Abelian Varieties Learning Seminar
Mordell-Weil Theorem

Stephanie Chen

December 1, 2023

1 Overview

The main focus of today's talk is to discuss a proof of the Mordell-Weil theorem.

Theorem 1.1 (Mordell-Weil Theorem). *Let K be a number field and A/K an abelian variety. Then $A(K)$ is finitely generated as a group.*

The proof is split into three main ingredients. The first is the Weak Mordell-Weil theorem, which states that $A(K)/mA(K)$ is a finite group for all $m \geq 2$. The second ingredient is the descent theorem, which allows us to conclude the Mordell-Weil theorem from the Weak Mordell-Weil theorem given the existence of a real-valued 'height' function on $A(K)$ satisfying certain properties. This motivates the discussion of heights, the final component of the proof. The main references used are [1] and [2]. Due to time constraints, many of the proofs will be only briefly sketched or omitted entirely. In all such cases, we refer readers to the references for a more detailed proof.

2 Weak Mordell-Weil Theorem

The first part of the talk is dedicated to proving the following theorem.

Theorem 2.1 (Weak Mordell-Weil Theorem). *Let K be a number field and A/K an abelian variety. Then for all integers $m \geq 2$, $A(K)/mA(K)$ is a finite abelian group.*

We mostly follow section VIII.1 of [1], with the appropriate modifications for generalizing to abelian varieties. Throughout this section, we fix $K, A/K, m$ as in Theorem 2.1. For a field extension L/K and $x \in A(L)$, we write $[m]x$ for $x \circ [m]$. We begin by reducing to the case where $A[m] \subset A(K)$ with the following lemma.

Lemma 2.2. *Let L/K be a finite Galois extension. Then if $A(L)/mA(L)$ is a finite group, $A(K)/mA(K)$ is also finite.*

Proof. Let $\varphi : A(K)/mA(K) \to A(L)/mA(L)$ be the map induced by the inclusion $A(K) \hookrightarrow A(L)$. Then,

$$\ker(\varphi) = \frac{A(K) \cap mA(L)}{mA(K)},$$

hence for any representative x of $\underline{x} \in \ker(\varphi)$, we may pick $y_x \in A(L)$ such that $[m]y_x = x$. We may then define a map

$$\ker(\varphi) \to \mathrm{Map}(\mathrm{Gal}(L/K), A(L)[m]) \qquad \underline{x} \mapsto f_{\underline{x}}. \tag{1}$$

where $f_{\underline{x}} : \mathrm{Gal}(L/K) \to A(L)[m]$ is given by choosing a representative x of $\underline{x}$ and setting

$$f_{\underline{x}}(\sigma) = y_x^\sigma - y_x$$

for all $\sigma \in \text{Gal}(L/K)$. One may check that the mapping (1) is injective. As $\text{Gal}(L/K), A(L)[m]$ are both finite, $\text{Map}(\text{Gal}(L/K), A(L)[m])$ is finite, and it follows that $\ker(\varphi)$ is finite. The exact sequence

$$0 \to \ker(\varphi) \to A(K)/mA(K) \to A(L)/mA(L)$$

then tells us that $A(K)/mA(K)$ is finite, as desired. □

As $A[m]$ is finite, the field L generated over K by the elements of $A[m]$ is a finite field extension L/K such that $A[m] \subseteq A(L)$. By Lemma 2.2, it then suffices to show that $A(L)/mA(L)$ is finite. Moving forward, we thus assume that $A[m] \subseteq A(K)$.

As $A(\overline{K})$ is a divisible group, for any $x \in A(K) \subseteq A(\overline{K})$, there exists $y \in A(\overline{K})$ such that $[m]y = x$. We may then define the *Kummer pairing*

$$\kappa : A(K) \times \text{Gal}(\overline{K}/K) \to A[m]$$

by

$$\kappa(x, \sigma) = y^\sigma - y.$$

Observe that this mapping is similar to the mapping of $f_{\underline{x}}$ in the proof of Lemma 2.2. We have the following basic properties of the Kummer pairing.

Lemma 2.3. *(i) The Kummer pairing is well-defined.*

(ii) The Kummer pairing is bilinear.

(iii) The kernel of the Kummer pairing in $A(K)$ is $mA(K)$.

(iv) The kernel of the Kummer pairing on the right is Gal$(\overline{K}/L)$ where

$$L = K([m]^{-1}A(K))$$

is the compositum of all fields $K(Q)$ as Q ranges over points in $A(\overline{K})$ satisfying $[m]Q \in A(K)$.

Then the induced linear map

$$\Phi : A(K)/mA(K) \to \mathit{Hom}(\mathit{Gal}(L/K), A[m]) \qquad P \mapsto \kappa(P, \cdot)$$

is injective, where L is as in (iv).

Proof. Properties (i)-(iv) may be checked by a direct computation. As L is a key field of interest for this section, we prove (iv) and refer the reader to the proof Theorem VIII.1.2 in [1] for (i)-(iii).

Let $\sigma \in \text{Gal}(\overline{K}/L)$. Then,

$$\kappa(P, \sigma) = Q^\sigma - Q = 0$$

as $Q \in A(L)$ by definition of L. Conversely, if $\sigma \in \text{Gal}(\overline{K}/K)$ is such that $\kappa(P, \sigma) = 0$ for all $P \in A(K)$, then for all $Q \in A(\overline{K})$ such that $[m]Q \in A(K)$,

$$0 = \kappa([m]Q, \sigma) = Q^\sigma - Q. \tag{2}$$

As L is the compositum of $K(Q)$ ranging over all such Q, it follows that $\sigma \in \text{Gal}(\overline{K}/L)$.

For any $\sigma \in \text{Gal}(\overline{K}/K)$, $\sigma([m]^{-1}A(K)) = [m]^{-1}A(K)$. It then follows that $\sigma(L) = L$, so L/K is a Galois extension. As the Kummer pairing is bilinear by (ii), we then have an induced linear map

$$\Phi' : A(K) \to \text{Hom}(\text{Gal}(L/K), A[m]) \qquad P \mapsto \kappa(P, \cdot).$$

By (iii), the kernel of Φ' is $mA(K)$, so Φ as in the problem statement is injective. □

Lemma 2.3 reduces the proof of the Weak Mordell Weil theorem to showing that the field extension L/K is finite.

Denote by M_K^0 and M_K^∞ the set of non-archimedean and archimedean valuations of K respectively. Fix $v \in M_K^0$ and let R_v be the discrete valuation ring for v and k_v the corresponding residue field. The reduction of A at v is then given by the base change $\mathcal{A}_{k_v}$ where $\mathcal{A}$ is the Néron model of A with respect to R_v. We then say that A has *good reduction at* v is $\mathcal{A}_{k_v}$ is nonsingular and *bad reduction at* v otherwise. In the case that $v(m) \neq 0$ and A has good reduction at v, by [1, Prop VIII.4], the reduction map $A(K)[m] \to \mathcal{A}_{k_v}(k_v)$ given on points by $[x_0 : \dots : x_n] \mapsto [\pi(x_0) : \dots : \pi(x_n)]$ with $\pi : R_v \to k_v$ the projection and $x_0, \dots, x_n \in R_v$ is injective.

Recall that M_K^0 is in 1-to-1 correspondence with the nonzero prime ideals of $\mathcal{O}_K$, the ring of integers of K. Fix $v \in M_K^0$ and let $\mathfrak{p}$ be the prime ideal corresponding to v. Let L/K be an extension of fields. Then, L/K is unramified at v if all the exponents on the prime ideals in the unique prime factorization of $\mathfrak{p}\mathcal{O}_L$ in $\mathcal{O}_L$ are equal to 1. Two valuations $v, v' \in M_K$ have the same *place* if and only if they determine the same valuation ring.

Lemma 2.4. *Let*

$$L = K([m]^{-1}A(K))$$

be as defined in 2.3. Then,

(i) The extension L/K is abelian and has exponent m.

(ii) Let

$$S = \{v \in M_K^0 \mid A \text{ has bad reduction at } v\} \cup \{v \in M_K^0 \mid v(m) \neq 0\} \cup M_K^\infty.$$

Then for all $v \in M_K \setminus S$, L/K is unramified at v.

Proof. By Lemma 2.3, we have an injection

$$\mathrm{Gal}(L/K) \to \mathrm{Hom}(A(K), A[m]) \qquad \sigma \mapsto \kappa(\cdot, \sigma),$$

from which (i) follows.

For (ii), let $v \in M_K \setminus S$ and let $Q \in A(\overline{K})$ be such that $[m]Q \in A(K)$. Let $K' = K(Q)$. As L is the compositum of all such K', it suffices to show that K'/K is unramified at v. Let $v' \in M_{K'}$ be a place lying above v, i.e. the corresponding prime ideal of $\mathcal{O}_{K'}$ pulls back to the prime ideal of v in $\mathcal{O}_K$. We have a corresponding extension of residue fields $k'_{v'}/k_v$. As $v \notin S$, A has good reduction at v and thus also at v'. Let

$$\pi : A(K') \to \mathcal{A}_{k'_{v'}}(k'_{v'})$$

be the reduction map. Let $I_{v'/v} \subseteq \mathrm{Gal}(\overline{K}/K)$ be the inertia group for v'/v, i.e. the subgroup that acts trivially on $k'_{v'}/k_v$. Then by definition, for any $\sigma \in I_{v'/v}$,

$$\pi(Q^\sigma - Q) = \pi(Q)^\sigma - \pi(Q) = 0.$$

As $[m]Q \in A(K)$,

$$[m](Q^\sigma - Q) = ([m]Q)^\sigma - [m]Q = 0.$$

By [1, Prop VIII.4], it follows that $Q^\sigma - Q = 0$. Then, $I_{v'/v}$ acts trivially on Q, so K' is unramified over K at v'. As this holds for all v' lying over v, K'/K is unramified over v. □

Now that we have established these two properties of L, we show that as L satisfies these two properties, L/K must be a finite extension. We note that in Lemma 2.4, S is a finite set.

Lemma 2.5. *Let K be a number field, $S \subseteq M_K$ a finite set of places containing M_K^∞, and $m \geq 2$ an integer. Let L/K be the maximal abelian exension of K having exponent m that is unramified outside of S. Then, L/K is a finite extension.*

Proof. We give a rough sketch of the proof. First, we may assume that K contains the mth roots of unity μ_m by replacing K with a finite extension. From algebraic number theory, we have that the class number of K is finite. We may then enlarge S by adjoining finitely many elements such that the ring of S integers

$$R_S = \{a \in K \mid v(a) \geq 0 \text{ for all } v \in M_K \setminus S\}$$

is a principal ideal domain and $v(m) = 0$ for all $v \notin S$. By applying Kummer theory, we see that L is the largest subfield of $K(\sqrt[m]{a} : a \in K)$ that is unramified outside of S. The rest of the proof boils down to showing that the set

$$T_S = \{a \in K^*/(K^*)^m \mid \operatorname{ord}_v(a) \equiv 0 \pmod{m} \text{ for all } v \in M_K \setminus S\}$$

is finite, which follows from the surjection $R_S^*/(R_S^*)^m \to T_S$ and Dirichlet's S-unit theorem, which tells us tha R_S^* is a finitely generated group. See [1, Prop VIII.1.6] for the full proof. $\square$

By combining Lemma 2.4 and Lemma 2.5, we have that L/K is a finite extension. This completes the proof of the Weak Mordell-Weil theorem.

3 Heights

3.1 Descent Theorem

Theorem 3.1 (Descent Theorem)**.** *Let A be an abelian group. Suppose that there exists a mapping*

$$h : A \to \mathbb{R}$$

satisfying the following three properties

(i) For any $x \in A$, there is a constant $C_{1,x} \in \mathbb{R}$, depending on A and x, such that

$$h(x + y) \leq 2h(y) + C_{1,x} \quad \text{for all } y \in A.$$

(ii) There exists an integer $m \geq 2$ and a constant $C_2 \in \mathbb{R}$, depending on A, such that

$$h(mx) \geq m^2 h(x) - C_2 \quad \text{for all } x \in A.$$

(iii) For every $C \in \mathbb{R}$, the set

$$\{x \in A \mid h(x) \leq C\}$$

is finite.

If the quotient group A/mA is finite for m in (ii), then A is finitely generated.

Proof. For $x \in A$, we will also refer to $h(x)$ as the height of x. Let $x_1, \ldots, x_r$ be representatives for the finitely many cosets in A/mA and fix $y \in A$. Let $1 \leq i_1 \leq r$ be such that $y \equiv x_{i_1} \in A/mA$. We may then write

$$y_0 := y = my_1 + x_{i_1}$$

for some $y_1 \in A$. By iteratively applying this procedure, we may obtain a list of points

$$y_0 = my_1 + x_{i_1},$$
$$y_1 = my_2 + x_{i_2},$$
$$\vdots$$
$$y_{n-1} = my_n + x_{i_n}$$

for any $n \in \mathbb{N}^+$. Let

$$C_1 = \max\{C_{1,-x_1}, \ldots, C_{1,-x_r}\}$$

be the maximum of the constants for the $-x_i$ in (i). Fix $n \in \mathbb{N}^+$. Then for $1 \leq j \leq n$,

$$\begin{aligned}
h(y_j) &\leq \frac{h(mx_j) + C_2}{m^2} && \text{by (ii)} \\
&= \frac{h(y_{j-1} - x_{i_j}) + C_2}{m^2} \\
&\leq \frac{2h(y_{j-1}) + C_1 + C_2}{m^2} && \text{by (i)}
\end{aligned}$$

Applying this iteratively starting from y_n, we get

$$\begin{aligned}
h(y_n) &\leq \left(\frac{2}{m^2}\right)^n h(y_0) + C_1 \sum_{j=0}^{n-1} \frac{2^j}{m^{2j+2}} + C_2 \sum_{j=0}^{n-1} \frac{2^j}{m^{2j+2}} \\
&< \frac{h(y)}{2^n} + \frac{C_1 + C_2}{m^2 - 2} && m \geq 2 \\
&\leq \frac{h(y)}{2^n} + \frac{C_1 + C_2}{2} && m \geq 2
\end{aligned}$$

By taking n to be sufficiently large, we then get

$$h(y_n) < 1 + \frac{C_1 + C_2}{2}.$$

Note that both C_1, C_2 are independent of y. Observe that

$$y = m^n y_n + \sum_{j=1}^{n} m^{j-1} x_{i_j}.$$

It follows that for any $y \in A$, y may be written as a linear combination of

$$\{x_1, \ldots, x_r\} \cup \{x \in A \mid h(x) < 1 + \frac{C_1 + C_2}{2}\}.$$

By (iii), this is a finite set, hence A is finitely generated. $\square$

If we are able to find a height function $h : A(K) \to \mathbb{R}$ satisfying the conditions of Theorem (3.1), the Mordell-Weil Theorem will then follow from the Weak Mordell Weil theorem.

3.2 Heights on Projective Space

Recall that we may embed an abelian variety A/K into projective space $\mathbb{P}_K^{2g+1}$, where $g = \dim(A)$. We thus begin our precede our discussion of heights on abelian varieties by studying a height function for projective space. The main references for this subsection are [1, §VIII.5] and [2, §6.1]. Throughout this section, we take K to be a number field unless otherwise stated.

Definition 3.2. We denote by $M_{\mathbb{Q}}$ the *set of standard absolute values* on $\mathbb{Q}$, which consists of the following:

(i) The archimedean absolute value

$$|x|_\infty = \max\{x, -x\}$$

(ii) For each prime $p \in \mathbb{Z}$, the nonarchimedean absolute value

$$\left|p^n \frac{a}{b}\right|_p = p^{-n} \qquad a, b \in \mathbb{Z}, p \nmid ab$$

For any number field K, the *set of standard absolute values* on K is defined to be the set of all absolute values on K whose restriction to $\mathbb{Q}$ is an element of $M_{\mathbb{Q}}$. We denote this set by M_L. We will also denote by M_K^∞, M_K^0 the set of standard absolute values on K which are archimedean and nonarchimedean respectively.

Definition 3.3. For any $v \in M_K$, the *local degree at* v is

$$n_v := [K_v : \mathbb{Q}_v]$$

where $K_V, \mathbb{Q}_v$ denote the completions with respect to v.

We recall without proof two standard formulas from algebraic number theory.

Proposition 3.4 (Extension Formula)**.** *Let $\mathbb{Q} \subseteq K \subseteq L$ be a tower of number fields and let $v \in M_K$. Then*

$$\sum_{w \in M_L, w|v} n_w = [L : K] n_v \tag{3}$$

where $w|v$ indicates that the sum is taken over all standard absolute values w on L such that w restricted to K is equal to v.

Proposition 3.5 (Product Formula)**.** *For any $x \in K^*$,*

$$\prod_{v \in M_K} |x|_v^{n_v} = 1. \tag{4}$$

Definition 3.6. Let K' be a finite extension of K and let $P \in \mathbb{P}_K^N(K')$ be a point with homogeneous coefficients

$$P = [x_0 : \ldots : x_N] \qquad x_0, \ldots, x_N \in K'.$$

We define the multiplicative height of P relative to K' by

$$H_{K',N}(P) = \prod_{v \in M_{K'}} \max\{|x_0|_v, \ldots, |x_N|_v\}^{n_v} \tag{5}$$

and the additive height of P relative to K' by

$$h_{K',N}(P) = \sum_{v \in M_{K'}} n_v \max\{\log|x_0|_v, \ldots, \log|x_N|_v\}. \tag{6}$$

Observe that the two definitions are related by

$$h_{K',N}(P) = \log(H_{K',N}(P)). \tag{7}$$

Remark 3.7. In [1], Silverman focuses on the multiplicative height when discussing heights on projective space in §VIII.5. As our goal is to build up to defining the Néron-Tate canonical height, which comes from the additive height, we instead use the additive height here.

Proposition 3.8. *Let $P \in \mathbb{P}_K^N(K')$. Then,*

(i) The height $h_{K',N}(P)$ is invariant under scaling by K'^*.

(ii) $h_{K',N}(P) \geq 0$

(iii) For any finite extension L/K',

$$h_{L,N}(P) = [L : K] h_{K',N}(P).$$

Proof. For (i): By the product formula (Proposition 3.5),

$$\prod_{v \in M_{K'}} \max\{|\lambda x_0|_v : \ldots : |\lambda x_N|_v\}^{n_v} = \prod_{v \in M_{K'}} |\lambda|^{n_v} \max\{|x_0|_v, \ldots, |x_N|_v\}^{n_v} = \prod_{v \in M_{K'}} \max\{|x_0|_v, \ldots, |x_N|_v\}^{n_v}.$$

For (ii): There is some choice of homogeneous coordinates for P such that at least one of the coordinates is 1. It then follows that each factor in the sum for $h_K(P)$ is at least 0.

For (iii): A direct computation gives

$$\begin{aligned}
h_{L,N}(P) &= \sum_{w \in M_L} n_w \max\{\log |x_0|_w, \ldots, |x_N|_w\} \\
&= \sum_{v \in M_{K'}} \sum_{w \in M_L, w|v} n_w \max\{\log |x_0|_v, \ldots, |x_N|_v\} && x_i \in K' \\
&= \sum_{v \in M_K} [L : K'] n_v \max\{\log |x_0|_v, \ldots, |x_N|_v\} && \text{extension formula} \\
&= [L : K'] h_{K',N}(P).
\end{aligned}$$

□

Definition 3.9. Let $P \in \mathbb{P}^N_K(\overline{K})$. Let K' be a number field such that $P \in \mathbb{P}^N_K(K')$. The absolute height of P is then defined by

$$h_N(P) = \frac{1}{[K' : K]} h_{K',N}(P)$$

where we take the positive root. Note that by Proposition 3.8 (iii), the absolute height is independent of the choice of K. The other properties of Proposition 3.8 also hold for the absolute height.

Lemma 3.10. *Let*

$$F : \mathbb{P}^N_K \to \mathbb{P}^N_K$$

be an automorphism of projective space. Then there is some constant $C \in \mathbb{R}$ depending only on F such that

$$|h_N(F(P)) - h_N(P)| < C$$

for all $P \in \mathbb{P}^N_K(\overline{K})$

Proof. Recall from [3, Example II.7.1.1] that the automorphisms of $\mathbb{P}^N_K$ correspond to elements of $\mathrm{PGL}_N(K) = \mathrm{GL}_{N+1}(K)/K^*$. Let $M = (a_{i,j})$ be an invertible matrix corresponding to F, so

$$F([x_0 : \ldots : x_N]) = \left[\sum_{j=0}^{N} a_{0,j} x_j : \ldots : \sum_{j=0}^{N} a_{N,j} x_j \right].$$

For ease of notation, write

$$f_i = \sum_{j=0}^{N} a_{i,j} X_j \in K[X_0, \ldots, X_N]$$

for $1 \leq i \leq N$. Let $P = [x_0 : \ldots : x_N]$ and $K' = K(x_0, \ldots, x_N)$. For each absolute value $v \in M_K$, let

$$|P|_v = \max_{0 \leq i \leq N} |x_i|_v \qquad |F(P)|_v = \max_{0 \leq i \leq N} |f_i(P)|_v \qquad |F|_v = \max_{0 \leq i,j \leq N} |a_{i,j}|_v.$$

Then,

$$h_{K',N}(P) = \sum_{v \in M_{K'}} n_v \log |P|_v \qquad h_{K',N}(F(P)) = \sum_{v \in M_{K'}} n_v \log |F(P)|_v,$$

so correspondingly, we define

$$h_{K',N}(F) = \sum_{v \in M_{K'}} n_v \log |F|_v.$$

Define $\epsilon : M_{K'} \to \{0, 1\}$ by

$$\epsilon(v) = \begin{cases} 1 & v \in M^\infty_{K'} \\ 0 & v \in M^0_{K'} \end{cases},$$

so the triangle inequality for absolute values becomes

$$|t_1 + \ldots + t_n|_v \leq n^{\epsilon(v)} \max\{|t_1|_v, \ldots, |t_n|_v\}.$$

The triangle equality yields

$$|f_i(P)|_v \le (N+1)^{\epsilon(v)}|F|_v|P|_v,$$

so

$$|F(P)|_v \le (N+1)^{\epsilon(v)}|F|_v|P|_v,$$

hence

$$h_{K',N}(F(P)) - h_{K',N}(P) \le h_{K',N}(F) + \log(N+1)\sum_{v\in M_{K'}}\epsilon(v)n_v.$$

The extension formula tells us

$$\sum_{v\in M_{K'}}\epsilon(v)n_v = \sum_{v\in M_{K'}^\infty} n_v = [K':\mathbb{Q}],$$

so

$$h_N(F(P)) - h_N(P) \le h_N(F) + [K:\mathbb{Q}]\log(N+1).$$

For the lower bound, as M is an invertible matrix, there exist unique scalars $g_{i,j}\in K'$ such that

$$X_i = \sum_{j=0}^N g_{i,j}f_j.$$

Let

$$|G|_v = \max_{1\le i,j\le N}|g_{i,j}|_v \qquad h_{K,N}(G) = \sum_{v\in M_{K'}} n_v\log|G|_v.$$

Then,

$$|x_i|_v = \left|\sum_{j=0}^N g_{i,j}f_j(P)\right| \le (N+1)^{\epsilon(v)}\max_{0\le j\le N}|g_{i,j}(P)f_j(P)|_v \le (N+1)^{\epsilon(v)}\max_{0\le j\le N}|g_{i,j}(P)|_v|F(P)|_v,$$

hence taking the maximum over i gives

$$|P|_v \le (N+1)^{\epsilon(v)}\max_{0\le i,j\le N}|g_{i,j}(P)|_v|F(P)|_v \le (N+1)^{\epsilon(v)}|G|_v|F(P)|_v.$$

From here, it follows that

$$h_N(F(P)) - h_N(P) \ge -[K:\mathbb{Q}](\log(N+1)+\log|G|_v).$$

We thus have that $|h_N(F(P)) - h_N(P)|$ is bounded by a constant independent of P, as desired. □

The definition of an additive absolute height on projective space over K allows us to define (up to a bounded difference) a height for a projective K-scheme X relative to very ample line bundles on X. For ease of notation, we will write $h\sim h'$ for real-valued functions on the same set if $|h-h'|<C$ for some $C\in\mathbb{R}$.

Lemma 3.11. *Let X be a projective K-variety and $\mathcal{L}$ a very ample line bundle on X with associated closed embedding $\iota_{\mathcal{L}}: X\hookrightarrow \mathbb{P}^d_K$ and $f: X\to\mathbb{P}^N_K$ a K-morphism for some $n>0$ such that $f^*\mathcal{O}(1)\cong\mathcal{L}$. Let $h_f := h_N\circ f$, $h_{\iota_{\mathcal{L}}} := h_d\circ\iota_{\mathcal{L}}$ as functions $X(\overline{K})\to\mathbb{R}$. Then, $h_f\sim h_{\iota_{\mathcal{L}}}$.*

Proof. The main idea behind the proof is as follows. As f is a morphism of projective varieties, we may write

$$f(x_0,\dots,x_n)\to[f_0(x_0,\dots,x_n):\dots:f_N(x_0,\dots,x_n)]$$

with $f_0,\dots,f_n\in K[X_0,\dots,X_n]$. The closed embedding $\iota_{\mathcal{L}}$ is given by choosing $d+1$ sections $\ell_0,\dots,\ell_d\in\Gamma(X,\mathcal{L})$ that globally generate $\mathcal{L}$. Note that by Lemma 3.10, the choice of the sections does not affect the result. Then, we may write $\iota_{\mathcal{L}}$ as

$$\iota_{\mathcal{L}}(x_0,\dots,x_n)\to[\ell_0(x_0,\dots,x_n):\dots:\ell_d(x_0,\dots,x_n)].$$

Note that $d\le N$, so we may take $\iota_{\mathcal{L}}$ to be a closed embedding into $\mathbb{P}^N$ by

$$\iota_{\mathcal{L}}(x_0,\dots,x_n)\to[\ell_0(x_0,\dots,x_n):\dots:\ell_d(x_0,\dots,x_n):0\dots:0].$$

The assumption that $f^*(\mathcal{O}(1))\cong\mathcal{L}$ then tells us that $\iota_{\mathcal{L}}=\sigma\circ f$ for some automorphism $\sigma:\mathbb{P}^N\to\mathbb{P}^N$. Applying Lemma 3.10 then gives the desired result. For the full proof, see [2, Lem 6.1.3]. □

In particular, Lemma 3.11 tells us that for two isomorphic very ample line bundles $\mathcal{L} \cong \mathcal{L}'$ on X, $h_{\iota_{\mathcal{L}}} \sim h_{\iota_{\mathcal{L}'}}$.

To a line bundle $\mathcal{L}$ on X, we may associate a Weil height associated characterized by the following theorem.

Theorem 3.12 (Weil's Thesis)**.** *There exists a unique assignment of pairs $(X, \mathcal{L})$ with X a projective K-scheme and $\mathcal{L}$ a line bundle on X to functions $h_{\mathcal{L}} : X(\overline{K}) \to \mathbb{R}$ modulo $\sim$ satisfying the following properties*

(i) $h_{\mathcal{L}\otimes\mathcal{L}'} = h_{\mathcal{L}} + h_{\mathcal{L}'}$

(ii) $(\mathbb{P}^n_K, \mathcal{O}(1)) \mapsto h_n$

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

Furthermore, if $\mathcal{L}$ is very ample, then $h_{\mathcal{L}} = h_{i_{\mathcal{L}}}$.

See [2, Thm 6.1.4] for a proof.

3.3 Neron-Tate Canonical Height

We now return to abelian varieties. Throughout this section, let A/K be an abelian variety over a number field K. We recall some facts from Lecture 3 (line bundles on abelian varieties).

Lemma 3.13 (corollary to theorem of cube)**.** *Let Y be a K-scheme. Then for all triples of morphisms $f, g, h : Y \to A$ and any line bundle $\mathcal{L}$ on X, the line bundle given by*

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

is trivial on Y.

Lemma 3.14. *Let $\mathcal{L}$ be a line bundle on A. Then for all $m \in \mathbb{Z}$,*

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

We then obtain the following properties of the Weil height for a very ample line bundle on A.

Lemma 3.15. *Let $\mathcal{L}$ be a very ample line bundle on A. Then, $h_{\mathcal{L}} : A(\overline{K}) \to \mathbb{R}$ satisfies the following properties:*

(i) $h_{\mathcal{L}}$ *is almost quadratic, i.e. the mapping*

$$(x, y, z) \mapsto h_{\mathcal{L}}(x+y+z) - (h_{\mathcal{L}}(x+y) + h_{\mathcal{L}}(x+z) + h_{\mathcal{L}}(y+z)) + (h_{\mathcal{L}}(x) + h_{\mathcal{L}}(y) + h_{\mathcal{L}}(z))$$

is bounded as a function $A^3(\overline{K}) \to \mathbb{R}$.

(ii) If $\mathcal{L}$ is symmetric, i.e. $\mathcal{L} \cong [-1]^*\mathcal{L}$, then for all $m \in \mathbb{Z}$, there exists a constant $C_m \in \mathbb{R}$ such that for all $P \in A(\overline{K})$,

$$|h_{\mathcal{L}}([m]P) - m^2 h_{\mathcal{L}}(P)| < C_m.$$

Proof. We give only a brief sketch of the ideas of the proof here. Property (i) follows from Lemma 3.13 using Lemma 3.11. See [2, Lem 6.2.1] for a full proof. For property (ii), Lemma 3.14 together with Weil's Thesis properties (i) and (ii) tells us that

$$h_{\mathcal{L}} \circ [m] \sim h_{[m]^*\mathcal{L}} \sim \frac{m^2+m}{2} h_{\mathcal{L}} + \frac{m^2-m}{2} h_{[-1]^*\mathcal{L}} \sim m^2 h_{\mathcal{L}}.$$

$\square$

We now define the Néron-Tate canonical height, which turns all the equivalent up to a bounded difference conditions into actual equivalences.

Definition 3.16. Let $\mathcal{L}$ be a very ample line bundle on A. The Néron-Tate canonical height associated to $\mathcal{L}$ is the function $\hat{h}_{\mathcal{L}} : A(\overline{K}) \to \mathbb{R}$ defined by

$$\hat{h}_{\mathcal{L}}(P) = \lim_{n\to\infty} 4^{-n} h_{\mathcal{L}}([2^n]P) \tag{8}$$

for all $P \in A(\overline{K})$.

Proposition 3.17. *Let $\mathcal{L}, \mathcal{L}'$ be very ample line bundles on A and $f : B \to A$ a morphism of abelian varieties. The Néron-Tate canonical height then satisfies the following properties:*

(i) $\hat{h}_{\mathcal{L}\otimes\mathcal{L}'} = \hat{h}_{\mathcal{L}} + \hat{h}_{\mathcal{L}'}$

(ii) $\hat{h}_{f^*\mathcal{L}} = \hat{h}_{\mathcal{L}} \circ f$

(iii) For all $x, y, z \in A(\overline{K})$,

$$\hat{h}_{\mathcal{L}}(x+y+z) = \hat{h}_{\mathcal{L}}(x+y) + \hat{h}_{\mathcal{L}}(x+z) + \hat{h}_{\mathcal{L}}(y+z) - \hat{h}_{\mathcal{L}}(x) - \hat{h}_{\mathcal{L}}(y) - \hat{h}_{\mathcal{L}}(z)$$

(iv) If $\mathcal{L}$ is symmetric, then for all $m \in \mathbb{Z}$, $P \in A(\overline{K})$,

$$\hat{h}_{\mathcal{L}}([m]P) = m^2 \hat{h}_{\mathcal{L}}(P)$$

(v) For all $P, Q \in A(\overline{K})$

$$\hat{h}_{\mathcal{L}}(P+Q) + \hat{h}_{\mathcal{L}}(P-Q) = 2\hat{h}_{\mathcal{L}}(P) + 2\hat{h}_{\mathcal{L}}(Q)$$

(vi) If $\mathcal{L}$ is symmetric, then the set

$$\{P \in A(\overline{K}) \mid [K(P) : K] \le d, \hat{h}_{\mathcal{L}}(P) \le C\}$$

is finite for all $C > 0, d \ge 0$.

Proof. Properties (i) and (ii) follow from (i) and (iii) of Theorem 3.12 respectively. Similarly, properties (iii) and (iv) follow from (i) and (ii) of Lemma 3.15. Property (v) follows from setting $x = P, y = Q, z = -Q$ in (iii) and noting that $\hat{h}_{\mathcal{L}}(0) = 0$. Property (vi) is given by a result known as Northcott's Theorem (c.f. [4, Thm 10.1.6]). The starting observation is that the set

$$\{P \in \mathbb{P}^N(\mathbb{Q}) \mid h_N(P) < C\}$$

is finite for all $C > 0$ as it has at most $(2C+1)^N$ elements. □

From any very ample line bundle $\mathcal{L}$ on A, the line bundle $\mathcal{L}' = \mathcal{L} \otimes [-1]^*\mathcal{L}$ is a very ample symmetric line bundle on A. Observe that $\hat{h}_{\mathcal{L}'} : A(K) \to \mathbb{R}$ then satisfies the conditions of Theorem 3.1. This completes the proof of the Mordell-Weil Theorem.

One final remark we make is that the Mordell-Weil Theorem is also related to the Mordell Conjecture:

Theorem 3.18 (Mordell Conjecture)**.** *If X is an algebraic curve over a number field K of genus $g \ge 2$, then $X(K)$ is finite.*

I did not get around to preparing material related to this topic, but a nice reference that walks through Falting's proof of the Mordell Conjecture is [5].

References

[1] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2010.

[2] Zachary Gardner. The Mordell-Weil Theorem for abelian varieties over global fields. Notes for UT Austin Summer Minicourse "Abelian varieties and the Mordell-Weil Theorem".

[3] Robin Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics. Springer-Verlag, New York, USA, 1977.

[4] Brian Conrad. Math 249c: Abelian varieties. `https://virtualmath1.stanford.edu/~conrad/249CS15Page/handouts/abvarnotes.pdf`, 2015. Notes by Tony Feng.

[5] Bharghav Bhatt, Andrew Snowden, and et. al. Faltings's proof of the mordell conjecture. `https://www.math.purdue.edu/~murayama/Mordell.pdf`. Notes for the learning seminar, organized by Bharghav Bhatt and Andrew Snowden.