Math 6170 C, Lecture on April 20, 2020

Yongchang Zhu

Plan

(1). VIII. §1. The Weak Mordell-Weil Theorem (continued).

(2) VIII. §2. The Kummer Pairing via Cohomology.

(3) VIII. §3. The Decent Procedure.

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

Main Theorem in VIII (Mordell-Weil Theorem). Let E be an elliptic curve over a number field K, then $E(K)$ is finitely generated.

So

$$E(K) \simeq E_{\mathrm{tors}}(K) \times \mathbb{Z}^r$$

Theorem VIII 1.1. (Weak Mordell-Weil Theorem). Let E be elliptic curve over a number field K, and m is a positive integer. Then

$$E(K)/mE(k)$$

is a finite group.

Lemma 1.1.1. Let L/K be a finite Galois extension. If $E(L)/mE(L)$ is finite, then $E(K)/mE(K)$ is also finite.

In the view of Lemma 1.1.1, it is enough to prove the Weak Mordell-Weil theorem under the assumption that

$$E[m] \subset E(K).$$

Definition. The Kummer pairing

$$\kappa : E(K) \times G_{\bar{K}/K} \to E[m]$$

is defined as follows. Let $P \in E(K)$, and choose $Q \in E(\bar{K})$ satisfying

$$[m]Q = P.$$

Then

$$\kappa(P, \sigma) = Q^{\sigma} - Q.$$

Proposition VIII 1.2.

(a) The Kummer pairing is well defined.

(b) The Kummer pairing is bilinear.

(c) The kernel of the Kummer paring on the left is $m\,E(K)$.

(d) The kernel of the Kummer paring on the right is $G_{\bar{K}/L}$, where

$$L = K([m]^{-1}E(K))$$

Hence the Kummer paring induces a perfect bilinear pairing

$$E(K)/m\,E(K) \times G_{L/K} \to E[m].$$

Proof of (a). Existence of Q with $[m]Q = P$. We embed $K \subset \mathbb{C}$. Existence of $Q \in E(\mathbb{C})$ with $[m]Q = P$ is obvious since $E(\mathbb{C}) = S^1 \times S^1$ as an abelian group.

$$|[m]^{-1}P| = m^2$$

$\mathrm{Aut}(\mathbb{C}/K)$ acts on $[m]^{-1}P$.

Then $[m]^{-1}P \subset E(\bar{K})$ by the following lemma:

Proof of (a) (continued). Lemma. If $S \subset \mathbb{C}$ is a **finite** set, and it is stable under the action of $\mathrm{Aut}(\mathbb{C}/K)$, then

$$S \subset \bar{K} = \bar{\mathbb{Q}}.$$

Let T be a maximal subset in $\mathbb{C}$ that is algebraically independent over $\bar{K}$. Then $\overline{\bar{K}(T)}$. Any permutation of T can be extended to an automorphism of $\mathbb{C}$.

Proof of (a) (continued). We now prove $Q^\sigma - Q$ is independent of the choice of Q:

Suppose $Q' \in E(\bar{K})$ also satisfies $[m]Q' = P$, then $[m](Q' - Q) = 0$, so $T \stackrel{\text{def}}{=} Q' - Q \in E[m] \subset E(K)$,

$$Q'^\sigma - Q' = (Q + T)^\sigma - (Q + T) = Q^\sigma + T^\sigma - Q - T = Q^\sigma - Q.$$

Proof of (b). Let $P_1, P_2 \in E(K)$, choose $Q_1, Q_2 \in E(\bar{K})$ with $[m]\, Q_1 = P_1, [m]\, Q_2 = P_2$, then $[m](Q_1 + Q_2) = P_1 + P_2$,

$$
\begin{aligned}
& \kappa(P_1 + P_2, \sigma) \\
&= (Q_1 + Q_2)^\sigma - (Q_1 + Q_2) \\
&= Q_1^\sigma - Q_1 + Q_2^\sigma - Q_2 \\
&= \kappa(P_1, \sigma) + \kappa(P_2, \sigma)
\end{aligned}
$$

Proof of (b) (continued). For $\sigma, \tau \in G_{\bar{K}/K}$, $P \in E(K), [m]Q = P$,

$$
\begin{aligned}
&\kappa(P, \sigma\tau) \\
&= Q^{\sigma\tau} - Q \\
&= (Q^{\sigma} - Q)^{\tau} + Q^{\tau} - Q \\
&= Q^{\sigma} - Q + Q^{\tau} - Q \\
&= \kappa(P, \sigma) + \kappa(P, \tau)
\end{aligned}
$$

Proof of (c). Suppose $P \in mE(K)$, so $P = [m]Q$ for some $Q \in E(K)$

$$\kappa(P, \sigma) = Q^\sigma - Q = Q - Q = 0$$

Suppose $\kappa(P, \sigma) = 0$ for all $\sigma \in G_{\bar{K}/K}$,
For $Q \in E(\bar{K})$ with $[m]Q = P$,

$$0 = \kappa(P, \sigma) = Q^\sigma - Q$$

for all $\sigma \in G_{\bar{K}/K}$, Q is fixed by all elements in $G_{\bar{K}/K}$, $Q \in E(K)$
so $P = [m]Q \in mE(K)$.

Proof of (d).

Suppose $\sigma \in G_{\bar{K}/L}$, For every $P \in E(K)$, $Q \in E(\bar{K})$ with $[m]Q = P$, Then $Q \in E(L)$, so

$$\kappa(P, \sigma) = Q^\sigma - Q = Q - Q = 0.$$

Conversely, if $\kappa(P, \sigma) = 0$ for all $P \in E(K)$, For any $Q \in E(\bar{K})$ with $[m]Q = P$, $Q^\sigma = Q$. So $\sigma \in G_{\bar{K}/L}$.

□

Kummer Pairing in field theory.

Let F be a field with $\mathrm{char}\, F = 0$, $\bar{F}$ be the algebraic closure of F. Let m be a positive integer and let

$$\mu_m = \{u \in \bar{F}^* \mid u^m = 1\}.$$

Then $|\mu_m| = m$. Suppose

$$\mu_m \subset F.$$

The Kummer pairing is a pairing

$$\kappa : F^* \times G_{\bar{F}/F} \to \mu_m$$

defined as, for $a \in F^*, \sigma \in G_{\bar{F}/F}$, we choose $b \in \bar{F}^*$ with $b^m = a$.

$$\kappa(a, \sigma) = \frac{b^\sigma}{b}.$$

Analog of Proposition VIII 1.2.

(a) The Kummer pairing is well defined.

(b) The Kummer pairing is bilinear.

(c) The kernel of the Kummer paring on the left is ${F^*}^m = \{c^m \mid c \in F^*\}$.

(d) The kernel of the Kummer paring on the right is $G_{\bar{F}/L}$, where L is the subfield of $\bar{K}$ generated by F and the solutions of $x^m = a$ for $a \in F$.

The proof is parallel to that for elliptic curve case.

Proposition VIII 1.5. Let

$$L = K([m]^{-1}E(K))$$

be the field in Proposition VIII 1.2., then
(a) $G_{L/K}$ is abelian and every element has order dividing m.
(b) L/K is unramified at almost all prime ideals of R_K. (where R_K is the ring of algebraic integers in K).

Proof of (a).

By Kummer pairing

$$\kappa : E(K)/mE(K) \times G_{L/K} \to E[m]$$

Every $\sigma \in G_{L/K}$ given a linear map

$$T_\sigma : E(K)/mE(K) \to E[m], \quad T_\sigma(P) = \kappa(P, \sigma)$$

$$T_\sigma \in \mathrm{Hom}_{\mathbb{Z}}(E(K)/mE(K), E[m])$$

SO we have an injective group homomorphism

$$G_{L/K} \to \mathrm{Hom}_{\mathbb{Z}}(E(K)/mE(K), E[m]),$$

This $G_{L/K}$ is abelian and $\sigma^m = 1$ for all $\sigma \in G_{L/K}$.

We will skip (b) and just explain the meaning of the terminology used.

For a number field K, let R_K be the ring of algebraic integers in K. Then R_K is a Dedekind domain.

In any Dedekind domain, every non-zero ideal I can be factorized as a product of prime ideals in a unique way:

$$I = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_n^{m_n}$$

Let $K \subset E$ be a finite algebraic extension, R_E be the ring of algebraic integers in E, a prime ideal $\mathfrak{p} \subset R_K$ is **unramified** in E if in the factorization then the ideal $\mathfrak{p}R_E$ of R_E can be factorized

$$\mathfrak{p}R_E = \mathfrak{q}_1^{m_1} \cdots \mathfrak{q}_n^{m_n}$$

$\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ are distinct prime ideals of R_E, all $m_i = 1$.

Let $K \subset L$ be an infinite algebraic extension, a prime ideal $\mathfrak{p} \subset R_K$ is **unramified** in L if it is unramified in E for every finite sub-extension $K \subset E \subset L$.

If C and D are smooth projective curves over some field K with $\bar{K} = K$. Let $\phi : C \to D$ be a non-constant map, we have corresponding field extension

$$\phi^* : K(D) \to K(C).$$

Recall a point $P \in C(K)$ is call unramified if $\phi^*(t)$ is a uniformizer at P when t is a uniformizer at $\phi(P)$.

In this case, two notions of "being unrmified" agree.

Proposition. Let K be a number field, m be a positive integer. Suppose $K \subset L$ is an abelian extension such that $\sigma^m = 1$ for all $\sigma \in G_{L/K}$ and almost all primes ideals in R_K are unramified in L, then L is a finite extension.

Proof of Weak Mordell-Weil Theorem.

We have perfect pairing,

$$\kappa : E(K)/mE(K) \times G_{L/K} \to E[m]$$

Since L is a finite extension of K, $G_{L/K}$ is a finite group, so $E(K)/mE(K)$ is a finite group.

VIII. §2. The Kummer Pairing via Cohomology.

If a group G acts on an abelian group A as automorphism (A is called a G-module), the fixed point

$$A^G = \{a \in A \,|\, \sigma \cdot a = a \text{ for all } \sigma \in G\}$$

is a subgroup of A.
However $A \mapsto A^G$ doesn't preserve exact sequences:

If $0 \to A \to B \to C \to 0$ is an exact sequence of G-modules.
Then $0 \to A^G \to B^G \to C^G$ is exact, but
$0 \to A^G \to B^G \to C^G \to 0$ is not exact in general.

The theory of group cohomology allows to define groups

$$H^i(G, M), i = 0, 1, 2, \ldots$$

for a G-module M with $H^0(G, M) = M^G$, A short exact sequence

$$0 \to A \to B \to C \to 0$$

induces a long exact sequence

$$\begin{aligned} &0 \to A^G \to B^G \to C^G \to \\ &\to H^1(G, A) \to H^1(G, B) \to H^1(G, C) \to H^2(G, A) \to \dots \end{aligned}$$

For an elliptic curve E over K, we have exact sequence of $G_{\bar{K}/K}$-modules:

$$0 \to E[m] \to E(\bar{K}) \stackrel{[m]}{\to} E(\bar{K}) \to 0$$

It induces a long exact sequence

$$\begin{aligned} &0 \to E(K)[m] \to E(K) \stackrel{[m]}{\to} E(K) \to \\ &\to H^1(G_{\bar{K}/K}, E[m]) \to .... \end{aligned}$$

It induces

$$0 \to E(K)/m\,E(K) \to H^1(G_{\bar{K}/K}, E[m])$$

In the case that $E[m] \subset E(K)$, $E[m]$ is a trivial $G_{\bar{K}/K}$-module,

$$H^1(G_{\bar{K}/K}, E[m]) = \mathrm{Hom}(G_{\bar{K}/K}, E[m]).$$

This is the same as the map given by the Kummer pairing.

Proposition VIII 3.1 (Descent theorem) Let A be an abelian group. Suppose there is a "height" function

$$h : A \to \mathbb{R}$$

with the following properties:

(1) Let $Q \in A$. There is a constant C_1, depending on Q, so that for all $P \in A$,

$$h(P+Q) \leq 2h(P) + C_1$$

(2) There is an integer $m \geq 2$ and a constant C_2, so that for all $P \in A$,

$$h(mP) \geq m^2 h(P) - C_2$$

(To be continued)

(3) For every constant C_3,

$$\{P \in A \,|\, h(P) \leq C_3\}$$

is a finite set.

Suppose further that $|A/mA| < \infty$. Then A is finitely generated.

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 are 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, every $a \in \mathbb{Q} - \{0\}$ can be written as

$$a = p^m \frac{b}{c}$$

where $m \in \mathbb{Z}, b, c \in \mathbb{Z}, \gcd(b, p) = \gcd(c, p) = 1$.

$$|a|_p = p^{-m}, \quad |0|_p = 0$$

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

is an absolute value (call the p-adic absolute value).

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

Ostrowski Theorem.

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

End