Where we were

Computing $E(K)$.

Known to be f.g., but what is it?

know $E(K)/mE(K)$ is finite $\forall m \geq 2$,

→ This depends on some parameters C_i for ht fn descent,

which is computable given $E(K)/mE(K)$

VIII, 3.2

For Colin's talk, reduced a computation of $E/2$ to

finding $\mathbb{Q}$ points on some space.

This is where we're headed w/ homog spaces

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

want this ↑

∴ want to know image ⟺ want to know kernel

So want to know what triviality in this H^1 is, cohomology? Sure, but we give it geometric meaning.

Homog spaces

convention: curve = smooth + projective

K perfect

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

LES Galois cohomology

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

⇝ coh [m], ker [m].

$$0 \to \frac{E}{m} \to H^1(E[m]) \to H^1(E)[m] \to 0$$

↓ <u>image</u> consists of cocycles which are unramified outside a finite set – $\infty \cup$ bad red $\cup$ divides m

weak M-W used that max'l ab. exp m unram outside S is finite (CFT/Kummer)

Def. a cocycle is unramified

if $H^1(G(\bar{k}/k), M) \longrightarrow H^1(I_v, M)$

$\xi \longmapsto 0$

In our SES, we will analyze $H^1(G(\bar{k}/k), E)[m]$ by

geometry.

Def. A homog space C/K is a curve s.t.

$E \circlearrowright C$ trans + free

$C \times E \longrightarrow C \quad /K$

$(\gamma, P) \longmapsto \gamma + P$

for any $\gamma, \sigma \ \exists! \ P$ s.t. $\gamma + P = \sigma$

denote $P = \sigma - \gamma$

$C \times C \longrightarrow C$

Philosophize

gp - origin

affine in classical mechanics

potential energy

$+C$

"Lemma" $+$, $-$ are good names

Prop. $\gamma_0 \in C$, $E \xrightarrow{\theta} C$ an iso $/K(\gamma_0)$ — important! we lack a cf privilege

$p \longmapsto \gamma_0 + p$

$$\gamma + p = \theta(\theta^{-1}(\gamma) + p)$$

$$\gamma - \delta = \theta^{-1}(\gamma) - \theta^{-1}(\delta)$$

$\therefore C \times C \longrightarrow C$ def $/K$ by computing Galois action

Def. An equivalence is $\theta: C \longrightarrow C' /K$ iso s.t.

$$\theta(\gamma + p) = \theta(\gamma) + p$$

Def. $WC(E/K) = \{$homog spaces C/K of $E(K)\} /$ equivalence. $\leftarrow E$ is called trivial

This is a group geometrically, but we do this w/ cohom.

Aside: geometric WC addition

Let $C_1, C_2 \in WC(E/K)$

$E \circlearrowright C_1 \times C_2$ via

$$(\gamma_1, \gamma_2) + P = (\gamma_1 + P, \gamma_2 - P)$$

$\frac{C_1 \times C_2}{E}$ has a diagonal action $\overline{(\gamma_1, \gamma_2)} + P = \overline{(\gamma_1 + P, \gamma_2 + P)}$

This is the sum (?)

inverse is opposite action:

$$\gamma +' P = \gamma - P$$

$E \circlearrowright C \times C$ on diagonal

so quotient is ... C ?

Prop. C/K trivial $\iff C(K) \neq \emptyset$

Pf. A point latches an iso $E \to K$ and E has a K-point

Thm. $WC(E/K) \longrightarrow H^1(G(\bar{K}/K), E)$ iso

$$C/K \quad p_0 \in C \longmapsto \{\sigma \mapsto p_0^\sigma - p_0\}$$

$\uparrow$ denote cohom. class

$\rightsquigarrow$ difference. p_0^σ, p_0

$\ldots$ trivial $\longmapsto$ trivial

Pf. - $\sigma \longmapsto p_0^\sigma - p_0$ a cocycle

checked ✓

- $\theta : C \longrightarrow C'/K$ iso wrt E action

$p_0^\sigma - p_0 \quad p_0'^\sigma - p_0'$ differ by a coboundary

given by $(\theta(p_0) - p_0')^\sigma - (\theta(p_0) - p_0')$

- injectivity. Let $p_0^\sigma - p_0$, $p_0'^\sigma - p_0'$ cohomologous

so $\exists\, P_0 \in E$ s.t.

$$p_0^\sigma - p_0 = p_0'^\sigma - p_0' + (P_0^\sigma - P_0)$$

$C \xrightarrow{\theta} C' \quad p \longmapsto p_0' - (p - p_0) + P_0$, $\therefore$ $G(\bar{K}/K)$ invariant by above

- Surjectivity.

How to find a curve?

~~polynomials~~ fields!

take $\xi \in H^1(G(\bar{K}/K), E)$

i.e. $\xi : G(\bar{K}/K) \longrightarrow E$, 1 cocycle

$\xi_{\sigma\tau} = \xi_\sigma^\tau + \xi_\tau$

wtf C, $\varphi : C \xrightarrow{\sim} E$ / $\bar{K}$

s.t. $\varphi^\sigma \circ \varphi^{-1}$ = translation by $-\xi_\sigma$

idea: Take $\bar{K}(E)$ as a set and twist the Galois action via $-\xi_\sigma$

$Z : \bar{K}(E) \longrightarrow \bar{K}(E)_\xi$, id on field level

s.t. $Z(f)^\sigma = Z(f^\sigma \circ (-\xi_\sigma))$

↓ viewed as translation auto of E

Then let F be the fixed field of Galois of $\bar{K}(C)_\xi$.

F is the function field of our C. $\bar{K}(C) = F$.

- $F \cap \bar{K} = K$
- $\bar{K}F = \bar{K}(C)_\xi$

$\varphi : C \to E$ is s.t. $\varphi^* : \bar{K}(E) \to \bar{K}(C)$

$\bar{K}(C) = \bar{K}f = \bar{K}(E)_\xi$

is just Z from before

Then $Z(f) = f\varphi$

$\therefore (f\varphi)^\sigma = f^\sigma \circ (+\xi_\sigma)^\varphi \quad \forall f$

$\therefore \varphi^\sigma = (-\xi_\sigma)\varphi$

$\varphi^\sigma \varphi^{-1} = -\xi_\sigma$

$C \times E \to C$

$\gamma + P = \varphi^{-1}(\varphi(\gamma) + P)$

This is homog w/ cohomology class $\{\xi\}$

free + transitive? $\gamma + P = \delta$ forces $P = \varphi(\delta) - \varphi(\gamma)$

i.e. $\delta - \gamma = \varphi(\delta) - \varphi(\gamma)$

$/K$? Galois action +

$(\gamma + P)^\sigma = \varphi^{-1\sigma}(\varphi^\sigma(\gamma^\sigma) + P^\sigma)$

$= \varphi^{-1\sigma}(\varphi(\gamma^\sigma) - \xi_\sigma + P^\sigma) \qquad \varphi^\sigma = (-\xi_\sigma) \circ \varphi$

$= \varphi^{-1}(\varphi(\gamma^\sigma) - \xi_\sigma + P^\sigma + \xi_\sigma) \qquad \varphi \circ \varphi^{-1,\sigma} = +\xi_\sigma$

$\therefore \varphi^{-1,\sigma} = \varphi^{-1} \circ +\xi_\sigma$

def $= \gamma^\sigma + P^\sigma$

cohom class of C/F?

pick $\gamma_0 = \varphi^{-1}(0)$

$\gamma_0^{\sigma} - \gamma_0 = \varphi^{\sigma_i -1}(0) - \varphi^{-1}(0)$

$= \varphi^{-1}(0 + \xi_\sigma) - \varphi^{-1}(0)$

where $-\xi_\sigma$ in def

$= \varphi^{-1}(\xi_\sigma) - \varphi^{-1}(0)$ difference in C

by def of $\overline{\underline{I}}$

$= \varphi(\varphi^{-1}(\xi_\sigma)) - \varphi(\varphi^{-1}(0))$

$= \xi_\sigma - 0$

$= \xi_\sigma$

---

fun fact: $Pic^0(C) \longrightarrow E$ iso of Galois modules

$\sum n_i \gamma_0 \longmapsto \sum [n_i](\gamma_i - \gamma_0)$ for C a homog space

Jacobian

$\gamma_0 \in C$

indep of choice of C

Selmer + Shafarevich–Tate groups

X.4

(LES Galois cohomology to $0 \to E[\varphi] \to E \xrightarrow{\varphi} E' \to 0$)

For v a valuation on K, choose an extension to $\bar{K}$,

i.e. an embedding $\bar{K} \hookrightarrow \bar{K_v}$

yields $G_v \subseteq G(\bar{K}/K)$ as those σ fixing v, i.e. continuously extending to $\bar{K}_v$.

$\therefore$ get maps on cohomology $\forall v$. assemble to product

$$\begin{array}{ccccccccc}
0 & \to & E/\varphi & \xrightarrow{(1)} & H^1(E[\varphi]) & \xrightarrow{(2)} & \cancel{H^1(E)[\varphi]}\ \ WC & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \prod & \to & \prod & \to & \cancel{\prod}\ \ WC & \to & 0
\end{array}$$

Oh, recall the goal: compute E/φ

$\Leftarrow$ compute image (1)

$\Leftarrow$ compute ker (2)

$\therefore$ must detect triviality in WC, i.e. check if a space has a K-rat'l point

- Hard, but converse is easier

To show $\nexists$ K-rational pt, suffices to show $\exists$ K_v-rat'l point for some v

i.e. nontrivial in $WC(E/K_v)$

$\Downarrow$

nontrivial in $WC(E/K)$

For K_v this is feasible by Hensel's lemma, which reduces us to k_v, finite

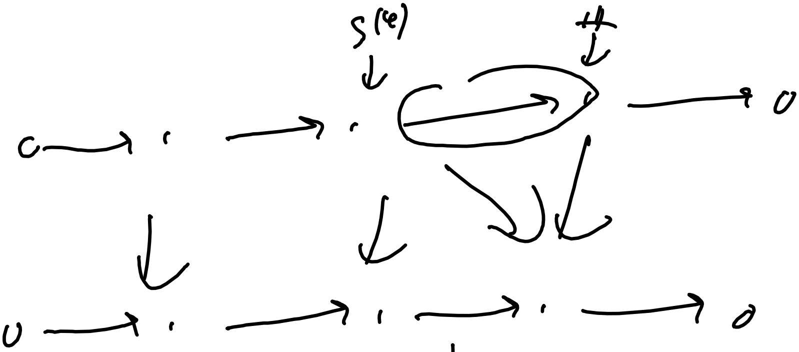
Def. φ-Selmer group

$$S^{(\varphi)}(E/K) = \ker\left(H^1(G(\bar{K}/K), E[\varphi]) \longrightarrow \prod WC(E/K_v)\right)$$

$$= \bigcap_v \ker\left(H^1(E[\varphi]) \longrightarrow WC(E/K_v)\right)$$

$$\text{Ш}(E/K) = \ker\left(WC(E/K) \longrightarrow \prod_v WC(E/K_v)\right)$$

$$= \bigcap_v \ker\left(WC(E/K) \longrightarrow WC(E/K_v)\right)$$



→ replace w/ something actually computable!

$S^{(\varphi)}$ is close to the kernel we're looking for, except an issue of Hasse principle

Ш measures failure of Hasse principle

Thm. $0 \to \frac{E'}{\varphi E}(k) \to S^{(\varphi)}(E/k) \to Ш(E/k)[\varphi] \to 0$

exact and $S^{(\varphi)}(E/k)$ finite

Pf. Trivial diagram chase for exactness, for finiteness, this ⇒ weak Mordell-Weil!

Here's the plan.

- show that $S^{(\varphi)}(E/k) \subseteq H^1(E[\varphi])$ consists of unramified cocycles, i.e. those which are trivial under $H^1(G(\bar{k}/k)) \longrightarrow H^1(I_v)$ for all places v outside some finite set S.

- L = max'l abelian unramified exp $m = \deg \varphi$ extension
  finite by Kummer / CFT → done in WMW pf

- use finiteness of L and $E[\varphi]$ to show that the S-unramified cocycles $H^1(G(\bar{k}/k), E[\varphi]; S)$ is finite

Can compute $H^1(G(\bar{K}/K), E[\varphi]; S)$ as it is finite

what is image of $S^{(\varphi)}$ in here?

Compute map to $WC(E/K_v)$ G_v

$\forall$?!

w, als $v \in S$

$v \notin S$ automatically trivial

$$\begin{array}{ccccccccc} 0 \to & E[\varphi]^{I_v} & \to & E^{I_v} & \to & E'^{I_v} & \to 0 \\ & \downarrow & & \downarrow & & \downarrow & \\ 0 \to & \tilde{E}_v[\varphi] & \to & \tilde{E}_v & \to & \tilde{E}'_v & \to 0 \end{array}$$

$\rightsquigarrow$ a LES cohom

middle map is iso as E_v, E_v' both have good reduction by Neron-Ogg-Shafarevich

$S \supseteq \infty \cup \text{bad}(E) \cup$ divisors of $\deg(\varphi)$ works

$$
\begin{array}{ccccccc}
E(K) & \longrightarrow & S^{(m)}(E/K) & \longrightarrow & Ш(E/K)[m] & \longrightarrow & 0 \\
\| & & \uparrow & & \uparrow \cdot m^{n-1} & & \\
E(K) & \longrightarrow & S^{(m^n)}(E/K) & \longrightarrow & Ш(E/K)[m^n] & & \\
 & & \downarrow & & & & \\
 & & \text{image} =: S^{(m,n)}(E/K) & & & &
\end{array}
$$

↓ compatible? ehh . . .

(def)

Then $0 \to \frac{E}{m}(K) \to S^{(m,n)}(E/K) \to m^{n-1} Ш(E/K)[m^n] \to 0$