

Lecture # 2

- Frobenii (quick review)

L/K Galois extension of number fields

$\mathfrak{p} \subset \mathcal{O}_K$ prime ideal with residue field $\kappa_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$

$\mathfrak{P} \subset \mathcal{O}_L$ prime above $\mathfrak{p}$, residue field $\kappa_{\mathfrak{P}} = \mathcal{O}_L/\mathfrak{P}$

Suppose $\mathfrak{p}$ unramified in L .

Then the natural map

$$\begin{aligned} \text{Gal}(L/K) \supset \text{Gal}(L_{\mathfrak{P}}/\kappa_{\mathfrak{p}}) &\longrightarrow \text{Gal}(\kappa_{\mathfrak{P}}/\kappa_{\mathfrak{p}}) \\ &\parallel \\ &\langle \text{Frob}_{\mathfrak{p}} : \alpha \mapsto \alpha^q \rangle \end{aligned}$$

is an isomorphism.

$$q = \# \kappa_{\mathfrak{p}}.$$

Definition. The Frobenius element $\left(\frac{L/K}{\mathfrak{p}} \right) \in \text{Gal}(L/K)$

is the unique element in $\text{Gal}(L_{\mathfrak{P}}/\kappa_{\mathfrak{p}})$

reducing to $\text{Frob}_{\mathfrak{p}}$:

Note. • $\wp$ determines a Frobenius conjugacy class

$$\left(\frac{L/K}{\wp}\right) := \left\{ \left(\frac{L/K}{\wp}\right) : \wp \mid \wp \right\} \subset \text{Gal}(L/K).$$

• $\wp$ splits completely in L iff $\left(\frac{L/K}{\wp}\right) = \text{id}$.

Back to Heegner points:

Given an elliptic curve $E/\mathbb{Q}$ of conductor N

and an imaginary quadr. field $K = \mathbb{Q}(\sqrt{D})$

satisfying the Heegner hypothesis ($D \neq -3, -4$).

we have Heegner points

$$y_n \in E(H_n)$$

$$\text{" } \Phi(z_n)$$

for every $n \geq 1$ prime to N ,

Last time:

Proposition 1 (Norm Relations)

Suppose $n = l \cdot m$, with $l + m$ inert in K .

Then

$$\text{Norm}_{H_n/H_m}(y_n) = a_l \cdot y_m.$$

Now we prove:

Proposition 2 (Congruence Relation)

Suppose $n = l \cdot m$, with $l + m$ inert in K ,

and write $l\mathcal{O}_K = \lambda$,

Then:

(i) λ splits completely in H_m .

(ii) Every prime $\lambda_m \mid \lambda$ in H_m
it totally ramified in H_m .

(iii)

$$y_n \equiv \left(\frac{H_m/\mathbb{Q}}{\lambda_m} \right) y_m \pmod{\lambda_n}$$

where λ_n is the unique prime of H_m above λ_m .

Equivalently,

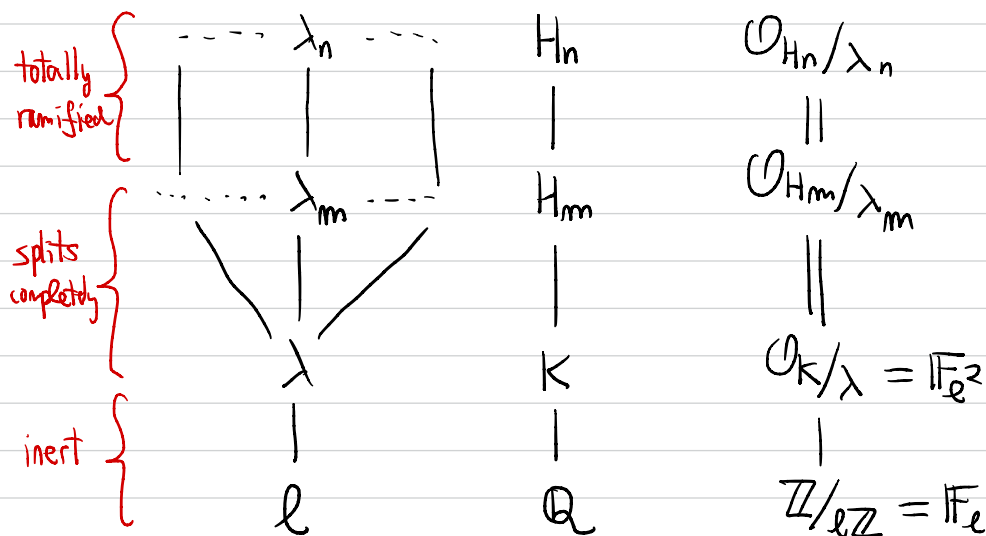
$$\text{red}_{\lambda_n}(y_n) = \text{Frob}_e \text{red}_{\lambda_m}(y_m) \in \tilde{E}(\mathbb{F}_{\ell^2})$$

where

$$\begin{array}{ccc} \text{red}_{\lambda_n}: E(H_n) & \longrightarrow & \tilde{E}(\mathcal{O}_{H_n}/\lambda_n) \\ & & \parallel \\ \text{red}_{\lambda_m}: E(H_m) & \longrightarrow & \tilde{E}(\mathcal{O}_{H_m}/\lambda_m) \\ & & \parallel \\ & & \tilde{E}(\mathbb{F}_{\ell^2}) \end{array}$$

are the reduction maps.

Picture:



Proof. (i) & (ii) follows from Class Field Theory.

For (iii), we'll compute $a_e \cdot \text{red}_{\lambda_m}(y_m)$ in two different ways:

① From Proposition 1,

$$a_e \cdot y_m = \sum_{\sigma \in \text{Gal}(H_n/H_m)} \sigma y_n$$

$$\begin{aligned}
 \Rightarrow a_e \cdot \text{red}_{\lambda_m}(y_m) &= \sum_{\sigma \in \text{Gal}(H_n/H_m)} \underbrace{\text{red}_{\lambda_n}(\sigma y_n)}_{\parallel} \\
 &\quad \underbrace{\sigma \text{red}_{\lambda_n}(y_n)}_{\parallel} \\
 &\quad \text{red}_{\lambda_n}(y_n) \\
 &= (l+1) \text{red}_{\lambda_n}(y_n).
 \end{aligned}$$

② Since $l+N$, by the Eichler-Shimura congruence relation

$$T_e = \text{Frob}_e + \text{Frob}_e^{\text{tr}} \quad \text{as correspondences on } X_0(N)/\mathbb{F}_e$$

$$\text{where } \text{Frob}_e^{\text{tr}}: y \mapsto \sum_{x \in \text{Frob}_e^{-1}(y)} x$$

$$\Rightarrow T_\ell \cdot z_m = \text{Frob}_\ell z_m + \text{Frob}_\ell^{\text{tr}} z_m$$

as divisors on $X_0(N)(\mathbb{F}_\ell^2)$

$$\Rightarrow a_\ell \cdot \underbrace{\text{red}_{\lambda_m}(y_m)}_{\substack{\text{applies } \Phi \\ // \\ (l+1) \text{ red}_{\lambda_n}(y_n) \\ \text{by } \textcircled{1}}} = \text{Frob}_\ell \text{red}_{\lambda_m}(y_m)$$

$$+ \text{Frob}_\ell^{\text{tr}} \text{red}_{\lambda_m}(y_m)$$

as divisors on $\tilde{E}(\mathbb{F}_\ell^2)$

$$\Rightarrow \text{red}_{\lambda_n}(y_n) = \text{Frob}_\ell \text{red}_{\lambda_m}(y_m) \quad \square$$

$$\alpha^l = \alpha^{1/l} \quad \forall \alpha \in \mathbb{F}_\ell^2$$

Note. Propositions 1 & 2 show that for any prime p ,
the Kummer images

$$\left\{ \delta(\gamma_n) \in H^1(H_m, T_p E) \right\}_{(m, N) = 1}$$

$\uparrow$
 $\square$ -free product
of primes inert in K

from an (anti-cyclotomic) Euler system
for $T_p E$.

• Kolyvagin's theorem "mod p "

Recall: $y_K := \text{Norm}_{H_1/K}(y_1) \in E(K)$.

Definition. We say that a prime p is "good" if

(a) $p > 2$

(b) $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \text{GL}_2(\mathbb{F}_p)$.

(c) $y_K \notin pE(K)$.

Theorem A (Kolyvagin)

Suppose $y_K \notin E(K)_{\text{tors}}$,

and let p be a good prime.

Then

(1) $\text{rank}_{\mathbb{Z}} E(K) = 1$.

(2) $\mathbb{W}(E/K)[p^{\infty}] = \{0\}$.

Remark. By Serre's open image theorem,

if E doesn't have CM

then $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \text{GL}_2(\mathbb{F}_p)$

for all but finitely
many p .

$\therefore$ Theorem A + variant "mod p " for the "bad" p

$\Rightarrow$ Kolyvagin's thm. from Lecture 1 for
non-CM $E/\mathbb{Q}$.

(For E with CM, need to work
over $\text{End}(E) \otimes \mathbb{Z}_p$ rather than $\mathbb{Z}_p$.)

Goal of next lectures: Proof of Theorem A.

Consider the p -descent exact sequence

$$0 \rightarrow \frac{E(K)}{pE(K)} \xrightarrow{\delta} \text{Sel}_p(E/K) \rightarrow \bigcup (E/K)[p] \rightarrow 0.$$

In fact, we'll prove:

Theorem A' (Kolyvagin).

Suppose $y_K \notin E(K)_{\text{tors}}$,
and let p be a good prime.

Then

$$\text{Sel}_p(E/K) = \mathbb{F}_p \delta(y_K).$$

Exercise. Thm. A $\Leftrightarrow$ Thm. A' (Use $E(K)[p] = \{0\}$.)

Note. Since $y_K \notin pE(K) \Rightarrow \dim_{\mathbb{F}_p} \text{Sel}_p(E/K) \geq 1$
(if p is good)

to prove Theorem A'

we need to bound the size of $\text{Sel}_p(E/K)$
from above!

• Bounding Selmer groups

We start more generally:

K = number field

p = prime

M = finite dimⁿ $\mathbb{F}_p$ -vector space

with continuous linear G_K -action

unramified outside finite set $\Sigma \supset \{v \mid p \infty\}$.

Definition. A Selmer structure $\mathcal{F}$ on M

is a collection of subspaces

$$\mathcal{F} = \{ \mathcal{F}_v \subset H^1(K_v, M) \}_{v \text{ prime of } K}$$

$$\text{s.t. } \mathcal{F}_v = \ker \left(H^1(K_v, M) \rightarrow H^1(\mathcal{I}_v, M) \right)$$


unramified
or "finite" subspace.

for all but
finitely many v .

The associated Selmer group is

$$H^1_{\mathcal{F}}(K, M) := \ker \left(H^1(K, M) \rightarrow \bigoplus_v \frac{H^1(K_v, M)}{\mathcal{F}_v} \right)$$

Definition. Let $\mathcal{F}$ be a Selmer structure on M ,
and $S =$ finite set of primes of K
with $S \cap \Sigma = \emptyset$.

• The S -relaxed Selmer group

$$H^1_{\mathcal{F} \circledast S}(K, M) := \ker \left(H^1(K, M) \rightarrow \bigoplus_{v \notin S} \frac{H^1(K_v, M)}{\mathcal{F}_v} \right)$$

• The S -restricted Selmer group

$$H^1_{\mathcal{F} \circledast S}(K, M) := \left\{ c \in H^1_{\mathcal{F}}(K, M) \right. \\ \left. \text{s.t. } \underbrace{c_v}_{\substack{\uparrow \\ \text{image of } c \text{ in } H^1(K_v, M)}} = 0 \quad \forall v \in S \right\}$$

Thus we have tautological exact sequences

$$0 \rightarrow H_{\mathcal{F}}^1(K, M) \rightarrow H_{\mathcal{F}^S}^1(K, M) \xrightarrow[\bigoplus_{v \in S} \partial_v]{\partial_S} \bigoplus_{v \in S} \frac{H^1(K_v, M)}{\mathcal{F}_v}$$

!!
 $H_{\text{sing}}^1(K_v, M)$

$$0 \rightarrow H_{\mathcal{F}^S}^1(K, M) \rightarrow H_{\mathcal{F}}^1(K, M) \longrightarrow \bigoplus_{v \in S} \mathcal{F}_v$$

Apply to our case of interest :

$E/\mathbb{Q}$ elliptic curve of conductor N .

$$\Rightarrow \text{Sel}_p(E/K) = H_{\mathcal{F}}^1(K, E[p])$$

where $\mathcal{F} = \{\text{im } \delta_v\}_v$

$$\delta_v : E(K_v) / {}_p E(K_v) \hookrightarrow H^1(K_v, E[p])$$

local Kummer map.

(and can take $\Sigma = \{v \mid p \nmid N\}$).

Moreover, $\text{im } \delta_v$ is maximal isotropic
under local Tate duality

$$\langle, \rangle_v: H^1(K_v, E[p]) \times H^1(K_v, E[p]) \rightarrow H^2(K_v, \mathbb{F}_p) \cong \mathbb{F}_p.$$

and for any S with $S \cap \Sigma = \emptyset$ have the
exact sequence (by global duality)

$$0 \rightarrow \text{Sel}_p(E/K) \rightarrow H_{\mathbb{F}}^1(K, E[p]) \xrightarrow{\partial_S} \bigoplus_{v \in S} H_{\text{sing}}^1(K_v, E[p])$$

$$\parallel$$

$$\left(\bigoplus_{v \in S} \text{im } \delta_v \right)^\vee$$

$$0 \leftarrow H_{\mathbb{F}_S}^1(K, E[p])^\vee \leftarrow \text{Sel}_p(E/K)^\vee$$

Upshot. Suppose we can find S

$$\text{s.t. } H_{\mathcal{F}_S}^1(K, E[p]) = \{0\}.$$

Then

$$\# \text{Sel}_p(E/K)$$

||

$$\# \text{coker} \left(\underset{\substack{\parallel \\ \oplus_v \partial_v}}{\partial_S}: H_{\mathcal{F}_S}^1(K, E[p]) \rightarrow \bigoplus_{v \in S} H_{\text{sing}}^1(K, E[p]) \right)$$

↖ "residue" map