The Mordell-Weil Theorem for Abelian Varieties over Global Fields

Zachary Gardner

July 6-10, 2020

These notes accompany the course "Abelian varieties and the Mordell-Weil Theorem" taught at UT Austin Summer Minicourses 2020 (website). Please send all comments, complaints, corrections, and questions to `zacharygardner137@gmail.com`. Any and all feedback is very much appreciated.

Contents

1 Beginnings

1.1 Introduction

The goal of these notes is to prove the Mordell-Weil Theorem for abelian varieties over global fields. In its most basic form, the Mordell-Weil Theorem states that the set $E(\mathbb{Q})$ of $\mathbb{Q}$-rational points of an elliptic curve E is a finitely generated abelian group. By the structure theorem for such groups,

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}$$

with $E(\mathbb{Q})_{\text{tors}}$ torsion and $r \geq 0$ the **rank** of E. Much of arithmetic geometry, number theory, and cryptography has centered around the study of $E(\mathbb{Q})$ and r. It is therefore fair to say that the Mordell-Weil Theorem is a result of much importance. With basic motivation in place, we turn to the statement of the Mordell-Weil Theorem.

Theorem 1.1.1 (Mordell-Weil)**.** *Let k be a global field and A an abelian variety over k. Then, $A(k)$ is a finitely generated abelian group.*

Part of the wisdom of number theory is that number fields (i.e., finite extensions of $\mathbb{Q}$) and global function fields (i.e., finite extensions of $\mathbb{F}_q(t)$ or, equivalently, function fields of algebraic curves over $\mathbb{F}_q$) behave very similarly in many different situations. As such, we collectively refer to both types of fields as **global fields**. Soon we will define precisely what we mean by abelian variety. For now, think of an abelian variety as a variety that also carries a group structure.

Our strategy for proving the Mordell-Weil Theorem will rest on two key results. The first of these, the Weak Mordell-Weil Theorem, is handled in Section 5. The second of these, which concerns the construction of a suitably well-behaved bilinear pairing $\langle \cdot, \cdot \rangle : A(k) \times A(k) \to \mathbb{R}$, is handled in Section 6. The main reference for these notes is [Con15]. We also draw heavy inspiration from [Bha17], which is in turn patterned off of Mumford's classic *Abelian Varieties*.[1] We assume the reader is familiar with algebraic number theory as presented in chapters 1-2 of [Neu99] as well as algebraic geometry as presented in chapters 1-7 of [Liu02]. The next few subsections contain notational and conceptual preliminaries. The actual theory starts in Section 2.

1.2 Category Theory

Sans serif will generally be used to denote the names of categories – e.g., Ab is the category of abelian groups. Given a category C and objects X, Y in C, $\text{Mor}_{\mathsf{C}}(X, Y)$ will be used to denote the set of morphisms from X to Y. If C is additive then we may instead write $\text{Hom}_{\mathsf{C}}(X, Y)$. We write C^{op} for the opposite of C. Given another category D, $\mathsf{Fun}(\mathsf{C}, \mathsf{D})$ denotes the corresponding functor category – i.e., the category whose objects are morphisms from C to D and morphisms are natural transformations. $\mathscr{P}(\mathsf{C}) := \mathsf{Fun}(\mathsf{C}^{\text{op}}, \mathsf{Set})$ is the category of presheaves (of sets) on C, where Set is the category of sets. A functor $\mathscr{F}$ in $\mathscr{P}(\mathsf{C})$ is **representable** if there is an object X of C such that $\mathscr{F} \cong \text{Mor}_{\mathsf{C}}(\bullet, X)$ in $\mathscr{P}(\mathsf{C})$. In this situation, we say X **represents** $\mathscr{F}$.[2]

[1] [Bha17] also includes an enlightening treatment of the theory of Fourier-Mukai transforms and derived categories of coherent sheaves on abelian varieties.

[2] It is important to remember that we need more data than just X for representability.

1.3 Algebraic Geometry

Unless otherwise stated, k denotes a field. Given such a k, fix once and for all compatible choices of algebraic closure $\overline{k}$ and separable closure k_s – i.e., $k_s \subseteq \overline{k}$. All separable and algebraic extensions of k should be assumed compatible with these choices.

Mathscript will generally be used for line bundles – e.g., $\mathscr{L}$ and $\mathscr{P}$.

We let Sch denote the category of schemes. Given a scheme S, we let Sch_S denote the category of S-schemes – i.e., the over category of schemes over S.[3] Given S-schemes X and T, we let X_T denote the base change $X \times_S T$. If either S or T is affine then we may replace them by their underlying ring in notation. For example, if $S = \operatorname{Spec} k$ then $X \times_S T$ becomes $X \times_k T$. The subscript on the fiber product may be dropped if it is clear from context or doing so makes things less cluttered.

Fix a scheme X and consider the following.

- Let $|X|$ denote the underlying set of X. Unless otherwise stated, it is assumed that $|X| \neq \emptyset$. Note that, in general, $|X \times Y|$ is not in bijection with $|X| \times |Y|$.
- Let $\mathsf{Mod}_{\mathcal{O}_X}$ denote the abelian category of (left) $\mathcal{O}_X$-modules. This has full abelian subcategories $\mathsf{QCoh}(X)$ and $\mathrm{Coh}(X)$ of quasi-coherent and coherent $\mathcal{O}_X$-modules, respectively.
- Let $h_X = \mathrm{Mor}_{\mathsf{Sch}}(\bullet, X)$ denote the functor-of-points of X. This resides in $\mathscr{P}(\mathsf{Sch})$ and encodes the same data as X by Yoneda's Lemma. We refer to objects in $\mathscr{P}(\mathsf{Sch})$ or the closely related category $\mathsf{Fun}(\mathsf{CRing}, \mathsf{Set})$ as **spaces**.
- Given $\mathscr{F}$ a sheaf of abelian groups on X, let $H^i(X, \mathscr{F})$ denotes the ith sheaf cohomology group of $\mathscr{F}$. One may think of this as the ith cohomology of $R\Gamma(X, \bullet)$ or as the ith Čech cohomology group of $\mathscr{F}$.
- Let ω_X denote the canonical sheaf of X.[4] Assuming $X \in \mathsf{Sch}_S$, let $\Omega_{X/S} = \Omega^1_{X/S}$ denote the sheaf of Kähler differential 1-forms. Assume $S = \operatorname{Spec} k$ and let $x \in X$ be any k-point. Let $T_{X/k,x} = T_{X,x} = T_x X$ denote the (k-linear) tangent space of X at x. Note that $\Omega_{X/k,x}$ and $T_{X/k,x}$ are canonically dual. Given $f : X \to Y$ a morphism of k-schemes and letting $y = f(x) \in Y$, there is an associated k-linear map $df : T_{X/k,x} \to T_{Y/k,y}$.

Given a scheme X, we let $\mathrm{Pic}(X)$ denote the Picard group of X – i.e., the abelian group consisting of isomorphism classes of line bundles on X whose group structure is encoded by tensor product. This is the same as the sheaf cohomology group $H^1(X, \mathcal{O}_X^\times)$. If $X = \operatorname{Spec} R$ is affine then we may write $\mathrm{Pic}(R)$ instead of $\mathrm{Pic}(X)$. If R is a Dedekind domain then this is the same as the (ideal) class group of R – i.e., the abelian group obtained as the quotient of the group of fractional ideals of R by its subgroup of principal fractional ideals. For X a curve, we let $\mathrm{Pic}^0(X)$ denote the subgroup consisting of isomorphism classes of line bundles of degree 0.

Fix a scheme X and let $\mathscr{F} \in \mathsf{QCoh}(X)$. We say that $\mathscr{F}$ is **globally generated** or **generated by global sections** if, for every $x \in X$, the canonical homomorphism $\phi_x : \mathscr{F}(X) \otimes_{\mathcal{O}_X(X)} \mathcal{O}_{X,x} \to \mathscr{F}_x$ is surjective. Equivalently, there exists a sheaf surjection $\mathcal{O}_X^{\oplus I} \twoheadrightarrow \mathscr{F}$ for some index set I. Given $S \subseteq \mathscr{F}(X)$, $\mathscr{F}$ is **S-globally generated** or **globally generated by** S if, for every $x \in X$, the restriction of ϕ_x to S is surjective. Equivalently, there is a sheaf surjection $\mathcal{O}_X^{\oplus I} \twoheadrightarrow \mathscr{F}$. Finally,

[3] Note that S is the terminal object of this category.

[4] Note that this may not exist in general.

given $d \geq 1$, we say that $\mathscr{F}$ is **d-globally generated** or **generated by d global sections** if there exist sections $s_1, \ldots, s_d \in \mathscr{F}(X)$ such that $\mathscr{F}$ is $\{s_1, \ldots, s_d\}$-globally generated.

Let X be a scheme and $\mathscr{L}$ a line bundle on X. We say that $\mathscr{L}$ is **ample** if, given $\mathscr{F} \in \mathrm{Coh}(X)$, $\mathscr{F} \otimes \mathscr{L}^{\otimes n}$ is globally generated for every $n \gg 0$. If X is an S-scheme, we say that $\mathscr{L}$ is **very ample** (relative to S) if there exists $\mathscr{E} \in \mathsf{QCoh}(S)$ and $i : X \hookrightarrow \mathbb{P}(\mathscr{E})$ a locally closed embedding of S-schemes such that $\mathscr{L} \cong i^*\mathcal{O}_{\mathbb{P}(\mathscr{E})}(1)$. If $S = \operatorname{Spec} R$ then it suffices that there be a closed embedding $i : X \hookrightarrow \mathbb{P}^n_R$ for some $n > 0$. Note that very ample line bundles are always ample. If X is separated of finite type over an affine base and $\mathscr{L}$ is ample then $\mathscr{L}^{\otimes n}$ is very ample for every $n \gg 0$.

1.4 Number Theory

Given a global field k, denote the set of (archimedean and nonarchimedean) places of k by Σ_k.[5] Given $v \in \Sigma_k$, denote the completion of k at v by k_v. Thinking of v as an absolute value on k_v, there is an associated normalized absolute value $\|\cdot\|_v := v^{\epsilon_v}$ on k_v, where

$$\epsilon_v := \begin{cases} 2, & v \text{ is complex} \iff k_v \cong \mathbb{C}, \\ 1, & \text{otherwise.} \end{cases}$$

We let $\Gamma := \mathrm{Gal}(k_s/k)$ denote the absolute Galois group of k, which is naturally a profinite group built up from the Galois groups of finite Galois extensions of k. Similarly, given any Galois extension K of k, we let $\Gamma_K := \mathrm{Gal}(k_s/K)$ denote the profinite Galois group of K. Given $v \in \Sigma_k$ and $w \in \Sigma_K$, we write $w \mid v$ in the case that w extends v (such extensions always exist but need not be unique).

Switching gears, let $S \subseteq \Sigma_k$ be a finite set of places containing the archimedean places. Define the **ring of S-integers** of k to be

$$\mathcal{O}_{k,S} := \{a \in k : v(a) \geq 0 \text{ for every } v \notin S\},$$

which is a Dedekind domain with fraction field k. The S-unit theorem says that $\mathcal{O}_{k,S}^\times$ is a finitely generated abelian group. Similarly, the S-class number theorem says that $\mathrm{Pic}(\mathcal{O}_{k,S})$ is a finite abelian group. As a result, $\mathcal{O}_{k,S}^\times/(\mathcal{O}_{k,S}^\times)^m$ is finite for every $m \in \mathbb{Z}^{>0}$ since it is necessarily torsion.

1.5 Group and Étale Cohomology

Our proof of the Weak Mordell-Weil Theorem will make use of group and étale cohomology. Our discussion here begins with a review of basic notions and notation for group cohomology. Fix G a finite group. Let Mod_G denote the category of (left) G-modules, which is equivalent to the abelian category $\mathsf{Mod}_{\mathbb{Z}[G]}$. Given a G-module M, let $H^\bullet(G, M)$ denote the cohomology of G with coefficients in M, obtained as the derived functor cohomology of $\bullet^G : \mathsf{Mod}_G \to \mathsf{Ab}$ applied to M. Given $H \leq G$, functoriality yields a **restriction** map $\mathrm{Res} : H^\bullet(G, M) \to H^\bullet(H, M)$ induced by $H \hookrightarrow G$. If in addition $H \trianglelefteq G$ then functoriality also yields an **inflation** map $\mathrm{Inf} : H^\bullet(G/H, M) \to H^\bullet(G, M)$ induced by $G \twoheadrightarrow G/H$. There is an associated inflation-restriction sequence

$$0 \longrightarrow H^1(G/H, M) \xrightarrow{\mathrm{Inf}} H^1(G, M) \xrightarrow{\mathrm{Res}} H^1(H, M)$$

[5] Note for the sake of intuition that $\mathbb{Q}$ has only one archimedean place and $\mathbb{F}_q(t)$ has no archimedean places.

whose exactness may be verified either directly or as a consequence of the degeneration of the associated Lyndon-Hochschild-Serre spectral sequence.

Group cohomology generalizes to the setting of profinite groups. Fix G a profinite group (e.g., $G = \Gamma_k$ for any field k). The notion of a (left) G-module M is the same as in the finite group case except that the action of G on M is also required to be continuous. We can talk about G-group cohomology for **discrete** G-modules – i.e., G-modules M such that M is a filtered colimit of M^H for H ranging over the open normal subgroups of G (which are the same as the finite index closed normal subgroups). We then define

$$H^\bullet(G, M) := \varinjlim H^\bullet(G/H, M^H)$$

ranging over the open normal subgroups. This generalized group cohomology is suitably functorial and we obtain versions of inflation, restriction, and the inflation-restriction exact sequence. In either case, $H^1(G, M)$ admits an explicit description as 1-cocycles mod 1-coboundaries, where a 1-cocycle is a continuous crossed homomorphism $\xi : G \to M$ (i.e., $\xi_{gh} = \xi_g + g \cdot \xi_h$ for every $g, h \in G$) and a 1-coboundary is a function $G \to M$ determined by $g \mapsto g \cdot a - a$ for some $a \in M$. Thus, if M is a split G-module in the sense that G acts trivially on M then $H^1(G, M)$ may be identified with the group $\mathrm{Hom}_{\mathrm{cont}}(G, M)$ of continuous homomorphisms.

Shifting our discussion to étale cohomology, we begin with some general categorical preliminaries. A **site** is the data of a category C together with a set $\mathrm{Cov}(\mathsf{C})$ (called a **Grothendieck topology**) of families of morphisms $\{U_i \to U\}_{i \in I}$ with fixed target that contains all isomorphisms in C, is closed under pullback, and is closed under composition in the sense that if $\{U_i \to U\}_{i \in I}$ is a family in $\mathrm{Cov}(\mathsf{C})$ and $\{V_{ij} \to U_i\}_{j \in J_i}$ is also a family in $\mathrm{Cov}(\mathsf{C})$ for every $i \in I$ then $\{V_{ij} \to U\}_{i \in I, j \in J_i}$ is a family in $\mathrm{Cov}(\mathsf{C})$. A **sheaf** (of sets) on a site $(\mathsf{C}, \mathrm{Cov}(\mathsf{C}))$ is a presheaf $\mathscr{F}$ (of sets) on C (so an element of $\mathscr{P}(\mathsf{C})$ defined as before) such that the natural map

$$\mathscr{F}(U) \to \mathrm{Eq}\left(\prod_i \mathscr{F}(U_i) \rightrightarrows \prod_{i,j} \mathscr{F}(U_i \times_U U_j)\right)$$

is an isomorphism for every family $\{U_i \to U\}_{i \in I}$ in $\mathrm{Cov}(\mathsf{C})$. These sheaves form a category called a **Grothendieck topos**. In most situations which we will care about, such as the étale setting described below, the functor-of-points $h_X = \mathrm{Mor}_{\mathsf{C}}(\bullet, X)$ associated an object X in C defines a sheaf on the chosen site associated to C.

There are many interesting and useful Grothendieck topologies that appear in practice, such as the fppf, syntomic, smooth, étale, and Zariski topologies (only the last one is an honest topology in the usual sense). Both the étale and Zariski topologies give rise to small and big variants of a site obtained by varying the underlying category C but keeping the same procedure for building $\mathrm{Cov}(\mathsf{C})$. Enter the notion of étale covering. An **étale covering** of a scheme X is a family $\{f_i : X_i \to X\}_{i \in I}$ of étale morphisms such that $X = \bigcup_{i \in I} f_i(X_i)$. Fix a scheme S. The **big étale site** $(\mathsf{Sch}_S)_{\text{ét}}$ consists of all étale coverings of all S-schemes. The **small étale site** $S_{\text{ét}}$ consists of all étale coverings of all étale S-schemes.[6] The associated Grothendieck topos $\mathsf{Shv}(S_{\text{ét}})$ of sheaves of abelian groups is an abelian category. Given $\mathscr{F}$ an étale sheaf of abelian groups on S, let $H^\bullet_{\text{ét}}(S, \mathscr{F})$ denote the étale cohomology of $\mathscr{F}$ over S, obtained as the derived functor cohomology of the global section

[6] Technically, we need to carry out a refinement procedure in each case to ensure that $\mathrm{Cov}(\mathsf{C})$ is actually a set. The details do not matter for our purposes and so we say nothing further about this.

functor $\Gamma : \mathsf{Shv}(S_{\text{ét}})^{\text{op}} \to \mathsf{Ab}$ applied to $\mathscr{F}$. Note that, given A a k-scheme, there is a canonical identification

$$H^i_{\text{ét}}(\operatorname{Spec} k, A) \cong H^i(\Gamma, A(k_s))$$

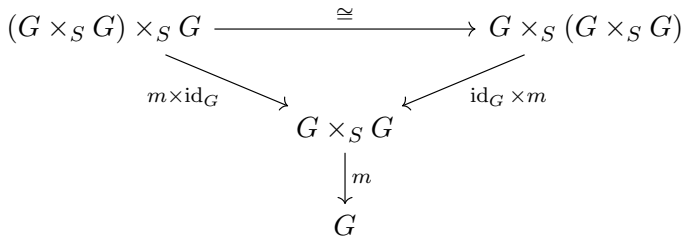
for every i and so we let $H^i(k, A)$ denote either group.

2 Group and Abelian Schemes

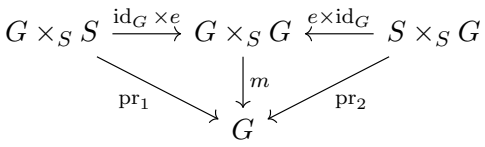
2.1 Group Schemes

Let S be a scheme. An **S-group scheme** is a group object in Sch_S – i.e., an S-scheme G together with morphisms $m : G \times_S G \to G$, $i : G \to G$, and $e : S \to G$ such that the following diagrams commute:

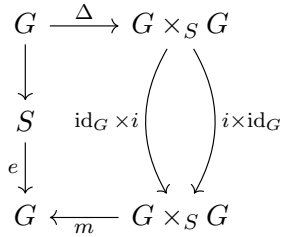
(Associativity)



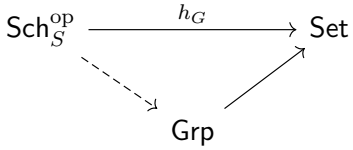
(Identity)



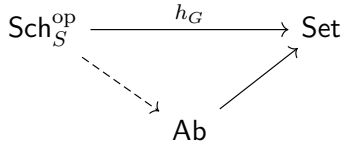
(Inverses)



In the above, $\Delta : G \to G \times_S G$ denotes the (canonical) diagonal morphism and pr_i denotes a (canonical) projection morphism. By Yoneda's Lemma, this is the same data as a group structure on the functor-of-points h_G of G – i.e., for every S-scheme T a group structure on $G(T)$ that is functorial in T. Equivalently, there is a factorization



where the solid unmarked arrow is forgetful. We say that G is **commutative** if there is a factorization



which is equivalent to requiring that G is pointwise invariant under the action of conjugation.

Remark 2.1.1. *The notion of a group scheme is relatively well-behaved. For example, products and base changes of groups schemes are both themselves group schemes.*

Example 2.1.2. *The following are important examples of S-group schemes. We assume for simplicity that $S = \operatorname{Spec} R$ is affine.*

(1) *The **additive group scheme** $\mathbb{G}_{\mathbf{a},S} = \mathbb{G}_{\mathbf{a}}$ has functor-of-points*

$$\mathbb{G}_{\mathbf{a}}(T) := \mathcal{O}_T(T) = \Gamma(T, \mathcal{O}_T)$$

and is represented by $\operatorname{Spec} R[t]$.

(2) *The **multiplicative group scheme** $\mathbb{G}_{\mathbf{m},S} = \mathbb{G}_{\mathbf{m}}$ has functor-of-points*

$$\mathbb{G}_{\mathbf{m}}(T) := \mathcal{O}_T(T)^\times = \Gamma(T, \mathcal{O}_T^\times)$$

and is represented by $\operatorname{Spec} R[t^{\pm 1}]$.

(3) *The **group scheme of mth roots of unity** $\mu_{m,S} = \mu_m$ has functor-of-points*

$$\mu_m(T) := \{f \in \mathbb{G}_{\mathbf{m}}(T) : f^m = 1\}$$

and is represented by $\operatorname{Spec} R[t]/(t^m - 1)$. Its behavior depends heavily on the characteristic of R.

Note that all of these group schemes are commutative.

A **morphism of S-group schemes**[7] is an S-morphism $\phi : G \to H$ such that the diagram

$$\begin{array}{ccc} G \times_S G & \xrightarrow{\phi \times \phi} & H \times_S H \\ \downarrow{\scriptstyle m_G} & & \downarrow{\scriptstyle m_H} \\ G & \xrightarrow{\phi} & H \end{array}$$

commutes. In this way, S-group schemes form their own (non-full) subcategory of Sch_S. As with usual group homomorphisms, we deduce that $\phi \circ e_G = e_H$ and $\phi \circ i_G = i_H \circ \phi$. Similarly, G is commutative if and only if inversion $i : G \to G$ is a morphism of S-group schemes. Given $\phi : G \to H$ a morphism of S-group schemes, $\ker \phi$ is described as a space via

$$(\ker \phi)(T) = \ker(\phi(T) : G(T) \to H(T)),$$

where $T \in \mathsf{Sch}_S$. This space is represented by the S-scheme fiber product of

[7] Common alternative names include S-group homomorphism or simply S-homomorphism.

$$\begin{array}{ccc} & & S \\ & & \downarrow{\scriptstyle e_H} \\ G & \xrightarrow{\phi} & H \end{array}$$

which is a locally closed subscheme of G. It follows that $\ker \phi$ is a well-defined S-group scheme.[8]

Proposition 2.1.3. *Let G be a k-group scheme. Then, there exists a canonical closed k-subgroup scheme G^0 of G such that*

(1) *$G^0 \hookrightarrow G$ is a flat closed embedding;*

(2) *$|G^0|$ is the connected component of the identity of G;*

(3) *G^0 is geometrically irreducible and quasi-compact.*

The scheme G^0 is constructed by taking $|G_0|$ to be the connected component of the identity in G and then attaching the associated canonical scheme structure built up affine locally.[9] The notation G^0 is meant to suggest the relationship of G^0 with the identity element of G. Note that there is an isomorphism of tangent spaces $T_e G^0 \cong T_e G$.

2.2 Abelian Schemes and Varieties

Definition 2.2.1. *An **abelian scheme** over a scheme S is a smooth, proper S-group scheme A with geometrically connected fibers.*[10] *If $S = \operatorname{Spec} k$ then we call A an **abelian variety**. A **morphism of abelian S-schemes** is just a morphism of the underlying S-group schemes.*

It is fruitful to think of abelian schemes as families of abelian varieties over an appropriate base.

Remark 2.2.2. *Note that morphisms of abelian schemes are always proper. To see this, let $f : A \to B$ be a morphism of abelian S-schemes and factor f via the commutative diagram*

$$\begin{array}{ccc} A & \xrightarrow{\quad f \quad} & B \\ & {\scriptstyle \Gamma_f} \searrow \quad \nearrow {\scriptstyle \mathrm{pr}_2} & \\ & A \times_S B & \end{array}$$

where Γ_f is the graph morphism associated to f. Since the structure morphism $B \to S$ is separated, $\Delta_{Y/S} : Y \to Y \times_S Y$ is a closed embedding and so Γ_f is a closed embedding hence proper. The structure morphism $A \to S$ is proper and so pr_2 is proper. It follows that f is proper since properness is preserved under composition. As a result, $\ker f \to S$, obtained as a base change of f, is proper and thus quasi-compact. Moreover, f is finite if and only if it has finite fibers if and only if $\ker f$ is a finite group scheme (as seen by translation).

It follows immediately that the base change of an abelian scheme is an abelian scheme. Given A/k an abelian variety, A is locally of finite type over $\operatorname{Spec} k$ by assumption and so is locally Noetherian by Hilbert's Basis Theorem. It follows that A is Noetherian since it is quasi-compact

[8] The situation for cokernels is a lot more delicate.

[9] See [aut, Tag 047J] for details.

[10] We will see below that abelian schemes are commutative. The term "abelian" here is a reference to the mathematician Niels Henrik Abel.

by assumption.[11] A is geometrically integral since a normal ring whose spectrum is connected is a domain. The condition that the fibers of A be geometrically connected may be relaxed to them being connected since any connected k-scheme with a k-rational point is automatically geometrically connected.[12] The smoothness condition on A can also be relaxed for k perfect, essentially since the smooth locus of A is translation-invariant and will be open and dense under mild hypotheses.

Remark 2.2.3. *Some sources define an abelian variety to be a geometrically integral projective algebraic group, an algebraic group itself being defined as a smooth k-group scheme. Projectivity here is a particularly nontrivial condition to verify given our definition – the verification is precisely Theorem 4.1.2.*

Example 2.2.4. *Perhaps the most important example of an abelian k-variety is an elliptic curve over k (i.e., a smooth projective genus 1 curve over k with distinguished k-rational point), which is automatically connected (and thus geometrically connected as mentioned above) and carries a group scheme structure.*[13] *We see that elliptic curves are precisely the 1-dimensional abelian varieties.*

Exercise 2.2.5. *Given a scheme S, precisely define the notion of a "family of elliptic curves over S."*

Example 2.2.6. *Let C be a smooth, proper curve over k of genus g. Then, its Jacobian $\mathrm{Jac}(C)$ is a k-scheme with the defining property that $\mathrm{Jac}(C)(k) = \mathrm{Pic}^0(C)$ in a functorial manner (e.g., $\mathrm{Jac}(C)(K) = \mathrm{Pic}^0(C_K)$ for every finite field extension K/k). For $k = \mathbb{C}$, $\mathrm{Jac}(C)$ may be identified with the "analytic" Jacobian $\Omega^1_{dR}(C)^*/H_1^{\mathrm{sing}}(C,\mathbb{Z})$ induced by the embedding*

$$H_1^{\mathrm{sing}}(C,\mathbb{Z}) \hookrightarrow \Omega^1_{dR}(C)^*, \qquad [\sigma] \mapsto \int_\sigma \bullet$$

More generally, $\mathrm{Jac}(C)$ is an abelian variety over k of dimension g (more on this later).[14]

Exercise 2.2.7. *Show that the analytic Jacobian satisfies the universal property of the Jacobian in the case $k = \mathbb{C}$ (note that this implicitly involves checking that $\Omega^1_{dR}(C)^*/H_1^{\mathrm{sing}}(C,\mathbb{Z})$ is a complex manifold of the appropriate dimension).*[15]

Remark 2.2.8. *It is somewhat difficult to give examples of abelian varieties that are not the "same as" (i.e., isogenous to) a Jacobian. If you are interested in this topic then you should check out David Masser and Umberto Zannier's paper "Abelian varieties isogenous to no Jacobian."*

Definition 2.2.9. *Let A be an abelian S-scheme, $T \in \mathsf{Sch}_S$, and $x \in A(T)$. Then, the **left translation** morphism $t_x : A_T \to A_T$ is defined to be the composition*

$$A_T \cong T \times_T A_T \xrightarrow{x_T \times \mathrm{id}_{A_T}} A_T \times_T A_T \xrightarrow{m} A_T$$

where $x_T := x \times \mathrm{id}_T : T \to A \times_S T = A_T$. One can check that t_x is given on the level of the functor-of-points by $y \mapsto x + y$.

[11] This result holds in general for abelian schemes over a locally Noetherian base.

[12] See [aut, Tag 0361] for details.

[13] The group law can be specified concretely by choosing a Weierstraß model.

[14] Technically, the construction we have given is actually for what would be called an Albanese variety. Various duality results show the two approaches agree in this setting.

[15] Technically, what we have written here is an Albanese variety.

The remaining results in this section are stated for general abelian schemes but the arguments given technically only work for abelian varieties. The fiberwise reduction to the abelian variety case is left to the reader.

Theorem 2.2.10 (Rigidity)**.** *Let X, Y, Z be k-schemes with X proper, Z separated, and X, Y geometrically integral and finite type. Let $f : X \times_k Y \to Z$ be a k-morphism such that there exists an algebraically closed extension K/k and $y_0 \in Y(K)$ such that the restriction $f_{y_0} : X_K \to Z_K$ of f_K to $X_K \times_K \{y_0\}$ is a constant morphism 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 the diagram*

$$\begin{array}{ccc} X \times_k Y & & \\ {\scriptstyle \mathrm{pr}_2}\downarrow & \searrow^{f} & \\ Y & \xrightarrow[\exists!\ g]{} & Z \end{array}$$

commutes.

The slogan is that if one map is constant in a family of maps $X \to Z$ with X proper then every map in the family is constant. We will most often apply the Rigidity Theorem in the case that $K = \overline{k}$ and y_0 is obtained by pulling back $y_0' \in Y(k)$ such that $f|_{X \times_k \{y_0'\}}$ is constant.

Proof. See [Con15, Thm 1.7.1]. □

Corollary 2.2.11. *Let A, B be abelian S-schemes and $f : A \to B$ an S-morphism. Then, there exists $\phi : A \to B$ a morphism of S-group schemes such that f factors as $f = t_{f(e_A)} \circ \phi$. In particular, if $f(e_A) = e_B$ then f is a morphism of S-group schemes.*

Proof. Post-composing f with $t_{f(e_A)}^{-1} = t_{-f(e_A)}$ if necessary, we may assume that $f(e_A) = e_B$. Consider the k-morphism $h : A \times_k A \to B$ defined by

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

which is constant with value e_B when restricted to $A \times_k \{e_A\}$ and $\{e_A\} \times_k A$.[16] By the Rigidity Theorem, we have commutative diagrams

$$\begin{array}{ccc} A \times_k A & & \\ {\scriptstyle \mathrm{pr}_1}\downarrow & \searrow^{h} & \\ A & \xrightarrow[\exists!\ g_1]{} & B \end{array}$$

and

$$\begin{array}{ccc} A \times_k A & & \\ {\scriptstyle \mathrm{pr}_2}\downarrow & \searrow^{h} & \\ A & \xrightarrow[\exists!\ g_2]{} & B \end{array}$$

[16] Some care is necessary here since $X \times_k Y$ is not in general given as a set by $|X| \times |Y|$. A more rigorous definition of h is

$$h := m_B(f \circ m_A, i_B \circ f \circ \mathrm{pr}_2, i_B \circ f \circ \mathrm{pr}_1).$$

What we do in this argument is work on the level of the functor-of-points.

Given any $a_1, a_2 \in A$, we have $g_1(a_1) = h(a_1, a_2) = g_2(a_2)$ and so

$$g_1(a) = h(a, e_A) = e_B = h(e_A, a) = g_2(a)$$

for every $a \in A$. Hence, h is constant with value e_B – i.e., f is a homomorphism. □

One consequence of this theorem is the following.

Corollary 2.2.12. *Let $A \in \mathsf{Sch}_S$ and $e \in A(S)$. Then, there is at most one abelian S-scheme structure on A such that e is the identity section.*

Thus, the multiplication and inversion morphisms for an abelian scheme carry redundant information already encoded by a choice of identity section. This is useful for deformation theory arguments as it means that the we do not have to keep as careful track of group laws as would a priori seem necessary.

Proof. Let (m_1, i_1) and (m_2, i_2) encode abelian S-scheme structures on A, each with identity section e. By the Rigidity Theorem, $\mathrm{id}_A : (A, m_1, i_1) \to (A, m_2, i_2)$ is a homomorphism and so $m_1 = m_2$ and $i_1 = i_2$. □

Corollary 2.2.13. *Let A be an abelian scheme. Then, A is commutative.*

Proof. Apply the Rigidity Theorem to $i : A \to A$. □

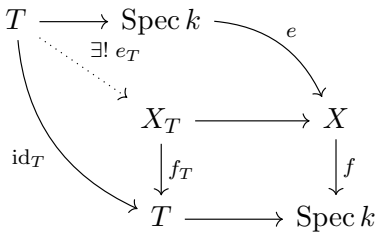
Remark 2.2.14. *An alternative proof comes from showing that the action of conjugation is infinitesimally trivial. See [Con15, Thm 1.5.1] for more details.*

3 Line Bundles on Abelian Varieties

3.1 Rigidification and Picard Functors

Throughout this section, let X be a proper, geometrically reduced, geometrically connected k-scheme with $X(k) \neq \emptyset$. Our goal is to understand how to classify families of line bundles on X. We will do this by constructing the Picard functor for X/k and explaining why it is representable, thereby obtaining the Picard scheme of X/k. In order to avoid the theory of stacks, we employ rigidification constraints to guarantee that the Picard functor satisfies the Zariski sheaf condition. Note that, though in general the assumption that $X(k)$ is nonempty is too strong if we want to construct Picard schemes, the assumption is harmless for our purposes as we will be applying the theory to the case of abelian varieties.

Let $f : X \to \operatorname{Spec} k$ denote the structure morphism of X. Let $T \in \mathsf{Sch}_k$ and $e \in X(k)$. We obtain a commutative diagram

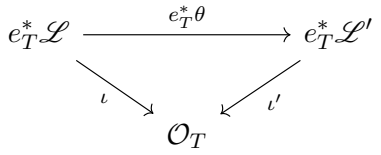


with $e_T \in X_T(T)$ a section of f_T induced by the universal property of X_T as a pullback.

Definition 3.1.1. *Let $T \in \mathsf{Sch}_k$ and choose $e \in X(k)$. Define $\mathcal{R}_{T,X/k,e}$ to be the category of rigidified line bundles on X_T consisting of pairs $(\mathscr{L}, \iota)$ with $\mathscr{L}$ a line bundle on X_T and*

$$\iota : e_T^* \mathscr{L} \xrightarrow{\sim} \mathcal{O}_T,$$

*called a **rigidification** of $\mathscr{L}$ along e. A morphism in $\mathcal{R}_{T,X/k,e}$ is $\theta : (\mathscr{L}, \iota) \to (\mathscr{L}', \iota')$ such that $\theta : \mathscr{L} \to \mathscr{L}'$ is an X_T-sheaf morphism and the diagram*



commutes.

The set $\mathcal{R}_{T,X/k,e}/\cong$ of isomorphism classes carries a natural group structure encoded by tensor product. This group structure is contravariantly functorial in the sense that, given $T \to T'$ a k-scheme morphism, there is a group homomorphism

$$\mathcal{R}_{T',X/k,e}/\cong \to \mathcal{R}_{T,X/k,e}/\cong .$$

This allows us to define the **Picard functor** $\underline{\mathrm{Pic}}_{X/k,e} : \mathsf{Sch}_k \to \mathsf{Ab}$ by

$$T \mapsto \mathcal{R}_{T,X/k,e}/\cong .$$

The discussion following [Con15, Def 2.2.11] shows that $\underline{\mathrm{Pic}}_{X/k,e}$ is independent of the choice of e in the sense that, given $e' \in X(k)$ and $T \in \mathsf{Sch}_k$, there is a natural change of base point isomorphism

$$\underline{\mathrm{Pic}}_{X/k,e}(T) \xrightarrow{\sim} \underline{\mathrm{Pic}}_{X/k,e'}(T).$$

As such, we may omit e from the notation $\underline{\mathrm{Pic}}_{X/k,e}$.[17] The following result shows that the Picard functor admits a more concrete description that is useful for computational purposes.[18]

Proposition 3.1.2. *The natural map $\mathcal{R}_{T,X/k,e}/\cong \to \mathrm{Pic}(X_T)/f_T^* \mathrm{Pic}(T)$ given by*

$$[(\mathscr{L}, \iota)] \mapsto \mathscr{L} \ \mathit{mod}\ f_T^* \mathrm{Pic}(T)$$

is a group isomorphism compatible with change of base point.

Our goal is to show that the Picard functor is representable. An important step toward representability is the following.

[17] Grothendieck actually gave a construction that makes no explicit mention of a k-rational point.
[18] See [Con15, Prop 2.2.12] for details.

Theorem 3.1.3. $\underline{\mathrm{Pic}}_{X/k,e}$ *is a Zariski sheaf.*

Proof. Given $T \in \mathsf{Sch}_k$ and $\{U_i\}$ a Zariski open cover of T by k-schemes, we need to show that a system of isomorphism classes $[(\mathscr{L}_i, \iota_i)] \in \mathcal{R}_{U_i,X/k,e}/\cong$ agreeing on overlaps glues uniquely to $[(\mathscr{L}, \iota)] \in \mathcal{R}_{T,X/k,e}/\cong$ which restricts to each $[(\mathscr{L}_i, \iota_i)]$. Paraphrasing, we need to show that a system of isomorphisms

$$\mathscr{L}_i|_{X_{U_{ij}}} \xrightarrow{\sim} \mathscr{L}_j|_{X_{U_{ij}}}$$

compatible with ι_i, ι_j extends to a globally defined rigidified line bundle $\mathscr{L}$ on X_T unique up to isomorphism of rigidified line bundles on X_T. This reduces to showing that $(\mathscr{L}, \iota) \in \mathcal{R}_{T,X/k,e}$ has no nontrivial automorphisms, as such automorphisms are precisely the obstruction to gluing. To see this, let θ be an automorphism of $(\mathscr{L}, \iota)$. Then, θ is a line bundle automorphism of $\mathscr{L}$ and so corresponds to some element of $\Gamma(X_T, \mathcal{O}_{X_T}^\times)$. By [Con15, Lemma 2.2.1], $f_T : X_T \to T$ induces a natural isomorphism $\mathcal{O}_T \xrightarrow{\sim} (f_T)_*\mathcal{O}_{X_T}$ and hence a natural isomorphism $\mathcal{O}_T^\times \xrightarrow{\sim} (f_T)_*\mathcal{O}_{X_T}^\times$.[19] Passing to global sections gives $\Gamma(T, \mathcal{O}_T^\times) \cong \Gamma(X_T, \mathcal{O}_{X_T}^\times)$ and so θ is multiplication by some $u \in \Gamma(T, \mathcal{O}_T^\times)$. It follows that $e_T^*\theta$ is also multiplication by u. Since $\iota = \iota \circ e_T^*\theta$ by assumption and ι is an isomorphism, $e_T^*\theta$ is the identity map and so $u = 1$. □

The full picture is provided by the following.

Theorem 3.1.4 (Grothendieck/Oort-Murre/Artin)**.** *The Picard functor* $\underline{\mathrm{Pic}}_{X/k,e}$ *is represented by a locally finite type* k*-scheme* $\mathrm{Pic}_{X/k,e} = \mathrm{Pic}_{X/k}$.

Proof. See [Fan+05, Part 5] for a proof as well as a wealth of other information on Picard functors. □

Note that, in general, if $\underline{\mathrm{Pic}}_{X/k,e}$ is representable then it is represented by a separated k-group scheme.[20] For C a smooth proper k-curve with $C(k) \neq \emptyset$, the associated Picard scheme is none other than the familiar Jacobian $\mathrm{Jac}(C)$.

3.2 The Theorems of the Cube and Square

Now that we have the notion of Picard scheme, we are well-equipped to study the behavior of families of line bundles. Let $X, Y \in \mathsf{Sch}_k$, $y \in Y(k)$, and $\mathscr{L}$ a line bundle on $X \times_k Y$. Define $\mathscr{L}_y$ to be the restriction

$$\mathscr{L}_y := \mathscr{L}|_{X \times_k \{y\}}.$$

The restriction of $\mathscr{L}$ to $x \in X(k)$ is defined similarly. Assuming that X and Y are proper, geometrically integral, and finite type, one might hope that if $\mathscr{L}_x$ and $\mathscr{L}_y$ are trivial for some $x \in X(k)$ and $y \in Y(k)$ then $\mathscr{L}$ itself is trivial. Unfortunately, this is not the case in general.

Example 3.2.1. *Let* (E, e) *be an elliptic curve over* k *and* p *any* k*-rational point of* E*. Then, it is easy to check that* $\mathcal{O}(\Delta - \mathrm{pr}_1^* e - \mathrm{pr}_2^* e)$ *restricts to* $\mathcal{O}_E(p - e)$ *on both* $\{p\} \times_k E$ *and* $E \times_k \{p\}$*. Taking* $p = e$ *therefore yields trivial restrictions, and taking* $p \neq e$ *yields non-trivial restrictions (as follows from Riemann-Roch).*

[19] Here, it is essential that X is geometrically reduced since then $\Gamma(X, \mathcal{O}_X) \cong k$. See [aut, Tag 0366] for details.

[20] This follows since any group scheme over a field is separated. See [aut, Tag 047G and 047J] for details.

Fortunately, the situation can be remedied by passing from pairs of k-schemes to triples.

Theorem 3.2.2 (Theorem of the Cube)**.** *Let $X, Y, Z \in \mathsf{Sch}_k$ such that X, Y are proper, X, Z are geometrically integral and finite type, and Y is geometrically reduced and geometrically connected. Let $\mathscr{L}$ be a line bundle on $X \times_k Y \times_k Z$ and $x_0 \in X(k), y_0 \in Y(k), z_0 \in Z(k)$. Suppose that $\mathscr{L}_{x_0}, \mathscr{L}_{y_0}, \mathscr{L}_{z_0}$ are all trivial. Then, $\mathscr{L}$ is trivial.*

Proof. By Theorem 3.1.4, $\underline{\mathrm{Pic}}_{Y/k,y_0}$ is represented by a separated, locally finite type k-scheme $\mathrm{Pic}_{Y/k}$ and so the data of a trivialization of $\mathscr{L}_{y_0}$ is equivalent to the data of a k-morphism $f : X \times_k Z \to \mathrm{Pic}_{Y/k}$. We claim that f vanishes and so $\mathscr{L}$ is trivial. By assumption, $\mathscr{L}_{z_0}$ is trivial and so applying the universal property of $\mathrm{Pic}_{Y/k}$ once again gives that the restriction $f_{z_0} : X \times_k \{z_0\} \to \mathrm{Pic}_{Y/k}$ vanishes. By the Rigidity Theorem, there is a commutative diagram

$$\begin{array}{ccc} X \times_k Z & & \\ {\scriptstyle \mathrm{pr}_2}\downarrow & \searrow^{f} & \\ Z & \overset{\exists!\, g}{\dashrightarrow} & \mathrm{Pic}_{Y/k} \end{array}$$

Since $\mathscr{L}_{x_0}$ is trivial, the restriction $f_{x_0} : \{x_0\} \times_k Z \to \mathrm{Pic}_{Y/k}$ vanishes and so g hence f vanishes by commutativity of the diagram. □

Corollary 3.2.3. *Let A/k be an abelian variety, $T \in \mathsf{Sch}_k$, $a_1, a_2, a_3 \in A(T)$, and $\mathscr{L}$ a line bundle on A. Then, $\mathscr{L}(a_1, a_2, a_3)$ defined by*

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

is a canonically trivial line bundle on T.

Remark 3.2.4. *Since $e^*\mathscr{L}$ is trivial, we may remove the term $(e^*\mathscr{L})_T^{-1}$ in the above at the cost of making the isomorphism non-canonical.*

Proof. Since $A^3 = A \times_k A \times_k A$ is the universal k-scheme with a triple of k-morphisms to A, it suffices to consider the case that $T = A^3$ and each a_i is a projection morphism. More precisely, the canonical isomorphism $\mathscr{L}(\mathrm{pr}_1, \mathrm{pr}_2, \mathrm{pr}_3) \to \mathcal{O}_{A^3}$ induces an isomorphism

$$\begin{aligned} \mathscr{L}(a_1, a_2, a_3) &\cong (a_1 \times a_2 \times a_3)^*\mathscr{L}(\mathrm{pr}_1, \mathrm{pr}_2, \mathrm{pr}_3) \\ &\cong (a_1 \times a_2 \times a_3)^*\mathcal{O}_{A^3} \\ &\cong \mathcal{O}_T. \end{aligned}$$

Having made this reduction, the Theorem of the Cube tells us that it suffices to check triviality on $\{e\} \times A \times A$, $A \times \{e\} \times A$, and $A \times A \times \{e\}$. By symmetry we need only consider $\{e\} \times A \times A \cong A^2$. We obtain a series of canonical isomorphisms

$$\begin{aligned} (a_1 + a_2 + a_3)^*\mathscr{L} \otimes (a_2 + a_3)^*\mathscr{L}^{-1} &\cong \mathcal{O}_{A^2}, \\ (a_1 + a_2)^*\mathscr{L}^{-1} \otimes a_2^*\mathscr{L} &\cong \mathcal{O}_{A^2}, \\ (a_1 + a_3)^*\mathscr{L}^{-1} \otimes a_3^*\mathscr{L} &\cong \mathcal{O}_{A^2}, \\ a_1^*\mathscr{L} \otimes (e^*\mathscr{L})_{A^2}^{-1} &\cong \mathcal{O}_{A^2}, \end{aligned}$$

from which the result follows after tensoring up. □

Let $\mathscr{L}$ be a line bundle on an abelian scheme A/S. Then, the **Mumford bundle** of A is the line bundle $\Lambda(\mathscr{L})$ on $A \times_S A$ defined by

$$\Lambda(\mathscr{L}) := m^*\mathscr{L} \otimes \mathrm{pr}_1^*\mathscr{L}^{-1} \otimes \mathrm{pr}_2^*\mathscr{L}^{-1}.$$

Theorem 3.2.5 (Theorem of the Square)**.** *Let A/k be an abelian variety, $\mathscr{L}$ a line bundle on A, $T \in \mathsf{Sch}_k$, and $x, y \in A(T)$. Then, there is a natural isomorphism*

$$t_{x+y}^*\mathscr{L}_{A_T} \otimes \mathscr{L}_{A_T} \cong t_x^*\mathscr{L}_{A_T} \otimes t_y^*\mathscr{L}_{A_T} \otimes [(x \times y)^*\Lambda(\mathscr{L}) \otimes e^*\mathscr{L}]_{A_T}$$

of line bundles on A_T, where the subscript A_T denotes pullback by the projection $p : A_T \to A$. In particular, since $(x \times y)^*\Lambda(\mathscr{L}) \otimes e^*\mathscr{L}$ is a line bundle on $\operatorname{Spec} k$ hence trivial, there is a non-canonical isomorphism

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

Proof. Let c_x denote the constant morphism given by the composition

$$A_T \longrightarrow T \xrightarrow{x} A$$

Define c_y in a similar manner. By Corollary 3.2.3, there is a natural isomorphism

$$(p + c_x + c_y)^*\mathscr{L} \otimes p^*\mathscr{L} \cong (p + c_x)^*\mathscr{L} \otimes (p + c_y)^*\mathscr{L} \otimes (c_x + c_y)^*\mathscr{L} \otimes c_x^*\mathscr{L}^{-1} \otimes c_y^*\mathscr{L}^{-1} \otimes (e^*\mathscr{L})_{A_T}.$$

We have $p + c_x = p \circ t_x$, $p + c_y = p \circ t_y$, and $c_x + c_y = c_{x+y}$. Hence,

$$(p + c_x)^*\mathscr{L} = (p \circ t_x)^*\mathscr{L} = t_x^*\mathscr{L}_{A_T},$$

with similar results for y and $x+y$. Unpacking the definition of $\Lambda(\mathscr{L})$ yields a natural isomorphism

$$c_{x+y}^*\mathscr{L} \otimes c_x^*\mathscr{L}^{-1} \otimes c_y^*\mathscr{L}^{-1} \cong ((x \times y)^*\Lambda(\mathscr{L}))_{A_T}.$$

The result follows. □

Corollary 3.2.6. *Let A/k be an abelian variety and $\mathscr{L}$ a line bundle on A. Then, the k-morphism $\phi_{\mathscr{L}} : A \to \mathrm{Pic}_{A/k}$ defined by*

$$x \mapsto t_x^*\mathscr{L} \otimes \mathscr{L}^{-1}$$

is a morphism of group schemes.[21]

Morphisms of the type $\phi_{\mathscr{L}}$ are massively important for their relationship to dual abelian varieties.

Proof. The definition of $\phi_{\mathscr{L}}$ given above is somewhat imprecise. A more precise definition is as follows. Let $T \in \mathsf{Sch}_k$ and $x \in A(T)$. Then,

$$\phi_{\mathscr{L}}(T)(x) = \phi_{\mathscr{L}}(x) := t_x^*\mathscr{L}_{A_T} \otimes \mathscr{L}_{A_T}^{-1}.$$

[21] Technically, $\phi_{\mathscr{L}}$ sends x to the isomorphism class of $t_x^*\mathscr{L} \otimes \mathscr{L}^{-1}$. We will often ignore this technicality and freely interchange between isomorphism classes of line bundles and their representatives.

Given $x, y \in A(T)$, applying the Theorem of the Square yields

$$\begin{aligned}\phi_{\mathscr{L}}(x+y) &= t_{x+y}^*\mathscr{L}_{A_T} \otimes \mathscr{L}_{A_T}^{-1} \\ &\cong (t_x^*\mathscr{L}_{A_T} \otimes t_y^*\mathscr{L}_{A_T} \otimes \mathscr{L}_{A_T}^{-1}) \otimes \mathscr{L}_{A_T}^{-1} \\ &\cong (t_x^*\mathscr{L}_{A_T} \otimes \mathscr{L}_{A_T}^{-1}) \otimes (t_y^*\mathscr{L}_{A_T} \otimes \mathscr{L}_{A_T}^{-1}) \\ &= \phi_{\mathscr{L}}(x) \otimes \phi_{\mathscr{L}}(y).\end{aligned}$$

The result follows. □

Exercise 3.2.7. *Use the Theorem of the Square to deduce other properties of $\phi_{\mathscr{L}}$. For example, what can be said about $\phi_{t_x^*\mathscr{L}}$ for $x \in A(k)$?*

4 Dual Abelian Varieties

Now that we understand some of the behavior of families of line bundles on an abelian variety, let's put that understanding to use.

4.1 Line Bundles and Duals

The subscheme $\mathrm{Pic}^0_{X/k}$ has many nice properties by Lemma 2.1.3. In the case of an abelian variety A,

$$A^\vee := \mathrm{Pic}^0_{A/k}$$

is called the **dual** of A. Some justification for the superscript notation comes from the case of curves.

Exercise 4.1.1. *Let X be a proper, geometrically reduced, geometrically connected k-scheme of dimension 1 with $X(k) \neq \emptyset$ and genus g. Then, $\mathrm{Pic}^0_{X/k}$ is smooth of dimension g and satisfies*

$$\mathrm{Pic}_{X/k}(K) \cong \{[\mathscr{L}] \in \mathrm{Pic}(X_K) : \deg \mathscr{L} = 0\}$$

for every field extension K/k.[22]

Letting $Y := \mathrm{Pic}_{X/k}$, we have $\underline{\mathrm{Pic}}_{X/k,e}(Y) = [(\mathscr{U}_X, \iota_X)]$. The pair $(\mathscr{U}_X, \iota_X)$ is called the **universal rigidified line bundle of** X (relative to e) and is unique up to isomorphism of rigidified line bundles. By definition, $\mathscr{U}_X$ is a line bundle on $X \times_k Y = X_Y$ and $\iota_X : e_Y^*\mathscr{U}_X \xrightarrow{\sim} \mathcal{O}_Y$. Given any $T \in \mathsf{Sch}_k$ and $(\mathscr{L}, \iota)$ a rigidified bundle on X_T, there exists a unique k-morphism $\varphi : T \to Y$ such that

$$(\mathscr{L}, \iota) = (\mathrm{id}_X \times \varphi)^*(\mathscr{U}_X, \iota_X).$$

Restricting now to the case of abelian varieties, let $(\mathscr{U}_A, \iota_A)$ be the universal rigidified line bundle of A associated to e, so that $\mathscr{U}_A$ is a line bundle on $A \times_k \mathrm{Pic}_{A/k}$ and $\iota_A : \mathscr{U}_A|_{\{e\}\times_k \mathrm{Pic}_{A/k}} \xrightarrow{\sim} \mathcal{O}_{\mathrm{Pic}_{A/k}}$. Define the **Poincaré bundle** $\mathscr{P}_A$ to be the line bundle on $A \times_k A^\vee$ obtained by restricting $(\mathscr{U}_A, \iota_A)$ to $A \times_k A^\vee$. We have a rigidification $\mathscr{P}_A|_{A\times_k\{0\}} \xrightarrow{\sim} \mathcal{O}_A$, which can be made canonical by fixing the

[22] This exercise is [Con15, Exercise 2.4.3]. See the reference for hints.

image of $(e,0)$. Every k-morphism $Y \to \mathrm{Pic}_{A/k}$ corresponds uniquely to the data of a rigidified line bundle $(\mathscr{L}, \iota)$ with $\mathscr{L}$ a line bundle on $A \times_k Y$ and $\iota : \mathscr{L}_e \xrightarrow{\sim} \mathcal{O}_Y$, obtained via $(\mathrm{id}_A \times \varphi)^*(\mathscr{U}_A, \iota_A)$ for a unique k-morphism $\varphi : Y \to \mathrm{Pic}_{A/k}$. By the universal property of $\mathscr{P}_A$, the morphism $Y \to \mathrm{Pic}_{A/k}$ factors through $A^\vee$ precisely when $\mathscr{L}$ is pr_2-trivialized in the sense that pulling back $(\mathscr{P}_A, \iota_A)$ and restricting induces a compatible family of trivializations $\mathscr{L}_y \xrightarrow{\sim} \mathcal{O}_A$ for $y \in Y(k)$.

Let's apply all of the above to $\phi_{\mathscr{L}} : A \to \mathrm{Pic}_{A/k}$ for $\mathscr{L}$ a line bundle on A. We deduce immediately that φ as above is exactly $\phi_{\mathscr{L}}$ in this context. We claim that $\phi_{\mathscr{L}}$ factors through $A^\vee$ – i.e., $(\mathrm{id}_A \times \phi_{\mathscr{L}})^*(\mathscr{P}_A)$ is pr_2-trivialized. [Con15, Prop 3.3.1] shows that there is a natural identification $(\mathrm{id}_A \times \phi_{\mathscr{L}})^*(\mathscr{P}_A) \cong \Lambda(\mathscr{L})$ compatible with the rigidifications on each. But, $\Lambda(\mathscr{L})$ is pr_2-trivialized since, given $x \in A(k)$,

$$\Lambda(\mathscr{L})|_{A \times_k \{x\}} = (m^*\mathscr{L} \otimes \mathrm{pr}_1^*\mathscr{L}^{-1} \otimes \mathrm{pr}_2^*\mathscr{L}^{-1})|_{A \times_k \{x\}} \cong \mathscr{L} \otimes \mathscr{L}^{-1} \otimes \mathcal{O}_A \cong \mathcal{O}_A.$$

Theorem 4.1.2. *Let A/k be an abelian variety. Then, A is projective.*

Proof. The goal is to produce an ample line bundle on A. Our argument is a sketch of the one given in the proof of [Con15, Thm 3.4.1]. Here are the steps.

(1) Using Galois descent, reduce to the case $k = \overline{k}$.

(2) Let U be an open affine neighborhood of e in A. Show that $D := (A - U)_{\mathrm{red}}$ is an effective Weil divisor.[23]

(3) Show that $\{x \in A(k) : t_x^* D = D\}$ is finite.

(4) Letting $\mathscr{L} := \mathcal{O}_A(D)$, deduce that $\mathscr{L}^{\otimes 2}$ is globally generated with $i_{\mathscr{L}} : A \to \mathbb{P}\Gamma(A, \mathscr{L}^{\otimes 2})$ finite (note that $i_{\mathscr{L}}$ need not a priori be an embedding).

Since $i_{\mathscr{L}}$ is finite, $\mathscr{L}^{\otimes 2} \cong i_{\mathscr{L}}^* \mathcal{O}(1)$ is ample by [aut, Tag 0B5V] and so we deduce that $\mathscr{L}$ is ample. □

4.2 Duals as Abelian Varieties

Our goal in this section is to show that the dual of an abelian variety is itself an abelian variety and explore some of its geometry useful for proving the Mordell-Weil Theorem.

Theorem 4.2.1. *Let A/k be an abelian variety. Then, the dual $A^\vee$ is an abelian variety.*

Remark 4.2.2. *Note that, for $X \in \mathsf{Sch}_k$ and $x \in X(k)$, there is a natural identification of k-vector spaces*

$$T_{X/k,x} = T_x X = \{y \in X(k[\epsilon]) : \mathcal{C}(y) \text{ commutes}\},$$

where $k[\epsilon]$ is the k-algebra defined by $\epsilon^2 = 0$ and $\mathcal{C}(y)$ is the diagram

$$\begin{array}{ccc} \operatorname{Spec} k & \longrightarrow & \operatorname{Spec} k[\epsilon] \\ & {\scriptstyle x} \searrow \quad \swarrow {\scriptstyle y} & \\ & X & \end{array}$$

[23] See [Bha17, Lemma 10.10] for details.

with horizontal arrow induced by the map $k[\epsilon] \to k$ given by $\epsilon \mapsto 0$.

Proof. This boils down to showing that $A^\vee/k$ is

(i) a geometrically connected group scheme;

(ii) proper;

(iii) smooth.[24]

We check each of these conditions separately.

(i) By construction, $A^\vee = \mathrm{Pic}^0_{A/k}$ is a geometrically irreducible closed k-group subscheme of $\mathrm{Pic}_{A/k}$ and so is a fortiori geometrically connected.

(ii) It suffices to show that $\mathrm{Pic}_{A/k}$ is proper. The idea is to use the valuative criterion of properness. Since the structure morphism $\mathrm{Pic}_{A/k} \to \operatorname{Spec} k$ is finite type, we need only consider DVRs (discrete valuation rings) instead of valuation rings more generally. Let R be a DVR which is a k-algebra and K its fraction field. We claim any commutative diagram

$$\begin{array}{ccc} \operatorname{Spec} K & \longrightarrow & \mathrm{Pic}_{A/k} \\ \downarrow & & \downarrow f \\ \operatorname{Spec} R & \longrightarrow & \operatorname{Spec} k \end{array}$$

can be filled in uniquely to get a commutative diagram

$$\begin{array}{ccc} \operatorname{Spec} K & \longrightarrow & \mathrm{Pic}_{A/k} \\ \downarrow & \overset{\exists!}{\nearrow} & \downarrow f \\ \operatorname{Spec} R & \longrightarrow & \operatorname{Spec} k \end{array}$$

The k-morphism $\operatorname{Spec} K \to \mathrm{Pic}_{A/k}$ is equivalent to the data of a line bundle on A_K with a rigidification $\iota : \mathscr{L}_{e_K} \xrightarrow{\sim} \mathcal{O}_{\operatorname{Spec} K}$, where $e_K \in A_K(K)$ is induced by $e \in A(k)$. A similar statement applies to $\operatorname{Spec} R$ and so our goal is to construct a line bundle $\mathscr{M}$ on A_R with rigidification $\iota' : \mathscr{M}_{e_R} \xrightarrow{\sim} \mathcal{O}_{\operatorname{Spec} R}$ compatible with $(\mathscr{L}, \iota)$ under pullback. Identifying X with A_R, this boils down to the following statement. Let η by the generic point of R and $\mathscr{L}$ a line bundle on the generic fiber X_η. Then, $\mathscr{L}$ extends to a line bundle defined on all of X. The idea is to use that X_η is an integral K-scheme to think of $\mathscr{L}$ as a Cartier divisor on X_η and then use the projectivity of X to extend this to a Cartier divisor on X. See [Alt14] for details.

(iii) Let $g := \dim A$. By translation, smoothness reduces to showing that $\dim A^\vee = \dim_k T_0 A^\vee$. We will show that both of these numbers are g. Here are the steps.

(1) $\dim_k T_0 A^\vee = \dim_k H^1(A, \mathcal{O}_A)$.

(2) $g \leq \dim A^\vee \leq \dim_k T_0 A^\vee$.

(3) $\dim_k H^1(A, \mathcal{O}_A) \leq g$.

[24] If $\operatorname{char} k = 0$ then $A^\vee$ is automatically smooth since a celebrated theorem of Cartier gives that every finite type k-group scheme is smooth. The argument we give shows that $\mathrm{Pic}_{A/k}$ is smooth. This is perhaps somewhat surprising since Picard schemes, even if they exist, need not in general be smooth in positive characteristic.

By the remark, there is an isomorphism of k-vector spaces given by

$$T_0 A^\vee \cong T_0 \operatorname{Pic}_{A/k} \cong \ker(\operatorname{Pic}_{A/k}(k[\epsilon]) \to \operatorname{Pic}_{A/k}(k)).$$

The inclusion $k \hookrightarrow k[\epsilon]$ makes $\operatorname{Spec} k[\epsilon]$ into a k-scheme. Let $A[\epsilon] := A_k \times_k [\epsilon]$ and denote by $f[\epsilon] : A[\epsilon] \to \operatorname{Spec} k[\epsilon]$ the corresponding base change of the structure morphism $f : A \to \operatorname{Spec} k$. By Proposition 3.1.2, there are isomorphisms $\operatorname{Pic}_{A/k}(k) \cong \operatorname{Pic}(A)$ and

$$\operatorname{Pic}_{A/k}(k[\epsilon]) \cong \operatorname{Pic}(A[\epsilon])/f[\epsilon]^* \operatorname{Pic}(k[\epsilon]) \cong \operatorname{Pic}(A[\epsilon])$$

that fit into a commutative diagram

$$\begin{array}{ccc} \operatorname{Pic}_{A/k}(k[\epsilon]) & \longrightarrow & \operatorname{Pic}_{A/k}(k) \\ \cong\downarrow & & \downarrow\cong \\ \operatorname{Pic}(A[\epsilon]) & \longrightarrow & \operatorname{Pic}(A) \end{array}$$

with horizontal arrows given by pullback. We have a sort of exponential short exact sequence

$$1 \longrightarrow 1 + \epsilon \mathcal{O}_{A[\epsilon]} \longrightarrow \mathcal{O}_{A[\epsilon]}^\times \longrightarrow \mathcal{O}_A^\times \longrightarrow 1$$

Under the identification $1 + \epsilon \mathcal{O}_{A[\epsilon]} \xrightarrow{\sim} \mathcal{O}_A$ given by $1 + \epsilon\sigma \mapsto \sigma$, we get a short exact sequence

$$1 \longrightarrow \mathcal{O}_A \xrightarrow{\exp} \mathcal{O}_{A[\epsilon]}^\times \longrightarrow \mathcal{O}_A^\times \longrightarrow 1$$

and hence a commutative diagram

$$\begin{array}{ccccccccc} H^0(A, \mathcal{O}_{A[\epsilon]}^\times) & \xrightarrow{\psi} & H^0(A, \mathcal{O}_A^\times) & \longrightarrow & H^1(A, \mathcal{O}_A) & \xrightarrow{\exp} & H^1(A, \mathcal{O}_{A[\epsilon]}^\times) & \longrightarrow & H^1(A, \mathcal{O}_A^\times) \\ & & & & & & \cong\downarrow & & \downarrow\cong \\ & & & & & & \operatorname{Pic}(A[\epsilon]) & \longrightarrow & \operatorname{Pic}(A) \end{array}$$

We have $H^1(A, \mathcal{O}_A^\times) \cong k^\times$ and so dimensional considerations give that ψ is surjective. Hence, $\ker \exp \cong \operatorname{coker} \psi = 0$ and so

$$T_0 A^\vee \cong H^1(A, \mathcal{O}_A) \implies \dim_k T_0 A^\vee = \dim_k H^1(A, \mathcal{O}_A).$$

This shows (1). By Theorem 4.1.2, A is projective and so it has an ample line bundle $\mathscr{L}$. By Lemma 5.1.12, $\phi_{\mathscr{L}} : A \to A^\vee$ is finite and so is a fortiori quasi-finite. It follows that $g \leq \dim A^\vee$. This shows (2) since $\dim A^\vee \leq \dim_k T_0 A^\vee$ is automatic. (3) is precisely [Con15, Prop 5.1.1], which uses Serre duality, the Künneth formula, and a theorem of Borel on the structure of Hopf algebras to deduce that the map $\wedge^i H^1(A, \mathcal{O}_A) \to H^i(A, \mathcal{O}_A)$ induced by cup product is an isomorphism for every $i \geq 0$.[25] □

5 The Weak Mordell-Weil Theorem

We now embark on our first of two major tasks involved in proving the Mordell-Weil Theorem, starting with a discussion of isogeny and torsion.

[25] [Bha17, Cor 15.4] gives a different proof using Koszul complexes which, with some extra work, shows that the cohomology algebra of A is isomorphic to the exterior k-algebra of $H^1(A, \mathcal{O}_A)$. This is an important starting point for the theory of the Fourier-Mukai transform.

5.1 Isogeny and Torsion

In every field of mathematics, it is important to know in what sense the objects of interest are the "same." In the context of abelian varieties, that notion of equivalence is isogeny.

Definition 5.1.1. *An **isogeny** is a finite flat surjective morphism of abelian varieties. An abelian variety A is said to be **isogenous** to another abelian variety B if there exists an isogeny $f : A \to B$. For such f, the **degree** is defined to be* $\deg(f) := [k(A) : k(B)]$.

Remark 5.1.2. *It is clear that isogeny is a reflexive and transitive relation. We will see later that it is also symmetric and so defines an equivalence relation.*

Given $f : A \to B$ a morphism of abelian varieties, it is natural to ask when f is an isogeny.

Example 5.1.3. *If A, B are elliptic curves and f is nonzero then it is a classical fact that f is an isogeny (and is an isomorphism if and only if* $\deg(f) = 1$*).*[26] *This need not be the case for A, B general abelian varieties of the same dimension.*

Exercise 5.1.4. *Construct such a counterexample.*

Lemma 5.1.5. *Let $f : A \to B$ be a morphism of abelian k-varieties.*

(a) *Suppose f is flat. Then, f is surjective.*

(b) *Suppose f is surjective. Then, f is flat.*

(c) *Suppose f is finite and surjective. Then,* $\dim A = \dim B$.

(d) *Suppose* $\dim A = \dim B$. *Then, f is flat if and only if it is finite.*

Proof. We begin by noting some facts about dimension. Let e denote the identity of A. Given $x \in A$, $t_x : A \to A$ is an isomorphism and so induces a k-linear isomorphism $dt_x : T_eA \to T_xA$. Hence,

$$\dim \mathcal{O}_{A,x} = \dim_k T_xA = \dim_k T_eA = \dim \mathcal{O}_{A,e}$$

by smoothness and so $\dim A = \dim \mathcal{O}_{A,x}$. At the same time, f is flat if and only if

$$\dim \mathcal{O}_{A,x} = \dim \mathcal{O}_{B,y} + \dim \mathcal{O}_{f^{-1}(y),x} \tag{1}$$

for every $x \in A$ with $y = f(x) \in B$.[27]

(a) Since f is a flat morphism between irreducible schemes, f is dominant.[28] Since f is proper, f has closed image and so is surjective.

(b) By Grothendieck's Generic Flatness, there is a nonempty open $U \subseteq B$ such that the restriction $f^{-1}(U) \to U$ is flat.[29] Equation (1) therefore holds on $f^{-1}(U) \neq \emptyset$ and so holds everywhere by translation.

[26] More generally, morphisms between projective curves are either constant or surjective.
[27] See [aut, Tag 00R4] for details. This result often goes by the name of Miracle Flatness.
[28] The point is that f lifts generalizations. See [edg18] for details.
[29] See [aut, Tag 0529] for details.

(c) The key is that a scheme has dimension n if and only if it has a cover by affine opens each of dimension $\leq n$ with at least one open having dimension exactly n. With that said, choose such a cover $\mathcal{C}$ realizing the dimension of B. Since f is finite hence affine, f pulls back $\mathcal{C}$ to a cover of A by open affines. For each $U \in \mathcal{C}$, $f^{-1}(U)$ is nonempty and so has the same dimension as U (recall that f is proper and so is integral in this setting). It follows that $\dim A = \dim B$.

(d) The empty fibers of f are obviously well-behaved, so we will handle the nonempty fibers. Let $x \in A$ with $y = f(x) \in B$. Since $\dim A = \dim B$, Equation (1) gives that f is flat at x if and only if $\dim \mathcal{O}_{f^{-1}(y),x} = 0$. Since $f^{-1}(y)$ is quasi-compact, it is finite if and only if it has dimension 0 and so f is flat if and only if it is finite. □

An important notion in our discussion of isogeny is that of torsion. Given $m \in \mathbb{Z}$ and A an abelian group, let $A[m]$ denote the m-torsion subgroup of A (i.e., the kernel of the multiplication map $[m] : A \to A$). If A/S is an abelian scheme then we let $A[m]$ denote the m-torsion subscheme of A, which naturally fits into a Cartesian diagram

$$\begin{array}{ccc} A[m] & \longrightarrow & S \\ \downarrow & & \downarrow{\scriptstyle e} \\ A & \xrightarrow[[m]]{} & A \end{array}$$

Theorem 5.1.6. *Let A/S be an abelian scheme and $m \in \mathbb{Z}^{\neq 0}$. Then, $[m] : A \to A$ is an isogeny.*[30] *If in addition m is invertible in S (i.e., $m \in \mathcal{O}_S(S)^\times$) then $[m]$ is étale.*

Proof. Suppose first that m is invertible in S. We claim it suffices to show that $[m]$ is étale. To see this, suppose that $[m]$ is étale. Then, $[m]$ is flat and locally quasi-finite with open image. Since $[m]$ is also proper, $[m]$ is finite by [aut, Tag 02LS] and surjective since it has closed image. Hence, we are reduced to showing that $[m]$ is étale. Since flatness may be checked fiber-wise, we may assume without loss of generality that $S = \operatorname{Spec} k$.[31] Since the structure morphism $A \to \operatorname{Spec} k$ is smooth by assumption, [BLR90, Cor 2.2/10] gives that $[m]$ is étale at $x \in A$ if and only if the canonical homomorphism $[m]^*\Omega_{A/k} \to \Omega_{A/k}$ induces an isomorphism on stalks at x. Dualizing, this is equivalent to the natural homomorphism $d[m] : T_{A/k,x} \to T_{A/k,[m]x}$ being an isomorphism of k-vector spaces. A small inductive argument gives that $d[m]$ is simply multiplication by m.[32] It follows that $d[m] : T_{A/k,e} \to T_{A/k,e}$ is an isomorphism (since m is invertible in k) and the diagram

$$\begin{array}{ccc} T_{A/k,e} & \xrightarrow{d[m]} & T_{A/k,e} \\ {\scriptstyle dt_x}\downarrow & & \downarrow{\scriptstyle dt_{[m]x}} \\ T_{A/k,x} & \xrightarrow[d[m]]{} & T_{A/k,[m]x} \end{array}$$

commutes. Since t_x and $t_{[m]x}$ are both isomorphisms, dt_x and $dt_{[m]x}$ are isomorphisms and so $d[m] : T_{A/k,x} \to T_{A/k,[m]x}$ is an isomorphism.

[30] Note that the notion of isogeny generalizes easily from abelian varieties to all abelian schemes.

[31] See [BLR90, Section 2.2 and 2.4] for details.

[32] We see immediately that $[m]$ is not étale if m is not invertible in k since then $d[m]$ is not an automorphism of $T_e A$.

Now, consider the more general case where $[m]$ is not assumed to be invertible in S. As mentioned earlier, flatness may be checked fiber-wise. Since surjectivity and finiteness may also be checked fiber-wise, we may assume without loss of generality that $S = \operatorname{Spec} k$. By Lemma 5.1.5, it suffices to show that $[m]$ is finite, which is the same as showing that $A[m]$ has dimension 0. By Theorem 4.1.2, A is projective and so we may choose $\mathscr{L}$ an ample line bundle on A. Consider the symmetric line bundle $\mathscr{M} := \mathscr{L} \otimes [-1]^*\mathscr{L}$, which is ample since $\mathscr{L}$ is ample and $[-1]$ is an automorphism.[33] By Lemma 5.1.7 (statement and proof below), we have

$$[m]^*\mathscr{M} \cong \mathscr{M}^{\otimes (m^2+m)/2} \otimes [-1]^*\mathscr{M}^{\otimes (m^2-m)/2} \cong \mathscr{M}^{\otimes m^2},$$

which is ample since $\mathscr{M}$ is ample and $m^2 > 0$. At the same time,

$$([m]^*\mathscr{M})|_{A[m]} \cong [m]^*(\mathscr{M}|_{A[m]}) \cong \mathcal{O}_{A[m]}.$$

Hence, $A[m]$ is affine along with all of its (nonempty) closed subschemes.[34] It follows that $A[m]$ must have dimension 0 since otherwise it would contain a proper closed k-curve which must necessarily be non-affine. □

Lemma 5.1.7. *Let A/k be an abelian variety, $m \in \mathbb{Z}$, and $\mathscr{L}$ a line bundle on A. Then,*

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

Proof. The claim clearly holds for $m = 0, 1$. The idea of the proof is to use Corollary 3.2.3 to induct up and down. The argument for inducting down is very similar to the one for inducting up and so we omit it. Let $m \in \mathbb{Z}$ and assume the result holds for m and $m+1$. Consider the maps $[m+1], [1] = \mathrm{id}_A, [-1] = -\mathrm{id}_A : A \to A$. By Corollary 3.2.3,

$$\mathcal{O}_A \cong [m+1]^*\mathscr{L} \otimes [m+2]^*\mathscr{L}^{-1} \otimes [m]^*\mathscr{L}^{-1} \otimes [m+1]^*\mathscr{L} \otimes \mathscr{L} \otimes [-1]^*\mathscr{L},$$

where we have used that pulling back by [0] gives a trivial bundle. Rearranging and applying the inductive hypothesis gives

$$\begin{aligned}
[m+2]^*\mathscr{L} &\cong ([m+1]^*\mathscr{L})^{\otimes 2} \otimes ([m]^*\mathscr{L})^{-1} \otimes \mathscr{L} \otimes [-1]^*\mathscr{L} \\
&\cong \mathscr{L}^{\otimes (m^2+3m+2)} \otimes [-1]^*\mathscr{L}^{\otimes (m^2+m)} \otimes \mathscr{L}^{\otimes -(m^2+m)/2} \otimes [-1]^*\mathscr{L}^{\otimes -(m^2-m)/2} \mathscr{L} \otimes [-1]^*\mathscr{L} \\
&= \mathscr{L}^{\otimes (m^2+5m+6)/2} \otimes [-1]^*\mathscr{L}^{\otimes (m^2+3m+2)/2},
\end{aligned}$$

which is of the desired form. □

Moreover, the following result shows that $[m]$ is in some sense the prototypical example of an isogeny between abelian varieties.

Theorem 5.1.8. *Let $f : A \to B$ be a morphism of abelian k-varieties. Then, f is an isogeny if and only if there exists $d \in \mathbb{Z}^{\neq 0}$ and $g : B \to A$ an isogeny such that $g \circ f = [d]_A$. In either case, $f \circ g = [d]_B$.*

[33] A line bundle $\mathscr{L}$ on A is **symmetric** if $\mathscr{L} \cong [-1]^*\mathscr{L}$ and **anti-symmetric** if $\mathscr{L}^{-1} \cong [-1]^*\mathscr{L}$.

[34] Here, we have made use of a combination of Serre's criteria for ampleness and affineness, which together say that a proper R-scheme X for R a Noetherian ring is affine if and only if $\mathcal{O}_X$ is ample.

Proof. Suppose first that f is an isogeny and let $d := \deg(f) \in \mathbb{Z}^{\neq 0}$. Then, $\ker f$ is a finite group scheme of rank d and so is annihilated by multiplication by d. It follows that $[d]_A$ factors as

$$A \xrightarrow{f} B \xrightarrow{g} A$$

for $g : B \to A$ some morphism of abelian varieties. Since $[d]_A$ is surjective, g is also surjective. Since f is an isogeny, $\dim A = \dim B$ and so g is finite flat hence an isogeny. Since g is a morphism of abelian varieties,

$$g \circ [d]_B = [d]_A \circ g = (g \circ f) \circ g = g \circ (f \circ g) \tag{2}$$

and so $[d]_B = f \circ g$. For the converse, suppose that there exists $d \in \mathbb{Z}^{\neq 0}$ and $g : B \to A$ an isogeny such that $g \circ f = [d]_A$. The computation in Equation (2) shows that $[d]_B = f \circ g$ and so f is surjective since $[d]_B$ is surjective. Since g is an isogeny, $\dim A = \dim B$ and so f is finite flat hence an isogeny. □

Exercise 5.1.9. *Fill in the following details to complete the proof of the previous theorem.*

(1) *Let $\pi : G \to S$ be locally free group scheme of rank r with S a reduced irreducible scheme.*[35] *Show that G is annihilated by multiplication by r – i.e., $[r]_G$ given on points by $g \mapsto g^r$ is the 0-morphism $[0]_G = e \circ \pi : G \to S \to G$.*[36]

(2) *Let $f : A \to B$ be a morphism of abelian k-varieties and $d \in \mathbb{Z}$ such that multiplication by d annihilates $\ker f$. Show that $[d]_A$ factors*

$$A \xrightarrow{f} B \xrightarrow{g} A$$

for $g : B \to A$ a morphism of abelian varieties.

(3) *Let W, X, Y, Z be abelian k-varieties. Let $f : W \to X$ and $h : Y \to Z$ be isogenies and $g_1, g_2 : X \to Y$ homomorphisms such that $h \circ g_1 \circ f = h \circ g_2 \circ f$. By working with $\overline{k}$-points, show that f, h can be canceled to get $g_1 = g_2$.*

Given a group scheme G/S, G determines a sheaf of groups on the small étale site $S_{\text{ét}}$ via its functor-of-points h_G. For commutative group schemes, we similarly get étale sheaves of abelian groups. Group subschemes give rise to injections on the level of étale sheaves. One reason this matters is the following result.

Corollary 5.1.10. *Let A/S be an abelian scheme and $m \in \mathbb{Z}$ invertible in S. Then, the sequence*

$$0 \longrightarrow A[m] \longrightarrow A \xrightarrow{[m]} A \longrightarrow 0$$

of commutative S-group schemes is short exact

Proof. The only nontrivial part is checking exactness at the right term (exactness elsewhere can be verified directly or by looking at geometric stalks). Let U be an étale S-scheme and $\alpha \in h_A(U)$. The morphism $[m] : A \to A$ induces a corresponding natural transformation $[m] : h_A \to h_A$. Define U' so that it sits in a Cartesian diagram

[35] Recall that this means that π is affine and $\pi_* \mathcal{O}_G$ is a rank r locally free $\mathcal{O}_S$-module.
[36] This is [MGE14, Exercise (4.4)].

$$\begin{array}{ccc} U' & \xrightarrow{\beta} & A \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle[m]} \\ U & \xrightarrow[\alpha]{} & A \end{array}$$

Then, ϕ is an étale surjection since $[m]$ is an étale surjection by Theorem 5.1.6 and so $\{\phi : U' \to U\}$ is an étale covering of U. By construction, $[m]\beta = \alpha$ and we have our result. □

Exercise 5.1.11. *Given A an abelian k-variety and $m \in \mathbb{Z}^{\neq 0}$, Theorem 5.1.6 shows that $[m] : A \to A$ is an isogeny. It is then natural to ask for the degree. There are several ways of going about this (such as using intersection theory) but we will take the approach of using Euler characteristic. Namely, let X be a proper k-scheme, $\mathscr{L}$ a line bundle on X, and $\mathscr{F} \in \mathrm{Coh}(X)$. Then, $\chi(\mathscr{F} \otimes \mathscr{L}^{\otimes r})$ is a numeric polynomial in r of degree $\leq g = \dim X$ – i.e., it assumes integral values at integers and so is a $\mathbb{Z}$-linear combination of binomial coefficients. Hence, there is some $d_{\mathscr{L}}(\mathscr{F}) \in \mathbb{Z}$ such that*

$$\chi(\mathscr{F} \otimes \mathscr{L}^{\otimes r}) = \frac{d_{\mathscr{L}}(\mathscr{F})}{g!} r^g + (\textit{lower order terms}).$$

We let $\deg(\mathscr{L}) := d_{\mathscr{L}}(\mathcal{O}_X)$.

(1) *Given $n \in \mathbb{Z}$, show that $\deg(\mathscr{L}^{\otimes n}) = n^g \deg(\mathscr{L})$.*

(2) *Let $f : X' \to X$ be a finite morphism of schemes with X proper integral and d the degree of the generic fiber. Given $\mathscr{L}$ a line bundle on X, show that $\deg(f^*\mathscr{L}) = d \cdot \deg(\mathscr{L})$.*

(3) *Show that $\deg([m]) = m^{2g}$, where $g = \dim A$.*

(Bonus!) *Let X be a smooth proper k-curve. Show that our notion of degree agrees with the one for line bundles on X defined in terms of divisors.*

(Bonus!) *Let X be a proper integral k-scheme and $\mathscr{L}$ a very ample line bundle over X. Show that our notion of degree agrees with the one obtained by taking the k-rank of the finite intersection with a generic codimension-g linear subspace.*

Though not directly relevant to the remainder of these notes, the last two results in this section help tie the notion of isogeny to the structure of abelian varieties and their duals.

Proposition 5.1.12. *Let A/k be an abelian variety and $\mathscr{L}$ an ample line bundle on A. Then, $\phi_{\mathscr{L}} : A \to A^\vee$ is an isogeny.*

Proof. Since $\dim A = \dim A^\vee$, Lemma 5.1.5 tells us that $\phi_{\mathscr{L}}$ is an isogeny if it is finite.[37] By previous work, we know that $\phi_{\mathscr{L}}$ is proper and $\phi_{\mathscr{L}}$ is finite if and only if $\ker \phi_{\mathscr{L}}$ is finite. Since $\ker \phi_{\mathscr{L}}$ is quasi-compact, the latter holds if and only if the abelian subvariety $B := (\ker \phi_{\mathscr{L}})^0_{\mathrm{red}}$ has dimension 0.[38] Since $\mathscr{L}$ is ample, $\mathscr{M} := \mathscr{L}|_B$ is also ample. At the same time, $\phi_{\mathscr{M}} = 0$ by assumption. Hence,

$$\mathcal{O}_{B \times_k B} \cong (\mathrm{id}_B \times \phi_{\mathscr{M}})^* \mathscr{P}_B \cong \Lambda(\mathscr{M}).$$

Restricting to the anti-diagonal in $B \times_k B$, we have

$$\mathcal{O}_B \cong (e^*\mathscr{M})_B \otimes \mathscr{M}^{-1} \otimes [-1]^*\mathscr{M}^{-1} \cong \mathscr{M}^{-1} \otimes [-1]^*\mathscr{M}^{-1}.$$

[37] Such isogenies (i.e., those that map an abelian variety to its dual) are called **polarizations**.

[38] We take the reduction so that B has nonzero smooth locus, which we then translate to show B is smooth.

Inverting this gives $\mathcal{O}_B \cong \mathscr{M} \otimes [-1]^*\mathscr{M}$, which is ample since $\mathscr{M}$ is ample and $[-1]$ is an isomorphism. Hence, B is affine. It follows that B must have dimension 0 since otherwise it would contain a proper closed k-curve which necessarily must be non-affine. □

Corollary 5.1.13. *Let A/k be an abelian variety. Under the identification $\mathrm{Pic}^\vee_{A/k}(\overline{k}) = \mathrm{Pic}(A_{\overline{k}})$,*

$$A^\vee(\overline{k}) = \{[\mathscr{L}] \in \mathrm{Pic}(A_{\overline{k}}) : \phi_{\mathscr{L}} = 0\}.$$

Proof. Assume without loss of generality that $k = \overline{k}$. Given $\mathscr{L}$ a line bundle on A with $\phi_{\mathscr{L}} = 0$, $\Lambda(\mathscr{L})$ is trivial and so $[\mathscr{L}] \in A^\vee(k)$ by earlier discussion. For the converse, let $[\mathscr{L}] \in A^\vee(k)$. Using that A is projective, choose $\mathscr{M}$ an ample line bundle on A. Then, $\phi_{\mathscr{M}} : A \to A^\vee$ is an isogeny and so is surjective on k-points since $k = \overline{k}$. Hence, there is $x \in A(k)$ such that $\mathscr{L} \cong \phi_{\mathscr{M}}(x)$. Given $y \in A(k)$,

$$\phi_{\mathscr{L}}(y) = t_y^*\mathscr{L} \otimes \mathscr{L}^{-1} \cong t_{x+y}^*\mathscr{M} \otimes t_y^*\mathscr{M}^{-1} \otimes t_x^*\mathscr{M}^{-1} \otimes \mathscr{M} \cong \mathcal{O}_A$$

by the Theorem of the Square and so $\phi_{\mathscr{L}} = 0$. □

5.2 Proof of the Weak Mordell-Weil Theorem

Now we get to the heart of the matter.

Theorem 5.2.1 (Weak Mordell-Weil)**.** *Let k be a global field, A an abelian variety over k, and $m \in \mathbb{Z}^{\geq 2}$ such that $m \nmid \operatorname{char} k$. Then, the quotient $A(k)/m$ is finite.*

Proof. The main idea of the proof is to realize $A(k)/m$ as a subgroup of an appropriate cohomology group which is finite. Where does cohomology enter the picture? By Corollary 5.1.10, the sequence

$$0 \longrightarrow A[m] \longrightarrow A \xrightarrow{[m]} A \longrightarrow 0$$

of commutative k-group schemes is short exact over the étale site of $\operatorname{Spec} k$. Hence, passing to group/étale cohomology yields an exact sequence

$$A(k) \xrightarrow{[m]} A(k) \xrightarrow{\delta} H^1(k, A[m])$$

and hence an embedding $A(k)/m \hookrightarrow H^1(k, A[m])$ with image $\delta(A(k))$. We need to carefully analyze this image since $H^1(k, A[m])$ is not in general finite.[39] As explained in the proof of [Con15, Thm 9.3.11], we can "spread out" the abelian variety $A \to \operatorname{Spec} k$ to get an abelian scheme $\mathcal{A} \to U$ whose generic fiber is A, where $U := \operatorname{Spec} \mathcal{O}_{k,S}$ for some $S \subseteq \Sigma_k$ finite containing the archimedean places such that m and $\#|A[m]| = \#A[m](k_s)$ are S-units.[40] It then follows that we may identify $A(k)$ and $\mathcal{A}(U)$ as well as their quotients $A(k)/m$ and $\mathcal{A}(U)/m$.[41] By Corollary 5.1.10, the sequence

[39] Even in the nice case that $\mu_m \subseteq k$, Kummer theory tells us that $H^1(k, \mu_m) \cong k^\times/(k^\times)^m$ and so $H^1(k, A[m])$ is a product of infinite groups since $A[m](k_s) \cong \mu_m^{2g}$ for $g := \dim A$.

[40] Classically, one takes S to include the places of bad reduction for A and uses Néron models to construct $\mathcal{A}$. See [Poo17, Section 3.2] for more on spreading out.

[41] This boils down to denominator chasing at the places away from S and the valuative criterion for properness over a Dedekind base at the places in S.

$$0 \longrightarrow \mathcal{A}[m] \longrightarrow \mathcal{A} \xrightarrow{[m]} \mathcal{A} \longrightarrow 0$$

is exact on $U_{\text{ét}}$ and so passing to étale cohomology yields an embedding $\mathcal{A}(U)/m \hookrightarrow H^1_{\text{ét}}(U, \mathcal{A}[m])$ fitting into a commutative diagram

$$\begin{array}{ccc} \mathcal{A}(U)/m & \hookrightarrow & H^1_{\text{ét}}(U, \mathcal{A}[m]) \\ \| & & \downarrow \\ A(k)/m & \hookrightarrow & H^1(k, A[m]) \end{array}$$

with unmarked vertical arrow induced by $U \to \operatorname{Spec} k$. Thus, instead of studying the image $\delta(A(k))$ we may study the image of $\mathcal{A}(U)/m \hookrightarrow H^1_{\text{ét}}(U, \mathcal{A}[m])$. We accomplish this by imposing certain ramification conditions.

Given $u \in U$ a closed point (equivalently, a nonzero prime ideal of $\mathcal{O}_{k,S}$), the **inertia group** I_u of u is a subgroup of Γ obtained in one of two equivalent ways.[42] The first approach is to view it as the Galois group $\operatorname{Gal}((k_u)_s/k_u^{\text{unr}})$ for $(k_u)_s$ and k_u^{unr} compatible separable closure and maximal unramified extension of the completion k_u, respectively. This embeds into the absolute Galois group Γ_{k_u} and hence Γ by restriction (i.e., by sending σ to $\sigma|_{k_s}$, thinking of k_s as embedded nicely in $(k_u)_s$). The second approach is to view I_u as the Galois group of the fraction field of the strict henselization $\mathcal{O}_{U,u}^{\text{sh}}$ of the local ring $\mathcal{O}_{U,u}$, which has the important property that every finite étale cover of $\operatorname{Spec} \mathcal{O}_{U,u}^{\text{sh}}$ is split and so it is cohomologically trivial for the étale topology (we think of $\operatorname{Spec} \mathcal{O}_{U,u}^{\text{sh}}$ as the étale local neighborhood of U at u). This again embeds into Γ via an appropriate restriction procedure.

No matter the approach taken, we obtain I_u as a subgroup of Γ well-defined up to conjugation (i.e., different choices of embedding yield conjugate subgroups). The equivalence between these two approaches comes from unpacking the construction of k_u^{unr} and $\mathcal{O}_{U,u}^{\text{sh}}$. $\mathcal{O}_{U,u}^{\text{sh}}$ is characterized by being universally strictly henselian with respect to $\mathcal{O}_{U,u}$ and so is a henselian local ring (i.e., it satisfies the conclusion of Hensel's Lemma) with maximal ideal $\mathfrak{m}\mathcal{O}_{U,u}^{\text{sh}}$ (for $\mathfrak{m}$ the maximal ideal of $\mathcal{O}_{U,u}$) such that $\mathcal{O}_{U,u}^{\text{sh}}/\mathfrak{m}\mathcal{O}_{U,u}^{\text{sh}} \cong \kappa^{\text{sep}}$ (for κ the residue field of U at u). We construct $\mathcal{O}_{U,u}^{\text{sh}}$ as a filtered colimit of finite étale $\mathcal{O}_{U,u}$-algebras. It follows that $\operatorname{Frac} \mathcal{O}_{U,u}^{\text{sh}}$ is a filtered colimit of finite étale k_u-algebras, which we can then replace with a filtered colimit of finite unramified (field) extensions of k_u.

With this information in hand, we claim that $\delta(A(k))$ lands in the subgroup of $\xi \in H^1(k, A[m])$ unramified outside S in the sense that $\xi|_{I_u} = 0$ in $H^1(I_u, A[m])$ for every closed point $u \in U$. This follows since, given $u \in U$ a closed point, the composition

$$\mathcal{A}(U)/m \hookrightarrow H^1_{\text{ét}}(U, \mathcal{A}[m]) \longrightarrow H^1(k, A[m]) \longrightarrow H^1(I_u, A[m])$$

factors through $H^1_{\text{ét}}(\operatorname{Spec} \mathcal{O}_{U,u}^{\text{sh}}, \mathcal{A}[m]) = 0$ since I_u is the Galois group of $\operatorname{Frac} \mathcal{O}_{U,u}^{\text{sh}}$. Phrased in more concrete terms, given u a closed point of U, we want to know if the restriction to I_u of $\xi_a \in H^1(k, A[m])$ vanishes, where ξ_a is the image of $[a] \in A(k)/m$. If we view ξ_a as an obstruction to m-divisibility then this is the same as viewing $[a]$ as an obstruction to m-divisibility as an element of $A(\operatorname{Frac} \mathcal{O}_{U,u}^{\text{sh}})/m$. That is, we want to know if $[m] : A(\operatorname{Frac} \mathcal{O}_{U,u}^{\text{sh}}) \to A(\operatorname{Frac} \mathcal{O}_{U,u}^{\text{sh}})$ is

[42] Recall that Γ denotes the absolute Galois group of k.

surjective. We get an affirmative answer after identifying $A(\operatorname{Frac}\mathcal{O}^{\mathrm{sh}}_{U,u})$ with $\mathcal{A}(\mathcal{O}^{\mathrm{sh}}_{U,u})$ and noting that every finite étale cover of $\mathcal{O}^{\mathrm{sh}}_{U,u}$ is split. By [Con15, Cor 9.3.4], we also have that $A[m](k_s)$ is unramified outside S in the sense that I_u acts trivially on $A[m](k_s)$ for every closed point $u \in U$. Thus, we are done by the following theorem. □

Theorem 5.2.2. *Let k be a global field with absolute Galois group $\Gamma := \mathrm{Gal}(k_s/k)$, $S \subseteq \Sigma_k$ finite containing the archimedean places, and M a finite discrete Γ-module such that $m := \#M$ is an S-unit and M is unramified outside S. Then,*

$$H^1_S(k, M) := \{\xi \in H^1(k, M) : \xi \text{ is unramified outside } S\}$$

is finite.

Proof. We claim it suffices to show the result assuming $\mu_m \subseteq k$, $M = \mu_m$, and the places of k associated to m are contained in S. To see this, let K/k be a finite Galois extension splitting M in the sense that $\Gamma_K := \mathrm{Gal}(k_s/K)$ acts trivially on M.[43] If K' is any finite Galois extension of K then K' also splits M and so we may assume $\mu_m \subseteq K$. Note that, since m is an S-integer, $\operatorname{char} k \nmid m$ and so μ_d is cyclic of order d for every $d \mid m$. The elements of μ_m are ramified only at the places of k associated to m. Enlarging S by these places increases the size of $H^1_S(k, M)$, so if we prove finiteness for the larger group then we have finiteness for the smaller one. Hence, we may assume the places of k associated to m are contained in S. Now, let $S_K \subseteq \Sigma_K$ denote the set of places extending the places in S. We have an inflation-restriction exact sequence

$$0 \longrightarrow H^1(\mathrm{Gal}(K/k), M) \xrightarrow{\mathrm{Inf}} H^1(k, M) \xrightarrow{\mathrm{Res}} H^1(K, M)$$

satisfying $\mathrm{Res}(H^1_S(k, M)) \subseteq H^1_{S_K}(K, M)$.[44] Since $H^1(\mathrm{Gal}(K/k), M)$ is finite, it follows that $H^1_S(k, M)$ is finite if $H^1_{S_K}(K, M)$ is finite. The isomorphism of abelian groups

$$M \cong \prod_i \mu_{d_i}$$

for some finite collection of integers $d_i \mid m$ is an isomorphism of Γ_K-modules since all of the Γ_K-modules involved are split. By assumption, each term in the product is finite and so $H^1_{S_K}(K, M)$ is finite. Hence, we may assume $\mu_m \subseteq k$, $M = \mu_m$, and the places of k associated to m are contained in S.

With the simplifying assumptions established, our goal now is to construct an exact sequence

$$1 \longrightarrow \mathcal{O}^\times_{k,S}/(\mathcal{O}^\times_{k,S})^m \longrightarrow H^1_S(k, \mu_m) \longrightarrow \mathrm{Pic}(\mathcal{O}_{k,S})[m]$$

The left-hand and right-hand terms are finite by the S-unit and S-class number theorems, respectively, from which we get the finiteness of $H^1_S(k, \mu_m)$.[45] Let L be the extension of k maximal with respect to being unramified outside S, obtained as the compositum of all finite extensions of k

[43] Since M is a finite discrete Γ-module, the corresponding homomorphism $\varphi : \Gamma \to \mathrm{Aut}_{\mathsf{Set}}(M)$ is continuous and has kernel a finite index closed normal subgroup of Γ. The Fundamental Theorem of Galois Theory then guarantees that $\ker\varphi = \Gamma_K$ for K/k a finite Galois extension.

[44] This uses the assumption that M is unramified outside S.

[45] One could forego the S-class number theorem by noting that suitably enlarging S kills $\mathrm{Pic}(\mathcal{O}_{k,S})[m]$.

unramified outside S.[46] Let $\mathcal{O}_L$ be the compositum of $\mathcal{O}_E$ for E ranging over the finite extensions of k unramified outside S.[47] The extension L/k is Galois since roots of the same irreducible polynomial in $k[t]$ give rise to extensions with the same discriminant, with Galois group $G := \mathrm{Gal}(L/k)$ satisfying $(\mathcal{O}_L)^G = \mathcal{O}_{k,S}$. Why should we consider L? Since Γ acts trivially on μ_m, we have

$$H^1_S(k, \mu_m) = \{\xi \in \mathrm{Hom}_{\mathrm{cont}}(\Gamma, \mu_m) : \xi|_{I_u} = 1 \text{ for every closed point } u \in U\}.$$

This says that elements of $H^1_S(k, \mu_m)$ are entirely determined by their action on the complement in Γ of the union of the inertia groups I_u ranging over the closed points $u \in U$ (what a mouthful!). In other words, they are determined by their action on G![48] Hence, there is a natural isomorphism

$$H^1_S(k, \mu_m) \cong \mathrm{Hom}_{\mathrm{cont}}(G, \mu_m) = H^1(G, \mu_m).$$

Consider now the sequence

$$1 \longrightarrow \mu_m \longrightarrow \mathcal{O}_L^\times \xrightarrow{(\cdot)^m} \mathcal{O}_L^\times \longrightarrow 1$$

We claim that this is an exact sequence of abelian groups. Exactness at the left term is just the fact that $\mu_m \subseteq \mathcal{O}_{k,S}^\times \subseteq \mathcal{O}_L^\times$. Exactness at the middle term is clear. To check exactness at the right term, let $a \in \mathcal{O}_L^\times$. Let $\alpha \in k_s$ be an mth root of a. Let E be any subfield of $L(\alpha)$ such that E/k is finite. Then, E is either a subfield of L or of the form $F(\alpha)$ for F a subfield of L. The first case leaves nothing to check so we address the second case, in which F is necessarily unramified outside S. The minimal polynomial $p_\alpha(t) \in \mathcal{O}_F[t]$ of α over $\mathcal{O}_F$ divides $t^m - a$. Let $\mathfrak{p} \in \mathrm{Spec}\, \mathcal{O}_F$ representing the extension to Σ_F of a place of $\Sigma_k \setminus S$. Then, the image of $t^m - a$ in $(\mathcal{O}_F/\mathfrak{p})[t]$ has formal derivative mt^{m-1} and so is separable since m is nonzero in $\mathcal{O}_F/\mathfrak{p}$. It follows that $p_\alpha(t)$ has separable image in $(\mathcal{O}_F/\mathfrak{p})[t]$ and so $F(\alpha)/k$ is unramified outside S. Hence, E is a subfield of L and so $\alpha \in \mathcal{O}_L^\times$, giving exactness at the right term of the sequence. Passing to group cohomology relative to G, we obtain a commutative diagram

$$\begin{array}{ccccccccc}
H^0(G, \mathcal{O}_L^\times) & \xrightarrow{(\cdot)^m} & H^0(G, \mathcal{O}_L^\times) & \longrightarrow & H^1(G, \mu_m) & \longrightarrow & H^1(G, \mathcal{O}_L^\times) & \xrightarrow{(\cdot)^m} & H^1(G, \mathcal{O}_L^\times) \\
\downarrow\cong & & \downarrow\cong & & \downarrow\cong & & \downarrow & & \downarrow \\
\mathcal{O}_{k,S}^\times & \xrightarrow[(\cdot)^m]{} & \mathcal{O}_{k,S}^\times & \longrightarrow & H^1_S(k, \mu_m) & \longrightarrow & \mathrm{Pic}(\mathcal{O}_{k,S}) & \xrightarrow[(\cdot)^{\otimes m}]{} & \mathrm{Pic}(\mathcal{O}_{k,S})
\end{array}$$

with exact rows. Where do the embeddings come from? Letting $V := \mathrm{Spec}\, \mathcal{O}_L$, the embedding $H^1(G, \mathcal{O}_L^\times) \hookrightarrow \mathrm{Pic}(\mathcal{O}_{k,S})$ is obtained by noting that

$$\mathrm{Pic}(\mathcal{O}_{k,S}) \cong \mathrm{Pic}(U) \cong H^1_{\text{ét}}(U, \mathbb{G}_{\mathbf{m}}) \text{ and } H^1(G, \mathcal{O}_L^\times) \cong H^1_{\text{ét}}(V, \mathbb{G}_{\mathbf{m}})$$

and then applying the map induced by $V \to U$. Hence, we obtain the desired exact sequence

[46] Recall that a general extension E/k is unramified outside S if it is the compositum of finite subextensions unramified outside S. In the case $k = \mathbb{Q}$, the theory of discriminants and the Minkowski discriminant bound show that $L = \mathbb{Q}$ if $S = \emptyset$ and L is an infinite degree extension of $\mathbb{Q}$ if $S \neq \emptyset$. In general, L is almost certainly an infinite degree extension of k.

[47] This construction technically only makes sense for number fields since the ring of integers has no analogue for global function fields. We leave the modification of this construction to that approach to the reader.

[48] The following should help if this seems perplexing. Kummer theory gives us an isomorphism $k^\times/(k^\times)^m \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{cont}}(\Gamma, \mu_m)$ via $[a] \mapsto \xi_a$ sending $\sigma \in \Gamma$ to $\sigma(\alpha)/\alpha$ for $\alpha \in k_s$ an mth root of a. Then, ξ_a is unramified at a closed point $u \in U$ if and only if any extension of k obtained by adjoining an mth root of a is unramified at u.

$$1 \longrightarrow \mathcal{O}_{k,S}^{\times}/(\mathcal{O}_{k,S}^{\times})^m \longrightarrow H_S^1(k,\mu_m) \longrightarrow \mathrm{Pic}(\mathcal{O}_{k,S})[m]$$

from the bottom row of the above two-row diagram. □

Remark 5.2.3. *A useful way of conceptualizing the above proof of the Weak Mordell-Weil Theorem is to appeal to Selmer and Shafarevich-Tate groups.*[49] *Given $v \in \Sigma_k$, we obtain a map Res_v as the composition*

$$H^1(k,A) = H^1(\Gamma, A(k_s)) \xrightarrow{\mathrm{Res}} H^1(\Gamma_{k_v}, A(k_s)) \longrightarrow H^1(\Gamma_{k_v}, A((k_v)_s)) = H^1(k_v, A)$$

From Corollary 5.1.10, we get a short exact sequence

$$0 \longrightarrow A(k)/m \longrightarrow H^1(k, A[m]) \longrightarrow H^1(k,A)[m] \longrightarrow 0$$

which fits into a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(k)/m & \longrightarrow & H^1(k,A[m]) & \xrightarrow{\rho} & H^1(k,A)[m] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & \overset{\tilde{\rho}}{\searrow} & \downarrow & & \\ 0 & \longrightarrow & \prod_{v\in\Sigma_k} A(k_v)/m & \longrightarrow & \prod_{v\in\Sigma_k} H^1(k_v, A[m]) & \longrightarrow & \prod_{v\in\Sigma_k} H^1(k_v,A)[m] & \longrightarrow & 0 \end{array}$$

with exact rows, vertical arrows induced by the collection of Res_v, and diagonal arrow induced by composition. Define the ***Shafarevich-Tate group***[50] *of A over k to be*

$$Ш(k,A) := \ker\left(H^1(k,A) \to \prod_{v\in\Sigma_k} H^1(k_v,A)\right).$$

*The group $\ker\rho$ is too unwieldy to work with in practice but the same is not true for the larger group $\ker\tilde{\rho}$. We denote the latter group by $\mathrm{Sel}_m(k,A)$ and call it the m-**Selmer group** of A over k. Applying the Snake Lemma to the modified diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(k)/m & \longrightarrow & H^1(k,A[m]) & \longrightarrow & H^1(k,A)[m] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle\tilde{\rho}} & & \downarrow & & \\ 0 & \longrightarrow & 0 & \longrightarrow & \prod_{v\in\Sigma_k} H^1(k_v,A)[m] & = & \prod_{v\in\Sigma_k} H^1(k_v,A)[m] & \longrightarrow & 0 \end{array}$$

yields a short exact sequence

$$0 \longrightarrow A(k)/m \longrightarrow \mathrm{Sel}_m(k,A) \longrightarrow Ш(k,A)[m] \longrightarrow 0$$

Thus, finiteness of $A(k)/m$ (and of $Ш(k,A)[m]$) follows from finiteness of $\mathrm{Sel}_m(k,A)$. The point here is that $\mathrm{Sel}_m(k,A)$ is readily computable. Letting $S \subseteq \Sigma_k$ be as in the proof of the Weak Mordell-Weil Theorem, $\mathrm{Sel}_m(k,A)$ sits inside of $H_S^1(k,A[m])$ via

$$\mathrm{Sel}_m(k,A) = \{\xi \in H_S^1(k,A[m]) : \xi \text{ maps to } 0 \text{ in } H^1(k_v,A)[m] \text{ for every } v \in S\}.$$

[49] The reference for this material is [Poo02].

[50] Several important open problems in number theory, notably the BSD conjecture, are concerned with the structure of this group.

Both $H^1_S(k, A[m])$ and $\mathrm{Sel}_m(k, A)$ can then be computed using the theory of torsors. See [Poo02] for examples of how this works in practice.

6 Construction of the Pairing

Having completed the first of two major tasks involved in proving the Mordell-Weil Theorem, we now turn to the second major task, starting with some preliminaries on heights.

6.1 Heights

Given a global field k and $n \geq 1$, the standard height function is $h_{k,n} : \mathbb{P}^n_k(\overline{k}) \to \mathbb{R}^{\geq 0}$ defined by

$$[t_0, \ldots, t_n] \mapsto \frac{1}{[K : k]} \sum_{w \in \Sigma_K} \max_{0 \leq i \leq n} \log \|t_i\|_w ,$$

where K/k is a finite extension such that $k(t_0, \ldots, t_n) \subseteq K$.[51]

Proposition 6.1.1. *Let k be a global field and $n \geq 1$. Then, $h_{k,n}$ is well-defined – i.e., it is*

(1) *non-negative and invariant under scaling by $K^\times$;*

(2) *not dependent on the choice of finite extension K/k.*

Proof. (1) Scaling by $\lambda \in K^\times$ changes the value of the height by

$$\frac{1}{[K : k]} \sum_{w \in \Sigma_K} \log \|\lambda\|_w ,$$

which vanishes since the Product Formula says $\prod_{w \in \Sigma_K} \|\lambda\|_w = 1$. The standard height is non-negative because we can always scale $t_0, \ldots, t_n$ so that at least one of them has value 1.

(2) Suppose we have finite extensions $k(t_0, \ldots, t_n) \subseteq K \subseteq K'$. Given $w \in \Sigma_K, w' \in \Sigma_{K'}$ with $w' \mid w$,

$$\|t_i\|_{w'} = \|t_i\|_w^{[K'_{w'} : K_w]} .$$

We also have $[K' : k] = [K' : K][K : k]$ and $[K' : K] = \sum_{w'|w} [K'_{w'} : K_w]$. Hence,

$$\frac{1}{[K' : k]} \sum_{w' \in \Sigma_{K'}} \max_i \log \|t_i\|_{w'} = \frac{1}{[K : k]} \sum_{w \in \Sigma_K} \left(\frac{1}{[K' : K]} \sum_{w'|w} \max_i \log \|t_i\|_{w'} \right)$$

and

$$\begin{aligned} \frac{1}{[K' : K]} \sum_{w'|w} \max_i \log \|t_i\|_{w'} &= \frac{1}{[K' : K]} \sum_{w'|w} \max_i \log \|t_i\|_w^{[K'_{w'} : K_w]} \\ &= \max_i \log \|t_i\|_w \cdot \frac{1}{[K' : K]} \sum_{w'|w} [K'_{w'} : K_w] \\ &= \max_i \log \|t_i\|_w . \end{aligned}$$

[51] An alternative way of going about this is to think of $h_{k,n}$ as a function from $\mathbb{A}^{n+1}_k \setminus 0$ to $\mathbb{R}$ which satisfies certain invariance properties.

The result follows. □

One might hope that $h_{k,n}$ does not depend on a choice of homogeneous coordinates and so is $\mathrm{PGL}_{n+1}(k)$-invariant on $\mathbb{P}^n_k(\overline{k})$.[52] This is false on the nose but turns out to be true modulo bounded functions. Since we will be working a lot modulo bounded functions, it makes sense to write $h \sim h'$ if $h - h'$ is bounded for h, h' any functions from the same set into $\mathbb{R}$.

Lemma 6.1.2. *Let k be a global field, $n \geq 1$, and $S \in \mathrm{PGL}_{n+1}(k)$. Then, $h_{k,n} \sim h_{k,n} \circ S$.*

Proof. We may assume without loss of generality that S is an elementary transformation since, given any $T \in \mathrm{PGL}_{n+1}(k)$,

$$h_{k,n} \circ S \sim h_{k,n} \sim h_{k,n} \circ T \implies h_{k,n} \circ ST \sim h_{k,n} \sim h_{k,n} \circ TS.$$

Given $[x_0, \ldots, x_n] = x \in \mathbb{P}^n_k(\overline{k})$, there are three possibilities for S:

(1) S swaps the ith and jth entries of x;

(2) S scales x_i by $\lambda \in k^\times$;

(3) S adds x_i to x_j.

Let $Sx = [x'_0, \ldots, x'_n]$ and note that

$$(h_{k,n} - h_{k,n} \circ S)(x) = (h_{k,n} \circ S^{-1} - h_{k,n})(Sx). \tag{3}$$

Case (1) is clear since then $h_{k,n} = h_{k,n} \circ S$ as the sums involved in the height computations are invariant under permutation. For case (2), given $0 \leq j \leq n$ and $w \in \Sigma_K$, we have

$$\log \left\|x'_j\right\|_w = \begin{cases} \log \|x_j\|_w, j \neq i, \\ \log \|\lambda\|_w + \log \|x_i\|_w, \quad j = i \end{cases}$$

and so $\log \left\|x'_j\right\|_w \leq \log \|x_j\|_w + |\log \|\lambda\|_w|$. Hence,

$$(h_{k,n} \circ S - h_{k,n})(x) = \frac{1}{[K:k]} \sum_{w \in \Sigma_K} (\max_j \log \left\|x'_j\right\|_w - \max_j \log \|x_j\|_w) \leq \frac{1}{[K:k]} \sum_{w \in \Sigma_K} |\log \|\lambda\|_w|.$$

S^{-1} multiplies x_i by λ^{-1} and so is of the same form as S. Equation (3) and the above computation then give that $h_{k,n} \sim h_{k,n} \circ S$. For case (3), note first of all that, given $a, b \in K$ and $w \in \Sigma_K$,

$$\log \|a + b\|_w \leq \max\{\log \|a\|_w, \log \|b\|_w\} + c_w$$

with

$$c_w := \begin{cases} 0, & w \text{ is non-archimedean}, \\ \log 2, & w \text{ is archimedean}. \end{cases}$$

Hence, given $0 \leq t \leq n$ and $w \in \Sigma_K$,

$$\log \left\|x'_t\right\|_w \leq \max\{\log \|x_i\|_w, \log \|x_j\|_w, \log \|x_t\|_w\} + c_w$$

[52] PGL here means projective general linear group.

and so

$$(h_{k,n} \circ S - h_{k,n})(x) \leq \frac{1}{[K:k]} \sum_{w \in \Sigma_K} c_w.$$

S^{-1} is given by precomposing S with a transformation of type (2) that multiplies x_i by -1 and so $h_{k,n} \sim h_{k,n} \circ S$ by Equation (3) and the above computation. □

Lemma 6.1.3. *Let X be a projective k-scheme, $\mathscr{L}$ a very ample line bundle on X with associated closed embedding $i_{\mathscr{L}} : X \hookrightarrow \mathbb{P}\Gamma(X, \mathscr{L}) = \mathbb{P}^d_k$, and $f : X \to \mathbb{P}^n_k$ a k-morphism for some $n > 0$ such that $f^*\mathcal{O}(1) \cong \mathscr{L}$. Define $h_f := h_{k,n} \circ f$ and $h_{i_{\mathscr{L}}} := h_{k,d} \circ i_{\mathscr{L}}$, viewed as functions from $X(\bar{k})$ to $\mathbb{R}$. Then, $h_f \sim h_{i_{\mathscr{L}}}$.*

Technically, $i_{\mathscr{L}}$ depends on a choice of $d+1$ sections that globally generate $\mathscr{L}$. Lemma 6.1.2 shows that this choice does not matter. Moreover, Lemma 6.1.3 shows that even the choice of embedding projective space relative to $\mathscr{L}$ does not matter.

Proof. By Lemma 6.1.2, we may without loss of generality change coordinates on $\mathbb{P}^n_k$ so that $f(X)$ is non-degenerate and hence $f^* : \Gamma(\mathbb{P}^n_k, \mathcal{O}(1)) \to \Gamma(X, \mathscr{L})$ is injective. We claim first that $h_f \leq h_{i_{\mathscr{L}}}$. Let $T_0, \ldots, T_n$ be a k-basis for $\Gamma(\mathbb{P}^n_k, \mathcal{O}(1))$. Then, letting $Z_j := f^*T_j$ for $0 \leq j \leq n$, we have $f = [Z_0, \ldots, Z_n]$. The map $f^* : \Gamma(\mathbb{P}^n_k, \mathcal{O}(1)) \to \Gamma(X, \mathscr{L})$ is injective by assumption and so we may complete $Z_0, \ldots, Z_n$ to a k-basis $Z_0, \ldots, Z_d$ for $\Gamma(X, \mathscr{L})$. Changing coordinates on $\mathbb{P}^d_k$ if necessary, this gives $i_{\mathscr{L}} = [Z_0, \ldots, Z_d]$ and so $h_f \leq h_{i_{\mathscr{L}}}$ since we are taking a maximum over a larger list of numbers.

Next, we claim that $h_{i_{\mathscr{L}}} \leq h_f + O(1)$. By assumption, X is covered by the open preimages $D_+(Z_j) = f^{-1}(D_+(T_j))$ and so the zero locus $\{Z_0 = \cdots = Z_n = 0\}$ on X is empty. Since $\mathscr{L}$ is very ample, $i_{\mathscr{L}}$ is closed and so its image is of the form $\operatorname{Proj} S$ for

$$S := k[Z_0, \ldots, Z_d]/I \subseteq \bigoplus_{r \geq 0} \Gamma(X, \mathscr{L}^{\otimes r}).$$

The ideal $J := (Z_0, \ldots, Z_n) \subseteq S$ satisfies

$$\operatorname{Proj} S/J = \operatorname{Proj} S \cap \{Z_0 = \cdots = Z_n = 0\} = \emptyset$$

as a subset of $\mathbb{P}^d_k$ and so the Nullstellensatz implies that the irrelevant ideal $(Z_0, \ldots, Z_d)$ hence $(Z_{n+1}, \ldots, Z_d)$ has nilpotent image in S/J. It follows that $Z^e_{n+1}, \ldots, Z^e_d \in J$ for some $e \geq 1$ and so each such Z_j satisfies

$$Z^e_j = \sum_{i=0}^{n} F_{ij} Z_i \bmod I$$

with $F_{ij} \in k[Z_0, \ldots, Z_d]$ homogeneous of degree $e-1$. Given $x \in X(\bar{k})$, it follows that

$$e h_{i_{\mathscr{L}}}(x) \leq (e-1) h_{i_{\mathscr{L}}}(x) + h_f(x) + C \tag{4}$$

for some constant C independent of x. Where does this come from? By assumption, each F_{ij} can be written as

$$F_{ij} = \sum_I a^{ij}_I Z^I,$$

where $I = (t_0, \ldots, t_d)$ with $t_0 + \cdots + t_d = e - 1$, $a_I^{ij} \in k$ is some coefficient, and $Z^I := Z_0^{t_0} \cdots Z_d^{t_d}$. Let N be the number of such tuples I. Given $x \in X(\overline{k})$, let K/k be a finite extension containing $Z_0(x), \ldots, Z_d(x)$. Adopting the notation in the proof of Lemma 6.1.2, we have

$$\log \|b_0 + \cdots + b_M\|_w \leq \max_{0 \leq i \leq M} \|b_i\|_w + (M-1)c_w$$

given $b_0, \ldots, b_M \in K$ and $w \in \Sigma_K$. Careful application of this formula gives the result of Equation (4), with C given by

$$C := \frac{1}{[K:k]} \sum_{w \in \Sigma_K} \left[(n+N-2)c_w + \sum_{i,j} \max_I \log \left\| a_I^{ij} \right\|_w \right].$$

The argument given in the proof of Proposition 6.1.1 shows that C is independent of x. □

Theorem 6.1.4 (Weil's Thesis)**.** *There exists a unique assignment of pairs $(X, \mathscr{L})$ with X a projective k-scheme and $\mathscr{L}$ a line bundle on X to functions $h_{k,\mathscr{L}} = h_{\mathscr{L}}$ from $X(\overline{k})$ to $\mathbb{R}$ modulo bounded functions satisfying*

(1) $h_{\mathscr{L} \otimes \mathscr{L}'} = h_{\mathscr{L}} + h_{\mathscr{L}'}$;

(2) $(\mathbb{P}_k^n, \mathcal{O}(1)) \mapsto h_{k,n}$;

(3) $h_{f^*\mathscr{L}} = h_{\mathscr{L}} \circ f$ *for* $f : X' \to X$ *a morphism of projective k-schemes.*

Moreover, if $\mathscr{L}$ is very ample then $h_{\mathscr{L}} = h_{i_{\mathscr{L}}}$.

We call any function from $X(\overline{k})$ to $\mathbb{R}$ representing $h_{\mathscr{L}}$ a **Weil height** associated to $\mathscr{L}$.

Proof. Given X a projective k-scheme and $\mathscr{L}$ a very ample line bundle on X, define $h_{\mathscr{L}} := h_{i_{\mathscr{L}}}$. This immediately verifies (2). Given $\mathscr{L}, \mathscr{L}'$ very ample line bundles on X, define $i_{\mathscr{L} \otimes \mathscr{L}'}$ to be the composition

$$X \xrightarrow{\Delta_{X/k}} X \times_k X \xrightarrow{(i_{\mathscr{L}}, i_{\mathscr{L}'})} \mathbb{P}_k^n \times_k \mathbb{P}_k^m \hookrightarrow \mathbb{P}_k^{(n+1)(m+1)-1}$$

where the unlabeled arrow is the Segre embedding defined by

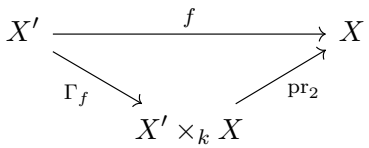
$$([s_0, \ldots, s_n], [t_0, \ldots, t_m]) \mapsto [s_0 t_0, \ldots, s_n t_m].$$

[Zha11] implies $i_{\mathscr{L} \otimes \mathscr{L}'}$ is a closed embedding and so $\mathscr{L} \otimes \mathscr{L}'$ is very ample. The fact that logarithms take products to sums implies that $h_{\mathscr{L} \otimes \mathscr{L}'} = h_{\mathscr{L}} + h_{\mathscr{L}'}$. Now, let $\mathscr{L}$ be any line bundle on X. Since X is projective, it has an ample line bundle $\mathscr{M}$. Then, there exists some $n > 0$ such that $\mathscr{M}^{\otimes n}$ and $\mathscr{L} \otimes \mathscr{M}^{\otimes n}$ are both very ample.[53] This suggests the following extension procedure. Given $\mathscr{L}$ a line bundle on X, choose $\mathscr{M}$ a very ample line bundle on X such that $\mathscr{L} \otimes \mathscr{M}$ is also very ample and define $h_{\mathscr{L}} := h_{\mathscr{L} \otimes \mathscr{M}} - h_{\mathscr{M}}$. This procedure is well-defined since, given two such line bundles $\mathscr{M}, \mathscr{M}'$,

$$h_{\mathscr{L} \otimes \mathscr{M}} + h_{\mathscr{M}'} = h_{\mathscr{L} \otimes \mathscr{M} \otimes \mathscr{M}'} = h_{\mathscr{L} \otimes \mathscr{M}'} + h_{\mathscr{M}}.$$

This immediately verifies (1). Property (3) requires a bit more care. Factor $f : X' \to X$ via the commutative diagram

[53] To see this, note that, since $\mathscr{M}$ is ample, $\mathscr{M}^{\otimes n_1}$ is very ample and $\mathscr{L} \otimes \mathscr{M}^{\otimes n_2}$ is globally generated for some $n_1, n_2 > 0$. Then, $\mathscr{M}^{\otimes (n_1+n_2)}$ is very ample and $\mathscr{L} \otimes \mathscr{M}^{\otimes (n_1+n_2)}$ is very ample by [Zha11].



where Γ_f is the graph morphism associated to f. To verify (3), it suffices to verify (3) with f replaced by Γ_f and pr_2. Γ_f is obtained as the base change via f of the diagonal $\Delta_{X/k} : X \to X \times_k X$ and so is a closed embedding (hence finite) since X is projective. Given any very ample line bundle $\mathscr{M}$ on $X' \times_k X$, $\Gamma_f^* \mathscr{M}$ is ample and so $(\Gamma_f^* \mathscr{M})^{\otimes N} \cong \Gamma_f^*(\mathscr{M}^{\otimes N})$ is very ample for some $N > 0$.[54] Hence, replacing $\mathscr{M}$ with $\mathscr{M}^{\otimes N}$, we may assume by (1) without loss of generality that $\mathscr{M}, f^*\mathscr{M}$ are both very ample. (3) then follows from Lemma 6.1.3 applied to $i_{\mathscr{L}} \circ f$ and $i_{f^*\mathscr{L}}$. To verify (3) for pr_2, it suffices to consider the case $X' = \mathbb{P}^n_k$, $X = \mathbb{P}^m_k$, and $\mathscr{L} = \mathcal{O}_{\mathbb{P}^m_k}(1) = \mathcal{O}(1)$. This follows from applying (1) and the work we just did to the commutative diagram

$$\begin{array}{ccc} X' \times_k X & \xrightarrow{\mathrm{pr}_2} & X \\ {\scriptstyle (i_{\mathscr{L}}, i_{\mathscr{L}'})}\downarrow & & \downarrow{\scriptstyle i_{\mathscr{L}}} \\ \mathbb{P}^n_k \times_k \mathbb{P}^m_k & \xrightarrow[\mathrm{pr}_2]{} & \mathbb{P}^m_k \end{array}$$

with $\mathscr{L}'$ any very ample line bundle on X'. We have

$$\mathrm{pr}_2^* \mathcal{O}(1) \cong \mathcal{O}(0,1) \cong \mathcal{O}(2,2) \otimes \mathcal{O}(2,1)^{-1},$$

where $\mathcal{O}(a,b)$ is the image of $(\mathcal{O}(a), \mathcal{O}(b))$ under $\mathrm{Pic}(\mathbb{P}^n_k) \times \mathrm{Pic}(\mathbb{P}^m_k) \hookrightarrow \mathrm{Pic}(\mathbb{P}^n_k \times_k \mathbb{P}^m_k)$. The line bundles $\mathcal{O}(2,2)$ and $\mathcal{O}(2,1)$ are both very ample.[55] Direct computation then shows

$$h_{\mathcal{O}(2,2)} - h_{\mathcal{O}(2,1)} = h_{\mathcal{O}(1)} \circ \mathrm{pr}_2 \,.$$

To see that h is unique, let h' be another assignment of pairs satisfying properties (1)-(3). By (2), h and h' agree on projective spaces and so by (3) they agree on very ample line bundles. But then h and h' agree on all line bundles by (1). □

6.2 Pairings

Given an abelian group A and $h : A \to \mathbb{R}$, h is **almost quadratic** if the induced function

$$(x,y,z) \mapsto h(x+y+z) - (h(x+y) + h(x+z) + h(y+z)) + (h(x) + h(y) + h(z))$$

from A^3 to $\mathbb{R}$ is bounded.[56] This notion extends to equivalence classes of functions from A to $\mathbb{R}$ modulo bounded functions.

Lemma 6.2.1. *Let A/k be an abelian variety and $\mathscr{L}$ a line bundle on A. Then, $h_{\mathscr{L}} : A(\overline{k}) \to \mathbb{R}$ is almost quadratic.*

[54] Note that the pullback of a very ample line bundle under a scheme morphism (even a finite morphism) is not in general very ample. For an example, take an elliptic curve E with distinguished k-rational point p and consider the line bundle $\mathcal{O}_E(2p)$ with induced morphism $E \to \mathbb{P}^1_k$.

[55] In general, $\mathcal{O}(a,b)$ is globally generated if and only if $a, b \geq 0$ and both ample and very ample if and only if $a, b > 0$.

[56] Check for yourself that any quadratic function vanishes under this process.

Proof. By Corollary 3.2.3,

$$\mathscr{M} := (\mathrm{pr}_1 + \mathrm{pr}_2 + \mathrm{pr}_3)^*\mathscr{L} \otimes (\mathrm{pr}_1 + \mathrm{pr}_2)^*\mathscr{L}^{-1} \otimes (\mathrm{pr}_1 + \mathrm{pr}_3)^*\mathscr{L}^{-1} \otimes (\mathrm{pr}_2 + \mathrm{pr}_3)^*\mathscr{L}^{-1} \otimes \mathrm{pr}_1^*\mathscr{L} \otimes \mathrm{pr}_2^*\mathscr{L} \otimes \mathrm{pr}_3^*\mathscr{L}$$

is a trivial line bundle on A^3 and so $h_{\mathscr{M}}$ is bounded.[57] Given $(x, y, z) \in A^3(k) = A(k)^3$,

$$h_{\mathscr{M}}(x, y, z) = h_{\mathscr{L}}(x + y + z) - (h_{\mathscr{L}}(x + y) + h_{\mathscr{L}}(x + z) + h_{\mathscr{L}}(y + z)) + (h_{\mathscr{L}}(x) + h_{\mathscr{L}}(y) + h_{\mathscr{L}}(z))$$

by (1) and (3) of Weil's Thesis. □

Since $h_{\mathscr{L}}$ is almost quadratic, is it possible to "perturb" $h_{\mathscr{L}}$ so that it is quadratic? The answer, which rests on the following algebraic result, is yes.

Theorem 6.2.2 (Tate)**.** *Let A be an abelian group and $h : A \to \mathbb{R}$ almost quadratic. Then, there exist unique symmetric $\mathbb{Z}$-bilinear $b : A \times A \to \mathbb{R}$ and $\mathbb{Z}$-linear $\ell : A \to \mathbb{R}$ such that*

$$h \sim \frac{1}{2}(b \circ \Delta) + \ell,$$

where $\Delta : A \to A \times A$ is the diagonal map.[58]

Lemma 6.2.1 and Tate's Theorem together tell us that, given an abelian variety A and $\mathscr{L}$ a line bundle on A, there exist unique symmetric $\mathbb{Z}$-bilinear $b_{\mathscr{L}} : A(\overline{k}) \times A(\overline{k}) \to \mathbb{R}$ and $\mathbb{Z}$-linear $\ell_{\mathscr{L}} : A(\overline{k}) \to \mathbb{R}$ such that

$$\hat{h}_{\mathscr{L}} := \frac{1}{2}(b_{\mathscr{L}} \circ \Delta) + \ell_{\mathscr{L}} : A(\overline{k}) \to \mathbb{R}$$

is a Weil height associated to $\mathscr{L}$. The function $\hat{h}_{\mathscr{L}}$ is called the **Tate canonical height** associated to $\mathscr{L}$.

Theorem 6.2.3. *Let A/k be an abelian variety. Let $\mathscr{L}, \mathscr{L}'$ be line bundles on A and $f : B \to A$ a morphism of abelian varieties.*

(1) $\hat{h}_{\mathscr{L}\otimes\mathscr{L}'} = \hat{h}_{\mathscr{L}} + \hat{h}_{\mathscr{L}'}$.

(2) $\hat{h}_{f^*\mathscr{L}} = \hat{h}_{\mathscr{L}} \circ f$.

(3) *Suppose $\mathscr{L}$ is symmetric. Then, $\ell_{\mathscr{L}} = 0$.*

(4) *Suppose $\mathscr{L}$ is ample and symmetric. Then, $b_{\mathscr{L}}$ is positive semi-definite.*

(5) *Suppose $\mathscr{L}$ is ample and symmetric. Then, the set*

$$\{x \in A(\overline{k}) : [k(x) : k] \leq d, \hat{h}_{\mathscr{L}}(x) \leq C\}$$

is finite for every $C > 0$ and $d \geq 0$.

Proof. (1) Part (1) of Weil's Thesis gives $\hat{h}_{\mathscr{L}\otimes\mathscr{L}'} \sim \hat{h}_{\mathscr{L}} + \hat{h}_{\mathscr{L}'}$. Since both sides are quadratic of the desired form, the uniqueness part of Theorem 6.2.2 gives that $b_{\mathscr{L}\otimes\mathscr{L}'} = b_{\mathscr{L}} + b_{\mathscr{L}'}$ and $\ell_{\mathscr{L}\otimes\mathscr{L}'} = \ell_{\mathscr{L}} + b_{\mathscr{L}'}$.

[57] Both A and A^3 are projective and so $\mathscr{L}$ and $\mathscr{M}$ have well-defined Weil heights by Weil's Thesis.

[58] See [Con15, Thm 10.3.6], which proves a statement for more general multilinear maps.

(2) Part (3) of Weil's Thesis gives $\hat{h}_{f^*\mathscr{L}} \sim \hat{h}_{\mathscr{L}} \circ f$. We have

$$\hat{h}_{\mathscr{L}} \circ f = \frac{1}{2}(b_{\mathscr{L}} \circ \Delta_A) \circ f + \ell_{\mathscr{L}} \circ f = \frac{1}{2}((b_L \circ (f \times f)) \circ \Delta_B) + \ell_{\mathscr{L}} \circ f,$$

with $b_{\mathscr{L}} \circ (f \times f)$ symmetric $\mathbb{Z}$-bilinear and $\ell_{\mathscr{L}} \circ f$ $\mathbb{Z}$-linear since f induces a group homomorphism $B(\overline{k}) \to A(\overline{k})$. Hence, the uniqueness part of Theorem 6.2.2 gives that $b_{f^*\mathscr{L}} = b_{\mathscr{L}} \circ (f \times f)$ and $\ell_{f^*\mathscr{L}} = \ell_{\mathscr{L}} \circ f$.

(3) Since $\mathscr{L}$ is symmetric, $\mathscr{L} \cong [-1]^*\mathscr{L}$ and so $\hat{h}_{\mathscr{L}} = \hat{h}_{\mathscr{L}} \circ [-1]$. Hence, given $x \in A(\overline{k})$,

$$b_{\mathscr{L}}(x,x) + \ell(x) = b_{\mathscr{L}}(-x,-x) + \ell_{\mathscr{L}}(-x) = b_{\mathscr{L}}(x,x) - \ell_{\mathscr{L}}(x) \implies \ell_{\mathscr{L}}(x) = 0.$$

(4) Since $\mathscr{L}$ is ample, $\mathscr{M} := \mathscr{L}^{\otimes n}$ is very ample for some $n \gg 0$ and so $\mathscr{M} \cong i_{\mathscr{M}}^*\mathcal{O}(1)$. By parts (2) and (3) of Weil's Thesis, $\hat{h}_{\mathscr{M}} \sim h_{i_{\mathscr{M}}}$. Since $\hat{h}_{\mathscr{M}} = n\hat{h}_{\mathscr{L}}$ by (1),

$$n\hat{h}_{\mathscr{L}} = h_{i_{\mathscr{M}}} + \epsilon$$

for $\epsilon : A(\overline{k}) \to \mathbb{R}$ bounded. Since the function $h_{i_{\mathscr{M}}}$ is non-negative, $\hat{h}_{\mathscr{L}}$ is therefore bounded below. A quick inductive argument using (3) shows

$$\hat{h}_{\mathscr{L}} \circ [m] = \frac{m(m+1)}{2} \cdot \hat{h}_{\mathscr{L}}$$

for every $m \geq 1$. It follows that torsion points of $A(\overline{k})$ have vanishing height (Is the converse true?) and non-torsion points have multiples whose heights increase in absolute value without bound.[59] Hence, $\hat{h}_{\mathscr{L}}$ cannot take on negative values and so $b_{\mathscr{L}}$ is positive semi-definite.

(5) This follows from Northcott's Theorem, which is [Con15, Thm 10.1.6]. □

6.3 Proof of the Mordell-Weil Theorem

Now that we have all of the ingredients needed to prove the Mordell-Weil Theorem, we state the final result tying everything together.

Theorem 6.3.1. *Let A be an abelian group, $m \in \mathbb{Z}^{\geq 2}$ such that $A/mA = A/m$ is finite, and $\langle \cdot, \cdot \rangle : A \times A \to \mathbb{R}$ a symmetric positive semi-definite $\mathbb{Z}$-bilinear form such that $\{a \in A : \langle a, a \rangle < C\}$ is finite for every $C > 0$. Then, A is finitely generated.*

Using that A is projective, we choose $\mathscr{L}$ an ample line bundle on A. By Theorem 6.2.3, the pairing

$$\langle \cdot, \cdot \rangle_{A/k} : A(k) \times A(k) \to \mathbb{R}$$

obtained by restricting $\hat{h}_{\mathscr{L}}$ is $\mathbb{Z}$-bilinear, symmetric, positive semi-definite, and satisfies that

$$\{x \in A(k) : [k(x) : k] \leq d, \langle x, x \rangle \leq C\}$$

is finite for every $C > 0$ and $d \geq 0$. Combining this with Theorems 6.3.1 and 5.2.1 proves the Mordell-Weil Theorem!

[59] Note that it is wrong to assume that $A(\overline{k})$ has a non-torsion point on the grounds that it is an infinite abelian group since, e.g., $\mathbb{Q}/\mathbb{Z}$ is infinite and torsion.

Remark 6.3.2. *The attentive reader might wonder what $A^\vee$ has to do with all of this. For a general abelian variety, there is no "canonical" choice of ample line bundle. However, for $A \times_k A^\vee$ there is such a canonical choice, namely the Poincaré bundle $\mathscr{P}_A$. The associated Tate canonical height yields a map $A(\overline{k}) \times A^\vee(\overline{k}) \to \mathbb{R}$ called the* ***Néron-Tate pairing****. This pairing is of great historical and computational importance.*

To conclude, we present a proof of Theorem 6.3.1.

Proof. Analogous to the situation for inner products, we define $\|a\| := \langle a, a\rangle^{1/2}$ given $a \in A$. Since $\langle \cdot, \cdot \rangle$ is symmetric, $\mathbb{Z}$-bilinear, and semi-definite, the Cauchy-Schwarz inequality $|\langle x, y\rangle| \leq \|x\| \, \|y\|$ holds.

Let $\{a_1, \ldots, a_n\}$ be a complete system of representatives for A/m. Define

$$C := 2 \max_{1 \leq j \leq n} \|a_j\|$$

and let $A_0 := \{a \in A : \|a\| < 2C\}$, which is finite by assumption. We claim that A_0 generates A. The key ingredient is the following. Given $a \in A \setminus A_0$ and $1 \leq j \leq n$, we have

$$\|a - a_j\|^2 = \langle a - a_j, a - a_j\rangle = \langle a, a\rangle - 2\langle a, a_j\rangle + \langle a_j, a_j\rangle$$

and so

$$\begin{aligned}
\|a - a_j\|^2 &\leq \|a\|^2 + 2\,|\langle a, a_j\rangle| + \|a_j\|^2 \\
&\leq \|a\|^2 + 2\,\|a\|\,\|a_j\| + \|a_j\|^2 \text{ by Cauchy-Schwarz} \\
&= \|a\|^2 + \|a_j\|\,(2\,\|a\| + \|a_j\|) \\
&\leq \|a\|^2 + \frac{1}{2}\,\|a\| \left(2\,\|a\| + \frac{1}{2}\,\|a\|\right) \\
&= \frac{9}{4}\,\|a\|^2,
\end{aligned}$$

where we have used that

$$\|a\| \geq 2C \geq 2\,\|a_j\| \implies \|a_j\| \leq \frac{1}{2}\,\|a\|.$$

Hence,

$$a \in A \setminus A_0, 1 \leq j \leq n \implies \|a - a_j\| \leq \frac{3}{2}\,\|a\|. \tag{5}$$

This sets us up for a proof by induction. To see this, let a be as above. By assumption, given $\alpha \in A$, there exists $1 \leq j \leq n$ such that $\alpha - a_j \in mA$. Using this, we obtain $b_1, b_2, \ldots \in A$ and $i_1, i_2, \ldots \in \{1, \ldots, n\}$ such that

$$\begin{aligned}
mb_1 &= a - a_{i_1} \\
mb_2 &= a - a_{i_1} - a_{i_2} \\
mb_3 &= a - a_{i_1} - a_{i_2} - a_{i_3} \\
&\vdots
\end{aligned}$$

Induction and Equation (5) together give that, for every $v \geq 1$, either $\|b_v\| < 2C/m$ or

$$\|b_v\| \leq \left(\frac{3}{2m}\right)^v \|a\|.$$

Since $m \geq 2$, we have $(3/2)m < 1$ and so choosing v large enough yields

$$\left(\frac{3}{2m}\right)^v \|a\| < \frac{2C}{m}.$$

Hence, $a = mb_v + a_{i_1} + \cdots + a_{i_v}$ lies in the $\mathbb{Z}$-linear span of A_0. $\square$

7 Acknowledgments

These notes represent an expanded version of my undergraduate honors thesis. As such, a huge shout-out goes to those who helped me with the writing of that document. In particular, I would like to thank my good friend Leon Liu for supporting me emotionally and bringing me fresh mathematical excitement all these years I have spent at the University of Texas at Austin. I would like to thank my brother Nathan, my sister-in-law Alicia Tokarski, Mom, and Joe for housing me during the trying times of COVID-19 and quarantine. Much of this document was written at their houses, atop a TV dinner tray kindly lent to me by Nathan. I would also like to thank Mom and Joe for supporting me financially during my undergraduate experience. I would like to thank my advisor Sam Raskin for mentoring me in algebraic geometry, number theory, and much more ever since he arrived at UT back in Fall 2018. You have been a tremendous help and inspiration to me both in terms of how to do mathematics and how to be a responsible mathematician. Finally, thanks goes to Arun, Richard, and Desmond for organizing an amazing SMC 2020.

References

[Alt14] Altinior. *Extension of a Line Bundle given on the generic fibre [sic]*. Mathematics Stack Exchange. Feb. 15, 2014. URL: https://math.stackexchange.com/questions/677190/extension-of-a-line-bundle-given-on-the-generic-fibre (visited on 05/08/2020).

[aut] The Stacks project authors. *The Stacks project*. URL: http://stacks.math.columbia.edu (visited on 05/08/2020).

[Bha17] Bhargav Bhatt. *Math 731: Topics in Algebraic Geometry I - Abelian Varieties*. Notes by Matt Stevenson. 2017. URL: http://www-personal.umich.edu/~stevmatt/abelian_varieties.pdf (visited on 05/08/2020).

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron Models*. Ergebnisse der Mathematik und ihrer Grenzgebiete vol. 21. Springer-Verlag, 1990. ISBN: 9783642080739.

[Con15] Brian Conrad. *Math 249C: Abelian Varieties*. Notes by Tony Feng. 2015. URL: http://virtualmath1.stanford.edu/~conrad/249CS15Page/handouts/abvarnotes.pdf (visited on 05/08/2020).

[edg18] edgarlorp. *Why does a flat finite type morphism of irreducible noetherian schemes map generic pt to generic pt [sic]*. Mathematics Stack Exchange. Sept. 7, 2018. URL: https://math.stackexchange.com/questions/2908265/why-does-a-flat-finite-type-morphism-of-irreducible-noetherian-schemes-map-gener (visited on 05/08/2020).

[Fan+05] Barbara Fantechi et al. *Fundamental Algebraic Geometry: Grothendieck's Algebraic Geometry Explained*. Mathematical Surveys and Monographs vol. 123. American Mathematical Society, 2005. ISBN: 0821835416.

[Liu02] Qing Liu. *Algebraic Geometry and Arithmetic Curves*. Oxford Graduate Texts in Mathematics. Oxford University Press, 2002. ISBN: 0198502842.

[MGE14] Ben Moonen, Gerard van der Geer, and Bas Edixhoven. *Abelian Varieties*. 2014. URL: https://www.math.ru.nl/~bmoonen/research.html#bookabvar (visited on 07/03/2020).

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften vol. 322. Spring-Verlag, 1999. ISBN: 3540653996.

[Poo02] Bjorn Poonen. *The Selmer Group, the Shafarevich-Tate Group, and the Weak Mordell-Weil Theorem*. Feb. 20, 2002. URL: http://math.mit.edu/~poonen/f01/weakmw.pdf (visited on 07/03/2020).

[Poo17] Bjorn Poonen. *Rational Points on Varieties*. Graduate Studies in Mathematics vol. 186. American Mathematical Society, 2017. ISBN: 9781470437732.

[Zha11] Li Zhan. *$\mathcal{L}$ is very ample, $\mathcal{U}$ is generated by global sections $\implies$ $\mathcal{L}\otimes\mathcal{U}$ is very ample*. Mathematics Stack Exchange. Nov. 28, 2011. URL: https://math.stackexchange.com/questions/86202/mathcall-is-very-ample-mathcalu-is-generated-by-global-sections-rig (visited on 05/08/2020).