Cor 2.4.2 For every $P \in E(\bar{K})$, the limit

$$\hat{h}(P) = \lim_{n \to \infty} \frac{1}{n^2} h_{[O]}(nP)$$ exists and it satisfies

a) $\hat{h}(P) \approx h_{[O]}(P)$

b) $\hat{h}(mP) = m^2 \hat{h}(P)$.

Def $\hat{h}(P)$ is called canonical / Neron-Tate height of P. (Some authors use $2\hat{h}$ instead!)

Pf Let C_n be the error bound from Thm 2.4.1:

$$|h(nP) - n^2 h(P)| \leq C_n \quad \forall P \in E(\bar{K}). \quad (I)$$

First prove the claim when only considering powers of two: $n = 2^e$.

$$(I) \Rightarrow \left| \frac{1}{4^e} h(2^e P) - \frac{1}{4^{e-1}} h(2^{e-1} P) \right| \leq \frac{C_2}{4^e}$$

$$\Rightarrow \left| \frac{1}{4^e} h(2^e P) - h(P) \right| \leq \underbrace{\frac{C_2}{4^e} + \frac{C_2}{4^{e-1}} + \dots + \frac{C_2}{4}}_{\xrightarrow[e \to \infty]{} \frac{C_2}{3} < \infty}$$

$\Rightarrow$ The limit $\lim_{e \to \infty} \frac{1}{4^e} h(2^e P)$ exists and

claim a) holds.

For b), note that

$$(I) \Rightarrow \left| \frac{1}{4^e} h(2^e m P) - \frac{m^2}{4^e} h(2^e P) \right| \leq \frac{C_m}{4^e}$$

$$\downarrow \qquad\qquad \downarrow \qquad\qquad \downarrow e \to \infty$$

$$\hat{h}(mP) \qquad\qquad m^2 \hat{h}(P) \qquad\qquad 0 .$$

For the limit's existence when considering all natural numbers n (not just powers of two):

Let D be the ~~error~~ bound from a).

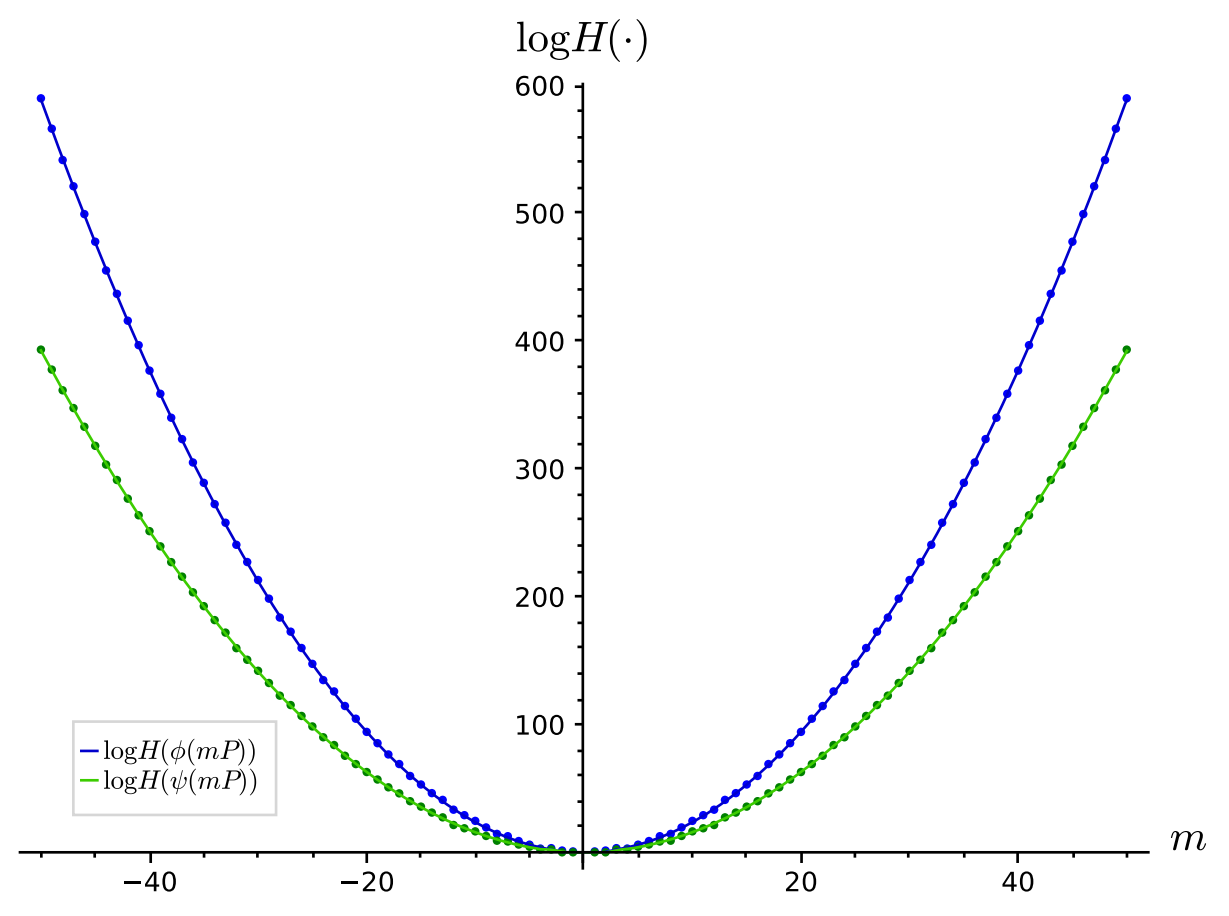
$$\left| \hat{h}(P) - h(P) \right| \leq D \qquad \forall P \in E(\bar{k}). \qquad (II)$$

$\Rightarrow$ For any n, we get

$$\left| \underbrace{\hat{h}(nP)}_{n^2 \hat{h}(P)} - h(nP) \right| \leq D$$

$$\Rightarrow \left| \hat{h}(P) - \frac{1}{n^2} h(nP) \right| \leq \frac{D}{n^2} \xrightarrow{n \to \infty} 0 .$$

□


$\log H(\cdot)$
600
500
400
300
200
100
m
−40
−20
20
40
$\log H(\phi(mP))$
$\log H(\psi(mP))$

Thm 2.4.3 Let $P \in E(\bar{k})$, TFAE:

a) P is a torsion-point ($nP = O$ for some $n \geq 1$)

b) $h_{(0)}(nP)$ is bounded for $n \in \mathbb{N}$.

c) $\hat{h}(P) = 0$.

Pf a) $\Rightarrow$ b) clear

b) $\Rightarrow$ c) clear

b) $\Rightarrow$ a) Let $P \in E(L)$ for a fin. ext. L/k.

$\Rightarrow nP \in E(L)\ \forall n \geq 1$

But for any $T \geq 0$, there are only finitely many $Q \in E(L)$ with $h_{(0)}(Q) \leq T$.

$\Rightarrow nP = mP$ for some $n \neq m$.

c) $\Rightarrow$ b) $\hat{h}(nP) = n^2 \hat{h}(P) = 0$

$\| \wr$

$h_{(0)}(nP)$

□

B. Divisors on higher-dimensional varieties

Let V be an n-dimensional smooth variety defined over K.

Def A (Weil) divisor on V (def. over K) is a finite formal sum

$$\sum_{\substack{W \subseteq V \\ (n-1)\text{-dimensional} \\ \text{irred. subvar.} \\ \text{def. over } K}} n_W W \qquad \text{with } n_W \in \mathbb{Z}.$$

Rmk $\mathcal{O}_{V,W} := \left\{ \frac{a}{b} \in K(V) \;\middle|\; b|_W \neq 0 \right\}$ is a discrete valuation ring. Denote the normalized valuation $v_{V,W}$ and a uniformizer by $t_{V,W}$.

("$v_{V,W}(f)$ is the mult. of a zero of f along W, negative if there's a pole along f")

Def The divisor associated to $f \in K(V)^\times$ is

$$\operatorname{div}(f) = \sum_W v_{V,W}(f)\, W.$$

Ex $V = \mathbb{A}^2_K$, $f = \dfrac{x^2 - y}{y^3}$

$\rightsquigarrow \operatorname{div}(f) = \{(x,y) : x^2 - y = 0\} - 3\cdot\{(x,y) : y = 0\}$.

Def For a morphism $\varphi : V \to V'$ between n-dimensional smooth varieties, the image of $D = \sum n_W W \in \operatorname{Div}(V)$ is

$$\varphi(D) = \sum_{\substack{W \subseteq V \\ \text{s.t.} \\ \overline{\varphi(W)} \subseteq V' \text{ is} \\ (n-1)\text{-dimensional} \\ (\text{it's always irreducible!})}} n_W \, \overline{\varphi(W)}$$

If φ is dominant, the pullback of $D' = \sum n_{W'} W' \in \operatorname{Div}(V')$ is

$$\varphi^*(D') = \sum_{\substack{W \subseteq V \\ \cdots \\ \text{s.t. } \overline{\varphi(W)} = W'}} n_{W'} e_{W|W'} W$$

with the ramification index $e_{W|W'} = v_{V,W}(t_{V',W'} \circ \varphi)$.

Def Fix a morphism $\varphi : V \longrightarrow \mathbb{P}^n_K$ whose image is not contained in any hyperplane $S \subseteq \mathbb{P}^n_K$, we associate the divisor class

$$D = \sum_{W \subseteq V} v_{V,W}\left(t_{\mathbb{P}^n_K, S} \circ \varphi\right) W \in \mathrm{Div}(V)$$

$\uparrow$

e.g. $\frac{a}{b}$ for lin. pol. $a, b \in K[x_0, \dots, x_n]$ where a vanishes on S and b vanishes on $S' \neq S$.

(Note that $\varphi(V) \subseteq S$ implies that $t_{\mathbb{P}^n_K, S} \circ \varphi$ is (for any S) a well-defined nonzero element of $K(V)$.)

Def A divisor $D \in \mathrm{Div}(V)$ is *very ample* if it is associated to some closed embedding $\varphi : V \longrightarrow \mathbb{P}^n_K$.

The question of very-ample-ness is more difficult than for curves, but at least:

Thm If V is a smooth proj. var., then any $D \in \mathrm{Div}(V)$ is the difference of two very ample divisors.

↝ The definition of heights $h_D : V(\bar{k}) \to \mathbb{R}$ works "like for curves" (and satisfies the same properties).

2.4. Heights of points on elliptic curves (cont.)

Generalization of Thm 2.4.1:

Thm 2.4.4

$$h_{(0)}(P+Q) + h_{(0)}(P-Q) \approx 2\left(h_{(0)}(P) + h_{(0)}(Q)\right)$$

$$\forall P, Q \in E(\bar{k}).$$

Sketch of pf (cf. Silverman, Thm VIII.6.2)

Consider $V = E \times E$ and the morphism

$$S : E \times E \longrightarrow \mathbb{P}^2 \times \mathbb{P}^2 \hookrightarrow \mathbb{P}^8$$

$$(P, Q) \longmapsto (\phi(P), \phi(Q))$$

$$(R, S) \longmapsto R \otimes S$$

$$([x:y:z], [x':y':z']) \mapsto [xx' : xy' : \dots : zz']$$

Consider the hyperplane $H := \{[v_0 : \dots : v_8] \mid v_8 = 0\}$.

Its preimage for $\mathbb{P}^2 \times \mathbb{P}^2 \hookrightarrow \mathbb{P}^8$ is

$$\left(\{[x:y:z] \mid z=0\} \times \mathbb{P}^2\right) \cup \left(\mathbb{P}^2 \times \{[x':y':z'] \mid z'=0\}\right).$$

$\Rightarrow$ Its preimage for Σ is

$$(\{0\}\times E)\cup(E\times\{0\}).$$

$\Rightarrow$ The divisor associated to $\Sigma: E\times E\to\mathbb{P}^8$ is

$$a\underbrace{\left((\{0\}\times E)+(E\times\{0\})\right)}_{=:D}, \text{ for some } a\geq 1$$

(actually $a=3$).

$$h_{aD}(P,Q)\approx h(\Sigma(P,Q))\approx h(\phi(P))+h(\phi(Q))$$

$$\approx 3h_{(0)}(P)+3h_{(0)}(Q)$$

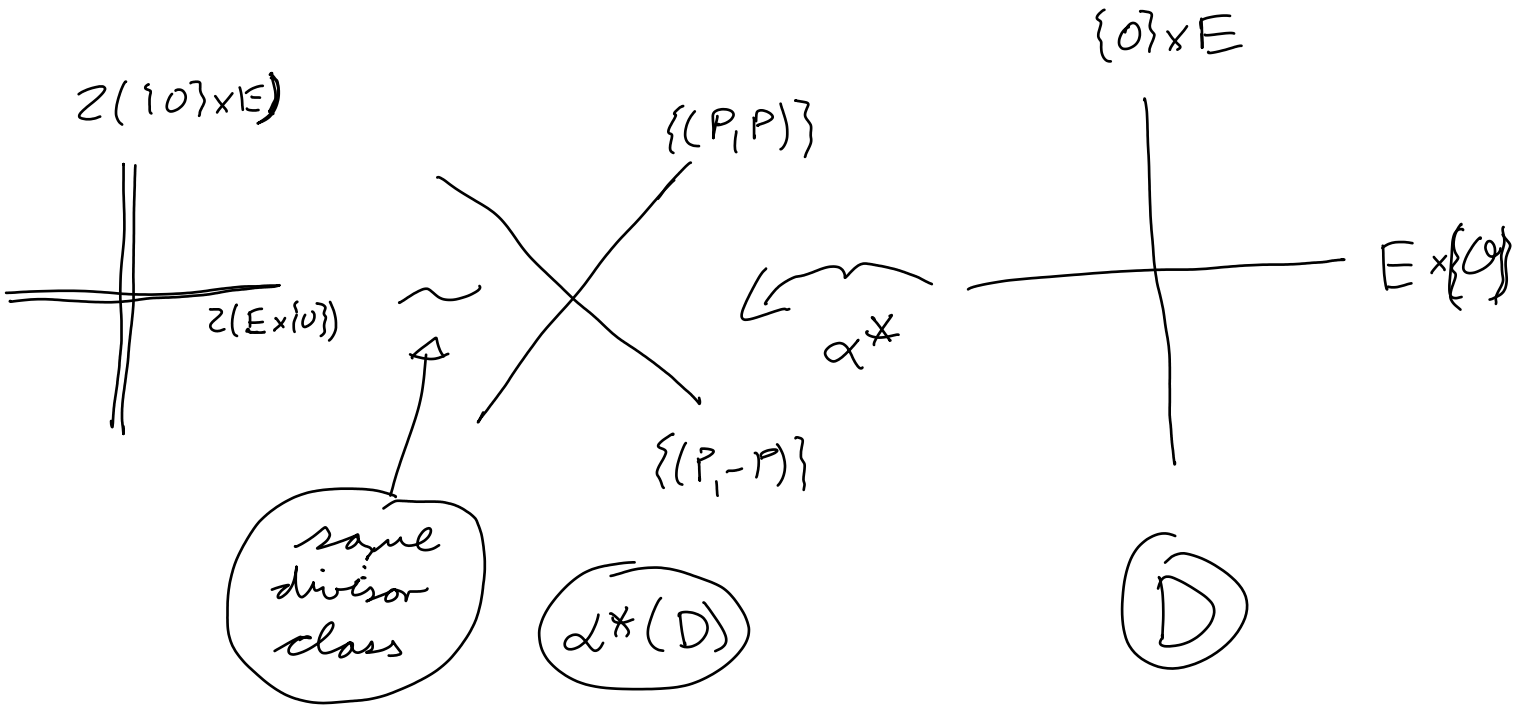
$$ah_D(P,Q)$$

$$\Rightarrow h_D(P,Q)\approx \frac{3}{a}\left(h_{(0)}(P)+h_{(0)}(Q)\right).$$

Consider the morphism

$$\alpha: E\times E\longrightarrow E\times E$$

$$(P,Q)\longmapsto(P+Q,P-Q).$$



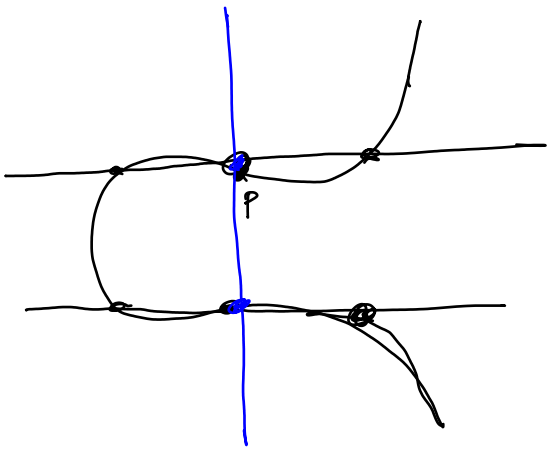
$$\alpha^*(D) = b\left(\{(P,P) \mid P \in E\} + \{(P,-P) \mid P \in E\} \right)$$

for some $b \geq 1$
(actually $b = 1$).

The rational function f on $E \times E$ given by

$$f(P,Q) = \cancel{y_P^2 - y_Q^2} \quad x_P - x_Q$$

for $\phi(P) = [x_P : y_P : 1]$, $\phi(Q) = [x_Q : y_Q : 1]$



has divisor

$$d\left(\{(P,P)\mid P\in E\}+\{(P,-P)\mid P\in E\}\right)$$

$$-d\left(\{O\}\times E+E\times\{O\}\right)$$

poles of x_P ↑ , poles of x_Q ↑

for some $c,d\geq 1$

(actually, $c=1$, $d=2$.)

$\Rightarrow c\cdot\alpha^*(D)$ lies in the same divisor class as $bd(\{O\}\times E+E\times\{O\})=bdD$.

$$\Rightarrow \underbrace{h_{cD}(\alpha(P,Q))}_{\| \; c\cdot h_D(P+Q,P-Q)} \approx h_{c\alpha^*(D)}(P,Q) \approx \underbrace{bdh_D(P,Q)}_{\geq \frac{3}{q}bd(h(P)+h(Q))}$$

$$\frac{3c}{q}\left(h(P+Q)+h(P-Q)\right)$$

$$\Rightarrow h(P+Q)+h(P-Q)\approx \frac{bd}{c}(h(P)+h(Q)).$$

$\forall P,Q\in E(\bar{k})$

For $P=Q$, we get

$$\underbrace{h(2P)}_{4h(P)}+\underbrace{h(O)}_{0}\approx 2\frac{bd}{c}h(P)\quad\forall P\in E(\bar{k}).$$

If $h(P)$ is unbounded (for $P \in E(\mathbb{R})$), this implies $\frac{bd}{c} = 2$,
(it is!)

so $h(P+Q)+h(P-Q) \approx 2(h(P)+h(Q))$.

If $h(P)$ were bounded, then trivially

$$h(P+Q)+h(P-Q) \approx 0 \approx 2(h(P)+h(Q)).$$

□