Contents

The goal of this note is to go through the book “height in dio geo”, chapter 10, 11 and 14. In particular,

1. chapter 10 is based on chapter 8 and 9.
2. chapter 11 is based on chap $2, 8, 9, 10$.
3. chapter 14 is based on chap 12 (abc conjecture), chap 13 (Nevanlinna theory).

Hence, we organize the study into a brief introduction to the naive height theory, without going as deep as the subspace theorem. Then, we immediately begin study chapter 8 and 9, and then proceed to the three main chapters I want to cover.

Chapter 1

Heights

Throughout the book, it is safe to assume we are working with number fields only (so no function fields).

In particular, this chapter is more detailed than necessary for our purpose, just so that we start slowly.

1.1 A Bit Algebraic Number Theory

Definition 1.1.1

A ***place*** v is an equivalence class of non-trivial absolute value on K, where two absolute values $v \sim v'$ if they induce the same topology.

Remark 1.1.2

Recall two absolute values $|\cdot|_1$ and $|\cdot|_2$ are equivalent if and only if there is real number $s > 0$ so $|x|_1 = |x|_2^s$ for all $x \in K$.

Let L/K be a field extension, and w be a place on L and v a place on K, then we write $w \mid v$ to mean $w|_K = v$, or more precisely, any representative of w restrict to K is a representative of v.

Definition 1.1.3

The completion of K with respect to the place v is an extension field K_v with place w of K, such that:

1. $w \mid v$
2. The topology of K_v induced by w is complete
3. K is dense subset of K_v in the above topology

Let $K = \mathbb{Q}$, then the ordinary absolute value $|\cdot| := |\cdot|_\infty$ gives $\mathbb{R}$ as its completion. On the other hand, for prime number p define $|m/n|_p := p^{-a}$, where a is the unique

number such that $m/n = p^a \cdot (m'/n')$ with $\gcd(m', p) = 1 = \gcd(n', p)$. Equivalently, $|\cdot|_p$ is uniquely determined by the condition

$$|q|_p := \begin{cases} 1 & \text{for primes } q \neq p \\ \frac{1}{p} & \text{if } p = q \end{cases}$$

The completion of this is the p-adic numbers and we denote by $\mathbb{Q}_p$.

Recall we call an absolute value non-archimedean if $|x + y| \leq \max(|x|, |y|)$ for all $x, y \in K$. Thus, if $|x + y| < \max(|x|, |y|)$ for some $x, y \in K$ then we call this absolute value archimedean.

Theorem 1.1.4

The only complete archimedean fields are $\mathbb{R}$ and $\mathbb{C}$.

Recall that for fintie extension L/K, we define the norm $N_{L/K}$ and trace $T_{L/K}$ as follows. Each $a \in L$ determines a K-linear map $m : L \to L$ by $x \mapsto ax$, and we define

$$N_{L/K}(a) = \det(m_a), \quad T_{L/K}(a) := \operatorname{tr}(m_a)$$

Example 1.1.5

If L/K is Galois extension, then

$$N_{L/K}(a) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(a)$$

Explicitly, if $L = \mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$, then $N(a + b\sqrt{2}) = (a + b\sqrt{2})(a - b\sqrt{2})$ because the Galois group in this case has order 2, and its generated by the element which sends $\sqrt{2}$ to $-\sqrt{2}$.

Not Relevant

More generally, for $f : X \to Y$ finite locally free morphism of schemes of rank $k > 0$, we can define a norm $N_{X/Y} : \mathrm{Pic}(X) \to \mathrm{Pic}(Y)$ as follows. By assumption, $f_*\mathscr{O}_X$ is finite locally free $\mathscr{O}_Y$-algebra, and thus we can define a morphism of sheaves $N_{f_*\mathscr{O}_X/\mathscr{O}_Y} : f_*\mathscr{O}_X \to \mathscr{O}_Y$ by $N_{f_*\mathscr{O}_X/\mathscr{O}_Y}(V)(b) := \det(m_b)$, where for $b \in \Gamma(V, f_*\mathscr{O}_X)$ we define $m_b : \Gamma(V, f_*\mathscr{O}_X) \to \Gamma(V, f_*\mathscr{O}_X)$ as the multplication by b.

Then for line bundle $\mathscr{L}$ on X, we see $f_*\mathscr{L}$ is an invertible $f_*\mathscr{O}_X$-module and thus we can find open cover $V = (V_i)$ of Y so $f_*\mathscr{L}$ is given by Čech 1-cocycle (g_{ij}) of $(f_*\mathscr{O}_X)^\times$, i.e. $g_{ij} \in \Gamma(V_i \cap V_j, (f_*\mathscr{O}_X)^\times)$ and $g_{kj}g_{ji} = g_{ki}$ on the triple intersection. Then one checks $(N_{f_*\mathscr{O}_X/\mathscr{O}_Y}(g_{ij}))$ is a Čech 1-cocycle of $\mathscr{O}_Y^\times$, i.e. it defines a line bundle on Y. This is the global norm map.

Proposition 1.1.6

Let K be a field which is complete with respect to place v and L/K finite extension.

Then there is a unique extension w of $|\cdot|_v$ on L, such that

$$|x|_w := |N_{L/K}(x)|_v^{1/[L:K]}$$

In particular, L is complete with respect to $|\cdot|_w$.

For K with non-archimedean place v and L a finite extension of K, define

$$R_v := \{x \in K : |x|_v \leq 1\}$$

This is a local ring with unique maximal ideal $\mathfrak{m}_v := \{x \in K : |x|_v < 1\}$. In particular, we have residue field $\kappa(v) := R_v/\mathfrak{m}_v$.

Definition 1.1.7

Let L/K be a finite extension and v a non-archimedean place on K and w extends v. Then we define:

1. the ***residue degree*** $f_{w/v}$ of L/K in w is the dimension of $\kappa(w)$ over $\kappa(v)$.
2. the ***ramification index*** $e_{w/v}$ of L/K is defined to be the index of the subgroup $|K^\times|_v$ in $|L^\times|_w$.

Geometrically, the ramification index keep track of how the prime ideal associated with v splits in L, i.e. say $w_1, ..., w_r$ are all the places induced by prime ideals $\mathfrak{q}_1, ..., \mathfrak{q}_r$ lying over the prime ideal $\mathfrak{p}$ of v, then $\mathfrak{p}\mathcal{O}_L = \amalg_1^{e_1} ... \amalg_r^{e_r}$ where $e_i := e_{w_i/v}$.

A place v is called ***discrete*** if $|K^\times|_v$ is cyclic. In this case, $\mathfrak{m}_v$ is a principal ideal and any generator is called a uniformizer.

Lemma 1.1.8: Hensel Lemma

Let K be a complete non-archimedean field with place v. Let $f \in K[t]$ be monic with reduction $\overline{f}(t) = \overline{g}(t)\overline{h}(t)$ in $\kappa(v)[t]$, where $\overline{g}$ and $\overline{h}$ are monic and coprime. Then there are monic $G, H \in R_v[t]$ with $f(t) = G(t)H(t)$ and $\overline{G}(t) = \overline{g}(t)$ and $\overline{H}(t) = \overline{h}(t)$.

Theorem 1.1.9: Approximation Theorem

Let $v_1, ..., v_n$ be inequivalent non-trivial absolute values on a field K. Then for $x_1, ..., x_n \in K$ and $\epsilon > 0$ there is $x \in K$ so

$$|x - x_k|_{v_k} < \epsilon$$

for $k = 1, ..., n$.

The next result classifies absolute values on finite extension L/K extending place v on K.

Proposition 1.1.10

Let L be a fintie extension of K and K is generated by a single element ξ. Let $f(t)$ be the monic minimal polynomial of ξ and $f(t) = f_1^{k_1}(t)...f_r^{k_r}(t)$ be the decomposition

into different irreducible monic factors $f_j(t) \in K_v[t]$. Then:

1. *for each $1 \leq j \leq r$ there is an injective morphism*

$$\iota : L \to K_j := K_v[t]/(f_j(t))$$

   of field extensions over K, given by $\xi \mapsto t$, so that K_j is the completion of L with respect to $|\cdot|_j$ and ι
2. *there is a unique extension $|\cdot|_j$ of K_v to K_j, and they are pairwise inequivalent*
3. *for any absolute value $|\cdot|_w$ extending $|\cdot|_v$ to L, there is unique $1 \leq j \leq r$ so $|\cdot|_j$ on K_j restrict to L is $|\cdot|_w$*

Corollary 1.1.10.1

If L is finite separable extension of K, then

$$\sum_{w|v} [L_w : K_v] = [L : K]$$

where w is sum over all palces w of L with $w \mid v$.

In particular, we call the number $[L_w : K_v]$ the local degree of L/K in w.

Corollary 1.1.10.2

Let L/K be finite Galois extension with $G = \mathrm{Gal}(L/K)$, and w_0, w two absolute values on L extending v on K. Then there is $\sigma \in G$ such that

$$|x|_w = |\sigma(x)|_{w_0}$$

for all $x \in L$. The completions L_w and L_{w_0} are isomorphic over K_v (but need not be isomorphic over L).

For K with non-trivial absolute value w, and L/K with $w \mid v$, we define

$$\|x\|_w = |N_{L_w/K_v}(x)|_v$$

for $x \in L$ and

$$|x|_w := |N_{L_w/K_v}(x)|_v^{1/[L:K]}$$

By Proposition 1.1.6 we know the restriction of $|N_{L_w/K_v}(x)|_v^{1/[L:K]}$ to L is a representative of w extending v. This absolute value is the normalization of v.

Lemma 1.1.11

Let $x \in K \backslash \{0\}$ and $y \in L \backslash \{0\}$. Then

$$\sum_{w|v} \log|x|_w = \log|x|_v$$

$$\sum_{w|v} \log \|y\|_w = \log |N_{L/K}(y)|_v$$

Proof. Corollary 1.1.10.1 gives the first statement. Now we prove the second. By primitive element, we know there is $\xi \in L$ so $L = K(\xi)$. With the notation of 1.1.10, we have $k_1 = \ldots = k_r = 1$ and an isomorphism

$$L \otimes_K K_v \xrightarrow{\sim} \prod_{j=1}^{r} K_v[t]/(f_j(t))$$

of K_v-algebra, given by $\xi \mapsto (t)_{j=1,\ldots,r}$. By Proposition 1.1.10 we get

$$N_{L/K}(y) = \prod_{w|v} N_{L_w/K_v}(y)$$

which concludes the second claim.

Next we talk about the product formula.

Let K be a field, M_K a set of non-trivial places such that the set

$$\{|\cdot|_v \in M_K : |x|_v \neq 1\}$$

is finite for any $x \in K\backslash\{0\}$. Then we say M_K satisfies the ***product formula*** if

$$\prod_{v \in M_K} |x|_v = 1$$

for all $x \in K\backslash\{0\}$.

Now suppose M_K satisfies product formula, and let M_L be the set of places on L defined by the normalizations, i.e. $M_L = \{|N_{L_w/K_v}(\cdot)|_v^{1/[L:K]} : v \in M_K, w \mid v\}$.

Proposition 1.1.12

The set of places M_L as above also satisfies product formula, if M_K does.

Now, for $\mathbb{Q}$ we define

$$M_{\mathbb{Q}} = \{|\cdot|_p : p \text{ a prime or } p = \infty\}$$

where we take the usual representatives, i.e. $|p|_p = 1/p$ for p a prime, or the usual absolute value when $p = \infty$. Then, for any number field K, we define M_K as the set of places and normalized absolute values, obtained by the above construction to the extension $K/\mathbb{Q}$. In other words, for any number field K, we always define

$$M_K = \{|N_{K_w/\mathbb{Q}_p}(\cdot)|_p^{1/[K:\mathbb{Q}]} : p \in M_{\mathbb{Q}}, w \mid p\}$$

Proposition 1.1.13

If K be a number field, then M_K (defined as above) satisfies the product formula.

The proof of this can be reduced to the fact every integer can be factored uniquely into product of prime numbers.

Convention

In this note, whenever we talk about M_K for a number field K, it will always be the the of places over $M_{\mathbb{Q}}$ defined as above. In particular, for $M_{\mathbb{Q}}$ we will always use the normalized absolute values, i.e. $|p|_p = 1/p$ for all primes and $|x|_\infty$ the usual absolute value. Specifically, M_K consists of places v so that $v \mid p$ and

$$|x|_v = |N_{K_v/\mathbb{Q}_p}(x)|_p^{1/[K:\mathbb{Q}]}$$

for $x \in K$.

By the product formula, we obtain a refinement of the approximation theorem for number fields.

Theorem 1.1.14

Let $(|\cdot|_v)_{v\in S}$ be representatives for a fintie set S of non-archimedean places of number field K, $x_v \in K_v$ for every $v \in S$, and let $\epsilon > 0$. Then there is $x \in K$ with $|x - x_v|_v < \epsilon$ for all $v \in S$ and $|x|_v \leq 1$ for all non-archimedean $v \notin S$.

We will spend the remaining of this section investigate M_K for number field K more closely.

Given number field K of degree n, we know M_K consists of places $v \mid \infty$, and $v \mid p$ for some prime number p.

First assume v extends ∞. In this case, observe K_v must be either $\mathbb{R}$ or $\mathbb{C}$, as $\mathbb{Q}_\infty = \mathbb{R}$. By field theory we konw there are n many embeddings $\sigma : K \hookrightarrow \mathbb{C}$, and we see each can define an absolute value by $|x|_\sigma := |\sigma(x)|_\infty$, where $|\cdot|_\infty$ is the usual absolute value on $\mathbb{R}$ or $\mathbb{C}$, depends on $\mathrm{im}(\sigma)$ lies in $\mathbb{C}$ or $\mathbb{R}$. In particular, we see if $\mathrm{im}(\sigma)$ is not real, then σ and the conjugate $\overline{\sigma}$ defines the same absolute value. On the other hand, if $\mathrm{im}(\sigma) \subseteq \mathbb{R}$ then it gives one place. Thus, we see if (r_1, r_2) is the signature of K (i.e. r_1 is the number of real embeddings and $2r_2$ the number of complex embeddings), then we have $r_1 + r_2$ many distinct places in M_K extending $\infty \in M_{\mathbb{Q}}$.

Next, let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$, the ring of integers of K. Then $\mathfrak{p}$ lies over some prime number p. Then, we can define a valuation on $\mathcal{O}_K$ via $\mathrm{ord}_\mathfrak{p}(x)$ be the exponent of $\mathfrak{p}$ in the factorization of the fractional ideal xR_k. This extends to a map $\mathrm{ord}_\mathfrak{p} : K^\times \to \mathbb{Z}$, and thus we obtain a place associated to $\mathfrak{p}$. The normalization here is given by

$$|x|_\mathfrak{p} = p^{-\mathrm{ord}_\mathfrak{p}(x)/e_\mathfrak{p}}$$

where $e_\mathfrak{p}$ is the ramification index of $\mathfrak{p}$ over $\mathbb{Q}$.

In particular, we can prove those are all the places in M_K, i.e. M_K consists of two parts, one obtained by just computing all embeddings $K \hookrightarrow \mathbb{C}$, and one obtained by computing all primes in $\mathcal{O}_K$ lying over p, as p range over all primes of $\mathbb{Z}$.

1.2 Heights In Projective and Affine Spaces

Let $\overline{\mathbb{Q}}$ be a choice of algebraic closure of $\mathbb{Q}$, and $\mathbb{P}^n = \mathbb{P}^n_{\overline{\mathbb{Q}}}$ the projective space with global coordinates $\mathbf{x} = (x_0 : x_1 : \ldots : x_n)$. Let $P \in \mathbb{P}^n$, we will now define a function, called height, on algebraic points of $\mathbb{P}^n_{\overline{\mathbb{Q}}}$. This should be thought as a measure of the algebraic complication needed to describe the point P.

Let $P \in \mathbb{P}^n$ be represented by homogeneous coordinate $(P_0 : \ldots : P_n)$, where $P_0, \ldots, P_n \in K$ for some number field K. Then we define

$$h(P) := \sum_{v \in M_K} \max_j \log |P_j|_v$$

Lemma 1.2.1

$h(P)$ is independent of the choice of K.

Proof. Let L be another number field containing the coordinates $P_0, \ldots, P_n$ of P. We can assume $K \subseteq L$. Then

$$\sum_{w \in M_L} \max_j \log |P_j|_w = \sum_{v \in M_K} \sum_{w|v} \max_j \log |P_j|_w$$

Now by Lemma 1.1.11 we see $\sum_{w|v} \log |x|_w = \log |x|_v$ for any $x \in K \backslash \{0\} \subseteq L \backslash \{0\}$, which concludes our proof.

Lemma 1.2.2

$h(P)$ is independent of the choice of coordinates.

Proof. Let Q be another coordinate representing the same point of $\mathbb{P}^n_{\overline{\mathbb{Q}}}$. By the above, we may assume $Q, P \in \mathbb{P}^n_K$ for number field K. Thus, there is $\lambda \in K \backslash \{0\}$ so $Q = \lambda P$. Thus

$$h(Q) = \sum_{v \in M_K} \log |\lambda|_v + \sum_{v \in M_K} \max_j \log |P_j|_v$$

where $\sum_{v \in M_K} \log |\lambda|_v = 0$ by product formula, and we are done.

Definition 1.2.3

We call $h(P)$ the ***absolute log height*** (briefly, ***height***) of P. We also define the multiplicative height $H(P) := e^{h(P)}$.

Example 1.2.4

Let α be an algebraic integer in a number field K of degree n.

We can identify α as the point $(\alpha : 1)$ in $\mathbb{P}^1_K$, and compute its height. In particular, we see

$$h(\alpha) = \sum_{v \in M_K} \log(\max(|\alpha|_v, 1))$$

Then note $\alpha\mathcal{O}_K$ factors as a bunch of prime ideals of $\mathcal{O}_K$ with all exponents, and thus almost all $|\alpha|_{\mathfrak{p}}$ should be less than 1, except one of them equal 1 (here we are using the fact α lies in $\mathcal{O}_K$). Hence, we see

$$h(\alpha) = \sum_{v|\infty} \log(\max(|\alpha|_v, 1))$$

For example, if we take $\alpha = i$, then we have two embeddings of $\mathbb{C} \hookrightarrow \mathbb{C}$, the trivial one and the conjugate. Hence

$$h(i) = \log(\max(|i|_\infty, 1)) + \log(\max(|-i|_\infty, 1)) = 0$$

Similarly, if we take $\sqrt{2}+1 \in \mathbb{Q}[\sqrt{2}]$, then we have two embeddings and so

$$\begin{aligned} h(\sqrt{2}+1) &= \log(\max(|1+\sqrt{2}|_\infty, 1)) + \log(\max(|1-\sqrt{2}|_\infty, 1)) \\ &= \frac{1}{2}\log(1+\sqrt{2}) \end{aligned}$$

More generally, if $\alpha \in K$ is an algebraic number, and write $\alpha\mathcal{O}_K = \mathfrak{b}/\mathfrak{c}$ for relative prime ideals of $\mathcal{O}_K$. Then

$$h(\alpha) = N(\mathfrak{b}) + \sum_{v|\infty} \log(\max(|\alpha|_v, 1))$$

where $N(\mathfrak{b})$ is the absolute norm of the ideal $\mathfrak{b}$.

As an very silly case of the above example, we see $h(a/b) = \log(\max(|a|, |b|))$ for rational number $a/b \in \mathbb{Q}$ with $\gcd(a, b) = 1$. In particular, this implies there are only finitely many points in $\mathbb{Q}$ so that $h(a/b) \leq B$ for a fixed B. It is not hard to convince oneself the same claim holds for points in $\mathbb{P}^n(\mathbb{Q})$.

Remark 1.2.5

Let $S \subseteq M_K$ be a finite set of places, which includes the set S_∞ of all archimedean places of K. Then we say $x \in K$ is an S-integer if $|x|_v \leq 1$ for all $v \notin S$. The

S-integers of K form a subring $\mathcal{O}_{S,K}$ of K. The units in $\mathcal{O}_{S,K}$ are called the S-units of K, and form a group $\mathcal{U}_{S,K}$. An element $x \in \mathcal{O}_{S,K}$ is S-unit if and only if $|x|_v = 1$ for all $v \notin S$.

In particular, we can show S_∞-integers is the same as an algebraic integer. Indeed, x is S_∞-integer, then $|x|_v \leq 1$ for all non-archimedean places, i.e. $x\mathcal{O}_K$ decomposes as a bunch of primes with only positive exponents, i.e. $x \in \mathcal{O}_K$.

Theorem 1.2.6: Kronecker

The height of $\xi \in \overline{\mathbb{Q}}^\times$ is zero if and only if ξ is a root of unity.

Proof. First, if ξ is a root of unity, then its absolute values are all equal to 1, and hence its height is 0. Thus it suffices to show the converse.

Suppose $h(\xi) = 0$, then we must have $|\xi|_v \leq 1$ for all $v \in M_K$. This implies ξ must be algebraic integer because $|\xi|_v \leq 1$ for all finite places indicates $\xi\mathcal{O}_K$ factors as positive product of primes in $\mathcal{O}_K$, i.e. $\xi \in \mathcal{O}_K$.

Now let d be the degree of ξ, and denote $\mathbf{x} := (\xi_1, ..., \xi_d)$ be a vector consists of all the conjugates of ξ. We write $\mathbf{x}^m$ to denote $(\xi_1^m, ..., \xi_d^m)$.

Now let s_i be the ith elementary symmetric polynomial with d variables. This gives

$$(x - \xi_1^m)...(x - \xi_d^m) = \sum_{i=0}^{d} (-1)^i s_i(\mathbf{x}^m) x^{d-i}$$

and in particular since $\xi \in \mathcal{O}_K$ we see $s_i(\mathbf{x}^m) \in \mathbb{Z}$.

Now, $|\xi_j|_v \leq 1$ for all j and v, and s_i consists of $\binom{d}{i}$ monomials, we see

$$\sum_{i=0}^{d} |s_i(\mathbf{x}^m)| \leq \sum_{i=0}^{d} \binom{d}{i} = 2^d$$

The above bound says that $\{(s_0(\mathbf{x}^m), ..., s_n(\mathbf{x}^m)) : m \geq 1\}$ must be a finite set, and hence by pigeonhole principle, there exists $m \neq n$, so $s_i(\mathbf{x}^m) = s_i(\mathbf{x}^n)$ for $i = 0, ..., d$. By defining property of elementary symmetric functions, we see this happens if and only if $\mathbf{x}^m = \sigma(\mathbf{x}^n)$ for some permutation σ on d letters. WLOG assume $m > n$. Repeat this argument $\mathrm{ord}(\sigma)$ many times, we may assume $\sigma = \mathrm{Id}$, and this gives $\xi^{m^{\mathrm{ord}(\sigma)}} = \xi^{n^{\mathrm{ord}(\sigma)}}$, showing ξ is a root of unity.

Detour

Consider $\phi : \mathcal{U}_{S,K} \to \mathbb{R}^{|S|}$ given by $x \mapsto (\log|x|_v)_{v \in S}$ in category of groups. By taking log of the product formula, we see $\mathrm{im}(\phi)$ is contained in the hyperplane $\sum_{v \in S} y_v = 0$. By Kronecker's theorem, the kernel of ϕ is the group μ_K of roots of unity in K. This is part of the Dirichlet's unit theorem.

Theorem 1.2.7

Let S be as above. The image of ϕ is a lattice of maximal rank $|S|-1$ in the hyperplane $\sum_{v\in S} y_v = 0$. Hence $U_{S,K} \cong \mu_K \times \mathbb{Z}^{|S|-1}$

Next, recall the Segre embedding $\mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^{(n+1)(m+1)-1}$, given coordinate wise by

$$(\mathbf{x}, \mathbf{y}) = ((x_0 : \ldots : x_n), (y_0 : \ldots : y_m)) \mapsto \mathbf{x} \otimes \mathbf{y} := (x_i y_j)$$

where the (ij) are ordered, e.g. lexicographically. This shows

$$h(\mathbf{x} \otimes \mathbf{y}) = h(\mathbf{x}) + h(\mathbf{y})$$

using $\max_{ij}|x_i y_j|_v = \max_i |x_i|_v \cdot \max_j |y_j|_v$.

For local computations, its often convenient to introduce the following function $\log^+(x) := \max(0, \log(x))$. In particular, we see for any point $P \in \mathbb{A}^n$, which identified as $(1, P_1, \ldots, P_n) \in \mathbb{P}^n$, we have

$$h(P) = h(1 : P_1 : \ldots : P_n) = \sum_{v \in M_K} \max_j \log^+ |x_j|_v$$

Proposition 1.2.8

Let $P^1, \ldots, P^r$ be points of $\mathbb{A}^n$, then

$$h(P^1 + \ldots + P^r) \leq h(P^1) + \ldots + h(P^r) + \log r$$

Proof. WLOG we may assume $P^i \in \mathbb{A}^n_K$ for some number field K. Then

$$h(P^1 + \ldots + P^r) = \sum_{v \in M_K} \max_j \log^+ |P^1_j + \ldots + P^r_j|_v$$

If v is non-archimedean, then

$$|P^1_j + \ldots + P^r_j|_v \leq \max_k |P^k_j|_v$$

If v is archimedean, by triangle inequality we see

$$|P^1_j + \ldots + P^r_j|_v \leq |r|_v \cdot \max_k |P^k_j|_v$$

but then $\sum_{v|\infty} \log|r|_v = \log r$. Thus we see

$$h(P^1 + \ldots + P^r) \leq \log r + \sum_{v \in M_K} \max_{j,k} \log^+ |P^k_j|_v \leq \log r + \sum_k \max_j \log^+ |P^k_j|_v$$

The following result says the height is invariant under Galois action.

Proposition 1.2.9

Let $P \in \mathbb{P}^n_{\overline{\mathbb{Q}}}$ and $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, then $h(P) = h(\sigma(P))$.

This result follows from the observation that σ induces a permutation on M_K.

Lemma 1.2.10

If $\alpha \in K\backslash\{0\}$ and $\lambda \in \mathbb{Q}$, then $h(\alpha^\lambda) = |\lambda| \cdot h(\alpha)$. In particular, $h(1/\alpha) = h(\alpha)$.

This result follows from the observation that $\log|\alpha|_v = \log^+|\alpha|_v - \log^+|1/\alpha|_v$, and now sum over all the places, we get $0 = h(\alpha) - h(1/\alpha)$.

Let $S \subseteq M_K$ be a finite set of places. For $\alpha \in K\backslash\{0\}$, we have

$$\sum_{v \in S} \log|\alpha|_v \leq h(\alpha)$$

If we use $1/\alpha$ instead of α, then the above lemma shows

$$\sum_{v \in S} \log|\alpha|_v \geq -h(\alpha)$$

This concludes the so-called fundamental inequality

$$-h(\alpha) \leq \sum_{v \in S} \log|\alpha|_v \leq h(\alpha) \qquad \text{(Eq. 1.2.1)}$$

The next theorem is a very important result, namely:

Theorem 1.2.11: Northcott's Theorem

There are only finitely many algebraic numbers of bounded degree and bounded height.

Proof. To make the statement above more precise, we will show the following. For any $B, D \geq 0$, the set

$$\{P \in \mathbb{P}^n_{\overline{\mathbb{Q}}} : H(P) \leq B \text{ and } [\mathbb{Q}(P) : \mathbb{Q}] \leq D\}$$

is finite. In particular, for any fixed number field K, $\{P \in \mathbb{P}^n_k : H(P) \leq B\}$ is finite. In the above, $\mathbb{Q}(P)$ is the minimal number field containing all coordinates of P.

Now let $P = (P_0 : \ldots : P_n)$ where we assume some $P_i = 1$. Then for any absolute value v and index i we have

$$\max(\|P_0\|_v, \ldots, \|P_n\|_v) \geq \max(\|P_i\|_v, 1)$$

Hence, we see

$$H(P) \geq H(P_i)$$

for all $0 \leq i \leq n$. Further, its clear $\mathbb{Q}(P) \supseteq \mathbb{Q}(P_i)$, hence it suffices to prove for each $1 \leq d \leq D$, the set

$$\{x \in \overline{\mathbb{Q}} : H(x) \leq B \text{ and } [\mathbb{Q}(x) : \mathbb{Q}] = d\}$$

is finite.

Let $\xi \in \overline{\mathbb{Q}}$ have degree d and $k = \mathbb{Q}(x)$. We write $\mathbf{x} := (\xi_1, ..., \xi_d)$ for the conjugates of ξ over $\mathbb{Q}$, and we let

$$F_\xi(x) = \prod_{j=1}^{d}(x - x_j) = \sum_{r=0}^{d}(-1)^r s_r(\mathbf{x}) x^{d-r}$$

the minimal polynomial of x over $\mathbb{Q}$. However, we see

$$\begin{aligned} |s_r(\mathbf{x})|_v &= \left| \sum_{1 \leq i_1 < ... < i_r \leq d} \xi_{i_1} ... \xi_{i_r} \right|_v \\ &\leq c(v, r, d) \max_{1 \leq i_1 < ... < i_r \leq d} |\xi_{i_1} ... \xi_{i_r}|_v \\ &\leq c(v, r, d) \max_{1 \leq i \leq d} |\xi_i|_v^r \end{aligned}$$

where $c(v, r, d) = \binom{d}{r} \leq 2^d$ if v is archimedean, and 1 if v is non-archimedean.

Thus we see

$$\max(|s_0(\mathbf{x})|_v, ..., |s_d(\mathbf{x})|_v) \leq c(v, d) \prod_{i=1}^{d} \max(|\xi_i|_v, 1)^d$$

where $c(v, d) = 2^d$ if v is archimedean and 1 otherwise.

Now multiply this inequality over all $v \in M_K$, where $K = \mathbb{Q}(x)$, and take $[K : \mathbb{Q}]$th root, we see

$$H(s_0(\mathbf{x}), ..., s_d(\mathbf{x})) \leq 2^d \prod_{i=1}^{d} H(x_i)^d$$

But the x_i's are conjugates, and we know heights are invariant under Galois action, thus $H(x_i)$'s are all equal. This shows

$$H(s_0(\mathbf{x}), ..., s_d(\mathbf{x})) \leq 2^d H(x)^{d^2}$$

Now suppose x is in the set

$$\{x \in \overline{\mathbb{Q}} | H(x) \leq B \text{ and } [\mathbb{Q}(x) : \mathbb{Q}] = d\}$$

Then we just proven x is the root of a polynomial $F_x(T)$ whose coefficients $s_0, ..., s_d$ are bounded by $2^d B^{d^2}$. However, it is easy to see $\mathbb{P}^d(\mathbb{Q})$ has only finitely many points of bounded height, so there are only finitely many possibilities for $F_x(T)$, and we are done.

Chapter 2

Weil Heights

In this chapter, we will look at heights from a geometric point of view. In particular, we will define local Weil heights associated to a Cartier divisor on projective X, and studying their properties. Then we move to the global case, and we will prove Northcott's property in this case.

2.1 Review: Cartier Divisors

One of the main goal of introduce divisors is to ask, given zero and pole configuration on an open cover, whether these configurations are induced from global rational functions.

There are two ways to do this, one is explicitly keep track of where they have pole and zero, on codimension 1 pieces. This gives Weil divisor, i.e. a Weil divisor is a formal linear combination of $\sum_{i=1}^{n} n_i Y_i$ where Y_i are irreducible closed subschemes of codimension 1. The other definition is Cartier divisors, which roughly says a configuration is an equivalence class of rational functions where $f \sim g$ iff $f = ug$ for some $u \in \Gamma(U, \mathscr{O}_X)^\times$. The later is less geometric, but it defines on wider range of schemes.

For us we will just work with integral schemes (otherwise the discussion will be longer than I want).

Say X is integral, the function field $K(X)$ is well-defined. Denote $\mathscr{K}_X$ the constant sheaf with value $K(X)$. Then a Cartier divisor D on X is a tuple (U_i, f_i) where U_i form an open cover of X and where $f_i \in K(X)^\times$ are elements with $f_i f_j^{-1} \in \Gamma(U_i \cap U_j, \mathscr{O}_X^\times)$ for all i, j. We denote this set by $\mathrm{Div}(X)$, and it forms an abelian group with the obvious addition (i.e. $(U_i, f_i) + (V_i, g_i) = (U_i \cap V_i, f_i g_i)$).

A Cartier divisor is principal if it is equal (X, f), and two divisors D, E are equivalent (and write $D \equiv E$) if $D - E$ is principal. This gives an equivalence relation and hence we get $\mathrm{CDiv}(X) := \mathrm{Div}(X)/\equiv$, i.e. we have exact sequence

$$1 \to \Gamma(X, \mathscr{O}_X)^\times \to K(X)^\times \to \mathrm{Div}(X) \to \mathrm{CDiv}(X) \to 0$$

Next, we say a divisor (U_i, f_i) is effective if f_i lies in $\mathscr{O}_X$ instead, i.e. they are not

rational, but regular.

Given a Cartier divisor $D = (U_i, f_i)$ we can define associated line bundle $\mathscr{O}_X(D)$ defined by

$$\Gamma(V, \mathscr{O}_X(D)) := \{f \in K(X) : f_i f \in \Gamma(U_i \cap V, \mathscr{O}_X) \text{ for all } i\}$$

for V open in X. Now take open cover U_i in the definition of D, then we see $\mathscr{O}_X(D)$ is locally of a free $\mathscr{O}_X$-module of rank 1. Explicitly, over U_i, $\mathscr{O}_X(D)$ is isomorphic to the rank 1 submodule of $\mathscr{K}_X$ generated by f_i^{-1}, i.e. it is a line bundle. In particular, this map is an isomorphism of abelian groups.

For a Cartier divisor D, we define

$$\operatorname{supp}(D) = \{x \in X : (f_i)_x \notin \mathscr{O}_{X,x}^\times \text{ for some } i \text{ with } x \in U_i\}$$

Now for a more geometric view, assume X is in addition Noetherian. For $C \subseteq X$ closed irreducible, we see $C = \overline{\{\xi\}}$ for generic point ξ, and in particular recall

$$\operatorname{codim}_X(C) = \dim \mathscr{O}_{X,\xi}$$

Now define $Z^1(X)$ be the free abelian group generated by all codimension 1 closed irreducible subsets of X, and we call an element of that a Weil divisor.

Then, we can define $\operatorname{cyc} : \operatorname{Div}(X) \to Z^1(X)$ as follows.

For $f \in \Gamma(U, \mathscr{K}_X)$, we need to define the order $\operatorname{ord}_C(f)$ along prime Weil divisor C (meaning C is a codimension 1 closed irreducible subset). If $\mathscr{O}_{X,\xi}$ is DVR, where ξ is the generic point of C, then f_C is a non-zero element in $\operatorname{Frac}(\mathscr{O}_{X,\xi})$, and thus we just set $\operatorname{ord}_C(f) = v_C(f_C)$, where $v_C(f)$ is the normalized discrete valuation of $f \in K$ given by $\mathscr{O}_{X,\xi}$.

Now for Cartier divisor $D \in \operatorname{Div}(X)$, say represented by (U_i, f_i), and prime Weil divisor C, we define $\operatorname{ord}_C(D)$ as follows. Choose i so that the generic point ξ_C of C is contained in U_i. Let $f \in \operatorname{Frac}(\mathscr{O}_{X,\xi_C})$ be the germ of f_i at η_C, then f does not depend on the choice of presentation (U_i, f_i) or on i up to a unit of $\mathscr{O}_{X,\xi_C}$. Thus

$$\operatorname{ord}_C(D) := \operatorname{ord}_{\mathscr{O}_{X,\xi_C}}(f)$$

depends only on D and C.

This particular quantity is called the order of vanishing of D at C.

Then, we simply define

$$\operatorname{cyc}(D) := \sum_C \operatorname{ord}_C(D)[C]$$

as we sum over all prime Weil divisors C. Now, for $f \in \Gamma(X, \mathscr{K}_X)^\times$ an invertible rational function, we define $\div(f) := \sum_C \operatorname{ord}_C(f)C$, and we define

$$\operatorname{Cl}(X) := Z^1(X)/\left\langle \div(f) : f \in \Gamma(X, \mathscr{K}_X)^\times \right\rangle$$

$\operatorname{ord}_C(f) = \operatorname{ord}_C(\div(f))$ and we simply write $\operatorname{cyc}(f)$ to mean $\operatorname{cyc}(\div(f))$.

and we have the following result:

Theorem 2.1.1

Let X be Noetherian scheme.

1. *If X is normal, then* cyc *is injective, and thus we have injection* $\mathrm{CDiv}(X) \hookrightarrow \mathrm{Cl}(X)$
2. *If X is locally factorial, then* cyc *is bijective, and we have isomorphism* $\mathrm{CDiv}(X) \cong \mathrm{Cl}(X)$

Notation/Convention

So, for X nice enough,

$$\text{line bundles+a rational section} = \text{Cartier divisors} = \text{sheaf of sections}$$

For a line bundle L and a section $s : X \to L$, we can define its associated Cartier divisor by $D(s) := (U_i, \phi_i \circ s)$ where U_i is a choice of trivialization (U_i, ϕ_i) of L. On the other hand, given Cartier divisor $D = (U_i, f_i)$, we see $g_{ij} = f_i/f_j$ is a unit in $\mathscr{O}_X(U_i \cap U_j)$. Let $\mathscr{O}(D)$ be the line bundle on X given by transition functions g_{ij}, i.e. we glue trivial bundles $U_i \times \mathbb{A}^1$ along the isomorphisms given by g_{ij}. This gives a trivialization of $\mathscr{O}(D)$ over U_i, and we consider f_i as rational/meromorphic sections of $U_i \times \mathbb{A}^1$, then $f_i = g_{ij} f_j$, i.e. we obtain a section s_D of $\mathscr{O}(D)$ and we see $D \mapsto (\mathscr{O}(D), s_D)$ is the inverse of the above map.

Example 2.1.2

Let $X = \operatorname{Spec} \mathcal{O}_K$, where K is a number field and $\mathcal{O}_X$ its ring of integers. Then $\mathrm{Cl}(X) = \mathrm{Pic}(X)$ is in fact just the divisor class group studied in algebraic number theory. In particular, the exact sequence

$$1 \to \Gamma(X, \mathscr{O}_X)^\times \to K(X)^\times \to \mathrm{Div}(X) \to \mathrm{CDiv}(X) \to 0$$

becomes

$$1 \to \mathcal{O}_K^\times \to K^\times \to \mathrm{Div}(\mathcal{O}_K) \to \mathrm{Pic}(\mathcal{O}_K) \to 1$$

Now by basic result from number theory, we see $\mathrm{Pic}(\mathcal{O}_K)$ is a finite group and $\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{r+s-1}$, where (r, s) is the signature of K and $\mu(K)$ the roots of unity in K.

2.2 Local Heights

From now on, we will assume X is projective variety.

In this case, if we want to define a reasonable notion of height on X, the most basic definition would be embed X into $\mathbb{P}^N$, then apply the height for projective space. However, this is bad because we have more than one way to embed. Thus, in order to get a sensible notion of heights, we must also keep track of how we embed X into $\mathbb{P}^n$, i.e. we need to define heights relative to divisors and the sections on them.

To define local Weil heights, we need information beyond the divisor D itself. Namely, we need a realization $\mathscr{O}(D) = \mathscr{O}(D_+) \otimes \mathscr{O}(-D_-)$, where $\mathscr{O}(D_\pm)$ are base-point-free line bundles coming with given set of generating global sections. The set of Cartier divisors with these additional data forms a monoid, and the local heights so defined will behave functorially with respect to this structure. This removes the need of working modulo bounded functions when studying Weil heights, a point of crucial importance for applications as it allows precise estimates.

Convention

Throughout this section, we will let K be a field and $|\cdot|$ a fixed absolute value on $\overline{K}$.

Let X be a projective variety over K, which for simplicity we assume its irreducible. Let $D = (U_i, f_i)$ be a Cartier divisor on X with associated line bundle $\mathscr{O}(D)$ and meromorphic section s_D, where s_D is obtained using f_i. Then there are base-point free line bundles $\mathscr{L}, \mathscr{M}$ on X such that $\mathscr{O}(D) = \mathscr{L} \otimes \mathscr{M}^{-1}$. Now choose generating global sections $\mathbf{s} = (s_0, ..., s_n)$ of L and $\mathbf{t} = (t_0, ..., t_m)$ of M, we call the data $\mathcal{D} = (s_D, L, \mathbf{s}, M, \mathbf{t})$ a presentation of D.

Remark 2.2.1

To see why every line bundle $\mathscr{D}$ can be written as $\mathscr{L}\mathscr{M}^{-1}$, we work with divisors. Let D be a Cartier divisor, then let H be a very ample divisor on X (such divisor exists as X is projective), and we set $D_1 = mH + D$ and $D_2 = mH$. For m large enough, D_1, D_2 will be ample, while $D_1 - D_2$ clearly equal D.

Definition 2.2.2

For $P \notin \mathrm{supp}(D)$, we define the ***local height*** (with respect/relative to $\mathcal{D}$) to be

$$\lambda_{\mathcal{D}}(P) := \max_k \min_l \log \left| \frac{s_k}{t_l s_D}(P) \right|$$

In the above, we use the notation $t_l s_D$ for $t_l \otimes s_D$ and s_k/s' for $s_k \otimes (s')^{-1}$, i.e. $s_l/(t_l s_D)$ is a rational function on X. In addition, if D is a Cartier divisor with a presentation $\mathcal{D}$, then we also (by abuse of notation) write $\lambda_D(P)$ and say local height with respect/relative to D.

This local height depends on the choice of s_D, L, M as well as their generating sections.

Example 2.2.3

Let f be non-zero rational function on X with Cartier divisor $D = D(f)$. Then $\mathscr{O}(D) = \mathscr{O}_X$ and f is a meromorphic section of $\mathscr{O}(D)$. Thus there is a local height λ_f relative to D, given by the presentation $(f, \mathscr{O}_X, 1, \mathscr{O}_X, 1)$. For $P \notin \mathrm{supp}(D)$, we have

$$\lambda_f(P) = -\log|f(P)|$$

If g is another non-zero rational function on X, then $\lambda_{fg} = \lambda_f + \lambda_g$ and $\lambda_{f^{-1}} = -\lambda_f$.

Let D_1 and D_2 be Cartier divisors with presentations $\mathcal{D}_i = (s_{D_i}, \mathscr{L}_i, \mathbf{s}_i, \mathscr{M}_i, \mathbf{t}_i)$ nad local heights λ_{D_i}. Then $\mathbf{s}_1\mathbf{s}_2 = (s_{1k}s_{2k'})$ and $\mathbf{t}_1\mathbf{t}_2 = (t_{1l}t_{2l'})$ are generating sections of $\mathscr{L}_1 \otimes \mathscr{L}_2$ and $\mathscr{L}_2 \otimes \mathscr{M}_2$ respectively. Thus we can define $\lambda_{\mathcal{D}_1+\mathcal{D}_2}$ as the local height relative to the presentation

$$\mathcal{D}_1 + \mathcal{D}_2 = (s_{D_1}s_{D_2}, \mathscr{L}_1 \otimes \mathscr{L}_2, \mathbf{s}_1\mathbf{s}_2, \mathscr{M}_1 \otimes \mathscr{M}_2, \mathbf{t}_1\mathbf{t}_2)$$

By definition we see

$$\lambda_{D_1+D_2}(P) = \lambda_{D_1}(P) + \lambda_{D_2}(P)$$

for $P \notin \operatorname{supp}(D_1) \cup \operatorname{supp}(D_2)$. Thus, we see the space of local heights admits an addition operation. Next, for λ_D with presentation $(s_D, \mathscr{L}, \mathbf{s}, \mathscr{M}, \mathbf{t})$, we can define λ_{-D} by $(s_D^{-1}, \mathscr{M}, \mathbf{t}, \mathscr{L}, \mathbf{s})$. This makes the space of local heights an monoid.

Next, let $\mathcal{D} = (s_D, \mathscr{L}, \mathbf{s}, \mathscr{M}, \mathbf{t})$ be a presentation of D, then for $\pi : Y \to X$ a dominant morphism of irreducible projective varieties over K, we can pullback the presentation to get $\pi^*\mathcal{D} := (\pi^*s_D, \pi^*\mathscr{L}, \pi^*\mathbf{s}, \pi^*\mathscr{M}, \pi^*\mathbf{t})$. In particular, $\lambda_{\pi^*\mathcal{D}}(P) = \lambda_{\mathcal{D}}(\pi(P))$ for well-defined P, i.e. we require $P \in Y$, $\pi(P) \notin \operatorname{supp}(D)$.

Our next goal is compare how the presentation would affect our local height, and the conclusion is that it affects the computation by a constant.

Definition 2.2.4

Let U be a closed variety of $\mathbb{A}^n$. A set $E \subseteq U(\overline{K})$ is ***bounded*** in U if for any $f \in K[U] = K[t_1, ..., t_n]/I(U)$, the function $|f|$ is bounded on E.

Lemma 2.2.5

Let $\{f_1, ..., f_N\}$ be a generators of $K[U]$, the set of regular functions on affine closed U. If

$$\sup_{P\in E} \max_{j=1,...,N} |f_j(P)| < \infty$$

then E is bounded.

Proof. Let $f \in K[U]$, then we can write $f = p(f_1, ..., f_N)$ with p a polynomial in $K[U]$. Let C be the number of monomials in p and d the degree of p. Define

$$\delta = \begin{cases} 1 & \text{if the absolute value is archimedean} \\ 0 & \text{otherwise} \end{cases}$$

Then, for a place v define

$$|p|_v = \max_{\mathbf{j}} |a_{\mathbf{j}}|_v$$

where the max is taken over all coefficients of p. Then we see

$$\sup_{P\in E} |f(P)| \leq C^{\delta}|p| \cdot \max\left(1, \sup_{P\in E} \max_{j=1,..,N} |f_j(P)|\right)^d < \infty$$

Lemma 2.2.6

If $\{U_i\}$ be a finite affine open cover of affine K-variety U and E bounded in U. Then there are bounded subsets E_i of U_i such that $E = \bigcup_i E_i$.

Proof. It suffices to prove this claim after passing to a refinement of U_i. Thus we might assume there are regular functions h_i on U so $U_i = \{x \in U : h_i \neq 0\}$. By partition of unity, we see there are regular functions g_i so $\sum_i g_i h_i = 1$. If C is the cardinality of the cover and δ is defined as in the proof of Lemma 2.2.5. Then we see

$$\inf_{P\in E} \max_i |h_i(P)| \geq C^{-\delta} \left(\sup_{P\in E} \max_i |g_i(P)| \right)^{-1} > 0 \tag{Eq. 2.2.1}$$

We define

$$E_i = \{P \in E : |h_i(P)| = \max_k |h_k(P)|\}$$

Obviously, $E_i \subseteq U_i(\overline{K})$ and $E = \bigcup E_i$. Let $f_i, ..., f_N$ be a set of generators of $K[U]$, then $f_1, ..., f_N, 1/h_i$ generates $K[U_i]$. By Lemma 2.2.5, its enough to show $|1/h_i|$ is bounded on E_i. In fact, the bound

$$\sup_{P\in E_i} |1/h_i(P)| \leq C^{\delta} \sup_{P\in E} \max_k |g_k(P)| < \infty$$

follows from Eq. 2.2.1.

Theorem 2.2.7

Let X be a projective variety over K and $\mathcal{D}, \mathcal{D}'$ be two presentations of Cartier divisor D. Then

$$|\lambda_{\mathcal{D}} - \lambda_{\mathcal{D}'}| \leq \gamma$$

for some constant $\gamma < \infty$.

Proof. Note $\lambda_{\mathcal{D}} - \lambda_{\mathcal{D}'} = \lambda_{\mathcal{D}-\mathcal{D}'}$. This means $\lambda_{\mathcal{D}} - \lambda_{\mathcal{D}'}$ is a local height with respect to $D - D$. Thus, it suffices to prove the claim for D and assume one of the presentation, say $\mathcal{D}'$, is equal $(1, \mathcal{L}, 1, \mathcal{M}, 1)$. Then, $\mathcal{D}$ has the form $(1, \mathscr{L}, \mathbf{s}, \mathscr{M}, \mathbf{t})$. We need to find γ so that

$$-\gamma \leq \max_k \min_l \log \left| \frac{s_k}{t_l}(P) \right| \leq \gamma$$

To that end, it suffices to only prove

$$\max_k \min_l \log |s_k / t_l(P)| \leq \gamma$$

as we can interchange the role of $\mathbf{s}$ and $\mathbf{t}$.

Now choose closed embedding X into $\mathbb{P}^N_K$ with coordinates $(x_0 : ... : x_N)$, and $U_i := \{x \in X : x_i \neq 0\}$ be affine open, and U_{il} be the affine open $\{x \in U_i : t_l(x) \neq 0\}$.

The restriction of $g_{kl} := s_k/t_l$ to U_{il} are regular functions. The functions $f_{ij} = x_j/x_i$, for $j = 0, \ldots, N$, generate $K[U_i]$. Then define sets E_i by

$$E_i = \{P \in X(\overline{K}) : |x_i(P)| = \max_j |x_j(P)|\}$$

Its clear that if $P \in E_i$ we have

$$\max_j |f_{ij}(P)| = 1$$

hence E_i is bounded in U_i by Lemma 2.2.5. Thus we can apply Lemma 2.2.6 to U_i, E_i and the covering $\{U_{il}\}$, obtaining bounded subsets E_{il} of U_{il} such that $E_i = \bigcup_l E_{il}$ and

$$\sup_{P \in E_{il}} \max_k |g_{kl}(P)| < \infty$$

Since E_{il} covers $X(\overline{K})$, we are done.

2.3 Global Heights

In the previous section, we defined the local height with respect to a Cartier divisor D, for a fixed field K and fixed absolute value on $\overline{K}$. Now we will consider summing those local heights together to get the global one.

Convention

Throughout this section, we will let K be a number field.

Now let X be irreducible projective variety over K with Cartier divisor D and presentation $(s_D, \mathscr{L}, \mathbf{s}, \mathscr{M}, \mathbf{t})$. Let F/K an algebraic extension. Then for $P \in X(F) \backslash \mathrm{supp}(D)$ we define the local height

$$\lambda_{\mathcal{D}}(P, v) := \max_k \min_l \log \left| \frac{s_k}{t_l s_D}(P) \right|_v$$

for $v \in M_F$ normalized.

Now let p be the place lying below v, and u an absolute value on $\overline{K}$ extends v, then we see

$$\lambda_{\mathcal{D}}(P, v) = \frac{[F_v : \mathbb{Q}_p]}{[F : \mathbb{Q}]} \lambda_{\mathcal{D}}(P, u)$$

Now note $\overline{u}$ is an absolute value on the algebraic closure $\overline{K}$, and hence $\lambda_{\mathcal{D}}(P, u)$ reduces to the case we studied above for local heights. Thus, we see by the above computation, we can apply results from above to $\lambda_{\mathcal{D}}(P, v)$ as well, since this quantity is related to $\lambda_{\mathcal{D}}(P, u)$ by a constant.

Example 2.3.1

Consider the Cartier divisor $\{x_0 = 0\}$ in $\mathbb{P}^n_K$, with presentation

$$\mathcal{D} = (x_0, \mathscr{O}(1), \{x_0, ..., x_n\}, \mathscr{O}, 1)$$

For $P \in \mathbb{P}^n(F)$ with $x_0(P) \neq 0$ and $v \in M_F$, the corresponding local height is

$$\lambda_{\mathcal{D}}(P, v) = \max_k \log|\frac{x_k}{x_0}(P)|_v$$

and the product formula becomes

$$h(P) = \sum_{v \in M_F} \lambda_{\mathcal{D}}(P, v)$$

where $h(P)$ is the naive height we defined before.

Let $\lambda_{\mathcal{D}}$ be a local height relative to the presentation $\mathcal{D} = (s_D, \mathscr{L}, \mathbf{s}, \mathscr{M}, \mathbf{t})$ of a Cartier divisor D on X. For $P \in X$ there are s_j and t_l such that $s_j(P) \neq 0$ and $t_l(P) \neq 0$. Thus, we can find non-zero meromorphic section s of $\mathscr{O}(D)$ such that P is not contained in the support of the Cartier divisor $D(s)$. Then $\mathcal{D}(s) = (s, \mathscr{L}, \mathbf{s}, \mathscr{M}, \mathbf{t})$ is a presentation of $D(s)$ and we have

$$\lambda_{\mathcal{D}(s)} = \lambda_{\mathcal{D}} + \lambda_f$$

where f is the rational section s/s_D.

If F is a finite extension $K \subseteq F \subseteq \overline{K}$ such that $P \in X(F)$, the local height $\lambda_{\mathcal{D}(s)}(P, v)$ is finite for any $v \in M_F$ because P is not in the support of $D(s)$.

Definition 2.3.2

In the situation above, we define the ***global height*** of P relative to $\lambda = \lambda_{\mathcal{D}}$ by

$$h_\lambda(P) := \sum_{v \in M_F} \lambda_{\mathcal{D}(s)}(P, v)$$

The following result justifies the definition.

Proposition 2.3.3

The global height h_λ is independent of the choice of F and of the section s.

Proof. By Lemma 1.1.11, the global height is independent of F.Its independence from the choice of s can be verified as follows. Let t be another non-zero meromorphic section of $\mathscr{O}(D)$ with $P \notin \mathrm{supp}(D(t))$. Then by previous sections we see

$$\lambda_{\mathcal{D}(s)}(P, v) - \lambda_{\mathcal{D}(t)}(P, v) = \lambda_{s/t}(P, v)$$

for any $v \in M_F$. On the other hand, the product formula shows the global height of P relative to $\lambda_{s/t}$ is 0, hence we are done.

As an immediate consequence, the global height relative to the natural local height of a non-zero rational function is identically 0. Its also clear the map $\lambda \mapsto h_\lambda$ is a group homomorphism.

Theorem 2.3.4

Let λ, λ' be local heights relative to Cartier divisor D, D' with $D - D'$ a principal divisor. Then $h_\lambda - h_{\lambda'}$ is a bounded function.

Proof. Since $D - D'$ is a principal divisor, it suffices to prove our theorem for $D = D' = 0$ and $\lambda' = 0$. Hence we need only to show h_λ is a bounded function for any local height relative to the zero divisor. By Theorem 2.2.7 we can find a family $\{\gamma_v\}_{v \in M_K}$ of non-negative real numbers, almost all 0, so

$$|\lambda(P, u)|_u \leq \gamma_v$$

for any $P \in X$ and any place u on $\overline{K}$ with $u \mid v$. As before, let F be a finite extension $K \subseteq F \subsetneq \overline{K}$ so $P \in X(F)$. Then we see

$$|\lambda(P, w)| \leq \frac{[F_w : \mathbb{Q}_p]}{[F : \mathbb{Q}]} \gamma_v$$

for any $w \in M_F$, which divides $v \in M_K$ and $p \in M_{\mathbb{Q}}$. By Corollary 1.1.10.1, we have

$$\sum_{w \mid v} [F_w : K_v] = [F : K]$$

and thus

$$|h_\lambda(P)| \leq \sum_{w \in M_F} |\lambda(P, w)| \leq \sum_{v \in M_K} \frac{[K_v : \mathbb{Q}_p]}{[K : \mathbb{Q}]} \gamma_v < \infty$$

Now let $\mathscr{L}$ be a line bundle, then we see it correspond to some Cartier divisor D, and hence we get a local height λ relative to D, i.e. we get a function $X \to \mathbb{R}$. If we choose two different Cartier divisors associated to the same line bundle, then by the above $h_\lambda - h_{\lambda'}$ differ by a bounded function. Thus a line bundle $\mathscr{L}$ determines an unique element in $\mathbb{R}^X / \mathcal{O}(1)$, the space of real functions from X to $\mathbb{R}$ mod the set of bounded functions.

This construction of global height, although it is functorial (Theorem 2.3.5 below), but we lose the finer control for estimations needed to prove deeper results in Diophantine geometry. On the other hand, Weil heights, which we will define later, does give us the refined control over things.

Theorem 2.3.5

The map

$$h : \mathrm{Pic}(X) \to \mathbb{R}^X / \mathcal{O}(1)$$

described above is a homomorphism. If $\phi : Y \to X$ is a morphism of irreducible projective varieties over K, then

$$h_{\phi^* \mathscr{L}} = h_{\mathscr{L}} \circ \phi$$

for any $\mathscr{L} \in \mathrm{Pic}(X)$.

This claim follows from Theorem 2.3.4 and definition of pullback.

Next, we observe that a base-point-free line bundle has always a non-negative height function. The following is a generalization.

Proposition 2.3.6

Let D be an effective Cartier divisor on X. Then there is a local height λ relative to D such that, for $P \notin \mathrm{supp}(D)$ and for any place u of $\overline{K}$, it holds $\lambda(P, u) \geq 0$.

Proof. There are base-point free line bundles $\mathscr{L}, \mathscr{M}$ on X so $\mathscr{O}(D) \cong \mathscr{L} \otimes \mathscr{M}^{-1}$. Choose generating global sections $t_0, \ldots, t_l$ of $\mathscr{M}$, we can complete $s_D t_0, \ldots, s_D t_l$ to a family $\mathbf{s} := (s_0, \ldots, s_k)$ of generating global sections of $\mathscr{L}$. The local height given by presentation

$$\mathcal{D} = (s_D . \mathscr{L}, \mathbf{s}, \mathscr{M}, \mathbf{t})$$

is non-negative outside the support of D.

Remark 2.3.7

1. Our results in this section and last section extends to non-irreducible varieties.
2. Global heights can be defined over any field with product formula as long as we work with properly normalized absolute values.
3. We may replace K by $\overline{K}$, as we are just working with varieties and properties are geometric.

2.4 Weil Heights

In this section we consider global heights given by a morphism $X \to \mathbb{P}^n$. In fact, we will see that any global height is the difference of two Weil heights.

Let X be projective over $\overline{\mathbb{Q}}$.

Definition 2.4.1

Let $\phi : X \to \mathbb{P}^n_{\overline{\mathbb{Q}}}$ be a morphism over $\overline{\mathbb{Q}}$. The ***Weil height*** of $P \in X(\overline{\mathbb{Q}})$ relative to ϕ is defined by $h_\phi(P) = h \circ \phi(P)$, with h the usual height on $\mathbb{P}^n_{\overline{\mathbb{Q}}}$.

Construction: Join

Let $\phi : X \to \mathbb{P}^n_{\overline{\mathbb{Q}}}$ and $\psi : X \to \mathbb{P}^m_{\overline{\mathbb{Q}}}$, then we define the join $\phi \# \psi$ as the morphism

$$s_{n,m} \circ (\phi \times \mathrm{Id}) \circ G(\psi)$$

where $s_{n,m}$ is the Segre embedding, $\phi \times \mathrm{Id}$ fiber product, $G(\psi)$ the graph of ψ. More explicitly, $\phi \# \psi$ is the morphism

$$X \to \mathbb{P}^{(n+1)(m+1)-1}_{\overline{\mathbb{Q}}}, \quad x \mapsto (\phi_i(x)\psi_j(x))$$

where the index (i, j) are ordered lexicographically.

If ϕ is closed embedding, then $\phi \# \psi$ is closed embedding. Indeed, $G(\psi)$ is always closed embedding as we are working with separated schemes (separated=closed diagonal=closed graph=closed equalizer). The Segre embedding is always closed, and closed immersion is stable under base change, hence $\phi \otimes \mathrm{Id}$ is also closed.

Proposition 2.4.2

If $\phi : X \to \mathbb{P}^n_{\overline{\mathbb{Q}}}$ and $\psi : X \to \mathbb{P}^m_{\overline{\mathbb{Q}}}$ are morphisms over $\overline{\mathbb{Q}}$, then

$$h_{\phi \# \psi} = h_\phi + h_\psi$$

This follows from the relation between Segre embedding and heights on $\mathbb{P}^n$.

Next, we claim every Weil height may be viewed as a global height defined in previous section. Indeed, there is a linear form $\ell = \ell_0 x_0 + \ldots + \ell_n x_n$ which does not vanish identically on any irreducible component of X. Then we see h_ϕ is given by the global height associated with $\phi^*(\ell, \mathscr{O}_{\mathbb{P}^n}(1), x_0, \ldots, x_n, \mathscr{O}_{\mathbb{P}^n}, 1)$.

Conversely, we will show every global height is a difference of two Weil heights. Suppose h_λ is the global height relative to the presentation $\mathcal{D} = (s, \mathscr{L}, \mathbf{s}, \mathscr{M}, \mathbf{t})$. Then we get two morphisms ϕ and ψ, induced by $(\mathscr{L}, \mathbf{s})$ and $(\mathscr{M}, \mathbf{t})$, respectively. Then it follows from the independence of h_λ from s that

$$h_\lambda = h_\phi - h_\psi$$

Theorem 2.4.3

If $\phi : X \to \mathbb{P}^n_{\overline{\mathbb{Q}}}$ and $\psi : X \to \mathbb{P}^m_{\overline{\mathbb{Q}}}$ are morphisms over $\overline{\mathbb{Q}}$ with $\phi^* \mathscr{O}_{\mathbb{P}^n}(1) \cong \psi^* \mathscr{O}_{\mathbb{P}^m}(1)$,

then $h_\phi - h_\psi$ is a bounded function.

The proof is immediate.

Theorem 2.4.4: Northcott's Theorem

Let X be a projective variety defined over the number field K and $h_{\mathscr{L}}$ a height function associated with ample $\mathscr{L} \in \mathrm{Pic}(X)$. Then the set

$$\{P \in X(\overline{K}) : h_{\mathscr{L}}(P) \leq C, [K(P) : K] \leq d\}$$

is finite for any constant $C, d \in \mathbb{R}$.

Proof. There is $m \in \mathbb{N}$ so $\mathscr{L}^{\otimes m}$ is very ample. By Theorem 2.3.5, $mh_{\mathscr{L}}$ is a height function associated with $\mathscr{L}^{\otimes m}$. Thus we can assume WLOG $\mathscr{L}$ is very ample. By Theorem 2.4.3 it suffices to prove the statement for $X = \mathbb{P}^n_{\overline{\mathbb{Q}}}$ and $\mathscr{L} = \mathscr{O}_{\mathbb{P}^n}(1)$, i.e. for standard height on $\mathbb{P}^n_{\overline{\mathbb{Q}}}$. But then this follows almost immediately from Theorem 1.2.11.

In the rest of this section, we will derive some explicit bounds on Weil heights. This will be techinical. Let us fix a situation below for the rest of the section.

Setup 2.4.5

Let X be irreducible projective over $\overline{\mathbb{Q}}$ of dimension r. Then there is a $\overline{\mathbb{Q}}$-morphism

$$\pi : X \to \mathbb{P}^{r+1}_{\overline{\mathbb{Q}}}$$

so X is mapped birationally onto a hypersurface (to see this, note $K(X)$ is separable over K, hence $K(X)$ is finite dimension $K(f_1, ..., f_r)$-vector space, with f_i algebraically independent. Thus $K(X)$ is generated over $K(f_1, ..., f_r)$ by a rational function f_{r+1}. Now let p be the minimal polynomial of f_{r+1} over $K(f_1, ..., f_r)$, and assume $p = q(f_1, ..., f_r)$ with $q \in K[x_1, ..., x_{r+1}]$, then $V(q)$ is a birational model of X.). We denote by $z_0, ..., z_{r+1}$ the standard coordinates of $\mathbb{P}^{r+1}_{\overline{\mathbb{Q}}}$. Then we may assume the hypersurface is given by irreducible homogeneous polynomial f of degree d of the form

$$f(z_0, ..., z_{r+1}) = f_0 + f_1 z_{r+1} + ... + f_{d-1} z_{r+1}^{d-1} + z_{r+1}^d$$

with $f_i \in \overline{\mathbb{Q}}[z_0, ..., z_r]$ homogeneous of degree $d - i$, $f(0, ..., 0, 1) \neq 0$ and d the degree of X with respect to $\pi^* \mathscr{O}_{\mathbb{P}^{r+1}}(1)$.

Now let S be the homogeneous coordiante ring of $\pi(X)$. We have

$$S = \overline{\mathbb{Q}}[z_0, ..., z_{r+1}]/J$$

where J is the homogeneous ideal generated by f. Let $\overline{z}_i$ be the image of z_i in S $(0 \leq i \leq r+1)$ and note $\overline{z}_{r+1}$ is integral over $\overline{\mathbb{Q}}[\overline{z}_0, ..., \overline{z}_r]$. The variables $\overline{z}_0, ..., \overline{z}_r$ are

algebraically independent, because the transcendence degree of $\overline{\mathbb{Q}}(\pi(X)) = \overline{\mathbb{Q}}(X)$ is r. By abuse of notation, we denote them by $z_0, ..., z_r$ again. The minimal polynomial of $\overline{z}_{r+1}$ over $\overline{\mathbb{Q}}[z_0, ..., z_r]$ is $f(z_0, ..., z_r)$, since

$$0 = f_0 + f_1\overline{z}_{r+1} + ... + f_{d-1}\overline{z}_{r+1}^{d-1} + \overline{z}_{r+1}^{d} \tag{Eq. 2.4.1}$$

The elements $1, \overline{z}_{r+1}, \overline{z}_{r+1}^2, ..., \overline{z}_{r+1}^{d+1}$ forms a basis of S over $\overline{\mathbb{Q}}[z_0, ..., z_r]$ and so we have an isomorphism of $\overline{\mathbb{Q}}$-vector spaces

$$S \xrightarrow{\sim} \{p \in \overline{\mathbb{Q}}[z_0, ..., z_{r+1}] : \deg_{z_{r+1}}(p) < d\}$$

By means of this map, we define the height of an element of S as the height of the corresponding polynomial (defined below).

Definition 2.4.6

The ***height of a polynomial***

$$f(t_1, ..., t_n) = \sum_{(j_1,...,j_n)} a_{(j_1,...,j_n)} t_1^{j_1} ... t_n^{j_n} = \sum_{\mathbf{j}} a_{\mathbf{j}} t^{\mathbf{j}}$$

with coefficients in a number field K is the quantity

$$h(f) = \sum_{v \in M_K} \log |f|_v$$

where

$$|f|_v := \max_{\mathbf{j}} |a_{\mathbf{j}}|_v$$

is called the Gauss norm.

Now, for $l \in \mathbb{N}$, there are uniquely determined $q_{lj} \in \overline{\mathbb{Q}}[z_0, ..., z_r]$ for $j = 0, ..., d-1$ so

$$\overline{z}_{r+1}^{l} = \sum_{j=0}^{d-1} q_{lj} \overline{z}_{r+1}^{j} \tag{Eq. 2.4.2}$$

The polynomials q_{lj} are homogeneous of degree $l - j$ (elements of negative degree are 0), and $q_{lj} = \delta_{lj}$ for $0 \leq l \leq d-1$, where δ_{lj} is Kronecker delta. We may now assume $l \geq d$. Then equation Eq. 2.4.1 shows

$$\overline{z}_{r+1}^{l} = -\sum_{k=0}^{d-1} f_k \overline{z}_{r+1}^{k+l-d} = -\sum_{j=0}^{d-1} \sum_{k=0}^{d-1} f_k q_{k+l-d,j} \overline{z}_{r+1}^{j}$$

leading to recursive formula

$$q_{lj} = -\sum_{k=0}^{d-1} f_k q_{k+l-d,j} \tag{Eq. 2.4.3}$$

where $j = 0, ..., d-1$.

Now let F be a number field containing the coefficients of $f_0, ..., f_{d-1}$ and for $v \in M_F$ define δ_v be 1 if v is archimedean and 0 otherwise. The recursion Eq. 2.4.3 gives

$$|q_{lj}|_v \leq \left| \binom{d+r+1}{r+1} \right|_v^{\delta_v} \cdot |f|_v \max_{l'=l-d,...,l-1} |q_{l'j}|_v$$

for the Gauss norms. Here we used the fact f_k has $\binom{d-k+r}{r}$ summands and

$$\sum_{k=0}^{d}\binom{d-k+r}{r}=\binom{d+r+1}{r+1} \tag{Eq. 2.4.4}$$

By induction we obtain

$$|q_{lj}|_v \leq \left|\binom{d+r+1}{r+1}\right|_v^{(l-d)\delta_v}\cdot |f|_v^{l-d+1} \tag{Eq. 2.4.5}$$

and thus Lemma 1.1.11 leads to

$$h(q_{lj}) \leq (l-d+1)h(f)+(l-d)\log\binom{d+r+1}{r+1}$$

Let $\phi : X \to \mathbb{P}^n_{\overline{\mathbb{Q}}}$ be a closed embedding and $x_0,...,x_n$ be the standard coordinates on $\mathbb{P}^n$. Let $\mathbf{p}$ be a vector with entries $p_i \in S$ (here S is defined below Setup 2.4.5), $i=0,...,n$, homogeneous of degree $d(\mathbf{p})$.

Definition 2.4.7

The vector $\mathbf{p}$ is said to be a ***presentation*** of ϕ if the following conditions are satisfied:

1. If $l \in \{0,...,n\}$ and $x_l|_X \neq 0$, then $p_l \neq 0$
2. If l as in (1) and $i \in \{0,...,n\}$, then

$$\frac{p_i}{p_l}=\frac{x_i}{x_l}|_X$$

in $\overline{\mathbb{Q}}(X)$

The number $d(\mathbf{p})$ is called the degree of presentation $\mathbf{p}$. Consider the vector whose entries are given by all the coefficients of $p_0,...,p_n$. The height of the corresponding point in appropriate projective space is called the height of $\mathbf{p}$.

Lemma 2.4.8

Let $\phi_j : X \to \mathbb{P}^{n_j}_{\overline{\mathbb{Q}}}$, $j=1,...,k$, be closed embeddings with presentations $\mathbf{p}^{(i)}$ and $n=(n_1+1)...(n_k+1)-1$. Then:

1. *the join $\phi_1\#...\#\phi_k$ gives a closed embedding $\phi : X \to \mathbb{P}^n_{\overline{\mathbb{Q}}}$.*
2. *ϕ has a presentation defined by*

$$p_{\mathbf{i}} := p_{i_1}^{(1)}...p_{i_k}^{(k)}$$

of degree $d(\mathbf{p})=\sum_i d(\mathbf{p}^{(i)})$ and height

$$h(\mathbf{p}) \leq \sum_{j=1}^{k} h(\mathbf{p}^{(j)})+r\sum_{j=1}^{k-1}\log\left(6+\frac{6d(\mathbf{p}^{(j)}}{r}\right)+C(k-1)$$

with $C = (d-1)h(f) + d(d+r+1)$.

Proof. Since ϕ_j are closed immersions, their join is also closed immersion. Also, $\mathbf{p}$ is a presentation of ϕ of degree $\sum d(\mathbf{p}^{(i)})$. It remains to prove the estimation on heights, and we will do this by induction. In fact, it suffices to prove the claim for $k = 2$.

We have decomposition

$$p_{i_j}^{(j)} = \sum_{m=0}^{d-1} p_{i_j,m}^{(j)} \overline{z}_{r+1}^{m}$$

whence

$$p_{\mathbf{i}} = \left(\sum_{m_1=1}^{d-1} p_{i_1,m_1}^{(1)} \overline{z}_{r+1}^{m_1} \right) \left(\sum_{m_2=0}^{d-1} p_{i_2,m_2}^{(2)} \overline{z}_{r+1}^{m_2} \right)$$

Then, Eq. 2.4.2 leads to decomposition

$$p_{\mathbf{i}} = \sum_{m=0}^{d-1} p_{\mathbf{i},m} \overline{z}_{r+1}^{m}$$

with

$$p_{\mathbf{i},m} := \sum_{m_1+m_2=m} p_{i_1,m_1}^{(1)} p_{i_2,m_2}^{(2)} + \sum_{l=d}^{2d-2} \sum_{\substack{m_1+m_2=l \\ m_1,m_2 \leq d-1}} p_{i_1,m_1}^{(1)} p_{i_2,m_2}^{(2)} q_{lm}$$

Let F be a number field extension of $\mathbb{Q}$ containing the coefficients of $f_0, \ldots, f_{d-1}$ and of all $p_{i_j,m_j}^{(j)}$ for $j = 1, 2$, and for $v \in M_F$ define $\delta_v = 1$ for archimedean places and 0 otherwise. Then we see

$$|p_{\mathbf{i},m}|_v \leq |B|_v^{\delta_v} \cdot |p_{i_1}^{(1)}| \cdot |p_{i_2}^{(2)}|_v \cdot \max_{l=d,\ldots,2d-2} (1, |q_{lm}|_v) \tag{Eq. 2.4.6}$$

where B is an upper bound for

$$\sum_{m_1=0}^{m} \binom{r + d(\mathbf{p}^{(1)}) - m_1}{r} + \sum_{l=d}^{2d-2} \sum_{m_1=l-d+1}^{d-1} \binom{r + d(\mathbf{p}^{(1)}) - m_1}{r} \binom{r+l-m}{r}$$

Thereby we have used the fact the number of monomials of degree D in $r+1$ variables is equal to $\binom{r+D}{D}$. We use the estimate

$$\binom{r + d(\mathbf{p}^{(1)}) - m_1}{r} \leq \frac{1}{r!} (r + d(\mathbf{p}^{(1)}))^r < \left(3 + \frac{3d(\mathbf{p}^{(1)})}{r} \right)^r$$

and

$$\binom{r+l-m}{r} \leq r^{r+l-m}$$

to conclude

$$B = d 2^{r+2d} \left(3 + \frac{3d(\mathbf{p}^{(1)})}{r} \right)^r$$

is such an upper bound. For Eq. 2.4.5 and Eq. 2.4.6 we see

$$h(\mathbf{p}) \leq h(\mathbf{p}^{(1)}) + h(\mathbf{p}^{(2)}) + \log B + (d-1)h(f) + (d-2) \log \binom{r+d+1}{d+1}$$

With the above value of B, we see

$$h(\mathbf{p}) \leq h(\mathbf{p}^{(1)}) + h(\mathbf{p}^{(2)}) + r\log(6 + 6d(\mathbf{p}^{(1)})/r) + C$$

with

$$C = (d-1)h(f) + d(d+r+1)$$

Notations

For any list of elements in additive abelian group G, say $\mathbf{a} = (a_1, ..., a_n) \in G^n$, we use $|\mathbf{a}| = \sum a_i$. For any list of integers $\mathbf{a} = (a_1, ..., a_n)$ and a list of elements in a multiplicative abelian group G, say $\mathbf{x} \in G^n$, we define

$$\mathbf{x}^{\mathbf{a}} = x_1^{a_1} ... x_n^{a_n}$$

For closed subvariety Y of $\mathbb{P}^N$, we denote $\mathscr{I}(Y)$ the ideal sheaf of Y.

Proposition 2.4.9

Let $\phi : X \to \mathbb{P}^n_{\overline{\mathbb{Q}}}$, $\psi : X \to \mathbb{P}^m_{\overline{\mathbb{Q}}}$ be closed embeddings over $\overline{\mathbb{Q}}$, with corresponding presentations $\mathbf{p}, \mathbf{q}$. We assume

$$\phi^* \mathscr{O}_{\mathbb{P}^n}(1) \cong \psi^* \mathscr{O}_{\mathbb{P}^m}(1)$$

There is a positive integer k_ψ such that if $k \geq k_\psi$, then

$$H^1(\mathbb{P}^m_{\overline{\mathbb{Q}}}, \mathscr{I}(\psi X) \otimes \mathscr{O}_{\mathbb{P}^m}(k)) = 0$$

If $k \geq k_\psi$ and $\chi(k) := \dim(H^0(X, \psi^* \mathscr{O}_{\mathbb{P}^m}(k)))$ and $P \in X$, then

$$h_\phi(P) - h_\psi(P) \leq (n+1)\chi(k) \cdot (A_{\mathbf{p},\mathbf{q}} + B_{\mathbf{p},\mathbf{q}} + C)$$

where

$$A_{\mathbf{p},\mathbf{q}} = h(\mathbf{p}) + h(\mathbf{q})$$

$$B_{\mathbf{p},\mathbf{q}} = r\log\left(6 + \frac{6d(\mathbf{p})}{r}\right) + r\log\left(6 + \frac{6d(\mathbf{q})}{r}\right)$$

$$C = \frac{1}{k}\log((n+1)\chi(k)) + (d-1)h(f) + d(d+r+1)$$

Proof. The existence of k_ψ is just Kodaira vanishing. There is short exact sequence

$$0 \to \mathscr{I}(\psi X) \to \mathscr{O}_{\mathbb{P}^m} \to \psi_* \mathscr{O}_X \to 0$$

of coherent sheaves on $\mathbb{P}^m$. Tensor with $\mathscr{O}_{\mathbb{P}^m}(k)$ we have

$$0 \to \mathscr{I}(\psi X) \otimes \mathscr{O}_{\mathbb{P}^m}(k) \to \mathscr{O}_{\mathbb{P}^m}(k) \to (\psi_* \mathscr{O}_X) \otimes \mathscr{O}_{\mathbb{P}^m}(k) \to 0$$

The projection formula gives

$$(\psi_* \mathscr{O}_X) \otimes \mathscr{O}_{\mathbb{P}^m}(k) \cong \psi_* \psi^* \mathscr{O}_{\mathbb{P}^m}(k)$$

Consider the induced long exact sequence of cohomology, we get

$$0 \longrightarrow H^0(\mathbb{P}^m, \mathscr{I}(\psi X) \otimes \mathscr{O}_{\mathbb{P}^m}(k)) \longrightarrow H^0(\mathbb{P}^m, \mathscr{O}_{\mathbb{P}^m}(k))$$

$$H^0(X, \psi^* \mathscr{O}_{\mathbb{P}^m}(k)) \longrightarrow H^1(\mathbb{P}^m, \mathscr{I}(\psi X) \otimes \mathscr{O}_{\mathbb{P}^m}(k)) \longrightarrow \dots$$

The last cohomology is 0 by the choice of k, and we infer that the map

$$H^0(\mathbb{P}^m, \mathscr{O}_{\mathbb{P}^m}(k)) \longrightarrow H^0(X, \psi^* \mathscr{O}_{\mathbb{P}^m}(k))$$

is surjection. By assumption, $\phi^* \mathscr{O}_{\mathbb{P}^n}(1) \cong \psi^* \mathscr{O}_{\mathbb{P}^m}(1)$ and we may identify them as the same. Let $\mathbf{x} = (x_0 : \dots : x_n)$ and $\mathbf{y} = (y_0 : \dots : y_m)$ be the standard coordinates and choose $B \subseteq \{\mathbf{b} \in \mathbb{N}^{m+1} : |\mathbf{b}| = k\}$ such that

$$(\mathbf{y}^{\mathbf{b}}|_X)_{\mathbf{b} \in B}$$

is a basis of $H^0(X, \psi^* \mathscr{O}_{\mathbb{P}^m}(1))$. There are uniquely determined $\alpha_{i,\mathbf{b}} \in \overline{\mathbb{Q}}$ so

$$x_i^k|_X = \sum_{\mathbf{b} \in B} a_{i,\mathbf{b}} \mathbf{y}^{\mathbf{b}}|_X \tag{Eq. 2.4.7}$$

Let $P \in X(\overline{\mathbb{Q}})$. Choose a number field F containing $x_i(P), y_j(P)$ and $a_{i,\mathbf{b}}$ for all $i, j, \mathbf{b}$. By Proposition 2.4.2, we obtain ,for the k-fold $\psi^{(k)} = \psi \# \dots \# \psi$, the equation

$$\begin{aligned} k(h_\phi(P) - h_\psi(P)) &= \sum_{v \in M_F} \log \max_i |x_i^k(P)|_v - h_{\psi^{(k)}}(P) \\ &= \sum_{v \in M_F} \log \max_i |x_i^k(P)|_v - \sum_{v \in M_F} \log \max_{|\mathbf{b}|=k} |\mathbf{y}^{\mathbf{b}}(P)|_v \end{aligned}$$

By Eq. 2.4.7, the triangle inequality and Lemma 1.1.11, we deduce

$$h_\phi(P) - h_\psi(P) \leq \frac{1}{k} h(a) + \frac{1}{k} \log \chi(k) \tag{Eq. 2.4.8}$$

where a is the matrix $(a_{i,\mathbf{b}})$ and $h(a)$ is the height of the matrix viewed as a vector.

We take the ratio of Eq. 2.4.7 with indices i and l and deduce, using the definition of presentation, that

$$\sum_{\mathbf{b} \in B} a_{l,\mathbf{b}} p_i^k \mathbf{q}^{\mathbf{b}} = \sum_{\mathbf{b} \in B} a_{i,\mathbf{b}} p_l^k \mathbf{q}^{\mathbf{b}} \quad \text{for } i, l \in \{0, \dots, n\} \tag{Eq. 2.4.9}$$

Conversely, assume $(a_{i,\mathbf{b}})$ is a non-trivial solution of this equation. Then we have

$$(x_i|_X)^k \sum_{\mathbf{b} \in B} a_{l,\mathbf{b}} (\mathbf{y}|_B)^{\mathbf{b}} = (x_l|_X)^k \sum_{\mathbf{b} \in B} a_{i,\mathbf{b}} (\mathbf{y}|_X)^{\mathbf{b}}$$

Let i be such that $x_i|_X$ is not identically 0. Then the last displayed equation shows that rational function on X defined by

$$g := \frac{\sum_{\mathbf{b}\in B} a_{i,\mathbf{b}}\mathbf{y}^{\mathbf{b}}}{x_i^k|_X}$$

does not depend on the index i. We claim g is constant. To prove this, it suffices to show g is a regular function (use X is projective). Indeed, since $x_0, ..., x_n$ generate $\mathscr{O}_{\mathbb{P}^n}(1)$, we see for any $P \in X(\overline{\mathbb{Q}})$, there is an index i so $x_i(P) \neq 0$, hence g is regular at P.

This proves the space of solutions of Eq. 2.4.9 is spanned by the matrix $a = (a_{i,\mathbf{b}})$ given by Eq. 2.4.7.

Our next task is to estimate $h(\mathbf{a})$. Since a scalar factor does not change the height, we may estimate the height of any non-trivial solution of Eq. 2.4.9. By Lemma 2.4.8, we have a natural presentation of $\phi^{(k)}\#\psi^{(k)}$ in terms of $\mathbf{p}$ and $\mathbf{q}$. The elements $p_i^k\mathbf{q}^{\mathbf{b}}$ of S are entries of that presentation. The decomposition

$$p_i^k\mathbf{q}^{\mathbf{b}} = \sum_{j=0}^{d-1} c_{\mathbf{b},i,j}\overline{z}_{r+1}^j$$

with uniquely determined $c_{\mathbf{b},i,j} \in \overline{\mathbb{Q}}[z_0, ..., z_r]$ leads to the system of equations

$$\sum_{\mathbf{b}\in B} c_{\mathbf{b},i,j}a_{l,\mathbf{b}} - \sum_{\mathbf{b}\in B} c_{\mathbf{b},l,j}a_{i,\mathbf{b}} = 0 \qquad \text{(Eq. 2.4.10)}$$

with $i, l \in \{0, ..., n\}$ and we have $j \in \{0, ..., d-1\}$.

Let $c_{\mathbf{b},i,j} = \sum c_{\mathbf{b},i,j,\mathbf{a}} z_0^{a_0} ... z_r^{a_r}$, so that the coefficients $c_{\mathbf{b},i,j,\mathbf{a}}$ of the polynomials $c_{\mathbf{b},i,j}$ form a matrix $\mathbf{c}$ with

$$h(\mathbf{c}) \leq k(h(\mathbf{p}) + h(\mathbf{q}) + r\log(6 + 6d(\mathbf{p})/r) + r\log(6 + 6d(\mathbf{q})/r) + C) \qquad \text{(Eq. 2.4.11)}$$

again by Lemma 2.4.8. Moreover, Eq. 2.4.10 is equivalent to the linear system of equations

$$\sum_{\mathbf{b}\in B}(c_{\mathbf{b},i,j,\mathbf{a}}a_{l,\mathbf{b}} - c_{\mathbf{b},l,j,\mathbf{a}}a_{i,\mathbf{b}}) = 0$$

indexed by $i, j, l, \mathbf{a}$ and unknowns $a_{i,\mathbf{b}}$. Let A denote the matrix associated to this linear system; its entries are either 0 or $\pm c_{\mathbf{b},i,j,\mathbf{a}}$. The numbers of unknowns is $(n+1)|B|$ and, as remarked before, the space of solutions has dimension 1. Therefore, the rank R of the matrix A is

$$R = (n+1)\chi(k) - 1$$

Let A' be a $R \times (R+1)$ submatrix of A of full rank R. Since A and A' have the same kernel, we look for a non-zero solution of $A' \cdot \mathbf{a} = 0$. The estimate

$$\max_{\rho=0,...,R} |a_\rho|_v \leq |R!|_\delta^{\delta_v} \cdot \max_{\mathbf{b},i,j,\mathbf{a}} |c_{\mathbf{b},i,j,\mathbf{a}}|_v^R$$

and Eq. 2.4.11 lead to

$$h(\mathbf{a}) \leq Rk(h(\mathbf{p}) + h(\mathbf{q}) + r\log(6 + 6d(\mathbf{p})/r) + r\log(6 + 6d(\mathbf{q})/r) + C) + \log(R!)$$

By Eq. 2.4.8 and the definition of R, we now get

$$h_\phi(P) - h_\psi(P) \leq (n+1)\chi(k)(A_{\mathbf{p},\mathbf{q}} + B_{\mathbf{p},\mathbf{q}} + C)$$

as desired.

In the above proposition, almost all terms besides $\chi(k)$ are quite explicit. The following lemma estimates $\chi(k)$, which solves the problem.

Lemma 2.4.10

Let $\psi : X \to \mathbb{P}^m_{\overline{\mathbb{Q}}}$ be a closed embedding over $\overline{\mathbb{Q}}$ with presentation $\mathbf{q}$ and $k \geq k_\psi$, $\chi(k)$ be as in Proposition 2.4.9. Then

$$\chi(k) \leq \binom{kd(\mathbf{q}) + r + 1}{r+1} - \binom{kd(\mathbf{q}) - d + r + 1}{r+1}$$

Proof. Let $y_0, \ldots, y_m$ be the standard coordinates of $\mathbb{P}^m_{\overline{\mathbb{Q}}}$. We have seen the linear map

$$H^0(\mathbb{P}^m, \mathscr{O}_{\mathbb{P}^m}(k)) \to H^0(X, \psi^* \mathscr{O}_{\mathbb{P}^m}(k))$$

is surjective. Choose $B \subseteq \{\mathbf{b} \in \mathbb{N}^{m+1} : |\mathbf{b}| = k\}$ such that $(\mathbf{y}^{\mathbf{b}}|_X)_{\mathbf{b}\in B}$ such that is a basis of $H^0(X, \psi^* \mathscr{O}_{\mathbb{P}^m}(k))$. The above monomials are linearly independent iff the polynomials $(\mathbf{q}^{\mathbf{b}})_{\mathbf{b}\in B}$ are linearly independent, by definition of a presentation. Thus

$$\chi(k) \leq \dim S_{kd(\mathbf{q})} = \binom{kd(\mathbf{q}) + r + 1}{r+1} - \binom{kd(\mathbf{q}) - d + r + 1}{r+1}$$

because $S_{kd(\mathbf{q})}$ is isomorphic to the space of homogeneous polynomials $p(z_0, \ldots, z_{r+1})$ of degree $kd(\mathbf{q})$ such that $\deg_{z_{r+1}}(p) < d$, and then we apply Eq. 2.4.5.

For the main estimation we want to achieve, we will need the following result.

Lemma 2.4.11

Let $Y \subseteq \mathbb{P}^m_{\overline{\mathbb{Q}}}$ be irreducible smooth closed and $c = \min(1 + \dim(Y), \operatorname{codim}_{\mathbb{P}^m}(Y))$. Then

$$H^i(\mathbb{P}^m_{\overline{\mathbb{Q}}}, \mathscr{I}_Y \otimes \mathscr{O}_{\mathbb{P}^m}(k)) = 0$$

for $i \geq 1$, $k \geq c(\deg(Y) - 1) - \dim(Y)$.

Lemma 2.4.12

If $\psi : X \to \mathbb{P}^m_{\overline{\mathbb{Q}}}$ be closed immersion with presentation $\mathbf{q}$, then

$$\deg(\psi X) \leq d(\mathbf{q})^r d$$

Proof. The Hilbert polynomial of ψX has degree r and its leading coefficient is equal to $\deg(\psi X)/r!$. For large k, the Hilbert polynomial at k equals the left-hand side of the inequality in Lemma 2.4.10. On the other hand, the right-hand side of that inequality is also a polynomial of degree r in k, with leading coefficient

$$\frac{d(\mathbf{q})^r}{(r+1)!}((r+1)+\cdots+1) - \frac{d(\mathbf{q})^r}{(r+1)!}((r+1-d)+\cdots+(1-d)) = \frac{d(\mathbf{q})^r d}{r!}$$

This concludes the proof.

Now we are ready to summarize the explicit bound we worked out, in the previous lemmas and propositions.

Let X be smooth irreducible projective variety over $\overline{\mathbb{Q}}$, $r = \dim X$ and $\pi : X \to \mathbb{P}^{r+1}_{\overline{\mathbb{Q}}}$ a morphism over $\overline{\mathbb{Q}}$, mapping X birationally to a hypersurface given by a homogeneous polynomial f of degree d.

Assume $\phi : X \to \mathbb{P}^n$ and $\psi : X \to \mathbb{P}^m$ are closed $\overline{\mathbb{Q}}$-immersions with $\phi^* \mathcal{O}_{\mathbb{P}^n}(1) \cong \psi^* \mathcal{O}_{\mathbb{P}^m}(1)$ and corresponding presentations $\mathbf{p}$ and $\mathbf{q}$. We assume $d(\mathbf{q}) \geq 1$.

Theorem 2.4.13

For each $P \in X$, it holds

$$h_\phi(P) - h_\psi(P) \leq C_1(n+1)d(\mathbf{q})^{r^2+r}(A_{\mathbf{p},\mathbf{q}} + B_{\mathbf{p},\mathbf{q}} + \log(n+1) + C_2)$$

where

$$C_1 = d\frac{(d+1)^r(r+1)^r}{r!}, C_2 = (d-1)h(f) + d(d+r+1) + r + 1$$

$$A_{\mathbf{p},\mathbf{q}} = h(\mathbf{p}) + h(\mathbf{q})$$

$$B_{\mathbf{p},\mathbf{q}} = r\log\left(6 + \frac{6d(\mathbf{p})}{r}\right) + r\log\left(6 + \frac{6d(\mathbf{q})}{r}\right)$$

Proof. Let $k := d(r+1)d(\mathbf{q})^r$, then $k \geq k_\psi$ by Lemma 2.4.11 and Lemma 2.4.12. We

have

$$\begin{aligned}\chi(k) &\leq \binom{kd(\mathbf{q})+r+1}{r+1} - \binom{kd(\mathbf{q})+r+1-d}{r+1} \\ &\leq d\binom{kd(\mathbf{q})+r}{r} \\ &\leq \frac{d}{r!}(kd(\mathbf{q})+r)^r\end{aligned}$$

where the first step comes from Lemma 2.4.10 and the second step uses Eq. 2.4.4. From the definition of k, we see

$$\chi(k) \leq d\frac{(d+1)^r(r+1)^r}{r!}d(\mathbf{q})^{r^2+r}$$

An easy majorization shows $k^{-1}\log\chi(k) \leq r+1$ and the result follows from Proposition 2.4.9.

2.5 Bounded Subsets

In order to show the differences between the local height of two presentations diff by a constant, we introduced bounded sets in affine varieties. In this section, we will extend this notion to arbitrary varieties.

Let K be a field and fix an embedding $K \subseteq \overline{K}$. For the moment, we fix an absolute value $|\cdot|$ on $\overline{K}$.

Definition 2.5.1

A subset $E \subseteq X(\overline{K})$ is called ***bounded*** in X, if there is a finite affine open cover $(U_i)_{i\in I}$ of X, and sets E_i with $E_i \subseteq U_i(\overline{K})$, such that E_i is bounded (as in Definition 2.2.4) in U_i and $E = \bigcup_{i\in I} E_i$.

Remark 2.5.2

If E is bounded in X, Lemma 2.2.6 shows for any fintie open affine cover $\{U_i\}$ of X, there is a subdivision

$$E = \bigcup_{i\in I} E_i$$

with $E_i \subseteq U_i(\overline{K})$, such that each E_i is bounded in U_i.

It is easy to show the image of a bounded set under a morphism is again bounded. Moreover, if $Y \subseteq X$ is closed and $E \subseteq Y(\overline{K})$ is bounded, then E is bounded in X.

Example 2.5.3

Assume K is locally compact with respect to $|\cdot|$ (e.g. the completion of a number field with respect to a place). We consider $X(K)$ the topology induced locally by open balls with respect to closed embeddings into affine spaces and maximum norm. Then the topology is locally compact and independent of the embeddings. It depends only on the place v represented by $|\cdot|$ and its called the v-topology on $X(K)$. A subset E of $X(K)$ is bounded in X if and only if E is relatively compact in $X(K)$.

Example 2.5.4

The set $\mathbb{P}^n(\overline{K})$ is bounded in the projective space $\mathbb{P}^n_K$. We can use affine cover $X_i = \{\mathbf{x} \in \mathbb{P}^n_K : x_i \neq 0\}$ and decomposition $E_i = \{\mathbf{x} \in \mathbb{P}^n_K : |x_i| = \max_{j=0,\dots,n}|x_j|\}$ of E. By Remark 2.5.2, the set of $\overline{K}$-rational points is bounded in any projective variety.

Proposition 2.5.5

If X is a complete variety over K, then $X(\overline{K})$ is bounded in X. More generally, the inverse image of a bounded subset under a proper morphism remains bounded.

Proof. By Chow's lemma, there is projective Y over K and surjective birational $Y \to X$. Using Remark 2.5.2 and Example 2.5.4, $X(\overline{K})$ is bounded in X.

More generally, if $\phi : X' \to X$ is proper over K and $E \subseteq X(\overline{K})$ is bounded in X. By Chow's lemma, the proof is reduced to the case of a projective morphism and hence $X' = X \times \mathbb{P}^n_K$ with ϕ the first projection. By Remark 2.5.2 we can assume X is affine and the same argument as in Example 2.5.4 shows $\phi^{-1}(E)$ is bounded in $X \times \mathbb{P}^n_K$.

Remark 2.5.6

Its trivial that any subset of a bounded subset is bounded. However, we may not pass from X to an open subset. For example, the set $E = \{\mathbf{x} \in \mathbb{P}^n(\overline{K}) : x_0 \neq 0\}$ is bounded but it is certainly not bounded in the affine space $\{\mathbf{x} \in \mathbb{P}^n_K : x_0 \neq 0\}$. Thus the notion of bounded subset is not local and some care is needed.

Definition 2.5.7

A real function f on a K-variety X is ***locally bounded*** if $f(E)$ is bounded for every bounded E in X.

Setup 2.5.8

To apply this later on the theory of heights, we need a generalization to several absolute values. Let M_K be a set of places on K. For every $v \in M_K$, an absolute value $|\cdot|_v$ is fixed in the equivalence class of v. We assume $\{v \in M_K : |\alpha|_v \neq 1\}$ is finite. Let M be a set of places on $\overline{K}$. We assume every $u \in M$ restricts to a $v \in M_K$ and we denote by $|\cdot|_u$ the unique extension of $|\cdot|_v$ to an absolute value representing u.

Definition 2.5.9

Let U be affine K-variety and $(E^u)_{u\in M}$ a family of subsets of $U(\overline{K})$. The family is said to be M-***bounded*** in U if for any $f \in K[U]$ the quantity

$$C_v(f) = \sup_{u\in M} \sup_{u|v} \sup_{P\in E^u} |f(P)|_u$$

is finite for every $v \in M_K$ and $C_v(f) > 1$ for only finitely many v.

More generally, if X is K-variety and $(E^u)_{u\in M}$ a family of subsets of $X(\overline{K})$. Then (E^u) is M-***bounded*** if there is finite affine open cover $\{U_i\}$ so

$$E^u = \bigcup_{i\in I} E_i^u, \quad E_i^u \subseteq U_i(\overline{K})$$

such that $(E_i^u)_{u\in M}$ is M-bounded in U_i for all i.

If M has only one element, then $E \subseteq U(\overline{K})$ is M-bounded iff E is bounded in U in the sense we defined before.

Remark 2.5.10

We note Lemma 2.2.5 and Lemma 2.2.6 extend to the situation with several absolute values instead of one.

Definition 2.5.11

A subset $E \subseteq X(\overline{K})$ is M-***bounded*** if the constant family $(E)_{u\in M}$ is M-bounded.

Example 2.5.12

The set $\mathbb{P}^n(\overline{K})$ is M-bounded in $\mathbb{P}^n_K$.

Proposition 2.5.13

A complete K-variety is M-bounded. More generally, the inverse image of an M-bounded family of subsets under a proper morphism is M-bounded.

Definition 2.5.14

A real function f on $X \times M$ is called ***locally M-bounded*** if, for any M-bounded family $(E^u)_{u \in M}$ in X, there is for every $v \in M_K$ a non-negative real number γ_v, with $\gamma_v \neq 0$ only for finitely many $v \in M_K$, so for all $u \in M$ with $v \mid u$, we have

$$|f(E^u, u)| \leq \gamma_v$$

Chapter 3

Abelian Varieties

In this chapter, we will study basic properties of abelian varieties and Jacobians of algebraic curves.

3.1 Group Varieties

We let K be a field and $\overline{K}$ an algebraic closure. We assume all varieties and morphisms are over K.

After definition, we will prove constancy lemma, which roughly says if ϕ is constant on $X \times Y$ on one fiber, then ϕ is constant on all fibers. As an application, we will show abelian varieties are commutative and every morphism of abelian varieties is a translation of a homomorphism.

Next, we will show a generic property of a group variety holds everywhere, and thus prove abelian varieties are smooth, dimension formula and other properties holds for homomorphisms and that tangent bundle is trivial. Then, we will show a rational map to an abelian variety is a morphism at all smooth points. Finally, we show complex abelian varieties are biholomorphic to complex tori with positive definite Riemann forms.

Definition 3.1.1

Let S be a scheme and G an S-scheme, then we say G is a ***group scheme (over S)*** if there is a factorization of the functor $h_G : (\mathbf{Sch}/S)^{\mathrm{opp}} \to (\mathbf{Set})$ through the forgetful functor $(\mathbf{Grp}) \to (\mathbf{Set})$.

By Yoneda's lemma, the above definition is equivalent to the following two data:

1. For all S-scheme T, there is a group structure on $G_S(T) := \mathrm{Hom}_S(T, G)$ which is functorial in T (i.e. the morphism $G_S(T) \to G_S(T')$ induced by $T' \to T$ is always a group homomorphism)
2. Three S-morphisms $m : G \times_S G \to G$, $i : G \to G$ and $e : S \to G$, which correspond to multiplication, inverse and unit of the group.

In particular, if G happends to be a variety, then we say G is a group variety (over K).

Definition 3.1.2

An ***abelian variety*** is a geometrically irreducible and geometrically reduced complete group variety.

Example 3.1.3

Let M_n be the set of n by n matrices. Then this is an irreducible affine group variety over K. The determinant is a morphism $\det : M_n \to \mathbb{A}^1_K$ and thus we have affine open irreducible subvariety $\mathrm{GL}(n)$ defined as the complement of the vanishing locus of the determinant. In particular, $\mathrm{SL}(n)$, which is defined by $\det(a) = 1$, is a subvariety of $\mathrm{GL}(n)$ that is also an affine group variety.

Here are some facts about group varieties:

1. Every affine group variety is isomorphic to a closed subgroup of $\mathrm{GL}(n)$.
2. Let G be irreducible group variety over perfect field K, then there is a smallest irreducible affine closed subgroup H and abelian variety A so we have exact sequence
$$0 \to H \to G \to A \to 0$$

Thus, to study general group varieties, we have to understant both affine group varieties and abelian varieties. In particular, since the trivial group variety $\mathbb{A}^0_K$ is the only complete geometrically irreducible affine variety, no other affine group variety is abelian variety.

Before we can prove the constancy lemma, we note the following remark.

Remark 3.1.4

Let X be proper irreducible over K and suppose $X \to Y$ is a K-morphism with Y affine of finite type, then this morphism must be constant. To see this, note we may assume both X, Y are reduced by passing to their underlying reduced subscheme. Say $Y = \mathrm{Spec} A$, i.e. $X \to Y$ is the same as $A \to \Gamma(X, \mathscr{O}_X)$. Now since X is proper hence complete, $\Gamma(X, \mathscr{O}_X)$ is finite dimensional K-vector space (to see this, X reduced means $\Gamma(X, \mathscr{O}_X)$ is reduced finite dimensional K-algebra, but X is also irreducible, thus it must be a field). Hence the image of A in $\Gamma(X, \mathscr{O}_X)$ must be a field, say k, then we see $X \to Y$ factor through $X \to \mathrm{Spec}\, k \to Y$ as desired.

Lemma 3.1.5: Constancy Lemma

Let X, Y, Z be varieties such that X is complete and X, Y geometrically irreducible. If $f : X \times Y \to Z$ is a morphism such that $f(X \times \{y_0\}) = \{z_0\}$ for some $y_0 \in Y$ and $z_0 \in Z$, then $f(X \times \{y\})$ is a point for all $y \in Y$.

Proof. By base change, we may assume $K = \overline{K}$ is ACF. Let U be open affine around z_0.

The image

$$C = \{y \in Y : \exists x \in X, f(x,y) \in Z \backslash U\}$$

of $f^{-1}(Z \backslash U)$ by the projection $X \times Y \to Y$ is closed as X is complete. Then

$$V = Y \backslash C = \{y \in Y : \forall x \in X, f(x,y) \in U\}$$

is open neighbourhood of y_0 and, for any $y \in V$, we have $X \to U$, given by $x \mapsto f(x,y)$. Since X is complete and irreducible and U is affine, the morphism has to be constant for any $y \in V$, with image $f(x_0, y)$ choice of a point $x_0 \in X$ (Remark 3.1.4 above). Now note

$$S = \{y \in Y : |f(X \times \{y\})| = 1\} = \bigcap_{x_1, x_2 \in X} \{y \in Y : f(x_1, y) = f(x_2, y)\}$$

is closed in Y. Since it contains the non-empty open subset V of Y and since Y is irreducible, we conclude $S = Y$, proving our claim.

Corollary 3.1.5.1

Let X, Y be geometrically irreducible variety with at least one K-rational point. We assume X is complete. A morphism $f : X \times Y \to G$ of a product into a group variety factorizes as $f(x,y) = g(x)h(y)$, for suitable morphism $g : X \to G$ and $h : Y \to G$.

Proof. We choose $y_0 \in Y(K)$ and define $g : X \to G$ by $g(x) = f(x, y_0)$. The morphism $F : X \times Y \to G$ defined by $F(x,y)g(x)^{-1}f(x,y)$ satisfies $F(X \times \{y_0\}) = \{\epsilon\}$ where $\epsilon \in G$ is the identity of G. Now Constancy Lemma 3.1.5 shows $F(X \times \{y\})$ is a point, say $h(y)$, for every $y \in Y$, and $f(x,y) = g(x)h(y)$. In order to verify h is a K-morphism, note $h = f(x_0, \cdot)g(x_0)^{-1}$ for any $x_0 \in X(K)$.

Corollary 3.1.5.2

Let $\phi : A \to G$ be a morphism of abelian variety A into group variety G. Then the map

$$\phi : A \to G, \quad a \mapsto \phi(a)\phi(\epsilon_A)^{-1}$$

is a homomorphism of group varieties.

Proof. Apply the Constancy lemma 3.1.5 with $f : A \times A \to G$, given by

$$(x,y) \mapsto \psi(x)\psi(y)\psi(xy)^{-1}$$

and with y_0, z_0 the identity of A, G, respectively. We conclude the restriction of f to $A \times \{y\}$ is a constant map for every y. Since $f(\{\epsilon_A\} \times A) = \{\epsilon_G\}$, we deduce f is constant, with image the identity of G.

Corollary 3.1.5.3

An abelian variety is commutative.

Proof. By Corollary 3.1.5.2, the inverse map ι is a homomorphism of group varieties. This is equivalent to commutativity.

Example 3.1.6

The affine line $\mathbb{A}^1_K$ is not complete because $xy = 1$ is closed subvariety of $\mathbb{A}^1 \times \mathbb{A}^1$, while its projection on the second factor is $\mathbb{A}^1 \backslash \{0\}$, not closed in $\mathbb{A}^1_K$. Now consider the morphism $f : \mathbb{A}^1 \times \mathbb{A}^1 \to \mathbb{A}^1$ given by $(x, y) \mapsto xy$. Then f satisfies the hypothesis of Lemma 3.1.5. This shows constancy lemma does not hold for non-complete X.

From now on, we will use additive notation for abelian varieties, i.e. $m(x, y) = x + y$, $i(x) = -x$, and denote the identity by 0. For $a \in A$, we have the translation map $\tau_a(x) = x + a$. For $n \in \mathbb{Z}$, we denote $[n]$ the endomorphism of A, which is multplication by n. The kernel of $[n]$ is denoted by $A[n]$, and it forms the torsion subgroups of A.

Remark 3.1.7

In the following, we note if X is locally of finite type and geometrically reduced scheme over K, then X contains an open dense locus of smooth points.

This problem is local on X, thus assume X is quasi-compact with irreducible components X_i. Then $Z = \bigcup_{i \neq j} X_i \cap X_j$ is nowhere dense, and thus we may replace X by $X \backslash Z$. Thus we may assume X is irreducible as $X \backslash Z$ is disjoint union of irreducible schemes. Since X is irreducible and reduced, its integral (integral=irreducible+reduced). Let $\eta \in X$ be its generic point. Then the function field $K(X) = \kappa(\eta)$ is geometrically reduced over K, hence separable over K. Let $U = \operatorname{Spec} A \subseteq X$ be any nonempty affine open so $\kappa(\eta) = A_{(0)}$ is the fraction field of A. This implies (recall the following: if S is finite type k-algebra, $\mathfrak{p} \in \operatorname{Spec} S$ and $\kappa(\mathfrak{p})$ separable over k, then S is smooth at $\mathfrak{p}$ over k if and only if $S_{\mathfrak{p}}$ is regular) A is smooth at (0) over K. By definition this means some principal localization of A is smooth over K.

Proposition 3.1.8

A geometrically reduced group variety is smooth.

Proof. By base change, we may assume K is ACF. The set of smooth points of X is open, and since X is geometrically reduced, the smooth locus is dense (Remark 3.1.7). As above, we can define left and right translation by a point of the group variety. They

are automorphisms and so the left translation of U is also smooth. If we vary the left translations, then we get an open cover of the group variety, proving the claim.

Remark 3.1.9

Suppose X is K-scheme, then clearly it is geometrically connected implies X is connected.

Next, suppose X is of finite type and connected over K. Then we show if X admits a K-rational point then X is geometrically connected. First, we see if X is quasi-compact, then X is geometrically connected if and only if $X_{K'}$ is connected for all finite separable extension K' of K. We will assume this fact.

Now, if K'/K is finite separable, then we see $\operatorname{Spec} K' \to \operatorname{Spec} K$ is finite flat, and hence universally closed and universally open at the same time. Thus $X_{K'} \to X_K = X$ is open and closed, finite and flat. This means any connected component of $X_{K'}$ surjects onto connected components of X (say Z is a connected component of $X_{K'}$, then $Z \hookrightarrow X_{K'}$ is open and closed, thus $Z \hookrightarrow X_{K'} \to X$ is open and closed, thus the image of Z is open and closed in X, hence a connected component of X).

To conclude the proof, note we assumed X is connected, thus every connected component surjects onto X, which means all connected components have the same K-rational point $x : \operatorname{Spec} K \to X$ in their image. But the base change of this rational point $x_{K'} : \operatorname{Spec} K' \to X$ along $\operatorname{Spec} K' \to \operatorname{Spec} K$ is just a single K'-rational point, thus all the connected components of $X_{K'}$ meet at this single K'-rational point, i.e. $X_{K'}$ is connected.

Proposition 3.1.10

For a group variety G over K, the following are equivalent:

1. *G is connected*
2. *G is geometrically connected*
3. *G is irreducible*
4. *G is geometrically irreducible*

In particular, a connected complete geometrically reduced group variety over K is abelian variety.

Proof. First, we note K-variety with at least one K-rational point is connected iff its geometrically connected (Remark 3.1.9). Thus (1) $\iff$ (2). Every irreducible variety is connected, so it remains to prove (2) $\Rightarrow$ (4). We may assume K is ACF and G connected. By Proposition 3.1.8 shows G is smooth and thus its disjoint union of its irreducible components, i.e. G is irreducible.

Next, as you would guess, we want to study $\mathrm{im}(\phi)$ and $\ker(\phi)$ for $\phi : G \to H$ a homomorphism of group varieties. It can be shown (e.g. you can find this result in SGA) $\mathrm{im}(\phi)$ is a closed subgroup variety of H, but the kernel need more care. To be exact, it will always be a scheme, but its possible to have non-reduced structure, e.g. take $G = H = \mathbb{G}_m$ and $\phi(t) = t^2$, then $\ker(\phi) = \operatorname{Spec} k[t]/(t^2-1)$, where $k[t]/(t^2-1)$ is not a integral domain. However, since all our main results will only concern varieties, we will take

$$\ker(\phi) := \{x \in G(\overline{K}) : \phi(x) = \epsilon_H\}$$

which will be a closed subgroup variety of G.

Theorem 3.1.11: Dimension Theorem

Let $\phi : G \to H$ be a surjective homomorhpism of irreducible group varieties. Then

$$\dim(G) = \dim(H) + \dim(\ker(\phi))$$

This roughly follows from the following: if Y is Noetherian and universally catenary, $f : X \to Y$ surjective morphism of irreducible schemes of finite type, then

$$\dim X = \dim Y + \dim f^{-1}(\eta)$$

where η is the generic point of Y. Using this, and note all fibers of $\phi : G \to H$ are isomorphic to $\ker(\phi)$, we are done.

Lemma 3.1.12

Let R be Noetherian integral domain, A finitely generated R-algebra, and M a finitely generated A-module. Then there is $s \in R\backslash\{0\}$ such that the localization M_s is free R_s-module.

Theorem 3.1.13: Generic Flatness

Let $f : X \to Y$ be quasi-compact morphism locally of finite presentation and assume Y is integral. Let $\mathscr{F}$ be quasi-coherent $\mathscr{O}_X$-module of finite presentation. Then there is open dense $U \subseteq Y$ such that $\mathscr{F}|_{f^{-1}(U)}$ is flat over U.

Proof. The question is local on Y, so we assume $Y = \operatorname{Spec} A$ is affine, where A is integral domain. Since f is quasi-compact, we find open affine fintie cover $X = \bigcup_i U_i$. If we find dense open subsets U of Y as in the theorem for each $U_i \to Y$, then their intersection wil lsatisfy the desired conclusion for f.

Thus we may assume $X = \operatorname{Spec} B$ is affine, and then B is A-algebra of finite presentation, and $\mathscr{F}$ is quasi-coherent $\mathscr{O}_X$-module associated with the B-module $M = \Gamma(X, \mathscr{F})$ of finite presentation. By elimination of Noetherianness, we may assume the situation arises by base change for $A_0 \to A$, where A_0 is a Noetherian subring of A, from an analogous situation over A_0. Over A_0, the conclusion follows from Lemma 3.1.12, and since flatness is stable under base change, we are done.

Corollary 3.1.13.1

Let $f : X \to Y$ be a morphism of finite type and locally of finite presentation, and assume Y is integral. Then there is dense open $U \subseteq Y$ such that $f|_{f^{-1}(U)} : f^{-1}(U) \to U$ is flat.

Proposition 3.1.14

Let $\phi : G \to H$ be surjective homomorphism of irreducible group varieties. Then ϕ is flat. Moreover, if $\dim(G) = \dim(H)$, then ϕ is finite and $|\ker(\phi)|$ is equal the separable degree of the field extension $K(G)$ over $K(H)$.

Proof. By generic flatness (Corollary 3.1.13.1), there is open dense subset U of G such that $\phi|_U$ is flat. Of course, any translate of U is as good as U. Assuming for a moment K is ACF, we may cover G by translates of U. This proves flatness of ϕ. If K is not ACF, we base change to $\overline{K}$, and since flat satisfies fppf descent (actually fpqc descent), see Stack Project, Tag 02YJ, we see ϕ is flat over K iff $\phi_{\overline{K}}$ is flat.

Next, assume $\dim(G) = \dim(H)$, then there is an open dense subset U' of H such that ϕ induces a fintie map $U := \phi^{-1}(U') \to U'$ whose fibers have cardinality equal the separable degree of $K(G)$ over $K(H)$. Also, this cardinality equals $|\ker(\phi)|$. Again, we assume K is ACF to cover G by translates of U proving finiteness of ϕ overall, and if K is not ACF, we can prove this by a base change as we have fppf descent.

A rational curve is a curve birational to $\mathbb{P}^1_K$. A variety is rationally connected if any two points in $X(\overline{K})$ may be connected by a rational curve over $\overline{K}$. It follows from Constancy Lemma 3.1.5 that abelian varieties do not contain rational curves. In particular, a morphism $X \to A$ into abelian variety contracts the rational curves of X to points. It follows that any morphism of a rationally connected variety, such as $\mathbb{P}^n$, into abelian variety is constant.

Proposition 3.1.15

Any morphism $f : \mathbb{P}^1_K \to G$ of the projective line into a group variety is constant.

Proof. Let $(x_0 : x_1)$ be homogeneous coordinates on $\mathbb{P}^1_K$. The map $\mathbb{P}^1 \times \mathbb{A}^1 \to \mathbb{P}^1$ given by $((x_0 : x_1), y) \mapsto (x_0 : (x_1 + x_0 y))$ is a morphism. Now let $f : \mathbb{P}^1 \to G$ be a morphism, we apply Corollary 3.1.5.1 to the composition

$$\mathbb{P}^1 \times \mathbb{A}^1 \xrightarrow{s} \mathbb{P}^1 \xrightarrow{f} G$$

and see $f \circ s$ factors as $f(s(x, y)) = g(x)h(y)$ for two suitable morphisms $g : \mathbb{P}^1 \to G$ and $h : \mathbb{A}^1 \to G$.

We set $y = 0$ and note $s(x, 0) = x$, i.e. $g(x) = f(x)h(0)^{-1}$. Thus

$$f(s(x, y)) = f(x)h(0)^{-1}h(y)$$

Next set $x = \infty$, we see $s(\infty, y) = \infty$ and hence

$$f(\infty) = f(\infty)h(0)^{-1}h(y)$$

This shows $h(y) = h(0)$, i.e. h is a constant map and $f(s(x,y)) = f(x)$. Finally, take $x = 0$ we see $s(0,y) = y$ and so $f(y) = f(0)$.

Corollary 3.1.15.1

Let $U \subseteq \mathbb{P}^1_K$ be open and A be an abelian variety. Then $f : U \to A$ is constant for any f.

Proof. By valuative criterion of properness f extends to a morphism $\mathbb{P}^1 \to A$.

Theorem 3.1.16

Let $\phi : X \dashrightarrow G$ be rational map of smooth X into group variety G and $U_{\max}$ the domain of ϕ. Then every irreducible component of $X \backslash U_{\max}$ is of codimension 1.

Corollary 3.1.16.1

A ratinoal map from a smooth variety to an abelian variety is a morphism.

Proof. Let $\phi : X \dashrightarrow A$ be a rational map with domain $U_{\max}$. By valuative criterion of properness, $X \backslash U_{\max}$ has codimension at least 2. But then we see $U_{\max} = X$ by Theorem 3.1.16.

Our next goal is to prove the differential of multiplication on a group variety is given by addition.

Proposition 3.1.17

Let $m : G \times G \to G$ be multiplication of a smooth group variety G. Then the differential of m at ϵ is the map $T_{G,\epsilon} \oplus T_{G,\epsilon} \to T_{G,\epsilon}$ given by addition of tangent vectors.

Proof. In general we have $T_{X \times X', (x,x')} = T_{X,x} \oplus T_{X',x'}$. Thus $T_{G \times G, (\epsilon,\epsilon)} = T_{G,\epsilon} \oplus T_{G,\epsilon}$. For $\partial \in T_{G,\epsilon}$, we have

$$dm(\partial, 0) = dm \circ d\iota(\partial)$$

where $\iota : G \to G \times G$ is given by $g \mapsto (g, \epsilon)$. Since $dm \circ d\iota = d(m \circ \iota)$, we conclude $dm(\partial, 0) = \partial$. In the same say, we prove $dm(0, \partial) = \partial$. By linearity of dm, this gives the claim.

Corollary 3.1.17.1

Let G be smooth group variety and for $n \in \mathbb{Z}$, let $[n] : G \to G$ be the map $x \mapsto x^n$. Then the differential of $[n]$ at ϵ is the endomorphism of $T_{G,\epsilon}$ given by multiplying tangent vectors with n.

Proposition 3.1.18

Let G be an irreducible smooth group variety. Then the tangent bundle T_G on G is a trivial vector bundle of rank equal $\dim(G)$.

Proof. Let $\partial_\epsilon \in T_{G,\epsilon}$. By translation, we extend ∂_ϵ to a vector field ∂ on G. More precisely, let $\tau_x(y) := yx$ be right translation on G and $\partial_x(f) = \partial_\epsilon(f \circ \tau_x)$ for any $x \in G$ and $f \in \mathcal{O}_{G,x}$. Standard arguments for derivatives show ∂ is a vector field on G. Clearly, linearly independent tangent vectors in ϵ extends to vector fields, which are linearly independent in every fiber.

3.2 Review: Curves and Surfaces

A curve over a field K is a pure dimensional K-variety of dimension 1.

Note any curve K is birational to a regular projective curve over K. To see this, note a disjoint union of projective curves is projective. Hence we may assume C is irreducible. Now passing to open affine then to projective closure, we may assume C is projective. The normalization $\pi : C' \to C$ is a birational fintie morphism. In particular, C' will still be projective, and since normal curve is regular, we are done.

Now, if K is perfect, then a regular curve is smooth. This does not necessarily hold for non-perfect fields. Thus for any curve C over K, $C_{\overline{K}}$ is birational to a smooth projective curve over $\overline{K}$.

We use $\mathcal{K}_C$ to denote the canonical line bundle, which is the dual of the tangent bundle.

Definition 3.2.1

Let C be a geometrically irreducible smooth projective curve over K. We define

the ***genus*** of C to be

$$g(C) = \dim \Gamma(C, K_C)$$

In other words, $g(C)$ is the dimension of the globally defined 1-forms on C. For example, if C is smooth plane curve of degree d (i.e. $C = V(f(x_0, x_1, x_2))$ of some suitable polynomial of degree d), then the genus formula

$$g(C) = \frac{1}{2}(d-1)(d-2)$$

holds.

We see the degree of a zero-dimensional cycle does not depend on its rational equivalence class, thus we see $\deg(\mathscr{L})$ is well-defined.

Theorem 3.2.2: Riemann-Roch

Let $\mathscr{L}$ be a line bundle on the geometrically irreducible smooth projective curve C over K, then

$$\dim \Gamma(C, \mathscr{L}) - \dim \Gamma(C, \mathscr{K}_C \otimes \mathscr{L}^{-1}) = \deg(\mathscr{L}) + 1 - g(C)$$

As an application of this, by setting $\mathscr{L} = \mathscr{K}_C$, we see $\deg(\mathscr{K}_C) = 2g(C) - 2$. Using cohomology, we can reformulate the Riemann-Roch theorem by

$$\chi(\mathscr{L}) = \deg(\mathscr{L}) + 1 - g(C)$$

where $\chi(\mathscr{L}) = H^0(C, \mathscr{L}) - H^1(C, \mathscr{L})$ is the Euler characteristic of $\mathscr{L}$. To see this, just note by Serre duality, $H^1(C, \mathscr{L})$ is the dual space of $H^0(C, \Omega_C^1 \otimes \mathscr{L}^{-1})$.

Remark 3.2.3

Let C be a smooth geometrically irreducible projective curve over K and $\mathscr{L}$ a line bundle on C. Then $\mathscr{L}$ is ample if and only if $\deg(\mathscr{L}) > 0$. If $\deg(\mathscr{L}) \geq 2g(C) + 1$, then $\mathscr{L}$ is very ample.

3.3 Elliptic Curves

By Proposition 3.1.18, the cotangent bundle of an abelian variety over K is trivial. Thus an abelian variety of dimension 1 has genus 1, i.e. is an elliptic curve. In this section, we prove the converse, i.e. elliptic curve has a group structure and is an abelian variety.

Definition 3.3.1

An ***elliptic curve*** over K is a geometrically irreducible smooth projective curve E of genus $g(E) = 1$, equipped with a rational point $P_0 \in E(K)$.

Note geometrically irreducible is the same as irreducible for us, since we have at least one K-rational point. Let E be elliptic curve over K and D be a divisor on $E_{\overline{K}}$ of degree $\deg(D) > 0$. The space of global sections $\Gamma(E_{\overline{K}}, \mathscr{O}(D))$ may be realized as the subspace

$$\overline{\mathscr{L}}(D) := \{f \in \overline{K}(E_{\overline{K}})^\times : \div(f) \geq -D\} \cup \{0\}$$

in $\overline{K}(E_{\overline{K}})$, using the homomorphism $s \mapsto s/s_D$. By Riemann-Roch, we see

$$\dim_{\overline{K}} \overline{\mathscr{L}}(D) = \deg(D) \tag{Eq. 3.3.1}$$

hence the corresponding linear system $|D_{\overline{K}}|$ has dimension $\deg(D) - 1$. It follows that two distinct points (viewed as Weil divisors) on E are rationally equivalent over $\overline{K}$.

Let us fix a base point $P_0 \in E(K)$. For two point $P_1, P_2 \in E(\overline{K})$, let $D := [P_1] + [P_2] - [P_0]$. Thus $\deg(D) = 1$ and $\overline{\mathscr{L}}(D)$ is one-dimensional, generated by a function f, unique up to multiplication by a scalar. By construction, if $P_0 \notin \{P_1, P_2\}$, then f has pole divisor $[P_1] + [P_2]$ and vanishes at P_0 and at exactly one other point P_3 (this one extra point is because $\dim(\overline{\mathscr{L}}(D)) = 1$), which is the unique point rationally equivalent to $[P_1] + [P_2] - [P_0]$. This make sense even if P_1 or P_2 equals P_0. Thus we get a well-defined composition law on E by $(P_1, P_2) \mapsto P_1 + P_2 := P_3$.

We should distinguish carefully between addition of points P_1, P_2 on E and of the corresponding divisors $[P_1], [P_2]$. Remembering that $\mathrm{Pic}^0(E_{\overline{K}})$ is the group of rational equivalence classes of divisors of degree 0, we get an additive map

$$E \to \mathrm{Pic}^0(E_{\overline{K}}), \quad P \mapsto [P] - [P_0]$$

By Eq. 3.3.1 this map is bijective. We will later give more geometric interpretation of the addition rule.

Proposition 3.3.2

If the group structure on an elliptic curve E over K with base point P_0 is given by bijective map

$$E \to \mathrm{Pic}^0(E_{\overline{K}}), \quad P \mapsto [P] - [P_0]$$

then E is an abelian variety defined over K.

We will prove this result throughout the section, as we gain more understanding of elliptic curves.

Now let us first give a classical argument showing E has a model given by a smooth cubic curve. Let us realize $\Gamma(E, \mathscr{O}(D))$ via

$$\mathscr{L}(D) = \{f \in K(E)^\times : \div(f) \geq -D\} \cup \{0\}$$

for any divisor D on E. If $\deg(D) > 0$, then by Riemann-Rock, $\mathscr{L}(D)$ has dimension $\deg(D)$. We have an ascending chain of K-vector spaces

$$\mathscr{L}([P_0]) \subseteq \mathscr{L}(2[P_0]) \subseteq \ldots \subseteq \mathscr{L}(6[P_0])$$

and the jth member has dimension j.

Clearly 1 is a basis of $\mathscr{L}([P_0])$. Since P_0 is defined over K, there are $x, y \in K(E)$ such that $1, x$ is a basis of $\mathscr{L}(2[P_0])$ and $1, x, y$ is a basis of $\mathscr{L}(3[P_0])$. By looking at the order of pole at P_0, its clear $1, x, y, x^2$ is a basis of $\mathscr{L}(4[P_0])$ and $1, x, y, x^2, xy$ is a basis of $\mathscr{L}(5[P_0])$. Moreover, $x^3, y^2 \in \mathscr{L}(6[P_0])$. This gives 7 elements $1, x, y, x^2, xy, x^3, y^2$ spanning $\mathscr{L}(6[P_0])$, where $\dim \mathscr{L}(6[P_0]) = 6$. Thus there must be $c_i \in K$ so

$$c_0 + c_1 x + c_2 y + c_3 x^2 + c_4 xy + c_5 x^3 + c_6 y^2 = 0$$

By the above, c_5 and c_6 are different from 0, so that we may normalize $c_5 = -1$. If we divide by c_6^3 and replace x by x/c_6 and y by y/c_6^2, we get a relation of the form

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \qquad \text{(Eq. 3.3.2)}$$

with $a_i \in K$. Since $\deg(3[P_0]) = 3 = 2g(E)+1$, the divisor $3[P_0]$ is very ample. Hence the basis of $\mathscr{L}(3[P_0])$ corresponding to $1, x, y$ induces a closed embedding of E into $\mathbb{P}^2_K$. We know by Eq. 3.3.2 that the image of E is contained in the projective curve with ***Weierstrass equation***

$$x_0 x_2^2 + a_1 x_0 x_1 x_2 + a_3 x_0^2 x_3 = x_1^3 + a_2 x_0 x_1^2 + a_4 x_0^2 x_1 + a_6 x_0^3$$

in the homogeneous coordinates $(x_0 : x_1 : x_2)$ of $\mathbb{P}^2_K$.

It is easy to prove the curve defined above is geometrically irreducible, hence it gives a projective model of E as a smooth plane cubic curve. Note also that the ratinoal functions $x = x_1/x_0$ and $y = x_2/x_0$ are nothing else than the two functions x, y defined before, hence the affine form Eq. 3.3.2 of the Weierstrass equation describes the affine curve $E \cap \{x_0 \neq 0\}$. The only point of E outside this part is the point $(0 : 0 : 1) \in \mathbb{P}^2_K$, corresponding to $P_0 \in E$. It is easily seen that, in this model, P_0 is an inflexion point of E.

Remark 3.3.3

If $\mathrm{char}(K) \neq 2$, then replacing y by $\frac{1}{2}(y - a_1 x - a_3)$ leads to a Weierstrass equation with $a_1 = a_3 = 0$, i.e. we get

$$y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6$$

where

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1 a_3, \quad b_6 = a_3^2 + 4a_6$$

Then the Jacobi criterion shows a Weierstrass equation describes a smooth curve C in $\mathbb{P}^2_K$ if and only if the discriminant of the cubic polynomial $x^3 + a_2 x^2 + a_4 x + a_6$ is not zero. By the genus formula

$$g(C) = \frac{1}{2}(\deg(C) - 1)(\deg(C) - 2)$$

this is an elliptic curve. If in addition $\mathrm{char}(K) \neq 3$, then a further linear transformation $(x, y) \mapsto (\frac{x - 3b_2}{36}, \frac{y}{108})$ leads to the Weierstrass short form

$$y^2 = x^3 - 27c_4 x - 54c_6$$

where

$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6$$

Now let us go back to any characteristic. We will describe a more explicit group structure on the abelian group E, beginning by proving the inverse operation is a morphism.

Consider the rational equivalence relation

$$[P_1] + [P_2] + [P_3] \sim 3[P_0] \tag{Eq. 3.3.3}$$

on $E_{\overline{K}}$. This relation is equivalent to the geometric statement that the points P_1, P_2, P_3 are the three intersection points, counted with multiplicity, of a straight line with E. We verify this as follows. The lines in $\mathbb{P}^2_{\overline{K}}$ are just the divisors of the global sections of $\mathscr{O}_{\mathbb{P}^2_{\overline{K}}}(1)$ and, by construction, the restriction of this line bundle to E is isomorphic to $\mathscr{O}(3[P_0])$. First, we assume $[P_1]+[P_2]+[P_3] \sim 3[P_0]$, then there is $s' \in \Gamma(E_{\overline{K}}, \mathscr{O}(3[P_0]))$ with $\div(s') = [P_1] + [P_2] + [P_3]$. By construction of the embedding $E \hookrightarrow \mathbb{P}^2_{\overline{K}}$, there is $s \in \Gamma(\mathbb{P}^2_{\overline{K}}, \mathscr{O}_{\mathbb{P}^2_{\overline{K}}(1)})$ with $s' = s|_E$. Then the line $\ell = \div(s)$ is the line through the three points P_i. Indeed, by definition of proper intersection product, we have

$$\ell \cdot E = \div(s|_E) = \div(s') = [P_1] + [P_2] + [P_3]$$

The converse is proved the same way by reversing the previous argument.

The zero element of E is $P_0 = (0:0:1)$. The inverse $P_2 := -P_1$ of a point $P_1 \in E$ is characterized by the rational equivalence $[P_1] + [P_2] \sim 2[P_0]$, which can be rewritten as the special case

$$[P_0] + [P_1] + [P_2] \sim 3[P_0]$$

of Eq. 3.3.3. It follows P_0, P_1, P_2 are on a straight line and in fact, noting $P_0 = (0:0:1)$, we see that, if $P_1 \neq P_0$, then P_2 is the residual finite intersection of E with the vertical line in (x, y)-plane going through P_1. If (x_1, y_1) are the affine coordinates of P_1, then, using Eq. 3.3.2, the affine coordinates (x_2, y_2) of P_2 are given by

$$x_2 = x_1, \quad y_2 = -a_1x_1 - a_3 - y_1$$

Thus the inverse map is an automorphism of the affine part of E defined over K. On the other hand, a rational map of a smooth projective curve is always a morphism. We conclude the above restriction extends to an automorphism of E. This requires 0 map to 0, hence the inverse map is a morphism on E defined over K.

Now we study the addition on the elliptic curve a bit closer. By the above, it is enough to construct

$$P_3 = -(P_1 + P_2)$$

The point P_3 is characterized by the rational equivalence Eq. 3.3.3. As we have seen above, P_3 is the third intersection point of the line ℓ through P_1 and P_2 with E, taking this line to be the tangent line to E at P_1 if $P_1 = P_2$.

If $P_1 \neq P_0$ and $P_2 \notin \{P_0, -P_1\}$, then the third intersection point of the line through P_1, P_2 with E is contained in the (x, y)-plane. Let $y = ax + b$ be the equation for this line. We eliminate y in Eq. 3.3.2 obtaining a cubic equation for x, with two known solutions x_1, x_2. This equation has the form

$$x^3 - (a^2 + a_1a - a_2)x^2 + \text{ lower degree terms} = 0$$

The third solution x_3 is determined by the trace $x_1 + x_2 + x_3 = a^2 + a_1 a - a_2$. Since $P_1 + P_2 = -P_3$, applying the inverse as above, we conclude the following result.

Proposition 3.3.4: Addition Law

Let E be the elliptic curve in normal form

$$y^2 = a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

Then the origin O of the group E is the unique point at infinity and the group law $+$ is defined as follows. Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ be two finite points on E and set

$$a = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } x_1 \neq x_2 \\ \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3} & \text{otherwise} \end{cases}$$

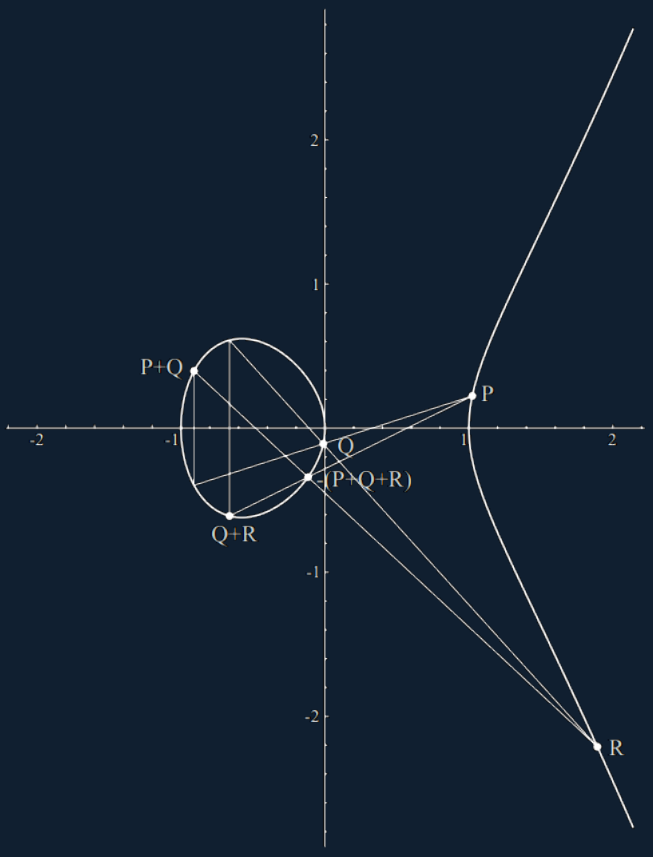
$$b = y_1 - a x_1$$

Then:

1. *The inverse of P_1 is given by $-P_1 = (x_1, -a_1 x_1 - a_3 - y_1)$*
2. *If $x_2 = x_1$ and $y_2 = -a_1 x_1 - a_3 - y_1$, then $P_1 + P_2 = O$*
3. *Otherwise, we have*

$$P_1 + P_2 = (a^2 + a_1 a - a_2 - x_1 - x_2, -(a + a_1)(a^2 + a_1 a - a_2 - x_1 - x_2) - a_3 - b)$$

The addition law can be seen visually as the following:



The addition law shows that addition is a rational map. In order to finish proof of Proposition 3.3.2, it remains to show $+$ is a morphism. To show rational map extends to a morphism, it suffices to prove that over $\overline{K}$. In a first step, we show translation τ_Q by $Q \in E$ is a morphism. We may assume $Q \neq O$. By the formulae in Proposition 3.3.4, τ_Q is a rational map which restricts to a morphism $E\backslash\{O,Q,-Q\} \to E\backslash\{Q,O,Q+Q\}$. Since every rational map between projective smooth curves extends to a morphism (valuative criterion), we get a morphism $\tau'_Q : E \to E$ which agrees with τ_Q on $E\backslash\{O,Q,-Q\}$. It remains to prove $\tau_Q = \tau'_Q$. For $R \in E$, we see $\tau'_Q \circ \tau'_R = \tau'_{Q+R}$. In particular, every τ'_Q is an isomorphism with inverse τ'_{-Q}. Thus τ'_Q maps $\{O,Q,-Q\}$ onto $\{Q,Q+Q,O\}$. For any $R \notin \{O,Q,-Q,Q+Q,-Q-Q\}$ we have

$$\tau'_R(\tau'_Q(Q)) = \tau'_{Q+R}(Q) = \tau'_Q(\tau'_R(Q)) = \tau'_Q(Q+R) = Q+Q+R$$

This excludes $\tau'_Q(Q) = Q$ immediately. On the other hand, we know $\tau'_R(O) \in \{O,R,R+R\}$, hence $\tau'_Q(Q) = O$ is only possible if $Q+Q = O$. This proves

$$\tau'_Q(Q) = Q+Q = \tau_Q(Q)$$

The equation

$$\tau'_Q(-Q) = O = \tau_Q(-Q)$$

is proved in a similar fashion. Thus, using that τ'_Q is a bijection, we conclude $\tau'_Q(O) = Q = \tau_Q(O)$. We have handled all exceptions, thereby proving $\tau_Q = \tau'_Q$.

Next we show addition is a morphism. The formulae in Proposition 3.3.4 show that addition is a rational map m, which is a morphism outside

$$Z := \{(P,P) : P \in E\} \cup \{(P,-P) : P \in E\} \cup (E \times \{O\}) \cup (\{O\} \times E)$$

For $(P,Q) \in Z$, there are $R,S \in E$ such that $(P+R,Q+S) \notin Z$. Since translations are morphisms, we see

$$\tau_{-P-Q} \circ m \circ (\tau_R \times \tau_S)$$

is a morphism in a neighbourhood of (P,Q) and agrees with $+$ everywhere. This proves $+$ is a morphism.

Remark 3.3.5

Complex analytically, an elliptic curve is biholomorphic to $\mathbb{C}/\Lambda$ where Λ is a lattice in $\mathbb{C}$. In dimension 1 the converse is true, i.e. every one-dimensional complex torus is biholomorphic to an abelian variety. The description of the elliptic curve determined by $\mathbb{C}/\Lambda$ is done quite explicitly by means of Weierstrass $\wp$-function associated to the lattice Λ, namely

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda\backslash\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

It is Λ-periodic meromorphic function on $\mathbb{C}$ with double periods at lattice points. In particular it satisfies the first-order differential equation

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$$

where

$$g_2 = 60 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^4}, \quad g_3 = 140 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^6}$$

The map $z \mapsto (\wp(z), \wp'(z))$ is biholomorphic from $\mathbb{C}/\Lambda$ onto the elliptic curve with affine Weierstrass equation $y^2 = 4x^3 - g_2 x - g_3$.

3.4 The Picard Variety

Elliptic curves are the only standard explicit examples of abelian varieties. This is because higher-dimensional abelian varieties can be defined only by means of a very large number of equations, and little can be understood by just looking at the equations.

For example, in Flynn's paper "The Jacobian and Formal Group of a Curve of Genus 2 over an Arbitrary Ground Field", they wrote down a set of defining equations for a 2 dimensional abelian variety, which contains 72 equations, and they look like

$$\begin{aligned}
&a_0 a_3 = a_1 a_1 - a_5^2 f_0 - a_3^2 f_4 + 4a_4 a_{13} f_0 f_5 + a_5 a_{10} f_1 f_5 + 8a_4 a_{10} f_1 f_6 + a_3 a_{10} (4f_2 f_6 - \\
&f_3 f_5) + 8a_4 a_{11} f_0 f_6 + 2a_{13} a_{15} f_0 f_1 f_5 + a_{10} a_{15} \left(4f_0 f_2 f_6 + 2f_0 f_3 f_5 + 3f_1^2 f_6\right) + \\
&4a_{11} a_{15} f_0 f_1 f_6 + 2a_{10} a_{13} \left(f_0 f_5^2 + 3f_1 f_3 f_6\right) + 8a_{11} a_{13} f_0 f_3 f_6 + \\
&a_{10}^2 \left(4f_1 f_5 f_6 + 4f_2 f_4 f_6 - f_2 f_5^2 - f_3^2 f_6\right) + a_{10} a_{11} \left(4f_0 f_5 f_6 + 4f_1 f_4 f_6 - f_1 f_5^2\right) \\
&+ a_{11}^2 f_0 \left(4f_4 f_6 - f_5^2\right)
\end{aligned}$$

The above is just one equation.

However, abelian varieties are ubiquitous in algebraic geometry and they occur most naturally through the Picard variety, which we will study here.

Let us fix a ground field K and algebraic closure $\overline{K}$.

If $\phi : X \to Y$ is a morphism of varieties over K and $y \in Y$, then the fiber of ϕ over y is denoted by X_y. The pullback of $\mathscr{L} \in \mathrm{Pic}(X)$ to the fiber X_y is denoted $\mathscr{L}_y$. Its an element of $\mathrm{Pic}(X_y)$. Note X_y and $\mathscr{L}_y$ are only defined over $\kappa(y)$. Often we identify X with X_y using the map $x \mapsto (x, y)$, which is only defined over $\kappa(y)$.

In the following, we consider $\mathscr{L} \in \mathrm{Pic}(X \times Y)$ and the fibers with respect to the projections p_1, p_2 onto the factors. For $x \in X, y \in Y$, we have

$$\mathscr{L}_y = \mathscr{L}|_{X \times \{y\}} \in \mathrm{Pic}(X_{\kappa(y)}), \quad \mathscr{L}_x = \mathscr{L}|_{\{x\} \times Y} \in \mathrm{Pic}(Y_{\kappa(x)})$$

Theorem 3.4.1: Seesaw Principle

Let X be a geometrically irreducible smooth complete variety over K and Y an irreducible smooth variety over K. Let $\mathscr{L} \in \mathrm{Pic}(X \times Y)$ and suppose there is dense open $U \subseteq Y$ so $\mathscr{L}_y = 0$ for all $y \in U$. Then $\mathscr{L}$ is equal to the pullback of an element of $\mathrm{Pic}(Y)$ by p_2.

This result holds even without the smoothness assumption. We often use this principle in the following form.

Corollary 3.4.1.1

Let X, Y be smooth varieties over K and assume Y is irreducible and that X is complete and geometrically irreducible. Let $\mathscr{L} \in \mathrm{Pic}(X \times Y)$ with $\mathscr{L}_y = 0$ for all y in an open dense subset of Y and with $\mathscr{L}_x = 0$ for all $x \in X(K)$. Then $\mathscr{L} = 0$.

Proof. By Theorem 3.4.1, we have $\mathscr{L} = p_2^*\mathscr{L}'$ for some $\mathscr{L}' \in \mathrm{Pic}(Y)$. Now consider the closed embedding $\iota_x : Y \to X \times Y$, $y \mapsto (x, y)$. Since $p_2 \circ \iota_x$ is the identity map on Y, we see

$$\mathscr{L}' = \iota_x^* p_2^* \mathscr{L}' = \mathscr{L}_x = 0$$

Since this holds for all x, we are done.

Corollary 3.4.1.2

Let A be abelian variety over K, p_i the ith projection $A \times A$ onto A, and m be addition as usual. The following are equivalent for $\mathscr{L} \in \mathrm{Pic}(A)$:

1. $m^*(\mathscr{L}) = p_1^*\mathscr{L} + p_2^*\mathscr{L}$
2. $\tau_a^*(\mathscr{L}) = \mathscr{L}$ *for all* $a \in A$

If (1) or (2) holds, then $[-1]^*(\mathscr{L}) = -\mathscr{L}$.

Proof. The equivalence is a consequence of

$$(m^*(\mathscr{L}) - p_1^*(\mathscr{L}) - p_2^*(\mathscr{L}))|_{A \times \{a\}} = \tau_a^*(\mathscr{L}) - \mathscr{L}$$

and the seesaw principle from Corollary 3.4.1.1. If we pullback equation in (1) by the morphism

$$A \to A \times A, \quad a \mapsto (a, -a)$$

then we get $[-1]^*(\mathscr{L}) = -\mathscr{L}$.

Theorem 3.4.2: Poincaré

There is a subfamily $\mathscr{P}$ of $\mathrm{Pic}^0(X)$, parametrized by an irreducible smooth complete variety B, with the following universal property. For any subfamily $\mathscr{L}$ of $\mathrm{Pic}^0(X)$, parametrized by an irreducible variety T, there is a unique morphism $\phi : T \to B$ with $(\mathrm{Id}_X \times \phi)^*(\mathscr{P}) = \mathscr{L}$.

The variety B is called the Picard variety of X and $\mathscr{P}$ is called the ***Poincaré*** class. If $(B', \mathscr{P}')$ is another such pair, then we have $\phi : B' \to B$ and $\phi' : B \to B'$ such that $\phi \circ \phi' = \mathrm{Id}_B$ by uniqueness, and similarly $\phi' \circ \phi = \mathrm{Id}_{B'}$. In other words, $(B, \mathscr{P})$ is uniquely determined.

The proof of this result is beyond the scope of this note, but it follows from the existence of Picard scheme.

We will denote the Picard variety of X by $\mathcal{P}\mathrm{ic}^0(X)$, and will show the F-rational point of Picard variety may be identified with $\mathrm{Pic}^0(X_F)$ for any extension F/K. From this, we see byu taking $X = E$ for some elliptic curve over non-algebraically closed field, it is easy to choose a divisor of degree 0 which is not invariant under $\mathrm{Gal}(\overline{K}/K)$, and hence not defined over K. This shows $\mathcal{P}\mathrm{ic}^0(X)$ has more points than $\mathrm{Pic}^0(X)$.

Corollary 3.4.2.1

Let F/K be field extension, then:

1. *By base change, we have $\mathrm{Pic}(X) \subseteq \mathrm{Pic}(X_F)$*
2. *$\mathcal{P}\mathrm{ic}^0(X_F) = \mathcal{P}\mathrm{ic}^0(X)_F$ and its Poincaré class is obtained from $\mathscr{P}$ by base change to F*
3. *$\mathcal{P}\mathrm{ic}^0(X)(F) = \mathrm{Pic}^0(X_F)$ by identifying b with $\mathscr{P}_b$*

Remark 3.4.3

By the seesaw principle as in Corollary 3.4.1.1 and Corollary 3.4.2.1, the Poincaré class $\mathscr{P}$ is uniquely characterized by the conditions:

1. $\mathscr{P}_{\mathscr{L}} = \mathscr{L}$ for any $\mathscr{L} \in \mathcal{P}\mathrm{ic}^0(X)$, i.e. the fiber of $\mathscr{P}$ at any degree 0 line bundle is just that line bundle itself
2. $\mathscr{P}_{P_0} = 0$

Note that, in the situation of Theorem 3.4.2, the morphism ϕ is given by

$$\phi(t) = \mathscr{L}_t = \mathscr{P}_{\phi(t)}$$

This is clear by restriction of $(\mathrm{Id}_X \times \phi)^*(\mathscr{P}) = \mathscr{L}$ to the fiber $X \times \{t\}$ and then using the rule $(f \circ g)^* = g^* \circ f^*$ to show that

$$\mathscr{L}_t = (\mathrm{Id}_X \times \phi)^*(\mathscr{P})|_{X \times \{t\}}(\mathrm{Id}_X \times \phi(t))^*(\mathscr{P}) = \mathscr{P}_{\phi(t)} = \phi(t)$$

Theorem 3.4.4

Together with its canonical group structure induced by tensor product of line bundles, $\mathcal{P}\mathrm{ic}^0(X)$ is an abelian variety over K.

Proof. Its enough to show $B = \mathcal{P}\mathrm{ic}^0(X)$ is a group variety, then use the fact B is smooth and Proposition 3.1.10. Let p_1, p_2 be the projections of $X \times B \times B \to X \times B$. For $\mathscr{L} = p_1^*\mathscr{P} + p_2^*\mathscr{P}$ and $\mathscr{A}, \mathscr{B} \in B$, the restriction of $\mathscr{L}$ to the fiber $X \times \{\mathscr{A}\} \times \{\mathscr{B}\}$ is

equal $\mathscr{A}+\mathscr{B}$. In order to see this, note the restriction of $p_1^*\mathscr{P}$ is equal the restriction of $\mathscr{P}$ to $X\times\{\mathscr{A}\}$ and then use Remark 3.4.3, we obtain

$$m(\mathscr{A},\mathscr{A}) = \mathscr{P}_{m(\mathscr{A},\mathscr{B})} = \mathscr{L}_{(\mathscr{A},\mathscr{B})} = \mathscr{A}+\mathscr{B}$$

and so addition is a morphism. Let $\iota : B \to B$ be the unique morphism with

$$(\mathrm{Id}_X \times \iota)^*(\mathscr{P}) = -\mathscr{P}$$

We get similarly

$$\iota(\mathscr{B}) = \mathscr{P}_{\iota(\mathscr{B})} = -\mathscr{P}_{\mathscr{B}} = -\mathscr{B}$$

so the inverse is also a morphism.

We summarize our results as follows.

Theorem 3.4.5

Let X be an irreducible smooth complete variety over K and $P_0 \in X(K)$ a base point of X. Then the group $\mathrm{Pic}^0(X_{\overline{K}})$ has a unique structure as an abelian variety over K, called the Picard variety and denoted by $\mathcal{P}\mathrm{ic}^0(X)$, with the properties:

1. *There is $\mathscr{P} \in \mathrm{Pic}(X \times \mathcal{P}\mathrm{ic}^0(X))$ such that $\mathscr{P}_{\mathscr{B}} = \mathscr{B}$ for $\mathscr{B} \in \mathcal{P}\mathrm{ic}^0(X)$ and $\mathscr{P}_{P_0}$ is trivial*
2. *For any subfamily $\mathscr{L}$ of $\mathrm{Pic}^0(X)$ parametrized by an irreducible variety T over K, the set-theoretic map*

$$T \to \mathcal{P}\mathrm{ic}^0(X), \quad t \mapsto \mathscr{L}_t$$

is actually a morphism over K.

The uniquely determined class $\mathscr{P}$ is called the ***Poincaré class****.*

Now given $\phi : X \to X'$ a pointed morphism between complete smooth variety over K with base point $P_0 \in X(K)$ and $P_0' \in X'(K)$ respectively (i.e. we require $\phi(P_0) = P_0'$). Then the map

$$\hat{\phi} : \mathcal{P}\mathrm{ic}^0(X') \to \mathcal{P}\mathrm{ic}(X), \quad \mathscr{L}' \mapsto \phi^*\mathscr{L}'$$

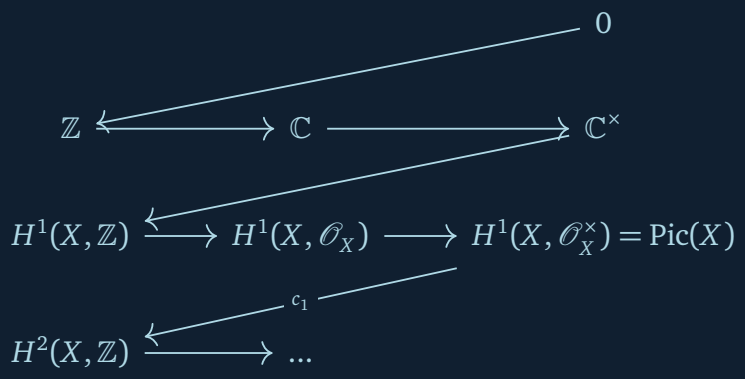
is called the dual map of ϕ, which is a homomorphism of abelian varieties.

Remark 3.4.6

In the complex analytic situation, take X be irreducible proper smooth complex variety viewed as a compact connected complex manifold. View the transition functions $(g_{\alpha,\beta})$ for a line bundle $\mathscr{L}$ on X as a Čech cocycle valued in $\mathscr{O}_X^\times$, we see $\mathrm{Pic}(X) = H^1(X, \mathscr{O}_X^\times)$. Now consider the exponential map short exact sequence

$$0 \to \mathbb{Z}_X \to \mathscr{O}_X \xrightarrow{\exp} \mathscr{O}_X^\times \to 0$$

Now take cohomology long sequence, we get



where c_1 gives the first Chern class of line bundles. A line bundle is equivalent to 0 if and only if $\mathscr{L}$ has (first) Chern class 0. If we use canonical isomorphism

$$H^1(X,\mathscr{O}_X) \cong H^{0,1}(X)$$

from Dolbeault complex, we conclude the Picard variety is biholomorphic to the complex torus $H^{0,1}(X)/H^1(X,\mathbb{Z})$.

3.5 The Theorem of Square

In the above, we defined the Picard variety $\mathcal{P}\mathrm{ic}^0(X)$ of irreducible smooth complete variety X with K-rational base point. In this section, we assume X is abelian variety over K and the base point is the origin.

Definition 3.5.1

Let A be smooth complete abelian variety, then $\mathcal{P}\mathrm{ic}^0(A)$ is called the ***dual abelian variety*** of A and denoted by $\hat{A}$.

The theorem of square says for any $\mathscr{L} \in \mathrm{Pic}(A)$, the point $\phi_{\mathscr{L}}(a) := \tau_a^*(\mathscr{L}) - \mathscr{L}$ is in $\hat{A}$ and additive in $a \in A$. Over $\mathbb{C}$, its clear that the translated $\tau_a^*(\mathscr{L})$ is algebraically equivalent to $\mathscr{L}$ using a path from 0 to a for the deformation. In the special case of an elliptic curve E with origin P_0 and divisor D we have

$$\tau_p^*(D) \sim D - [P] + [P_0]$$

and the theorem of the square is evident from $[P]-[P_0]$ algebraically equivalent to 0 and $[P+Q] \sim [P]+[Q]-[P_0]$.

As a consequence of the theorem of the square, we will prove that an abelian variety is always projective. If $\mathscr{L}$ is ample, we will see $\phi_{\mathscr{L}}$ is surjective and has finite kernel, thus $\hat{A}$ has the same dimension as A.

Theorem 3.5.2

Let $\mathscr{L} \in \mathrm{Pic}(A)$ and $a \in A$. Then $\phi_{\mathscr{L}}(a) := \tau_a^*(\mathscr{L}) - \mathscr{L} \in \mathcal{P}\mathrm{ic}^0(A)(\kappa(a))$ and $\phi_{\mathscr{L}} : A \to \mathcal{P}\mathrm{ic}^0(A)$ is a homomorphism of abelian varieties over K.

Proof. Let p_i be the ith projection of $A \times A$ onto A and consider

$$\mathscr{L}' = m^*(\mathscr{L}) - p_1^*(\mathscr{L}) - p_2^*(\mathscr{L})$$

on $A \times A$. We already remarked in the proof of Corollary 3.4.1.2 that

$$\mathscr{L}'|_{A\times\{a\}} = \tau_a^*(\mathscr{L}) - \mathscr{L}$$

for $a \in A$. Thus $\phi_{\mathscr{L}}(a) \in \mathrm{Pic}^0(A_{\kappa(a)}) = \mathcal{P}\mathrm{ic}^0(A)(\kappa(a))$ by the definition of algebraic equivalence and Corollary 3.4.2.1. Since $\mathscr{L}'|_{\{0\}\times A} = 0$, $\mathscr{L}'$ is a subfamily of $\mathrm{Pic}^0(A)$ parametrized by A. Theorem 3.4.5 shows $\phi_{\mathscr{L}}$ is a morphism of varieties defined over K. Since $\phi_{\mathscr{L}}(0)$ is trivial, the map is a homomorphism of abelian varieties (Corollary 3.1.5.2).

Theorem 3.5.3: Theorem of Square

For $a, b \in A$, we have

$$\tau_{a+b}^*(\mathscr{L}) + \mathscr{L} = \tau_a^*(\mathscr{L}) + \tau_b^*(\mathscr{L})$$

Proof. Apply Theorem 3.5.2, then subtract $2\mathscr{L}$ on both side.

Theorem 3.5.4

Let $\mathscr{B} \in \mathrm{Pic}(A)$ such that $\phi_{\mathscr{B}} = 0$. Then for any ample $\mathscr{L} \in \mathrm{Pic}(A)$, there is some $a \in A$ with

$$\mathscr{B} = \tau_a^*(\mathscr{L}) - \mathscr{L}$$

Remark 3.5.5

The kernel of $\phi_{\mathscr{L}}$ gives much information about $\mathscr{L}$. If $\mathscr{L}$ is ample, then the kernel is finite. We will prove a partial converse of this statement, which we will use later. On the other hand, $\ker(\phi_{\mathscr{L}}) = A$ if $\mathscr{L} \in \mathrm{Pic}^0(A)$. These statements about kernel will be proved next.

Fact 3.5.6: Ample $\mathscr{L} \cong \mathscr{O}_X$ means X affine

We first recall the following result. Let X be qcqs scheme, the following are equivalent:

1. X is quasi-affine
2. There is line bundle $\mathscr{L}$ such that $\mathscr{L}$ and $\mathscr{L}^{-1}$ are ample
3. Every quasi-coherent $\mathscr{O}_X$-module is generated by its global sections
4. The canonical morphism $X \to \operatorname{Spec}(\Gamma(X, \mathscr{O}_X))$ is quasi-compact open schematically dominant immersion.

Now, we claim if X proper variety over k, $\mathscr{L}$ ample line bundle with $\mathscr{L} \cong \mathscr{O}_X$, then X is affine. To see this, by assumption and the result above we see $X \to \operatorname{Spec}\Gamma(X, \mathscr{O}_X)$ is open immersion. Now X is also proper, which means $X \to \operatorname{Spec}\Gamma(X, \mathscr{O}_X)$ is closed. Thus X must be affine as desired. In particular, note X proper and affine means X is finite.

Proposition 3.5.7

A class $\mathscr{L} \in \operatorname{Pic}(A)$ is ample if and only if $\ker(\phi_{\mathscr{L}})$ is finite and $H^0(A, \mathscr{L}^n) \neq 0$ for some $n > 0$.

Proof. Assume $\mathscr{L}$ is ample. Let B be the connected component of the closed subgroup $\ker(\phi_{\mathscr{L}})$ containing 0. For $b \in B$ we have

$$\tau_v^* \mathscr{L} = \mathscr{L}$$

and hence

$$[-1]^*(\mathscr{L}|_B) = -\mathscr{L}|_B$$

by Corollary 3.4.1.2. Since

$$0_B = \mathscr{L}|_B + [-1]^*(\mathscr{L}|_B)$$

is ample, B has to be the trivial abelian subvariety $\{0\}$ (using the fact A is complete and then Fact 3.5.6). Thus $\ker(\phi_{\mathscr{L}})$ is finite. Choose n so large that $\mathscr{L}^n$ is very ample, which gives $H^0(A, \mathscr{L}^n) \neq 0$.

In the other direction, we may assume $H^0(A, \mathscr{L}) \neq 0$, i.e. there is an effective divisor D so $\mathscr{O}(D) \cong \mathscr{L}$. Thus Lemma 3.5.8 shows $\mathscr{L}$ is ample.

Lemma 3.5.8

Let D be effective divisor on A and suppose the subgroup $\{a \in A : \tau_a^*(D) = D\}$ is finite. Then D is ample on A.

Proof. Note D is ample iff $D_{\overline{K}}$ is ample over $A_{\overline{K}}$. Thus we assume K is ACF. The proof then proceeds by proving first the linear system $|2D|$ is base-point free and define a morphism ϕ of A into some projective space. Then we show ϕ is finite morphism and the conclusion comes by pullback. The details are as follows.

Let $a, b \in A$. If b is in the support of the effective divisor

$$E_a := \tau_a^*(D) + \tau_{-a}^*(D)$$

then $a+b$ or $b-a$ is in the support of D. For any given $b \in A$ we can always find $a \notin (D-b) \cup (b-D)$, i.e. $b \notin \operatorname{supp}(E_a)$. Then by the theorem of the square 3.5.3 the effective divisor E_a is an element of $|2D|$. Thus the linear system $|2D|$ is base-point free and thus defines a morphism $\phi : A \to \mathbb{P}^n_K$.

The morphism ϕ is proper. Let F be an irreducible component of any fiber. All elements of $|2D|$ are pullbacks of hyperplanes by the definition of ϕ. Now for any $a \in A$ either F is contained in the support of E_a or $F \cap \operatorname{supp}(E_a) = \emptyset$, hence we can find $a \in A$ so F and the support of E_a are disjoint, i.e. $a \notin \operatorname{supp}(D) - F$. Let Z be an irreducible component of D, then $Z - F$ is irreducible closed subset of A not containing a. We conclude $Z - F$ is of codimension 1. Now note for any $b \in F$, we have

$$Z - F = Z - b$$

whence it follows Z is invariant by translation in $F - F$. Therefore, the same is true for D instead of Z. By assumption, this is only possible for $\dim(F) = 0$ and we conclude ϕ has finite fiber. Thus, since ϕ is proper, it must also be finite (finite fiber=quasi-fintie, proper+quasi-finite means finite). Now recall pullback of ample by finite morphism is ample, we see $2D$ is ample.

Corollary 3.5.8.1

An abelian variety is projective.

Proof. Let U be affine open subset of A containing 0. We may assume $\dim(A) \geq 1$. Let $Z_1, ..., Z_r$ be irreducible components of $A \backslash U$. Enlarging them, we may assume $Z_1, ..., Z_r$ are prime divisors. In order to see this note the complement of a divisor in an affine smooth variety is smooth. Setting

$$D = \sum Z_i$$

the subgroup $B = \{a \in A : \tau_a^*(D) = D\}$ is closed and for $b \in B$, $U + b = B$. Since $0 \in U$, we have

$$B \subseteq U$$

As a complete variety, B must be finite. Lemma 3.5.8 shows D is ample, hence A is projective.

Proposition 3.5.9

For $\mathscr{B} \in \operatorname{Pic}(A)$, the following are equivalent:

1. $\mathscr{B} \in \operatorname{Pic}^0(A)$
2. $\ker(\phi_{\mathscr{B}}) = A$
3. *For every ample $\mathscr{L} \in \operatorname{Pic}(A)$, there is $a \in A$ so $\mathscr{B} = \tau_a^*(\mathscr{L}) - \mathscr{L}$*

4. *There is ample $\mathscr{L} \in \mathrm{Pic}(A)$, such that $\mathscr{B} = \tau_a^*(\mathscr{L}) - \mathscr{L}$ for some $a \in A$*

Proof. (1) $\Rightarrow$ (2): By Corollary 3.4.2.1, we may assume K is ACF. Let

$$\phi : A \to \mathcal{P}\mathrm{ic}^0(A) \to \mathcal{P}\mathrm{ic}^0(A)$$

be the map given by $(a, \mathscr{B}) \mapsto \tau_a^*\mathscr{B}$. We will prove below this is a morphism. For $T = A \times \mathcal{P}\mathrm{ic}^0(A)$, consider

$$\mathscr{L} := (m \times \mathrm{Id}_{\mathcal{P}\mathrm{ic}^0(A)})^*(\mathscr{P}) \in \mathrm{Pic}(A \times T)$$

where m denotes the addition morphism as usual. Note the restriction of $m \times \mathrm{Id}_{\mathcal{P}\mathrm{ic}^0(A)}$ to $A \times \{a\} \times \{\mathscr{B}\}$ is given by $\tau_a \times \{\mathscr{B}\}$, by identifying $A \times \{a\} \times \{\mathscr{B}\}$ with A. By Remark 3.4.3 and the rule $(f \circ g)^* = g^* \circ f^*$ we get

$$\mathscr{L}|_{A \times \{a\} \times \{\mathscr{B}\}} = \tau_a^*\mathscr{B}$$

and similarly

$$\mathscr{L}|_{\{0\} \times T} = \mathscr{P}$$

Let us denote by p_2 the projection of $A \times T$ onto T. The subfamily $\mathscr{L} - p_2^*\mathscr{P}$ of $\mathrm{Pic}^0(A)$ parametrized by T induces a morphism $T \to \mathcal{P}\mathrm{ic}^0(A)$, which is equal to ϕ (Theorem 3.4.5). Since $\phi(A \times \{0\}) = 0$, the constancy lemma 3.1.5 shows $\tau_a^*(\mathscr{B}) = \mathscr{B}$ for all $a \in A$, which proves the claim.

(2) $\Rightarrow$ (3): This is Theorem 3.5.4.

Clearly (3) $\Rightarrow$ (4) as the existence of an ample class is by Corollary 3.5.8.1.

(4) $\Rightarrow$ (1): Theorem 3.5.2.

Definition 3.5.10

The Picard variety $\mathcal{P}\mathrm{ic}^0(A)$ is called the ***dual abelian variety*** of A and will be denoted by $\hat{A}$.

Corollary 3.5.10.1

The dual abelian variety of A has the same dimension as A.

Proof. There is an ample $\mathscr{L} \in \mathrm{Pic}(A)$, and thus $\phi_{\mathscr{L}} : A \to \hat{A}$ is surjective and finite. Thus they have the same dimension.

3.6 Theorem of the Cube

Theorem of the Cube roughly says the pullback of a fixed line bundle on abelian variety is a quadratic function in the morphism.

Definition 3.6.1

Let M be an abelian group with an involution $*$, i.e. a linear map

$$M \to M, \quad x \mapsto x^*$$

with $(x^*)^* = x$ for all $x \in M$. Then an element $x \in M$ is called ***even*** if $x^* = x$ and ***odd*** if $x^* = -x$.

Even and odd elements both form a subgroup of M, and their intersection is the 2-torsion points of M. For $x \in M$, we are looking for a decomposition $x = x_+ + x_-$ into even x_+ and odd x_-. Note such decomposition is determined up to 2-torsions.

Lemma 3.6.2

Let $x \in M$. Then $2x$ has a decomposition into even and odd parts. If the subgroup of odd elements is divisible by 2 (recall p-divisible means $pM = M$), then x has also such decomposition.

Proof. Just note $2x = (x + x^*) + (x - x^*)$ is such a decomposition. Next, divisibility by 2 means we can find odd z such that $2z = x - x^*$ because $x - x^*$ is odd. Now we set $x_+ = x - z$ and $x_- = z$, then observe

$$\begin{aligned}(x_+)^* &= x^* - z^* = x^* + z \\ &= (x - 2z) + z \\ &= x - z = (x_+)\end{aligned}$$

This concludes the proof.

Definition 3.6.3

Let A be abelian variety over K and consider $\mathscr{L} \mapsto [-1]^*\mathscr{L}$ on the abelian group $\mathrm{Pic}(A)$. Hence a line bundle is ***even*** if $[-1]^*\mathscr{L} \cong \mathscr{L}$ and ***odd*** if $[-1]^*\mathscr{L} \cong \mathscr{L}^{-1}$

Proposition 3.6.4

On every abelian variety, there is an even vary ample line bundle.

Proof. By Corollary 3.5.8.1, there is a very ample $\mathscr{L} \in \mathrm{Pic}(A)$. Then $\mathscr{L} + [-1]^*\mathscr{L}$ is even and very ample (since $\mathscr{L}$ and $[-1]^*\mathscr{L}$ are both very ample).

Definition 3.6.5

Now let $q : M \to N$ be a set-theoretic map of abelian groups. If the function $b : M \times M \to N$

$$(x, y) \mapsto q(x+y) - q(x) - q(y)$$

is bilinear, then q is called a ***quadratic function*** with ***associated bilinear form*** b.

Obviously, b is symmetric.

Definition 3.6.6

A ***quadratic form*** is a quadratic function which is homogeneous of degree 2 with respect to multiplication by integers, i.e. $q(kx) = k^2 q(x)$ for all $k \in \mathbb{Z}$.

The quadratic functions forms an abelian group, and on this group we have an involution given by $q^*(x) := q(-x)$. To see this is an involution on the group of quadratic functions, just note $(q^*)^*(x) = q^*(-x) = q(x)$.

By the proof of Lemma 3.6.2, we have a canonical decomposition of $2q$ into an even quadratic function O and odd L, given by

$$Q(x) = q(x) + q(-x), \quad L(x) = q(x) - q(-x)$$

Definition 3.6.7

Let q be a quadratic function with decomposition Q, L as above. Then Q is called the ***associated quadratic form*** of q and L is called the ***associated linear form***.

Note $q(0) = 0$ and thus $b(x, -x) = -Q(x)$. We get $Q(x) = b(x, x)$ as b is bilinear, and thus $Q(x)$ is inded homogeneous of degree 2. An easy computation shows L is linear.

Lemma 3.6.8

Let $q : M \to N$ be quadratic function and $n \in \mathbb{Z}$, then

$$q(nx) = \frac{n^2+n}{2} q(x) + \frac{n^2-n}{2} q(-x)$$

Proof. We proceed on induction on $|n|$. If $|n| = 1$ then $q(x) = q(x) + 0q(-x)$ and $q(-x) = 0q(x) + q(-x)$. Suppose our claim holds for values $\leq n$. Let b be the associated bilinear form, then

$$0 = b(nx, x) + b(nx, -x)$$

and expand we get

$$\begin{aligned} 0 &= q(nx+x)-q(nx)-q(x)+q(nx-x)-q(nx)-q(-x) \\ &= q((n+1)x)-2q(nx)+q((n-1)x)-q(x)-q(-x) \end{aligned}$$

and so

$$\begin{aligned} q((n+1)x) &= 2q(nx)-q((n-1)x)+q(x)+q(-x) \\ &= (n^2+n+1)q(x)+(n^2-n+1)q(-x) \\ &\quad -\frac{n^2-n}{2}q(x)-\frac{n^2-3x+2}{2}q(-x) \\ &= \frac{n^2+3n+1}{2}q(x)+\frac{n^2+n}{2}q(-x) \\ &= \frac{(n+1)^2+(n+1)}{2}q(x)+\frac{(n+1)^2-(n+1)}{2}q(-x) \end{aligned}$$

Corollary 3.6.8.1

A quadratic function is even/odd iff its homogeneous of degree 2/1.

Example 3.6.9

Let $M = (\mathbb{Z}/2\mathbb{Z})^2$ and $N = \mathbb{Z}/2\mathbb{Z}$. Consider $q : M \to N$ given by $q(x) = 0$ iff $x = 0$. Then q is odd quadratic function which is not linear.

Now let $I \subseteq \{1, ..., k\}$ where $k \in \mathbb{Z}_{>0}$, then we define

$$S_I : M^k \to M, \quad S_I(x_1, ..., x_k) = \sum_{i \in I} x_i$$

with the special case of $S_\emptyset(\mathbf{x}) = 0$.

Remark 3.6.10

Let $q : M \to N$ be a set-theoretic function and $b(x,y) = q(x+y)-q(x)-q(y)$. Then a direct computation shows

$$\begin{aligned} &q(x+y+z)-q(x+z)-q(x+y)-q(y+z)+q(x)+q(y)+q(z) \\ &= q(x+y+z)-b(x,y)-q(x+z)-q(y+z)+q(z)+q(x)-q(x) \\ &= q(x+y+z)-b(x,y)-b(x,z)-q(y+z)-q(x) \\ &= b(x,y+z)-b(x,y)-b(x,z) \end{aligned}$$

Thus, we see if $b(x,y)$ is bilinear then

$$q(x+y+z)-q(x+z)-q(x+y)-q(y+z)+q(x)+q(y)+q(z) = 0$$

as $b(x,y+z)-b(x,y)-b(x,z) = b(x,y+z)-b(x,y+z) = 0$. Conversely, if

$$q(x+y+z)-q(x+z)-q(x+y)-q(y+z)+q(x)+q(y)+q(z) = 0$$

then we see

$$b(x, y+z) - b(x, y) - b(x, z) = 0$$

which says $b(x, y)$ is bilinear. Thus $b(x, y)$ is bilinear (at one input, but this argument is symmetric) iff for all x, y, z we have

$$q(x+y+z) - q(x+z) - q(x+y) - q(y+z) + q(x) + q(y) + q(z) = 0$$

Lemma 3.6.11

Let q be a quadratic function and k an integer. If $k \geq 3$, then for all $\mathbf{x} \in M^k$ we have

$$\sum_{I \subseteq \{1,\ldots,k\}} (-1)^{|I|} q(S_I(\mathbf{x})) = 0$$

Proof. We proceed by induction on k. Suppose $k = 3$, then by Remark 3.6.10 we are done. Suppose it holds for $k-1$ now, then we get

$$\begin{aligned}
&\sum_{I \subseteq \{1,\ldots,k\}} (-1)^{|I|} q(S_I(\mathbf{x})) \\
&= \sum_{I \subseteq \{1,\ldots,k-1\}} (-1)^{|I|} q(S_I(\mathbf{x})) - \sum_{J \subseteq \{1,\ldots,k-1\}} (-1)^{|J|} q(S_J(\mathbf{x}) + x_k) \\
&= - \sum_{J \subseteq \{1,\ldots,k-1\}} (-1)^{|J|} b(S_J(\mathbf{x}), x_k) - \sum_{J \subseteq \{1,\ldots,k-1\}} (-1)^{|J|} q(x_k)
\end{aligned}$$

because

$$\begin{aligned}
&\sum_{J \subseteq \{1,\ldots,k-1\}} (-1)^{|J|} b(S_J(\mathbf{x}), x_k) \\
&= \sum_{J \subseteq \{1,\ldots,k-1\}} (-1)^{|J|} (q(S_J(\mathbf{x}) + x_k) - q(S_J(\mathbf{x})) - q(x_k))
\end{aligned}$$

Now note $b(-, x_k)$ is a quadratic function, and hence we can apply our induction hypothesis to conclude the first term is 0, i.e.

$$\begin{aligned}
\sum_{I \subseteq \{1,\ldots,k\}} (-1)^{|I|} q(S_I(\mathbf{x})) &= - \sum_{J \subseteq \{1,\ldots,k-1\}} (-1)^{|J|} q(x_k) \\
&= -q(x_k) \sum_{J \subseteq \{1,\ldots,k-1\}} (-1)^{|J|} \\
&= -q(x_k) \sum_{i=1}^{k-1} \binom{k-1}{i} (-1)^i \\
&= -q(x_k)(1-1)^{k-1} \\
&= 0
\end{aligned}$$

Now let us apply the above results to $M = \mathrm{Hom}_K(X, A)$ and $N = \mathrm{Pic}(X)$.

Theorem 3.6.12

Let X be a variety over the field K and A an abelian variety over K with $\mathscr{L} \in \mathrm{Pic}(A)$. Then the map $\mathrm{Hom}_K(X,A) \to \mathrm{Pic}(X)$ given by $\phi \mapsto \phi^*\mathscr{L}$ is quadratic.

Let $k \geq 3$ and $X = A^k$ with ith projection p_i onto A. For $I \subseteq \{1,...,k\}$ we have

$$S_I(p_1,...,p_k) = \sum_{i \in I} p_i$$

Lemma 3.6.11 shows the theorem implies

$$\sum_{I \subseteq \{1,...,k\}} (-1)^{|I|} S_I(p_1,...,p_k)^*(\mathscr{L}) = 0$$

For $k = 3$, this equation

$$\sum_{I \subseteq \{1,2,3\}} (-1)^{|I|} \left(\sum_{i \in I} p_i \right)^* (\mathscr{L}) = 0 \tag{Eq. 3.6.1}$$

is called the theorem of the cube.

Proof. Let $\phi_1, \phi_2, \phi_3 : X \to A$ and let

$$\Phi : X \to A^3, \quad x \mapsto (\phi_1(x), \phi_2(x), \phi_3(x))$$

We pullback Eq. 3.6.1 to X using Φ, then we can prove bilinearity using Remark 3.6.10. So it is enough to prove the theorem of the cube. Let $\mathscr{L}'$ be the left-hand side of Eq. 3.6.1. For $a, b, c \in A$, we see

$$\mathscr{L}'|_{\{a\}\times\{b\}\times A} = \tau_{a+b}^*(\mathscr{L}) - \tau_a^*(\mathscr{L}) - \tau_b^*(\mathscr{L}) + \mathscr{L}$$

and this is equal to 0 by Theorem of the square 3.5.3. In the same way, the restriction of $\mathscr{L}$ to $\{a\} \times A \times \{c\}$ is trivial. Now apply seesaw principle 3.4.1.1, we see $\mathscr{L}|_{\{a\}\times A\times A}$ is trivial for any $a \in A$. Now $\mathscr{L}|_{A\times\{b\}\times\{c\}}$ is also trivial, and apply seesaw principle again, $\mathscr{L}$ is trivial.

Let A be an abelian variety over K. Now we will study the endomorphism $[n] : A \to A$, and the main result deals with the kerne $A[n]$ of $[n]$. This map plays a fundamental role in the study of abelian varieties, both geometrically and arithmetically. The arithmetic importances comes from the construction of the Néron-Tate height and hence in the proof of the Mordell-Weil.

Proposition 3.6.13

Let $\mathscr{L} \in \mathrm{Pic}(A)$ and $n \in \mathbb{Z}$, then

$$[n]^*\mathscr{L} = \frac{n^2+n}{2}\mathscr{L} + \frac{n^2-n}{2}[-1]^*\mathscr{L}$$

In particular, we have $[n]^*\mathscr{L} = n^2\mathscr{L}$ if $\mathscr{L}$ is even and $[n]^*\mathscr{L} = -\mathscr{L}$ if $\mathscr{L}$ is odd.

Proof. By Theorem 3.6.12 the function

$$q : \mathbb{Z} \to \mathrm{Pic}(A), \quad n \mapsto [n]^*\mathscr{L}$$

is quadratic. Thus the result follows from Lemma 3.6.8.

Proposition 3.6.14

Let $n \in \mathbb{Z}\backslash\{0\}$. Then $[n]$ is a finite flat surjection of degree $n^{2\dim(A)}$. The separable degree of $[n]$ equal the number of points of any fiber. If $\mathrm{char}(K) \nmid n$, then $[n]$ is an étale morphism and

$$A[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2\dim(A)}$$

If $p = \mathrm{char}(K)$ divides n, then $[n]$ is not separable.

Proof. Let g be the dimension of A. By Corollary 3.5.8.1, there is an ample $\mathscr{L} \in \mathrm{Pic}(A)$. The restriction of $[n]^*\mathscr{L}$ to $A[n]$ is trivial. Since $[-1]$ is an automorphism, $[-1]^*\mathscr{L}$ is also ample. Proposition 3.6.13 shows $[n]^*\mathscr{L}$ is ample and in particular it is ample when restricted to $A[n]$. Therefore, $A[n]$ must be finite (i.e. Fact 3.5.6). Now the dimension theorem 3.1.11 and Proposition 3.1.14 shows $[n]$ is surjective finite flat morphism, whose fiber have cardinality equal the separable degree of $[n]$. In order to compute its degree, we use intersection theory. There is a very ample even line bundle $\mathscr{L}$ on A (Proposition 3.6.4), say $\mathscr{L} = \mathscr{O}(D)$ for a divisor D. By projection formula (i.e. if $\phi : X \to X'$ is proper, then $\phi_*(\phi^*(D') \cdot Z) = D' \cdot \phi_*(Z)$ for any cycle Z on X and divisor D' on X') we see

$$[n]^*(D) \cdot \ldots \cdot [n]^*(D) = \deg[n](D \cdot \ldots \cdot D)$$

where we take g-fold intersection. By Proposition 3.6.13 we see $[n]^*(D) \sim n^2 D$ where $\sim$ denotes rational equivalence of divisors. Noting $D \cdot \ldots \cdot D = \deg(X) \neq 0$, we deduce

$$n^{2g} = \deg[n]$$

Now recall the differential $d[n]$ is multiplication by n on the tangent space at 0 (Corollary 3.1.17.1).

If $\mathrm{char}(K) \nmid n$, then we see by a translation argument that $d[n]$ induces an isomorphism on tangent space. Thus $[n]$ is étale and hence separable. We have seen that the number of points of $A[n]$ is equal to the separable degree of $[n]$, thus $|A[n]| = n^{2g}$. For any $m \mid n$, it follows the subgroup $A[m]$ has m^{2g} elements. Thus by the theory of finite abelian groups, $A[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.

If $p = \mathrm{char}(K)$ divides n, then the differential $d[n]$ vanishes at 0. Hence $d[n]$ vanishes everywhere by a translation argument. Since a separable dominant morphism is generically étale, and $[n]$ is surjective, we see $[n]$ cannot be separable.

Remark 3.6.15

A surjective homomorphism of abelian varieties of the same dimension is called an isogeny. Thus by the above we see $[n]$ is an isogeny.

The next topic is characterization of odd elements in Picard group of A, where A is abelian variety over K.

Recall Definition 3.6.3, where we defined a canonical involution of $\mathrm{Pic}(A)$ which gives even and odd elements. First, we will prove $\mathrm{Pic}^0(A)$ is divisible subgroup and get a decomposition into even and odd parts on the Picard group. Then, we will show the classes in the Picard group algebraically equivalent to 0 are precisely the odd classes. Finally, we will show the Poincaré class of an abelian variety is even.

Proposition 3.6.16

If $\mathscr{L} \in \mathrm{Pic}(A)$ and $r \in \mathbb{Z}\backslash\{0\}$ with $r\mathscr{L} \in \mathrm{Pic}^0(A)$, then $\mathscr{L} \in \mathrm{Pic}^0(A)$.

Proof. Note $r\phi_{\mathscr{L}} = \phi_{r\mathscr{L}}$ and the latter is equal to 0 by Proposition 3.5.9. Theorem 3.5.2 shows $\phi_{\mathscr{L}}$ is a homomorphism of abelian varieties and so $\phi_{\mathscr{L}} = 0$ by Proposition 3.6.14. Using once more Proposition 3.5.9 we see $\mathscr{L} \in \mathrm{Pic}^0(A)$ as desired.

Corollary 3.6.16.1

Let $\mathscr{L} \in \mathrm{Pic}(A)$. Then there are odd element $\mathscr{L}_-$ and even element $\mathscr{L}_+$ of $\mathrm{Pic}(A)$ such that $\mathscr{L} = \mathscr{L}_- + \mathscr{L}_+$. The element $\mathscr{L}_-$ is determined only up to 2-torsion elements in $\mathrm{Pic}(A)$.

Proof. This follows from Lemma 3.6.2 and Proposition 3.6.16.

Theorem 3.6.17

If $\mathscr{L} \in \mathrm{Pic}(A)$, then $[-1]^*\mathscr{L} - \mathscr{L} \in \mathrm{Pic}^0(A)$. Moreover, TFAE:

1. *$\mathscr{L}$ is odd*
2. *For any variety X, the map $\mathrm{Hom}(X, A) \to \mathrm{Pic}(A)$ given by $\phi \mapsto \phi^*\mathscr{L}$ is linear.*
3. *If p_i is the ith projection of $A \times A$ onto A, then*

$$(p_1 + p_2)^*(\mathscr{L}) = p_1^*\mathscr{L} + p_2^*\mathscr{L}$$

4. *$\tau_a^*\mathscr{L} = \mathscr{L}$ for all $a \in A$*
5. *$\mathscr{L} \in \mathrm{Pic}^0(A)$*
6. *For all ample $\mathscr{L}' \in \mathrm{Pic}(A)$, there is an $a \in A$ so $\mathscr{L} = \tau_a^*(\mathscr{L}') - \mathscr{L}'$*

7. *There is an ample $\mathscr{L}' \in \mathrm{Pic}(A)$ so $\mathscr{L} = \tau_a^*(\mathscr{L}') - \mathscr{L}'$ for some $a \in A$*

Proof. Note (4),(5),(6) and (8) are equivalent by Proposition 3.5.9. By Corollary 3.4.1.2, (3) and (4) are equivalent. We also note (2) $\Rightarrow$ (1) is trivial.

(3) $\Rightarrow$ (2): Choose $\phi_1, \phi_2 \in \mathrm{Hom}(X, A)$ and define ϕ be $\phi(x) = (\phi_1(x), \phi_2(x))$. Pulling back the identity in (3) we see $(\phi_1 + \phi_2)^*(\mathscr{L}) = \phi_1^*(\mathscr{L}) + \phi_2^*(\mathscr{L})$, which gives linearity, i.e. we get (2).

We note at this point we have (5) $\Leftrightarrow$ (4) $\Leftrightarrow$ (3) $\Rightarrow$ (2) $\Rightarrow$ (1), i.e. (5) $\Rightarrow$ (1).

Now it suffices to prove (1) $\Rightarrow$ (5), but before that we will show $[-1]^*\mathscr{L} - \mathscr{L} \in \mathrm{Pic}^0(A)$.

For $a \in A$, we have $[-1] \circ \tau_a = \tau_{-a} \circ [-1]$ and thus

$$\tau_a^*([-1]^*\mathscr{L}) - [-1]^*\mathscr{L} = [-1]^*(\tau_{-a}^*\mathscr{L} - \mathscr{L}) \tag{Eq. 3.6.2}$$

Since $\tau_{-a}^*\mathscr{L} - \mathscr{L} \in \mathrm{Pic}^0(A)$ (Theorem 3.5.2), the above Eq. 3.6.2 is equal to $\mathscr{L} - \tau_{-a}^*(\mathscr{L})$ by the implication (5) $\Rightarrow$ (1). By Theorem of the square 3.5.3, the latter is equal $\tau_a^*\mathscr{L} - \mathscr{L}$, and thus we have proved

$$\tau_a^*([-1]^*\mathscr{L}) - [-1]^*\mathscr{L} = \tau_a^*\mathscr{L} - \mathscr{L}$$

Now we finish (1) $\Rightarrow$ (5). Let $\mathscr{L}$ be an odd element of $\mathrm{Pic}^0(A)$, then

$$-2\mathscr{L} = [-1]^*\mathscr{L} - \mathscr{L} \in \mathrm{Pic}^0(A)$$

and thus $\mathscr{L} \in \mathrm{Pic}^0(A)$ by Proposition 3.6.16.

Theorem 3.6.18

Let $\hat{A}$ be the dual abelian variety with corresponding Poincaré class $\mathscr{P} \in \mathrm{Pic}(A \times \hat{A})$. Then $\mathscr{P}$ is even.

Proof. Let $\mathscr{B} \in \hat{A}$. By Remark 3.4.3 and Theorem **??** we see

$$([-1]^*\mathscr{P})|_{A\times\{\mathscr{B}\}} = [-1]^*(\mathscr{P}|_{A\times\{-\mathscr{B}\}})[-1]^*(-\mathscr{B}) = \mathscr{B}$$

Let $B = \mathcal{P}\mathrm{ic}^0(A)$, then since

$$([-1]^*\mathscr{P})|_{\{0\}\times B} = [-1]^*(\mathscr{P}|_{\{0\}\times B}) = 0$$

we see $[-1]^*\mathscr{P} = \mathscr{P}$ by Remark 3.4.3.

3.7 Curves and Jacobians

Throughout we will let C be irreducible smooth projective curve over field K of genus $g \geq 1$ with base point $P_0 \in C(K)$. Note the existence of P_0 implies C is geometrically irreducible.

Definition 3.7.1

The Picard variety of C is called the ***Jacobian variety*** of C.

We denote the Jacobian by J. Note J is equal as a group to the rational equivalence class of divisors of degree 0 on $C_{\overline{K}}$. For every intermediate field $K \subseteq L \subseteq \overline{K}$, Corollary 3.4.2.1 shows the L-rational points of J may be identified with the rational equivalence classes defined over L.

In the context of complex geometry, there is a more familiar construction of the Jacobian variety.

Let γ be a 1-cycle on C. Then $\int_\gamma \omega$ is a linear functional on the holomorphic 1-forms on C, whose value depends only on the homology class of γ in $H_1(C,\mathbb{Z})$. Thus we obtain a homomorphism

$$H_1(C,\mathbb{Z}) \to H^1(C,\Omega_C^1)^*$$

of the homology group $H_1(C,\mathbb{Z})$ into the dual $H^0(C,\Omega_C^1)^*$ of the space of holomorphic 1-forms on C. This embeds $H_1(C,\mathbb{Z})$ as a lattice in $H^0(C,\Omega_C^1)^*$. Then the complex torus

$$J := H^1(C,\Omega_C^1)^*/H_1(C,\mathbb{Z})$$

realizes the Jacobian variety complex analytically. We have an embedding

$$j : C \to J, \quad P \mapsto \int_{\gamma_P}$$

where γ_P is any path connecting the base point P_0 with P. The value $j(P)$ is independent of the choice of the path. Independently of the choice of the base point P_0, we have homomorphism

$$\mathrm{Pic}^0(C) \to J, \quad \sum_{i=1}^n ([P_i]-[Q_i]) \mapsto \sum_{i=1}^n (j(P_i)-j(Q_i))$$

Abel's theorem gives the injectivity and Jacobi inversion theorem the surjectivity of this homomorphism. There is a natural isomorphism of $H^0(J,\Omega_J^1)$ onto the dual of the tangent space $T_{J,0}$ (Proposition 3.1.18). Pullback induces an isomorphism

$$H^0(J,\Omega_J^1) \xrightarrow{\sim} H^0(C,\Omega_C^1) \qquad \text{(Eq. 3.7.1)}$$

In particular, this isomorphism holds for any base field K (not just over $\mathbb{C}$). More precisely, let $J = \mathcal{P}\mathrm{ic}^0(C)$ and consider $j : C \to J$ given by $P \mapsto [P]-[P_0]$. It follows from the theory of Picard variety that j is a morphism of varieties over K. In fact, let Δ be the diagonal in $C \times C$, p_1, p_2 the two projections, then $[\Delta]-p_1^*[P_0]-p_2^*[P_0]$ is a subfamily of $\mathrm{Pic}^0(C)$ parametrized by C. By Theorem 3.4.5, we conclude j is a morphism.

Proposition 3.7.2

The Jacobian variety of C has dimension g.

Proof. By Proposition 3.1.18, the tangent bundle T_J is a trivial vector bundle of rank $\dim(J)$. By duality, the same holds for the cotangent bundle. Now recall the only regular functions on an irreducible complete variety over ACF are constants. Since J is geometrically reduced, compatibility of cohomology and base change holds. This shows

$$H^0(J, \mathscr{O}_J) = K$$

and hence

$$\dim H^0(J, \Omega^1_J) = \dim(J) \cdot \dim H^0(J, \mathscr{O}_J) = \dim(J)$$

Now the claim follows from the isomorphism Eq. 3.7.1.

Definition 3.7.3

The ***theta divisor*** of J is defined to be

$$\Theta = j(C) + j(C) + \ldots + j(C) = \sum_{i=1}^{g-1} j(C)$$

In the following we will show Θ is indeed a divisor on J, but before that we will need three lemmas. Note for divisor D and line bundle $\mathscr{L}$, we use $\mathscr{L}(D)$ to denote $\mathscr{L} \otimes \mathscr{O}(D)$.

Remark 3.7.4

For any $r \in \mathbb{N}$, we have a map

$$j_r : C^r \to J, \quad (P_1, \ldots, P_r) \mapsto \sum_{j=1}^{r} [P_j] - r[P_0]$$

Since $j = j_1$ and addition on J are both morphisms, we see j_r is a morphism. Note its image is closed as C^r is complete. Let $a := j_r(P_1, \ldots, P_r)$, then the fiber over a is

$$j_r^{-1}(a) = \left\{ (Q_1, \ldots, Q_r) \in C^r : \sum_{j=1}^{r} [Q_j] \sim \sum_{j=1}^{r} [P_j] \right\}$$

Suppose $1 \leq r \leq g$ and $(P_1, \ldots, P_r) \in C^r$ satisfies $i \neq j \Rightarrow P_i \neq P_j$, and

$$\Gamma(C_{\overline{K}}, \mathscr{O}(\sum [P_j])) = 1$$

then the fiber over a is obtained by permuting the entries, namely

$$j_r^{-1}(j_r(P_1, \ldots, P_r)) = \{(P_{\pi(1)}, \ldots, P_{\pi(r)}) : \pi \in S_r\}$$

By the dimension theorem (for dominant $\phi : X \to Y$ between irreducible, there is open dense $U \subseteq Y$ so $y \in Y$ implies $\dim(X_y) = \dim(X) - \dim(Y)$), we conclude $\dim j_r(C^r) = r$. In particular, Proposition 3.7.2 implies j_g is surjective. Moreover, $\Theta = j_{g-1}(C^{g-1})$ is indeed a divisor.

Proposition 3.7.5

The map $j : C \to J$, $P \mapsto [P] - [P_0]$ is a closed embedding.

Proof. We may assume K is ACF. Since $g \geq 1$, two points of $C_{\overline{K}}$ are rationally equivalent iff they are equal (use Riemann-Roch). Hence j is one-to-one. We claim dj induces an injective map between tangent spaces. In order to prove this, its enough to show the dual is surjective between cotangent spaces. We have seen for any $a \in J$, a cotangent vector in a extends canonically to a global section of Ω^1_J (Proposition 3.1.18). By the isomorphism Eq. 3.7.1, its enough to show the evaluation map $\Gamma(C, \Omega^1_C) \to T^*_{C,P}$ is surjective for $P \in C$. Note the kernel of the evaluation map is $\Gamma(C, \Omega^1_C(-[P]))$. By injectivity of j, we know $\Gamma(C, \mathcal{O}([P]))$ has dimension 1. By the Riemann-Roch theorem, we conclude that the kernel is $g-1$ dimensional and hence the evaluation map is surjective.

Since J is a projective variety (Corollary 3.5.8.1), we have a closed embedding $J \to \mathbb{P}^n_K$. In order to prove j is a closed embedding, we have to show the linear system corresponding to the induced map $C \to \mathbb{P}^n_K$ separates points and tangent vectors. The first (resp. second) conditions follows by injectivity of j (resp. dj).

As a divisor on J, we also consider

$$\Theta^- = [-1]^*\Theta = -j(C) - \ldots - j(C)$$

In $\mathrm{Pic}(J)$, we use $\theta := \mathcal{O}(\Theta)$ and $\theta^- = [-1]^*\theta$. For $a \in J$, we set $j_a := \tau_{-a} \circ j$, i.e. $j_a(P) = j(P) - a$.

The pull-back of a divisor D' with respect to a morphism $\phi : X \to X'$ of irreducible smooth varieties over K is well defined as a divisor if $\phi(X)$ is not contained in the support of D'. In this case, viewing D' as a Cartier divisor on X' locally given on U'_α by a rational function f'_α, the pullback $\phi^*(D')$ is given on $\phi^{-1}(U'_\alpha)$ by $f'_\alpha \circ \phi$. Note $\phi^*(D')$ is well-defined in $CH^1(X)$ (here CH denotes the Chow group of X, which is cycles on X mod out by rational equivalence) for any divisor D' on X. If ϕ is an isomorphism (as $[-1]$ is in the cases above) and if D' is a prime divisor, then $\phi^*(D') = \phi^{-1}(D')$

Proposition 3.7.6

Assume K is ACF. For all $(P_1, \ldots, P_g) \in C^g$, we have the rational equivalence relation

$$\sum_{i=1}^{g} [P_i] \sim j_a^*(\Theta^-)$$

of divisors on C, where $a = j_g(P_1, \ldots, P_g)$.

Now for $1 \leq r \leq g$, define

$$U_r := \left\{ (P_1, \ldots, P_r) \in C^r : (\forall i \neq j, P_i \neq P_j) \wedge \dim \Gamma\left(C_{\overline{K}}, \mathscr{O}\left(\sum_{j=1}^{r} [P_j] \right) \right) = 1 \right\}$$

One can prove this is open dense in C^r, but we will not prove it here.

Corollary 3.7.6.1

For all $(P_1, \ldots, P_g) \in U_g$ and $a = j_g(P_1, \ldots, P_g)$, we have

$$\sum_{i=1}^{g} [P_i] = j_a^*(\Theta^-)$$

as an identity of divisors.

Proof. We may assume, by base change, K is ACF. By Proposition 3.7.6 we see

$$\sum_{i=1}^{g} [P_i] \sim j_a^*(\Theta^-)$$

Both sides are effective divisors on C. By assumption, the linear system $|\sum_{i=1}^{g} [P_i]|$ is zero-dimensional proving the claim.

Corollary 3.7.6.2

For $a \in J = \mathcal{P}\mathrm{ic}^0(C)$, we have

$$j_a^*(\theta^-) - j^*(\theta^-) = a$$

Proof. By base change and Corollary 3.4.2.1, we may assume K is ACF. Then the claim follows from surjectivity of j_g (Remark 3.7.4) and Proposition 3.7.6.

There are two Poincaré classes in the context of Jacobians. One is the Poincaré class $\mathscr{P}_C \in \mathrm{Pic}(C \times J)$, the other is the Poincaré class $\mathscr{P}_J \in \mathrm{Pic}(J \times \hat{J})$, where $\hat{J}$ is the dual abelian variety of J. In the last part of this section, we will study those.

Proposition 3.7.7

Let Δ be the diagonal of $C \times C$. Then

$$(\mathrm{Id}_C \times j)^*(\mathscr{P}_C) = \mathscr{O}(\Delta - C \times \{P_0\} - \{P_0\} \times C)$$

Proof. By characterization of Poincaré class in Remark 3.4.3, we get for $P \in C$:

$$(\mathrm{Id}_C \times j)^*(\mathscr{P}_C)|_{C\times\{P\}} \cdot \mathscr{P}_C|_{C\times\{j(P)\}} = \mathscr{O}([P] - [P_0])$$

Since the restriction of $\mathscr{O}(\Delta - C \times \{P_0\} - \{P_0\} \times C)$ to $C \times \{P\}$ is in the same class ,we get the claim by the seesaw principle in Corollary 3.4.1.1 (noting that the restriction to $\{P_0\} \times C$ of both classes are 0).

Proposition 3.7.8

Let $m : J \times J \to J$ be addition and p_1, p_2 two projections. For

$$\mathscr{L} := m^*\theta^- - p_1^*\theta^- - p_2^*\theta^- \in \mathrm{Pic}(J \times J)$$

we have

$$(j \times \mathrm{Id}_J)^*(\mathscr{L}) = -\mathscr{P}_C$$

Proposition 3.7.9

Let ϕ_θ, ϕ_{θ^-} be the morphisms $J \to \hat{J}$ defined before (i.e. for $a \in J$, we define $\phi_a(\mathscr{L}) = \tau_a^*(\mathscr{L}) - \mathscr{L}$). Let

$$\mathscr{L} = m^*\theta^- - p_1^*\theta^- - p_2^*\theta^-$$

Then

$$(\mathrm{Id}_J \times \phi_{\theta^-})^*(\mathscr{P}_J) = (\mathrm{Id}_J \times \phi_\theta)^*(\mathscr{P}_J) = \mathscr{L}$$

Let us conclude our findings.

Given a curve C of genus $g \geq 1$ with base point $P_0 \in C(K)$, there is a natural embedding j of C into the Jacobian variety. By Theorem 3.5.2 we have a dual homomorphism $\hat{j} : \hat{J} \to J$. The theta divisor is defined by

$$\Theta = j(C) + \ldots + j(C) = \sum_{i=1}^{g-1} j(C)$$

and the corresponding class in $\mathrm{Pic}(J)$ is denoted by θ. Let $\theta^- = [-1]^*\theta$ and $\phi_\theta : J \to \hat{J}$ the natural morphism in Theorem 3.5.2. There are three canonical morphisms from $J \times J$ to J, namely m, p_1 and p_2. The pullback of the Poincaré class $\mathscr{P}_J \in \mathrm{Pic}(J \times \hat{J})$ by $\mathrm{Id}_J \times \phi_\theta$ is equal to the class

$$\mathscr{C} := m^*\theta^- - p_1^*\theta^- - p_2^*\theta^-$$

and it follows that

$$\mathscr{C} = m^*\theta - p_1^*\theta - p_2^*\theta$$

Theorem 3.7.10

The map ϕ_θ is an isomorphism of J onto $\hat{J}$ whose inverse is $-\hat{j}$. Moreover, θ is ample.

Chapter 4

Néron-Tate Heights

There are many advantages of Weil's normalized height $h(x)$ on $\mathbb{G}_m$ compared with more naive definitions: its homogeneous of degree 1, its not negative, and torsion points on $\mathbb{G}_m$ are the points of height 0. In particular it gives a distance function on $\mathbb{G}_m(\overline{\mathbb{Q}})/\text{tors}$. The heights associated to a divisor retain similar properties only if we consider them up to a bounded function. Working with them is formally pleasing because its functorial properties, but the price we paid is this equivalence relation is too coarse for some of the most important applications.

It was a fundamental discovery of Néron that Weil's equivalence class of heights associated to a divisor on abelian varieties contain a unique representative with all the nice functorial properties of Weil's equivalence class. Then, it was Tate who gave an elementary proof of the existence of a normalized height associated to a divisor class on an abelian variety.

Thus, we will first construct the Néron-Tate height, and study the associated bilinear form, then consider this height on the Jacobians, which we need for the proof of Falting's theorem.

Thus, we will only cover section 9.2 to 9.4 of the book here.

4.1 Néron-Tate Heights

Let X be complete variety over K. By Theorem 2.3.5 we have the height homomorphism

$$\mathbf{h} : \text{Pic}(X) \to \mathbb{R}^{X(\overline{K})}/O(1)$$

which associates to a line bundle $\mathscr{L}$ its equivalence class of heights $h_{\mathscr{L}}$.

In general there is no canonical height function associated to $\mathscr{L} \in \text{Pic}(X)$. They are only determined up to a bounded function in $O(1)$. But on an abelian variety, there is a canonical choice $\hat{h}_{\mathscr{L}}$ of a height function in any class $\mathbf{h}_{\mathscr{L}}$ characterized by good behaviour with respect to the group operation.

By the theorem of the cube 3.6.12, for every $\mathscr{L} \in \text{Pic}(A)$, we have a quadratic

function

$$\mathrm{Mor}(X,A) \to \mathrm{Pic}(X), \quad \phi \mapsto \phi^*\mathscr{L}$$

Note the decomposition $\mathscr{L} = \mathscr{L}_+ + \mathscr{L}_-$ in to an even part and an odd part (Corollary 3.6.16.1) gives a decomposition of our quadratic function into quadratic form $\phi \mapsto \phi^*\mathscr{L}_+$. Hence with the homogeneity property (Proposition 3.6.13)

$$(n\phi)^*(\mathscr{L}_+) = n^2\phi^*(\mathscr{L}_+)$$

and into a linear form $\phi \mapsto \phi^*\mathscr{L}_-$ (Theorem 3.6.17). The composite of the height homomorphism and the quadratic function is a quadratic function

$$q : \mathrm{Mor}(X,A) \to \mathbb{R}^{X(\overline{K})}/O(1), \quad \phi \mapsto \mathbf{h}_{\phi^*\mathscr{L}}$$

We conclude that $q = q_+ + q_-$ for the quadratic form $q_+(\phi) = \mathbf{h}_{\phi^*(\mathscr{L}_+)}$ and linear form $q_-(\phi) = \mathbf{h}_{\phi^*(\mathscr{L}_-)}$. Since 2 is invertible in the abelian group $\mathbb{R}^{X(\overline{K})}/O(1)$, this decomposition is unique, in contrast to $\mathscr{L} = \mathscr{L}_+ + \mathscr{L}_-$, which is unique only up to 2-torsion in $\mathrm{Pic}(X)$.

By homogeneity, we see for any integer n, we have $n^2\mathbf{h}_{\mathscr{L}_+} = \mathbf{h}_{[n]^*\mathscr{L}_+}$ and $n\mathbf{h}_{\mathscr{L}_-} = \mathbf{h}_{[n]^*\mathscr{L}_-}$. Note $\mathbf{h}_{\mathscr{L}}$ represents an equivalence class of heights, for any representative $h_{\mathscr{L}}$, by Theorem 2.3.5 there is a constant $C(n)$ so that for every $a \in A$ we have

$$|h_{\mathscr{L}_+}(na) - n^2 h_{\mathscr{L}_+}(a)| \leq C(n)$$

$$|h_{\mathscr{L}_-}(na) - nh_{\mathscr{L}_-}(a)| \leq C(n)$$

These conditions serve to choose a canonical height function.

Let us consider the abstract situation first.

Let $\mathcal{N}$ be a multiplicative closed subset of $\mathbb{R}$ (resp. $\mathbb{R}_+$) acting on a set S by means of a map such that $n(mx) = nmx$ for $x \in S$.

Definition 4.1.1

A function $h : S \to \mathbb{R}$ is:

1. ***quasi-homogeneous*** of degree $d \in \mathbb{N}$ (resp. $d \in \mathbb{R}_+$) for $\mathcal{N}$ if for $n \in \mathcal{N}$ there is a positive constant $C(n)$ such that

$$|h(nx) - n^d h(x)| \leq C(x) \text{ for every } x \in S \qquad \text{(Eq. 4.1.1)}$$

   for every $x \in S$
2. ***homogeneous*** of degree d for $\mathcal{N}$ if $h(nx) = n^d h(x)$

The example we should keep in mind is $S = A(\overline{K})$, $h = h_{\mathscr{L}}$, $\mathcal{N} = \mathbb{Z}$ and the action of n is multiplication by n in the abelian group $A(\overline{K})$.

Lemma 4.1.2

Let $\mathcal{N}$ act on the set S as before and $h : S \to \mathbb{R}$ be quasi-homogeneous of degree $d > 0$. If $\mathcal{N}$ has an element of absolute value > 1, then there is a unique homogeneous

function $\hat{h} : S \to \mathbb{R}$ of degree d for $\mathcal{N}$ such that $\hat{h} - h$ is bounded.

Proof. Assume for a moment a homogeneous $\hat{h}$ of degree d for $\mathcal{N}$ exists, and $h - \hat{h}$ is bounded. Then for $x \in S$ and $n \in \mathcal{N}$, we have

$$\hat{h}(x) = \lim_{|n|\to\infty} n^{-d}\hat{h}(nx) = \lim_{|n|\to\infty} n^{-d}h(nx)$$

as $h - \hat{h}$ is bounded. This proves uniqueness and gives us an idea of how to show existence. Apparently, in order for this argument to work, we need $C(n) = o(n^d)$, a condition we do not want to impose a priori. On the other hand, note $h(mnx) = h(m(nx))$ allows us to get control of $C(mn)$ in terms of $C(m)$ and $C(n)$. This is enough for proving the existence of the limit if we stay with a suitable subsequence, and this suffices for the proof. The details are as follows.

Let us fix $m \in \mathcal{N}$, $m > 1$. For a positive integer r, estimate Eq. 4.1.1 with $n = m$ and $m^{r-1}x$ in place of x gives

$$|h(m^r x) - m^d h(m^{r-1}x)| \leq C(m)$$

and hence

$$\begin{aligned} |h(m^r x) - m^{rd}h(x)| &= \left|\sum_{i=1}^{r} m^{d(i-1)}h(m^{r-i+1}x) - m^{di}h(m^{r-i}x)\right| \\ &\leq \sum_{i=1}^{r} m^{d(i-1)}\left|h(m^{r-i+1}x) - m^d h(m^{r-i}x)\right| \\ &\leq \frac{m^{dr}-1}{m^d-1}C(m) \end{aligned}$$

Replacing x by $m^s x$ for any $s \in \mathbb{N}$ we get

$$|h(m^{r+s}x) - m^{rd}h(m^s x)| \leq \frac{m^{dr}-1}{m^d-1}C(m)$$

and we conclude

$$|m^{-(r+s)d}h(m^{r+s}x) - m^{-sd}h(m^s x)| \leq \frac{C(m)}{(m^d-1)m^{ds}} \qquad \text{(Eq. 4.1.2)}$$

for every $r, s \in \mathbb{N}$. This shows

$$(m^{-sd}h(m^s x))_{s\in\mathbb{N}}$$

is a Cauchy sequence and we denote $\hat{h}(x)$ its limit. Using Eq. 4.1.2 for $s = 0$ and $r \to \infty$, we get

$$|\hat{h}(x) - h(x)| \leq \frac{C(m)}{m^d-1}$$

If we use Eq. 4.1.1 again with $m^s x$ in pace of x and $n \in \mathcal{N}$, we get

$$\begin{aligned} \hat{h}(nx) &= \lim_{s\to\infty} m^{-sd}(h(m^s nx) - n^d h(m^s x) + n^d h(m^s x)) \\ &= n^d \hat{h}(x) \end{aligned}$$

We have proved the existence of a homogeneous function $\hat{h}$ of degree d for $\mathcal{N}$, such that $\hat{h} - h$ remains bounded.

The above prove is known as Tate's limit argument.

If we combine the results above, then we obtain a canonical global height function associated to every class of $\mathrm{Pic}(A)$.

Corollary 4.1.2.1

Let $\mathscr{L} \in \mathrm{Pic}(A)$ and $\mathscr{L} = \mathscr{L}_+ + \mathscr{L}_-$ be a decomposition into even and odd parts. Then:

1. *the class $\mathbf{h}_{\mathscr{L}_\pm}$ are independent of the choice of the decomposition*
2. *there is a unique homogeneous height function $\hat{h}_{\mathscr{L}_\pm}$ in the class $\mathbf{h}_{\mathscr{L}_\pm}$, of degree 2 in the $+$ case, and degree 1 in the $-$ case*

Now all the results about heights on abelian varieties is now true for Néron-Tate heights as exact equations, not just up to bounded functions. More precisely, we have the following theorem.

Theorem 4.1.3

The Néron-Tate heights on abelian varieties has the following property:

1. *The map*
$$\hat{h} : \mathrm{Pic}(A) \to \mathbb{R}^{A(\overline{K})}, \quad \mathscr{L} \mapsto \hat{h}_{\mathscr{L}}$$
is a group homomorphism
2. *If $\phi : A \to B$ is a homomorphism of abelian varieties, then*
$$\hat{h}_{\phi^*\mathscr{L}} = \hat{h}_{\mathscr{L}} \circ \phi$$
for any $\mathscr{L} \in \mathrm{Pic}(B)$
3. *Let $\mathscr{L} \in \mathrm{Pic}(A)$ be even. If $\mathscr{L}$ is base-point free or ample, then $\hat{h}_{\mathscr{L}} \geq 0$*

Proof. Part (1) and (2) mostly just follow from Theorem 2.3.5 and Corollary 4.1.2.1. For part (3), note we may just assume $\mathscr{L}$ is base-point free, as if $\mathscr{L}$ just ample, then $m\mathscr{L}$ is very ample (hence base-point free) for some $m \gg 0$, but $m\hat{h}_{\mathscr{L}} = \hat{h}_{m\mathscr{L}}$. Thus WLOG assume $\mathscr{L}$ is base-point free and even. This means it induces a morphism $\phi : A \to \mathbb{P}^n$ for some n, so that $\phi^*\mathscr{O}_{\mathbb{P}^n}(1) \cong \mathscr{L}$. Thus h_ϕ is in the class of $\mathbf{h}_{\mathscr{L}}$. But we have seen in the proof of Lemma 4.1.2 that

$$\hat{h}_{\mathscr{L}}(a) = \lim_{n\to\infty} n^{-2} h_\phi(na)$$

for any $a \in A$. Since h_ϕ is non-negative, so is $\hat{h}_{\mathscr{L}}$.

Theorem 4.1.4

The Néron-Tate height $\hat{h}_{\mathscr{L}}$ is the unique quadratic function in the class $h_{\mathscr{L}}$. Moreover, $2\hat{h}_{\mathscr{L}_+}$ is the associated quadratic form and $2\hat{h}_{\mathscr{L}_-}$ is the associated linear form.

Proof. First, we note the function

$$b(a,a') := \hat{h}_{\mathscr{L}}(a+a') - \hat{h}_{\mathscr{L}}(a) - \hat{h}_{\mathscr{L}}(a')$$

is bilinear in a, a'. This follows from the Theorem of the cube 3.6.12, using Theorem 4.1.3. The associated quadratic and linear form are given by

$$\hat{h}_{\mathscr{L}}(a) \pm \hat{h}_{\mathscr{L}}(-a) = \hat{h}_{\mathscr{L}\pm[-1]^*\mathscr{L}}(a) = 2\hat{h}_{\mathscr{L}_\pm}(a)$$

again by Theorem 4.1.3.

It remains to prove uniqueness. By definition, the quadratic function is determined up to bounded functions. Hence the same is true for the associated quadratic/linear forms. Corollary 4.1.2.1 shows they are unique.

Now let A be an abelian variety over a field K with product formula.

Let M be an abelian group and b a real-valued symmetric bilinear form on M. The example we have in mind is $M = A(\overline{K})$ and certain bilinear form associated to a Néron-Tate height. The kernel of b is the abelian group

$$N := \{x \in M : b(x,y) = 0 \text{ for all } y \in M\}$$

Then b induces a symmetric bilinear form $\overline{b}$ on $\overline{M} = M/N$ and the kernel of $\overline{b}$ is zero. Since b is real valued, $\overline{M}$ is torsion free and all torsion elements of M are contained in N. We conclude

$$\overline{M} \to \overline{M}_{\mathbb{R}}, \quad \overline{m} \mapsto \overline{m} \otimes 1$$

is injective. Let $\overline{M}'$ be a f.g. subgroup of $\overline{M}$. The restriction of $\overline{b}$ to the free abelian group $\overline{M}'$ extends uniquely to a bilinear form $\overline{b}'$ on $\overline{M}'_{\mathbb{R}}$. Let $\overline{M}'_{\mathbb{Q}} = \overline{M}' \otimes_{\mathbb{Z}} \mathbb{Q}$. An easy argument shows $\overline{M}'_{\mathbb{Q}} \subseteq \overline{M}_{\mathbb{Q}}$ and $\overline{M}'_{\mathbb{R}} \subseteq \overline{M}_{\mathbb{R}}$. Since $\overline{M}_{\mathbb{R}}$ is the union of all $\overline{M}'$ and the bilinear forms $\overline{b}'$ agrees on the overlaps, we have a unique extension of $\overline{b}$ to a bilinear form $b_{\mathbb{R}}$ on $\overline{M}_{\mathbb{R}}$.

Now we would like that the bilinear form $b_{\mathbb{R}}(x,y)$ determines a scalar product and an associated norm $\|x\|^2 = b_{\mathbb{R}}(x,x)$ on $\overline{M}_{\mathbb{R}}$.

To this end, of course is necessary that $\overline{b}(x,x) > 0$ for all $0 \neq x \in \overline{M}$. Suppose that is the case. By clearing denominators, $\overline{b}(x,x) > 0$ for $x \in \overline{M}_{\mathbb{Q}} \backslash \{0\}$ and thus by continuity we see $b_{\mathbb{R}}(x,x) \geq 0$ for $x \in \overline{M}_{\mathbb{R}} \backslash \{0\}$. Note however this is not enough for $b_{\mathbb{R}}$ to be positive definite, as is seen in the following example.

Example 4.1.5

Let α be a transcendental number in $\mathbb{R}$, then the quadratic form in $\mathbb{R}^2$ given by

$q(\mathbf{x}) = (x_1 - \alpha x_2)^2$ is positive semidefinite. We have $q(\alpha, 1) = 0$ but $q(\mathbf{x}) > 0$ whenever $x \in \overline{\mathbb{Q}}^2 \backslash \{0\}$ as α is transcendental.

Lemma 4.1.6

With the notation and assumptions as above, the bilinear form $b_{\mathbb{R}}$ is positive definite if and only if for every finitely generated subgroup $\overline{M}'$ of $\overline{M}$ and every $C > 0$ the set

$$\{x \in \overline{M} : b_{\mathbb{R}}(x, x) \leq C\}$$

is finite.

Proof. We may assume $\overline{M}$ is finitely generated. Since $\overline{M}$ is torsion-free, its a lattice in $\overline{M}_{\mathbb{R}}$. If $b_{\mathbb{R}}$ is a scalar product, then there are only finitely many lattice points in a bounded set. This proves the result in one direction.

Conversely, assume that $b_{\mathbb{R}}$ is not positive definite. We may assume that $b_{\mathbb{R}}$ is positive semidefinite. Otherwise, the set

$$\{x \in \overline{M} : b_{\mathbb{R}}(x, x) \leq C\}$$

is clearly infintie. There is a $y \in \overline{M}_{\mathbb{R}} \backslash \{0\}$ such that $b_{\mathbb{R}}(y, y) = 0$. For $b_{\mathbb{R}}$ positive semidefinite, the Cauchy-Schwarz inequality is valid. Thus y is in the kernel of $b_{\mathbb{R}}$. By construction, the restriction of $b_{\mathbb{R}}$ to $\overline{M} \times \overline{M}$ has trivial kernel and hence $y \notin \overline{M}_{\mathbb{Q}}$.

Choose a basis $x_1, ..., x_r$ of $\overline{M}$. Its also a basis of $\overline{M}_{\mathbb{R}}$. For any $n \in \mathbb{N}$ there is a $y_n \in \overline{M}$ such that the coordinates of $y_n - ny$ are in the interval $[0, 1]$. The elements $y_n - ny$ are contained in the compact cube

$$\{\sum_{i=1}^{r} a_i x_i : 0 \leq a_i \leq 1\}$$

while on the other hand

$$b(y_n, y_n) = b(y_n - ny, y_n - ny)$$

Since $b_{\mathbb{R}}$ is continuous, its bounded on that cube, say C. Since $y \notin \overline{M}_{\mathbb{Q}}$, the set $\{y_n : n \in \mathbb{N}\}$ is infinite and contained in

$$\{x \in \overline{M} : b_{\mathbb{R}}(x, x) \leq C\}$$

This proves the lemma.

Now we will apply these considerations to $M = A(\overline{K})$. Let $\mathscr{L} \in \mathrm{Pic}(A)$ and b the bilinear form associated to the quadratic function $\hat{h}_{\mathscr{L}}$. The associated quadratic form and hence b itself depend only on $\mathscr{L}_+$ by Theorem 4.1.4. Hence we may assume $\mathscr{L}$ is even. In view of the paragraphs above (and below Theorem 4.1.4), we get a symmetric bilinear form $b_{\mathbb{R}}$ on $\overline{M}_{\mathbb{R}}$.

Assume $\mathscr{L}$ is also ample. Then $\hat{h}_{\mathscr{L}}$ is non-negative function by Theorem 4.1.3 and hence $b_{\mathbb{R}}$ is positive semidefinite. There are now two problems:

1. we would like to know the kernel N of b
2. we would like to have at our disposal the necessary and sufficient condition of Lemma 4.1.6 for a scalar product

The latter is satisfied if there are only finitely many L-rational points of bounded height relative to $\mathscr{L}$ for any finite field extension L/K. By Northcott's theorem 2.4.4, this holds for a number field.

Now we assume the condition of Lemma 4.1.6 holds. Our goal is to determine N. Let $x \in A$ be a point with $\hat{h}_{\mathscr{L}}(x) = 0$. Then for every integer n we have $\hat{h}_{\mathscr{L}}(nx) = n^2\hat{h}_{\mathscr{L}}(x) = 0$, hence the set $\{nx : n \in \mathbb{Z}\}$ is finite. By the pigeon-hole principle, there will be two distinct integers m, n so $nx = mx$. Hence x is a torsion point. We have already seen above the torsion elements of M are contained in side N, and hence N is the torsion subgroup of $M = A(\overline{K})$.

Theorem 4.1.7

Let K be a number field and $\mathscr{L}$ ample and even. Then $\hat{h}_{\mathscr{L}}$ vanishes exactly on the torsion subgroup of $A(\overline{K})$. Moreover, there is a unique scalar product $\langle \cdot, \cdot \rangle$ on the abelian group $A(\overline{K}) \otimes_{\mathbb{Z}} \mathbb{R}$ so

$$\hat{h}_{\mathscr{L}}(x) = \langle x \otimes 1, x \otimes 1 \rangle$$

for every $x \in A(\overline{K})$.

Proof. This follows from the above discussion, as $\overline{M}_{\mathbb{R}} = \overline{M} \otimes_{\mathbb{Z}} \mathbb{R}$ is canonically isomorphic to $M \otimes_{\mathbb{Z}} \mathbb{R}$, as N is the torsion subgroup of $M = A(\overline{K})$.

In the next result, we relate b to the Néron-Tate height of the Poincaré class.

Proposition 4.1.8

Let $\mathscr{L} \in \mathrm{Pic}(A)$ and b the symmetric bilinear form associated to $\hat{h}_{\mathscr{L}}$. Moreover, let $\mathscr{P} \in \mathrm{Pic}(A \times \hat{A})$ be the Poincaré class of A and $\phi_{\mathscr{L}} : A \to \hat{A}$ the homomorphism of Theorem 3.5.2. Then

$$b(a, a') = \hat{h}_{\mathscr{P}}(a, \phi_{\mathscr{L}}(a'))$$

for every $a, a' \in A(\overline{K})$.

Proof. By definition

$$\begin{aligned} b(a, a') &= \hat{h}_{\mathscr{L}}(a + a') - \hat{h}_{\mathscr{L}}(a) - \hat{h}_{\mathscr{L}}(a') \\ &= \hat{h}_{\mathscr{L}} \circ \tau_{a'}(a) - \hat{h}_{\mathscr{L}}(a) - \hat{h}_{\mathscr{L}}(a') \end{aligned}$$

For the moment, let us keep a' fixed and view the above as functions of a. By Theorem 2.3.5, we conclude

$$\hat{h}_{\mathscr{L}} + b(\cdot, a')$$

is a representative in the class $\mathbf{h}_{\tau^*_{a'}\mathscr{L}}$. Then the representative above is a quadratic function too, being a sum of a quadratic function and a linear form. Now Theorem 4.1.4 says

$$\hat{h}_{\tau^*_{a'}\mathscr{L}}(a) = \hat{h}_{\mathscr{L}}(a) + b(a,a')$$

and hence by Theorem 4.1.3 we see

$$b(a,a') = \hat{h}_{\phi_{\mathscr{L}}(a')}(a)$$

It follows that its enough to prove

$$\hat{h}_{\mathscr{L}'} = \hat{h}_{\mathscr{P}}(\cdot, \mathscr{L}') \qquad \text{(Eq. 4.1.3)}$$

for $\mathscr{L}' \in \hat{A} := \mathcal{P}\mathrm{ic}^0(A)$.

On the other hand, the point $\mathscr{L}'$ is the pullback of $\mathscr{P}$ to $A \times \{\mathscr{L}'\}$ (see Theorem 3.4.5), hence Eq. 4.1.3 holds up to a bounded function on $A(\overline{K})$ (by Theorem 2.3.5). In order to get equality, by Theorem 4.1.4 it is enough to show that $\hat{h}_{\mathscr{P}}$ is bilinear. If $a \in A$, then applying Theorem 4.1.3 to the homomorphism $\phi : A \to A \times \hat{A}$ given by $\phi(a) = (a, 0)$ and using $\phi^*\mathscr{P} = 0$ (Theorem 3.4.5), we get

$$\hat{h}_{\mathscr{P}}(a,0) = \hat{h}_{\phi^*\mathscr{P}}(a) = 0$$

In the same way we see

$$\hat{h}_{\mathscr{L}}(0,a') = 0$$

for $a' \in \hat{A}$. We conclude the bilinear form associated to the quadratic function $\hat{h}_{\mathscr{P}}$, evaluated at $((a,0),(0,a'))$, is equal to $\hat{h}_{\mathscr{P}}(a,a')$. This proves bilinearity.

Corollary 4.1.8.1

With the notation of the proof of Proposition 4.1.8, it holds

$$\hat{h}_{\tau^*_{a'}\mathscr{L}}(a) = \hat{h}_{\mathscr{L}}(a) + b(a,a')$$

$$\hat{h}_{\mathscr{L}'} = \hat{h}_{\mathscr{P}}(\cdot, \mathscr{L}')$$

Corollary 4.1.8.2

Let $\mathscr{L}' \in \mathrm{Pic}^0(A)$ and $\mathscr{L} \in \mathrm{Pic}(A)$ be an even ample class. Then

$$\hat{h}_{\mathscr{L}'} = O(\hat{h}^{1/2}_{\mathscr{L}})$$

Proof. Let $a \in A(\overline{K})$. Corollary 4.1.8.1 shows

$$\hat{h}_{\mathscr{L}'}(a) = \hat{h}_{\mathscr{P}}(a, \mathscr{L}')$$

By previous results, we know there is $a' \in A$ so $\mathscr{L}' = \phi_{\mathscr{L}}(a')$. Let b be the bilinear form associated to $\hat{h}_{\mathscr{L}}$. Then applying Proposition 4.1.8 we conclude

$$\hat{h}_{\mathscr{L}'}(a) = b(a,a')$$

We seen above (see here) that b induces a symmetric bilinear form on $A(\overline{K})\otimes_{\mathbb{Z}}\mathbb{R}$, which is positive semidefinite because $\hat{h}_{\mathscr{L}}$ is non-negative (see here and Theorem 4.1.3). So we can apply Cauchy-Schwarz to get

$$|\hat{h}_{\mathscr{L}'}(a)|^2 \leq b(a,a)\cdot b(a',a') = 4\hat{h}_{\mathscr{L}}(a)\cdot\hat{h}_{\mathscr{L}}(\phi_{\mathscr{L}}(a'))$$

This proves the claim.

Corollary 4.1.8.3

Let X be a projective smooth variety over K, $\mathscr{L}\in\mathrm{Pic}(X)$ be ample and $\mathscr{L}'\in\mathrm{Pic}(X)$ be algebraically equivalent to $\mathscr{L}$. Then

$$h_{\mathscr{L}'} = h_{\mathscr{L}} + O(|h_{\mathscr{L}}|^{1/2}+1)$$

Recall we say two line bundles $\mathscr{L}_1,\mathscr{L}_2$ on variety X are algebraically equivalent if there is irreducible smooth variety T and line bundle $\mathscr{L}$ on $X\times T$ so $\mathscr{L}_1\cong\mathscr{L}|_{X_{t_1}}$ and $\mathscr{L}_2\cong\mathscr{L}|_{X_{t_2}}$ for some $t_1,t_2\in T(K)$, where X_t is the fiber of X at t.

4.2 Néron-Tate Heights on Jacobians

This section is not needed until the proof of Falting's theorem.

Let C be an irreducible smooth projective curve of genus $g>0$ over a field K with product formula. By base change, we assume C has K-rational base point P_0. We denote the Jacobian of C by J and identify J with its dual $\hat{J}$ as in Theorem 3.7.10 and the paragraph above it. Then the Poincaré class $\mathscr{P}$ correspond to

$$\mathscr{P} = m^*\theta - p_1^*\theta - p_2^*\theta \in \mathrm{Pic}^0(J\times J)$$

where θ is the theta divisor defined in Definition 3.7.3, m the multiplication and p_i the projections.

Proposition 4.2.1

The Néron-Tate height $\hat{h}_{\mathscr{P}}: J(\overline{K})\to J(\overline{K})\to\mathbb{R}$ is a symmetric positive semidefinite bilinear form.

Proof. Using the above identification of J and $\hat{J}$ by ϕ_θ, Proposition 4.1.8 asserts $\hat{h}_{\mathscr{P}}$ is the symmetric bilinear form associated to the quadratic function $\hat{h}_\theta$. It remains to show positive semidefinite.

Let $\Delta: J\to J\times J$ be the diagonal homomorphism. Proposition 3.6.13 shows $[2]^*\theta = 3\theta+\theta^-$ where $\theta^- = [-1]^*\theta$ as usual. Thus

$$\begin{aligned}\Delta^*\theta &= (m\circ\Delta)^*\theta - (p_1\circ\Delta)^*\theta - (p_2\circ\Delta)^*\theta\\ &= [2]^*\theta - 2\theta\\ &= \theta+\theta^-\end{aligned}$$

For $a \in J(\overline{K})$, we see

$$\hat{h}_{\mathscr{P}}(a,a) = \hat{h}_{\theta+\theta^-}(a)$$

by Theorem 4.1.3 again. Since θ is ample (see Theorem 3.7.10), we see $\theta^- = [-1]^*\theta$ is also ample. Thus $\theta + \theta^-$ is an ample even class and the corresponding Néron-Tate height is a non-negative function (Theorem 4.1.3).

In light the above result, we will use the following notation for $a, a' \in J(\overline{K})$

$$\left\langle a, a' \right\rangle := h_{\mathscr{P}}(a,a')$$

$$|a| = \hat{h}_{\mathscr{P}}(a,a)^{1/2} = \hat{h}_{\theta+\theta^-}(a)^{1/2}$$

Definition 4.2.2

The symmetric positive semidefinite bilinear form $\langle \cdot, \cdot \rangle$ is called the ***canonical form*** of J.

In the following, for a divisor D, we will also use h_D to mean $h_{\mathscr{O}(D)}$.

Proposition 4.2.3: Mumford's Formula

Let Δ be the diagonal in $C \times C$ and $j : C \to J, P \mapsto [P] - [P_0]$ the natural embedding from Remark 3.7.4. Then for any $P, Q \in C(\overline{K})$,

$$\begin{aligned} h_\Delta(P,Q) = \frac{1}{2g}|j(P)|^2 + \frac{1}{2g}|j(Q)|^2 - \langle j(P), j(Q)\rangle \\ - \frac{1}{2g}\hat{h}_{\theta-\theta^-}(j(P)) - \frac{1}{2g}\hat{h}_{\theta-\theta^-}(j(Q)) + O(1) \end{aligned}$$

Proof. We denote $z := j(P)$ and $w := j(Q)$. By what was proved in Proposition 3.7.7 to Proposition 3.7.9, we see

$$(j \times j)^* \mathscr{P} = O(C \times \{P_0\} + \{P_0\} \times C - \Delta)$$

By Theorem 2.3.5 we see

$$h_\Delta(P,Q) = h_{C\times\{P_0\}}(P,Q) + h_{\{P_0\}\times C}(P,Q) - \langle z, w\rangle + O(1) \tag{Eq. 4.2.1}$$

By Theorem 2.3.5 again, we have

$$h_{C\times\{P_0\}}(P,Q) = h_{p_2^*[P_0]}(P,Q) = h_{[P_0]}(Q) + O(1) \tag{Eq. 4.2.2}$$

and similarly

$$h_{\{P_0\}\times C}(P,Q) = h_{[P_0]}(P) + O(1) \tag{Eq. 4.2.3}$$

Now Proposition 3.7.6 shows $g[P_0]$ is in the class $j^*\theta^-$ and Theorem 2.3.5 implies

$$\begin{aligned} h_{[P_0]}(P) &= \frac{1}{g}\hat{h}_{\theta^-}(z) + O(1) \\ &= \frac{1}{2g}|z|^2 - \frac{1}{2g}\hat{h}_{\theta-\theta^-}(z) + O(1) \end{aligned}$$

Now just substituting this in Eq. 4.2.2 and Eq. 4.2.3, and putting the result in Eq. 4.2.1 we are done.

Remark 4.2.4

Since $\theta - \theta^-$ is an odd class and $\theta + \theta^-$ is an even ample class, we get by Corollary 4.1.8.2

$$h_\Delta(P,Q) = \frac{1}{2g}|j(P)|^2 + \frac{1}{2g}|j(Q)|^2 - \langle j(P), j(Q)\rangle + O(|j(P)| + |j(Q)| + 1)$$

As shown by Mumford, this formula has some rather interesting consequences for curves of genus $g \geq 2$.

Proposition 4.2.5

Assume C has genus $g \geq 2$ and let $\cos\alpha \in (\frac{1}{g}, 1)$, $\epsilon > 0$. Then there is a constant $B = B(C, P_0, \epsilon) > 0$ so for any pair $(P,Q) \in C(\overline{K})^2$, one of the following four possibilities occurs:

1. $P = Q$
2. $\langle j(P), j(Q)\rangle < \cos\alpha \cdot |j(P)| \cdot |j(Q)|$
3. $\min(|j(P)|, |j(Q)|) \leq B$
4. $(2g\cos\alpha - 1 - \epsilon)\min(|j(P)|, |j(Q)|) \leq \max(|j(P)|, |j(Q)|)$

Proof. We may assume (1), (2) do not hold. Then we need to prove either (3) or (4) holds. Again, denote $z = j(P)$ and $w = j(Q)$ and assume $|z| \geq |w|$. By Remark 4.2.4 we have

$$\langle z, w\rangle + h_\Delta(P,Q) = \frac{1}{2g}|z|^2 + \frac{1}{2g}|w|^2 + O(|z| + 1)$$

Since $P \neq Q$ and Δ is an effective divisor, we may assume by Proposition 2.3.6 that $h_\Delta(P,Q) \geq 0$. Using the negation of (2), we conclude

$$(\cos\alpha)|z| \cdot |w| \leq \frac{1}{2g}|z|^2 + \frac{1}{2g}|w|^2 + O(|z| + 1)$$

We may also assume $|z| \geq 1$. We set $r = |z|/|w|$ and find from the preceding inequality that

$$\cos\alpha \leq \frac{1}{2g}(r + \frac{1}{r}) + O(\frac{1}{|w|})$$

We multiply the last inequality by $2g$, note $1/r \leq 1$ and find

$$2g\cos\alpha - 1 - O(\frac{1}{|w|}) \leq r = \frac{|z|}{|w|}$$

If we choose B sufficiently large, then either (3) or (4) holds.

Corollary 4.2.5.1

With the notation as above, let P,Q be points on C. Then, if $j(P)-j(Q)$ is in the kernel of $\langle\cdot,\cdot\rangle$, either $P=Q$ or $|j(P)|=|j(Q)|\leq B$. In particular if $j(P)-j(Q)$ is a torsion point and $|j(Q)|>B$, then $P=Q$.

The next goal of this section is to count rational points of C, assuming $g \geq 2$. As in above, the canonical bilinear form $b = \hat{h}_{\mathscr{P}}$ extends to a symmetric positive semidefinite bilinear form $\tilde{b}$ on $J(\overline{K}) \otimes_{\mathbb{Z}} \mathbb{R}$. Let $N_{\mathbb{R}}$ be its kernel; then $\tilde{b}$ induces a scalar product on $E := (J(\overline{K}) \otimes_{\mathbb{Z}} \mathbb{R})/N_{\mathbb{R}}$, again denoted by $\langle\cdot,\cdot\rangle$. By Corollary 4.2.5.1 we see the map

$$i : C(\overline{K}) \to E, \quad P \mapsto j(P) \otimes 1 + N_{\mathbb{R}}$$

is one-to-one on the subset of points P such that $|j(P)|>B$.

Definition 4.2.6

A point $P \in C(\overline{K})$ is called ***small*** if $|j(P)|\leq B$, otherwise its called ***large***.

Now let us fix $0<\alpha<\pi/2$ and $\epsilon>0$ so $1/g<\cos\alpha<1$ and $\lambda := 2g\cos\alpha - 1 - \epsilon > 1$. In the euclidean space $E = (J(\overline{K}) \otimes_{\mathbb{Z}} \mathbb{R})/N_{\mathbb{R}}$, we have the following geometric interpretation of Proposition 4.2.5. If P,Q are different large points such that $i(P)$ and $i(Q)$ includes an angle $\leq \alpha$ and if $|j(P)|\leq|j(Q)|$, then $\lambda|j(P)|\leq\lambda|j(Q)|$. THis shows we have gaps between points on C pointing in approximatively the same direction.

Let us consider the cone

$$T := \{x \in E : \langle x,a\rangle \geq \cos(\alpha/2)\cdot|x|\cdot|a|\}$$

with center 0, angle $\alpha/2$ and axis through $a \in E$. We order the large points in $C(\overline{K})$ mapping to T in a sequence $Q_0, Q_1, Q_2, \ldots$ such that

$$B < |j(Q_0)| \leq |j(Q_1)| \leq |j(Q_2)| \leq \ldots$$

The above shows $|j(Q_k)| \geq \lambda^k |j(Q_0)|$ for every k. For $H>B$, let $n_T(H)$ be the number of large points $Q \in C(\overline{K})$ mapping to T with $|j(Q)|\leq H$. We get

$$n_T(H) \leq \left\lceil \frac{\log(H/B)}{\log\lambda} \right\rceil$$

The above bound for $n_T(H)$ is uniform with respect to T (for a fixed angle) and yields a counting of all large $\overline{K}$-rational points of C mapping to T. This can be used,

in some circumstances, to count all large points in $C(K)$ with bounded height. To this end, it is necessary to assume $J(K)$ is finitely generated group. Another possibility consists of fixing a pirori a finitely generated subgroup Γ of $J(\overline{K})$, and consider only the subset of large points $P \in C(\overline{K})$ for which $j(P) \in \Gamma$. The question whether we can take $J(K)$ for such a group Γ can then be examined independently. As we shall see later, if K is a number field or function field over finite field then $J(K)$ is indeed finitely generated.

Thus let us fix a subgroup Γ of $J(\overline{K})$ of rank $r = \mathrm{rank}_{\mathbb{Q}}(\Gamma)$, where the rank is the maximum number of $\mathbb{Z}$-linearly independent elements of Γ.

We associate to Γ the finite-dimensional real vector subspace E_Γ spanned by the image of Γ in E, and its clear $\dim(E_\Gamma) \leq r$.

For $x \in E\backslash\{0\}$, we set $\nu(x) = x/|x|$. Then ν maps cones to spherical caps and we get a bound for the minimal number of cones needed to cover E_Γ from the following lemma.

Lemma 4.2.7

Let $\|\cdot\|$ be a norm on $\mathbb{R}^r$. Let E be a subset of the ball $B_t := \{\mathbf{x} \in \mathbb{R}^r : \|x\| \leq t\}$. Then for any $\epsilon > 0$, we can cover E with $(1 + 2t/\epsilon)^r$ translates, all centred on the set E, of the ball B_ϵ.

Corollary 4.2.7.1

Let $\|\cdot\|$ be a norm on $\mathbb{R}^r$ and $\rho > 0$. If $\mathbf{x}_1, ..., \mathbf{x}_n \in \mathbb{R}^r$ have norm 1 and if $\|\mathbf{x}_i - \mathbf{x}_j\| > \rho$ then $n \leq (1 + 2/\rho)^r$.

As a particular application of the above result, we get a finer bound on the number of large points.

Proposition 4.2.8

For $\rho = 2\sin(\alpha/2)$ and $r = \mathrm{rank}_{\mathbb{Q}}(\Gamma)$, the number $n_\Gamma(H)$ of large points Q with $j(Q) \in \Gamma$ and $|j(Q)| \leq H$ does not exceed

$$n_\Gamma(H) \leq \left\lceil \frac{\log(H/B)}{\log \lambda} \right\rceil \cdot \lfloor (1 + 2/\rho)^r \rfloor$$

In particular, $n_\Gamma(H) \ll \log H$.

Proof. For any $k \in \mathbb{N}$, we count the number of $Q \in C(\overline{K})$ with $\lambda^k B < |j(Q)| \leq \lambda^{k+1} B$. By the above paragraph, the angle between two such points Q, Q' is $> \alpha$. We conclude that $|\nu(Q) - \nu(Q')| > \rho$ for $\rho := 2\sin(\alpha/2)$. By Lemma 4.2.7.1, there are at most $(1 + 2/\rho)^r$ such points. Now the interval $(B, H]$ may be covered by $\lceil \log(H/B) \rceil$ such intervals, proving the claim.

Still assuming $g \geq 2$, take $\alpha = \pi/6$, $\epsilon > 0$ so $\lambda := 2g\cos\alpha - 1 - \epsilon \geq 2$ and $\rho = 2\sin(\pi/12) > \frac{1}{2}$. With this choice of parameters, we get the following result.

Theorem 4.2.9: Mumford's Gap Principle

Let C be irreducible smooth projective curve of genus $g \geq 2$ over K with base point $P_0 \in C(K)$ leading to a closed embedding j of C into the Jacobian J and Γ a subgroup of J of fintie $\mathbb{Q}$-rank r. Then there is a constant $B > 0$ depending on C and P_0, with the following properties:

1. *If we choose any cone T in E with center 0 and angle $\alpha/2$ and if we order $\{Q \in C : j(Q) \in \Gamma, |j(Q)| > B, i(Q) \in T\}$ by increasing norm, then $|j(Q_{n+1})| \geq 2|j(Q_n)|$ for every $n \in \mathbb{N}$*
2. *For $H > B$, the number $n_\Gamma(H)$ of points $Q \in C$ with $j(Q) \in \Gamma$, $B < |j(Q)| \leq H$ is bounded by*
$$n_\Gamma(H) \leq \left\lceil \frac{\log(H/B)}{\log 2} \right\rceil 5^r$$
3. *In particular, $n_\Gamma(2H) - n_\Gamma(H) \leq 2 \cdot 5^r$*

For small points, we must use a different method, which we will not include here.

Chapter 5

Mordell-Weil Theorem

The content of this chapter is to prove the following claim: the group of rational points of an abelian variety defined over a number field is finitely generated. With this, we can apply the counting we obtained in the end of last chapter to any abelian varieties.

The proof of the theorem consists of two stages:

1. we prove weak Mordell-Weil theorem: we show $A(K)/\phi(A(K))$ is finite for some non-trivial isogeny ϕ, normally $\phi = [m]$.
2. we use Fermat descent argument to conclude the proof

The explicit approach by Mordell (where he only proved for elliptic curves) used elliptic functions, and this is not practical enough to be carried out explicitly on elliptic curves, not to mention general abelian variety A. Thus for us we will use what's called Galois cohomology instead.

We will first give an elementary proof of weak Mordel-Weil for elliptic curves (with many parts skipped), then proceed to the actual proof of Mordel-Weil for general abelian varieties.

5.1 Weak Mordel-Weil Theorem for Elliptic Curves

In this section we prove the finiteness of $E(K)/2E(K)$, for an elliptic curve E over a field K of characteristic $\mathrm{char}(K) \neq 2$.

First recall we can view E as a plane curve in $\mathbb{P}^2_K$, given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

for some $a_i \in K$. Replacing y by $y - \frac{1}{2}(a_1x + a_3)$ (which is allowed as $\mathrm{char}(K) \neq 2$), we may assume $a_1 = a_3 = 0$. Thus we can assume the affine part of E has equation

$$y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

for $\alpha_i \in \overline{K}$.

The intersection of E with the line $\mathbb{P}^2_K \backslash \mathbb{A}^2_K$ is a divisor $3O$, and the point $O = (0:0:1)$ is an inflexion point of E, which is taken as the identity of the group multiplication. The affine part of E is just $E\backslash\{O\}$, and in what follows we often write a point $P \in E\backslash\{O\}$ as $P = (x, y)$ in the affine coordinate.

Proposition 5.1.1

Let $\alpha_i \in \overline{K}$ for $1 \leq i \leq 3$ and $f(x) = \prod(x - \alpha_i)$. Then $y^2 = f(x)$ is an elliptic curve over $\overline{K}$ if and only if the discriminant

$$D_f := \prod_{i \neq j} (\alpha_i - \alpha_j)$$

of f is not 0.

Since $\mathrm{char}(K) \neq 2$, we can actually describe the morphism $[2]$ explicitly, which we will do so now.

Let (x, y) be standard affine coordinates of E, recall the group law is given by Proposition 3.3.4.

Let $P = (x_0, y_0)$, then $-2P$ is equal to the third intersection point of the tangent at P with E. If $2P = -2P = O$, this tangent is vertical. Thus we get a description of the 2-torsion points:

Proposition 5.1.2

The group $E[2]$ of 2-torsion points of E consists of the identity element O and the points $(\alpha_i, 0)$, $i = 1, 2, 3$, of order 2.

Now let $P = (x_0, y_0) \in E(\overline{K})$ and suppose P is not a 2-torsion point. The tangent line at P has equation

$$y = ax + b$$

with a, b determined as in Proposition 3.3.4, i.e. $a = f'(x_0)/(2y_0)$ and $b = y_0 - ax_0$. In order to determine the x-coordinate of the third intersection point $-2P$, we eliminate y from the above equation and the equation $y^2 = f(x)$, obtaining

$$(ax + b)^2 - (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) = 0 \qquad \text{(Eq. 5.1.1)}$$

The polynomial on the left has a zero at x_0 of multiplicity at least 2 (it is 3 if P is a torsion point of order 3 on E), which accounts for two solutions. The third solution x_1 is the x-coordinate of $-2P$. Hence factoring the left-hand side of the above into linear terms gives

$$(ax + b)^2 - (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) = -(x - x_0)^2(x - x_1)$$

of cubic polynomials in x. We specialize x to α_i, and find

$$(a\alpha_i + b)^2 = -(\alpha_i - x_0)^2(\alpha_i - x_1)$$

and

$$x_1 - \alpha_i = \left(\frac{a\alpha_i + b}{x_0 - \alpha_i}\right)^2 \qquad \text{(Eq. 5.1.2)}$$

for $i = 1, 2, 3$. In affine coordinates, we conclude

$$2P = (x_1, -ax_1 - b)$$

Now suppose $\alpha_i \in K$ for $i = 1, 2, 3$. Then the above equation shows $x_1 - \alpha_i$ is a square in K for $i = 1, 2, 3$. The following result gives the converse.

Lemma 5.1.3

Under the hypotheses above, suppose $\alpha_i \in K$. Let (x_1, y_1) be the affine coordinates of a point $Q \in E(K)$, $Q \neq O$. Then $Q \in 2E(K)$ if and only if $x_1 - \alpha_i$ is a square in K for $i = 1, 2, 3$.

Next, we consider addition. Let $P_1, P_2, P_3 \in E(K)$ such that $P_1 + P_2 + P_3 = O$ and $P_i \neq O$ for $i = 1, 2, 3$. Let $y = ax + b$ be the line through P_1, P_2, P_3 and (x_i, y_i) be the affine coordinates of the points P_i. Say Equation Eq. 5.1.1 has roots x_1, x_2, x_3, giving

$$(ax + b)^2 - \prod_{i=1}^{3}(x - \alpha_i) = \prod_{i=1}^{3}(x_i - x) \tag{Eq. 5.1.3}$$

Now set $x = \alpha_i$ we get

$$(a\alpha_i + b)^2 = (x_1 - \alpha_i)(x_2 - \alpha_i)(x_3 - \alpha_3) \tag{Eq. 5.1.4}$$

for $i = 1, 2, 3$.

This gives us evidence for a group homomorphism $\phi_i : E(K) \to K^\times/(K^\times)^2$ given by

$$(x, y) \mapsto x - \alpha_i \pmod{(K^\times)^2}$$

However, this is defined only for $x \neq \alpha_i$. If we proceed as before but with $P_1 = (\alpha_i, 0)$, then differentiating Eq. 5.1.3 at the point α_i gives the equation

$$-(\alpha_i - \alpha_j)(\alpha_i - \alpha_k) = -(x_2 - \alpha_i)(x_3 - \alpha_i) \tag{Eq. 5.1.5}$$

where j, k are the remaining two indices. Now, as we will verify in a moment, we obtain a homomorphism

$$\phi = (\phi_1, \phi_2, \phi_3) : E(K) \to (K^\times/(K^\times)^2)^3$$

with

$$\phi_i(P) = \begin{cases} 1 & \text{if } P = O \\ x - \alpha_i \pmod{(K^\times)^2} & \text{if } P = (x, y), x \neq \alpha_i \\ (\alpha_i - \alpha_j)(\alpha_i - \alpha_k) & \text{if } P = (\alpha_i, 0) \end{cases}$$

where j, k denotes the two other indices.

Lemma 5.1.4

The map $\phi : E(K) \to (K^\times/(K^\times)^2)^3$ is a group homomorphism with kernel $2E(K)$.

Proposition 5.1.5

Let R be a unique factorization domain with quotient field K. Assume $\mathrm{char}(K) \neq 2$ *and the group of units $R^\times$ in R is finitely generated. Let E be the elliptic curve given by*

$$y^2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$$

where $\alpha_i \in R$ are distinct elements. Then

$$|E(K)/2E(K)| \leq 4^r \cdot 2^{\sum_{i<j} \omega(\alpha_j - \alpha_i)}$$

where $\omega(\alpha)$ denotes the number of distinct prime factors of $\alpha \in R\backslash\{0\}$ and r is the dimension of the $\mathbb{F}_2$-vector space $R^\times/(R^\times)^2$.

Proof. By Lemma 5.1.4 we have a homomorphism $\phi : E(K) \to (K^\times/(K^\times)^2)^3$ with kernel $2E(K)$. We need to estimate the cardinality of the image.

Let S be a set of representatives of the primes of R and $P \in E(K)\backslash\{O\}$ with affine coordinates (x, y). For $i = 1, 2, 3$, there are $b_i \in K$, $u_i \in R^\times$ and a_i a product of distinct primes of S such that

$$x - \alpha_i = b_i^2 u_i a_i \tag{Eq. 5.1.6}$$

It follows from

$$y^2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$$

that the primes of the denominator of x occur with even multiplicity. Therefore, a_i is coprime to the denominator of b_i and, substituting Eq. 5.1.6 into the last equation, we see $a_1a_2a_3$ and $u_1u_2u_3$ are squares in R. Hence there are $c_1, c_2, c_3 \in R$ pairwise coprime and product of distinct primes of S, such that

$$a_1 = c_2c_3, \quad a_2 = c_1c_3, \quad a_3 = c_1c_2$$

Let π be a prime of S dividing c_i. Since a_j and the denominator of b_j are coprime, π divides the numerator of $x - \alpha_j$ for $j \neq i$ and it follows that π divides $\alpha_j - \alpha_k$, where j, k are the other two indices. Therefore, the number of possibilities for π is bounded by $\omega(\alpha_j - \alpha_k)$ and there at most

$$2^{\sum_{i<j} \omega(\alpha_j - \alpha_i)}$$

such tuples (c_1, c_2, c_3).

The image of $R^\times$ in $K^\times/(K^\times)^2$ is isomorphic to $\mathbb{F}_2^r$, restricting the image of u_i to 2^r possibilities. We also know $u_1u_2u_3$ is a square, hence the number of triples (u_1, u_2, u_3) is bounded by 4^r. Finally, its easily seen the points of $\phi(E[2])$ may be represented by $(u_1c_2c_3, u_2c_3c_1, u_3c_1c_2)$ for admissible choices of u_i and c_j.

The following gives a special case of weak Mordell-Weil theorem for elliptic curves:

Corollary 5.1.5.1

Let E be an elliptic curve over a number field K with 2-torsion also defined over K. Then $E(K)/2E(K)$ is finite.

Proof. The ring of integers $\mathcal{O}_K$ is not necessarily a unique factorization domain. However, by the following Proposition, we can find a finite set of places S of K so for any finite set of places $T \in M_K$ with $T \supseteq S$, the ring R of T-integers in K is a unique factorization domain. Its group of units $R^\times$ is finitely generated by Dirichlet's unit theorem 1.2.7. We have seen in the above discussion and Proposition 5.1.2 that E is K-isomorphic to an elliptic curve of the form required in Proposition 5.1.5, because we can always enlarge the ring R so as to ensure that every $\alpha_i \in R$. The result now follows from Proposition 5.1.5.

Proposition 5.1.6

Let K be a number field. Then we can find a finite set of places S of K such that for any finite set of places $T \in M_K$ with $T \supseteq S$, the ring $\mathcal{O}_{T,K}$ is a principal ideal domain and hence a unique factorization domain.

If the 2-torsion of E is not defined over the number field K, we can still prove the finiteness of $E(K)/2E(K)$ by base change to a finite extension L/K over which the 2-torsion becomes rational. Then we use $E(L)/2E(L)$ is finite to show $E(L)$ is finitely generated by Fermat descent, and to conclude, by general results about abelian groups, that the subgroup $E(K)$ is also finitely generated of rank not exceeding the rank of $E(L)$.

Lemma 5.1.7

Let A be an abelian variety defined over K and L/K finite separable extension of K. Let m be a positive integer and suppose $A(L)/mA(L)$ is a finite group. Then $A(K)/mA(K)$ is a finite group.

Proof. Let $d = [L : K]$ and δ be a positive integer such that we can write $d = d_0 d_1$ with $d_0 \mid m^{\delta-1}$ and $\gcd(d_1, m) = 1$. Let $\mathcal{E}$ be the set of representatives of $A(L)/mA(L)$ in $A(L)$.

The group $A(L)/m^\delta A(L)$ is again a finite group, since a set of representatives for it is contained in the finite set

$$\mathcal{E}(\delta) := \mathcal{E} + m\mathcal{E} + \ldots + m^{\delta-1}\mathcal{E}$$

Let F be the Galois closure of L over K, let $G = \mathrm{Gal}(F/K)$, let H be the subgroup of G of index d fixing L, and denote by R a full set of representatives for the left cosets of H in G.

Let $x \in A(K) \subseteq A(L)$. Then we see

$$x - m^{\delta} y \in \mathcal{E}(\delta)$$

for some $y \in A(L)$. We apply the automorphisms $\sigma \in R$ to this equation and deduce

$$dx - m^{\delta} z \in \mathcal{E}'(\delta)$$

where $z := \sum_{\sigma} \sigma y$ and

$$\mathcal{E}'(\delta) := \left(\sum_{\sigma \in R} \sigma \right) \mathcal{E}(\delta)$$

Clearly, $z \in A(K)$ because any element $\tau \in \mathrm{Gal}(F/K)$ permutes the left cosets of H. Since d_0 divides $m^{\delta-1}$, we may divide by d_0, getting

$$d_1 x - m(m^{\delta-1}/d_0) z \in A(K) \cap \frac{1}{d_0} \mathcal{E}'(\delta)$$

and $A(K) \cap \frac{1}{d_0} \mathcal{E}'(\delta)$ is still a finite set (use Proposition 3.6.14).

Finally, since d_1 and m are coprime, the euclidean algorithm produces integers u and v so $d_1 u - mv = 1$. After multiplication by u, it follows

$$x - m((m^{\delta-1}/d_0) uz - vx) \in A(K) \cap \frac{1}{d_0} u \mathcal{E}'(\Delta)$$

Thus, combine this lemma with Corollary 5.1.5.1, we conclude the following theorem.

Theorem 5.1.8: Weak Mordell-Weil (for elliptic curves)

Let E be an elliptic curve defined over a number field K. Then $E(K)/2E(K)$ is finite.

5.2 Weak Mordell-Weil For Abelian Varieties

Before we proceed to give a proof, we need the following results.

Theorem 5.2.1: Chevalley-Weil Theorem

Let K be a number field, $\overline{K}$ an algebraic closure of K, and $\phi : Y \to X$ a finite unramified morphism of K-varieties. If X is complete, then there is a number field L, $K \subseteq L \subseteq \overline{K}$ such that $P \in Y(L)$ for any $P \in Y(\overline{K})$ with $\phi(P) \in X(K)$.

The form we will need is for abelian varieties. Let A be an abelian variety over K. For a non-zero integer m, we denote by $\frac{1}{m}A(K)$ the subset $[m]^{-1}A(K)$ of $A(\overline{K})$. For $S \subseteq A(\overline{K})$, the field $K(S)$ is the smallest intermediate field $K \subseteq L \subseteq \overline{K}$ with $S \subseteq A(L)$.

Corollary 5.2.1.1

Let A be an abelian variety defined over a number field K. Then $[K(\frac{1}{m}A(K)) : K] < \infty$.

Now, the main result we will prove in this section is the following.

Theorem 5.2.2: Weak Mordell-Weil

Let A be an abelian variety over a number field K and let m be a positive integer. Then $A(K)/mA(K)$ is finite.

To begin with, we need to introduce some notation. As usual, $\mathrm{Gal}(L/K)$ is the Galois group of L/K, where we fix an algebraic closure $\overline{K}$ and assume $\overline{K}/L$. Let $g \in \mathrm{Gal}(L/K)$ and X a variety over K. We view a point $x \in X(L)$ as belonging to some affine chart, with affine coordinates in L. Applying g^{-1} to the coordinates, we get well-defined point $x^g \in X(L)$. Clearly $x^{gh} = (x^g)^h$ and hence we have an action of $\mathrm{Gal}(L/K)$ on $X(L)$. If $\phi : X \to Y$ is a morphism over K, then $\phi(x^g) = \phi(x)^g$. If F denotes the fixed field of $\mathrm{Gal}(L/K)$ (i.e. $F := \{x \in L : gx = x \forall g \in \mathrm{Gal}(L/K)\}$), then $x \in X(F)$ is equivalent to $x^g = x$ for all $g \in \mathrm{Gal}(L/K)$. In particular, if X is abelian, then we have $(ma)^g = ma^g$ and $(a+b)^g = a^g + b^g$ for $a, b \in X(L)$ and $m \in \mathbb{Z}$.

Recall $A[m]$ is the m-torsion of A, i.e. the kernel of $[m] : A \to A$. The next statement is contained in the previous section (Lemma 5.1.7). We give an alternative proof using methods of Kummer theory.

Lemma 5.2.3

Let L be a finite Galois extension of K and $0 \neq m \in \mathbb{Z}$. If $A(L)/mA(L)$ is finite, then $A(K)/mA(K)$ is finite.

Proof. The inclusion $A(K) \subseteq A(L)$ induces a homomorphism

$$A(K)/mA(K) \to A(L)/mA(L)$$

of abelian groups. Let N be its kernel. Its enough to show N is finite. Choose a system of representatives in $A(K)$ for N. For each representative a, choose $b_a \in A(L)$ such that $a = mb_a$. Consider an element $g \in \mathrm{Gal}(L/K)$ and define

$$\lambda_a(g) := b_a^g - b_a$$

By the above, we see

$$m\lambda_a(g) = (mb_a)^g - mb_a = a^g - a$$

By K-rationality of a, this is zero. Using our system of representatives, the rule $a \mapsto \lambda_a$ defines a map from N to the set of maps

$$\mathrm{Gal}(L/K) \to A[m]$$

That is, we have

$$N \to \mathrm{Hom}_{(\mathbf{Grp})}(\mathrm{Gal}(L/K), A[m]), \quad a \mapsto \lambda_a$$

We see N will be finite if this map is injective and the range if finite. The latter follows from Proposition 3.6.14. In order to prove the former, suppose $\lambda_a = \lambda_{a'}$ for representatives a, a'. We have

$$b_{a'}^g - b_{a'} = b_a^g - b_a$$

and hence

$$(b_{a'} - b_a)^g = b_{a'} - b_a$$

for every g, or equivalently $b_{a'} - b_a \in A(K)$. Thus, applying $[m]$ we get $a = a'$.

An important step in the proof of weak Mordell-Weil is the generalization of some aspects of Kummer theory to abelian varieties.

Let $0 \neq m \in \mathbb{Z}$ be not divisible by $\mathrm{char}(K)$ and assume $A[m] \subseteq A(K)$. We denote the separable algebraic closure of K in $\overline{K}$ by K^s. For $a \in A(K)$, there is $b \in A(K^s)$ such that $a = mb$ (using $[m]$ is unramified from Proposition 3.6.14, every such $b \in A(\overline{K})$ is in $A(K^s)$). If $g \in \mathrm{Gal}(K^s/K)$, then we define

$$\langle a, g \rangle = b^g - b$$

By the above discussion, we see $\langle a, g \rangle \in A[m]$.

Let $a' \in A(K)$ and $b' \in A(K^s)$ with $a' = mb'$, then

$$(b + b')^g - (b + b') = (b^g - b) + (b'^g - b')$$

This shows $\langle a, g \rangle$ is independent of the choice of b. Moreover, we see $\langle \cdot, \cdot \rangle$ is linear in the first variable.

The map

$$\langle \cdot, \cdot \rangle : A(K) \to \mathrm{Gal}(K^s/K) \to A[m]$$

is called the ***Kummer pairing***. The right-kernel of $\langle \cdot, \cdot \rangle$ is defined by

$$\{g \in \mathrm{Gal}(K^s/K) : \langle a, g \rangle = 0 \forall a \in A(K)\}$$

and the left-kernel is defined similarly by

$$\{a \in A(K) : \langle a, g \rangle = 0 \forall g \in \mathrm{Gal}(K^s/K)\}$$

As in Corollary 5.2.1.1, let $K(\frac{1}{m}A(K))$ be the smallest intermediate field $K \subseteq L \subseteq \overline{K}$ such that for any $b \in A(\overline{K})$ with $mb \in A(K)$ is rational over L.

Proposition 5.2.4

The Kummer pairing is bilinear, with left-kernel $mA(K)$ and right-kernel the subgroup $\mathrm{Gal}(K^s/K(\frac{1}{m}A(K)))$ of $\mathrm{Gal}(K^s/K)$.

Proof. Let $g, g' \in \mathrm{Gal}(K^s/K)$. Using the notation and arguments of above paragraphs, we see

$$\left\langle a, gg' \right\rangle = b^{gg'} - b = (b^g - b)^{g'} + b^{g'} - b$$

Since $\langle a, g \rangle$ is K-rational by assumption, we get

$$\left\langle a, gg' \right\rangle = \langle a, g \rangle + \left\langle a, g' \right\rangle$$

This proves linearity in the second variable and thus $\langle \cdot, \cdot \rangle$ is bilinear.

For $a \in mA(K)$, choose $b \in A(K)$ such that $a = mb$. By K-rationality of b, we have

$$\langle a, g \rangle = b^g - b = 0$$

for every $g \in \mathrm{Gal}(K^s/K)$. Conversely, say a is in the left-kernel. For any $b \in A(K^s)$ with $a = mb$, we have

$$0 = \langle a, g \rangle = b^g - b$$

Since this is true for every $g \in \mathrm{Gal}(K^s/K)$ and since K is the fixed field of the Galois group, we conclude $b \in A(K)$. So the left-kernel is equal $mA(K)$.

Obviously $\mathrm{Gal}(K^s/K(\frac{1}{m}A(K)))$ is contained in the left-kernel H. On the other hand, let g be an element of the right-kernel. For $b \in A(K^s)$ with $mb \in A(K)$, we have $b^g = b$. It follows the restriction of g to the residue field $\kappa(b)$ is equal to the identity, hence the same is true for the restriction of g to $K(\frac{1}{m}(A(K)))$. This proves $H \subseteq \mathrm{Gal}(K^s/K(\frac{1}{m}A(K)))$, which proves the result.

Remark 5.2.5

It follows from Proposition 5.2.4 that the right-kernel is a closed normal subgroup of $\mathrm{Gal}(K^s/K)$. By Galois theory, $K(\frac{1}{m}A(K))$ is a Galois extension of K. By the same Proposition 5.2.4, we conclude the Kummer pairing induces a non-degenerate (i.e. left and right kernel equal zero) pairing

$$(A(K)/mA(K)) \times \mathrm{Gal}(K(\frac{1}{m}A(K))/K) \to A[m]$$

Thus in order to prove the finiteness of the group $A(K)/mA(K)$, its enough to show $\mathrm{Gal}(K(\frac{1}{m}A(K))/K)$ is finite.

Proof of Theorem 5.2.2. By Lemma 5.2.3 and Proposition 3.6.14, we may assume

$$A[m] \subseteq A(K)$$

Since K is a number field, we see $K(\frac{1}{m}A(K))/K$ is finite by Corollary 5.2.1.1. As we have seen in Remark 5.2.5, this is enough to conclude the proof.

5.3 Mordell-Weil Theorem

We will prove the following result.

Theorem 5.3.1: Mordell-Weil Theorem

If A is an abelian variety over a number field K, then $A(K)$ is a finitely generated abelian group.

In order to prove this, we need the Fermat descent:

Lemma 5.3.2

Let G be an abelian group and $m \geq 2$ a positive integer. Let also $\|\cdot\|$ a real function on G satisfying

$$\|x-y\| \leq \|x\| + \|y\|, \quad \|mx\| = m\|x\|$$

for any $x, y \in G$. Assume S is a set of representatives for G/mG, bounded relative to $\|\cdot\|$ by a constant C. Then for any $x \in C$, there is a decomposition

$$x = \sum_{i=0}^{l} m^i y_i + m^{l+1} z$$

where $y_i \in S$ and $z \in G$ satisfies $\|z\| \leq C+1$. In particular, G is generated by elements in the ball

$$\{x \in G : \|x\| \leq C+1\}$$

Proof. There are $y_0 \in S$, $x_0 \in G$ such that $x = y_0 + mx_0$. We have

$$\|x_0\| \leq \frac{1}{m}(C + \|x\|)$$

Proceeding by induction, there are $y_l \in S$, $x_l \in G$ such that $x_{l-1} = y_l + mx_l$ and

$$\|x_l\| \leq \left(\sum_{i=1}^{l+1} \frac{1}{m^i}\right) \cdot C + \frac{1}{m^{l+1}} \|x\|$$

We choose l so large that $\|x\| \leq m^{l+1}$ and set $z := x_l$, getting

$$\|z\| \leq \frac{1}{m-1} C + 1 \leq C + 1$$

Moreover, we have

$$x = y_0 + my_1 + \ldots + m^l y_l + m^{l+1} z$$

which proves the first claim. The second claim is a trivial consequence of the first.

Proof of Theorem 5.3.1. Choose an integer $m \geq 2$. The weak Mordell-Weil 5.2.2 gives finiteness of $A(K)/mA(K)$. By Proposition 3.6.4 there is an even ample $\mathscr{L} \in \mathrm{Pic}(A)$. By Theorem 4.1.7, the assumptions of Lemma 5.3.2 for $\|\cdot\| := \hat{h}_{\mathscr{L}}^{1/2}$ on $G := A(K)$ are satisfied. Thus Lemma 5.3.2 shows the group $A(K)$ is generated by a bounded set. Finally, Northcott's theorem 2.4.4 shows $A(K)$ is finitely generated.