LECTURE 1 - SILVERMAN

CONSTRUCTION AND PROPERTIES OF CANONICAL HEIGHTS

K field, char 0
number field / 1-dim'l function field

Heights on $\mathbb{P}^N(K)$

$h : \mathbb{P}^N(K) \to [0,\infty)$

$h(P) =$ "# of bits it takes to store P"

$[a_0, a_1, \ldots, a_N]$

$=$ arithmetic complexity of P

$\#\{P \in \mathbb{P}^N(K) : h(P) \leq B\}$ is finite $\propto$

$h : \mathbb{P}^N(\overline{K}) \to [0,\infty)$

In general, for $P \in \mathbb{P}^N(L)$,

$h(P) \approx \frac{1}{[L:\mathbb{Q}]}$ # of bits

Weil Height Machine

X/K smooth proj. variety

$\varphi : X \hookrightarrow \mathbb{P}^N$

$h_{\varphi, X} = h \circ \varphi$

If D is ample divr $\in \mathrm{Div}(X)$,

choose n s.t. nD very ample

$\varphi_{nD} : X \hookrightarrow \mathbb{P}^N$

Def $h_{X,D} = \frac{1}{n} h_{\varphi_{nD}, X}$

$D \in \mathrm{Div}(X)$ arbitrary

$D = D_1 - D_2$, D_1, D_2 ample

$D = (mH + D) - mH$

$h_{X,D} = h_{X,D_1} - h_{X,D_2}$

Every $D \in \mathrm{Div}(X)$ has a Weil height $h_D : X(K) \to \cancel{\mathbb{Z}}\,\mathbb{R}$

Theorem:

1. If D is very ample, $\varphi_D : X \hookrightarrow \mathbb{P}^N$, then $h_D = h \circ \varphi_D + O(1)$

2. Linear Eq.
$$D \sim D' \Longrightarrow h_D = h_{D'} + O(1)$$

3. Functoriality
$$\varphi : X \to Y \Longrightarrow h_{X,\varphi^* D} = h_{Y,D} \circ \varphi + O(1)$$

4. Additivity
$$h_{D+D'} = h_D + h_{D'} + O(1)$$

Geometry $\Longrightarrow$ Arithmetic

5. (Northcott Property) D ample
$\{P \in X(K) : h_D(P) \leq B\}$ is finite

Canonical Heights

A = abelian variety

Def $D \in \mathrm{Div}(A)$

D is symmetric if $[-1]^* D \sim D$

antisymmetric if $[-1]^* D \sim -D$

$D \rightsquigarrow D + [-1]^* D$ symmetric

$[m] : A \to A$

Thm

$$[m]^* D \sim \frac{m^2+m}{2} D + \frac{m^2-m}{2} [-1]^* D$$

If D is symmetric,

$$[m]^* D \sim m^2 D$$

D symmetric

$[m]^* D \sim m^2 D$ geometry

$$h_D([m]P) = h_{[m]^* D}(P) + \underset{A,D,m}{O(1)}$$

$$= h_{m^2 D}(P) + O(1)$$

$$= m^2 h_D(P) + O(1)$$

$[m]P$ is m^2 more complex than P

Intuition

Note: That $O(1)$ is annoying!!

Theorem (Néron-Tate) 1960s

$$\hat{h}_D(P) = \lim_{n\to\infty} \frac{1}{4^n} h_D([2^n]P)$$

converges.

$\cancel{4^n h_D(P) + O_n(1)}$ e

$\boxed{\text{Canonical (Néron-Tate) height}}$

① $\hat{h}_D(P) = h_D(P) + O(1)$

contain arith complexity info

② $\hat{h}_D([m]P) = m^2 \hat{h}_D(P)$ No $O(1)$

③ $D' \sim D \implies \hat{h}_{D'} = \hat{h}_D$

Pf: $\left(4^{-n} h_D(2^n P)\right)_{n \geq 1}$ is Cauchy ✓

$$|h_D(2Q) - 4h_D(Q)| \leq C \quad (\ast)$$

$$\left|4^{-n} h(2^n P) - 4^{-k} h(2^k P)\right|$$

$$\leq \sum_{i=k}^{n-1} \left|4^{-(i+1)} h(2^{i+1} P) - 4^{-i} h(2^i P)\right|$$

$$= \sum_{i=k}^{n-1} 4^{-(i+1)} \left|h(\underbrace{2^{i+1}P}_{2Q}) - 4h(\underbrace{2^i P}_{Q})\right|$$

$$\leq \sum_{i=k}^{n-1} 4^{-(i+1)} C$$

$n \to \infty$

$$\leq \frac{C}{3 \cdot 4^k} \xrightarrow[k \to \infty]{} 0 \quad ✓$$

$k=0$ $\quad |4^{-n} h(2^n P) - h(P)| \leq \frac{C}{3}$

$$\left|4^{-n} h(2^n P) - h(P)\right| \le \frac{C}{3}$$

Let $n \to \infty$.

$$\left|\hat{h}(P) - h(P)\right| \le \frac{C}{3}$$

Theorem: D ample & symmetric

$$\hat{h}_D : A(K) \to \mathbb{R}$$

① $\hat{h}_D$ is a quadratic form

$$(P,Q) \to \underbrace{\frac{1}{2}\left(\hat{h}_D(P+Q) - \hat{h}_D(P) - \hat{h}_D(Q)\right)}_{\langle P,Q\rangle_D}$$

is bilinear,

② $\hat{h}_D(P) \geq 0 \quad \forall P \in A(\overline{K})$

③ $\hat{h}_D(P) = 0 \iff P \in A(\overline{K})_{tors}$

④ $\hat{h}_D$ extends to a pos def quad form on $A(K) \otimes \mathbb{R} \cong \mathbb{R}^{\operatorname{rank} A(K)}$

Def Néron - Tate regulator

Basis $P_1, \dots, P_r \in A(K)$ mod tors

$$\mathrm{Reg}(A/K) = \det\left(\langle P_i, P_j \rangle_D\right)_{1 \le i,j \le r}$$

$$> 0$$

$\boxed{\hat{h} \geq 0}$

$$D \text{ ample} \Rightarrow h_D(Q) \geq -C \quad \forall Q$$

$$\hat{h}_D(P) = \lim 4^{-n} h_D(2^n P)$$
$$\geq \lim 4^{-n} (-C)$$
$$= 0$$

$P \in A_{tors} \implies \hat{h}_D(P) = 0$

$$\hat{h}(P) = \lim_{n \to \infty} 4^{-n} \underbrace{h(2^n P)}_{\text{fin. many values}}$$

$= 0$ ✓

$$\hat{h}(P)=0 \implies P \text{ torsion}$$

$$\hat{h}(P)=0 \implies m^2\hat{h}(P)=0$$

$$\implies \hat{h}(mP)=0$$

$$\implies h(mP) < C$$

indep of m & P

$$\implies \{mP\in A(K) : m\in\mathbb{Z}\} \subseteq \underbrace{\{Q\in A(K) : h_D(Q)\le C\}}_{\text{finite set}}$$

$$\implies \exists\, m_1 > m_2 \text{ s.t. } m_1P = m_2P$$

$$\implies P\in A_{\text{tors}}.$$

$$D \sim D'$$

$$\frac{h_D(2^n P)}{4^n} = \frac{h_{D'}(2^n P)}{4^n} + \cancel{\frac{O(1)}{4^n}}$$

$$\frac{1}{4^n} h(2^n P)$$

$$\hat{h}(P) = \lim \frac{1}{4^n} h(2^n P)$$

$$h(mP) = m^2 h(P) + O(1)$$

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

$$h(2P) = 4h(P) + O(1)$$

$$\exists ?\ 0 \neq \hat{h}(P) \notin \overline{\mathbb{Q}}$$

$\langle \, , \, \rangle_D$

$$A(K) \otimes \mathbb{R} = \mathbb{R}^r$$
$$\cup \text{ lattice}$$
$$A(K)/A(K)_{tors}$$

Reg = covolume of $A(K)/A(K)_{tors}$ in $A(K) \otimes \mathbb{R}$

2