Fermat’s Last Theorem
Math 847 - March 21, 2013

Set-Up: Start with continuous $\overline{\rho} : G_{\mathbb{Q}} \to GL_2(F)$ with $F$ a finite field of characteristic $l > 2$, $\overline{\rho}$ absolutely irreducible and semistable, and $\Sigma$ a finite set of rational primes. Consider the bijection

$$H^1(G_{\mathbb{Q}}, Ad(\overline{\rho})) \leftrightarrow \{\text{Deformations of } \overline{\rho} \text{ to } F[c]\}.$$ 

Let $H^1_{\Sigma}(G_{\mathbb{Q}}, Ad(\overline{\rho}))$ be the subset of $H^1(G_{\mathbb{Q}}, Ad(\overline{\rho}))$ corresponding to the deformations of type $\Sigma$.

Recall that $Ad(\overline{\rho})$ is the set of $2 \times 2$ matrices over $F$ with $G_{\mathbb{Q}}$ action via conjugation by $\overline{\rho}(g) \in GL_2(F)$.

---

How big is $H^1_{\Sigma}(G_{\mathbb{Q}}, Ad(\overline{\rho}))$?

Note, given a homomorphism $H \to G$ we have a map $H^1(G, M) \to H^1(H, M)$ for all $M$. Interested in:

$$H^1(G_{\mathbb{Q}}, Ad(\overline{\rho})) \to H^1(G_{\mathbb{Q}_p}, Ad(\overline{\rho})).$$

Recall, from last time, for type $\Sigma$, property 1: for any lift $\sigma$, $\det(\sigma) = \chi$, the cyclotomic character, implies that $H^1_{1}(G_{\mathbb{Q}}, Ad(\overline{\rho})) \subseteq H^1(G_{\mathbb{Q}}, Ad^0(\overline{\rho}))$ where $Ad^0$ only includes trace 0 matrices.

Definition: By local conditions we mean a collection $L = \{L_p\}$ of subgroups, indexed by primes $p$, $L_p \subseteq H^1(G_{\mathbb{Q}_p}, Ad(\overline{\rho}))$ such that for all but finitely many primes $p$ we have

$$L_p = \ker(H^1(G_{\mathbb{Q}_p}, Ad^0(\overline{\rho})) \to H^1(I_p, Ad^0(\overline{\rho}))).$$

- $\ker(H^1(G_{\mathbb{Q}_p}, Ad^0(\overline{\rho})) \to H^1(I_p, Ad^0(\overline{\rho})))$ is called $H^1_{ur}(G_{\mathbb{Q}_p}, Ad^0(\overline{\rho}))$.
- $H^1_{L}(G_{\mathbb{Q}}, Ad^0(\overline{\rho})) = \{\mathfrak{c} \in H^1(G_{\mathbb{Q}}, Ad^0(\overline{\rho})) \mid res(\mathfrak{c}_p) \in L_p \forall p\}$.

These are generalized Selmer groups.

Note: Consider what $res(c_p) \in H^1_{ur}(G_{\mathbb{Q}_p}, Ad^0(\overline{\rho}))$ means in terms of the corresponding lift. Recall $\sigma(g) = (1 + \epsilon a(g))\overline{\rho}(g)$. To say $a|_{I_p} = 0$ is to say $\sigma|_{I_p} = \overline{\rho}|_{I_p}$. For $p \notin \Sigma$, want $\overline{\rho}$ unramified at $p$ implies $\sigma$ unramified at $p$. This captures that!

Note: $\infty$ is prime! $\mathbb{Q}_{\infty} = \mathbb{R}$. $G_{\mathbb{Q}_{\infty}} = Gal(\mathbb{C}/\mathbb{R}) \hookrightarrow G_{\mathbb{Q}}$. What is $H^1(G_{\mathbb{Q}_{\infty}}, Ad^0(\overline{\rho}))$?

Exercise: If $G$ and $M$ have finite coprime orders, then $H^1(G, M) = 0$.

Since $\text{char } F > 2$, $H^1(G_{\mathbb{Q}_{\infty}}, Ad^0(\overline{\rho})) = 0$. So no condition at $\infty$. ($L_{\infty}$ has to be 0, no choice).

Theorem $H^1_L(G_{\mathbb{Q}}, Ad^0(\overline{\rho})) = H^1_L(G_{\mathbb{Q}}, Ad^0(\overline{\rho}))$ where

- $L_p = H^1_{ur}(G_{\mathbb{Q}_p}, Ad^0(\overline{\rho}))$ if $p \notin \Sigma \cup \{l\}$
- $L_p = H^1(G_{\mathbb{Q}}, Ad^0(\overline{\rho}))$ if $p \in \Sigma$ and $p \neq l$
- $L_p = H^1_l(G_{\mathbb{Q}_l}, Ad^0(\overline{\rho}))$ if $p = l \notin \Sigma$
- $L_p = H^1_{ss}(G_{\mathbb{Q}_l}, Ad^0(\overline{\rho}))$ if $p = l \in \Sigma$


**Definition:** Given $\overline{\rho} : G \to GL_n(F)$, let $V = F^n$, an $F[G]$–module, and consider all extensions $E$ of $V$ by $V$, i.e. short exact sequences of $F[G]$-modules

$$0 \to V \overset{\alpha}{\to} E \overset{\beta}{\to} V \to 0.$$ 

We consider two short exact sequences equivalent if there exists an isomorphism $E_1 \to E_2$ such that the diagram

$$\begin{array}{ccc}
0 & \to & V \\
\downarrow{id} & & \downarrow{id} \\
0 & \to & V
\end{array} \begin{array}{ccc}
\to & V_1 & \to & V_1 \\
\to & \to & \to & \to \\
\to & V_2 & \to & 0
\end{array}$$ 

commutes. Let $\text{Ext}_{F[G]}(V,V)$ denote the set of equivalence classes.

**Theorem** There is a bijection $\text{Ext}(V,V) \leftrightarrow H^1(G, \text{Ad}(\overline{\rho}))$.

**Proof** Pick $\phi : V \to E$, such that $\beta(\phi(m)) = m$, for all $m \in V$. Given $g \in G$, define $T_g : V \to V$ by $m \mapsto \alpha^{-1}(g\phi(g^{-1}m) - g(m))$. Check that $T_g = T_{gh} = T_g + gT_h$. So $(g \mapsto T_g)$ is a cocycle and thus is in $Z^1(G, \text{Ad}(\overline{\rho}))$. Check that equivalent extensions correspond to cocycles differing by a boundary. □

**Recall:** An $F[G]$–module $V$ of finite size is \text{good} if there is a finite flat group scheme $H$ over $\mathbb{Z}_l$ such that $H(\overline{\mathbb{Q}_l}) \cong V$ as $F[G_{\mathbb{Q}_l}]$–modules. Recall that $V$ is \text{ordinary} if there exists a short exact sequence $0 \to V^{-1} \to V \to V^0 \to 0$ of $F[G]$–modules such that $I_l$ acts trivially on $V^0$ and via cyclotomic on $V^{-1}$. $V$ is \text{semistable} if it is good or ordinary.

**Definition:** Consider the bijection $H^1(G_{\mathbb{Q}_l}, \text{Ad}(\overline{\rho})) \leftrightarrow \text{Ext}_{F[G_{\mathbb{Q}_l}]}(V,V)$.

- Define $H^1_{ss}(G_{\mathbb{Q}_l}, \text{Ad}(\overline{\rho}))$ to be the subset of $H^1(G_{\mathbb{Q}_l}, \text{Ad}(\overline{\rho}))$ corresponding to semistable extensions.
- Define $H^1_f(G_{\mathbb{Q}_l}, \text{Ad}(\overline{\rho}))$ to be the subset of $H^1(G_{\mathbb{Q}_l}, \text{Ad}(\overline{\rho}))$ corresponding to extensions that are good if $\overline{\rho}$ is good at $l$ or semistable if $\overline{\rho}$ is not good at $l$, $(H^1_f = H^1_{ss})$.
- Likewise define $H^1_f(G_{\mathbb{Q}_l}, \text{Ad}^0(\overline{\rho}))$ and $H^1_{ss}(G_{\mathbb{Q}_l}, \text{Ad}^0(\overline{\rho}))$ by intersecting these subspaces with $H^1(G_{\mathbb{Q}_l}, \text{Ad}^0(\overline{\rho}))$.

**Goal:** Need to find a formula for $|H^1_{\text{ur}}(G_{\mathbb{Q}_p}, \text{Ad}^0(\overline{\rho}))|$.

**Inflation Restriction Sequence:** If $M$ is a $G$–module, $H \triangleleft G$ then $M^H = \{m \in M \mid hm = m \forall h \in H\}$ is a $G/H$-module and there exists an exact sequence

$$0 \to H^1(G/H, M^H) \overset{\text{Inf}}{\to} H^1(G, M) \overset{\text{Res}}{\to} H^1(H, M).$$

**Theorem** $|H^1_{\text{ur}}(G_{\mathbb{Q}_p}, \text{Ad}^0(\overline{\rho}))| = |H^0(G_{\mathbb{Q}_p}, \text{Ad}^0(\overline{\rho}))| = |\text{Ad}^0(\overline{\rho})|^{|G_{\mathbb{Q}_p}|}$
Proof: Let \( M = \text{Ad}^0(\mathfrak{p}) \). Consider the exact sequence

\[
0 \to M^G_{\mathbb{Q}_p} \to M^I_{\mathbb{Q}_p} \xrightarrow{\text{Fr}_p^{-1}} M^I_p \xrightarrow{(\text{Frob}_p - 1)M^I_p} 0.
\]

Exercise: If \( G \) is procyclic, and \( M \) is a finite \( G \)-module, then \( H^1(G, M) = M/(g - 1)M \) where \( g \) is a generator.

Hint: Given \( m \in M \) define \( f : G \to M \) by \( f(g^i) = m + gm + g^2m + \cdots + g^{i-1}m \).

\[
H^1(G_{\mathbb{Q}_p}/I_p, M^I_p) = H^1(\langle \text{Frob}_p \rangle, M^I_p) = \frac{M^I_p}{(\text{Frob}_p - 1)M^I_p}.
\]

By alternating-product-orders for exact sequences we have that \( |M^G_{\mathbb{Q}_p}| \cdot |M^I_p| = |M^I_p| \cdot |M^I_p| \cdot \prod_{p < \infty} |L^*| \cdot |L_p| \cdot |H^0(G_{\mathbb{Q}_p}, M)|^\cdot.
\]

Theorem (Wiles) Let \( \mathcal{L} \) be local conditions, \( \mathcal{L}^* = \{L^*_p\} \) where \( L^*_p \subseteq H^1(G_{\mathbb{Q}_p}, M^*) \) is the annihilator of \( L_p \) under Tate’s pairing. Then

\[
\frac{|H^1_{\mathcal{L}}(G_{\mathbb{Q}}, M)|}{|H^0_{\mathcal{L}}(G_{\mathbb{Q}}, M)|} = \frac{|H^0(G_{\mathbb{Q}}, M)|}{|H^0(G_{\mathbb{Q}}, M^*)|} \prod_{p < \infty} \frac{|L_p|}{|H^0(G_{\mathbb{Q}_p}, M)|}.\]