Math 6170 C, Lecture on April 22, 2020

Yongchang Zhu

Plan

(1) Elliptic Curves over $\mathbb{R}$.

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

Elliptic Curves over $\mathbb{R}$.

Assume E is an elliptic curve over $\mathbb{R}$, its Weierstrass equation can be written as

$$y^2 = x^3 + ax + b$$

where $a, b \in \mathbb{R}$ and the polynomial $x^3 + ax + b$ has 3 distinct complex zeros. At least one of them is real, because

$$\lim_{x \to +\infty} (x^3 + ax + b) = +\infty, \quad \lim_{x \to -\infty} (x^3 + ax + b) = -\infty.$$

So we have two cases.

Case 1. $x^3 + ax + b = 0$ has only one real zero r, then

$$x^3 + ax + b = (x - r)(x^2 + cx + d).$$

$x^2 + cx + d > 0$ for all $x \in \mathbb{R}$.

we have

$$x^3 + ax + b \begin{cases} < 0 & \text{if } x < r \\ \geq 0 & \text{if } x \geq r \end{cases}$$

The real solutions of $y^2 = x^3 + ax + b$ exists only for $x \geq r$.

If $x = r$, there is only one $y = 0$.

If $x > r$, there are two y's. Add the infinite point, we see the solution set is a circle. The group has to be S^1.

Case 2. $x^3 + ax + b = 0$ has three real zeros $r_1 < r_2 < r_3$, then

$$x^3 + ax + b = (x - r_1)(x - r_2)(x - r_3).$$

we have

$$x^3 + ax + b \begin{cases} < 0 & \text{if } x < r_1 \\ \geq 0 & \text{if } r_1 \leq x \leq r_2 \\ < 0 & \text{if } r_2 < x < r_3 \\ \geq 0 & \text{if } r_3 \leq x \end{cases}$$

$E(\mathbb{R})$ has two components: one for $r_1 \leq x \leq r_2$, the other for $r_3 \leq x$ together with ∞. Both components are S^1.

Because there are 4 2-torsion points $(r_1, 0), (r_2, 0), (r_3, 0)$ and ∞. So the group must be $S^1 \times \{\pm 1\}$.

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

For every point $P \in \mathbb{P}^N(\mathbb{Q})$, we can find $x_0, x_1, \ldots, x_N \in \mathbb{Z}$

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

such that

$$\gcd(x_0, x_1, \ldots, x_N) = 1.$$

We define the **height** of P to be

$$H(P) = \max(|x_0|, |x_1|, \ldots, |x_N|).$$

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

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

$$H(P) = 15.$$

For arbitrary C, the set

$$\{P \in \mathbb{P}^N(\mathbb{Q}) \mid H(P) \leq C\}$$

is a finite set.

We want to define heights for arbitrary number field.

Let F be a field.

Definition. An absolute value on F is a function

$$| \ | : F \to \mathbb{R}_{\geq 0}$$

satisfying the following conditions:

(1) $|a| = 0$ iff $a = 0$.

(2) $|ab| = |a| \, |b|$.

(3) $|a + b| \leq |a| + |b|$.

(4) $|F^*| \neq \{1\}$.

Two absolute values $| \ |_1$ and $| \ |_2$ on F is equivalent if there exists $r > 0$ such that

$$|a|_1^r = |a|_2$$

for all $a \in F$.

$F = \mathbb{Q}$.

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

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 $\mathbb{Q}$.

Ostrowski Theorem.

Every absolute value on $\mathbb{Q}$ is either equal to $|\ |_\infty$ or equivalent to $|\ |_p$ for some prime p.

Let C be a smooth projective over $\bar{K}$. For $P \in \bar{K}(C)$,

$$\mathrm{ord}_P : \ \bar{K}(C)^* \to \mathbb{Z}$$

satisfies the properties that

$$\mathrm{ord}_P(fg) = \mathrm{ord}_P(f) + \mathrm{ord}_P(g), \ \ \mathrm{ord}_P(f+g) \geq \min(\mathrm{ord}_P(f), \mathrm{ord}_P(g))$$

These properties implies that, for a fixed $q > 1$,

$$| \, |_P : \bar{K}(C)^* \to \mathbb{R}_{\geq 0}, \ \ |f|_P = q^{-\mathrm{ord}_P(f)}$$

is an absolute values. This absolute satisfied that $|\bar{K}^*| = 1$.

Different choices of q give equivalent absolute values.

The map $P \mapsto | \, |_P$ is an one-to-one correspondence from $C(\bar{K})$ to the set of equivalence classes of absolute values on $\bar{K}(C)$ with $|\bar{K}^*| = 1$.

Let $M_{\mathbb{Q}}$ denote the set of standard absolute values, by Ostrowski Theorem, $M_{\mathbb{Q}}$ is the set of equivalence classes of absolute values on $\mathbb{Q}$.

The set $M_{\mathbb{Q}}$ is an analog for $\mathbb{Q}$ of $C(\bar{K})$ for function field $\bar{K}(C)$.

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.

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

Every other absolute value on K is equivalent to a unique standard absolute value, so the set M_K can be identified with the set of equivalence classes of absolute values on K.

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

Archimedean absolute values: For every an embedding

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

The map

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

is an absolute value.

σ has a complex conjugate embedding

$$\bar{\sigma} : K \to \mathbb{C}, \ \ \bar{\sigma}(a) = \overline{\sigma(a)}.$$

It is clear that $| \ |_\sigma = | \ |_{\bar{\sigma}}$.

Note that $\sigma = \bar{\sigma}$ iff $\mathrm{Im}(\sigma) \subset \mathbb{R}$. In this case, we call σ a real embedding.

$\sigma \neq \bar{\sigma}$ iff $\mathrm{Im}(\sigma) \not\subset \mathbb{R}$. In this case, we call σ an complex embedding. Complex embedding appear in pairs: $\sigma, \bar{\sigma}$.

An absolute values on K obtained by an embeddings $K \to \mathbb{C}$ are called an **Archimedean absolute value**.

Theorem. Suppose K has $2m$ complex embeddings and r real embeddings, then

$$[K : \mathbb{Q}] = 2m + r.$$

and
K has $m + r$ Archimedean absolute values. They are all standard.

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

Example. $K = \mathbb{Q}(i)$, then $R = R_K = \mathbb{Z}[i]$.

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.

$$M_K = \text{Archemedean absolute values} \sqcup \{\text{Standard absolute values from non} - \text{zero prime ideals in } R\}$$

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).

Function field analog: let C and C' be smooth projective curves over $\bar{K}$, An embedding $\bar{K}(C') \to \bar{K}(C)$ induces a surjective morphism

$$C \to C'$$

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 $v \in M_K$, we use the same symbol v to denote its restriction on $\mathbb{Q}$, the **local degree** at v, denoted n_v, is given by

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

Example. $K = \mathbb{Q}(i)$, it has a unique Archimedean absolute value ∞, $\mathbb{Q}(i)_\infty = \mathbb{C}$,

$$n_\infty = [\mathbb{C} : \mathbb{R}] = 2$$

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

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

Example. $r = -\frac{7}{20}$, then

$$|r|_\infty = \frac{7}{20}, \;\; |r|_2 = 2^4, \;\; |r|_5 = 5, \;\; |r|_7 = 7^{-1}$$

and

$$|r|_p = 1 \;\; \text{for } p \neq 2, 5, 7.$$

Proof of Theorem. let

$$r = \pm p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$$

where $p_1, \dots, p_n$ are distinct primes, $k_i \in \mathbb{Z}$. Then

$$|r|_\infty = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$$

$$|r|_{p_1} = p_1^{-k_1},\ |r|_{p_2} = p_2^{-k_2}, \dots, |r|_{p_n} = p_n^{-k_n}$$

and

$|r|_p = 1$ for all other primes.

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

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

Function field analog: $f \in \bar{K}(C)^*$,

$$\sum_{P \in C} \mathrm{ord}_P(f) = 0$$

See Proposition II 3.1.

End