Math 6170 C, Lecture on April 27, 2020

Yongchang Zhu

Plan

(1) VIII. §5. Heights on Projective Spaces (continued).

(2) VIII. §6. Heights on Elliptic Curves.

To define height function on projective spaces over a number field, we need to study absolute values on a number field first.

Let F be a number field.

$F = \mathbb{Q}$.

$$|a|_\infty = \max(a, -a)$$

is an absolute value (the usual absolute value).

For each prime p, we have p-adic absolute value defined by $|0|_p = 0$ and

$$|p^m \frac{b}{c}|_p = p^{-m},$$

$m \in \mathbb{Z}, , b, c \in \mathbb{Z} - \{0\},\ p \not| b,\ p \not| c.$

The above absolute values are called **standard absolute values** on $\mathbb{Q}$.

Let $M_{\mathbb{Q}}$ denote the set of standard absolute values. By Ostrowski Theorem, every absolute value on $\mathbb{Q}$ is equivalent to a unique standard absolute value, so $M_{\mathbb{Q}}$ can be viewed as the set of equivalence classes of absolute values on $\mathbb{Q}$.

Explicitly

$$M_{\mathbb{Q}} = \{|\ |_\infty, |\ |_2, |\ |_3, |\ |_5, |\ |_7, |\ |_{11}, \dots\}$$

Absolute Values on Number Fields.

For every number field K, if $| \ |: K \to \mathbb{R}_{\geq 0}$ is an absolute value, then the restriction of $| \ |$ on $\mathbb{Q}$ is an absolute value on $\mathbb{Q}$.

An absolute value on K is called a **standard absolute value** if its restriction on $\mathbb{Q}$ is a standard absolute value on $\mathbb{Q}$.

Let M_K be the set of standard absolute values on K.

There are two types absolute values on a number field K.

Archimedean absolute values: For every embedding

$$\sigma : K \to \mathbb{C},$$

The map

$$|\ |_\sigma : K \to \mathbb{R}_{\geq 0}, \quad |a|_\sigma = |\sigma(a)|$$

is an standard absolute value.

Non-Archimedean absolute values.
Let R_K be the ring of (algebraic) integers in K.

For every non-zero prime ideal $\mathfrak{q} \subset R_K$. The localization $R_\mathfrak{q}$ is a PID with a unique non-zero prime ideal. Assume it is $\pi R_\mathfrak{q}$.

Let $R_\mathfrak{q}^*$ be the group of units in $R_\mathfrak{q}$.
Every non-zeros element a in K can be written uniquely as

$$a = \pi^m u, \quad m \in \mathbb{Z}, u \in R_\mathfrak{q}^*$$

Then

$$\mathrm{ord}_\mathfrak{q} : K^* \to \mathbb{Z}, \quad \mathrm{ord}_\mathfrak{q}(a) = m$$

is discrete valuation.

So for any $r > 1$,

$$|a|_{\mathfrak{q},r} = r^{-\mathrm{ord}_{\mathfrak{q}}(a)}$$

is an absolute value. Different r's give equivalent absolute values.

There is only one r so that $|\ |_{\mathfrak{q},r}$ is a standard absolute value.

$\mathfrak{q} \cap \mathbb{Z}$ is a non-zero prime ideal in $\mathbb{Z}$, so

$$\mathfrak{q} \cap \mathbb{Z} = p\mathbb{Z}$$

We choose r such that

$$|p|_{\mathfrak{q},r} = r^{-\mathrm{ord}_{\mathfrak{q}} p} = p^{-1}$$

such r is unique. For this r, $|\ |_{\mathfrak{q},r}$ is a standard absolute value.

An absolute values on K obtained from prime ideals in R as above are called **non-Archimedean** absolute values.

Completion of K with respect to an absolute value.

If $| \, |_v$ is an absolute value on K, but taking Cauchy sequences with respect to $| \, |_v$, we get a field K_v, the completion of K with respect to $| \, |_v$.

If $| \, |_v$ is obtained by a complex embedding $K \to \mathbb{C}$, then $K_v = \mathbb{C}$.

If $| \, |_v$ is obtained by a real embedding $K \to \mathbb{R}$, then $K_v = \mathbb{R}$.

If $| \ |_v$ is obtained from a non-zero prime ideal $\mathfrak{q} \subset R$, then

$$K_v = \mathrm{Frac} \varprojlim R/\mathfrak{q}^n.$$

The p-adic absolute value on $\mathbb{Q}$ gives the completion $\mathbb{Q}_p$, the p-adic field.

Fields like K_v are the **characteristic zero local fields**.

An number field extension $K \subset K'$ gives a map

$$M_{K'} \to M_K$$

where the image of $|\ |_w \in M_{K'}$ in M_K is the restriction $|\ |_w$ on K. This map is surjective. If $w \in M_{K'}$ maps to $v \in M_K$, we write $w|v$ (read as w divides v).

Every number field K is an extension of $\mathbb{Q}$, so we have

$$M_K \to M_{\mathbb{Q}}$$

every Archimedean absolute value goes to $|\ |_\infty$, the usual absolute value on $\mathbb{Q}$.

Definition. For $v \in M_K$, let $w \in M_{\mathbb{Q}}$ be its restriction on $\mathbb{Q}$. That is $v|w$. Then K_v is an extension of $\mathbb{Q}_w$.

The **local degree** at v, denoted n_v, is given by

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

Theorem. Let K be a number field, for a standard absolute value $v \in M_{\mathbb{Q}}$,

$$\sum_{w \in M_K, w | v} n_w = [K : \mathbb{Q}].$$

Theorem (Extension Formula 5.2.)

Let $\mathbb{Q} \subset K \subset L$ be a tower of number fields, for $v \in M_K$,

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

Product Formula on $\mathbb{Q}$

For every $r \in \mathbb{Q}^*$, we have $|r|_v = 1$ for almost all $v \in M_{\mathbb{Q}}$ and

$$\Pi_{v \in M_{\mathbb{Q}}} |r|_v = 1.$$

Product Formula 5.3.

Let K be a number field, $x \in K^*$. Then $|x|_v = 1$ for almost all $v \in M_K$, and

$$\Pi_{v \in M_K} |x|_v^{n_v} = 1.$$

Definition.

Let $P \in \mathbb{P}^N(K)$ with homogeneous coordinates

$$P = [x_0, x_1, \ldots, x_N].$$

The **height** of P is defined by

$$H_K(P) = \Pi_{v \in M_K} \max(|x_0|_v, \ldots, |x_N|_v)^{n_v}$$

The infinite product on the right makes sense because almost all the terms are 1.

Proposition VIII 5.4.

Let $P \in \mathbb{P}^N(K)$.

(a) The height $H_K(P)$ does not depend on the choice of the homogeneous coordinates for P.

(b) Let L/K be a finite extension. Then

$$H_L(P) = H_K(P)^{[L:K]}.$$

Proof. (a) Choose another homogeneous coordinate of P:

$$[\lambda x_0, \ldots, \lambda x_N], \quad \lambda \in K^*$$

Then for each $v \in M_K$,

$$\max(|\lambda x_0|_v, \ldots, |\lambda x_N|_v) = |\lambda_v| \max(|x_0|_v, \ldots, |x_N|_v)$$

So

$$\begin{aligned}
&\Pi_{v \in M_K} \max(|\lambda x_0|_v, \ldots, |\lambda x_N|_v)^{n_v} \\
&= \Pi_{v \in M_K} |\lambda|_v^{n_v} \cdot \Pi_{v \in M_K} \max(|x_0|_v, \ldots, |x_N|_v)^{n_v} \\
&= \Pi_{v \in M_K} \max(|x_0|_v, \ldots, |x_N|_v)^{n_v}
\end{aligned}$$

(b).

$$
\begin{aligned}
H_L(P) &= \Pi_{w \in M_L} \max(|x_0|_w, \ldots, |x_N|_w)^{n_w} \\
&= \Pi_{v \in M_K} \Pi_{w|v} \max(|x_0|_w, \ldots, |x_N|_w)^{n_w} \\
&= \Pi_{v \in M_K} \Pi_{w|v} \max(|x_0|_v, \ldots, |x_N|_v)^{n_w} \\
&= \Pi_{v \in M_K} \max(|x_0|_v, \ldots, |x_N|_v)^{n_v [L:K]} \\
&= H_K(P)^{[L:K]}
\end{aligned}
$$

The height function on $\mathbb{P}^N(\mathbb{Q})$ is the same as the height function we defined earlier.

Example. $P = [\frac{2}{3}, -\frac{4}{5}, 1] \in \mathbb{P}^2(\mathbb{Q})$,
The earlier method gives:

$$P = [10, -12, 15]$$

$$H(P) = 15.$$

The new definition:

$$H_{\mathbb{Q}} = \Pi_{v \in M_{\mathbb{Q}}} \max(|\frac{2}{3}|_v, \ |-\frac{4}{5}|_v, \ |1|_v)$$

For $v = \infty$,

$$\max(|\frac{2}{3}|_\infty, |-\frac{4}{5}|_\infty, |1|_\infty) = 1$$

For $v = 2$,

$$\max(|\frac{2}{3}|_2, |-\frac{4}{5}|_2, |1|_2) = 1$$

For $v = 3$,

$$\max(|\frac{2}{3}|_3, |-\frac{4}{5}|_3, |1|_3) = 3$$

For $v = 5$,

$$\max(|\frac{2}{3}|_5, |-\frac{4}{5}|_5, |1|_5) = 5$$

For any other prime p,

$$\max(|\frac{2}{3}|_p, |-\frac{4}{5}|_p, |1|_p) = 1$$

So

$$H_{\mathbb{Q}}(P) = 15$$

Definition.

Let $P \in \mathbb{P}^N(\bar{\mathbb{Q}})$. The absolute height of P, denoted by $H(P)$, is defined as follows. Choose any number field K such that $P \in \mathbb{P}^N(K)$. Then

$$H(P) = H_K(P)^{1/[K:\mathbb{Q}]}.$$

Proposition 5.4 implies that the right hand side is independent of the choice of K.

Definition.

A morphism of degree d between projective spaces is a map

$$F : \mathbb{P}^N(\bar{\mathbb{Q}}) \to \mathbb{P}^M(\bar{\mathbb{Q}})$$

$$F(P) = [f_0(P), \ldots, f_M(P)]$$

where $f_0, \ldots, f_M \in \bar{\mathbb{Q}}[X_0, \ldots, X_N]$ are homogeneous polynomials of degree d with no common zeros in $\bar{\mathbb{Q}}$ other than $X_0 = X_1 = \cdots = X_N = 0$.

If F can be written with polynomials f_i having coefficients in K, then F is said to be define over K.

Theorem VIII 5.6.

Let $F : \mathbb{P}^N \to \mathbb{P}^M$ be a morphism of degree d. Then there are constants C_1 and C_2, such that for all $P \in \mathbb{P}^N(\bar{\mathbb{Q}})$,

$$C_1 \, H(P)^d \leq H(F(P)) \leq C_2 \, H(P)^d.$$

Theorem VIII 5.9.

Let

$$f(T) = a_d T^d + a_{d-1} T^{d-1} + \cdots + a_0 = a_d(T - \alpha_1)\cdots(T - \alpha_d) \in \bar{\mathbb{Q}}[T]$$

Then

$$2^{-d}\Pi_{j=1}^{d} H(\alpha_j) \leq H([a_0, \ldots, a_d]) \leq 2^{d-1}\Pi_{j=1}^{d} H(\alpha_j)$$

Theorem VIII 5.11.

Let C and d be constants. Then the set

$$\{P \in \mathbb{P}^N(\bar{\mathbb{Q}}) \mid H(P) \leq C,\ [\mathbb{Q}(P), \mathbb{Q}] \leq d\}$$

is finite.

VIII. §6. Heights on Elliptic Curves.

Let E/K be an elliptic curve over K (K is a number field). For every $f \in \bar{K}(E)$, $f \notin \bar{K}$, f defines a surjective morphism

$$f : E \to \mathbb{P}^1$$

$$P \mapsto \begin{cases} [f(P), 1] & \text{for } P \text{ not a pole of } f \\ [1, 0] & \text{for } P \text{ a pole of } f \end{cases}$$

Definition.

The **absolute logarithmic height** on projective space is the function

$$h : \mathbb{P}^N(\bar{Q}) \to \mathbb{R}$$

given by

$$h(P) = \log\ H(P).$$

Definition. Let $f \in \bar{K}(E)$ be a non-constant function. The **height** on E relative to f is the function

$$h_f : \ E(\bar{K}) \to \mathbb{R}$$

$$h_f(P) = h(f(P)).$$

Proposition VIII 6.1.

Let E/K be an elliptic curve and $f \in K(E)$ is a non-constant function. The for every C,

$$\{P \in E(K) \,|\, h_f(P) \leq C\}$$

is a finite set.

Proof.
The set

$$S_C = \{Q \in \mathbb{P}^1(K) \,|\, h(P) \leq C\}$$

is a finite set.
The set in question is $f^{-1}(S_C)$, since f is a finite-to-one map, so $f^{-1}(S_C)$ is a finite set.

Theorem VIII 6.2.

Let E/K be an elliptic curve K and $f \in K(E)$ be an non-constant even function (i.e., $f \circ [-1] = f$). Then for all $P, Q \in E(\bar{K})$,

$$h_f(P+Q) + h_f(P-Q) = 2h_f(P) + 2h_f(Q) + O(1)$$

$$K(E) = \mathrm{Frac}\, K[x,y]/\left(y^2 - (x^3 + Ax + B)\right)$$

We will prove the case $f = x$ first.

We need to following results in the proof:
Let $y^2 = x^3 + Ax + B$ be the equation of E.

(1) If $P = (x_1, y_1) \in E$, then $-P = (x_1, -y_1)$.

(2) If $P = (x_1, y_1), Q = (x_2, y_2) \in E$, then

$$x(P+Q) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

See Group Law algorithm in III §2, page 58

$$x_3 = x(P+Q) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

$$x_4 = x(P-Q) = \left(\frac{-y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

$$x_3 + x_4 = \frac{2(x_1 + x_2)(A + x_1 x_2) + 4B}{(x_1 + x_2)^2 - 4x_1 x_2}$$

$$x_3 x_4 = \frac{(x_1 x_2 - A)^2 - 4B(x_1 + x_2)}{(x_1 + x_2)^2 - 4x_1 x_2}$$

Proof of Theorem 6.2. for $f = x$.

$$\begin{array}{ccc} E \times E & \stackrel{G}{\to} & E \times E \\ \downarrow & & \downarrow \\ \mathbb{P}^1 \times \mathbb{P}^1 & & \mathbb{P}^1 \times \mathbb{P}^1 \\ \downarrow & & \downarrow \\ \mathbb{P}^2 & \stackrel{g}{\to} & \mathbb{P}^2 \end{array}$$

where $G : (P, Q) \mapsto (P + Q, P - Q)$
(to be continued)

Proof of Theorem 6.2 (continued). Two vertical arrow $E \times E \to \mathbb{P}^1 \times \mathbb{P}^1$ is

$$(P, Q) \mapsto (x(P), x(Q)).$$

Two vertical arrow $\mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^2$ is

$$([\alpha_1, \beta_1], [\alpha_2, \beta_2]) \mapsto [\beta_1\beta_2, \alpha_1\beta_2 + \alpha_2\beta_1, \alpha_1\alpha_2].$$

$g : \mathbb{P}^2 \to \mathbb{P}^2$ is

$$[t, u, v] \mapsto [u^2 - 4tv, 2u(At + v), (v - At)^2 - 4Btu]$$

The above diagram is commutative,
that is, $g(\sigma(P, Q)) = \sigma(P + Q, P - Q)$.

Idea:

$$h_x(\sigma(P, Q)) \sim h_x(P) + h_x(Q)$$

$$h_x(\sigma(P + Q, P - Q)) \sim h_x(P + Q) + h_x(P - Q)$$

Because $g(\sigma(P, Q)) = \sigma(P + Q, P - Q)$, because $\deg g = 2$, so by Theorem 5.6,

$$h_x(\sigma(P + Q, P - Q)) \sim 2\, h_x(\sigma(P, Q))$$

Therefore

$$h_x(P + Q) + h_x(P - Q) \sim 2(h_x(P) + h_x(Q))$$

End