Seminar on Euler Systems + Selmer Groups

Goals:

Galois representations ↙

- Selmer groups
- Eisenstein congruences
- Euler systems & Kolyvagin systems.
- Special values of L-functions.

Galois representations

Let p be a rational prime.

$R :=$ local noetherian complete ring of residual characteristic p. Let $k_R = R/m_R$ the residue field.

If R is reduced, write F_R for its ~~field~~ total ring of fractions.

For K a number field or a locally compact local field of char 0, let G_K be its absolute Galois group $(= Gal(\overline{K}/K))$.

If v is a place of K (and set $S_K = \{$places of $K\}$), set $K_v =$ completion.

Choosing some $\overline{K_v}$ and an embedding $\overline{K} \hookrightarrow \overline{K_v}$ gives $D_v \subset G_K$ a decomposition subgroup at v (and a choice of D_v gives an embedding, as well).

$G_{K_v} \cong D_v \supset I_v \leftarrow$ inertia subgroup.

Let Frob_v be the geometric Frobenius: on $k_v = O_{K_v}/\mathfrak{p}_v$, it acts as

$\mathrm{Frob}_v(x) = x^{-q_v}$, $q_v = \# k_v$.

Let M be a finitely-generated R-module. (or co-finitely generated). (its Pontryagin dual is fin-gen)

~~Times~~ Most of the time M is free (or co-free over R) $M^{*} = \mathrm{Hom}(M, \mathbb{Q}_p/\mathbb{Z}_p)$

We consider representations

$$G_K \to GL_R(M)$$

Let T be a free R-module.

<u>Assumption</u> (irreducibility): $T \otimes F_R$ is absolutely irreducible.

(A')
<u>Assumption</u> (residual irreducibility): $T \otimes k_R$ is absolutely irreducible.

<u>Examples</u>: [illegible]

1) Characters of G_K.
2) Galois reps obtained from the Tate module of an abelian variety.

$$T = T_p A = \varprojlim_n A[p^n](\bar{K})$$

3) Galois reps attached to modular forms (or, more generally, to automorphic representations).
4) Deformations (p-adic) of the above. $\rightsquigarrow$ $R =$ (some quotient of) local components of a Hecke algebra.
5) Given T_0 from (1)-(3), can take twists:

$$T_0 \otimes \Lambda \quad , \Lambda = \mathbb{Z}_p [\![\mathrm{Gal}(K_\infty/K)]\!] \quad , \text{ where } K_\infty/K \text{ a } \overset{\text{some}}{\mathbb{Z}_p^d} \text{ extension.}$$

(eg $K = \mathbb{Q}$, $K_\infty \subset \mathbb{Q}(\zeta_{p^\infty})$, $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$.)

$\rightsquigarrow \Lambda = \mathbb{Z}_p[\![X]\!]$.

In this way ~~given a~~ we can consider all the Tate twists at once.

We will consider Galois modules of the form

$$M = T \text{ or } T^* = \mathrm{Hom}(T, \mathbb{Q}_p/\mathbb{Z}_p) \text{ with dual } G_K \text{ action.}$$

Also, we may take

$$M = V/T, \text{ where } V = T \otimes F_R.$$

To these G_K-reps there are attached Selmer groups.

* Extensions of Galois representations

$$0 \to M \to E \to \underset{\text{with the trivial action.}}{R} \to 0 \quad \text{in } \overset{\text{continuous}}{R[G_K]}\text{-modules.}$$

⇝ the class of E, $[E] \in \mathrm{Ext}^1_{G_K}(R, M)$.

⇝ an element of $H^1_{\mathrm{cont}}(G_K, M)$ (continuous cohomology).
$= H^1(K, M)$

(via: $0 \to M^{G_K} \to E^{G_K} \to R \longrightarrow H^1(G_K, M) \to \cdots$)
$1 \longmapsto [E]$

* "Selmer groups"

In general, we call a Selmer group an R-submodule of $H^1(K, M)$ defined by local conditions: for each $v \in S_K$, choose submodules

$$L_v(M) \subset H^1(K_v, M).$$

Let $\mathcal{F} = \{L_v(M) : v \in S_K\}$. We write also $H^1_{\mathcal{F}}(K_v, M) := L_v(M)$.

Define:

$$H^1_{\mathcal{F}}(K,M) = H^1_{\mathcal{F}} := \{c \in H^1(K, M) : c|_{D_v} \in L_v(M)\}.$$

$$= \mathrm{Ker}\left(H^1(K,M) \longrightarrow \prod_v \frac{H^1(K_v, M)}{L_v(M)} \right).$$

Remark: the Galois representations that we consider are unramified almost everywhere (ramified only at a finite set of places).

ie $\rho_M : G_K \to GL_R(M)$ is s.t

$\rho_M(I_v) = 1$ for almost all v.

The elements Cl_{D_v} is the isom. class of the $R[D_v]$-module E_v,

$$0 \to M \to E_v \to R \to 0$$

$$\rightsquigarrow \begin{tikzcd} 0 \arrow[r] & M^{I_v} \arrow[r] & E_v^{I_v} \arrow[r] & R \arrow[r] & H^1(I_v, M) \arrow[r] & \cdots \\ 0 \arrow[r] & M^{G_K} \arrow[r] \arrow[u] & E_w^{G_K} \arrow[r] \arrow[u] & R \arrow[r] \arrow[u, equal] & H^1(K, M) \arrow[u, "res"'] & \end{tikzcd}$$

If ρ is unram at v, then $M^{I_v} = M$, so ~~$\forall$~~ we expect E_v is unramified almost everywhere as well, ie

$\forall v$ ← for almost all, $L_v(M) := Ker\left(H^1(D_v, M) \to H^1(I_v, M)\right)$

$$= H^1(\underset{\overset{\wr\wr}{\hat{\mathbb{Z}}}}{G_{k_v}}, M^{I_v})$$ ← generated by $Frob_v$

This is called the unramified or (good reduction $(v \nmid p)$) condition:

$$L_v(M) = H^1_{ur}(K_v, M) = Ker\left(H^1(D_v, M) \to H^1(I_v, M)\right)$$

$$= M^{I_v} / (Frob_v - 1) M^{I_v}$$

We will consider only $\mathcal{F}$ such that

$$H^1_{\mathcal{F}}(K_v, -) = H^1_{ur}(K_v, -) \quad \text{for almost all } v.$$

(for all $v \notin S$ ← usually will contain p).

If $v|p$, there is also a *good reduction condition*, which is more complicated to define (using p-adic Hodge theory), at least when R is a finite extension of $\mathbb{Z}_p$.

In this case, T could ~~be~~:

a) crystalline ($\leftrightarrow$ good reduction)

b) semi-stable

c) de Rham $\leftarrow$ all coming from geometry.

Then $H^1_{\textcircled{f}}(K_v, T)$ classifies extensions which are crystalline $\left(\substack{\text{when} \\ T \text{ is crystalline}}\right)$. (Bloch-Kato definition). Also if $v \nmid p$, $H^1_f = H^1_{ur}$.

Still when $v|p$, there is the *ordinarity condition*: (R. Greenberg).

M is *ordinary*$^{(*)\text{ at } v}$ if there is a filtration which is stable by D_v, and such that on the graded pieces D_v acts by characters.

$(*)$ (we should say here *nearly-ordinary*, since *ordinary* gives also condition on the characters that appear in the graded pieces).

For the ordinarity condition, R is not required to be a finite extension of $\mathbb{Z}_p$, and it works well with Iwasawa theory (unlike the good reduction condition).

The *unobstructed condition* is $H^1_F(K_v, M) = H^1(K_v, M)$.

The *strict condition* is $H^1_F(K_v, M) = 0$

The *dual condition*: consider the local Tate duality: $M^*(1) = \overset{\text{as } \mathbb{Z}_p\text{-mod.}}{\mathrm{Hom}}(M, \mu_{p^\infty})$

$$v : H^1(K_v, M) \times H^1(K_v, M^*(1)) \longrightarrow H^2(K_v, \mu_{p^\infty}) \underset{\text{local CFT}}{\cong} \mathbb{Q}_p/\mathbb{Z}_p$$

(a perfect duality)

If $\mathcal{F}$ is a system of local conditions for M, we obtain local conditions for $M^*(1)$, $\mathcal{F}^*$, defined by:

$$\forall v \quad H^1_{\mathcal{F}^*}(K_v, M^*(1)) = H^1(K_v, M)^{\perp}.$$

<u>Prop</u>: $H^1_f(K_v, M)^{\perp} = H^1_f(K_v, M^*(1))$.

(and also $(\text{unobstructed})^* = \text{strict}$, $(\text{strict})^* = \text{unobstructed}$)

<u>L-functions.</u>

We first define local Euler factors. ~~Assume~~ T^{I_v} is a projective R-module $(\forall v)$, define

$$P_v(X,T) := \det\left(1 - X\rho_T(\mathrm{Frob}_v) \mid \boxed{T^{I_v}}\right) \in R[X]. \qquad (v \nmid p)$$

$$L_v(X,T) := P_v(X,T)^{-1}.$$

for $p \mid v$, replace with $D_{cris}(T)$.

If $P_v(X,T) \in \overline{\mathbb{Q}}[X]$ for all v, then we can consider the Euler product

$$L(s, \rho_T) := \prod_v L_v(q_v^{-s}, T)$$

One expects in general that this converges for $\mathrm{Re}(s) \gg 0$ and has meromorphic continuation + functional equation...

If $P_v(X,T) \notin \overline{\mathbb{Q}}[X]$, we can define in many cases a p-adic L-function $L(X,T)$.

The general expectation is that the size of $H^1_{\mathcal{F}}(K, T^*(1))$ is related to the behavior of $L(s, \rho_T)$ at $s=0$

$\nwarrow$ depending on $\mathcal{F}$.

<u>eg</u>: if $\mathcal{F} = \mathcal{F}_S = \begin{cases} L_v = H^1_f & \text{for } v \notin S \\ L_v = \text{unobstructed} & v \in S \end{cases}$

then $L_{\mathcal{F}}(s, \rho_T) = L^S(s, \rho_T)$ (take away the local factors at S).

The dual Selmer group

$$X_{\mathcal{F}}(K, T^*(1)) = H^1_{\mathcal{F}}(K, T^*(1))^{*}$$ ← Pontryagin dual.

is finitely-generated over R, and ~~its size~~ when we say "size" of $H^1_{\mathcal{F}}(K, T^*(1))$ we mean $\mathrm{rk}\, X_{\mathcal{F}}(K, T^*(1)) \otimes F_R$, and the Fitting ideal of the torsion part of $X_{\mathcal{F}}(K, T^*(1))$.

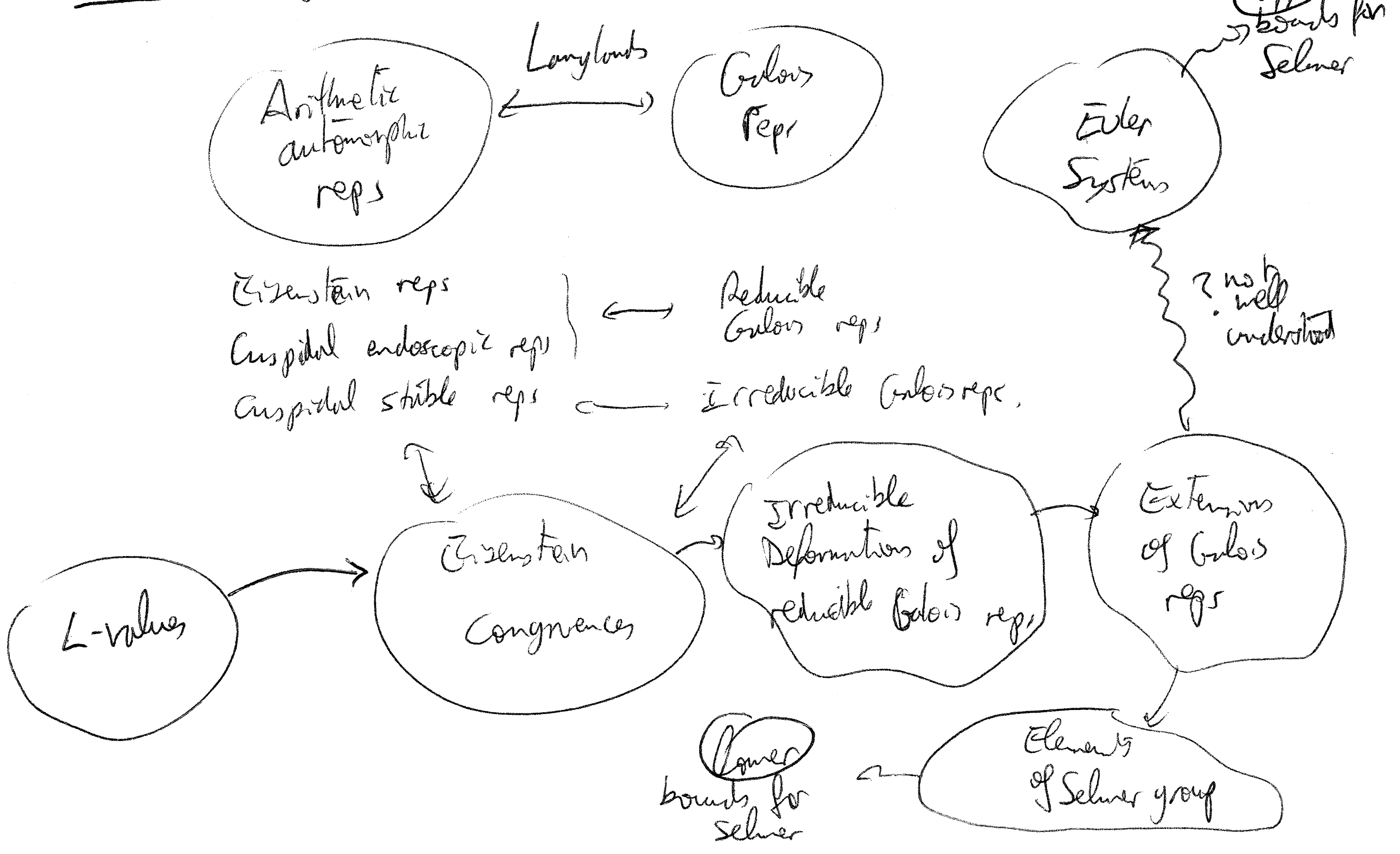
According to the choice of $\mathcal{F}$, the expectation is that

$$\mathrm{rk}\, X_{\mathcal{F}} = \text{order of vanishing of } L_{\mathcal{F}}(s, \rho_T) \text{ at } 0.$$

If $\mathrm{rk}\, X_{\mathcal{F}} = 0$, then the $\mathrm{Fitt}_R(X_{\mathcal{F}}) = (L_{\mathcal{F}}(0, \rho_T))$ ← principal ideal generated by..

This kind of statement includes conjectures BSD, Mazur, Greenberg, Bloch-Kato, ...
and some well-known cases (units, class # formula, Iwasawa Main conjecture, ...).

Eisenstein congruences



Suggested topics.

Ⓐ Local and Global Tate duality.

Ⓑ Proof of Iwasawa Main Conjecture using Eisenstein congruences. (following Wiles).

Ⓒ " ——————————— " following Rubin (Euler system).

Ⓓ Bloch-Kato conjectures on Tamagawa numbers
(including the definition of H^1_f of Bloch-Kato).

Ⓔ Examples of Selmer groups (using as reference a paper of Greenberg)
in the ordinary case

Ⓕ Kolyvagin systems. (following Mazur-Rubin).

An Euler system is a collection of ~~extensions~~ $c_m \in H^1_{S}(\mathbb{Q}(\zeta_m), T)$
for m coprime to some fixed set S, ~~good reduction away from~~ S.
satisfying some compatibility relation: $\mathrm{cores}_{\mathbb{Q}(\zeta_{m\ell})/\mathbb{Q}(\zeta_m)}(c_{m\ell}) = \begin{cases} c_m & \text{if } \ell \mid m \\ P_\ell(\ell^{-1}\underbrace{\sigma_{m,\ell}}_{\substack{\uparrow \\ \mathrm{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q}) \\ (x \mapsto x^\ell \bmod \ell.)}}, T^*) \cdot c_m & \ell \nmid m \end{cases}$

Kolyvagin classes are elements κ_m

$\kappa_m \in H^1(\mathbb{Q}, T/p^? T)$
with specific ramification conditions.

· Examples of Selmer groups

K a number field, M a G_K-module over R. ← local Noeth. complete.

$\mathcal{F} = \{ L_v(M) \subset H^1(K_v, M) \}$. (and $L_v(M) =: H^1_{\mathcal{F}}(K_v, M)$).

$$H^1_{\mathcal{F}} = \ker\left(H^1(K,M) \longrightarrow \prod \frac{H^1(K_v,M)}{L_v(M)} \right)$$

$H^1_{\mathcal{F}}(K,M)$.

①. $L/\mathbb{Q}_p$ finite extension, $\mathcal{O}_L \subset L$. $T = \mathcal{O}_L(\chi)$ $\chi : G_K \to \mathcal{O}_L^\times$

$\nwarrow$ $\mathcal{O}_L$ with action given by χ. $\nwarrow$ of finite order.

$M = T^* = \mathrm{Hom}(T, \mathbb{Q}_p/\mathbb{Z}_p)$.

$$H^1(K, T^*) = \mathrm{Hom}(G_{K'}, \mathbb{Q}_p/\mathbb{Z}_p)(\chi)$$

where $K' = \bar{K}^{\ker(\chi)}$.

Take $H^1_{\mathcal{F}}(K_v, T^*) = H^1_{ur}(K_v, T^*)$.

Then $H^1_{\mathcal{F}}(K, T^*) = \mathrm{Hom}(\mathrm{Gal}(H'/K'), \mathbb{Q}_p/\mathbb{Z}_p)(\chi) \cong \mathcal{C}\ell^*_{K'}[\chi]$

χ-component of dual of $\mathcal{C}\ell_{K'}$.

The class number formula gives a relation between

$$\# \mathcal{C}\ell_{K'} \leftrightarrow \mathrm{Res}(\zeta_{K'})\big|_{s=1}$$

(So if χ is not trivial) $\prod_{\chi \text{ odd}} \# \mathcal{C}\ell^*_{K'}[\chi] \rightsquigarrow \prod_{\chi \text{ odd}} L(\chi, 1)$.

② $T = \mathbb{Z}_p(1)$ $\rightsquigarrow$ Kummer theory:

$$1 \to \mu_{p^n}(\bar{K}) \to \bar{K}^\times \xrightarrow{(\ )^{p^n}} \bar{K}^\times \to 1$$

By H90, $H^1(K, \bar{K}^\times) = 1$, so get:

$$K^\times / (K^\times)^{p^n} \cong H^1(K, \mu_{p^n}).$$

Taking $\varinjlim_{n}$ get: $K^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p \cong H^1(K, \mathbb{Q}_p/\mathbb{Z}_p(1))$.

For v a finite place, get

$$K_v^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p \underset{\cancel{K_v}}{\cong} H^1(K_v, \mathbb{Q}_p/\mathbb{Z}_p(1)).$$

Then $x \in K_v^\times$, have $\kappa_v(x) \in H^1_{ur}(K_v, \mathbb{Q}_p/\mathbb{Z}_p(1))$ ~~or~~

$\iff v(x) = 0$. (b/c equivalent to $K_v(\mu_{p^n}, \sqrt[p^n]{x})/K_v(\mu_{p^n})$ unram).

~~Which~~

So if f = "unramified" get:

$$H^1_f(K_v, \mathbb{Q}_p/\mathbb{Z}_p(1)) = H^1_{ur}(\quad),$$

so $H^1_f(K, \mathbb{Q}_p/\mathbb{Z}_p(1)) \cong \mathcal{O}_K^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p$.

Therefore we get:

$$\text{corank } H^1_f(K, \mathbb{Q}_p/\mathbb{Z}_p(1)) = \text{rank } \mathcal{O}_K^\times = \text{ord } \zeta_K\big|_{s=0}.$$

(and note that $\zeta_K(s) = L(M^*(1), s)$ if $M = \mathbb{Q}_p/\mathbb{Z}_p(1)$).

③ Let E/K be an elliptic curve.

$$0 \to E[p^n](\bar{K}) \to E(\bar{K}) \xrightarrow{\cdot p^n} E(\bar{K}) \to 0$$

$$\rightsquigarrow 0 \to E(K)/p^nE(K) \to H^1(K, E[p^n]) \to H^1(K, E(\bar{K}))[p^n] \to 0$$

Rewriting for all localizations, gives (and taking ind lim):

$$0 \to E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1(K, E[p^\infty]) \to H^1(K, E(\bar{K}))[p^\infty] \to 0.$$

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & E(K)\otimes\mathbb{Q}_p/\mathbb{Z}_p \arrow[r] & \mathrm{Sel}(K,E) \arrow[r] \arrow[d] & Ш(K,E)[p^\infty] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & E(K)\otimes\mathbb{Q}_p/\mathbb{Z}_p \arrow[r] \arrow[d] & H^1(K,E[p^\infty]) \arrow[r] \arrow[d] & H^1(K,E)[p^\infty] \arrow[r] \arrow[d] & 0 \\
 & 0 \arrow[r] & \prod_v \frac{H^1(K_v,E[p^\infty])}{\mathrm{Im}\,K_v} \arrow[r] & \prod_v H^1(K_v,E)[p^\infty] \arrow[r] & 0
\end{tikzcd}$$

(so here $H^1_f(K_v, E[p^\infty]) = \mathrm{Im}(K_v)$).

Rmk: if $v\nmid p$, $\mathrm{Im}(K_v) = 0$.

This is b/c $E(K_v) \cong \mathbb{Z}_\ell^{[K_v:\mathbb{Q}_\ell]} \times$ finite. $\Rightarrow (\ )\otimes\mathbb{Q}_p/\mathbb{Z}_p = 0$ for $v\nmid p$.

If $v \mid p$,

$$\begin{array}{c} \mathrm{Im}(K_v) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{[K_v:\mathbb{Q}_p]} \\ \cap \\ H^1(K_v, E[p^\infty]) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{2[K_v:\mathbb{Q}_p]} \times \text{finite}. \end{array}$$

(so quotient has nontrivial corank).

If E has good ordinary reduction at v, let $\tilde{E}$ be its reduction,

let $$0 \to \underset{\uparrow\ \text{inertia grp.}}{I_v} \to \mathrm{Gal}(\overline{K_v}/K_v) \to \mathrm{Gal}(\overline{k_v}/k_v) \to 0$$

$$0 \to \overset{\cong\,\mathbb{Q}_p/\mathbb{Z}_p}{\mathcal{F}[p^\infty]} \xrightarrow{\varepsilon} E[p^\infty] \to \tilde{E}[p^\infty] \to 0$$ G_{K_v}-equiv exact sequence.

divisible part

Prop (Greenberg):

$$\mathrm{Im}\,\kappa_v = \mathrm{Im}\Big(H^1(K_v, \mathcal{F}[p^\infty]) \xrightarrow{\iota_*} H^1(K_v, E[p^\infty])\Big)_{\mathrm{div}/\mathrm{div}}$$

$$= \underbrace{\mathrm{Ker}\Big(H^1(K_v, E[p^\infty]) \to H^1(K_v, \hat{\tilde{E}}[p^\infty])\Big)_{\mathrm{div}}}.$$

called (Greenberg) $H^1_{\mathrm{ord}}(K_v, E[p^\infty])$

↑ described in terms of Galois cohomology!

If E has good supersingular reduction, then one can define

$H^1_f(K_v, E[p^\infty]) \longleftrightarrow \mathrm{Im}(\kappa_v)$ up to a finite part.

Conjecturally, Ш$(K,E) < \infty$ and therefore $\mathrm{rank}\, E(K) = \mathrm{corank}\, \mathrm{Sel}(K,E)$

and $\mathrm{corank}\,\mathrm{Sel}(K,E) = \mathrm{corank}\left(H^1_f(K, E[p^\infty])\right)$.

More generally:

T: f-gen free $\mathcal{O}_L$-module with G_{K_v}-action, $L/\mathbb{Q}_p$, $K_v/\mathbb{Q}_p$.

$V = T \otimes L$.

V ordinary $\Leftrightarrow$ $\exists$ filtration (G_{K_v}-stable) $\mathrm{Fil}^i V$ s.t

$$\mathrm{Gr}^i V = \frac{\mathrm{Fil}^i V}{\mathrm{Fil}^{i+1} V} \circlearrowleft G_{K_v} \supset I_{K_v} \text{ acts by } \chi_{\mathrm{cyc}}^i.$$

The integers s.t $\mathrm{Gr}^i V \neq 0$ are called the Hodge-Tate weights.

eg: if $T = T_pE$, E with good ord red or semi-stable $\Rightarrow$ $V_pE = T_pE \otimes \mathbb{Q}_p$ is ordinary.

Then $0 \to T^+ \to T \to T/T^+ \to 0$

where T^+ is defined s.t.
~~and if~~ T^+ has HT-weights > 0, then T/T^+ has HT-weights ≤ 0.

$$H^1_{ord}(K_v, T^*(1)) = \ker\left(H^1(K_v, T^*(1)) \to H^1(K_v, T^{+*}(1)) \right)$$

(if $T = T_pE$ and $\tilde{E}$ ordinary, $H^1(K_v, T^*(1)) = H^1_{ord}(K_v, E[p^\infty])$.)

Bloch-Kato's H^1_f

$B_{cris} \circlearrowleft Gal(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ + Filtration s.t. $B_{cris}^{G_{\mathbb{Q}_p}} = \mathbb{Q}_p$; $B_{cris}^{G_{K_v}} = K_v^{ur}$.
$\circlearrowleft \varphi$ (Frobenius)

w/

For V any ~~$G_{\mathbb{Q}_p}$-rep over [illegible] field $\mathbb{Q}_p$~~ G_{K_v}-rep over $\mathbb{Q}_p$

$$D_{cris,ur}(V) := (V \otimes B_{cris})^{~~G_{\mathbb{Q}_p}~~ G_{K_v}}$$

Def (Fontaine): V is crystalline $\Leftrightarrow$ $\dim_{~~K_v~~ K_v^{ur}} D_{cris}(V) = \dim_{\mathbb{Q}_p} V$

Given $0 \to V \to E \to \mathbb{Q}_p \to 0$, get (assume V crystalline)

$$\begin{tikzcd}
0 \arrow[r] & D_{cris}(V) \arrow[r] & D_{cris}(E) \arrow[r] & K_v^{ur} \arrow[r] & H^1(K_v, V \otimes B_{cris}) \\
0 \arrow[r] & V^G \arrow[r] \arrow[u] & E^G \arrow[r] \arrow[u] & \mathbb{Q}_p \arrow[r] \arrow[u] & H^1(K_v, V) \arrow[u] \\
 & & & 1 \arrow[r, mapsto] & {[E]}
\end{tikzcd}$$

So E is crystalline $\Leftrightarrow$ the image of $[E]$ in $H^1(K_v, V \otimes B_{cris})$ is zero.

So Bloch-Kato define (now for any rep V)

$$H^1_f = \ker\left(H^1(K_v, V) \to H^1(K_v, V \otimes B_{cris}) \right)$$

The same can be done for Bst.

Also, if T is a stable sublattice in V,

$$H^1_f(K_v, V/T) := \text{image of } H^1_f(K_v, V) \text{ in } H^1(K_v, V/T)$$

Example in Iwasawa Theory

Let K_∞/K a $\mathbb{Z}_p^d$-extension (e.g. $\mathbb{Z}_p$-cyclotomic extension $(d=1)$)

$$\begin{tikzcd} K(\mu_{p^\infty}) \arrow[d, dash] \\ K \end{tikzcd} \Big] \; \mathbb{Z}_p \times \underbrace{\text{finite gp}}_{\Delta}.$$

$$K_\infty = K(\mu_{p^\infty})^{\Delta}.$$

$\Gamma := \mathrm{Gal}(K_\infty/K)$.

$$\Lambda := \mathbb{Z}_p[[\Gamma]] := \varprojlim_n \mathbb{Z}_p[\Gamma/\Gamma^{p^n}]$$

Fixing $\{u_1, \dots, u_d\}$ ~~gen~~ topological generators of Γ, get $(T_i := u_i - 1)$.

$$\Lambda \cong \mathbb{Z}_p[[T_1, \dots, T_d]].$$

We choose for this example $R = \Lambda$. Let T be a fin. gen $\mathbb{Z}_p$-module, with action of G_K.

We'll define a Selmer gp $\subset H^1(K, (T \otimes_{\mathbb{Z}_p} \Lambda)^*)$ $\subset$ a Λ-module.

Using Shapiro's lemma $\left(\underset{M \text{ an } H\text{-mod}}{H \leq G} \Rightarrow H^1(H, M) = H^1(G, \mathrm{Ind}_H^G M)\right)$.

$$\mathrm{Ind}_H^G M = \{\varphi : G \to M : \varphi(gh) = h\varphi(g)\}$$

we see that

$$H^1(K, (T \otimes \Lambda)^*) = H^1(K_\infty, T^*) := \varinjlim_n H^1(K_n, T^*)$$

(where $K_n = (K_\infty)^{\Gamma^{p^n}}$).

If T is ordinary, one can define $H^1_{\mathrm{ord}}(K_{n,v}, T^*)$ for all n. and also $H^1_{\mathrm{ord}}(K_v, (T\otimes\Lambda)^*)$.

$\rightsquigarrow H^1_{\mathrm{ord}}(K, (T\otimes\Lambda)^*)$. This is related (often) to a p-adic L-function $L_{K_\infty/K}(T) \in \Lambda$.

Then $H^1_{\mathrm{ord}}(K, (T\otimes\Lambda)^*)$ cotorsion of co-finite type $\Longleftrightarrow L_{K_\infty/K}(T) \neq 0$.

<u>Example</u>: $T = \mathbb{Z}_p(\omega^i)$ $\overset{i \text{ odd}}{\text{where}}$ ω = Teichmuller character $\omega : G_{\mathbb{Q}} \to \mu_{p-1} \subset \mathbb{Z}_p^\times$.

~~Then $H^1_{\mathrm{ord}}(\mathbb{Q},$~~ $K_\infty = \mathbb{Q}_\infty$ = cyclotomic $\mathbb{Z}_p$-ext, $\Lambda = \mathbb{Z}_p[\![s]\!]$.

<u>Then</u>: $H^1_{\mathrm{ord}}(\mathbb{Q}, \Lambda(\omega^i)^*) = H^1_{\mathcal{F}}(\mathbb{Q}, \Lambda(\omega^i)^*)$ $\quad \mathcal{F}$ = unramified $\left(H^1_{\mathcal{F}}(\mathbb{Q}_v, -) = H^1_{\mathrm{ur}}(\mathbb{Q}_v, -)\right)$.

One then checks that

$$H^1_{\mathrm{ord}}(\mathbb{Q}, \Lambda(\omega^i)^*)^* \longleftrightarrow \text{Iwasawa module } X(\omega^i)$$

$$\begin{tikzcd} & M_\infty \arrow[dl, bend left, "X"] \\ \mathbb{Q}(\mu_{p^\infty}) \arrow[ur, dash] \arrow[d, dash, "\Gamma\times\Delta"'] & \\ \mathbb{Q} & \end{tikzcd}$$

M_∞ = maximal unramified p-abelian extension of $\mathbb{Q}(\mu_{p^\infty})$.

$X \nwarrow$ a Λ-torsion module.

Main conjecture: ~~[illegible]~~ $X(\omega^i)$ = Fitting ideal of the ω^i-branch of the Kubota-Leopoldt L-function.

Deformations of reducible Galois representations

k field.

Art_k : category of artinian local rings with residue field k.

$\widehat{\mathrm{Art}}_k$: pro-Artin — (proj limit of objects in Art_k)

$R \in \widehat{\mathrm{Art}}_k$; G a group, $A = R[G]$.

<u>Examples</u>:

1) $\underset{\underset{I}{\cup}}{R}, \underset{\underset{I_1}{\cup}}{R_1}, \underset{\underset{I_2}{\cup}}{R_2}$, assume $R/I \cong R_1/I_1 \cong R_2/I_2 =: S$

$\rho_i : G \to GL_{n_i}(R_i)$; $\rho : G \to GL_n(R)$, $n = n_1 + n_2$.

Assume that $tr(\rho)$ mod $I) = tr(\rho_1)$ mod I_1 $+ tr(\rho_2)$ mod I_2. (in S)

<u>Prop</u>: Assume that $\bar{\rho} = \rho$ mod m_R satisfies $(\bar{\rho_i} = \rho_i \text{ mod } m_{R_i})$.

$$0 \to \bar{\rho}_1 \to \bar{\rho} \to \bar{\rho}_2 \to 0$$ + non-split + $\bar{\rho}_1, \bar{\rho}_2$ absolutely irreducible non-isomorphic.

Then:

$$0 \to \rho_1 \otimes S \to \rho \otimes S \to \rho_2 \otimes S \to 0.$$

Pf Induction on the length of the quotients.

<u>Remark</u>: Can generalize it to $\rho_1, \dots, \rho_r$ representation with $\bar{\rho_i} \not\cong \bar{\rho_j}$ $i \neq j$.

Then given ρ s.t. $$\bar{\rho} = \begin{pmatrix} \bar{\rho}_1 & & * \\ & \bar{\rho}_2 & \\ 0 & & \ddots \; \bar{\rho}_r \end{pmatrix}$$

then $$\rho \text{ mod } I = \begin{pmatrix} \rho_1 \otimes S & * \\ & \ddots & \\ & & \rho_r \otimes S \end{pmatrix}.$$

② Assume still ρ_1, ρ_2, ρ but $\rho : G \to GL_n(F_R)$, where F_R = ring of fractions of R (so assume R is reduced)

Assume $tr(\rho) \in R$, and that $tr(\rho) \bmod I = tr(\rho_1) \bmod I_1 + tr(\rho_2) \bmod I_2$.

Assume $\bar{\rho}_1 \not\cong \bar{\rho}_2$, and $\bar{\rho}_i$ are abs. irred.

Then: there exists a lattice $\mathcal{L} \subset F_R^n$ which is G-stable, s.t there is a non-split extension

$$0 \to \mathcal{L}_1 \otimes \rho_1 \bmod I_1 \to \frac{\mathcal{L}}{I\mathcal{L}} \to \rho_2 \bmod I_2 \to 0 \quad (\text{as } G\text{-reps})$$

where $\mathcal{L} = \mathcal{L}_1 \oplus R$ as R-module.

- Deformations of reducible representations.

- R local, henselian, reduced $(+\text{ noetherian})$, $k = R/m_R$.
- $\rho_i : G \to GL_{n_i}(R)$ such that $(i=1,2)$.

  $\bar\rho_i : G \to GL_{n_i}(k)$ is absolutely irred, and $\bar\rho_1 \not\cong \bar\rho_2$

Let ~~$\rho = GL_n$~~ $\rho : G \to GL_n(F_R)$ $\overset{\text{absolutely}}{\text{irred.}}$ (F_R = total ring of fraction of R).

(Note that $R \hookrightarrow \prod_i A_i$, A_i integral domain, $F_R = \prod F_{A_i}$, F_{A_i} = fraction field of A_i).

Suppose that $tr(\rho) \in R$, and that for some ideal $I \subsetneq R$,

$$tr(\rho(g)) \equiv tr(\rho_1(g)) + tr(\rho_2(g)) \mod I \quad (\forall g)$$

Then: (a)• $\exists \underset{\nwarrow R\text{-module}}{\mathcal{L}} \subset F_R^n \circlearrowleft_\rho G$ stable under the action of G

($\Rightarrow \mathcal{L}$ is a lattice b/c ρ is irreducible).

Such that $\mathcal{L}$ has a unique irreducible quotient, and this quotient is isomorphic to $\bar\rho_2$.

(b)• $\mathcal{L}/I\mathcal{L}$ is reducible. More precisely, there is a s.es of RG-modules

$$0 \to \rho_1 \otimes \mathcal{I}/I\mathcal{I} \to \mathcal{L}/I\mathcal{L} \to \rho_2 \otimes R/I \to 0$$

for some faithful R-module $\mathcal{I}$ (contained $\mathcal{I} \subset R$ s.t $\mathcal{I} \otimes_R F_R = F_R$).

(c)• Moreover, $\mathcal{L}$ is unique up to isomorphism (satisfying (a)).

We will prove this in the case of ρ_1, ρ_2 being one-dimensional. In the general case the proof is essentially the same, but more technical.

Proof: Think of ρ as a map $\rho : R[G] \to M_2(F_R)$.

For $r \in R[G]$, write $\rho(r) = \begin{pmatrix} a_r & b_r \\ c_r & d_r \end{pmatrix}$.

Since $\bar\rho_1 \not\cong \bar\rho_2$, the map

$$\bar\rho_1 \oplus \bar\rho_2 : k[G] \twoheadrightarrow k \oplus k$$ is surjective (Brauer-Nesbitt).

Let $\bar r_1, \bar r_2$ s.t. $\bar\rho_i(\bar r_j) = \delta_{ij}$.

~~Since R is henselian, these lift to idempotents $r_1, r_2 \in R$, so $\rho_i(r_j) = \delta_{ij} \in R$.~~

If $\tilde r_i$ is any lift of $\bar r_i$ to R, then the characteristic polynomial of $\rho(\tilde r_i)$ is $\equiv X(X-1) \bmod m_R$.

Since R is henselian, $\exists$ lift of $\bar r_i$ s.t. $\rho(r_i)$ is an idempotent. In particular, char poly of $\rho(r_i)$ is $X(X-1)$,

We choose $e_2 \in F_R^2$ s.t. $\rho(r_2) \cdot e_2 = e_2$, and such that $F_R \cdot e_2 \cong F_R$.

Define $\mathcal{L}$ = R-submodule of F_R^2 generated by $\langle \rho(g) \cdot e_2 \mid g \in G \rangle$. (stable by construction)

write $\mathcal{L} = \mathcal{L}_1 \oplus \mathcal{L}_2$, $\mathcal{L}_i = \rho(r_i) \cdot \mathcal{L}$. (b/c $1 = \rho(r_1) + \rho(r_2)$).

So $\mathcal{L}_i$'s are R-modules (not G-stable!).

Write $\bar{\mathcal{L}} = \bar{\mathcal{L}}_1 \oplus \bar{\mathcal{L}}_2$, and note $\bar e_2 \in \bar{\mathcal{L}}_2$. Since $\bar{\mathcal{L}}$ is generated by $\bar e_2$ as $k[G]$-module,

$$\bar{\mathcal{L}}_2 = \rho(\bar r_2)\, \bar{\mathcal{L}} = \{ \rho(\bar r_2 \bar r) \cdot e_2 \} = k \bar e_2,$$ so $\bar{\mathcal{L}}_2$ is free of rk 1.

Since $\mathcal{L}_2 \otimes F_R$ is free of rank 1 over F_R, get $\mathcal{L}_2$ free of rank one over R.

We have:

$$\rho(r) = \begin{pmatrix} a_r & b_r \\ c_r & d_r \end{pmatrix}, \quad a_i \in F_R, \quad a_r \in \mathrm{Hom}_R(\mathcal{L}_1, \mathcal{L}_1)$$

$$b_r \in \mathrm{Hom}_R(\mathcal{L}_2, \mathcal{L}_1)$$

$$\vdots$$

Since $\rho(r_1) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $\rho(r_2) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, get:

$\mathrm{tr}(\rho(r_1 r)) = a_r \in R$, $\mathrm{tr}(\rho(r_2 r)) = d_r \in R$. (by hypothesis on traces).

Note that for $r, s \in R[G]$,

$$a_{rs} = a_r a_s + b_r c_s \in R \Rightarrow b_r c_s \in R \quad \forall r, s \in R[G].$$

Also, $\mathcal{L}_1 = \rho(r_1) \cdot \mathcal{L} = \{ \rho(r_1 r) \cdot e_2, \ r \in R[G] \} = \{ b_r e_2 \}$

So $\mathcal{L}_1$ is a faithful R-module (b/c ρ is irreducible, so $\{b_r\}$ generate an ideal s.t. $\otimes F_R \cong F_R$).

From $a_r + d_r \equiv \rho_1(r) + \rho_2(r) \mod I$, applying it to $r r_1$ and to $r r_2$ gives:

$a_r \equiv \rho_1(r) \mod I$

$d_r \equiv \rho_2(r) \mod I$.

(b/c $\rho_i(r_j) = \delta_{ij}$)

We also get $b_r c_s \in I$ $\forall r, s \in R[G]$.

$\Rightarrow c_s b_r e_2 \in I e_2 \Rightarrow c_s \mathcal{L}_1 \subset I e_2 = I \mathcal{L}_2$. (recall $\mathcal{L}_2 = R \cdot e_2$).

Since this holds $\forall s \in R[G]$, get: $\mathcal{L}_1 / I\mathcal{L}_1$ is G-stable, so get:

$$0 \to \mathcal{L}_1 / I\mathcal{L}_1 \to \mathcal{L} / I\mathcal{L} \to \mathcal{L}_2 / I\mathcal{L}_2 \to 0$$

$\uparrow$ action of G given by ρ_1 mod I.

$\uparrow$ action of G given by ρ_2 mod I

To show: $\mathcal{L}$ has a unique quotient. If not, let $\mathcal{L}' \subset \mathcal{L}$ be G-stable.

$$\mathcal{L}' = \mathcal{L}_1' \oplus \mathcal{L}_2',$$

$$\mathcal{L}/\mathcal{L}' = \mathcal{L}_1/\mathcal{L}_1' \oplus \mathcal{L}_2/\mathcal{L}_2' \quad \text{irreducible.}$$

If $\mathcal{L}_1/\mathcal{L}_1' \neq 0$, then $\mathcal{L}_1/\mathcal{L}_1' \cong \bar{\rho}_1$. In that case, $\mathcal{L}_2/\mathcal{L}_2' = 0$,

so $\mathcal{L}_2 = \mathcal{L}_2'$; so $e_2 \in \mathcal{L}_2' \Rightarrow e_2 \in \mathcal{L}' \Rightarrow \mathcal{L} = \mathcal{L}'$. ☒

(Rmk: for $n_1, n_2 > 1$ need a theorem of Carayol, that gives $tr(\rho') \equiv tr(\rho_1) \bmod I$ + ρ' irreducible rep $\Rightarrow \rho' \cong \rho \bmod I$).

Rmk: For the general proof, see [Urban] (Duke paper).

Pseudo-representations (of dimension G).

G a group (eg Gal group of a tot. real field).

Assume $\exists\, c \in G$, $c \neq id$, $c^2 = 1$. (complex conjugation) assume $2 \in R^\times$.

Consider then odd pseudorepresentations: for a ring R, consider a function $t : G \to R$ satisfying some relations so that t behaves like a trace.

[If $\rho : G \to GL_2(R)$ is odd, fix so so that $\rho(c) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$,

then set $r_1 = \frac{c + id}{2}$, $r_2 = \frac{id - c}{2}$, and if $\rho(r) = \begin{pmatrix} a(r) & b(r) \\ c(r) & d(r) \end{pmatrix}$,

then $a(r) = tr(\rho(r_1 r)) = \frac{tr(\rho(rc)) + tr(\rho(r))}{2}$, $d(r) = tr(\rho(r_2 r))$.

$$x(r,s) := b(r)\, c(s) \in R.$$
]

So a pseudorep is:

Def: An odd pseudorep of dimension 2 with values in R is the data of 3 maps:

$a : G \to R$

$d : G \to R$

$x(-,-) : G \times G \to R$

Satisfying the following relations:

i) $a(\sigma\tau) = a(\sigma)a(\tau) + x(\sigma,\tau)$

ii) $d(\sigma\tau) = d(\sigma)d(\tau) + x(\tau,\sigma)$

iii) $x(\sigma,\rho) = x(\rho,\sigma) = 0$ if $\rho = id$ or $\rho = c$.

iv) $x(\sigma,\tau)x(\rho,\eta) = x(\sigma,\eta)x(\rho,\tau)$

v) $x(\sigma\tau,\rho\gamma) = a(\sigma)a(\gamma)x(\tau,\rho)$ ← —— ~~← hard to write~~.

$+ a(\sigma)d(\rho)x(\tau,\gamma)$

$+ d(\tau)a(\gamma)x(\sigma,\rho)$

$+ a(\tau)d(\rho)x(\sigma,\gamma)$

Thm If π is a R-valued pseudorep and R is a field, then $\exists \rho$ s.t $\pi_\rho = \pi$.

Pf ① If $x(\sigma,\tau) = 0 \; \forall \sigma,\tau$, can take $\rho(\sigma) = \begin{pmatrix} a_\sigma & 0 \\ 0 & d_\sigma \end{pmatrix}$ and check this is a rep.

② If $\exists \sigma_0, \tau_0$ s.t $x(\sigma_0,\tau_0) \neq 0$. Then $\begin{cases} b_\sigma := \dfrac{x(\sigma,\tau_0)}{x(\sigma_0,\tau_0)} \\ c_\tau := \dfrac{x(\sigma_0,\tau)}{\cancel{x(\sigma_0,\tau_0)}} \end{cases}$

$\Rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a representation s.t $x(\sigma,\tau) = b_\sigma c_\tau$.

Prop: One can glue pseudorepresentations:

$\pi_1 : G \to R/I_1$; $\pi_2 : G \to R/I_2$. continuous pseudoreps . and $t_\sigma \in R/_{I_1 \cap I_2}$ $\forall \sigma \in \Sigma$

Suppose $\exists\, \Sigma \subset G$ dense (for G a topological group) such that

~~Suppose $\pi_1 \equiv \pi_2 \bmod I_1 + I_2$ on Σ.~~ $tr(\pi_i(\sigma)) \equiv t_\sigma \bmod I_i$ $\forall \sigma \in \Sigma$.

Then: $\exists\, \pi : G \to R/_{I_1 \cap I_2}$ pseudorep such that $\pi \equiv \pi_i \bmod I_i$.

In applications, Σ is a set of Frobenius elements in $Gal(\bar{F}/F)$, where F is a totally-real field.

Corollary: if $t_\sigma \in R$ $\forall \sigma \in \Sigma$, and a family $\mathfrak{P}_i \subset R$ s.t $\bigcap \mathfrak{P}_i = \{0\}$, and for each i we have $\pi_i : G \to R/_{\mathfrak{P}_i}$ pseudorep s.t $tr(\pi_i(\sigma)) \equiv t_\sigma \bmod \mathfrak{P}_i$, then

$\exists\, \pi : G \to R$ s.t $\pi \bmod \mathfrak{P}_i = \pi_i$.

Quick review of Hida Theory. p odd.

Λ-adic forms: Fix $u \in 1 + p\mathbb{Z}_p$ a top generator.

$\Lambda = \mathbb{Z}_p[[T]] \supset P_k = (1 + T - u^k)$.

Fix embeddings, $\bar{\mathbb{Q}} \xrightarrow{\iota_\infty} \mathbb{C}$, $\bar{\mathbb{Q}} \xrightarrow{\iota_p} \mathbb{C}_p$.

Let $f \in \Lambda[[q]]$. $f = a_0(T) + a_1(T)q + \cdots$

Fix an integer N, prime to p.

Def: f is a Λ-adic modular form of tame level N and nebentypus $\chi : (\mathbb{Z}/_{pN\mathbb{Z}})^\times \to \bar{\mathbb{Q}}^\times$ if for all $k \geq 2$, $\psi : (1 + p\mathbb{Z}_p) \to \bar{\mathbb{Q}}^\times$ of finite order,

$f(\overbrace{u^k \psi(u) - 1}^{\in \text{max ideal of } \bar{\mathbb{Z}}_p}) \in \bar{\mathbb{Z}}_p[[q]]$ is the q-expansion of a weight-k modular form of level Np^r and nebentypus $\chi\omega^{-k}\psi$

r = conductor of ψ

Denote by $M(N,\chi)$ the Λ-module of Λ-adic forms, we have an action of the Hecke algebra generated by $\left\{ \begin{array}{l} T_\ell \mid \ell \neq p \\ U_\ell \mid \ell \mid pN \\ \langle \ell \rangle \end{array} \right\}$ by the usual formulas on q-expansions.

Define $e_{\text{ord}} = \lim_{n \to \infty} U_p^{n!}$, which acts on $M(N,\chi)$.

We write $M^{\text{ord}} = e_{\text{ord}} \cdot M(N,\chi)$.

(the largest factor of $M(N,\chi)$ on which U_p acts invertibly).

<u>Theorem</u> (Hida, '80's).

a) $M^{\text{ord}}(N,\chi)$ is a fin. gen. free Λ-module.

Moreover, $M^{\text{ord}}(N,\chi) \otimes \Lambda/P_{\kappa,\chi} \cong M_\kappa^{\text{ord}}(Np^r, \chi\psi\omega^{-\kappa})$

(where $P_{\kappa,\chi} = (1+T-u^\kappa\psi(u))$).

b) Let $H^{\text{ord}}(N,\chi)$ be the Λ-subalgebra of $\text{End}_\Lambda(M^{\text{ord}}(N,\chi))$ generated by the Hecke operators. Then $H^{\text{ord}}(N,\chi)$ is a fin. gen. free Λ-module.

c) There is a perfect pairing

$$M^{\text{ord}}(N,\chi) \otimes H^{\text{ord}}(N,\chi) \longrightarrow \Lambda$$

$$F \otimes T \longmapsto a(1, F \mid T).$$

$$\left(\Rightarrow H^{\text{ord}}(N,\chi) \otimes \Lambda/P_{\kappa,\chi} \cong H_\kappa^{\text{ord}}(N, \chi\psi\omega^{-\kappa}). \right)$$

<u>Rmk.</u>

There is a similar theorem for cusp forms.

Example: $k \geq 3$,

$$E_k(q) = \frac{\zeta(1-k)}{2} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \qquad \sigma_{k-1}(n) = \sum_{d \mid n} d^{k-1},$$

Define $\sigma^{(p)}_{k-1}(n) = \sum_{\substack{d \mid n \\ (d,p)=1}} d^{k-1}$, and get:

$$E_k^{ord}(q) = \frac{\zeta^{(p)}(1-k)}{2} + \sum_{n=1}^{\infty} \sigma^{(p)}_{k-1}(n) q^n \qquad (\text{valid for } k \geq 2).$$

and $E_k^{ord} \mid U_p = E_k^{ord}$.

$$\sigma^{(p)}_{k-1,\psi}(n) = \sum_{\substack{d \mid n \\ p \nmid d}} d^{k-1} \psi(d)$$

$$\downarrow$$

(in fact, $E^{ord}_{k,\psi}(q) = \frac{L^{(p)}(1-k,\psi)}{2} + \sum \sigma^{(p)}_{k-1,\psi}(n) q^n$)

for $\psi : (\mathbb{Z}/p^r\mathbb{Z})^\times \to \bar{\mathbb{Q}}^\times$.

Then $\exists\, E_\mathcal{X}(T) \in M^{ord}(p, \mathcal{X})$ ~~such that~~

$$E_\mathcal{X}(T) = \frac{L_\mathcal{X}}{2} + \sum_{n \geq 1} \sigma_{\Lambda,\mathcal{X}}(n) q^n$$

such that $E_\mathcal{X}(u^k \psi(u) - 1) = E^{ord}_{k, \mathcal{X}\psi\omega^{-k}}$.

~~except if $\mathcal{X}$ =~~

Exercise: if $d \in \mathbb{Z}_p$, $(d,p)=1$, $\exists\, \langle d \rangle_T \in \Lambda$ such that

$$\langle d \rangle_{u^k \psi(u) - 1} = \psi(d) d^{k-1}.$$

Iwasawa Theory

1. Baby Case

p odd prime. $\mathbb{Q}_n \subset \mathbb{Q}(\mu_{p^n})$ the $\mathbb{Z}/p^n\mathbb{Z}$-ext, and $\mathbb{Q}_\infty = \bigcup_{n=1}^{\infty} \mathbb{Q}_n$.
Note that p is totally ramified in $\mathbb{Q}_\infty$.

Let L_n be the maximal unramified abelian p-extension of $\mathbb{Q}_n$, $L_\infty = \bigcup L_n$.

Arithmetic:

$X = \mathrm{Gal}(L_\infty/\mathbb{Q}_\infty)$ carries an action of $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$.

$\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]] \cong \mathbb{Z}_p[[T]]$, $\gamma \mapsto T+1$ (γ a top-generator of $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$)

Thus X is a Λ-module.

Claim: Let $\omega_n = \gamma^{p^n} - 1 = (1+T)^{p^n} - 1$.
Then $\mathrm{Gal}(L_n/\mathbb{Q}_n) \cong X/\omega_n X$.

$$\begin{tikzcd}
 & L_n^* \arrow[d, dash] & \\
 & L_n\mathbb{Q}_\infty \arrow[dl, dash] \arrow[dr, dash] & \\
L_n \arrow[dr, dash] & & \mathbb{Q}_\infty \arrow[dl, dash] \\
 & \mathbb{Q}_n &
\end{tikzcd}$$

Pf/ Let L_n^* = maximal abelian extension of $\mathbb{Q}_n$ in L_∞, then
ez to see: $\mathbb{Q}_\infty \subset L_n^*$, $L_n \subset L_n^*$.
By maximality of L_n, we have $L_n^*/L_n\mathbb{Q}_\infty$ must be totally ramified at p.
But L_∞ is unram. over $\mathbb{Q}_\infty$, so $L_n^* = L_n\mathbb{Q}_\infty$, $L_n \cap \mathbb{Q}_\infty = \mathbb{Q}_n$.

$\mathrm{Gal}(L_n/\mathbb{Q}_n) \cong \mathrm{Gal}(L_n^*/\mathbb{Q}_\infty)$, which is the abelianization of $\mathrm{Gal}(L_\infty/\mathbb{Q}_\infty)$
which is easily seen to be $\omega_n \cdot X$. (?.)

QED

Claim: X is finitely-generated (as a Λ-module).
Pf/ b/c $X/\omega_n X$ is finite ~~[illegible]~~ $\Lambda/$[illegible] :

There is a structure theory for finite torsion modules over Λ:
there is a Λ-module hom:

$$X \longrightarrow \bigoplus_{i=1}^{t} \Lambda / f_i(T)^{a_i}$$

with finite kernel + cokernel, with $f_i(T)$ irreducible polynomials, $a_i \geq 0$

Let $f_X(T) = \prod_i f_i(T)^{a_i}$

Let λ, μ be the degree of $f_X(T)$ and the largest integer μ s.t $p^\mu \mid f_X(T)$. (called λ-invariant and μ-invariant)

Theorem (Iwasawa): The p-part of the class number of $\mathbb{Q}_n$ is

$$p^{\lambda n + \mu p^n + 1} \quad \text{for } n \text{ sufficiently large.}$$

Iwasawa Main Conjecture (for totally real field).

Let F be a totally real field, and F_∞: cyclotomic $\mathbb{Z}_p$-extension of F.
So $\mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p$. Let $\gamma \in \underbrace{\mathrm{Gal}(F_\infty/F)}_{\Gamma_F}$ be a top-generator.
Let $u \in \mathbb{Z}_p^\times$ s.t $\gamma\zeta = \zeta^u$ $(\forall \zeta \in \mu_{p^\infty})$.
Define $\mathcal{E}_F$ to be the composition

$$G_F \longrightarrow \Gamma_F \hookrightarrow \Lambda_F^\times \qquad (\Lambda_F = \mathbb{Z}_p[[\Gamma_F]]).$$

Let ψ_F be an even Artin character of $\mathbb{A}_F$, and write F_ψ for the splitting field of ψ.
We say that ψ is of type $\begin{cases} S \text{ if } F_\infty \cap F_\psi = F. \\ W \text{ if } F_\psi \subset F_\infty \end{cases}$

Define: $L_p(1-n,\psi) := L(1-n, \psi\omega^{-n}) \prod_{\mathfrak{p} \in S_p} (1-\psi\omega^{-n}(\mathfrak{p}) N(\mathfrak{p}^{n-1}))$ $n \geq 1$ integer.

(ω = Teichmüller character)

Theorem (Deligne-Ribet).

Let $H_\psi(T) = \begin{cases} \psi(\gamma)(1+T) - 1 & \text{if } \psi \text{ is of type W} \\ 1 & \text{if } \psi \text{ is of type S.} \end{cases}$

There is a power series $G_\psi(T) \in \mathbb{Z}_p(\psi)[[T]]$ s.t.

$$L_p(1-s,\psi) = G_\psi(u^s-1) / H_\psi(u^s-1) \qquad \forall s \geq 1 \text{ integers.}$$

Moreover, if ρ is a character of type W, then:

$$G_{\psi\rho}(T) = G_\psi(\rho(\gamma)(1+T)-1).$$

Exceptional zeroes.

If for some $\mathfrak{p}$ we have $\psi\omega^{-1}(\mathfrak{p}) = 1$, then $L_p(1-n,\psi) = 0$ by definition (these are called trivial zeroes).

There are other possible zeroes of G_ψ for $T = 0$: coming from H_ψ (for ψ trivial)

Rmk: the second kind of zeros shouldn't exist! Colmez proved that there is such a zero, then there is a non-cyclotomic $\mathbb{Z}_p$-extension of F contradicting Leopoldt conjecture.

Galois side

Let χ be an odd Hecke character. Let $H = F_\chi(\mu_p)$, H_∞: cyclotomic $\mathbb{Z}_p$-ext of H. Write L_∞ for the maximal unramified abelian p-ext of H_∞.

Define $X = \mathrm{Gal}(L_\infty/H_\infty)$, a module for $\mathrm{Gal}(H_\infty/F)$ under conjugation.

$$\mathrm{Gal}(H_\infty/F) = \Delta \times \Gamma, \quad \text{for} \quad \Delta = \mathrm{Gal}(H_\infty/F_\infty) \cong \mathrm{Gal}(H/F)$$

and $\Gamma = \mathrm{Gal}(H_\infty/H) \cong \mathbb{Z}_p$. assume χ is of Type S.

Let X^χ = subset on which Δ acts by χ. This is a module over $\mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[T]]$.

Characteristic ideal

If A is a noetherian normal domain, and X is finite $/A$, define

$$\mathrm{char}_A X := \{x \in A \mid \mathrm{ord}_p(x) \geq \mathrm{length}_p X_p \ \forall p \text{ prime of } A \text{ of height } 1\}.$$

(if X is non-torsion, define $\mathrm{char}_A X = 0$).

<u>Main Conjecture</u>: If χ is odd of type S, then:

$$\mathrm{char}_\Lambda(X^\chi) = G_{\chi^{-1}\omega}(u(1+T)^{-1} - 1).$$

Proof For simplicity, assume $F=\mathbb{Q}$. Let V_χ be a adm'l Galois rep. $\left(V_\chi = T_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p\right)$

$$\begin{tikzcd}
H^1_{ur}(G_{\mathbb{Q}_n}, V_\chi) \arrow[r, phantom, "\cong"] & H^1_{ur}(G_{\mathbb{Q}_{n,\chi}}, V_\chi)^{G_{\mathbb{Q}_n}} \arrow[d, phantom, "\cong" rotate=90] \\
 & \operatorname{Hom}_{G_{\mathbb{Q}_n}}(G_{\mathbb{Q}_{n,\chi}}, V_\chi) \arrow[ul]
\end{tikzcd}$$

splitting field of χ adjoins p^nth roots of unity

Selmer group.

Then $\quad X^\chi = \varprojlim_n H^1_{ur}(G_{\mathbb{Q}_n}, V_\chi/T_\chi)^* \overset{\checkmark\ \text{Shapiro's lemma}}{=:} H^1_{ur}(\mathbb{Q}, \overset{T_\chi\otimes\varepsilon_{\mathbb{Q}}^*}{\cancel{V_\chi\otimes\varepsilon_{\mathbb{Q}}}})^*$

Now, the idea is to use families of Eisenstein series:

There are congruences:

$$\begin{tikzcd}
\text{families of Eisenstein series} \arrow[r] \arrow[d, leftrightarrow, "\text{congruences}"] & \text{reducible Galois reps} \arrow[d, leftrightarrow, "\text{cong}"] \\
\text{families of cusp forms} \arrow[r] \arrow[ur, phantom, ""] & \text{irred. Galois reps}
\end{tikzcd}$$

(with a dashed arrow from "congruences" to "cong")

Hida families:

Let $\mathbb{I}$ be a finite extension of Λ. A point $\phi \in \operatorname{Spec}\mathbb{I}$ is called "arithmetic" if there is $k \geq 2$ and $\zeta \in \mu_{p^\infty}$ s.t. the image of ϕ in $\operatorname{Spec}\Lambda$ corresponds to $\quad 1+T \longmapsto (1+p)^{k-2}\zeta$.

Write this $k = k_\phi$, the weight of ϕ.

Def: A Hida family is a formal q-expansion $\mathbb{f} = \sum_{n=1}^{\infty} a_n(\mathbb{f})q^n$, $(a_n(\mathbb{f}) \in \mathbb{I})$ such that for a Zariski dense set of arithmetic points ϕ,

$\sum a_n(\mathbb{f})_\phi q^n$ is the q-expansion of an <u>ordinary</u> modular form $\mathbb{f}_\phi$ of weight k_ϕ and nebentype determined by ϕ.

We first prove the conjecture ~~for~~ as ideals of $\Lambda \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

Step 1: For each $\alpha \in \overline{\mathbb{Q}_p}$, let $n_\chi(\alpha)$, $m_\chi(\alpha)$ be the multiplicities of the zeroes of α of LHS & RHS.

Claim: need only to prove $m_\chi(\alpha) \leq n_\chi(\alpha) \quad \forall \alpha \in \overline{\mathbb{Q}_p}$

(b/c by the asymptotic formula for the minus part of the class number of $\mathbb{Q}_{n,\chi}$ $\left(= p^{\lambda^- n + \mu^- p^n + \nu^-} \right)$

~~Also~~ $\Rightarrow$ $\operatorname{ord}_p h_n^- = p\tilde{\lambda}^- n + \tilde{\mu}^- p^n + \tilde{\nu}^-$ where $\tilde{\lambda}^-, \tilde{\mu}^-, \tilde{\nu}^-$ are defined

Similarly but replacing $\prod_{\chi \text{ odd}} f_\chi(T)$ by $\prod_{\chi \text{ odd}} G_{\chi^{-1}\omega}(1+p(1+T)^{-1}-1) \ldots$)

Taking $n \to \infty$, get $\lambda^- = \tilde{\lambda}^-$.

Step 2: Construct $\mathbb{E}_\chi$, a Hida family of Eisenstein series whose Galois rep. is $1 \oplus \chi^{-1}\omega^{-1} \cdot$ ~~f~~ $\cdot\, \varepsilon_{\mathbb{Q}}^{-1}$ where f = cyclotomic character.

$$\mathbb{E}_\chi = \frac{\widehat{G_{\chi^{-1}\omega^{-1}}(T)}}{2} + \sum \hat{A}_{\chi^{-1}\omega^{-1}}(n, T)\, q^n$$

where:
$$\widehat{G_{\chi^{-1}\omega^{-1}}}(T) = G_{\psi\omega^2}(u^2(1+T)-1)$$
$$\hat{A}_\psi(T) = A_{\psi\omega^2}(u^2(1+T)-1)$$

and
$$A_\psi(n,T) = \sum_{\substack{d \mid n \\ (d,p)=1}} \psi(d)\, d^{-1} \langle d \rangle_T .$$

Eisenstein congruences with fixed weight.

Fix N, p, and $k \geq 2$. ψ : Dirichlet character of level N.

We first assume that $N = \mathrm{cond}(\psi)$.

Consider the Eisenstein series of level N (or Np if $p \nmid N$), given by:

$$E_k(\psi)(q) = \frac{L(1-k,\psi)}{2} + \sum_{n\geq 1} \sigma^{(p)}_{k-1,\psi}(n) q^n \quad \leftarrow \text{level} \begin{cases} \Gamma_1(Np) & (p,N)=1 \\ \Gamma_1(N) & p \mid N \end{cases}$$

where $\sigma^{(p)}_{k-1,\psi}(n) = \sum_{\substack{d \mid n \\ (d,Np)=1}} \psi(d)\, d^{k-1}$.

It is an eigenform for the Hecke operators. In particular, $E_k | U_p = E_k$ (ordinary)

(recall, after fixing embeddings $\overline{\mathbb{Q}} \overset{\iota_\infty}{\hookrightarrow} \mathbb{C}$, $\overline{\mathbb{Q}} \overset{\iota_p}{\hookrightarrow} \overline{\mathbb{Q}}_p$ $\forall p$, ordinary means that the eigenvalues of U_p is a p-adic unit).

$$E_{k,\psi} | T_\ell = (1 + \psi(\ell)\, \ell^{k-1}) E_{k,\psi} \quad \forall \ell \nmid Np.$$

Galois rep attached to $E_{k,\psi}$ $\rightsquigarrow$ $\begin{pmatrix} 1 & 0 \\ 0 & \psi\, \varepsilon_{cyc}^{k-1} \end{pmatrix}$

(in general, if f is an eigenform, $\rho_f : G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{Q}}_p)$,

satisfies $tr(\rho_f(\mathrm{Frob}_\ell)) = \iota_p \circ \iota_\infty^{-1}(a_\ell)$?)

We look at forms which are congruent to $E_{k,\psi}$.

Let $h_{k,\psi}(\Gamma_1(N))$ (or Np.) = Hecke algebra generated by the T_ℓ $(\ell, Np)=1$, by U_p, acting on the space of cusp forms of weight k, nebentype ψ and level N (or Np).

Define the Eisenstein ideal to be $I_{k,\psi} \subset h_{k,\psi}$ generated by $\left(U_p - 1 ,\ T_\ell - (1+\ell^{k-1}\psi(\ell)).\ \forall \ell \right)$ $\left({}^{\text{all}}/\mathbb{Z}_p \right)$

So for any Hecke operator T, we have: $\leftarrow$ generated by the T_ℓ's and U_p.

$$T \equiv \lambda^{(E)}_{k,\psi}(T) \mod I_{k,\psi}.$$

We have a surjective map ($\mathcal{O}_\psi = \mathbb{Z}_p(\psi)$, finite ext of $\mathbb{Z}_p$).

$$\mathcal{O}_\psi \twoheadrightarrow h_{k,\psi}/I_{k,\psi}$$

Which gives an isomorphism:

$$\mathcal{O}_\psi/(\eta_{(E)}) \cong h_{k,\psi}/I_{k,\psi} . \qquad \eta_{(E)} \in \mathcal{O}_\psi .$$

Let $\mathfrak{m}$ be a maximal ideal of $h_{k,\psi}$ containing $I_{k,\psi}$.

Let R be the component of $h_{k,\psi}$ attached to $\mathfrak{m}$ (the localization).

Note that $h_{k,\psi}$ is semisimple b/c have the T_ℓ's and $N = \text{cond}(\psi)$.

So we have:

$$I_{k,\psi} \subset R \hookrightarrow \prod_f K_f$$

f cusp eigenforms of wt k, level $\Gamma_1(Np)$ s.t. $f \equiv E_{k,\psi}$ mod max'l ideal of $\overline{\mathbb{Z}}_p$.

$\Rightarrow a(p,f) \equiv 1$ $\quad \Rightarrow R$ is ordinary, i.e. U_p acts invertibly.

$\nwarrow$ p-adic unit

For each f as before, have a Galois rep, so get:

$$G_{\mathbb{Q}} \to \prod_f GL_2(K_f) = GL_2(R\otimes\mathbb{Q}_p).$$

irreducible (b/c all the f's are cusp forms).

If $\ell \nmid Np$, $\operatorname{tr}(\operatorname{Frob}_\ell) = T_\ell \leftarrow$ image of T_ℓ in R.

In particular, $\operatorname{tr}(\operatorname{Frob}_\ell) \equiv 1+\ell^{k-1}\psi(\ell) \mod I_{k,\psi}$

Assume now that $\psi\varepsilon^{k-1} \not\equiv 1$ mod max'l ideal of $\bar{\mathbb{Z}}_p$.

One can construct a lattice $\mathcal{L}$ such that $(I = I_{k,\psi})$

$$0 \to \mathcal{L}^+/I\mathcal{L}^+ \to \mathcal{L}/I\mathcal{L} \to R/I\,(\varepsilon^{k-1}\psi) \to 0$$

$\uparrow$ could choose anything here

where $\mathcal{L}^+ = \mathcal{L}^{c=id}$. (so $\mathcal{L} = \mathcal{L}^+\oplus\mathcal{L}^-$).

Since $R/I \cong \mathcal{O}/(\eta_{E,\psi})$ and $\mathcal{L}^+$ is a faithful R-module, commutative algebra gives length $\mathcal{L}^+/I\mathcal{L}^+ \geq$ length $\mathcal{O}/(\eta_{E,\psi})$, so can say:

$$0 \to \mathcal{I} \to \mathcal{L}/I\mathcal{L} \to (\mathcal{O}/\eta_{E,\psi})(\varepsilon^{k-1}\psi) \to 0$$

where $\mathcal{I}\ (= \mathcal{L}^+/I\mathcal{L}^+)$ is an $\mathcal{O}$-module with trivial Galois action and of length $\geq \operatorname{ord}(\eta_{E,\psi})$.

$$\rightsquigarrow \quad c \in H^1(\mathbb{Q}, \mathcal{I}(\psi^{-1}\varepsilon^{1-k})).$$

The lattice $\mathcal{L}$ is unramified away from Np. Also, $\mathcal{L}$ is "ordinary" at p, as a Galois rep.

$$f \text{ ordinary} \rightsquigarrow \rho_f\big|_{I_p} \sim \begin{pmatrix} \varepsilon^{k-1}\psi & * \\ 0 & 1 \end{pmatrix}.$$

Since $\varepsilon^{k-1}\psi \not\equiv 1 \bmod p$, $c|_{I_p}$ is a split extension (ie $c|_{I_p} = 0$).

$\Rightarrow$ $c \in H^1_{ur}(\mathbb{Q}, I(\psi^{-1}\varepsilon^{1-k}))$

We consider the Selmer group $H^1_{ur}(\mathbb{Q}, \mathcal{O}^*(\psi^{-1}\varepsilon^{1-k})) =: Sel(\psi^{-1}\varepsilon^{1-k})$.

where $\mathcal{O}^* = Hom(\mathcal{O}, \mathbb{Q}_p/\mathbb{Z}_p)$

Have a map

$$\begin{array}{ccc} Hom(I, \mathbb{Q}_p/\mathbb{Z}_p) & \hookrightarrow & Sel(\psi^{-1}\varepsilon^{1-k}) \\ \phi & \longmapsto & \phi \circ c \end{array}$$

injective b/c otherwise one could construct a quotient of $\mathcal{L}/I\mathcal{L}$ isomorphic to the trivial rep.

So $\text{ord}(\eta_{Eis}) \leq \text{length}(Sel(\psi^{-1}\varepsilon^{1-k}))$.

Connecting η_{Eis} to L-values.

There is a cusp form f (not necessarily eigen) s.t. $f \equiv E_{k,\psi} \bmod \eta_{Eis}$.

$\Rightarrow$ $\eta_{Eis} \mid L(1-k, \psi)$.. But we want the opposite divisibility to relate L-values to Sel !

One can show that there exists an ordinary cusp form s.t

$$f \equiv E_{k,\psi} \mod \frac{L(1-k,\psi)}{2}. \qquad H^0(X_1(N), \omega^{\otimes k}/\underset{\nwarrow \text{ ideal defining the cusps.}}{\mathcal{I}})$$

Why? There is a map

$$M_k(\Gamma_1(N), \psi, \mathbb{Z}_p) \longrightarrow \overset{\shortparallel}{\bigoplus_{\substack{[\gamma]\in \text{cusps} \\ \Gamma_1(N)\backslash SL_2(\mathbb{Z})}}} \mathbb{Z}_p$$

$$f \longmapsto \{ a(0, f|\gamma) : \gamma \in \text{cusps} \}$$

If k is sufficiently large, one can show that this map is surjective (use ample-ness of ω). (coker of the map is included in $H^1(X_1(N), \omega^{\otimes k}/\mathcal{I})$, which is 0 if $k \gg 0$.

For each cusp $[\gamma]$, choose $F_{[\gamma]}$ s.t $a(0, F_{[\gamma]}|\gamma') = \begin{cases} 1 & \gamma=\gamma' \\ 0 & \text{else} \end{cases}$,

and define $g = E_{k,\psi} - \sum_{[\gamma]} a(0, E_{k,\psi}|\gamma)\, F_{[\gamma]}$.

Then g is a cusp form by construction, and moreover $a(0, E_{k,\psi}|\gamma)$ is divisible by $L(1-k,\psi)$, so

$$g \equiv E_{k,\psi} \mod L(1-k,\psi)$$

In particular, $a(1,g) \equiv 1$ so $g \neq 0$.

Can send

$$\underset{\substack{\cap \\ h_{k,\psi}}}{T_\ell} \mapsto \frac{a(1, g|T_\ell)}{a(1,g)} \mod L(1-k,\psi)$$

$$= 1 + \ell^{k-1}\psi(\ell).$$

So

$$\mathcal{O}/\eta_{\mathrm{Eis}} \xrightarrow{\sim} h_{k,\psi}/I \twoheadrightarrow \mathcal{O}/L(1-k,\psi) \Rightarrow L(1-k) \mid \eta_{\mathrm{Eis}}.$$

Rmk: if $N \neq \mathrm{cond}(\psi)$, and still consider:

$$E^{N}_{k,\psi}(q) = \frac{L^{N}(1-k,\psi)}{2} + \sum_{n=1}^{\infty} \sigma^{(Np)}_{k-1,\psi}(n)\, q^{n}$$

Then the constant term at other cusps is not always divisible by

$L^{N}(1-k,\psi)$!

In this case, the good choice is given by:

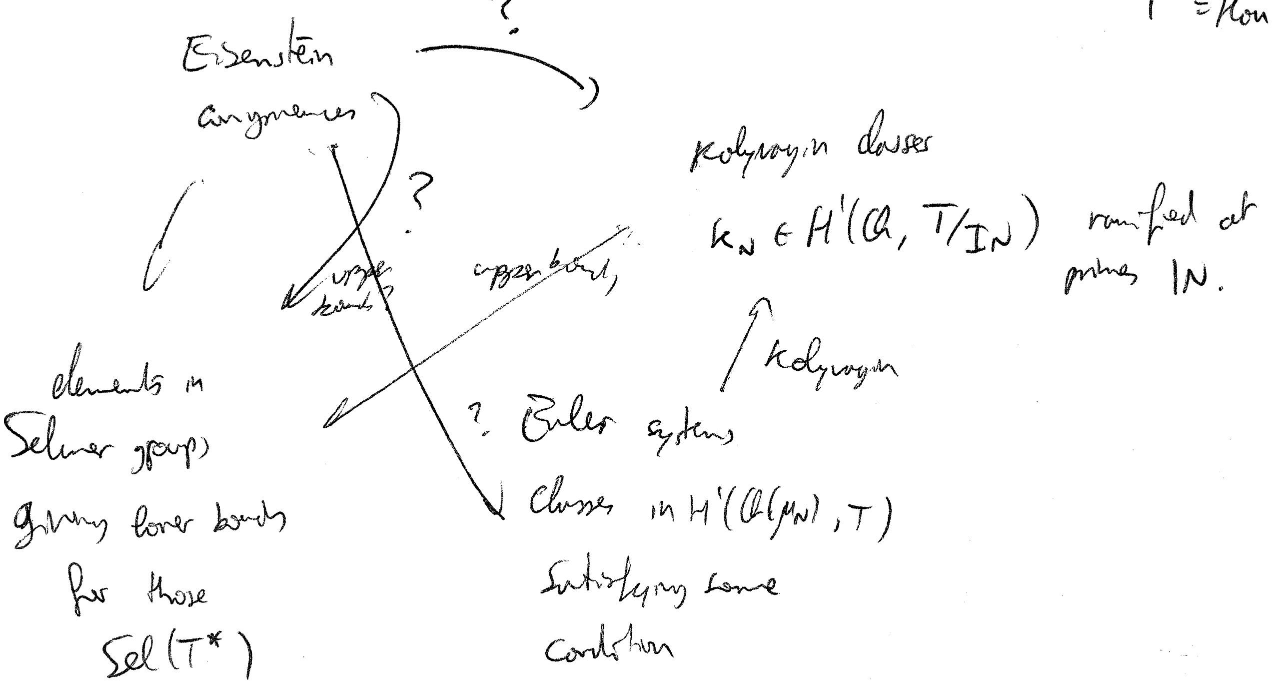
$$E^{N,\mathrm{good}}_{k,\psi} = \text{eigenform } \text{with eigenvalues} \quad U_p \leftrightarrow 1, \quad U_\ell \leftrightarrow \begin{cases} 1 & \text{if } \ell \mid \mathrm{cond}\,\psi \\ \ell^{k-1}\psi(\ell) & \text{if } \ell \mid \frac{N}{\mathrm{cond}\,\psi} \end{cases}$$

(rmk: need to have $\frac{N}{\mathrm{cond}\,\psi}$ squarefree, we can always do that in the applications).

Using Eisenstein congruences, one gets more classes in $Sel_N(\psi^{-1}\varepsilon^{1-k})$.

Therefore we get lower bounds for Sel.

Given T an $\mathcal{O}$-free module, $T^* = \mathrm{Hom}(T, \mu_{p^\infty})$.



Local Galois Cohomology

K a non-archimedean local field, $\mathbb{F}$ = residue field (assume finite).

$G_K = \mathrm{Gal}(\bar{K}/K)$. $\quad \bar{K} \supset K^{un} \supset K$.

$$\begin{matrix} G_K \\ \cup \\ I_K \end{matrix} \text{ inertia } \rightsquigarrow \quad 0 \to I_K \to G_K \to \overset{\mathrm{Gal}(K^{unr}/K)}{\overset{\parallel}{G_{\mathbb{F}}}} \to 1$$

Choose $Fr \in G_K$ a Frobenius element, so $Fr(x) = x^{\#\mathbb{F}} \quad \forall x \in \bar{\mathbb{F}}$.

Local CFT $\Rightarrow$ $W_K^{ab} \cong K^\times \cong \mathbb{Z} \times \mathcal{O}_K^\times$

Define $L \subset \bar{K}$ s.t L/K = maximal abelian totally tamely ramified ext'n.

(i.e $L = (K^{ab})^{\mathbb{Z} \times (1+\mathfrak{m}_K)}$, so $\mathrm{Gal}(L/K) \cong \mathbb{F}^\times$).

(e.g $K = \mathbb{Q}_\ell \rightsquigarrow L = \mathbb{Q}_\ell(\mu_\ell)$.)

Let T be a rep. of G_K (T an R-module).

- $H^1_{relax}(K,T) = H^1(K,T)$
- $H^1_{strict}(K,T) = 0$
- $H^1_{ur}(K,T) = \mathrm{Ker}\left(H^1(G_K,T) \to H^1(I_K,T)\right) \overset{\substack{\text{inf HS.}\\ \downarrow}}{=} H^1(G_{\mathbb{F}}, T^{I_K})$

If T is unramified, $T^{I_K} = T$, so $H^1_f(K,T) = H^1_{ur}(K,T) = H^1(G_{\mathbb{F}}, T)$.

Define also $H^1_s(K,T) = H^1(K,T)/H^1_f(K,T)$ (singular). ↖ finite part.

If K'/K is any extension,

$$H^1_{K'}(K,T) := \mathrm{Ker}\left(H^1(K,T) \to H^1(K',T)\right)$$

When $K' = L$, we call it the transverse condition, $H^1_{tr}(K,T) := H^1_L(K,T)$.

Lemma: Assume that T is unramified. Then:

- $H^1_f(K,T) \cong T/(Fr-1)T$
- $H^1_s(K,T) \cong \mathrm{Hom}(I_K, T)^{Fr=1}$

If $|\mathbb{F}^\times| \cdot R = 0$, then $H^1_s(K,T) = T^{Fr=1}$.

Proof: Have an exact sequence:

b/c $H^2(G_{\mathbb{F}}, T^{I_K}) = 0$.

$\uparrow$ Coh-dimension 1!

$$\begin{tikzcd}
0 \arrow[r] & H^1_f(K,T) \arrow[r] \arrow[d, equal] & H^1(K,T) \arrow[r] & H^1(I_K,T)^{Fr=1} \arrow[r] & 0 \\
& H^1(G_{\mathbb{F}},T) & & &
\end{tikzcd}$$

Note
$$\begin{tikzcd}
H^1(G_{\mathbb{F}},T) \arrow[r, "\cong"] & T \\
c \arrow[r, mapsto] & c(Fr)
\end{tikzcd}$$
and $\rightsquigarrow H^1(G_{\mathbb{F}},T) \cong T/(Fr-1)T$.

Finally, if $|\mathbb{F}^\times| R = 0$, ☒.

$$\mathrm{Hom}(I_K,T)^{Fr=1} = \mathrm{Hom}(\underbrace{I_K^{ab} \otimes \mathbb{F}^\times}_{\overset{\text{local CFT}}{\parallel}\ \mathbb{F}^\times}, T)^{Fr=1} \quad ☒.$$

Suppose now that:

- $|\mathbb{F}^\times| \cdot T = 0$
- T is free over R.
- $\det(1 - Fr \mid T) = 0$

Let $P(x) = \det(1 - Fr \cdot x \mid T)$. So $P(x) = (x-1)Q(x)$

Also, $P(Fr^{-1}) \cdot T = 0$ by Cayley Hamilton, so

$$Q(Fr^{-1}) \cdot T \subset T^{Fr=1} \quad \text{and} \quad Q(Fr^{-1})((Fr-1)\cdot T) = 0.$$

Therefore we get a map: $\phi^{fs} : H^1_f(K,T) \to H^1_s(K,T)$.

$$H^1_f(K,T) = T/(Fr-1)T \xrightarrow{Q(Fr^{-1})} T^{Fr=1} = H^1_s(K,T)$$ (called finite-singular hom).

Lemma: Assume $T/(Fr-1)T$ is free of rk $= 1$ over R. Then

$\phi^{fs} : H^1_f(K,T) \to H^1_s(K,T)$ is an isomorphism.

• Kolyvagin Systems

Refs: Mazur-Rubin "Kolyvagin Systems". ← book
"Introduction to Kolyvagin Systems".

Give axiomatic treatment + strengthening of Kolyvagin's method.

Simplicial sheaves

X : simplicial complex.

A simplicial sheaf ~~bd~~ on X is a group $\mathcal{H}(s)$ for every simplex s of X, together with maps $\mathcal{H}(s) \to \mathcal{H}(t)$ for all $s \subset t$.

(geometric realization: $U(s)$: open consisting of interiors of all simplices adjacent to s) then this corresponds on a sheaf on it: $U(t) \subset U(s)$ if $s \subset t$).

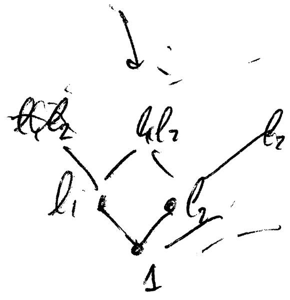
Let $\mathcal{L}$ be an (infinite) set of primes.

{vertices} = $\mathcal{N}(\mathcal{L})$ = {Squarefree products of elts of $\mathcal{L}$}

l. prime ⇝ edge n — ln. (two ~~edges~~ vertices n, n' are linked by an edge iff they differ by a prime).

$\mathcal{H}(n)$ = modified Selmer group,

$\mathcal{H}(e)$ = Local Galois cohomology group.



Local Galois Cohomology

R: complete noeth. local ring ~~R_p~~ (eg $\mathbb{Z}/p^n\mathbb{Z}$ ← main example, $R=\mathbb{Z}_p$, R = Iwasawa algebra).

T = finitely generated free R-module w/ action of $\mathcal{G}=\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

K = local field $(=\mathbb{Q}_v)$, $\mathbb{F}$ = residue field.

$\hat{\mathcal{F}} \subset H^1(K,T)$.

$\subset H^1_f$.

- $\hat{\mathcal{F}} = H^1_{un}(K,T) = \{c \in H^1(K,T) : c|_{I_v} = \text{trivial}\}$.
- $\hat{\mathcal{F}} = H^1_{lax}(K,T) = H^1(K,T)$
- $\mathcal{F} = H^1_{strict}(K,T) = 0$
- for L/K an ext, $H^1_L(K,T) = \mathrm{Ker}\left(H^1(K,T) \to H^1(L,T)\right)$.

$\rightsquigarrow \hat{\mathcal{F}} = H^1_{tr}(K,T) = H^1_L(K,T)$ where L/K = maximal abelian totally tamely ramified ext'n.

(eg $K=\mathbb{Q}_\ell \rightsquigarrow L=\mathbb{Q}_\ell(\mu_\ell)$)

Define also $H^1_s(K,T) = H^1(K,T)/H^1_{un}(K,T)$.

<u>Lemma</u>: if T is unramified as a $\mathcal{G}_K$-module. Then

$$H^1_f(K,T) = T/(\mathrm{Fr}-1)T$$

$$H^1_s(K,T) \cong \mathrm{Hom}(I_K, T^{\mathrm{Fr}=1})$$

Moreover, if $|\mathbb{F}^\times|\cdot R = 0$, then $H^1_s(K,T) = T^{\mathrm{Fr}=1}$.

(in general, $H^1_s(K,T) \otimes \mathbb{F}^\times = T^{\mathrm{Fr}=1}$)

Assume that $H^1_s \otimes \mathbb{F}^\times = T^{Fr=1}$ ~~and~~ then:

* $\det((1-Fr)|T) = 0$. $P(x) = \det(1-Fr\cdot x|T) = (1-x)Q(x)$.

$$\begin{tikzcd}
\rightsquigarrow \phi^{fs} : T/(Fr-1)T \arrow[r, "Q(Fr^{-1})"] \arrow[d, phantom, "\|"] & T^{Fr=1} \arrow[d, phantom, "\|"] \\
H^1_f & H^1_s \otimes \mathbb{F}^\times
\end{tikzcd}$$

If $T/(Fr-1)T$ is free of rk 1 over R, then ϕ^{fs} is an isomorphism.

Let $\mathcal{F}$ be a family of local conditions, $\mathcal{F}_v \subset H^1(\mathbb{Q}_v, T)$.

st $\underbrace{\forall' v}_{\text{almost all } v}$, $\mathcal{F}_v = H^1_{ur}(\mathbb{Q}_v, T)$.

$H^1_{\mathcal{F}}(\mathbb{Q}, T) = \{c \in H^1(\mathbb{Q}, T) : c_v \in \mathcal{F}_v \ \forall v\}$.

<u>Dual Selmer conditions:</u>

$T^* = \mathrm{Hom}(T, \mathbb{Q}_p/\mathbb{Z}_p(1))$. ~~Then $H^1(K,T)$~~

Then have $H^1(K,T) \times H^1(K,T^*) \to H^2(K, \mathbb{Q}_p/\mathbb{Z}_p(1)) \overset{\text{canonical}}{\cong} \mathbb{Q}_p/\mathbb{Z}_p$

So given $\mathcal{F}_v \subset H^1(K,T)$, get $\mathcal{F}_v^* := \mathcal{F}_v^\perp$.

$\longrightarrow$ Fix a selmer condition $\mathcal{F}$.

Let $\mathcal{L} = \{\ell :$ • T unramified at ℓ $\qquad R = \mathbb{Z}/p^k\mathbb{Z}$

• $\ell \equiv 1 \bmod p^k$ (or $|\mathbb{F}_\ell^\times| R = 0$)

• $\det(1 - Fr_\ell) = 0$ $\quad (Fr_\ell = Frob_\ell)$

• $\mathcal{F}_\ell = H^1_{ur}(\mathbb{Q}_\ell, T)$ $\}$.

Fact: if $\ell \in \mathcal{L}$ then there is a splitting

$$H^1(\mathbb{Q}_\ell, T) = H^1_f(\mathbb{Q}_\ell, T) \oplus H^1_{tr}(\mathbb{Q}_\ell, T)$$

Define the sheaf $\mathcal{H}$ on X as:

$$\mathcal{H}(1) = H^1_{\mathcal{F}}(\mathbb{Q}, T).$$

$$n \in \mathcal{N} = \mathcal{N}(\mathcal{L}) \Rightarrow \mathcal{H}(n) = H^1_{\mathcal{F}(n)}(\mathbb{Q}, T) \otimes \mathcal{G}_n, \quad \mathcal{F}(n)_v = \begin{cases} \mathcal{F}_v & \text{if } v \nmid n \\ H^1_{tr}(\mathbb{Q}_\ell, T) & v = \ell \mid n. \end{cases}$$

(where $\mathcal{G}_n = \bigotimes_{\ell | n} \underbrace{\mathbb{F}_\ell^\times}_{\cong \mathrm{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q})}$).

Rmk: in literature, often use: $\mathcal{F}(n)_v = H^1_{lax}(\mathbb{Q}_v, T)$ for each $v | n$.

This is enough to bound Selmer groups, but theory in general is "less rigid" (see later) ← these can be called "weak Kolyvagin systems".

Define also:

$$\mathcal{H}(\overset{n}{\bullet} \overset{e}{\rule[0.5ex]{2em}{0.4pt}} \overset{n\ell}{\bullet}) = H^1_{tr}(\mathbb{Q}_\ell, T).$$

$$\begin{tikzcd}
H^1_{\mathcal{F}(n)}(\mathbb{Q},T) \arrow[r, phantom, "="] \arrow[d, "\mathrm{loc}_\ell"'] \arrow[drr] & \mathcal{H}(n) \arrow[dr] & & \mathcal{H}(n\ell) \arrow[dl] \arrow[r, phantom, "="] & H^1_{\mathcal{F}(n\ell)}(\mathbb{Q},T) \arrow[dl, "\mathrm{loc}_\ell"] \\
H^1_{ur}(\mathbb{Q},T) \arrow[rr, "\phi^{fs}"'] & & \mathcal{H}(\ell) \arrow[r, phantom, "="] & H^1_{tr}(\mathbb{Q}_\ell,T) &
\end{tikzcd}$$

Def: A (strong) Kolyvagin $\kappa \in KS(T)$ is a global section of $\mathcal{H}$.

i.e. $\kappa_n \in H^1_{\mathcal{F}(n)}(\mathbb{Q}, T)$

$$(\kappa_{n\ell})_\ell = \phi^{fs}((\kappa_n)_\ell)$$

③

Examples:

- κ_n = derivative classes of cyclotomic units.
- derivative classes of Heegner points (see Howard, "The Heegner point Kolyvagin system").
- Kato's Euler system.

an abelian extension of $\mathbb{Q}$.

Def: An Euler system for $(T, \mathcal{F}, K)$ is a collection

$$c_F \in H^1(F,T) \quad \forall\ \mathbb{Q} \underset{\text{finite}}{\subseteq} F \subset K$$

s.t. $$N_{F'/F}\, c_{F'} = \prod_{\ell} P_\ell(\mathrm{Fr}_\ell^{-1}) \cdot c_F$$

Theorem ("K-S, appendix A"): Under reasonable conditions, given an Euler system E for T, can construct a Kolyvagin system κ for T such that $\kappa_1 = c_{\mathbb{Q}}$.

Def: The order of vanishing of $\kappa \in KS(T)$ is $\overset{\mathrm{ord}(\kappa)}{``\min}\{\overset{\#\text{ of prime factors}}{\omega(n)} : ~~\kappa_n~~\ \kappa_n \neq 0\}$

Def: Module of L-values for $T = \{\kappa_1 : \kappa \in KS(T)\} \subseteq \mathcal{H}(1) = \mathrm{Sel}(T)$.

Goal: relate $\mathrm{ord}(\kappa) \leftrightarrow \mathrm{corank}\ H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*)$.

(eg: $T = \mu_{p^k} \otimes \chi^{-1} \rightsquigarrow$ study $\mathcal{C}\ell(\mathbb{Q}(\mu_p))^{\chi}[p^k]$.).

Goal': relate Fitting ideals of $\dfrac{H^1_{\mathcal{F}}(\mathbb{Q},T)}{\mathcal{L}(T)} \leftrightarrow H^1_{\mathcal{F}^*}(\mathbb{Q},T^*)$.

• Hypotheses on T

(H0) T free of finite rank $/R$.

(H1) $\overline{T} := T/pT$ is absolutely irreducible as an $\mathbb{F}_p[\mathcal{G}_{\mathbb{Q}}]$-module.

(H2) $\exists\, \tau \in \mathcal{G}_{\mathbb{Q}}$ s.t. $\tau = 1$ on μ_{p^∞} and $T/(\tau-1)T$ is free of rk-1.

(H3) $H^1(\mathbb{Q}(T, \mu_{p^\infty})/\mathbb{Q}, \overline{T}) = H^1(\mathbb{Q}(T, \mu_{p^\infty})/\mathbb{Q}, T^*[p]) = 0.$

(H4) $p \geqslant 5$

(H6) $\forall \ell \in \overline{\Sigma(\mathcal{F})}$ ← ramification, the local condition at ℓ is "cartesian" ← behaves well under taking quotients of T.

Under (H0)-(H6), we have that

$H^1_f(\mathbb{Q}_\ell, T)$, $H^1_f(\mathbb{Q}_\ell, T^*)$, $H^1_s(\mathbb{Q}_\ell, T)$, $H^1_s(\mathbb{Q}_\ell, T^*)$ are all free of rank 1 over $R = \mathbb{Z}/p^k\mathbb{Z}$ $(\forall \ell \in \mathcal{L})$.

Let $\overline{R} = \mathbb{Z}/p$, $\overline{T} = T \otimes \overline{R}$, $\overline{T}^* = T^*[p]$.

Def:

$$\lambda(n, T) = \text{length}_R\, H^1_{\mathcal{F}(n)}(\mathbb{Q}, T) = \text{length}_R\, \mathcal{H}(n).$$

$$\lambda(n, T^*) = \text{length}_R\, H^1_{\mathcal{F}(n)^*}(\mathbb{Q}, T^*).$$

Prop:

1) $n \in \mathcal{N} \Rightarrow \lambda(n, \overline{T}) = 0 \Leftrightarrow \lambda(n, T) = 0$

2) $\lambda(n, T) - \lambda(n, T^*)$ is independent of n.

Pf-sketch:

1) $H^1_{\mathcal{F}(n)}(\mathbb{Q}, \overline{T}) = H^1_{\mathcal{F}(n)}(\mathbb{Q}, T) \otimes \mathbb{Z}/p$ ✓.

2) Local Galois cohomology calculation.

Theorem: $\exists\ r, s \geq 0$ and one of which is 0, s.t

$$\forall n,\ H^1_{\mathcal{F}(n)}(\mathbb{Q},T) \oplus R^r \underset{\substack{\uparrow \\ \text{non-canonical}}}{\cong} H^1_{\mathcal{F}(n)^*}(\mathbb{Q},T^*) \oplus R^s$$

Pf-Sketch:

Up to isomorphism, R-module M is determined by $i \mapsto \text{length } M[p^i]$

$\Rightarrow$ Suffices to show $\text{length } H^1_{\mathcal{F}(n)}(\mathbb{Q},T)[p^i] - \text{length}_R\, H^1_{\mathcal{F}(n)^*}(\mathbb{Q},T^*)[p^i] = i \cdot t$

which can be done by Galois Coh + (H6). ∎

Def: if $n \in \mathcal{N}$ and either $\lambda(n,T) = 0$ or $\lambda(n,T^*) = 0$,

we say that n is a core vertex.

← follows from previous Thm.

$H^1_{\mathcal{F}(n)^*}(\mathbb{Q},T^*)$

Fact: if n is a core vertex, then $\mathcal{H}(n)$, $\mathcal{H}^*(n)$ are free$/R$, the rank (as n varies over core vertices) is independent of n, and one of them is 0.

$\chi(T) := \text{rk } \mathcal{H}(n)$ for any core vertex n.

↑ Core Selmer rank

$\chi(T^*) = \text{rk } \mathcal{H}^*(n)$.

Fact:

- $\chi(T) = 0 \Rightarrow KS(T) = 0$
- $\chi(T) = 1 \Rightarrow KS(T) =$ free of rk $1/R$.
- $\chi(T) \geq 2 \Rightarrow KS(T)$ contains a free R-module of rk d $\forall d \geq 0$.

- **The stab subsheaf $\mathcal{H}'$.**

$$\mathcal{H}'(n) = p^{\lambda(n,T^*)}\mathcal{H}(n) = p^{\lambda(n,T^*)}\mathcal{H}'_{F(n)}(T) \otimes \mathcal{G}_n \subseteq \mathcal{H}(n)$$

$\mathcal{H}'(n \xrightarrow{e} n\ell)$ = image of $\mathcal{H}'(n)$ in $\mathcal{H}(e)$

(in particular, $\mathcal{H}'(n) \twoheadrightarrow \mathcal{H}'(n \text{---} n\ell)$ is surjective).

If $n \in \mathcal{N}$, we have: $\mathcal{H}'(n) = 0$ if $\lambda(n,T^*) \geq k$.

In general, $\mathcal{H}'(n)$ is free of rank $\chi(T)$ over $\mathbb{Z}/p^{k-\lambda(n,T^*)}\mathbb{Z}$

If $x \in \mathcal{H}'(n)$, then $x \in p^{k-\mathrm{length}(Rx)}\mathcal{H}(n)$.

Theorem (App. B of "K-S"). global sections

1) $\forall n$, $\Gamma(\mathcal{H}') \twoheadrightarrow \mathcal{H}'(n)$.

2) if $\chi(T) = 1$, then $\Gamma(\mathcal{H}') \cong$ free R-submodule of rk 1.

3) if $\chi(T) > 1$, then $\Gamma(\mathcal{H}') \supseteq$ free R-submodule of rk d, $\forall d \geq 0$.

The proof takes some work, - one needs to study $X_0 \subset X$ made of core vertices and some suitable edges, and prove that it is connected.

—·—

For $T = \mu_{p^k} \otimes \eta^{-1}$, $\eta \neq$ id, Teichmüller, then $\chi(T) = \begin{cases} 1 & \eta \text{ even} \\ 0 & \eta \text{ odd} \end{cases}$

Thm: Suppose either of $\begin{cases} \cdot\ \chi(T) = 1 \\ \cdot\ k = 1 \ (R = \text{field } \mathbb{F}_p) \\ \cdot\ \ldots \end{cases}$ Then

$\Gamma(\mathcal{H}') \subset \Gamma(\mathcal{H}) = KS(T)$ is an equality.

(ie $\kappa \in KS(T)$ is ~~at~~ $\kappa_n \in \mathcal{H}'(n)$).