§1 Weak Mordell-Weil

$K/\mathbb{Q}$ finite, E/K EC.

Prop (weak M-W) $E(K)/nE(K)$ is fin gen ab grp.

Lem If L/K finite Galois, $E(L)/n\cdot E(L)$ fin gen, then also $E(K)/n\cdot E(K)$ is.

Proof $\mathrm{Image}\left(E(K)/nE(K) \xrightarrow{\alpha} E(L)/nE(L) \right)$

is fin gen, so need to show $\ker(\alpha)$ fin gen.

$$\ker(\alpha) = \frac{E(K) \cap nE(L)}{n\cdot E(K)}.$$

Define a map (not group homs usually)

$$\ker(\alpha) \xrightarrow{c} \mathrm{Map}(G_{L/K}, E[n](L))$$

$$P \longmapsto [c_P : \sigma \longmapsto \sigma(Q) - Q]$$

$$Q \in E(L),\ n\cdot Q = P$$

(Left to reader:

c well-defined, $c_{P_1+P_2} = c_{P_1} + c_{P_2}$,

factors over P mod $n\cdot E(K)$.)

Rmk $c_P \in H^1(G_{L/K}, E[n](L))$.

Then $c_{P_1} = c_{P_2} \iff \sigma(Q_1 - Q_2) = Q_1 - Q_2 \ \forall \sigma$

$$\iff Q_1 - Q_2 \in E(k)$$

$$\iff P_1 - P_2 \in nE(k).$$

Thus c injects $\ker(\alpha)$ into a finite set, hence $\ker(\alpha)$ finite. $\square$

<u>Proof of weak M-W</u> May now assume $E[n](k) = E[n](\bar{K})$.

Let $\mathcal{E} \to S = \operatorname{Spec} \mathcal{O}_k[B^{-1}]$ be an EC extending E where $n \mid B$. ($B \in \mathbb{Z}$ product of "bad primes" and n.)

Seen before $\mathcal{E} \xrightarrow{[n]} \mathcal{E}$ is étale.

Given $a \in E(K)$, valuative criterion ensures extension

$$\begin{array}{ccc} S & \xrightarrow{\tilde{a}} & \mathcal{E}. \\ \uparrow & & \uparrow \\ \operatorname{Spec} k & \xrightarrow{a} & E \end{array}$$

Then $[n]^{-1}(\tilde{a}) := \mathcal{E} \underset{[n], \mathcal{E}, \tilde{a}}{\times} S \longrightarrow S$ is étale since this property is stable under base change.

Recall that a finite extension L/K is unramified outside B $\Leftrightarrow$ $\mathcal{O}_K[B^{-1}] \to \mathcal{O}_L[B^{-1}]$ is étale.

In our situation, $[n]^{-1}(a) = \coprod_{i \in I} \operatorname{Spec} K_i$

for certain finite K_i/K and

$[n]^{-1}(\tilde{a}) = \operatorname{Spec} \mathcal{O}$ for some $\mathcal{O}_K[B^{-1}]$-order $\mathcal{O} \subseteq \prod K_i$.

Recall $X \to Y$ smooth & Y regular $\Longrightarrow$ X regular.

Since $\mathcal{O}_K[B^{-1}] \to \mathcal{O}$ étale & $\mathcal{O}_K[B^{-1}]$ normal, also $\mathcal{O}$ is normal, so $\mathcal{O} = \prod \mathcal{O}_{K_i}[B^{-1}]$.

Conclusion Each K_i/K unramified outside B.

Recall $L_1, L_2 / K$ unramified outside B

$\Rightarrow$ any composite $M = L_1 \cdot L_2 / K$ unramified outside B.

Namely $\mathcal{O}_{L_1}[B^{-1}] \underset{\mathcal{O}_K}{\otimes} \mathcal{O}_{L_2}[B^{-1}] \longrightarrow \mathcal{O}_M[B^{-1}]$

is finite, but $\mathcal{O}_{L_1}[B^{-1}] \otimes_{\mathcal{O}_K} \mathcal{O}_{L_2}[B^{-1}]$ normal, so $\mathcal{O}_M[B^{-1}]$ is direct factor.

We conclude: $K([n]^{-1}(a)) / K$ is unramified outside B.

<u>Shown two lect. ago (use $E[n](K) = (\mathbb{Z}/n)^{\oplus 2}$)</u>:

$K([n]^{-1}(a)) / K$ is Galois with $G \hookrightarrow (\mathbb{Z}/n)^{\oplus 2}$.

In partic., $[K([n]^{-1}(a)) : K] \leq n^2$.

<u>Thm (Hermite-Minkowski)</u> There are only fin. many $L/\mathbb{Q}$ of deg d, unramified outside a given set B.

Conclusion $L := K([n]^{-1}E(K))/K$ is a finite extension.

Recall We constructed an injective homomorphism

$$G_{L|K} \longrightarrow \mathrm{Hom}(E(K), E[n](K))$$
$$\sigma \longmapsto \left[P \overset{\lambda_\sigma}{\longmapsto} \sigma(Q) - Q \right]$$
$$n \cdot Q = P$$

Refinement $G_{L|K} \times E(K)/mE(K) \longrightarrow E[n](K)$

$$(\sigma, P) \longmapsto \lambda_\sigma(P)$$

is a perfect pairing ie also

$$E(K)/_{n E(K)} \longrightarrow \mathrm{Hom}(G_{L|K}, E[n](K))$$

is injective.

Proof If $\lambda_\sigma(P) = \sigma(Q) - Q = 0 \ \forall \sigma$

and some $Q \in E(L)$, $n \cdot Q = P$, then

$Q \in E(L)^{G_{L|K}} = E(K)$, hence $P \in nE(K)$ $\square$

Conclusion $\# E(K)/_{nE(K)} = \# G_{L|K} < \infty$.

$\square$ weak M-W.

§2 An abstract principle

References

Appendix II to Mumford's AV

Silverman's ECs

Prop Γ ab. grp s.th.

1) $\Gamma / n\Gamma$ finite for some $n > 1$

2) $\exists$ symmetric bilinear $(\, , \,) : \Gamma \times \Gamma \longrightarrow \mathbb{R}$

a) $(x,x) \geq 0 \quad \forall x \in \Gamma$

b) $\forall C$, $\{ x \in \Gamma \mid (x,x) \leq C \}$ is finite.

Then Γ is fin generated.

Proof $x_1, \ldots, x_s \in \Gamma$ representatives of $\Gamma / n\Gamma$ $n > 1$.

Schwartz inequality: $x \in \Gamma$ any, $1 \leq i \leq s$

$$(px + qx_i, \, px + qx_i)$$

$$= p^2 (x,x) + 2pq (x, x_i) + q^2 (x_i, x_i) \geq 0 \quad \forall p, q \in \mathbb{Z}$$

$\Leftrightarrow$ $0 \geq$ Discriminant of

$$(x,x) T^2 + 2(x, x_i) T + (x_i, x_i)$$

$$= 4 (x, x_i)^2 - 4 (x_i, x_i)(x,x)$$

$\Leftrightarrow$ $(x, x_i) \leq (x,x)^{1/2} (x_i, x_i)^{1/2}$

So $\frac{(x,x)}{(x-x_i, x-x_i)} \sim 1$ for $(x,x) \gg 0$

Thus $\exists\ C>0$ s.th. $\forall i$

$$(x,x) > C \Rightarrow (x-x_i, x-x_i) < 2(x,x).$$

Set $M = \{x_1, \dots, x_s\} \cup \{x \in \Gamma \quad (x,x) \leq C\}$

<u>Claim</u> M generates Γ.

<u>Proof</u> Let $x \in \Gamma$ with $x > C$.

$\exists i$ s.th. $x - x_i = ny$ some $y \in \Gamma$.

Then $(y,y) = \frac{1}{n^2}(x-x_i, x-x_i)$

$$< \frac{2}{n^2}(x,x)$$

$$< (x,x).$$

Now use: $\{(x,x) \quad x \in \Gamma\} \subseteq \mathbb{R}$ lies discrete

by assumption b) $\square$

Obvious strategy now:

§1 showed $E(k)/nE(k)$ finite $\forall n$.

Need to construct $(\ ,\ )$ on $E(K)$ with a), b).

Will be the <u>Néron-Tate height pairing</u>.

§3 Height functions

$K \subset \overline{\mathbb{Q}}$, Σ_K places of K.

$\Sigma_K \ni v$ yields normalized $|\cdot|_v : K^\times \longrightarrow \mathbb{R}_{>0}$

$|\pi_v|_v = q_v^{-1}$, $\pi_v \in \mathcal{O}_{K_v}$ uniformizer , $q_v = |\mathcal{O}_{K_v}/\pi_v|$

(non-archimedean)

$|\alpha|_v = |\sigma(\alpha)|$ if $v \longleftrightarrow \sigma : K \longrightarrow \mathbb{R}$ (real)

$|\alpha|_v = |v(\alpha)|^2$ if $v \longleftrightarrow \{\sigma, \overline{\sigma}\} : K \longrightarrow \mathbb{C}$ (complex)

<u>Product formula</u> $\displaystyle\prod_{v \in \Sigma_K} |\alpha|_v = 1$.

<u>Def</u> <u>Standard height</u> $h : \mathbb{P}^n(\overline{\mathbb{Q}}) \longrightarrow \mathbb{R}$

$$h(x) := \frac{1}{[K:\mathbb{Q}]} \log \prod_{v \in \Sigma_K} \max\{|x_0|_v, \dots, |x_n|_v\}$$

where K any with $x \in \mathbb{P}^n(K)$ and $x = [x_0 : \cdots : x_n]$

with $x_i \in K$.

1) Normalization $\frac{1}{[K:\mathbb{Q}]}$ ensures independence of K.

(At non-archimedean v, this is formula

$$[L:K] = \sum_{w|v} f_w \cdot e_w.)$$

2) Product formula ensures independence of x_i:

$$[x_0 : \dots : x_n] = [\lambda x_0 : \dots : \lambda x_n]$$

3) Clear: $\prod_i \max_j \{a_{ij}\} \geq \max_j \prod_i \{a_{ij}\}$

So product formula $\Longrightarrow$ $h(x) \geq 0 \quad \forall x$.

<u>Example</u> $h([x_0 : \dots : x_n]) = \log \max |x_i|$

whenever $x_i \in \mathbb{Z}$, $\gcd(x_i) = 1$.

In this case $h(x)$ measures "size" in a very naive sense.

<u>Lem</u> $A \in GL_{n+1}(\overline{\mathbb{Q}})$. Then $\exists$ constant C_A s.th.

$$h(Ax) \leq h(x) + C_A \quad \forall x.$$

<u>Proof</u> (v non-arch)

$$\log \Big|\sum_j a_{ij} x_j\Big|_v \leq \max_j \log |x_j|_v + \max_j \log |a_{ij}|$$

resp. $\leq \max_j \log|x_j|_v + \max_j \log|x_j|_v$

$+ \log(n+1)$

Thus, picking K with $A \in GL_{n+1}(K)$, may put

$$C_A = \log \prod_{v \in \Sigma_K} \max_{i,j} |a_{ij}|_v + \underbrace{\log(n+1)}_{[K:\mathbb{Q}]}$$

$\square$

Important observation: Lemma also applies to A^{-1}, so coset $h + \{\text{bounded functions on } \mathbb{P}^n(\overline{\mathbb{Q}})\}$ is independent of coordinates on $\mathbb{P}^n$!

<u>Def</u> $X/\overline{\mathbb{Q}}$ variety, $h_1, h_2 : X(\overline{\mathbb{Q}}) \longrightarrow \mathbb{R}$ called

1) <u>equivalent</u> $:\overset{\text{def}}{\Longleftrightarrow}$ $h_1 - h_2$ bounded.

2) $\varphi : X \longrightarrow \mathbb{P}^n$ any. Then set

$$h_\varphi(x) := h(\varphi(x)).$$

Prop X/k proper, $\varphi : X \to \mathbb{P}^k$, $\psi : X \to \mathbb{P}^l$

s.th. $\varphi^* \mathcal{O}_{\mathbb{P}^k}(1) \cong \psi^* \mathcal{O}_{\mathbb{P}^l}(1)$.

Then $h_\varphi \sim h_\psi$.

(Reformulation: For globally generated $\mathcal{L}$ on X, the height defined from any choice of generating global sections only depends on $\mathcal{L}$, up to equivalence.)

Proof $s_0, \dots, s_k := \varphi^*(T_0, \dots, T_k) \in \Gamma(X, \mathcal{L})$

$s_{k+1}, \dots, s_n$ completing to K-basis of $\Gamma(X, \mathcal{L})$.

$\chi = [s_0 : \dots : s_n] : X \to \mathbb{P}^n$ resulting map.

To show $h_\varphi \sim h_\chi$. (* Footnote $\to$ cf. p. 13)

Easy direction: $\max_{i=0}^{k} |s_i(x)|_v \leq \max_{i=0}^{n} |s_i(x)|_v$

$\forall x, v$, so $h_\varphi \leq h_\chi$.

Interesting direction: $\mathrm{Im}(\chi)$ closed since X proper.

Say $\mathrm{Im}(\chi) = V_+(I)$ $I \subseteq K[T_0, \dots, T_n]$.

$s_i = T_i \mod I$ homogeneous

$$V_+(T_0) \cap \dots \cap V_+(T_k) \cap \mathcal{X}(X) = \emptyset$$

$$\Rightarrow \operatorname{rad}(S_0, \dots, S_k) = \left(K[T_0, \dots, T_n]/I\right)_+$$

In other words, $\exists\, q > 0$ s.th.

$$T_{k+i}^q = \sum_{j=0}^{k} F_{ij}(T_0, \dots, T_n)\, T_j \mod I$$

with $\deg F_{ij} = q-1$. $i = 1, \dots, n-k$

$\forall x, v$

$$\Rightarrow q\,|S_{k+i}(x)|_v \leq (q-1) \log \max_{j \leq n} |S_j(x)|_v$$

$$+ \log \max_{j \leq k} |S_j(x)|_v$$

$$+ C_v$$

with C_v from coefficients of the F_{ij}

+ additional constant at archimedean v

(log # monomials in F_{ij})

$\Big\}\ \neq 0$ only for fin many v

$$\Rightarrow \log \max_{j \leq n} |S_j(x)|_v \leq \log \max_{j \leq k} |S_j(x)|_v + C_v \qquad \square$$

* Footnote: The prev. Lem. already showed that h_χ (up to equivalence) is independent of the choice of basis of $\Gamma(X,\mathcal{L})$.

So the argument is

$$h_\varphi \underset{①}{\sim} h_\chi \underbrace{\sim}_{\text{from Lemma}} h_{\chi'} \underset{②}{\sim} h_\psi$$

:) χ' from completion of ψ to basis of $\Gamma(X,\mathcal{L})$

:) ① & ② same proof, so we only consider ①.

* Additional Footnote: Also pass to lin indep subset of $s_0, \ldots, s_k$ first

Thm (Weil) X proj var $/\overline{\mathbb{Q}}$

There is a unique way to define

$$\mathrm{Pic}\, X \longrightarrow \mathrm{Map}\left(X(\overline{\mathbb{Q}}), \mathbb{R}\right) \Big/ \text{Bounded fcts}$$

$$L \longmapsto h_L$$

s.th. 1) $h_{L_1 \otimes L_2} = h_{L_1} + h_{L_2}$

2) For L very ample, giving $\varphi : X \hookrightarrow \mathbb{P}^N$

$$h_L = h_\varphi .$$

Rmk Prev. prop shows that $h_L := h_\varphi$ is well-def in very ample case 2).

Proof Given L, write $L = L_1 \otimes L_2^{-1}$ with L_1, L_2 ample. Then 1) forces

$$h_L = h_{L_1} - h_{L_2} .$$

This is well defined if we can show

$h_{L_1 \otimes L_2} = h_{L_1} + h_{L_2}$ for very ample L_1, L_2.

Let $S_0, \dots, S_n$ resp. $T_0, \dots, T_m$ be generating sections for L_1 resp. L_2.

Then $\{ S_i \otimes T_j \}$ generate $L_1 \otimes L_2$.

By prev. prop, may be used to compute $h_{L_1 \otimes L_2}$.

Since
$$\max_{i,j} \left| S_i(x) \cdot T_j(x) \right|_v$$
$$= \max_i |S_i(x)| \cdot \max_j |T_j(x)| ,$$

get desired $h_{L_1 \otimes L_2} = h_{L_1} + h_{L_2}$. $\square$

§4 Northcott property

Clear from example: $\forall C$

$\{ x \in \mathbb{P}^n(\mathbb{Q}) , h(x) \leq C \}$ is finite.

Prop (Northcott) $\forall C, \quad d \in \mathbb{Z}_{\geq 0}$

$$\{ x \in \mathbb{P}^n(\overline{\mathbb{Q}}) , h(x) \leq C \quad [\mathbb{Q}(x):\mathbb{Q}] \leq d \} < \infty .$$

Proof By induction ok for $\mathbb{P}^{n-1}$ & degree $\leq d-1$.

So enough to consider

$$M = \{ x = [1 : x_1 : \dots : x_n] \in (\mathbb{P}^n \setminus \mathbb{P}^{n-1})(\overline{\mathbb{Q}}) \text{ s.th. } h(x) \leq C, \quad [\mathbb{Q}(x):\mathbb{Q}] = d \}$$

Define
$$M \xrightarrow{\tau} \mathbb{P}^{nd}(\mathbb{Q})$$
$$x \longmapsto [1 : \text{coeffs of all char pol of the } x_1, \dots, x_n \text{ for } \mathbb{Q}(x)/\mathbb{Q}.]$$

Then τ has finite fibers.

So enough to see **Claim** $\exists\, a, b > 0$ s.th.
$$h(\tau(x)) \leq a \cdot h(x) + b$$

Let $T^d + a_{d-1}T^{d-1} + \dots + a_0$

$$= \prod_{\sigma \in G_{\bar{\mathbb{Q}}|\mathbb{Q}} / G_{\bar{\mathbb{Q}}|K}} (T - \sigma(x))$$

be char poly of some $x \in K$, $[K:\mathbb{Q}] = d$.

Then $a_j = s_j(x, \sigma_1(x), \dots, \sigma_{d-1}(x))$

j-th elementary symmetric poly

We get $|a_j|_p^d = \prod_{v|p} |a_j|_v$ and

$$|a_j|_v \leq \begin{cases} \max_{v'|p} |x|_{v'}^j & (p < \infty) \\ \text{const} \cdot \max_{v'|p} |x|_{v'}^j & (p = \infty) \end{cases}$$

constant = # terms of s_j.

because $\{v' | p\} = G_{\bar{\mathbb{Q}}|\mathbb{Q}} \cdot v$ and thus

$$\max_i |\sigma_i(x)|_v = \max_{v'|p} |x|_{v'}.$$

Plug this into the defn. of height. $\square$

§5 Néron-Tate height

<u>Lem</u> (Tate) Γ ab grp, $h : \Gamma \to \mathbb{R}$ s.th. for $x_1, x_2, x_3 \in \Gamma$

$$h\left(\sum_i x_i\right) - \sum_{i<j} h(x_i + x_j) + \sum_i h(x_i) \sim 0$$

i.e. bounded on $\Gamma \times \Gamma \times \Gamma$

Then $\exists!$ symmetric bilinear

$$b : \Gamma \times \Gamma \to \mathbb{R}$$

and a unique linear

$$l : \Gamma \to \mathbb{R}$$

s.th. $h \sim \hat{h}$

$$\hat{h}(x) = \tfrac{1}{2} b(x, x) + l(x).$$

<u>Proof</u> $\beta(x_1, x_2) := h(x_1 + x_2) - h(x_1) - h(x_2).$

Then β is symmetric & bilinear up to a bounded fct on $\Gamma \times \Gamma \times \Gamma$:

$$\beta(x_1 + x_2, x_3) \sim \beta(x_1, x_3) + \beta(x_2, x_3)$$

Then $b(x_1, x_2) := \lim_{n \to \infty} 4^{-n} \beta(2^n x_1, 2^n x_2)$

<u>exists</u> and satisfies $b \sim \beta$ on $\Gamma \times \Gamma$.

(geometric series argument)

$$\lambda(x) := h(x) - \tfrac{1}{2} b(x,x)$$

is linear up to bounded fctn.

Then $\quad l(x) := \lim_{n\to\infty} 2^{-n} \lambda(2^n x)$

exists and $h \sim \hat{h} := \tfrac{1}{2} b + l$. $\square$

<u>Thm of Cube</u> (cf. AV Lect 20)

E/k EC, $\mathcal{L}$ an lb on E. Then, on $E\times E\times E$,

$$m^*\mathcal{L} \otimes \bigotimes_{i<j} (m_{ij}^*\mathcal{L})^{-1} \otimes \bigotimes_i p_i^*\mathcal{L} \cong \mathcal{O}_{E\times E\times E}.$$

<u>Cor / Defn</u> Case $k = \overline{\mathbb{Q}}$.

The height function $h_{\mathcal{L}} : E(\overline{\mathbb{Q}}) \to \mathbb{R}$ satisfies all assumption of Tate's Lemma.

$\Rightarrow \exists!\ \hat{h}_{\mathcal{L}} \sim h_{\mathcal{L}}$ of the form

$$\hat{h}_{\mathcal{L}}(x) = \tfrac{1}{2} b(x,x) + l(x).$$

<u>Canonical height</u> or <u>Néron-Tate height</u>

Proof of Mordell-Weil

Given E/K, pick $\mathcal{L}$ ample + symmetric,

meaning $[-1]^*\mathcal{L} \cong \mathcal{L}$.

For example, take $\mathcal{L} = \mathcal{O}([e])$.

Let $b(\ ,\ )$ be the quadratic form assoc. of $\hat{h}_{\mathcal{L}}$. Since $\hat{h}_{\mathcal{L}}(-x) = \hat{h}_{\mathcal{L}}(x)$, by the symmetry, actually

$$\hat{h}_{\mathcal{L}}(x) = \frac{1}{2} b(x,x)$$

Then b satisfies

a) $b(x,x) \geq 0 \quad \forall x$ (since h on $\mathbb{P}^n$ is ≥ 0)

b) $\{x \in E(K) \text{ s.th. } (x,x) \leq C\}$ finite for all C

by Northcott property for $\mathbb{P}^n$.

$\Longrightarrow$ Abstract principle from §2 applies and shows $E(K)$ fin gen. $\square$

Rmk All arguments work without change for abelian varieties.