Recap of objectives: want to prove the

MW Thm: $E/\mathbb{Q}$ an ell. curve. Then $E(\mathbb{Q})$ is fin. gen.

We know now that $E(\mathbb{Q})_{tors}$ is finite. Need 2 more ingredients

Weak MW thm: $E/\mathbb{Q}$ EC, $n \geq 2$. Then $\frac{E(\mathbb{Q})}{nE(\mathbb{Q})}$ finite.

Heights: $\exists$ a non-degen. quad form on $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q}$.

It will be easy to deduce from these that $E(\mathbb{Q})$ fin gen. (note $n=2$ is the n suffice - see HW).

To prove weak MW, will use p-adics & Galois cohomology, which we define now.

Galois Cohomology: Part 1: finite gps

Def: let G a finite gp. & Π an abelian gp. An action of G on Π is a gp. hom $G \to Aut(\Pi)$, or equivalently a map of sets

$$G \times \Pi \to \Pi$$

s.t. $\forall g, g' \in G$ & $m, m' \in \Pi$, have

- $g(m'+m) = gm + gm'$
- $g(g'm) = (gg')m$
- $id_G \, m = m$.

Def: A G-module is an ab. gp Π together with an action of G.

eg L/K fin. Gal ext, E/K elliptic, then $G = Gal(L/K)$. Then L & $L^\times$ are G-modules in obv. way. $E(L)$ is so is $E(L)$.

Def: A morphism of G-modules $\Pi_1 \xrightarrow{f} \Pi_2$ is a morphism of ab. gps s.t. $\forall g \in G$, $m \in \Pi_1$, have
$f(gm_1) = g \cdot f(m_1)$.

Def: If $f: \Pi_1 \to \Pi_2$ a morphism of G-modules then $\ker f$, $\operatorname{im} f$ & $\operatorname{coker} f$ have natural G-module structure, & the canonical maps between them & Π_1, Π_2 are maps of G-modules.

Def: A sequence $A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} A_3 \to \cdots$ of G-modules is called exact if it is exact as a seq of ab. gps ($\ker f_{i+1} = \operatorname{im} f_i \ \forall i$).

eg. $G = \mathbb{Z}/2$, sequence $0 \to \mathbb{Z}/2 \to \mathbb{Z}/4 \to \mathbb{Z}/2 \to 0$
(trivial action; $x \mapsto -x$ acting; trivial action)

$0 \to 0$, $1 \to 3$

Def: If Π is a G-module, write $\Pi^G = \{m \in \Pi \mid gm = m \ \forall g \in G\}$ with trivial G-action = 'invariants'.

Prop: If $0 \to A \to B \to C \to 0$ is an exact seq. of G-modules, then the sequence
$0 \to A^G \to B^G \to C^G$
(induced maps) is exact.

Pf: ex. ('limit commute').

eg. sequence as in eg above. Then invariants gives

$0 \to \mathbb{Z}/2 \xrightarrow{\sim} \mathbb{Z}/2 \xrightarrow{\text{zero map}} \mathbb{Z}/2$

not surjective!

The idea of group cohomology is to measure the failure of exactness, in a functorial way.

Def: Let Π a G-module.
A crossed hom is a map of sets $f: G \to \Pi$ s.t.

$$\forall g,h \in G, \text{ have } f(gh) = f(g) + g \cdot f(h).$$

A principal crossed hom is a map $f: G \to \Pi$ s.t. $\exists m \in \Pi$ s.t.

$$\forall g \in G, \ f(g) = gm - m.$$

~~[The sets of PCHs, and CHs, & form a subgp.]~~

~~Define $H^1(G,M)$ =~~

Ex: The set of CHs form an abelian gp under addition;
- Every PCH is a CH;
- The set of PCH is a subgp of CHs.

Define $H^1(G,M) = \dfrac{CH(G,M)}{PCH(G,M)}$, an abelian gp.

Also define $\Pi^0(G,\Pi) = \Pi^G$. — Made it to here, 16/3/20 (s(ended here)).
Ex: If G acts trivially on Π then $H^1(G,\Pi) = \mathrm{Hom}(G,\Pi)$.

If $f: A \to B$ a map of G-modules, then get natural homs

$$H^1(G,A) \to H^1(G,B), \text{ by composing.}$$

Prop

Pf

Thm

pf

Prop/Def: Let $0 \to A \to B \xrightarrow{\pi} C \to 0$ a SES of G-modules. Define $\delta: H^0(G,C) \to H^1(G,A)$ by:

Let $c \in H^0(G,C) = C^G$. Let $b \in B$ s.t. $\pi(b) = c$ (need that there $b \in B^G$),
& set $\delta(c)(g) = gb - b$.

Pf that δ is a well-def'd gp hom.

Let $b' \in B$ s.t. $\pi(b') = c$. Then $\pi(b'-b) = 0$. Let $a \in A$ s.t. $a+b = b'$.

Then $gb' - b' = g(b+a) - (b+a) = (gb-b) + \underbrace{(ga-a)}_{\text{PCH}}$,

so well def'd

Gp hom easy. ex.

□

Thm: Let $0 \to A \to B \to C \to 0$ a SES of G-modules. Then the following sequence is exact:

$$0 \to H^0(G,A) \to H^0(G,B) \to H^0(G,C) \xrightarrow{\delta} H^1(G,A) \to H^1(G,B) \to H^1(G,C).$$

where unlabelled maps are natural ones.

Pf: A whole bunch of easy checks - omitted (ex). (□)

Hilbert 90:

Thm [Dedekind]: Let F a field & G a gp. Then every finite set $\{\chi_1, \dots, \chi_n\}$ of homs $G \to F^\times$ is lin. indep over F, i.e. if

$$\sum_{i=1}^{n} c_i \chi_i = 0 \text{ then } c_i = 0 \ \forall i.$$

Pf: omitted (ask hand). □

Thm ['Hilbert 90']: Let L/K finite Galois extension, $G = \mathrm{Gal}(L/K)$. Then

$$H^1(G, L^\times) = 0.$$

Pf: Let $f: G \to L^\times$ a crossed hom. — wts $f(g) = \frac{g\gamma}{\gamma}$ some $\gamma \in L^\times$.

Fact that f is a crossed hom. means

$\forall g, g' \in G$, have $f(gg') = f(g) \cdot g \cdot f(g')$.

Since the $f(g)$ are non-zero, Dedekind's thm implies the map

$$L \longrightarrow L \qquad \text{is non-zero,}$$

$$\ell \longmapsto \sum_{g \in G} f(g) \cdot g \cdot \ell$$

so $\exists \alpha \in L$ s.t.

$$\beta := \sum_{g \in G} f(g)\, g \cdot \alpha \neq 0.$$

Then $\forall g \in G$,

$$g \cdot \beta = \sum_{h \in G} g \cdot f(h) \cdot g(h\alpha) = \sum_{h \in G} f(gh) f(g)^{-1} (gh)\alpha$$

$$= f(g)^{-1} \sum_{h \in G} f(gh)(gh)\alpha$$

$$= f(g)^{-1} \sum_{h \in G} f(h) \cdot h\alpha = f(g)^{-1} \cdot \beta$$

Hence $f(g) = \frac{\beta}{g\beta}$, so setting $\gamma = \beta^{-1}$ we're done. □

Thm: If G has order m, then for every G-module Π, we have

$$m \cdot H^1(G, \Pi) = 0.$$

Pf - Omitted, ~3 pages to prove. (□)

Inflation & restriction

Def Let $H \leq G$ a subgp & Π a G-module (hence also an H-module)

By restriction, we get a map

$$CH(G \to \Pi) \longrightarrow CH(H \to \Pi),$$

sending PCHs to PCHs, $\rightsquigarrow$ a restriction map

$$\mathrm{Res} : H^1(G, \Pi) \longrightarrow H^1(H, \Pi)$$

Def $H \leq G$, $\Pi \in G$-mod. Then $\Pi^H = H^0(G, \Pi)$ is naturally a G/H-module (check!) & a crossed hom $G/H \xrightarrow{f} \Pi^H$

defines by composition

$$G \longrightarrow G/H \xrightarrow{f} \Pi^H \hookrightarrow H, \text{ a CH } G \to \Pi$$

Again, sends PCH to PCH, $\rightsquigarrow$ inflation map

$$\mathrm{Inf} : H^1(G/H, \Pi^H) \longrightarrow H^1(G, \Pi)$$

Prop: The sequence $0 \to H^1(G_{/H}, M^H) \xrightarrow{\text{Inf}} H^1(G,M) \xrightarrow{\text{Res}} H^1(H,M)$ is exact.

Pf: see Hilton. □

Galois cohomology

Def. A field k is perfect if every finite ext. of k is separable.

eg. if $\text{char } k = 0$ or k finite or $k = k^{alg}$.

eg NOT $\mathbb{F}_p(t)$.

Fix a perfect field k and a (separable) algebraic closure $\bar{k}$.

$G := \text{Gal}(\bar{k}/k)$.

Def The Krull topology on G is the top s.t. a subgp $H \leq G$ is open iff it fixes some finite extension $k \leq L \leq \bar{k}$.

Nb every open subgp is the complement of the union of its non-trivial cosets, & so is closed.

Def: We define the Krull topology on G by saying a subset $U \subseteq G$ is

open iff $\forall u \in U$ $\exists$ a subgp $H \leq G$ with:

- $u \cdot H \subseteq U$
- $[\bar{k}^H : k]$ finite.

Ex: In the topology, a subgp $H \leq G$ is open iff $[\bar{k}^H : k]$ finite.

Note every open subgp is complement of union of its non-trivial cosets, & so is closed.

Alternative description of the topology:

- map G to $\prod_{\substack{k \subseteq L \subseteq \bar{k} \\ [L:k]<\infty}} \mathrm{Gal}(L/k)$ by restriction (injective map!);

- give each $\mathrm{Gal}(L/k)$ as above the discrete top, & give the product the product of topology;

- give G the subspace top.

$G \simeq$: This is the Krull top. def'd above!

- G is cpt.

Thm: [Galois correspondence]: Inclusion reversing bijection:

$$\{\text{closed subgps of } G\} \longleftrightarrow \{\text{intermediate fields } \bar{k} \supseteq L \supseteq k\}$$

$$H \longmapsto \bar{k}^H$$

$$\mathrm{Gal}(L/k) \longleftarrow L$$

Moreover, $\{\text{open subgps}\} \Leftrightarrow [L:k] < \infty$.

Pf omitted.

Cor: every closed subgp of G is an intersection of open subgroups.

(5a)

Def A G-module M is *discrete* if the map $G \times M \to M$ is cts when M is given discrete top.

Eg: $M = \bar{k}$, $M = \bar{k}^*$, $M = E(\bar{k})$ } are all discrete, since they are unions of pts over finite extensions (check - ex!)

$\bar{k} = \bigcup_{L \text{ finite}} L$, $\bar{k}^* = \bigcup_{L \text{ finite}} L^*$, $E(\bar{k}) = \bigcup_{(L:k)<\infty} E(L)$

Cohomology:

Let M a discrete G-module. PCHs $: G \to M$ are automatically continuous (ex).

Ex: A CH $: G \to M$ is cts iff $\exists$ open normal $N \trianglelefteq G$ s.t. f comes from inflation from some CH $\frac{G}{N} \to M^N$.

(see Hw?). ↳ Don't assume this in Homework!

Def: $H^1(G, M) = \dfrac{\{\text{continuous CH}: G \to M\}}{\text{PCH}}$

Prop: $H^1(G, M) = \varprojlim_H H^1(\frac{G}{H}, M^H)$ as H runs over open normal subgps.

$H^1(G, M)$ is torsion.

Pf: ex, see Hw. □

Cor: $H^1(G, \bar{k}^*) = \varprojlim_{L/k \text{ finite}} H^1(\mathrm{Gal}(L/k), L^*) = 0$.

Pf: ex (easy from above). □

Def: For a field L & $n \in \mathbb{Z}_{\geq 1}$, set $\mu_n(L) = \{s \in L^\times \mid s^n = 1\}$.

~~Theorem~~

Eg (useful later):

Since $\bar{k}$ is k perfect, get SES:

$$1 \to \mu_n(\bar{k}) \to \bar{k}^\times \xrightarrow{n} \bar{k}^\times \to 1$$

$\rightsquigarrow$ long exact seq

$$1 \to \mu_n(k) \to k^\times \xrightarrow{n} k^\times \to H^1(G, \mu_n(\bar{k})) \to H^1(G, \bar{k}^\times) = 0$$

$$\rightsquigarrow \quad \frac{k^\times}{(k^\times)^n} = H^1(G, \mu_n(\bar{k})).$$

Notation: for E/k EC, set $H^i(k, E) := H^i(\mathrm{Gal}(\bar{k}/k), E(\bar{k}))$

Change of field:

Let $E/\mathbb{Q}$ an EC, $\bar{\mathbb{Q}}$ an alg. cl. of $\mathbb{Q}$, & $\bar{\mathbb{Q}}_p$ an alg. cl. of $\mathbb{Q}_p$.

The canonical embedding $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ extends non-uniquely to an embedding

$$\mathbb{Q}_p(\bar{\mathbb{Q}}) \hookrightarrow \bar{\mathbb{Q}}_p,$$

yielding a restriction map $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

In fact this map is $\hookrightarrow$. We then obtain by composition a map $H^1(\mathbb{Q}, E) \to H^1(\mathbb{Q}_p, E)$,

$\leftarrow$ In fact, indep. of choice of $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$.

Pf of wk MW part I: Selmer & Tate-Shafarevich gps

E/k ell. curve, k perfect, $\bar{k}$ alg. cl., $n \in \mathbb{Z}_{\geq 1}$

Define a morphism of functors

$$E \xrightarrow{[n]} E \quad \text{by sending } p \in E(L) \text{ to } n \cdot p.$$

So $\ker([n](L) : E(L) \to E(L)) = E(L)[n]$ by def'n.

Recall: If $\mathrm{char}\, k \nmid n \in k^\times$ then

$$E(\bar{k})[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},$$

& if $n \in k$ then $E(\bar{k})[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

(proven for $n = 2$ & 3, which is all we really need & more).

Thm: $[n](\bar{k}) : E(\bar{k}) \to E(\bar{k})$ is surjective.

Pf: Many pfs, all need some non-trivial Ab Input. We do a fast one - If you don't understand don't worry, won't be on HW or exam

$\ker[n]$ is finite & $E(\bar{k})$ infinite, so $[n]$ is not constant. ~~A non-constant map between smooth projective curves is surjective.~~ Pf

Pf: E is projective hence proper, hence $[n]$ is proper, hence image of $[n]$ is closed. E is connected, so image of E is connected. Hence image is a closed, connected subvar & is not finite, so must be whole of E. □

Therefore the sequence of $G = \mathrm{Gal}(\bar{k}/k)$ modules

$$1 \to E[\bar{k})[n] \to E(\bar{k}) \xrightarrow{[n]} E(\bar{k}) \to 1 \text{ is exact,}$$

so we get a long exact seq. in cohomology:

$E(k)[n]$ $\quad$ $E(k)$ $\quad$ $E(k)$ $\quad$ ← see HW.

$$1 \to H^0(k, E(\bar{k})[n]) \to H^0(k, E(\bar{k})) \xrightarrow{[n]} H^0(E(k)) \to$$

$$\to H^1(k, E(\bar{k})[n]) \to H^1(k, E) \xrightarrow{[n]} H^1(k, E) \to$$

$\rightsquigarrow$ SES

$$1 \to \frac{E(k)}{nE(k)} \to H^1(k, E[n]) \to H^1(k, E)[n] \to 0.$$

If $k = \mathbb{Q}$, gets Mordell finite. But not in general finite;

eg. $n = 2$, and assume $E(\mathbb{Q})[2] = 4$,

so $E(\mathbb{Q})[2] = E(\bar{\mathbb{Q}})[2]$.

Then

$$H^1(\mathbb{Q}, E[2]) \simeq H^1(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \mu_2(\bar{\mathbb{Q}}) \times \mu_2(\bar{\mathbb{Q}}))$$

$$\overset{\text{ex}}{=} H^1(G, \mu_2) \times H^1(G, \mu_2)$$

$$\overset{\text{see earlier}}{=} \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}} \times \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}.$$

So not enough to show $\frac{E(\mathbb{Q})}{2E(\mathbb{Q})}$ finite.

Idea: Introduce p-adic data, to get more constraint on $\frac{E(\mathbb{Q})}{nE(\mathbb{Q})}$.

Have sequences

$$1 \to E(\mathbb{Q})/nE(\mathbb{Q}) \to H^1(\mathbb{Q}, E[n]) \to H^1(\mathbb{Q}, E)[n] \to 1$$

$$\downarrow \qquad\qquad \downarrow \qquad\qquad \downarrow \quad \text{exist from before}$$

$$1 \to E(\mathbb{Q}_p)/nE(\mathbb{Q}_p) \to H^1(\mathbb{Q}_p, E[n]) \to H^1(\mathbb{Q}_p, E)[n] \to 1$$

ex: check diagram commutes.

Def: Set $\mathbb{R} = \mathbb{Q}_\infty$, then above holds also for $p = \infty$.

Set $\Omega_{\mathbb{Q}} = \{2, 3, 5, \ldots\} \cup \{\infty\}$.

Def [Selmer gp]:

$$S^{(n)}(E/\mathbb{Q}) = \ker\left(H^1(\mathbb{Q}, E[n]) \to \prod_{p \in \Omega_{\mathbb{Q}}} H^1(\mathbb{Q}_p, E) \right)$$

So $S^{(n)}(E/\mathbb{Q})$ contains image of $E(\mathbb{Q})/nE(\mathbb{Q})$.

↑ will turn out to be finite!

Def [Tate-Shafarevich gp]:

$$Ш(E/\mathbb{Q}) = \ker\left(H^1(\mathbb{Q}, E) \to \prod_{p \in \Omega_{\mathbb{Q}}} H^1(\mathbb{Q}_p, E) \right).$$

Lemma For any pair of maps $A \xrightarrow{\alpha} B \xrightarrow{\beta} C$ in an ab. cat (eg. gps), have canonical exact seq

$$0 \to \ker\alpha \hookrightarrow \ker(\beta\circ\alpha) \xrightarrow{\alpha} \ker\beta \longrightarrow \operatorname{coker}\alpha \xrightarrow{\beta} \operatorname{coker}(\beta\circ\alpha) \to \operatorname{coker}\beta \to 0$$

Pf: omitted/ex/see 'Appendix: some homological algebra' in Milne's class field theory notes (online) □

Cor: Get a SES

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \longrightarrow S^{(n)}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[n] \to 0$$

Pf: Apply lemma to

$$H^1(\mathbb{Q}, E[n]) \longrightarrow H^1(\mathbb{Q}, E)[n] \longrightarrow \prod_{p \in \Omega_{\mathbb{Q}}} H^1(\mathbb{Q}_p, E)[n]$$

□

Next: finiteness of Selmer groups (~ Shafarevich-Tate gp. Don't forget heights!)