implies the desired "double duality" isomorphism result we have wanted to prove!

Proof. The flip $\sigma : B \times A \simeq A \times B$ satisfies $\chi(\sigma^*\mathscr{Q}) \simeq \chi(\mathscr{Q})$, and $f'_{\mathscr{Q}} = f_{\sigma^*(\mathscr{Q})}$, so it suffices to show that $|\chi(\mathscr{Q})| = 1 \iff f_{\mathscr{Q}}$ is an isomorphism.

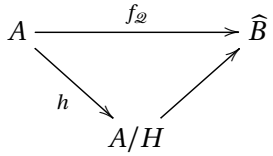
One direction is easy. If $f_{\mathscr{Q}}$ is an isomorphism then $(1 \times f_{\mathscr{Q}})^*(\mathscr{P}_B) = \mathscr{Q}$ (by definition of $f_{\mathscr{Q}}$), so since $1 \times f_{\mathscr{Q}} : A \times B \to B \times \widehat{B}$ is an isomorphism have $\chi(\mathscr{Q}) = \chi(\mathscr{P}_B) = \pm 1$.

In the other direction, the idea is that if $f_{\mathscr{Q}}$ isn't an isomorphism, it factors through some non-trivial isogeny, which imposes a nontrivial divisibility condition on $\chi(\mathscr{Q})$.

Suppose $|\chi(\mathscr{Q})| = 1$, so $\chi(\mathscr{Q}) \in \mathbf{Z}$ is not divisible by any prime. We want $f_{\mathscr{Q}} : A \to \widehat{B}$ to be an isomorphism. Since $\dim A = \dim B$, $f_{\mathscr{Q}}$ is an isomorphism if and only if $\ker(f_{\mathscr{Q}}) = 1$ as a *scheme* (since finiteness of the kernel forces f to be an isogeny by dimension and flatness considerations, and its degree as such then coincides with the order of its kernel scheme, and a finite flat map of degree 1 is an isomorphism).

We may assume $k = \overline{k}$. Suppose $K := \ker(f_{\mathscr{Q}}) \neq 1$. We seek a contradiction. By HW5, K^0_{red} is an abelian subvariety. If K is not finite, then $K^0_{\mathrm{red}}[\ell] \neq 0$ for some prime ℓ, which

we may assume is not char k. Therefore, if $K \neq 1$ then it always contains a finite closed k-subgroup scheme $H \neq 1$. Thus, we have a factorization



with h an isogeny of degree $\#H > 1$. Then

$$\chi(\mathscr{Q}) = \chi((f_{\mathscr{Q}} \times 1)^* \mathscr{P}_B) = \chi(h^*(\mathscr{L})) = (\deg h)\chi(\mathscr{L})$$

for the line bundle $\mathscr{L}$ on A/H pulling back $\mathscr{P}_B$. This shows that $\chi(\mathscr{Q})$ is divisible by $\deg h = \#H > 1$, a contradiction. □

7.4. **Symmetric morphisms.** Now that we know double duality is an isomorphism, it makes sense to consider the notion of a "symmetric" map $A \to \widehat{A}$. We first carry out a warm-up in linear algebra.

Parallels with linear algebra. Recall that if V, W are finite-dimensional over a field F, then

$$\left\{\begin{smallmatrix}\text{Bilinear maps}\\ V \times W \xrightarrow{B} F\end{smallmatrix}\right\} \longleftrightarrow \left\{\begin{smallmatrix}\text{linear maps}\\ V \xrightarrow{T} W^*\end{smallmatrix}\right\}$$
$$v \mapsto B(v, -).$$

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

If $W = V$, then $V \times V \xrightarrow{B} k$ is symmetric if and only if $V \xrightarrow{T_B} V^*$ is *symmetric* in the sense of double duality. Our starting point for abelian varieties will be analogous to this. (The connection with linear algebra in the analytic theory of abelian varieties over $\mathbf{C}$ is much more direct that we can express in the algebraic theory.)

Remark 7.4.1. There is a theory of "$\mathbf{G}_m$-biextensions" that gives a geometric construction akin to the viewpoint of bilinear forms, but we do not discuss this here.

For any bilinear form $B : V \times V \to F$ with induced linear map T_B, the composition

$$V \xrightarrow{(1, T_B)} V \times V^* \xrightarrow{\text{eval}} F$$

recovers B. Thus, the evaluation map $V \times V^* \to F$ has a universal property analogous to the Poincaré bundle.

Definition 7.4.2. A homomorphism $f : A \to \widehat{A}$ is *symmetric* if $f = \widehat{f} \circ \iota_A$:

$$\widehat{A} \xleftarrow{\widehat{f}} \widehat{\widehat{A}} \xleftarrow{\iota_A} A.$$

Here is an important supply of symmetric homomorphisms:

Proposition 7.4.3. *For any line bundle $\mathscr{L}$ on A, $\phi_{\mathscr{L}} : A \to \widehat{A}$ is symmetric.*

Before we prove this result, we make some remarks:

Remark 7.4.4. The correspondence $\mathscr{L} \leftarrow \phi_{\mathscr{L}}$ is analogous to the relationship between a quadratic form over $\mathbf{Z}$ and a symmetric bilinear form over $\mathbf{Z}$.

Remark 7.4.5. Over an algebraically closed field, all symmetric homomorphisms are obtained by the ϕ-construction (one uses Weil pairings – see §8 – and [Mum, Thm. 2, §20; Thm. 3, §23] to make a proof). In other words, the natural map of étale k-schemes

$$\mathrm{Pic}_{A/k}/\widehat{A} \to \underline{\mathrm{Hom}}(A, \widehat{A})^{\mathrm{sym}}$$

(defined functorially by $\mathscr{L} \to \phi_{\mathscr{L}}$) is bijective on $\overline{k}$-points and hence is an isomorphism of k-schemes.

By smoothness of $\widehat{A}$ we know that $\mathrm{Pic}_{A/k}(k_s) \to (\mathrm{Pic}_{A/k}/\widehat{A})(k_s)$ is surjective, so if $f : A \to \widehat{A}$ is a symmetric homomorphism then there exists a finite Galois extension k'/k and a line bundle $\mathscr{L}$ on $A_{k'}$ such that $f_{k'} = \phi_{\mathscr{L}}$. However, it isn't clear at all if we can choose $\mathscr{L}$ to arise on A (without the intervention of k'/k), and in general the obstruction lies in a Galois cohomology group $H^1(k, \widehat{A})$. Poonen and Stoll found examples over $k = \mathbf{Q}$ with $A = J$ a Jacobian and f the canonical isomorphism $J \simeq \widehat{J}$ (which is symmetric) for which such an $\mathscr{L}$ fails to exist!

Proof. We want to know if

$$A \xrightarrow{\iota_A} \widehat{\widehat{A}} \xrightarrow{\widehat{\phi_{\mathscr{L}}}} \widehat{A}$$

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

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

we know that

$$(1 \times \widehat{f})^* \mathscr{P}_A \simeq (f \times 1)^* \mathscr{P}_B.$$

As maps to the dual abelian variety are classified by the their pullback of the Poincaré bundle, we conclude that is equivalent to prove

$$\boxed{(1 \times (\phi_{\mathscr{L}} \circ \iota_A^{-1}))^* \mathscr{P}_A \simeq (\phi_{\mathscr{L}} \times 1)^* \mathscr{P}_{\widehat{A}}.}$$

$$\begin{array}{ccc} A \times \widehat{\widehat{A}} & \xrightarrow{\phi_{\mathscr{L}}\times 1} & \widehat{A} \times \widehat{\widehat{A}} \\ {\scriptstyle 1\times\iota_A^{-1}}\downarrow & \nearrow_{\phi_{\mathscr{L}}\times\iota_A} & \\ A \times A & & \\ {\scriptstyle 1\times\phi_{\mathscr{L}}}\downarrow & & \\ A \times \widehat{A} & & \end{array}$$

By functoriality, the left side is $(1\times\iota_A^{-1})^*(1\times\phi_{\mathscr{L}})^*\mathscr{P}_A$, so we want

$$\begin{aligned}(1\times\phi_{\mathscr{L}})^*\mathscr{P}_A &\overset{?}{\simeq}(1\times\iota_A)^*(\phi_{\mathscr{L}}\times 1)^*\mathscr{P}_{\widehat{A}}\\ &\simeq(\phi_{\mathscr{L}}\times 1)^*(1\times\iota_A)^*\mathscr{P}_{\widehat{A}}\\ \text{(double duality)}\implies&\simeq(\phi_{\mathscr{L}}\times 1)^*\sigma^*(\mathscr{P}_A)\end{aligned}$$

where $\sigma:\widehat{A}\times A\xrightarrow{\sim}A\times\widehat{A}$ is the flip. But $(\phi_{\mathscr{L}}\times 1)^*\circ\sigma^*=(\sigma\circ(\phi_{\mathscr{L}}\times 1))^*$ and $\sigma\circ(\phi_{\mathscr{L}}\times 1)=1\times\phi_{\mathscr{L}}$, so we are done. □

7.5. **Ampleness.** Although $\phi_{\mathscr{L}}$ only "knows" $\mathscr{L}$ up to $\mathrm{Pic}^0_{A/k}=\widehat{A}$, we will see that $\phi_{\mathscr{L}}$ can detect if $\mathscr{L}$ is ample or not.

Remark 7.5.1. The *Nakai-Moishezon* criterion says that for geometrically integral, projective k-schemes X, a line bundle $\mathscr{L}$ on X is ample if and only if it has positive degree on every integral curve in $X_{\overline{k}}$. In such a situation, ampleness of a line bundle on X depends *only* on the class of L in the Nerón–Severi group $(\mathrm{Pic}_{X/k}/\mathrm{Pic}^0_{X/k})(\overline{k})$, so ampleness is insensitive to moving in connected families. We will not use this, but it motivates what we will prove in the case of abelian varieties.

An analogy. Recall the analogy made precise by the complex analytic theory: $\mathscr{L}\mapsto\phi_{\mathscr{L}}$ is analogous to the association

$$\left\{\begin{smallmatrix}\text{quadratic form}\\ q:L\times L\to\mathbf{Z}\end{smallmatrix}\right\}\to\left\{\begin{smallmatrix}\text{symmetric bilinear form}\\ B:L\times L\to\mathbf{Z}\end{smallmatrix}\right\}$$

sending q to

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

But given $B:L\times L\to\mathbf{Z}$, for the associated quadratic form

$$Q_B=B|_{\mathrm{diag}}:\ell\mapsto B(\ell,\ell)$$

we have $Q_{(B_q)}=2q$. So we don't quite recover q, as there is an extra factor of 2. This is analgous to some annoying factors of 2 that we will encounter below.

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

$$(1,\phi_{\mathscr{L}})=(1\times\phi_{\mathscr{L}})\circ\Delta_{A/k}:A\to A\times\widehat{A}$$

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

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

$$[n]^*\mathscr{L}\simeq\mathscr{L}^{\otimes n^2}\pmod{\mathrm{Pic}^0_{A/k}}.$$

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

Example 7.5.3. For $n=2$, this tells us that $[2]^*\mathscr{L}\simeq\mathscr{L}^4\pmod{\mathrm{Pic}^0_{A/k}}$, so

$$([2]^*\mathscr{L}\otimes\mathscr{L}^{-2})\simeq\mathscr{L}^{\otimes 2}\pmod{\mathrm{Pic}^0_{A/k}}.$$

Hence, given $\phi_{\mathscr{L}}$ we can recover $\mathscr{L}^{\otimes 2}$ up to tensoring against something from Pic^0, so once it is known that the Pic^0-coset determines ampleness it will follow that $\phi_{\mathscr{L}}$ determines ampleness or not of $\mathscr{L}$ (as $\mathscr{L}^{\otimes 2}$ is ample if and only if $\mathscr{L}$ is ample).

Proof. We showed some time ago that

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

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

$$\phi_{\mathscr{L}} = \phi_{[-1]^*\mathscr{L}} \text{ as maps } A \to \widehat{A}.$$

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

$$\begin{aligned}
\phi_{[-1]^*(\mathscr{L})}(x) &= t_x^*([-1]^*\mathscr{L}) \otimes [-1]^*(\mathscr{L}^{-1}) \\
&\simeq [-1]^*(t_{-x}^*\mathscr{L}) \otimes [-1]^*\mathscr{L}^{-1} \\
&\simeq [-1]^*(t_{-x}^*\mathscr{L} \otimes \mathscr{L}^{-1}) \\
&\simeq \widehat{[-1]}\phi_{\mathscr{L}}(-x).
\end{aligned}$$

This, our problem is to show that $\widehat{[-1]}\phi_{\mathscr{L}}(-x) = \phi_{\mathscr{L}}(x)$. But $\widehat{[n]_A} = [n]_{\widehat{A}}$ for any integer n, so $\widehat{[-1]}\phi_{\mathscr{L}}(-x) = -\phi_{\mathscr{L}}(-x) = \phi_{\mathscr{L}}(x)$, so we are done. □

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

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

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

Recall that ampleness is insensitive to ground field extension, so we may and do assume that k is algebraically closed. Then we know that $\phi_{\mathscr{L}} : A(k) \to \widehat{A}(k)$ is *surjective*, so $\mathscr{N} = \phi_{\mathscr{L}}(x) = t_x^*\mathscr{L} \otimes \mathscr{L}^{-1}$ for some $x \in A(k)$. Hence, $\mathscr{L} \otimes \mathscr{N} \simeq t_x^*\mathscr{L}$, and this is ample since t_x is an automorphism. □

It is very important that $\phi_{\mathscr{L}}$ encodes ampleness of $\mathscr{L}$ through the Poincaré-pullback construction. One doesn't notice the role of the ϕ-construction in the theory of elliptic curves because in such cases these turn out (up to the canonical autoduality) to be exactly the multiplication maps against integers.

7.6. **Endomorphisms.** Let X, Y be abelian varieties over k. We now study $\mathrm{Hom}_k(X, Y)$. In particular, we want to show that it is $\mathbf{Z}$-finite. Since $\mathrm{Hom}_k(X, Y) \hookrightarrow \mathrm{Hom}_{\overline{k}}(X_{\overline{k}}, Y_{\overline{k}})$, 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

$$\mathrm{End}(X \times Y) = \mathrm{End}(X) \oplus \mathrm{Hom}(X, Y) \oplus \mathrm{Hom}(Y, X) \oplus \mathrm{End}(Y).$$

Thus, **Z**-finiteness of $\mathrm{Hom}(X,Y)$ is reduced to that for $\mathrm{End}_k(A)$ with general A. The advantage of $\mathrm{End}_k(A)$ is that it is an associative ring, and even torsion-free as an abelian group, so it naturally sits inside an associative **Q**-algebra:

$$\mathrm{End}_k(A) \hookrightarrow \mathrm{End}_k(A) \otimes_{\mathbf{Z}} \mathbf{Q}.$$

The reason that working rationally makes things easier can be seen from the analogy between **Z**-lattice representations of a finite group Γ versus finite-dimensional **Q**-linear representations of Γ - on the rational side we have much nicer basic properties: isotypic decomposition, semisimplicity, and so on.

To exploit the merits of "tensoring to **Q**" in the theory of abelian varieties, recall from HW6 Exercise 1 that we define $\mathrm{Hom}_k^0(A,B) := \mathrm{Hom}_k(A,B) \otimes \mathbf{Q}$ to make the *isogeny category* of abelian varieties over k, and saw that a map $f : A \to B$ becomes an isomorphism in the isogeny category if and only if f is an isogeny.

In the isogeny category, objects are abelian varieties but one doesn't speak of "points" because points are not functorial in the isogeny category. We claim that the isogeny *category* is semi-simple. The key to this is:

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 $A' \times A'' \to A$ is an isogeny.*

By the analogy with linear algebra, we want to construct a projector. We'll use an isogeny to the dual as a proxy for a non-degenerate symmetric invariant bilinar form, and try to construct A' as a kind of orthogonal complement.

Remark 7.6.2. The Poincaré reducibility theorem is false for non-algebraic complex tori.

Proof. Choose an ample line bundle $\mathscr{L}$ on A. Quite generally for $f : B \to A$ we have

$$\widehat{f} \circ \phi_{\mathscr{L}} \circ f = \phi_{f^*\mathscr{L}};$$

i.e. the diagram commutes

$$\begin{array}{ccc} B & \xrightarrow{f} & A \\ {\scriptstyle \phi_{i^*\mathscr{L}}}\downarrow & & \downarrow{\scriptstyle \phi_{\mathscr{L}}} \\ \widehat{B} & \xleftarrow{} & \widehat{A} \end{array}$$

Applying this to $B = A'$, we have a commutative diagram

$$\begin{array}{ccc} A' & \xrightarrow{i} & A \\ {\scriptstyle \phi_{i^*\mathscr{L}}}\downarrow & & \downarrow{\scriptstyle \phi_{\mathscr{L}}} \\ \widehat{A'} & \xleftarrow[\widehat{i}]{} & \widehat{A} \end{array}$$

Then consider $\ker(\widehat{i} \circ \phi_{\mathscr{L}})$. By homework, $A'' := \ker(\widehat{i} \circ \phi_{\mathscr{L}})_{\mathrm{red}}$ *is* an abelian variety (especially a smooth k-subgroup scheme, which doesn't generally work for closed subgroups of general commutative group schemes over imperfect fields). What can we say about $A'' \cap A'$? It lies in $\ker \phi_{i^*\mathscr{L}}$, which is *finite*. So we just need to know that $\dim A'' \geq \dim A - \dim A'$.

The point is that $\phi_{\mathscr{L}}$ is finite surjective, so its presence doesn't really affect the dimension. Thus,

$$\dim A'' = \dim \ker \widehat{i} \geq \dim \widehat{A} - \dim \widehat{A'} = \dim A - \dim A',$$

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.

If A, B are abelian varieties over k, then there exists an isogeny $A \to B$ if and only if there exists an isogeny $B \to A$ (all over k), as we see by using suitable multiplication maps against nonzero integers to kill certain kernels. We write $A \sim B$ to denote this symmetric (and transitive) relationship.

We have shown that if $A' \hookrightarrow A$ is an abelian subvariety then there is an "isogeny complement": an abelian subvariety $A'' \hookrightarrow A$ over k such that $A' \times A'' \to A$ is an isogeny. This shows that

$$A \sim \prod A_i^{e_i} \quad \text{with } k\text{-simple } A_i, \text{ pairwise non-isogeneous over } k.$$

If B is k-simple, then clearly

$$\mathrm{Hom}_k^0(B, A) \simeq \prod_i \mathrm{Hom}_k^0(B, A_i)^{e_i}$$

But for k-simple B and B' any non-zero element in $\mathrm{Hom}_k(B, B')$ *is* an isogeny! Therefore, $\mathrm{Hom}_k^0(B, A_i)$ is nonzero for at most one i. In other words:

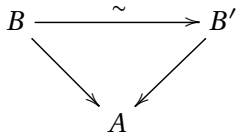
$$\mathrm{Hom}_k^0(B, A) \simeq \begin{cases} 0 & B \not\sim A_i \text{ for all } i, \\ \mathrm{End}_k^0(A_{i_0})^{e_{i_0}} & B \sim A_{i_0} \end{cases}$$

and $\mathrm{End}_k^0(A_{i_0})$ is a *division algebra*. Therefore, $\{A_i\}$ is unique up to k-isogeny and the e_i are also unique. We can say phrase this as follows.

$$\sum_{f : A_{i_0} \to A} f(A_{i_0}) \subset A$$

is *intrinsic* to A, and called the "A_{i_0}-isotypic piece," of dimension $e_{i_0} \dim A_{i_0}$. This is analogous to the representation theory of finite groups over a field of characteristic 0.

Remark 7.6.5. If $B, B' \subset A$ are abelian subvarieties and there exists a commutative diagram



in the *isogeny category*, then $B = B'$ inside A (proof: compose with $[n]_A$ for sufficiently divisible nonzero n to turn maps in the isogeny category into genuine homomorphisms).

This is analogous to the fact that if L is a finite free $\mathbf{Z}$-module then subspaces of $L_{\mathbf{Q}}$ are in bijective inclusion-preserving correspondence with *saturated* subgroups $L' \subset L$ (i.e., L/L' is torsion-free).

Now let's study $\mathrm{Hom}_k(A,B)$. We have k-simple decompositions

$$A \sim \prod A_i^{e_i}, \quad B \sim \prod B_j^{f_j}.$$

Tensoring with $\mathbf{Q}$, we get

$$\mathrm{Hom}_k^0(A,B) = \prod_{i,j} \mathrm{Hom}_k(A_i,B_j)^{e_i f_j}.$$

Now $\mathrm{Hom}_k(A_i,B_j)^{e_i f_j}$ vanishes unless $A_i \sim B_j$. Therefore, $L := \mathrm{Hom}_k(A,B)$ and $L' := \prod_{i,j} \mathrm{Hom}_k(A_i,B_j)^{e_i f_j}$ fit into a diagram of the form

$$L \longrightarrow L' \longrightarrow L, \qquad L \xrightarrow{\;n\;} L$$

for some nonzero integer n. Thus for $\mathbf{Z}$-finiteness, it's enough to study the case where A,B are k-simple and isogenous over k. By the same game comparing $\mathrm{Hom}(A,B)$ and $\mathrm{Hom}(A,A)$, we can reduce to studying $\mathrm{Hom}(A,A)$.

Remark 7.6.6. Once the $\mathbf{Z}$-finiteness is settled, $\mathrm{End}_k^0(A)$ is a finite-dimensional division algebra over $\mathbf{Q}$. Therefore, its center Z is a number field. What kind of number field? (We know from elliptic curves that you can only get $\mathbf{Q}$, or a quadratic imaginary field.) Such Z and the class of $\mathrm{End}_k^0(A) \in \mathrm{Br}(Z)$ are very restricted; see [Mum, §21] for the case $k = \overline{k}$. The presence of the polarization forces Z to be totally real or a CM field.

Theorem 7.6.7. *For A,B abelian varieties over k, $\mathrm{Hom}_k(A,B)$ is $\mathbf{Z}$-finite and for $\ell \neq \mathrm{char}\, k$,*

$$\mathbf{Z}_\ell \otimes_{\mathbf{Z}} \mathrm{Hom}_k(A,B) \to \mathrm{Hom}_{\mathbf{Z}_\ell[G_k]}(T_\ell A, T_\ell B) \subset \mathrm{Hom}_{\mathbf{Z}_\ell}(T_\ell A, T_\ell B)$$

is injective.

Remark 7.6.8.

(1) This gives a very crude upper bound on the $\mathbf{Z}$-rank:

$$\mathrm{rank}_{\mathbf{Z}} \mathrm{Hom}_k(A,B) \leq 4 \dim A \cdot \dim B.$$

If $\mathrm{char}\, k = 0$, then one can do better using the $\mathbf{C}$-analytic theory and the Lefschetz Principle to reduce to this case.

(2) There is a version for $\ell = p = \mathrm{char}(k) > 0$ using p-divisible groups in place of Tate modules (and even the ℓ-adic case above can be recast in terms of ℓ-divisible groups, thereby treating all ℓ and all characteristics in a uniform manner). But proving the injectivity result for $\ell = p$ requires already knowing the $\mathbf{Z}$-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 results of Tate and Zahrin carry over to the case $\ell = p$ too, but this is not easy to find in the literature. This is addressed (with references) in the book of Chai–Conrad–Oort.

(4) One might wonder if this injectivity of $\mathbf{Z}_\ell$ for many ℓ gives the $\mathbf{Z}$-finiteness for purely group-theoretic reasons. The answer is negative: for the group M of rational numbers with squarefree denominator we see that $M \otimes \mathbf{Z}_\ell = (1/\ell)\mathbf{Z}_\ell$ is $\mathbf{Z}_\ell$-finite for all ℓ but M is not $\mathbf{Z}$-finite.

Proof. Without loss of generality, $k = \overline{k}$ and $A = B$ is k-simple. Now we study the *ring* $\mathrm{End}_k A$ which is a division ring. Note in particular that any nonzero endomorphism of f is an isogeny. We have a *multiplicative* map

$$\deg\colon \mathrm{End}_k A \to \mathbf{Z}$$

where it is understood that $\deg(0) := 0$. Since

$$\deg(nf) = \deg([n])\deg(f) = n^{2g}\deg f,$$

we see that deg extends uniquely to a function homogeneous of degree $2g$

$$\deg\colon \mathrm{End}_k^0(A) = \mathrm{End}_k(A) \otimes_{\mathbf{Z}} \mathbf{Q} \to \mathbf{Q}$$

via $(1/m)f \mapsto (\deg f)/m^{2g}$ for nonzero integers m.

We claim that deg is a "polynomial function" on this $\mathbf{Q}$-vector space, but since we don't yet know that $\mathrm{End}_k^0(A)_{\mathbf{Q}}$ is finite-dimensional over $\mathbf{Q}$, we have to phrase this carefully:

Definition 7.6.9. Let W be a vector space over an infinite field F. A function $f\colon W \to F$ is *polynomial* if it is given by a polynomial in linear coordinates on every finite-dimensional subspace. The notion of "homogeneous polynomial of degree d" is defined similarly.

Proposition 7.6.10. *As defined above,* $\deg\colon \mathrm{End}_k^0(A) \to \mathbf{Q}$ *is polynomial (and so then even homogeneous of degree* $2g$*).*

Proof. We'll study degree by relating it to Euler characteristics of line bundles.

By HW7, it is enough to check on 2-dimensional subspaces. (The 1-dimensional case is clear by homogeneity.) By homogeneity, we just need to prove

$$n \mapsto \deg(n\phi + \psi)$$

is polynomial in n (over $\mathbf{Q}$) for fixed $\phi, \psi \in \mathrm{End}(A)$.

We know that one way to interpret the degree is from its effect on the Euler characteristic:

$$\deg(n\phi + \psi) = \frac{\chi((n\phi + \psi)^*\mathscr{L})}{\chi(\mathscr{L})}$$

for ample $\mathscr{L}$ such that $\chi(\mathscr{L}) \neq 0$. (Keep in mind that $n\phi + \psi$ is isogeny when it is nonzero, since we arranged for A to be simple. Alternatively, one can appeal to Remarkk 4.1.12.)

The condition $\chi(\mathscr{L}) \neq 0$ is easily achieved for some very ample $\mathscr{L}$. (There is a Riemann–Roch theorem for abelian varieties which gives the more precise result $\deg \phi_{\mathscr{L}} = \chi(\mathscr{L})^2$

for every line bundle $\mathscr{L}$; see [Mum, §16].) By the Theorem of the Cube applied to the A-valued points $n\phi+\psi, \phi, \psi \in A(A)$, the line bundle $\mathscr{L}_{(n)} = (n\phi+\psi)^*\mathscr{L}$ satisfies

$$\mathscr{L}_{(n+2)} = \mathscr{L}_{(n+1)}^2 \otimes \mathscr{L}_{(n)}^{-1} \otimes \underbrace{((2\phi)^*\mathscr{L} \otimes \phi^*\mathscr{L}^{-2})}_{\text{indep. of } n}.$$

By up/down induction,

$$\mathscr{L}_{(n)} = \mathscr{N}_1^{n(n-1)/2} \otimes \mathscr{N}_2^n \otimes \mathscr{N}_3$$

where $\mathscr{N}_3 = \mathscr{L}_{(1)}, \mathscr{N}_2 = \mathscr{L}_{(1)} \otimes \mathscr{L}_{(2)}, \mathscr{N}_1 = \mathscr{L}_{(2)}\mathscr{L}_{(1)}^{-1} \otimes \mathscr{L}_{(0)}^{-1}$.

Now, it's a general fact called the Snapper Theorem (and proved by slicing) that on any projective scheme,

$$\chi(\mathscr{L}_1^{n_1} \otimes \ldots \otimes \mathscr{L}_r^{n_r}) \in \mathbf{Q}[n_1, \ldots, n_r]$$

for any line bundles $\mathscr{L}_j$. □

We have shown that the map deg: $\mathrm{End}_k^0(A) \to \mathbf{Q}$ (where A is k-simple, to ensure that every non-zero endomorphism is an isogeny and hence has a nonzero degree) is non-zero away from 0, is $\mathbf{Z}$-valued on $\mathrm{End}_k(A)$, and is a homogeneous polynomial of degree $2g$. At this point, we can more or less emulate the proof for elliptic curves.

Claim. For $\mathbf{Z}$-finite $M \subset \mathrm{End}_k(A)$, $\mathbf{Q}M \cap \mathrm{End}_k(A)$ is $\mathbf{Z}$-finite.

Granting this claim, we can conclude as follows.

(1) The injectivity of $\mathbf{Z}_\ell \otimes \mathrm{End}_k(A) \to \mathrm{End}_{\mathbf{Z}_\ell}(T_\ell A)$ is goes exactly as for elliptic curves: consider a hypothetical element of the kernel, write it as a finite sum of elementary tensors (which only involves a $\mathbf{Z}$-finite part of the endomorphism ring), and then argue by contradiction.

Exercise 7.6.11. Do it.

(2) By (1), for $V_\ell(A) = T_\ell(A) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$ we have an injection $\mathbf{Q}_\ell \otimes_{\mathbf{Q}} \mathrm{End}_k^0(A) \hookrightarrow \mathrm{End}_{\mathbf{Q}_\ell}(V_\ell(A))$ whose target is finite-dimensional over $\mathbf{Q}_\ell$. Thus, $\mathrm{End}_k^0(A)$ is finite-dimensional over $\mathbf{Q}$.

(3) We can pick a $\mathbf{Z}$-finite $M \subset \mathrm{End}_k(A)$ such that $\mathbf{Q} \otimes M = \mathrm{End}_k^0(A)$. Then we use this M in the claim to conclude, since $\mathbf{Q}M = \mathrm{End}_k^0(A)$.

Proof of the Claim: Consider the $\mathbf{R}$-vector space $V = \mathbf{R} \otimes_{\mathbf{Q}} \mathbf{Q}M = \mathbf{R} \otimes_{\mathbf{Z}} M$. (At this moment, we only know that $\mathrm{End}_k^0(A)$ is a torsion-free abelian group of finite $\mathbf{Q}$-rank.) Polynomial functions on $\mathbf{Q}M$ extend uniquely to polynomial functions on V by density, so we get a polynomial function $\deg : V \to \mathbf{R}$. The additive subgroup $\mathbf{Q}M \cap \mathrm{End}_k(A)$ inside V meets the open set $\{|\deg| < 1\}$ in $\{0\}$, so it is a discrete subgroup of V. As such, it is $\mathbf{Z}$-finite. □

8. The Weil Pairing

There are two more general topics that we need to address before we discuss the Mordell–Weil Theorem:

(1) Weil pairings $(\cdot,\cdot)_{A,n}: A[n]\times\widehat{A}[n]\to\mu_n$ for $n>0$ are bi-additive and identify each with the Cartier dual of the other:

$$\widehat{A}[n]\to\underline{\mathrm{Hom}}_{\mathrm{gp}}(A[n],\mu_n)=\underline{\mathrm{Hom}}_{\mathrm{gp}}(A[n],\mathbf{G}_m)$$

(2) Polarizations: symmetric isogenies $\phi: A\to\widehat{A}$ such that $(1,\phi)^*\mathscr{P}_A$ is ample on A. (Over $\overline{k}$, these are exactly the maps $\phi_{\mathscr{L}}$ for ample $\mathscr{L}$.)

Using such ϕ, we get pairings

$$(\cdot,\cdot)_{\phi,n}: A[n]\times A[n]\xrightarrow{1\times\phi} A[n]\times\widehat{A}[n]\to\mu_n.$$

In the elliptic curve case of (2) there is always a canonical ϕ of degree 1 (sign convention depending on the reference used), 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,

$$E\xrightarrow{[n]}E\xrightarrow{\text{canonical}/\pm}\widehat{E}$$

using a "canonical" autoduality whose definition depends on the reference used (but only one of these is a polarization, and Silverman's books based on Weil divisors use the sign convention giving the negative of the unique degree-1 polarization).

The degree of a polarization turns out to always be a perfect square. In geometric terms, this is related to $\chi(\mathscr{L})$ always being a square (and is analogous to that fact that the dimension of a symplectic space is always even).

Let's address (1), beginning with a quick review of Cartier duality (developed in HW7).

8.1. **Cartier duality.** Suppose G is a finite locally free commutative group scheme over S (any scheme); i.e., $\pi_*\mathscr{O}_G$ is a locally free $\mathscr{O}_S$-module of finite rank. Then the *Cartier dual* of G is the group scheme $\mathbf{D}(G)$ whose functor of points on S-schemes is

$$T\rightsquigarrow\mathrm{Hom}_{T\text{-gp}}(G_T,\mathbf{G}_{m,T}).$$

We emphasize that this is *not* $\mathrm{Hom}(G(T),\mathbf{G}_m(T))$; the latter is not a functor in T!

On the homework, you show that $\mathbf{D}(G)$ is (represented by) a group scheme with structure sheaf whose underlying $\mathscr{O}_S$-module is the vector bundle

$$\pi_*(\mathscr{O}_{\mathbf{D}(G)})=\underline{\mathrm{Hom}}_{\mathscr{O}_S}(\pi_*\mathscr{O}_G,\mathscr{O}_S).$$

Example 8.1.1.

$$\mathbf{D}(\mu_n)=\underline{\mathrm{Hom}}_{S\text{-gp}}(\mu_n,\mathbf{G}_m)=\underline{\mathrm{Hom}}_{S\text{-gp}}(\mu_n,\mu_n)\xleftarrow{\sim}(\mathbf{Z}/n\mathbf{Z})_S$$

where the right map is determined by the condition $j\mapsto(t\mapsto t^j)$ for all $j\in\mathbf{Z}/n\mathbf{Z}$.

The formation of $\mathbf{D}(G)$ naturally commutes with base change, and there is an obvious bi-additive pairing $G\times_S\mathbf{D}(G)\to\mathbf{G}_m$ that induces an S-homomorphism

$$G\to\underline{\mathrm{Hom}}(\mathbf{D}G,\mathbf{G}_m)\simeq\mathbf{D}\mathbf{D}G$$

which is always an isomorphism.

Example 8.1.2. We have $\mathbf{D}(\alpha_p) = \alpha_p$ via a truncated exponential (in degrees $< p$). By base change it suffices to check this over $S = \mathrm{Spec}(\mathbf{F}_p)$. Of course, this has no geometric points, which is good because over a field there are no non-zero maps from α_p to $\mathbf{G}_m$.

The canonical pairing

$$\alpha_p \times \alpha_p \to \mathbf{G}_m?$$

is $(x, y) \mapsto \exp_{<p}(xy)$. For $G = \alpha_{p^n}$ with $n > 1$, computing the Cartier dual requires the Artin–Hasse exponential map, and it gets complicated quickly. (See Shatz' article on finite group schemes in the book *Arithmetic Geometry* for such calculations.)

The question we want to focus on:

How are $A[n]$ and $\widehat{A}[n]$ put in Cartier duality?

Of course, we will want to know also about functoriality in A and the effect of variation of n and double-duality.

Recall that $[n]_{\widehat{A}} = ([n]_A)^\wedge$. So more generally, if $f : A \to B$ is an isogeny, then we want to put $\ker f$ and $\ker \widehat{f}$ in Cartier duality. Special cases of interest will be $B = \widehat{A}$ and $B = A$.

Theorem 8.1.3. *There is a natural duality pairing*

$$\ker f \times \ker \widehat{f} \to \mathbf{G}_m;$$

i.e., the associated map $\ker \widehat{f} \to \mathbf{D}(\ker f)$ *is an isomorphism.*

Warning (to be addressed in HW9): the relationship between

$$(\cdot,\cdot)_{\widehat{f}} \colon \ker \widehat{f} \times \ker \widehat{\widehat{f}} \to \mathbf{G}_m$$

and $(\cdot,\cdot)_f$ via $f = \widehat{\widehat{f}}$ is not just via flip of components but there is also a sign discrepancy.

Proof. We want to construct an isomorphism

$$(\ker \widehat{f})(T) \stackrel{?}{\simeq} \mathrm{Hom}_{T\text{-gp}}(\ker(f_T), \mathbf{G}_{m,T})$$

naturally in k-schemes T. By definition, the left side is

$$\ker(\mathrm{Pic}^0_{B/k,e'}(T) \xrightarrow{f^*} \mathrm{Pic}^0_{A/k,e}(T)).$$

We claim that this kernel is the same if we drop the restriction to the identity component; this will be useful because we'll perform some descent theory arguments for which keeping track of the identity component is a pain. Obviously replacing the target by the entire Picard scheme no effect on the kernel from the identity component of $\mathrm{Pic}_{B/k,e'}$. More interestingly, we claim that the this kernel is the same as

$$\ker(\mathrm{Pic}_{B/k,e'}(T) \xrightarrow{f^*} \mathrm{Pic}_{A/k,e}(T)).$$

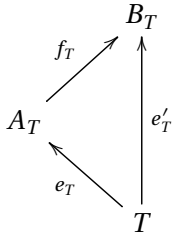
Since this is a Zariski-local statement, we can assume that T is local. (The problem is topological: we want to say that if a T-valued point of $\mathrm{Pic}_{B/k,e'}$ becomes trivial after composing to $\mathrm{Pic}_{A/k,e}$ then it factors through the identity component of $\mathrm{Pic}_{B.k,e'}$.) So without loss of generality, for this purpose we may assume that $T = \mathrm{Spec}\ K$ for a field

K (that we can even assume is algebraically closed). The map f^* is an isogeny, hence invertible up to composing with a nonzero integer, and $\mathrm{NS}(A_K)$ is torsion-free on which the effect of $[n]_A$ is multiplication by n^2. Thus, the induced map $\mathrm{NS}(B_K)_{\mathbf{Q}} \to \mathrm{NS}(A_K)_{\mathbf{Q}}$ is an isomorphism, so there is no kernel between Néron–Severi groups. This gives the result we wanted.

We conclude that

$$(\ker \widehat{f})(T) = \left\{(\mathscr{L}, i) \text{ on } B_T \mid \substack{f_T^*\mathscr{L} \simeq \mathscr{O}_{A_T} \\ i \longleftrightarrow 1}\right\}.$$

An isomorphism $f_T^*(\mathscr{L}) \simeq \mathscr{O}_{A_T}$ is ambiguous up to multiplying against a global unit on T, and that effect is removed by the compatibility condition $i \longleftrightarrow 1$. Since the diagram



commutes, we have

$$(\ker \widehat{f})(T) = \left\{\mathscr{L} \text{ on } B_T \mid f_T^*\mathscr{L} \simeq \mathscr{O}_{A_T}\right\} / \simeq = \ker(\mathrm{Pic}(B_T) \to \mathrm{Pic}(A_T))$$

because pulling back such an isomorphism on A_T along e_T gives a trivialization of $\mathscr{L}$ along e'_T!

For $G := \ker f$ and any k-scheme T we have $G_T = \ker f_T$, and likewise $B_T = A_T/G_T$ (in other words, $A_T \to B_T$ has the expected universal mapping property over T-schemes for G_T-invariant maps). We need to identify $\ker \widehat{f}(T) = \ker(\mathrm{Pic}(B_T) \to \mathrm{Pic}(A_T))$ with $\mathrm{Hom}_{T\text{-gp}}(G_T, \mathbf{G}_{m,T})$ naturally in T.

We now recast our problem in a broader setting.

Setup. Let $f : X \to S$ be proper and flat and finitely presented, with reduced and connected geometric fibers. (This implies that $\mathscr{O}_S \simeq f_*\mathscr{O}_X$ 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 $X(T)$ for all S-schemes T, or equivalently the action map $G \times_S X \to X \times_S X$ is a monomorphism.

Suppose furthermore that there exists a map of S-schemes $X \to Y$ which is a finite locally free surjection representing X/G in the sense discussed in HW6 (so the same holds for $X_T \to Y_T$ for all $T \to S$); in particular, the action map $G \times_S X \to X \times_Y X$ is an isomorphism.

An example of this setup is $f : A \to B$ with $G = \ker f$ over $S = \mathrm{Spec}(k)$, so the result below completes the proof. □

Proposition 8.1.4. *With the setup above, for all $T \to S$*

$$\ker(\mathrm{Pic}(Y_T) \to \mathrm{Pic}(X_T)) \simeq \mathrm{Hom}_{T\text{-gp}}(G_T, \mathbf{G}_{m,T})$$

naturally in T.

Proof. We'll see that this is basically an exercise in descent theory. The role of $\mathbf{G}_m$ is secretly that $f_*\mathbf{G}_{m,X} = \mathbf{G}_{m,S}$ as functors on S-schemes (i.e., for every S-scheme T, the

natural map $\mathscr{O}_T \to (f_T)_*(\mathscr{O}_{X_T})$ of sheaves of rings is an isomorphism and so upon passing to unit groups $\mathscr{O}_T^\times \simeq (f_T)_*(\mathscr{O}_{X_T}^\times)$ since f_T is surjective. Passing to global sections then gives $\mathbf{G}_m(T) \simeq \mathbf{G}_m(X_T)$ as desired.)

Since our entire setup is compatible with base change, "without loss of generality" we treat just the case $T = S$ (to simplify the notation); you have to check that what follows is compatible with base change, which will be easy to do.

The kernel $\ker(\mathrm{Pic}(Y) \to \mathrm{Pic}(X))$ consists of descents of $\mathscr{O}_X$ to a line bundle on Y, up to isomorphism on X. Consider the diagram

$$\begin{array}{ccc} X \times_Y X & \xleftarrow{(gx,x) \leftarrow (g,x)} & G \times_S X \\ {\scriptstyle p_1}\big(\quad \big){\scriptstyle p_2} & & \swarrow {\scriptstyle m,p_2} \\ & X & \end{array}$$

By descent theory, $\ker(\mathrm{Pic}(Y) \to \mathrm{Pic}(X))$ is equal to

$$\{\text{isomorphisms } p_1^*\mathscr{O}_X \simeq p_2^*\mathscr{O}_X \text{ satisfying cocycle condition as } \mathscr{O}_{X\times X}\text{-modules}\}.$$

What about coboundaries? Since $f_*\mathbf{G}_{m,X} = \mathbf{G}_{m,S}$, one can see that coboundaries are trivial! The data of an isomorphism between the p_1-pullback and p_2-pullback amounts to a unit on $G \times X$ satisfying a cocyle condition expressed in terms of the action. For any unit u on $G \times X$, S-scheme T, and point $g \in G(T)$, $u(g,\cdot)$ is a unit on X_T by pullback:

$$X_T \xrightarrow{(g,\mathrm{Id})} G_T \times X_T.$$

But a unit on X_T is the same as a unit on T; let's write $u(g)$ to denote this unit on T. If you unravel the cocycle condition on u as T-varies, then you'll see it expresses exactly the property that the map $G \to \mathbf{G}_m$ of group-valued functors on S-schemes defined by $g \mapsto u(g)$ is a homomorphism. □

Exercise 8.1.5. Check this.

8.2. **Explicit description of the Weil pairing.** We would like a more explicit description of the pairing

$$\langle \cdot, \cdot \rangle_f : (\ker f) \times (\ker \widehat{f}) \to \mathbf{G}_m$$

for an isogeny $f : A \to B$, because we want to know how these fit together as we vary f (such as for the maps $[n]$ with varying n which assemble to define Tate modules).

For a k-scheme T, choose $\widehat{b} \in (\ker \widehat{f})(T)$ and $a \in (\ker f)(T)$. We want to describe $\langle a, \widehat{b} \rangle \in \mathbf{G}_m(T)$. The T-point $\widehat{b}$ corresponds to a line bundle $\mathscr{L}$ on B_T with trivializing section σ along e_T' such that there is a trivialization $\varphi : f_T^*(\mathscr{L}) \simeq \mathscr{O}_{A_T}$ respecting the trivializations on both sides along e_T (note that $f_T \circ e_T = e_T'$).

Since $a \in (\ker f)(T)$, translation by a is invisible to B_T; i.e., the following diagram commutes

$$\begin{array}{ccc} A_T & \xrightarrow{t_a} & A_T \\ & {\scriptstyle f_T}\searrow \quad \swarrow{\scriptstyle f_T} & \\ & B_T & \end{array}$$

This provides a canonical isomorphism

$$t_a^* f_T^* \mathscr{L} \overset{\text{can}}{\simeq} f_T^* \mathscr{L}.$$

But the trivializations $t_a^*(\sigma)$ and σ on the respective sides (pulled back along e_T) are possibly not compatible with this isomorphism (corresponding to arguments with the ratio $\frac{f(x-a)}{x}$ in the classical study of elliptic curves). So there is some unit $u \in \mathbf{G}_m(A_T) = \mathbf{G}_m(T)$ such that $t_a^*(\sigma) = u\sigma$. This unit is $\langle a, \widehat{b} \rangle_f$.

Exercise 8.2.1. Check it.

Remark 8.2.2. For $k = \overline{k}$ and char $k \nmid n$, early in [Mum, Ch. IV, §20] the construction is translated into the language of divisors and rational functions in the special case $f = [n]_A$. In that setting one obtained the reciprocal of the "Silverman formula" because t_a-preimage is equal to t_{-a}!

Now we want to know about the functoriality of $\langle \cdot, \cdot \rangle_{A,n} : A[n] \times A[n] \to \mu_n$ with respect to A and n. To address variation in A, let $h : A' \to A$ be any homomorphism. We claim that the following diagram "commutes":

$$\begin{array}{ccccc} A'[n] & \times & \widehat{A'}[n] & & \\ \downarrow{\scriptstyle h} & & \uparrow{\scriptstyle \widehat{h}} & \searrow^{\langle \cdot,\cdot \rangle_{A',n}} & \\ & & & & \mu_n \\ & & & \nearrow_{\langle \cdot,\cdot \rangle_{A,n}} & \\ A[n] & \times & \widehat{A}[n] & & \end{array}$$

i.e., for any k-scheme T, $a' \in A'[n](T)$, and $\widehat{a} \in \widehat{A}[n](T)$, we claim that

$$\langle h(a'), \widehat{a} \rangle_{A,n} = \langle a', \widehat{h}(\widehat{a}) \rangle_{A',n}$$

in $\mu_n(T)$. Let $\mathscr{L}$ on A_T correspond to $\widehat{a}$, equipped with a trivialization $\sigma : [n]_A^* \mathscr{N} \simeq \mathscr{O}_A$. The pullback $h^*\mathscr{L}$ corresponds to $\widehat{h}(\widehat{a})$, and it admits the associated trivialization

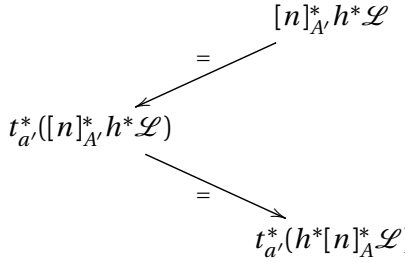
$$[n]_{A'}^*(h^*\mathscr{L}) = h^*([n]_A^*\mathscr{L}) \overset{h^*(\sigma)}{\simeq} \mathscr{O}_{A'}.$$

The unit $\langle a', \widehat{h}(\widehat{a}) \rangle_{A',n}$ is the multiplier arising from the isomorphism

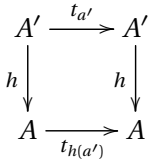
$$t_{a'}^*([n]_{A'}^* h^*\mathscr{L}) \overset{\text{can}}{\simeq} [n]_{A'}^* h^*\mathscr{L};$$

that is, this isomorphism carries $t_{a'}^*(h^*(\sigma))$ to $\langle a', \widehat{h}(\widehat{a}) \rangle_{A',n} \cdot h^*\sigma$. We're going to put this into a big commutative diagram and follow it around to get the other desired expression.

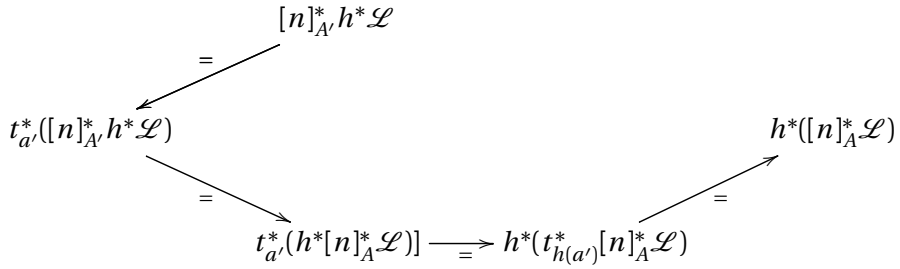
We start off with



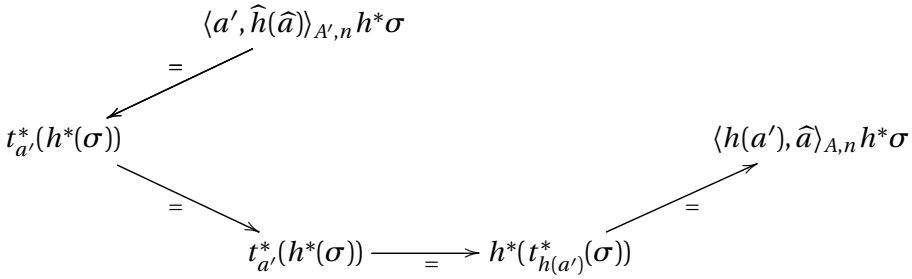
which is induced by moving multiplication by n past the homomorphism h. Next we move other translations through homomorphisms as expressed in the commutative diagram



(which just says $h(a'+x') = h(a') + h(x')$) to get



Following the trivialization through this commutative diagram, we get trivialization compatibilities



Going all the way around yields the desired equality of units.

What about the change in n? For prime $\ell \neq \mathrm{char}(k)$, we want to pass to $\varprojlim$ on $\langle\cdot,\cdot\rangle_{A,\ell^r}$ to get a $\mathbf{Z}_\ell$-bilinear pairing

$$T_\ell A \times T_\ell \widehat{A} \to \mathbf{Z}_\ell(1).$$

Since $\mathbf{Z}_\ell(1) = \varprojlim \mu_{\ell^n}$ using

$$\mu_{\ell^{n+1}} \xrightarrow{t \mapsto t^\ell} \mu_{\ell^n},$$

to pass to the inverse limit we need:

Proposition 8.2.3. *For $m, n \geq 1$, the following diagram commutes:*

$$\begin{array}{ccc} A[nm] \times \widehat{A}[nm] & \longrightarrow & \mu_{nm} \\ {\scriptstyle (m,m)}\downarrow & & \downarrow{\scriptstyle t^m} \\ A[n] \times \widehat{A}[n] & \longrightarrow & \mu_n. \end{array}$$

Proof. See the handout "Functoriality of pairings". □

On HW9, you'll show that the ℓ-adic pairings $(\cdot,\cdot)_{A,\ell^\infty}$ for A and $(\cdot,\cdot)_{\widehat{A},\ell^\infty}$ for $\widehat{A}$ are negative to each other via double duality (and the flip). As a final general functorial property of these pairings, we have the interaction with duality of morphisms:

Corollary 8.2.4. *For $f : A \to A$ any homomorphism, $T_\ell(f)$ is adjoint to $T_\ell(\widehat{f})$ under these perfect pairings.*

Here is a disorienting special case: if $f : A \to \widehat{A}$ is a homomorphism then we get a pairing

$$e_{f,\ell^\infty} : T_\ell(A) \times T_\ell(A) \xrightarrow{1\times f} T_\ell A \times T_\ell \widehat{A} \to \mathbf{Z}_\ell(1)$$

and on HW9 it is shown that f is symmetric if and only if e_f is skew-symmetric. So when we use symmetric f (such as polarizations) then we get *skew-symmetric* pairings.

For f an isogeny and $\ell \neq \mathrm{char}(k)$, the pairing e_{f,ℓ^∞} is perfect over $\mathbf{Z}_\ell$ if and only if $\ell \nmid \deg f$ (because inducing an isomorphism on the Tate modules implies that the ℓ-part of $\ker f$ must be trivial).

9. The Mordell–Weil Theorem

9.1. **Overview.** The remaining goal in the course is to prove:

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 $A(K)/mA(K)$ is finite for some $m \geq 2$. This is deduced from finiteness properties of "S-integral" Galois cohomology for m-torsion modules, when $\mathrm{char}\, k \nmid m$. 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 entire source of ineffectivity in the proof, because it requires contruct points.

2. Geometric step (Weil-Tate heights) There is a canonical "height pairing"

$$\langle \cdot, \cdot \rangle_{A,k} \colon A(\overline{K}) \times \widehat{A}(\overline{K}) \to \mathbf{R}$$

Moreover, for any polarization $\phi \colon A \to \widehat{A}$ for which $(1,\phi)^* \mathscr{P}_A =: \mathscr{L}_\phi$ is symmetric (i.e. $\mathscr{L} \simeq [-1]^* \mathscr{L}$), the pullback pairing

$$\langle \cdot, \cdot \rangle_\phi = \langle \cdot, \cdot \rangle_{A,K} \circ (1 \times \phi) \colon A(\overline{K}) \times A(\overline{K}) \to \mathbf{R}$$

satisfies the following properies:

(1) $\langle \cdot, \cdot \rangle_\phi$ is symmetric and positive-semidefinite; i.e., $\langle a', a' \rangle_\phi \geq 0$ for all $a' \in A(\overline{k})$ and
(2) $\{a \in A(K) \mid \langle a, a \rangle_\phi < C\}$ is finite for any $C > 0$.

Remark 9.1.3. It is easy to construct such ϕ. For instance, we can take $\phi = \phi_{\mathscr{L}}$ for ample symmetric $\mathscr{L}$, such as $\mathscr{N} \otimes [-1]^* \mathscr{N}$ for ample $\mathscr{N}$. Indeed, then

$$(1,\phi)^* \mathscr{P}_A \simeq \mathscr{L}^{\otimes 2} \otimes (\mathscr{L}^{\otimes 2} \otimes (\mathscr{L} \otimes [-1]^* \mathscr{L}^{-1})),$$

which is symmetric since $\mathscr{L}$ is symmetric.

Remark 9.1.4. The existence of such a pairing already forces $A(K)_{\mathrm{tors}}$ 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,

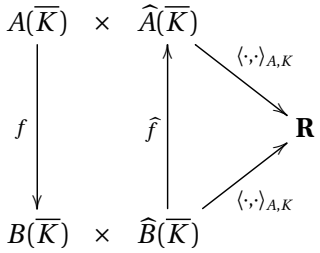
$$\langle \cdot, \cdot \rangle_{A,K'} = [K' : K] \langle \cdot, \cdot \rangle_{A,K}.$$

Because of this, there is a normalization convention: for number fields, people often use

$$\frac{1}{[K : \mathbf{Q}]} \langle \cdot, \cdot \rangle_{A,K}$$

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, we have a commutative diagram:



In other words:

$$\langle f(a), b'\rangle_{B,K} = \langle a, \widehat{f}(b')\rangle_{A,K}.$$

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 $a \in A(\overline{K})$, $a' \in \widehat{A}(\overline{K})$ and $\iota_A: A \xrightarrow{\sim} \widehat{\widehat{A}}$ we will have:

$$\langle a', \iota_A(a)\rangle_{\widehat{A},K} = \langle a, a'\rangle_{A,K}$$

Remark 9.1.5. Weil originally constructed a function that is quadratic "up to bounded error", and Tate recognized that with a refinement involving $\widehat{A}$ and a limiting process one could get an actual quadratic form.

9.2. **Proof assuming weak Mordell–Weil plus heights.** We now prove the full Mordell–Weil Theorem *assuming* the weak Mordell–Weil theorem and the existence of the height pairing with properties listed above.

Let L be an abelian group such that L/nL is finite for some $n \geq 2$ and there exists a symmetric bilinear form

$$\langle\cdot,\cdot\rangle: L \times L \to \mathbf{R}$$

such that

(1) $\langle \ell, \ell\rangle \geq 0$ for all $\ell \in L$ and
(2) $\{\ell \in L \mid \langle \ell, \ell\rangle < C\}$ 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 symmetric bilinear form, but something coarser which is computable. Verifying (2) is effective in practice; 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 ℓ_j to make it smaller. Then we can show that the set of points of L contained in a small "ball" (which is finite) together with the ℓ_j's generate L.

Lemma 9.2.1. *If $\|\ell\| \geq 2C$, then $\|\ell - \ell_j\| \leq (3/2)\|\ell\|$ for all j.*

Proof. We have

$$\begin{aligned}\|\ell-\ell_j\|^2 &= \langle \ell-\ell_j, \ell-\ell_j\rangle \\ &= \langle \ell,\ell\rangle - 2\langle \ell,\ell_j\rangle + \langle \ell_j,\ell_j\rangle\end{aligned}$$

and positive-semidefiniteness ensures Cauchy-Schwarz holds, so $|\langle \ell,\ell_j\rangle| \le \|\ell\|\cdot\|\ell_j\|$. Using this in the above identity gives

$$\|\ell-\ell_j\|^2 \le \|\ell\|^2 + \|\ell_j\|\cdot(2\|\ell\| + \|\ell_j\|).$$

Since by assumption $\|\ell\| \ge 2C \ge 2\|\ell_j\|$, we have $\|\ell_j\| \le \frac{1}{2}\|\ell\|$, so

$$\begin{aligned}\|\ell-\ell_j\|^2 &\le \|\ell\|^2 + \frac{1}{2}\|\ell\|(2\|\ell\| + \frac{1}{2}\|\ell\|) \\ &= \|\ell\|^2(1+5/4) \\ &= (9/4)\|\ell\|^2.\end{aligned}$$

Taking square roots, we obtain $\|\ell-\ell_j\| \le (3/2)\|\ell\|$. □

We claim that L is generated by $\{\ell_j\}$ and $L\cap$(ball of radius $2C$), the latter being finite of course. Choose $\ell \in L$, with $\|\ell\| \ge 2C$. We have $\ell \equiv \ell_j \bmod nL$ for some j with our fixed $n \ge 2$. Then $\ell - \ell_j = n\ell'$ for some $\ell' \in L$ with $n \ge 2$. Then by the Lemma,

$$n\|\ell'\| = \|\ell-\ell_j\| \le (3/2)\|\ell\|$$

so $\|\ell'\| \le \frac{3/2}{n}\|\ell\| \le (3/4)\|\ell\|$. Iterating, we can keep subtracting off various ℓ_i's 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 $n \ge 2$ with* char $K \nmid n$, $A(K)/nA(K)$ *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 related to why it is hard to make this effective. (A more serious difficulty is that we are merely injectiing what we care about into a finite set, without a good way to identity which elements of the finite set are obtained from the injection.)

Remark 9.3.2. The finite commutative K-group scheme $A[n]$ is étale, so it is equivalent to the data of a finite discrete $\mathrm{Gal}(K_s/K)$-module via passage to K_s-points. In particular, there is a finite Galois extension K'/K such that $A_{K'}[n]$ is "split", which is to say $A[n](K_s) = A[n](K')$. (If A is principally polarized then there exists a primitive nth root of unity $\zeta_n \in (K')^\times$ by pairing members of bases 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, as it is unclear if $A(K)/nA(K) \hookrightarrow A(K')/nA(K')$) we can replace K with a preliminary K' without loss of generality. However, this is something we don't want to do in practice. For that reason, we'll try to carry out as much of this proof as possible over the original ground field, but in the end we'll cave in and make a preliminary finite separable field extension.

We now begin the proof. We have an exact sequence of commutative K-groups

$$0 \to A[n] \to A \xrightarrow{n} A \to 0$$

where n is a finite étale surjection, since char $K \nmid n$. We claim that taking K_s-points gives a short exact sequence

$$0 \to A[n](K_s) \to A(K_s) \xrightarrow{n} A(K_s) \to 0. \tag{3}$$

The non-trivial point is surjectivity. For $a \in A(K_s)$, form the pullback square

$$\begin{array}{ccc} E & \longrightarrow & \operatorname{Spec} K_s \\ \downarrow & & \downarrow a \\ A & \xrightarrow[n]{} & A \end{array}$$

Since $E \to \operatorname{Spec} K_s$ is a base change of a finite étale cover, it is itself a finite étale cover of a separably closed field K_s, so it must have K_s-points.

The above short exact sequence of K_s-points is equivariant for the action of $\Gamma = \mathrm{Gal}(K_s/K)$, and these Γ-modules are discrete since any K_s-point arises from a K'-point for a finite extension K'/K inside K_s (and so is fixed by an open subgroup of Γ).

Now we apply Galois cohomology $H^\bullet(\Gamma, \cdot)$ to (3):

$$0 \longrightarrow A[n](K) \longrightarrow A(K) \xrightarrow{n} A(K) \xrightarrow{\delta} H^1(K, A[n]) \longrightarrow \dots$$

This gives an injection $A(K)/nA(K) \hookrightarrow H^1(K, A[n])$ (the latter means $H^1(\Gamma, A[n](K_s))$, or $H^1_{\text{ét}}(\operatorname{Spec} K, A[n])$ with $A[n]$ regarded as an étale sheaf on $\operatorname{Spec} K$). Unfortunately, this Galois cohomology group is very large. For example, if $A[n]$ were split over K and $\zeta_n \in K^\times$ then $A[n] \simeq (\mathbf{Z}/n\mathbf{Z})^{2g} \simeq \mu_n^{2g}$, so

$$H^1(K, A[n]) = H^1(K, \mu_n)^{2g} = (K^\times/(K^\times)^n)^{2g},$$

which is of course enormous (in particular, infinite).

We seek conditions on the image of $A(K)/nA(K)$ that cut down the space of possibilities to something finite. This requires using $A(K)$ is the group of K-points of a smooth proper K-scheme. It will turn out that the image $\delta(A(K)) \subset H^1(K, A[n])$ satisfies very stringent unramifiedness conditions. This has the effect of allowing us to replace K by $\mathcal{O}_S$. Then finiteness will follow from the S-unit theorem and finiteness of class numbers.

We want to realize the smooth proper geometrically connected group $A \to \operatorname{Spec} K$ as the generic fiber of a smooth proper commutative $\mathcal{O}_{K,S}$-group with geometrically connected fibers for suitable large S. The intuition here is that $K = \varinjlim \mathcal{O}_{K,S}$, and making S bigger allows us to account for more denominators. But tying this up with properties such as geometrically connected fibers is not so obvious.

There's a general principle in algebraic geometry that if you are given a 'finitely presented' algebro-geometric situation over a direct limit of rings then the structre should be the pullback of something with similar good properties at some stage of the limit process. In its easiest guise, this is a matter of "chasing denominators", but here it's

much less obvious because we want to keep track of structures such as being a group scheme, being smooth and proper, and having geometrically connected fibers. It is not clear how to capture properness and flatness in terms of equations. These matters are developed in awe-inspiring exhaustiveness in EGA IV_3–IV_4 (§8, §9, §11, etc). .

In our case, we don't really need such super-generality. For instance, we can create a flat model by choosing a closed immersion of A into some $\mathbf{P}^n_K$ and then taking the projective closure in $\mathbf{P}^n_{\mathscr{O}_{K,S}}$ for some S. This is flat because over a Dedekind base, flatness is equivalent to the being torsion-free. (However, it is worthwhile to know that spreading-out for flatness is a general phenomenon beyond the Dedekind case.)

With some more work, one can also spread out the group structure at the cost of increasing S, and also impose smoothness over $\mathscr{O}_{K,S}$ as well as geometric connectedness of fibers (which is really not at all obvious, but is treated in great generality in EGA). The upshot is that for suitable S we get a abelian scheme $\mathscr{A} \to \mathrm{Spec}\ \mathscr{O}_{K,S} =: U$ (i.e., a smooth proper commutative group scheme with geometrically connected fibers).

Because $\mathscr{O}_{K,S}$ is Dedekind, the "valuative criterion over a Dedekind base" implies that $A(K) = \mathscr{A}(U)$ (for any give $a \in A(K)$, use denominator-chasing to handle all but finitely many places away from S and then use the valuative criterion to clean up at the finitely many remaining places). Enlarge S if necessary so that $n \in \mathscr{O}^\times_{K,S}$; i.e., $n \in \mathbf{G}_m(U)$.

Remark 9.3.3. (1) In actual computations, rather than just proving an abstract finiteness theorem, one wants to control S very precisely. For this, it is best to use the finer theory of Néron models rather than the soft spreading-out mentioned above.

(2) Step 0 of the theory of Néron models is that an abelian scheme $\mathscr{A}$ over a Dedekind domain is the "Néron model" of its generic fiber; see 1.2/8 in the book *Néron Models* (whose proof requires some serious input from later in the book, such as the "Weil Extension Theorem" over a Dedekind base). Such an $\mathscr{A}$ is then (uniquely) functorial in A! We will not use this.

Now we claim that this U-group diagram is exact for the fpqc topology, and even for the étale topology:

$$0 \to \mathscr{A}[n] \to \mathscr{A} \xrightarrow{[n]_{\mathscr{A}}} \mathscr{A} \to 0$$

The main content is that the map $[n]_{\mathscr{A}}$ is a finite étale surjection (so in particular $\mathscr{A}[n]$ is finite étale over U). To see this, recall that the "fibral criterion" says that a map between flat and finitely presented schemes over a base is étale when it is so between geometric fibers. (The hard part is that flatness holds if it does so between fibers, which amounts to the local flatness criterion from commutative algebra.) We arranged n to be a unit on U, so the étaleness on geometric fibers is immediate from the theory over fields. Since $[n]_{\mathscr{A}}$ is proper, yet also quasi-finite (even étale), it is finite as well.

We say that a Γ-module M is *unramified* at a closed point $u \in U$ if the inertia subgroup $I_u \subset \Gamma$ at u (well-defined up to conjugation) acts trivially on M.

Corollary 9.3.4. *The discrete Γ-module $A[n](K_s)$ is unramified at all closed points $u \in U$.*

Proof. It suffices to show that if $\mathscr{G}$ is any finite étale group over a discrete valuation ring R, then $\mathscr{G}$ has unramified generic fiber. To prove this, we can pass to the completion $\widehat{R}$, so we may assume without loss of generality that R is complete.

The key tool is Hensel's Lemma. If $\mathscr{G} = \operatorname{Spec} B$, then by assumption $R \to B$ is finite étale. Since R is complete, B is a direct product of local rings. But R is regular, so B is regular by étaleness. More specifically, each local factor ring of B must be Dedekind and hence a discrete valuation ring. By étaleness, these discrete valuation rings are unramified over R: their residue field is separable over that of R and they admit as a uniformizer any one of R. This argument shows that the generic fiber of B is a direct product of finite separable extensions of $\operatorname{Frac}(R)$ that are unramified.

For each closed point $u \in U$, by applying the above to $\mathscr{A}[n]$ over the completed local ring $R = \widehat{\mathscr{O}}_{U,u}$ we see that the coordinate ring of $A[n]_{K_u}$ is a direct product of finite separable extensions of K_u that are unramified. Hence, $A[n]$ is unramified at u. □

Now we have $\mathscr{A}(U)/n\mathscr{A}(U) = A(K)/nA(K) \hookrightarrow H^1(K, A[n])$, with $A[n]$ unramified over U and $\#A[n]$ a unit on U. We'll use the integral structure over U to put some strong conditions on the image in cohomology, cutting it down to something known to be finite.

Lemma 9.3.5. *The image of $A(K)/nA(K) \hookrightarrow H^1(K, A[n])$ is contained in the subgroup of classes ξ unramified outside S; i.e., $\xi|_{I_u} \in H^1(I_u, A[n])$ is trivial for all closed points $u \in U$.*

We give two proofs: one using machinery which we feel better captures the "real reason" the lemma holds, and one which is more elementary.

First proof. We have an exact sequence of sheaves on $U_{\text{ét}}$:

$$0 \to \mathscr{A}[n] \to \mathscr{A} \xrightarrow{n} \mathscr{A} \to 0,$$

so passing to cohomology gives an inclusion $\mathscr{A}(U)/n\mathscr{A}(U) \hookrightarrow H^1_{\text{ét}}(U, \mathscr{A}[n])$. There is a restriction map

$$H^1_{\text{ét}}(U, \mathscr{A}[n]) \to H^1(K, A[n]),$$

and the image of $A(K)/nA(K)$ in $H^1(K, A[n])$ coincides with the image of $\mathscr{A}(U)/n\mathscr{A}(U)$ under the composite map – this is the reason for spreading out to an integral structure!

The composite map $H^1_{\text{ét}}(U, \mathscr{A}[n]) \to H^1(K, A[n]) \to H^1(I_u, A[n])$ factors through the cohomology group $H^1_{\text{ét}}(\mathscr{O}^{\text{sh}}_{U,u'}, \mathscr{A}[n])$ since I_u is the Galois group of the fraction field of the strict henselization $\mathscr{O}^{\text{sh}}_{U,u}$. Thus, we have the commutative diagram

$$\begin{array}{ccc} H^1_{\text{ét}}(U, \mathscr{A}[n]) & \longrightarrow & H^1_{\text{ét}}(\mathscr{O}^{\text{sh}}_{U,u'}, \mathscr{A}[n]) \\ \downarrow & & \downarrow \\ H^1(K, A[n]) & \longrightarrow & H^1(I_u, A[n]) \end{array}$$

But $H^1_{\text{ét}}(\mathscr{O}^{\text{sh}}_{U,u'}, A[n]) = 0$ because the spectrum of a strictly henselian ring is cohomologically trivial for the étale topology (as any étale neighborhood of the closed point admits a section, ultimately due to the local structure theorem for étale morphisms that depends in turn on Zariski's Main Theorem). □

Second proof. For $a \in A(K)/nA(K)$, we can view the image ξ_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 $A(F_u)/nA(F_u)$, where $F_u = K_u^{\mathrm{un}} = \mathrm{Frac}(\mathscr{O}_{U,u}^{\mathrm{sh}})$. Therefore, it suffices to show that $[n]\colon A(F_u) \to A(F_u)$ is surjective.

Let $R = \mathscr{O}_{U,u}^{\mathrm{sh}}$. Then we know that $A(F_u) = \mathscr{A}(R)$ by the valuative criterion, so it suffices to show that $[n]_{\mathscr{A}}\colon \mathscr{A}(R) \to \mathscr{A}(R)$ 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:

$$\begin{array}{ccccc} \mathscr{A} & \xrightarrow{[n]_{\mathscr{A}}} & \mathscr{A} & \longrightarrow & 0 \\ \uparrow & & \uparrow{\scriptstyle a} & & \\ \mathscr{E} & \longrightarrow & \mathrm{Spec}\ R & & \end{array}$$

Since we know that $\mathscr{A} \xrightarrow{[n]_{\mathscr{A}}} \mathscr{A}$ is finite étale cover, so is the base-change morphism $\mathscr{E} \to \mathrm{Spec}\ R$. But 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 of $[n]$ on K_s-points.) Therefore, there exists some element $a' \in \mathscr{E}(R)$ lying over a, which gives an R-point a' of $\mathscr{A}$ such that $na' = a$. □

Putting it all together, we've reduced finiteness to proving a general fact:

Theorem 9.3.6. *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 $\Gamma = \mathrm{Gal}(K_s/K)$-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 9.3.7. Taking $M = \mu_n$, and assuming that $K \supset \mu_n$, if the S-class number is trivial (i.e., $\mathscr{O}_{K,S}$ is a UFD) – as can be arranged by enlarging S due to the finiteness of class numbers – we have

$$H^1_S(K, M) \simeq \mathscr{O}_S^\times/(\mathscr{O}_S^\times)^n$$

and this is finite by the S-unit theorem. In general, without assuming triviality of the S-class number, with more effort one has an exact sequence

$$1 \to \mathscr{O}_{K,S}^\times/(\mathscr{O}_{K,S}^\times)^n \to H^1_S(K, M) \to \mathrm{Pic}(\mathscr{O}_{K,S})[n] \to 1$$

and so finiteness holds by the S-unit theorem and finiteness of class numbers.

Example 9.3.8. If $p = \mathrm{char}(K) > 0$ and $p \mid \#M$ then there are counterexamples. Consider the exact Artin-Scheier sequence

$$0 \to \mathbf{F}_p \to \mathbf{G}_a \xrightarrow{x \mapsto x^p} \mathbf{G}_a \to 0$$

on the étale side of $U = \mathrm{Spec}(\mathscr{O}_{K,S})$. The comparison of étale and Zariski cohomology for quasi-coherent sheaves, the étale cohomology group $H^1(U, \mathbf{G}_a)$ vanishes (since U

is affine), so inside $H^1(\Gamma, \mathbf{F}_p) = K/\mathscr{P}(K)$ one finds that the unramified part outside S is $\mathscr{O}_{K,S}/\mathscr{P}(\mathscr{O}_{K,S})$. But that is infinite by chasing poles at closed points outside U. In particular, we see that we can find a counterexample with $K = \mathbf{F}_p(t)$).

Proof. At this point, to avoid heavier cohomological machinery, we will cave in and use scalar extension on K. Let K'/K be a finite Galois extension splitting M; i.e., $\Gamma' := \Gamma_{K'}$ 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 nth roots of unity introduces ramification only at the primes dividing n, which we may assume lie in S. (Recall $\mathrm{char}(K) \nmid n$.)

Let $S' \subset K'$ be the set of places over S, so we have an isomorphism of discrete Γ'-modules

$$M \simeq \prod (\mathbf{Z}/d_i\mathbf{Z}) \simeq \prod \mu_{d_i}$$

for various integers $d_i | n$ (hence S-units), with the last equality following from the fact that K' contains μ_n.

By inflation-restriction, we have the exact sequence

$$0 \to H^1(K'/K, M = M^{\Gamma'}) \xrightarrow{\mathrm{Inf}} H^1(K, M) \xrightarrow{\mathrm{Res}} H^1(K', M).$$

The group $H^1(K'/K, M)$ is finite since M and $\mathrm{Gal}(K'/K)$ are finite. Under the restriction map $H^1(K, M) \xrightarrow{\mathrm{Res}} H^1(K', M)$, the subgroup $H^1_S(K, M)$ maps into $H^1_{S'}(K', M)$ (exercise). So it's enough to show that $H^1_{S'}(K', M)$ is finite. But $H^1_{S'}(K', M) \simeq \prod H^1_{S'}(K', \mu_{d_i})$, 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 rational integer n that is an S-unit when $\mu_n \subset K^\times$. By Kummer theory we have an isomorphism

$$K^\times/(K^\times)^n \xrightarrow{\sim} H^1(K, \mu_n)$$
$$[c] \mapsto \xi_c := K(\sqrt[n]{c})/K$$

The crucial question to understand here: when is ξ_c unramified outside S? We claim that ξ_c is unramified at $v \nmid \infty$ if and only if the extension $K(\sqrt[n]{c})/K$ is unramified at v.

Exercise 9.3.9. Prove it.

Now there are two approaches we could take at this point. First, we could use the Kummer sequence for $\mathscr{O}_{K,S}$ for the étale topology. However, we're going to do something more hands-on. We can increase S further so that $h_{k,S} = \mathrm{Pic}(\mathscr{O}_{K,S}) = 1$ (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 when $n \mid \mathrm{ord}_v(c)$; this is shown by using that $n \notin S$ and that $\mathscr{O}_{K,S}$ is a UFD.

Exercise 9.3.10. Fill in the details in that final step.

So now we have

$$H^1_S(K, \mu_n) \simeq \mathscr{O}^\times_{K,S}/(\mathscr{O}^\times_{K,S})^n$$

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 $x \in \mathbf{P}^n(\mathbf{Q}) = \mathbf{P}^n(\mathbf{Z})$ can be represented by $x = [x_0, \ldots, x_n]$ with $\gcd(\{x_i\}) = 1$, unique up to $\mathbf{Z}^\times = \{\pm 1\}$. A natural first definition to try is:

$$\mathrm{ht}(x) := \max\{\log|x_i|_\infty\}.$$

Clearly there are only many rational points with height less than some given constant.

For $\mathbf{P}^n(\mathbf{F}_q(t))$, any x can be represented by $x = [f_0, \ldots, f_n]$ with $f_i \in \mathbf{F}_q[t]$ satisfying $\gcd(\{f_i\}) = 1$, unique up to scaling by a common element of $\mathbf{F}_q[t]^\times = \mathbf{F}_q^\times$. Then we are led to define

$$\mathrm{ht}(x) := \max\{\log\|f_i\|_\infty := \deg(f_i)\cdot\log q\}.$$

There are a couple of drawbacks to these definitions:

(1) It's not clear how to extend this to $\mathbf{P}^n(K)$ for a general global field K,
(2) These are not $\mathrm{PGL}_{n+1}(K)$-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 Σ_K denote the set of all places of K (finite *and* infinite). The *standard height function* $h_{K,n} : \mathbf{P}^n(\overline{K}) \to \mathbf{R}$ 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 $K' \supset K(t_0, \ldots, t_n)$ is some finite extension of K and $\|t\|_{v_i}$ is the normalized absolute value on $K_{v'}$ (as used in the product formula, so at complex places we use the square of the usual absolute value).

For this to be well-defined, we should check a couple of properties:

(1) given K', it is unaffected by $(K')^\times$ scaling and is non-negative,
(2) it is unaffected by increasing K'.

Suppose we make change of variables $t_i \mapsto c\,t_i$ for some $c \in (K')^\times$. Then the formula changes by adding

$$\frac{1}{[K' : K]} \sum_{v' \in \Sigma_{K'}} \log\|c\|_{v'}$$

and this vanishes due to the product formula on K'. Hence, without loss of generality we may assume $t_i = 1$ for some i, 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) the definition relative to K''/K is

$$\frac{1}{[K'':K]}\sum_{v''}\max_i \log\|t_i\|_{v''} = \frac{1}{[K':K]}\sum_{v'}\left(\frac{1}{[K'':K']}\sum_{v''|v'}\max_i \log\|t_i\|_{v''}\right)$$

The normalized absolute values satisfy $\|t_i\|_{v''} = \|t_i\|_{v'}^{[K''_{v''}:K'_{v'}]}$. This is obviously true for an unramified extension, as well as at archimedean places. For a totally ramified extension the residue field size doesn't change but the uniformizer does, so it is easily verified in that case too, so the general case holds by consideration of a local tower at each place. Hence, we arrive at the expression:

$$\begin{aligned}
&= \frac{1}{[K':K]}\sum_{v'}\left(\frac{1}{[K'':K']}\sum_{v''|v'}\max_i \log\|t_i\|_{v'}^{[K''_{v''}:K'_{v'}]}\right)\\
&= \frac{1}{[K':K]}\sum_{v'}\left(\frac{1}{[K'':K']}\sum_{v''|v'}\max_i [K''_{v''}:K'_{v'}]\log\|t_i\|_{v'}\right)\\
&= \frac{1}{[K':K]}\sum_{v'}\max_i(\log\|t_i\|_{v'})\left(\frac{1}{[K'':K']}\sum_{v''|v'}[K''_{v''}:K'_{v'}]\right)\\
&= \frac{1}{[K':K]}\sum_{v'}\max_i(\log\|t_i\|_{v'})
\end{aligned}$$

Example 10.1.3. Let's see how this plays out for $K' = K = \mathbf{Q}$: if $t = [t_i] \in \mathbf{P}^n(\mathbf{Q}) = \mathbf{P}^n(\mathbf{Z})$ with $t_i \in \mathbf{Z}$ with $\gcd\{t_i\} = 1$, then for all finite p we have $|t_i|_p \le 1$ but for any given p at least one $|t_i|_p$ is equal to 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 original definition for this case.

A similar argument shows that for $K' = K = \mathbf{F}_q(t)$ this also recovers the initial definition in that case.

From the definition it is clear that $h_{K,n}$ is $\mathrm{Aut}(\overline{K}/K)$-invariant, so $h_{K,n}$ is a well-defined function on the set of closed points of $\mathbf{P}^n_K$. The problem with this is that the set of closed points do *not* form a group (whereas $A(\overline{K})$ 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 redefining the height function via division by $[K:\mathbf{Q}]$ (which really amount to only using $h_{\mathbf{Q},n}$), but as this doesn't have a canonical analogue for function fields we'll avoid it.

Exercise 10.1.5. On HW10, we'll show that $h_{K,n}$ is $\mathrm{PGL}_{n+1}(K)$-invariant on $\mathbf{P}^n(\overline{K})$ "modulo $O(1)$" (i.e., modulo bounded functions).

The basic finiteness theorem for naive heights is:

Theorem 10.1.6. *For any $C > 0$ and $d \geq 1$,*

$$\{\xi \in \mathbf{P}^n(\overline{K}) \mid [K(\xi) : K] \leq d, h_{K,n}(\xi) \leq C\}$$

is finite.

We'll reduce this to the case of rational points over $\mathbf{Q}$ or $\mathbf{F}_q(t)$ by some norm argument, at the cost of a large constant factor. What's actually going on is Weil restriction; e.g., a point over a quadratic field is a rational point on the Weil restriction.

Example 10.1.7. The preservation of projectivity under finite separable Weil restriction is non-trivial. Try doing it for $\mathbf{P}^1$ over a primitive field extension to see how complicated this can become when done explicity. (Beware however that under an inseparable finite extension, Weil restriction of a projective space is *never* proper; we won't need to deal with this, so we say nothing more about it.)

Remark 10.1.8. We'll only apply this finiteness result for ξ with $K(\xi)$ constrained to be within a finite set of possibilities, but remarkably the finiteness holds only bounded $[K(\xi) : K]$ rather than $K(\xi)/K$ as an extension field.

Proof. We'll eventually reduce to the (easy!) case $K = \mathbf{Q}$ or $\mathbf{F}_p(t)$ and $d = 1$, at the cost of increasing n and C in a controlled way.

The first order of business is a 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

$$x' := \mathrm{Frob}^r\, x = [x_0^{p^r}, \ldots, x_n^{p^r}] \in \mathbf{P}^n(\overline{K}).$$

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 $x \rightsquigarrow x'$ is injective). By the definition,

$$h_{K,n}(x') = p^r h_{K,n}(x) \leq p^r C \leq dC$$

because the exponentiation appears as a constant factor due to the logarithms in the definition of $h_{K,n}$. Thus, finiteness in the separable case with the constant dC will take care of the general case for C. Now for the purpose of proving the theorem, we may and do only consider ξ for which $K(\xi)/K$ is separable.

Choose a presentation of K as a finite (separable) extension of $\mathbf{F}$ of degree δ where $\mathbf{F} = \mathbf{Q}$ or $\mathbf{F}_p(t)$. (A separating transcendence basis always exists for a finitely generated extension of a perfect field.) Hence, we have a diagram

$$\begin{array}{ccc} K & \xrightarrow[\text{sep.}]{d} & K(x) \\ {\scriptstyle\delta}\,\big|\ \text{sep.} & & \big| \\ \mathbf{F} & \longrightarrow & \mathbf{F}(x). \end{array}$$

Then $K(x)/\mathbf{F}$ is separable of degree at most $\delta \cdot d$, and $\overline{K}$ is an algebraic closure of $\mathbf{F}$, so $h_{\mathbf{F},n} = [K : \mathbf{F}]^{-1} h_{K,n}$. This reduces us to proving the result over $K = \mathbf{F}$ at the cost of increasing the bound C by a uniform multiplier factor.

Without loss of generality, it suffices to study the case $[K(\xi):K]=d$ with general $d\geq 1$ since we only have to add up the finitely many contributions from the finitely many possibilities for the degree at most a given d. Consider $x=[x_0,\dots,x_n]\in\mathbf{P}^n(\overline{K})$ with $x_j\in K(x)$ (without loss of generality). The ring-theoretic norm

$$K(x)[T_0,\dots,T_n]\xrightarrow{\mathrm{Nm}}K[T_0,\dots,T_n]$$

is a homogeneous polynomial of degree d (in the T_j's):

$$\mathrm{Nm}_{K(x)/K}\left(\sum x_iT_i\right)=\sum_{\|I\|=d}X_I(x)T^I.$$

Now let's consider the product formulation of the norm:

$$\mathrm{Nm}_{K(x)/K}\left(\sum x_iT_i\right)=\prod_{\sigma:K(x)\hookrightarrow K_s}\left(\sum_i\sigma(x_i)T_i\right)=:\sum X_I(x)T^I.$$

If you think about what this looks like, you'll see that $X_I(x)\in K$, since every coefficient is a symmetric function in the embeddings σ (or more directly, these coefficients are certainly $\mathrm{Gal}(K_s/K)$-invariant).

Let $N:=N(n,d)=\binom{n+d}{d}-1$, which one less than $\#\{I:|I|=d\}$; i.e., the dimension of the projective space of homogenous polynomials in $x_0,\dots,x_n$ of degree d. The norm map can be interpreted as a map of sets

$$X:\left\{x\in\mathbf{P}^n(\overline{K})\mid {}^{K(x)/K\text{ sep'ble, degree }d}_{h_{K,n}(x)\leq C}\right\}\to\mathbf{P}^{N(n,d)}(K)$$

via $x\mapsto(X_I(x))$. The key point is that the size of the fibers is at most d (actually, it's exactly d). Indeed, $\sum_{\|I\|=d}X_I(x)T^I$ 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 $\mathrm{Nm}(x_i)$. Then the only ambiguity is in the "order" of the d linear factors.

Remark 10.1.9. This should probably have an interpretation of this in terms of Weil restriction. Can one formulate it in a precise way?

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 contribution at non-archimedean places. Recall that the height was defined in terms of a sum of logarithms at places of an extension over which the given $\overline{K}$-point is rational. Let $E(x)$ be the Galois closure of $K(x)$ over K, which has degree at most $d!$ over K. We now compare the terms contributing to the naive height from $v\in\Sigma_K$ and $v'\in\Sigma_{E(x)}$ lying over it:

$$\begin{aligned}\log\|X_I(x)\|_v&=\log\|X_I(x)\|_{v'}^{1/[E(x)_{v'}:K_v]}\\ \text{(non-archimedean inequality)}\implies&\leq\max_i\log\|x_i\|_{v'}^{[E(x):K]/[E(x)_{v'}:K_v]}\\&\leq d!\max_i\log\|x_i\|_{v'}.\end{aligned}$$

For archimedean v we can't use the non-archimedean inequality, so we amplify by some function $\mu(n,d)$ of n and d. (It seems that $(n+1)^{d!}$ should be enough.) Summing this inequality over $v \in \Sigma_K$ we obtain

$$h_{K,n}(X(x)) \leq A(n,d) \cdot h_{K,n}(x)$$

for some $A(n,d) > 0$. This completes the redution to considering only K-points with $K = \mathbf{Q}$ and $K = \mathbf{F}_p(t)$, which are elementary. □

10.2. **Intrinsic theory of heights.** Given an abelian variety over a global field and an ample line bundle, we wish to define an associated *coordinate-independent* height function. This will replace the theory of "functions up to bounded functions" on projective space.

On HW10, you'll show directly that $h_{K,n}$ is "$\mathrm{PGL}_{n+1}(\overline{K})$-invariant mod $O(1)$." For later purposes, we need more:

Theorem 10.2.1. *Let X be a proper K-scheme and $\mathscr{L}$ is a line bundle on X. If $X \xrightarrow{f} \mathbf{P}^n_K$ and $X \xrightarrow{g} \mathbf{P}^m_K$ are maps such that $f^*\mathscr{O}(1) \simeq \mathscr{L} \simeq g^*(\mathscr{O}(1))$, then*

$$h_f = h_{K,n} \circ f : X(\overline{K}) \to \mathbf{R}$$

and

$$h_g = h_{K,m} \circ g : X(\overline{K}) \to \mathbf{R}$$

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 "up to bounded functions" under change of coordinates.

If $X = \mathbf{P}^n$, $f = \mathrm{Id}$ and g is an automorphism induced by some $\tau \in \mathrm{PGL}_{n+1}(K)$, then this recovers the HW10 exercise. However, that is a "fake" deduction because we actually need that special case in the proof.

Example 10.2.3. If $\mathscr{L}$ is very ample and $f : X \hookrightarrow \mathbf{P}(\Gamma(X,\mathscr{L})) \simeq \mathbf{P}^{N(\mathscr{L})}$ is the canonical closed immersion upon specifying a basis of the space of global sections then we obtain a "naïve height" $h_{\mathscr{L}}$ on $X(\overline{K})$ that is well-defined mod $O(1)$.

Remark 10.2.4. The theorem allows us to define "$h_{\mathscr{L}} : X(\overline{K}) \to \mathbf{R}$" as a "function mod $O(1)$" for any $\mathscr{L}$ arising as $f^*\mathscr{O}(1)$ for a K-morphism $f : X \to \mathbf{P}^n_K$.

To later allow general $\mathscr{L}$ for projective X we write $\mathscr{L}$ as the ratio of two very ample line bundles and then subtract the associated heights. For this to be well-posed modulo $O(1)$, we need to relate $h_{\mathscr{L}_1 \otimes \mathscr{L}_2}$ and $h_{\mathscr{L}_1} + h_{\mathscr{L}_2}$ for $\mathscr{L}_1, \mathscr{L}_2$ as in Theorem 10.2.1. That will come down to understanding the Segre embedding.

The more general theory of heights (modulo $O(1)$) associated to arbitrary line bundles in this way will allow us to study the interaction between heights and the group law, which is necessary for the proof of the Mordell–Weil Theorem.

Now let us develop the theory beginning with Theorem 10.2.1. Let K be a global field, X a proper K-scheme, and $X \xrightarrow{f} \mathbf{P}^n_K$ a K-morphism. Define $h_f := h_{K,n} \circ f : X(\overline{K}) \to \mathbf{R}$. Theorem 10.2.1 amounts to:

Claim. The function h_f is determined modulo $O(1)$ by the isomorphism class of $\mathscr{L} = f^*\mathscr{O}(1)$.

Notice that such $\mathscr{L}$ are generated by global sections, since $\mathscr{O}(1)$ is on $\mathbf{P}^n_K$ (and we can pull back global sections along f). Conversely, if $\mathscr{L}$ on X is generated by global sections then by the universal property of $(\mathbf{P}^n_K, \mathscr{O}(1))$ there is a map $f: X \to \mathbf{P}(\Gamma(X,\mathscr{L}))$ such that $\iota^*_{\mathscr{L}}\mathscr{O}(1) \simeq \mathscr{L}$. From $i_{\mathscr{L}}$ we can also get $h_{i_{\mathscr{L}}}$. This is only determined up to a bounded function, since the map to projective space depends on a choice of basis of the space of global sections of $\mathscr{L}$.

A better statement of the Claim in light of HW10 is:

Theorem 10.2.5. *Given a projective K-scheme X, a line bundle $\mathscr{L}$ on X generated by global sections, and any $X \xrightarrow{f} \mathbf{P}^n_K$ such that $f^*\mathscr{O}(1) \simeq \mathscr{L}$, the difference*

$$h_f - h_{i_{\mathscr{L}}} : X(\overline{K}) \to \mathbf{R}$$

is bounded.

Proof. The map $f^*: \Gamma(\mathbf{P}^n, \mathscr{O}(1)) \to \Gamma(X,\mathscr{L})$ might have non-zero kernel, or in equivalent geometric terms $f(X)$ might lie in a hyperplane $\mathbf{P}^{n-1}_K \simeq H \subset \mathbf{P}^n_K$. But this is harmless, since h_f does not notice this (as we may confirm by using a linear change of coordinates – harmless modulo $O(1)$! – to make H one of the coordinate hyperplane). Thus, without loss of generality assume that $f(X)$ is non-degenerate; i.e., it does not lie in a proper linear subspace of $\mathbf{P}^n_K$, so $\Gamma(\mathbf{P}^n, \mathscr{O}(1)) \to \Gamma(X,\mathscr{L})$ is injective.

Upper bound. We bound h_f by $h_{\iota_{\mathscr{L}}}$ from above. Remember that we can choose whatever *fixed* basis of $\Gamma(X,\mathscr{L})$ we wish since that only changes $h_{i_{\mathscr{L}}}$ by a bounded function, which is harmless. So let us choose bases $T_0,\dots,T_n$ of $\Gamma(\mathbf{P}^n,\mathscr{O}(1))$ and $Z_0,\dots,Z_N$ of $\Gamma(X,\mathscr{L})$, where $Z_0,\dots,Z_n$ are the pullbacks $f^*(T_0),\dots,f^*(T_n)$. By definition it is clear that $h_f \le h_{\iota_{\mathscr{L}}}$ since we are taking a maximum over more values (from $Z_{n+1},\dots,Z_N$).

Lower bound. Now we bound h_f by $h_{\iota_{\mathscr{L}}}$ from below. The main point is that by design $Z_0,\dots,Z_n \in \Gamma(X,\mathscr{L})$ have no common zero on $X(\overline{K})$ since they generate the stalk $(\mathscr{L}_{\overline{K}})_x$ at each $x \in X(\overline{K})$. Thus, X is covered by the open pre-images $D_+(Z_j) = f^{-1}(D_+(T_j))$ for $0 \le j \le n$.

Let $S = K[Z_0,\dots,Z_N]/I \subset \bigoplus_{r\ge 0}\Gamma(X,\mathscr{L}^{\otimes r})$ be the homogeneous coordinate ring for the closed (!) image of $\iota_{\mathscr{L}}: X \to \mathbf{P}^N_K$. This factorizes

$$X \twoheadrightarrow \operatorname{Proj} S \hookrightarrow \mathbf{P}^N$$

For the ideal $J = (Z_0,\dots,Z_n) \subset S$ we have $\operatorname{Proj}(S/J) = \operatorname{Proj}(S) \cap \{Z_0 = \dots = Z_n = 0\}$ as subsets of $\mathbf{P}^N_K$, and this is empty since we observed that the zero locus of $Z_0,\dots,Z_n$ on X is empty. By the Nullstellensatz, it follows that the irrelevant ideal $(Z_0,\dots,Z_N)$ has nilpotent image in S/J (which is obviously equivalent to the same statement for $Z_{n+1},\dots,Z_N$). In other words, there exists $e \ge 1$ such that $Z^e_{n+1},\dots,Z^e_N \in (Z_0,\dots,Z_n)S$.

The upshot is that for $n+1 \le j \le N$,

$$Z_j^e = \sum_{i=1}^{n} F_{ij} Z_j \bmod I$$

where $F_{ij} \in K[Z_0, \dots, Z_n]$ 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):

$$e\, h_{K,\mathscr{L}} \le (e-1) h_{K,\mathscr{L}}(x) + h_f(x) + \text{constant}$$

The contribution $(e-1)h_{K,\mathscr{L}}(x) + h_f(x)$ 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

$$h_{K,\mathscr{L}}(x) \le h_f(x) + O(1).$$

□

Remark 10.2.6. There is a subtlety in that this $O(1)$-term must be uniform for all geometric points x, not just those rational over a fixed extension K'/K. One has to keep track of the factor $[K' : K]^{-1}$ in the definition of the height 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* $(X, \mathscr{L}) \to h_{\mathscr{L}} = h_{K,\mathscr{L}} \in \mathrm{Func}(X(\overline{K}), \mathbf{R})/O(1)$ *satisfying:*

(1) $h_{\mathscr{L}\otimes\mathscr{L}'} = h_{\mathscr{L}} + h_{\mathscr{L}'}$,

(2) $(\mathbf{P}^n_K, \mathscr{O}(1)) \mapsto h_{K,n}$, *the standard height for projective space*

(3) (functoriality) For $X' \xrightarrow{f} X$, *we have* $h_{f^*\mathscr{L}} = h_{\mathscr{L}} \circ f$.

Moreover, for $\mathscr{L}$ *generated by global sections this recovers our earlier construction.*

Proof. Our construction satisfies (2) and (3) for $\mathscr{L}$ generated by global sections. We now check (1) in such cases. Given maps $X \to \mathbf{P}^n$ and $X \to \mathbf{P}^m$ coming from $\mathscr{L}$ and $\mathscr{L}'$, we can build a map for $\mathscr{L} \otimes \mathscr{L}'$ by

$$X \to \mathbf{P}^n \times \mathbf{P}^m \xrightarrow{\text{Segre}} \mathbf{P}^{(n+1)(m+1)-1}$$

using $([t_i], [u_j]) \mapsto [t_i u_j]$. Hence, (1) follows from the identity $\log|ab| = \log|a| + \log|b|$.

In general, for any $\mathscr{L}$ on X and ample $\mathscr{N}$, both $\mathscr{N}^{\otimes n}$ and $\mathscr{L} \otimes \mathscr{N}^{\otimes n} =: \mathscr{N}'$ are very ample for $n \gg 0$, so $\mathscr{L}$ can be expressed as the difference of very ample line bundles $\mathscr{L} = \mathscr{N}_1 \otimes (\mathscr{N}_2)^{-1}$ with both $\mathscr{N}_1$ and $\mathscr{N}_2$ very ample. We may conclude via the following exercise. □

Exercise 10.2.9. Check that we can *uniquely* extend our construction via $h_{\mathscr{L}} = h_{\mathscr{N}_1} - h_{\mathscr{N}_2}$.

For K a global field and X a projective K-scheme, to each line bundle $\mathscr{L}$ on X we've associated a height function

$$h_{\mathscr{L}} : X(\overline{K}) \to \mathbf{R}$$

(well-defined modulo $O(1)$) such that

(1) When $X = \mathbf{P}^n$ and $\mathscr{L} = \mathscr{O}(1)$, then $h_{\mathscr{L}}$ is the standard height (modulo $O(1)$, as always),
(2) for $\varphi: Y \to X$ then $h_{\varphi^*\mathscr{L}} \sim h_{\mathscr{L}} \circ \varphi$, where $h \sim h'$ means $|h - h'|$ is bounded,
(3) $h_{\mathscr{L}_1+\mathscr{L}_2} \sim h_{\mathscr{L}_1} + h_{\mathscr{L}_2}$.

Theorem 10.2.10. *(1) $h_{\mathscr{L}}$ is bounded below on $(X-B)(\overline{K})$ where B is the base locus of $\mathscr{L}$ (i.e. $x \in B$ when every $x \in \Gamma(X, \mathscr{L})$ vanishes at x).*
(2) If $\mathscr{L}$ is ample, then $\#\{x \in X(\overline{K}), [K(x):K] \le n$ and $h_{\mathscr{L}}(x) \le B\} < \infty$.
(3) If $\mathscr{L}$ is ample, X is geometrically reduced and geometrically connected (so $\mathrm{Pic}_{X/K}$ exists), and $\mathscr{M}$ is a line bundle arising from $\mathrm{Pic}^0_{X/K}(K)$ then

$$\lim_{x \in X(\overline{K}), h_{\mathscr{L}}(x) \to \infty} \frac{h_{\mathscr{M}}(x)}{h_{\mathscr{L}}(x)} = 0.$$

That is, for any $\varepsilon > 0$ there exists $N > 0$ such that every $x \in X(\overline{K})$ saitsfying $h_{\mathscr{L}}(x) > N$ also satisfies $|h_{\mathscr{M}}(x)/h_{\mathscr{L}}(x)| < \varepsilon$.

The content of the third part is that $h_{\mathscr{M}+\mathscr{L}}$ and $h_{\mathscr{L}}$ are "basically the same." (They might differ by more than a bounded amount, but at least their ratio goes to 1 over geometric points of growing height.) We will only uses these results with X an abelian variety.

Proof. (1) is the handout "A height bound".

(2) Replacing $\mathscr{L}$ by $\mathscr{L}^{\otimes N}$, we can reduce to the case where $\mathscr{L}$ is very ample, and then to $X = \mathbf{P}^n$ and $\mathscr{L} = \mathscr{O}(1)$. We've already done this (Northcott's Theorem).

(3) For any line bundle $\mathscr{M}'$ arising from Pic^0, $\mathscr{L} \otimes \mathscr{M}'$ is ample; this follows from the Nakai-Moishzeon criterion, and for abelian varieties has been proved directly in this course. In particular, $\mathscr{L} \otimes \mathscr{M}^{\otimes(\pm 1000)}$ is ample. By (1), $h_{\mathscr{L} \otimes \mathscr{M}^{(\pm 1000)}}$ are bounded below so $h_{\mathscr{L}} \pm 1000 h_{\mathscr{M}} \ge C$. Hence, $\pm h_{\mathscr{M}} \le \frac{h_{\mathscr{L}} - C}{1000}$, so

$$|h_{\mathscr{M}}(x)/h_{\mathscr{L}}(x)| \le 1/1000 + C/1000 h_{\mathscr{L}}(x)$$

whenever $h_{\mathscr{L}}(x) > 0$. (Note that C depends on the choice of 1000.) Thus, if $h_{\mathscr{L}}(x) \ge C$ then the absolute ratio is at most $2/1000$. We can play a similar game with 1000 replaced by any large number. □

Theorem 10.2.11. *If A is an abelian variety and $\mathscr{L}$ is a line bundle on A, then*

$$h_{\mathscr{L}}(x+y+z) - h_{\mathscr{L}}(x+y) - h_{\mathscr{L}}(x+z) - h_{\mathscr{L}}(y+z) + h_{\mathscr{L}}(x) + h_{\mathscr{L}}(y) + h_{\mathscr{L}}(z) \sim 0;$$

i.e. $h_{\mathscr{L}}$ is an "approximately quadratic function" on $A(\overline{K})$ (which is to say that its second-difference is almost a constant).

We'll soon see an observation of Tate refining this: there exists a unique genuinely quadratic function $\widehat{h}_{\mathscr{L}} \sim h_{\mathscr{L}}$. Beware we do *not* claim it is a quadratic form for all $\mathscr{L}$; it is more like the quadratic function $a t^2 + b t + c$; i.e., it may have a linear term.

Proof. The Theorem of the Cube gives a similar isomorphism for line bundles on $A \times A \times A$. Plug that into the height machine and evaluate heights at (x, y, z) to conclude. □

10.3. **Tate's canonical height.** Let A be an abelian variety over a global field K and let $\mathscr{L}$ a line bundle on A. We've defined a height function

$$h_{\mathscr{L},K}: A(\overline{K}) \to \mathbf{R}$$

which is well-defined up to $O(1)$. Now we want to construct a *canonical* representative $h_{K,\mathscr{L}} \rightsquigarrow \widehat{h}_{K,\mathscr{L}}: A(\overline{K}) \to \mathbf{R}$ which is a "quadratic function."

Theorem 10.3.1 (Tate)**.** *Let Γ be an abelian group and $h: \Gamma \to \mathbf{R}$ be a function satisfying*

$$h(x_1+x_2+x_3) - h(x_1+x_2) - h(x_3+x_1) - h(x_2+x_3) + h(x_1) + h(x_2) + h(x_3) \sim 0.$$

Then there exists a unique symmetric bilinear form $b: \Gamma \times \Gamma \to \mathbf{R}$ and a linear function $\ell: \Gamma \to \mathbf{R}$ such that

$$h(x) \sim \frac{1}{2} b(x,x) + \ell(x).$$

Before proving this result, let's see how to use it. We may apply this theorem to the function $\Gamma = A(\overline{K}) \xrightarrow{h_{K,\mathscr{L}}} \mathbf{R}$ since we have seen via the Theorem of the Cube that $h_{K,\mathscr{L}}$ satisfies the hypothesis of Tate's theorem. Indeed, the height function for the abelian variety A^3 with respect the line bundle

$$\mathscr{M} = m_{123}^*\mathscr{L} \otimes m_{12}^*\mathscr{L}^{-1} \otimes m_{23}^*\mathscr{L}^{-1} \otimes m_{31}^*\mathscr{L}^{-1} \otimes p_1^*\mathscr{L} \otimes p_2^*\mathscr{L} \otimes p_3^*\mathscr{L} \simeq \mathscr{O}_{A^3}$$

is a bounded function.

By Tate's theorem, we obtain $b_{K,\mathscr{L}}: A(\overline{K}) \times A(\overline{K}) \to \mathbf{R}$ and $\ell_{K,\mathscr{L}}: A(\overline{K}) \to \mathbf{R}$ such that

$$h_{K,L} \sim \frac{1}{2} b_{K,\mathscr{L}} \circ \Delta + \ell_{K,\mathscr{L}}$$

where Δ is the diagonal for $A(\overline{K})$.

Definition 10.3.2. The *Tate canonical height* function on $A(\overline{K})$ is

$$\widehat{h}_{K,\mathscr{L}}(x) = \frac{1}{2} b_{K,\mathscr{L}}(x,x) + \ell_{K,\mathscr{L}}(x).$$

By the preceding discussion, $\widehat{h}_{K,\mathscr{L}} - h_{K,\mathscr{L}} = O(1)$ on $A(\overline{K})$.

We now turn to the proof of Tate's theorem. Actually, we can generalize it:

Definition 10.3.3. If $h: \Gamma \to \mathbf{R}$ is any function, for $r \geq 1$ the rth "polarization" $P_r(h): \Gamma^r \to \mathbf{R}$ is

$$P_r(h)(x_1, \ldots, x_r) = \frac{1}{r} \sum_{I \subset \{1,2,\ldots,r\}} (-1)^{r-\#I} h(x_I)$$

where $x_I = \sum_{i \in I} x_i$ (and $x_\emptyset := 0$).

For $r = 1$ we have $P_1(h): x \mapsto h(x) - h(0)$. If $r = 3$, this is basically the expression that appears in Theorem 10.3.1, except that we include the empty set with the convention that $x_\emptyset = 0$. This is called a polarization because for $r = 2$ it recovers the notion of polarization of quadratic form, whereby one obtains a symmetric bilinear form.

We now discuss the reverse direction.

Definition 10.3.4. Let $A\colon \Gamma^r \to \mathbf{R}$ be multilinear and symmetric. Define $\Delta_r(A)\colon \Gamma \to R$ by

$$\Delta_r(A)(x) = A(x,\dots,x).$$

This generalizes the passage from symmetric bilinear forms to quadratic forms.

Reformulating the condition of multilinearity and symmetry, A can be viewed as an element of $\mathrm{Hom}(S_r(\Gamma),\mathbf{R})$, where $S_r(\Gamma) = (\Gamma \otimes_{\mathbf{Z}} \dots \otimes_{\mathbf{Z}} \Gamma)_{S_r}$ (the coinvariants under the symmetric group).

Proposition 10.3.5. *There is a natural isomorphism*

$$\bigoplus_{j=0}^{r-1} \mathrm{Hom}(S_j\Gamma,\mathbf{R}) \simeq \{h\colon \Gamma \to \mathbf{R} \mid P_r(h) = 0\}$$

given by

$$(A_0, A_1, \dots, A_{r-1}) \mapsto h(x) := A_0 + A_1(x) + A_2(x,x) + \dots + A_{r-1}(x,\dots,x).$$

It's easy to see that P_r kills any such function. (Check it!) Less obvious is that anything killed by P_r actually arises from this construction. We'll prove this soon, but we first state a generalization of Tate's theorem.

Theorem 10.3.6. *The natural map*

$$\bigoplus_{j=1}^{r-1} \mathrm{Hom}(S_j\Gamma,\mathbf{R}) \to \{h\colon \Gamma \to \mathbf{R} \mid P_r h \sim 0\}/O(1)$$

is an isomorphism.

Proof of Proposition. This is a consequence of formal properties of P_r and Δ_r as follows.

(1) If $A \in \mathrm{Hom}(S_r(\Gamma),\mathbf{R})$, 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

$$(P_{r-1}h)(x_0 + x_1, x_2, \dots, x_r) - (P_{r-1}h)(x_0, x_2, \dots) - (P_{r-1}h)(x_1, x_2, \dots).$$

Then this is exactly equal to $P_r h(x_0, x_1, \dots)$.

Exercise 10.3.7. 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 $\mathrm{Hom}(S_{r-1}\Gamma,\mathbf{R})$. 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 $P_{r-1}\Delta_{r-1} = \mathrm{Id}$. Define $A_{r-1} := P_{r-1}h$, so

$$h = \Delta_{r-1}A_{r-1} + h', \quad \text{where } P_{r-1}h' = 0.$$

Then by induction we get the desired surjectivity.

It remains to prove injectivity. Since $P_r\Delta_r(A) = A$ and $P_{r'}\Delta_r(A) = 0$ for $r' > r$, injectivity is easily proved by induction on r. □

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 $P_r h$ may not be exactly 0, $P_{r-1}h$ is may not be exactly multilinear. But it's "asymptotically" multilinear in the sense that

$$(P_{r-1}h)(x_0+x_1,x_2,\dots,x_r)-(P_{r-1}h)(x_0,x_2,\dots)-(P_{r-1}h)(x_1,x_2,\dots)\sim 0.$$

Now Tate's idea is to take a limiting process. Define

$$A_{r-1}(x_1,x_2,\dots,x_{r-1}) = \lim_{N\to\infty} \frac{P_{r-1}h(2^N x_1,\dots,2^N x_{r-1})}{2^{N(r-1)}}.$$

We need to justify that this limit exists. Write $2^N x_1 = 2^{N-1}x_1 + 2^{N-1}x_1$, so

$$|P_{r-1}h(2^N x_1,x_2,\dots,x_{r-1}s)-2P_{r-1}h(2^{N-1}x_1,x_2,\dots,x_{r-1})| \le C.$$

Iterating this for all the coordinates, we obtain

$$|P_{r-1}h(2^N x_1,\dots,2^N x_{r-1})-2^{r-1}P_{r-1}h(2^{N-1}x_1,\dots,2^{N-1}x_{r-1})| \le 2^{r-1}\cdot C.$$

Dividing by $2^{N(r-1)}$, we get a bound

$$\left|\frac{P_{r-1}h(2^N x_1,\dots,2^N x_{r-1})}{2^{N(r-1)}} - \frac{P_{r-1}h(2^{N-1}x_1,\dots,2^{N-1}x_{r-1})}{2^{(N-1)(r-1)}}\right| \le \frac{2^r\cdot C}{2^{N(r-1)}}$$

and that shows that the limit exists (since this forms a Cauchy sequence).

This produces $A_{r-1}\in \mathrm{Hom}(S_{r-1}\Gamma,\mathbf{R})$. If $h' = h-\Delta_{r-1}A_{r-1}$, then

$$\begin{aligned} P_{r-1}h' &= P_{r-1}h - P_{r-1}\Delta_{r-1}A_{r-1} \\ &= P_{r-1}h - A_{r-1} \\ &\sim 0. \end{aligned}$$

Then we proceed by induction, reducing to the base case $P_1 h\sim 0 \iff h\sim 0$. But that's a tautology since $P_1(h)-h$ is a constant function (namely $h(0)$). □

Properties. We consider abelian varieties A over a global field K and varying $\mathscr{L}$ on A. As functions on $A(\overline{K})$ we have:

(1) (Additive) $\widehat{h}_{\mathscr{L}_1\otimes\mathscr{L}_2} = \widehat{h}_{\mathscr{L}_1}+\widehat{h}_{\mathscr{L}_2}$.

(2) (Functoriality) If $f: A\to B$ is a homomorphism of abelian varieties, then

$$\widehat{h}_{f^*\mathscr{L}} = \widehat{h}_{\mathscr{L}}\circ f.$$

(3) (Symmetry) If $\mathscr{L}$ is symmetric (i.e., $\mathscr{L}\simeq[-1]^*\mathscr{L}$) then $\widehat{h}_{\mathscr{L}}$ is even, so the linear part vanishes. We write $\langle\cdot,\cdot\rangle_{\mathscr{L}}$ for the associated symmetric bilinear form, so $\widehat{h}_{\mathscr{L}}(x) = \frac{1}{2}\langle x,x\rangle_{\mathscr{L}}$. (Similarly, if it's antisymmetric then $h_{\mathscr{L}}$ is linear, but that's less useful.)

(4) (Positivity) If $\mathscr{L}$ is ample and symmetric, then $\widehat{h}_{\mathscr{L}}(x)\ge 0$.

(5) (Boundedness) If $\mathscr{L}$ is ample and symmetric then

$$\{x\in A(\overline{K}) \mid [K(x):K]\le d, \widehat{h}_{\mathscr{L}}(x)\le C\}$$

is a finite set (this follows immediately from the analogous statement for $h_{\mathscr{L}}$).

All but (3) are immediate from properties of naive height functions. For the proof of (3), one needs some additional arguments; this is discussed in various references (e.g., see the section on heights my expository article on the Chow trace). The symmetric bilinear form attached to the quadratic form given by the canonical height attached to a symmetric ample line bundle satisfies the requirements for the proof of the Mordell–Weil theorem. Thus, the theorem is proved!

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 $A \times \widehat{A}$ we have the Poincaré line bundle $\mathscr{P}_A$. Then we have a canonical function

$$\widehat{h}_{A\times\widehat{A},\mathscr{P}_A} : A(\overline{K}) \times \widehat{A}(\overline{K}) \to \mathbf{R}.$$

This is the Néron-Tate bilinear pairing, denoted $\langle\cdot,\cdot\rangle_{\mathrm{NT}}$. The bilinearity is proved in various references, such as in the section on heights in my expository article on the Chow trace, where it is also shown that for any $\mathscr{L}$ on A, we have

$$\langle x, \phi_{\mathscr{L}}(x)\rangle_{\mathrm{NT}} = \langle x, x\rangle_{\mathscr{L}}.$$

In other words, the Néron–Tate height pairing encodes the canonical function $\widehat{h}_{\mathscr{L}}$ associated to every line bundle $\mathscr{L}$ on A.

Theorem 10.3.8. *If $\mathscr{L}$ is ample and symmetric then the quadratic form $x \mapsto \frac{1}{2}\langle x, x\rangle_{\mathscr{L}} =: \widehat{h}_{\mathscr{L}}(x)$ on $A(\overline{K})_{\mathbf{R}}$ is positive-definite.*

This is an important fact. To prove it, we just have show that for any finite extension K'/K, on $A(K')_{\mathbf{R}}$ the quadratic form $\widehat{h}$ is positive-definite. We may as welll rename $K' = K$. Without using the Mordell–Weil theorem, we may express $A(K)$ as the directed union of its finitely generated subgroups M_j, and just need to prove positive-definiteness on each $(M_j)_{\mathbf{R}}$. In this finite-dimensional quadratic space, the set of points in the lattice $(M_j)/(M_j)_{\mathrm{tor}}$ with bounded height is finite since $\{x \in A(K) \mid \widehat{h}_{\mathscr{L}}(x) \leq C\}$ is finite. A theorem of Minkowski on quadratic forms implies that any such finite-dimensional quadratic space over $\mathbf{R}$ is positive-definite.

REFERENCES

[BLR] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron Models*, Springer-Verlag, 1986.
[FGA] B. Fantechi et al., *FGA Explained*, AMS Surveys, 2006.
[Mat] H. Matsumura, *Commutative Algebra*, Cambridge University Press, 1990.
[Mum] D. Mumford, *Abelian varieties*, Oxford Univeristy Press, 1970.