

Introduction to Galois Cohomology

Seyfi Türkelli

September 1, 2008

The Big Picture. In the previous chapter, we saw that given a semistable, absolutely irreducible $\bar{\rho}$ and a finite set of primes Σ , there is a universal lift $\xi_{\Sigma} : G_{\mathbb{Q}} \rightarrow GL_2(\mathfrak{K}_{\Sigma})$ which parametrizes all lifts of $\bar{\rho}$ that are semistable at ℓ and that have no worse ramification at $p \notin \Sigma$ than $\bar{\rho}$ has. A very rough idea of how big \mathfrak{K}_{Σ} is, can be given by the dimension of its tangent space. In chapter 10, we shall shortly describe a universal lift of $\bar{\rho}$ of type Σ parametrizing those lifts associated to modular forms and describe a useful invariant for measuring how large that representing ring is. In chapter 9, some commutative algebra will establish how an inequality between these two invariants suffices for showing that the two universal lifts (type Σ and modular of type Σ) coincide. First, we need to describe how to compute the tangential dimension of \mathfrak{K}_{Σ} in terms of Galois cohomology.

A good introductory text for this chapter is [?]. For more advanced material, see [?].

In this chapter, G will stand for a profinite group. Homomorphisms will be continuous and by a subgroup, we will mean a closed subgroup.

1 Lifts and Galois Cohomology

Fix a homomorphism $\bar{\rho} : G \rightarrow GL_n(F)$. Consider the possible lifts σ of $\bar{\rho}$ to $GL_n(F[\epsilon])$. In particular, there is the trivial lift, which we shall also denote $\bar{\rho}$, arising from the embedding $F \rightarrow F[\epsilon]$. Then $\sigma(g) = (1 + \epsilon a(g))\bar{\rho}(g)$ for some map $a : G \rightarrow M_n(F)$. The fact that σ is a group homomorphism, i.e. $\sigma(gh) = \sigma(g)\sigma(h)$, translates into $a(gh) = a(g) + \bar{\rho}(g)a(h)\bar{\rho}(g)^{-1}$.

Definition 1. Let M be a G -module equipped with discrete topology where the action of G is continuous. Set $H^0(G, M) := M^G$ where

$$M^G := \{m \in M \mid gm = m \text{ for all } g \in G\}.$$

A 1-cocycle is a continuous map $f : G \rightarrow M$ such that $f(gh) = f(g) + gf(h)$ for all $g, h \in G$. A 1-coboundary is a continuous map $f : G \rightarrow M$ given by $f(g) = gx - x$ for some fixed $x \in M$. The 1-cocycles form an abelian group and 1-coboundaries form a subgroup and we denote the quotient group by $H^1(G, M)$.

Note that $GL_n(F)$ acts on $M_n(F)$ by conjugation (the *adjoint* action). Thus, the map $\bar{\rho}$ makes $M_n(F)$ into a G -module, to be denoted $\text{Ad}(\bar{\rho})$. As noted in the first paragraph above, every lift of $\bar{\rho}$ to $F[\epsilon]$ produces a 1-cocycle. One checks that if two lifts are strictly equivalent, then their 1-cocycles differ by a 1-coboundary. This yields a map from $E(F[\epsilon])$ (deformations to the dual numbers) to $H^1(G, \text{Ad}(\bar{\rho}))$. Conversely, given a 1-cocycle $a : G \rightarrow \text{Ad}(\bar{\rho})$, defining $\sigma(g) = (1 + \epsilon a(g))\bar{\rho}(g)$ gives a lift of $\bar{\rho}$ to $F[\epsilon]$. In this way, we get a bijection, actually an F -vector space isomorphism

$$E(F[\epsilon]) \cong H^1(G, \text{Ad}(\bar{\rho})).$$

If X is a property on the set of deformations of $\bar{\rho}$ which is closed under quotient, sub and direct product, then set of deformations of $\bar{\rho}$ that have X corresponds to some subgroup of $H^1(G, \text{Ad}(\bar{\rho}))$ which we denote $H_X^1(G, \text{Ad}(\bar{\rho}))$. In particular, if we start with a semistable, absolutely irreducible representation $\bar{\rho} : G_{\mathbb{Q}} \rightarrow GL_2(F)$ (F of odd characteristic ℓ) and consider lifts of type Σ , then the subgroup will be denoted by $H_{\Sigma}^1(G_{\mathbb{Q}}, \text{Ad}(\bar{\rho}))$. In summary, we have:

Proposition 2. *There exists an isomorphism between F -vector spaces*

$$E_{\Sigma}(F[\epsilon]) \cong H_{\Sigma}^1(G, \text{Ad}(\bar{\rho})).$$

In particular, the universal deformation ring \mathfrak{R}_{Σ} is generated by $\dim H_{\Sigma}^1(G, \text{Ad}(\bar{\rho}))$ many elements as a $W(F)$ -algebra.

We want to identify this set by considering what sort of 1-cocycles correspond to the properties involved in being of type Σ .

First, we impose the condition that the lift σ should have determinant the cyclotomic character χ , which is the same as the determinant of $\bar{\rho}$. Then $\det(1 + \epsilon a(g)) = 1$ for all $g \in G_{\mathbb{Q}}$. Since

$$1 + \epsilon a(g) = \begin{pmatrix} 1 + \epsilon a_{11} & \epsilon a_{12} \\ \epsilon a_{21} & 1 + \epsilon a_{22} \end{pmatrix},$$

and $\epsilon^2 = 0$, this gives $1 + \epsilon(a_{11} + a_{22}) = 1$, implying $\text{trace}(a(g)) = 0$. The $G_{\mathbb{Q}}$ -submodule of $\text{Ad}(\bar{\rho})$ consisting of trace 0 matrices will be denoted $\text{Ad}^0(\bar{\rho})$. We are therefore only interested in subgroups of $H^1(G_{\mathbb{Q}}, \text{Ad}^0(\bar{\rho}))$.

Second, we want to control local behaviour of the lifts. More precisely, if H is a subgroup of G and M a G -module, then we can restrict 1-cocycles and 1-coboundaries from G to H , thus producing a restriction map

$$\text{res} : H^1(G, M) \rightarrow H^1(H, M).$$

More generally, any homomorphism $H \rightarrow G$ will produce such a restriction map. The local behavior corresponding to type Σ will be captured by restrictions from $G_{\mathbb{Q}}$ to $G_{\mathbb{Q}_p}$ or I_p . For example, suppose a lift σ corresponds to an element of the kernel from $H^1(G_{\mathbb{Q}}, \text{Ad}^0(\bar{\rho})) \rightarrow H^1(I_p, \text{Ad}^0(\bar{\rho}))$. Then $\sigma(g) = \bar{\rho}(g)$ for all $g \in I_p$, so that σ is unramified at p if and only if $\bar{\rho}$ is unramified at p . Being in the kernel in fact ensures that the ramification at p of σ is no worse than that of $\bar{\rho}$.

Definition 3. By local conditions we mean a collection $\mathcal{L} = \{L_p\}$ of subgroups $L_p \leq H^1(G_{\mathbb{Q}_p}, \text{Ad}^0(\bar{\rho}))$ for each prime p (including infinity) such that for all but finitely many p , $L_p = H_{ur}^1(G_{\mathbb{Q}_p}, \text{Ad}^0(\bar{\rho}))$ where

$$H_{ur}^1(G_{\mathbb{Q}_p}, \text{Ad}^0(\bar{\rho})) = \ker(H^1(G_{\mathbb{Q}_p}, \text{Ad}^0(\bar{\rho})) \rightarrow H^1(I_p, \text{Ad}^0(\bar{\rho})))$$

is the subspace of unramified classes. The corresponding Selmer group is

$$H_{\mathcal{L}}^1(G_{\mathbb{Q}}, \text{Ad}^0(\bar{\rho})) = \{c \in H^1(G_{\mathbb{Q}}, \text{Ad}^0(\bar{\rho})) : \text{res}_p(c) \in L_p \text{ for all } p\}$$

where $\text{res}_p : H^1(G_{\mathbb{Q}}, \text{Ad}^0(\bar{\rho})) \rightarrow H^1(G_{\mathbb{Q}_p}, \text{Ad}^0(\bar{\rho}))$ is the restriction.

Note that by \mathbb{Q}_{∞} , we mean the real numbers, and so $G_{\mathbb{Q}_{\infty}} = \text{Gal}(\mathbb{C}/\mathbb{R})$ of order 2, identified as the subgroup of order 2 of $G_{\mathbb{Q}}$ generated by complex conjugation defined up to conjugation. Since F has odd characteristic, $H^1(G_{\mathbb{Q}_{\infty}}, \text{Ad}^0(\bar{\rho})) = \{0\}$ by the following, and so $L_{\infty} = \{0\}$.

Lemma 4. Suppose G has order 2 and M is a G -module of odd order. Then, $H^1(G, M) = \{0\}$.

Proof. Let $G = \{1, c\}$. A 1-cocycle is a map $f : G \rightarrow M$ such that $f(gh) = f(g) + gf(h)$ for $g, h \in G$. Setting $g = 1$ gives $f(1) = 0$. Setting $g = h = c$ gives $0 = f(c) + cf(c)$. So $f(c) \in M^- := \{m \in M \mid cm = -m\}$. Note also that if $m \in M^-$, defining f by $f(1) = 0, f(c) = m$ gives a 1-cocycle.

We want to show that f is a coboundary i.e. $f(g) = gx - x$ for some fixed $x \in M$. Let $m = f(c)$. Since M has odd order, we can take $x = -\frac{m}{2}$ and complete the proof. □

Theorem 5. $H_{\Sigma}^1(G_{\mathbb{Q}}, \text{Ad}(\bar{\rho})) = H_{\mathcal{L}}^1(G_{\mathbb{Q}}, \text{Ad}^0(\bar{\rho}))$ where local conditions \mathcal{L} is given by:

$$\begin{aligned} L_{\infty} &= 0, \\ L_p &= H_{ur}^1(G_{\mathbb{Q}_p}, \text{Ad}^0(\bar{\rho})) \text{ if } p \notin \Sigma \cup \{\ell\}, \\ &= H^1(G_{\mathbb{Q}_p}, \text{Ad}^0(\bar{\rho})) \text{ if } p \in \Sigma, p \neq \ell, \\ &= H_f^1(G_{\mathbb{Q}_p}, \text{Ad}^0(\bar{\rho})) \text{ if } p = \ell \notin \Sigma, \\ &= H_{ss}^1(G_{\mathbb{Q}_p}, \text{Ad}^0(\bar{\rho})) \text{ if } p = \ell \in \Sigma. \end{aligned}$$

Here, H_f^1 and H_{ss}^1 are the flat and semistable cohomology groups respectively, to be defined below.

This theorem is simply a restatement of what it means for a lift to be of type Σ - all we do is translate the conditions across to cohomology. Our main aim will be to compute the size of this Selmer group, giving the tangential dimension of \mathfrak{R}_{Σ} . First, since the property of $\bar{\rho}$ being good or ordinary is defined in terms of the $G_{\mathbb{Q}}$ -module F^2 , we need another interpretation of $H^1(G, \text{Ad}(\bar{\rho}))$.

Definition 6. Given $\bar{\rho} : G \rightarrow GL_n(F)$, consider $V = F^n$, a G -module via $\bar{\rho}$, and consider the set of extensions E of V by V , consisting of short exact sequences

$$0 \rightarrow V \xrightarrow{\alpha} E \xrightarrow{\beta} V \rightarrow 0$$

of $F[G]$ -modules. Call two such extensions equivalent if there is an isomorphism $i : E_1 \rightarrow E_2$ making the following diagram commute

$$\begin{array}{ccccccccc} 0 & \longrightarrow & V & \longrightarrow & E_1 & \longrightarrow & V & \longrightarrow & 0 \\ & & \downarrow 1_V & & \downarrow i & & \downarrow 1_V & & \\ 0 & \longrightarrow & V & \longrightarrow & E_2 & \longrightarrow & V & \longrightarrow & 0 \end{array}$$

Let $\text{Ext}_{F[G]}^1(V, V)$ denote the set of equivalence classes.

Theorem 7. *There is a bijection between $H^1(G, \text{Ad}(\bar{\rho}))$ and $\text{Ext}_{F[G]}^1(V, V)$.*

Proof. Pick a linear map $\phi : V \rightarrow E$ such that $\beta(\phi(m)) = m$ for all $m \in V$. Given $g \in G$, define $T_g : V \rightarrow V$ by

$$m \mapsto \alpha^{-1}(g\phi(g^{-1}m) - \phi(m)).$$

T_g can be considered as an n by n matrix. One checks that $T_{gh} = T_g + gT_h$, where gT_h means the matrix T_h conjugated by $\bar{\rho}(g)$. One also checks that equivalent extensions correspond to 1-cocycles that differ by a 1-coboundary.

Conversely, given a cocycle $T : G \rightarrow \text{Ad}(\bar{\rho})$, $g \mapsto T_g$, one defines a G -module structure on $E := V \times_T V$ by $g.(v, m) := (gv + T_g(gm), gm)$. One can easily show that these constructions are inverse to each other. \square

Definition 8. *Identify $H^1(G_{\mathbb{Q}_\ell}, \text{Ad}(\bar{\rho}))$ with $\text{Ext}_{F[G_{\mathbb{Q}_\ell}]}^1(V, V)$. Let $H_{ss}^1(G_{\mathbb{Q}_\ell}, \text{Ad}(\bar{\rho}))$ consist of those extensions of V by V that are semistable as an $F[G_{\mathbb{Q}_\ell}]$ -module. If $\bar{\rho}$ is not good at ℓ , take $H_f^1(G_{\mathbb{Q}_\ell}, \text{Ad}(\bar{\rho}))$ to be H_{ss}^1 . If $\bar{\rho}$ is good at ℓ , take $H_f^1(G_{\mathbb{Q}_\ell}, \text{Ad}(\bar{\rho}))$ to consist of those extensions of V by V that are good. $H_{ss}^1(G_{\mathbb{Q}_\ell}, \text{Ad}^0(\bar{\rho}))$ and $H_f^1(G_{\mathbb{Q}_\ell}, \text{Ad}^0(\bar{\rho}))$ are defined by intersecting the above subgroups with $H^1(G_{\mathbb{Q}_\ell}, \text{Ad}^0(\bar{\rho}))$.*

Note that we know that $H_{\mathcal{L}}^1(G_{\mathbb{Q}}, \text{Ad}^0(\bar{\rho}))$ is a finite group since its dimension over F is the tangential dimension of \mathfrak{R}_{Σ} which is finite.

2 Wiles' Formula on Selmer Groups

If H is a normal subgroup of G , then M^H is a G/H -module and we have a map, called *inflation*,

$$\text{inf} : H^1(G/H, M^H) \rightarrow H^1(G, M)$$

defined by $\text{inf}(f)(g) := f(gH)$ for all $g \in G$.

The next theorem identifies the kernel of the restriction maps introduced above.

Theorem 9. *(Inflation-Restriction) If M is a G -module and H is a normal subgroup of G , then M^H is a G/H -module and there is an exact sequence:*

$$0 \rightarrow H^1(G/H, M^H) \xrightarrow{\text{inf}} H^1(G, M) \xrightarrow{\text{res}} H^1(H, M).$$

Corollary 10. $H_{ur}^1(G_{\mathbb{Q}_p}, M) \cong H^1(G_{\mathbb{Q}_p}/I_p, M^{I_p})$.

The advantage of working with cohomology groups is that they fit into various exact sequences and perfect pairings, allowing them to be computed in terms of simpler objects. One such simpler object is $H^0(G, M)$. An example of this sort of simplification is the following theorem. But, first, we need a lemma:

Lemma 11. *If G is infinite procyclic generated by g and M is finite, then $H^1(G, M) \cong M/((g-1)M)$.*

Proof. If $m \in M$, define $f : G \rightarrow M$ by $f(g^i) = m + gm + g^2m + \dots + g^{i-1}m$. One can show that f is indeed a 1-cocycle. Conversely, for a given 1-cocycle f , one can easily obtain the form of $f(g^i)$ by induction on i . \square

Theorem 12. *For finite M , we have*

$$|H_{ur}^1(G_{\mathbb{Q}_p}, M)| = |H^0(G_{\mathbb{Q}_p}, M)|.$$

In particular, $H_{ur}^1(G_{\mathbb{Q}_p}, M)$ is finite.

Proof. The following short exact sequence of abelian groups

$$0 \rightarrow M^{G_{\mathbb{Q}_p}} \rightarrow M^{I_p} \xrightarrow{Fr_p - 1} (Fr_p - 1)M^{I_p} \rightarrow 0$$

implies that

$$|H^0(G_{\mathbb{Q}_p}, M)| = |M^{G_{\mathbb{Q}_p}}| = |M^{I_p}|/|((Fr_p - 1)M^{I_p})|.$$

On the other hand, by the lemma, we have

$$|H^1(G_{\mathbb{Q}_p}/I_p, M^{I_p})| = |H^1(\langle Fr_p \rangle, M^{I_p})| = |M^{I_p}|/|((Fr_p - 1)M^{I_p})|.$$

By corollary 10, we are done. \square

One can define cohomology groups $H^r(G, M)$ for any nonnegative integer r . For example, second cohomology group is defined as follows: 2-cocycles and 2-coboundaries to be certain continuous maps $f : G \times G \rightarrow M$. Namely, a 2-cocycle f is a continuous map that satisfies

$$gf(h, k) - f(gh, k) + f(g, hk) - f(g, h) = 0,$$

whereas a 2-coboundary is an f of the form

$$f(g, h) = gF(h) - F(gh) + F(g)$$

for some $F : G \rightarrow M$. As in the case of 1-cocycles, the 2-cocycles form an abelian group and 2-coboundaries form a subgroup, and we denote the quotient group by $H^2(G, M)$.

Theorem 13. [?,] Suppose $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ is a short exact sequence of G -modules. Then there is a long exact sequence of cohomology groups

$$\begin{aligned} 0 \rightarrow H^0(G, A) \rightarrow H^0(G, B) \rightarrow H^0(G, C) \rightarrow \\ H^1(G, A) \rightarrow H^1(G, B) \rightarrow H^1(G, C) \rightarrow \\ H^2(G, A) \rightarrow H^2(G, B) \rightarrow H^2(G, C) \dots \end{aligned}$$

Before giving Wiles' main result on sizes of Selmer groups, we need some preparatory results. Note that if A and B are G -modules, then $\text{Hom}(A, B)$ has a G -action given by $(g.f)(a) = g(f(g^{-1}a))$ where $g \in G, f \in \text{Hom}(A, B), a \in A$.

Theorem 14. (Local Tate duality, [?]) Suppose M is a $G_{\mathbb{Q}_p}$ -module of finite cardinality, n . Set $M^* = \text{Hom}(M, \mu_n(\overline{\mathbb{Q}_p}))$, where $\mu_n(\overline{\mathbb{Q}_p})$ is the n th roots of 1 in $\overline{\mathbb{Q}_p}$ given its natural $G_{\mathbb{Q}_p}$ -action. There is a nondegenerate pairing for $i = 0, 1, 2$

$$H^i(G_{\mathbb{Q}_p}, M) \times H^{2-i}(G_{\mathbb{Q}_p}, M^*) \rightarrow H^2(G_{\mathbb{Q}_p}, \mu_n) \hookrightarrow \mathbb{Q}/\mathbb{Z}.$$

where the second map $\text{inv} : H^2(G_{\mathbb{Q}_p}, \mu_n) \hookrightarrow \mathbb{Q}/\mathbb{Z}$ in the composition is the invariant. If p does not divide the order of M , then under the pairing $H_{ur}^1(G_{\mathbb{Q}_p}, M)$ and $H_{ur}^1(G_{\mathbb{Q}_p}, M^*)$ are the exact annihilators of each other.

Note that, by Theorem 14, annihilators of local conditions are also local conditions and so the following definition makes sense.

Definition 15. Given local conditions $\mathcal{L} = \{L_p\}$, $L_p \subseteq H^1(G_{\mathbb{Q}_p}, \text{Ad}^0(\bar{\rho}))$, one defines dual local conditions $\mathcal{L}^* = \{L_p^*\}$, where $L_p^* \subseteq H^1(G_{\mathbb{Q}_p}, \text{Ad}^0(\bar{\rho})^*)$ is the annihilator of L_p under Tate's pairing. And, one defines dual Selmer group by

$$H_{\mathcal{L}^*}^1(G_{\mathbb{Q}}, \text{Ad}^0(\bar{\rho})^*) = \{c \in H^1(G_{\mathbb{Q}}, \text{Ad}^0(\bar{\rho})^*) : \text{res}_p(c) \in L_p^* \text{ for all } p\}.$$

Theorem 16. (Wiles) For any given local conditions $\mathcal{L} = \{L_p\}$, we have the following equality

$$\frac{|H_{\mathcal{L}}^1(G_{\mathbb{Q}}, \text{Ad}^0(\bar{\rho}))|}{|H_{\mathcal{L}^*}^1(G_{\mathbb{Q}}, \text{Ad}^0(\bar{\rho})^*)|} = \frac{|H^0(G_{\mathbb{Q}}, \text{Ad}^0(\bar{\rho}))|}{|H^0(G_{\mathbb{Q}}, \text{Ad}^0(\bar{\rho})^*)|} \prod_{p \leq \infty} \frac{|L_p|}{|H^0(G_{\mathbb{Q}_p}, \text{Ad}^0(\bar{\rho}))|}.$$

Note that since for all but finitely many primes $L_p = H_{ur}^1(G_{\mathbb{Q}_p}, \text{Ad}^0(\bar{\rho}))$, which has the same order as $H^0(G_{\mathbb{Q}_p}, \text{Ad}^0(\bar{\rho}))$, the right-hand side is a finite product.

Proof. Here is the idea. The Poitou-Tate 9-term sequence (see [?], p 55) and the definition of the Selmer group yield the following exact sequence, where S is the set of bad primes introduced earlier and c is the complex conjugation:

$$\begin{aligned} 0 \rightarrow H^0(G_{\mathbb{Q}, S}, \text{Ad}^0(\bar{\rho})) \rightarrow (\oplus_{p \in S} H^0(G_{\mathbb{Q}_p}, \text{Ad}^0(\bar{\rho}))) / ((1+c)\text{Ad}^0(\bar{\rho})) \rightarrow H^2(G_{\mathbb{Q}, S}, \text{Ad}^0(\bar{\rho})^*)^\wedge \rightarrow \\ H_{\mathcal{L}}^1(G_{\mathbb{Q}}, \text{Ad}^0(\bar{\rho})) \rightarrow \oplus_{p \in S} L_p \rightarrow H^1(G_{\mathbb{Q}, S}, \text{Ad}^0(\bar{\rho})^*)^\wedge \rightarrow H_{\mathcal{L}^*}^1(G_{\mathbb{Q}}, \text{Ad}^0(\bar{\rho})^*)^\wedge \rightarrow 0 \end{aligned}$$

Here A^\wedge denotes the Pontrjagin dual $\text{Hom}(A, \mathbb{Q}/\mathbb{Z})$.

The alternating product of orders of groups in an exact sequence is 1, and so

$$\frac{|H_{\mathcal{L}}^1(G_{\mathbb{Q}}, \text{Ad}^0(\bar{\rho}))|}{|H_{\mathcal{L}^*}^1(G_{\mathbb{Q}}, \text{Ad}^0(\bar{\rho})^*)|} = \frac{|H^0(G_{\mathbb{Q}, S}, \text{Ad}^0(\bar{\rho}))||H^2(G_{\mathbb{Q}, S}, \text{Ad}^0(\bar{\rho})^*)||\prod_{p \in S} |L_p|}{|H^1(G_{\mathbb{Q}, S}, \text{Ad}^0(\bar{\rho})^*)|\prod_{p \in S} |H^0(G_{\mathbb{Q}_p}, \text{Ad}^0(\bar{\rho}))|}.$$

Since it is easiest to compute orders of H^0 's (or if necessary H^1 's), we need some way of removing the H^2 term here, which is provided by the *global Euler characteristic formula* (see [?], p 64):

$$\frac{|H^1(G_{\mathbb{Q}, S}, \text{Ad}^0(\bar{\rho})^*)|}{|H^0(G_{\mathbb{Q}, S}, \text{Ad}^0(\bar{\rho})^*)||H^2(G_{\mathbb{Q}, S}, \text{Ad}^0(\bar{\rho})^*)|} = \frac{|\text{Ad}^0(\bar{\rho})^*|}{|H^0(G_{\mathbb{Q}_\infty}, \text{Ad}^0(\bar{\rho})^*)|}.$$

One can easily show that the term on the right-hand side equals to $|(1+c)\text{Ad}^0(\bar{\rho})|$ and completes the proof, see exercise 6. \square

There is also a *local Euler characteristic formula* (see [?], p 34):

Theorem 17. *If M is a finite $G_{\mathbb{Q}_p}$ -module, then*

$$\frac{|H^1(G_{\mathbb{Q}_p}, M)|}{|H^0(G_{\mathbb{Q}_p}, M)||H^2(G_{\mathbb{Q}_p}, M)|} = p^{v_p(|M|)}.$$

This will be needed in studying how H_{Σ}^1 varies as we vary Σ . Suppose, for instance, we add a prime into Σ , yielding Σ' . Then $\mathfrak{R}_{\Sigma'}$ maps onto \mathfrak{R}_{Σ} . We can control the difference in their tangential dimensions as follows.

Theorem 18. *Suppose $|M|$ is a power of ℓ and $q \neq \ell$ a prime for which $L_q = H_{\text{ur}}^1(G_{\mathbb{Q}_q}, M)$. Define \mathcal{L}' by $L'_p = L_p$ if $p \neq q$, and $L'_q = H^1(G_{\mathbb{Q}_q}, M)$. (This corresponds to $\Sigma' = \Sigma \cup \{q\}$.) Then*

$$\frac{|H_{\mathcal{L}'}^1(G_{\mathbb{Q}}, M)|}{|H_{\mathcal{L}}^1(G_{\mathbb{Q}}, M)|} \leq |H^0(G_{\mathbb{Q}_q}, M^*)|.$$

Proof. If \mathcal{L} is replaced by \mathcal{L}' , consider what happens to the terms on the right-hand-side of Wiles' formula. They remain the same except for the term for $p = q$, which changes from 1 to $|H^1(G_{\mathbb{Q}_q}, M)|/|H^0(G_{\mathbb{Q}_q}, M)| = |H^2(G_{\mathbb{Q}_q}, M)|$, using the local Euler characteristic formula. By the local Tate duality pairing, $|H^2(G_{\mathbb{Q}_q}, M)| = |H^0(G_{\mathbb{Q}_q}, M^*)|$.

We must also consider the effect on \mathcal{L}^* . Let \mathcal{L}'^* denote the new dual local conditions. Since $L_q^* = 0$, the conditions defining $H_{\mathcal{L}'^*}^1$ are more restrictive than those defining $H_{\mathcal{L}^*}^1$. Thus, $|H_{\mathcal{L}'^*}^1(G_{\mathbb{Q}}, M^*)| \leq |H_{\mathcal{L}^*}^1(G_{\mathbb{Q}}, M^*)|$.

Putting this together,

$$\frac{|H_{\mathcal{L}'}^1(G_{\mathbb{Q}}, M)|}{|H_{\mathcal{L}}^1(G_{\mathbb{Q}}, M)|} = \frac{|H_{\mathcal{L}'^*}^1(G_{\mathbb{Q}}, M^*)|}{|H_{\mathcal{L}^*}^1(G_{\mathbb{Q}}, M^*)|} |H^0(G_{\mathbb{Q}_q}, M^*)| \leq |H^0(G_{\mathbb{Q}_q}, M^*)|.$$

\square

3 Bounding Selmer Groups

Recall that the main purpose is to compute the size of Selmer groups which give us the tangential dimension of the universal deformation ring \mathfrak{R}_Σ . This will be established in chapter?????. In this section, we will bound the right-hand side of Wiles' formula and thus this will induce a bound on the ratio of Selmer group and its dual. Let $M = \text{Ad}^0(\bar{\rho})$. There are several cases to compute:

Case 1: Global Terms

Note that the “global” terms, e.g. $|H^0(G_\mathbb{Q}, M)|$ will typically be 1, since we assume that $\bar{\rho}$ is absolutely irreducible, whence $M^{G_\mathbb{Q}}$ consists of scalar matrices, but the only such of trace 0 is the zero matrix, see exercise 3.

Case 2: $p = \infty$

$H^0(G_{\mathbb{Q}_\infty}, M) = M^{G_{\mathbb{Q}_\infty}}$. We are assuming $\bar{\rho}$ is odd so, up to conjugation, can take the image of complex conjugation to be $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. We seek those trace 0 matrices fixed under conjugation by that matrix, easily computed to be $\left\{ \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix} \mid a \in F \right\}$. $|L_\infty| = 1$ and so the $p = \infty$ term contributes $1/|F|$.

Case 3: $p \neq \ell$ and $p \notin \Sigma$

In this case, we already noted that $|L_p| = |H^0(G_{\mathbb{Q}_p}, M)|$ and so the ratio in the formula is 1 for such primes.

Case 4: $p \neq \ell$ and $p \in \Sigma$

By local Euler characteristic formula and local Tate duality, we have

$$\frac{|L_p|}{|H^0(G_{\mathbb{Q}_p}, M)|} = \frac{|H^1(G_{\mathbb{Q}_p}, M)|}{|H^0(G_{\mathbb{Q}_p}, M)|} = |H^2(G_{\mathbb{Q}_p}, M)| = |H^0(G_{\mathbb{Q}_p}, M^*)|.$$

Thus, the only hard part lies in computing the $p = \ell$ contribution to the formula.

Case 5: $p = \ell$ and $\ell \notin \Sigma$

In this case, $L_p = H_f^1(G_{\mathbb{Q}_\ell}, M)$ and the theory of Fontaine and Lafaille is used, whereby they work with a category equivalent to that of finite flat $W(F)[G_{\mathbb{Q}_\ell}]$ -modules, namely whose objects are $W(F)$ -modules D of finite cardinality together with a distinguished submodule D^0 and $W(F)$ -linear maps $\phi_{-1} : D \rightarrow D$ and $\phi_0 : D \rightarrow D$ satisfying $\phi_{-1}|_{D^0} = \ell\phi_0$ and $\text{Im}(\phi_{-1}) + \text{Im}(\phi_0) = D$. This reduces the computations to linear algebra, and it turns out that

$$\frac{|L_\ell|}{|H^0(G_{\mathbb{Q}_\ell}, \text{Ad}^0(\bar{\rho}))|} = |F|.$$

Case 6: $p = \ell$ and $\ell \in \Sigma$

In this case $L_p = H_{ss}^1(G_{\mathbb{Q}_\ell}, M)$. If we let $W \leq \text{Ad}^0(\bar{\rho}) = M$ be $\left\{ \begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix} \right\}$, then this is a $G_{\mathbb{Q}_\ell}$ -submodule since $\bar{\rho}$ restricted to $G_{\mathbb{Q}_\ell}$ has the form (taking a suitable basis) $\begin{pmatrix} \chi\psi_1 & * \\ 0 & \psi_2 \end{pmatrix}$. Here, the form of L_ℓ translates the fact that I_ℓ should act trivially on M/W . Since

$$\begin{pmatrix} r & s \\ 0 & t \end{pmatrix} \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \begin{pmatrix} r & s \\ 0 & t \end{pmatrix}^{-1} = \begin{pmatrix} 0 & ra/t \\ 0 & 0 \end{pmatrix},$$

the $G_{\mathbb{Q}_\ell}$ -action on W is via the character $\chi\psi_1/\psi_2$ (*).

If we want to consider lifts to $F[\epsilon]$ that are ordinary at ℓ too, then we need to set

$$L_\ell := \ker(H^1(G_{\mathbb{Q}_\ell}, M) \rightarrow H^1(I_\ell, M/W)).$$

and consider the following diagram

$$\begin{array}{ccccccc} & & & H^1(G_{\mathbb{Q}_\ell}, M) & & & \\ & & & \downarrow \theta & & & \\ 0 & \longrightarrow & H_{ur}^1(G_{\mathbb{Q}_\ell}, M/W) & \longrightarrow & H^1(G_{\mathbb{Q}_\ell}, M/W) & \xrightarrow{\text{res}} & H^1(I_\ell, M/W) \end{array}$$

Then $L_\ell = \ker(\text{res} \circ \theta)$.

The short exact sequence of $G_{\mathbb{Q}_\ell}$ -modules

$$0 \rightarrow W \rightarrow M \rightarrow M/W \rightarrow 0$$

yields a long exact sequence of cohomology groups:

$$\begin{aligned} 0 \rightarrow H^0(G_{\mathbb{Q}_\ell}, W) \rightarrow H^0(G_{\mathbb{Q}_\ell}, M) \rightarrow H^0(G_{\mathbb{Q}_\ell}, M/W) \rightarrow \\ H^1(G_{\mathbb{Q}_\ell}, W) \rightarrow H^1(G_{\mathbb{Q}_\ell}, M) \rightarrow \text{Im}(\theta) \rightarrow 0. \end{aligned}$$

Since the alternating product of the orders is 1,

$$|\text{Im}(\theta)| = \frac{|H^0(G_{\mathbb{Q}_\ell}, W)||H^0(G_{\mathbb{Q}_\ell}, M/W)||H^1(G_{\mathbb{Q}_\ell}, M)|}{|H^0(G_{\mathbb{Q}_\ell}, M)||H^1(G_{\mathbb{Q}_\ell}, W)|}.$$

Next note that

$$|\text{Im}(\text{res} \circ \theta)| \geq \frac{|\text{Im}(\theta)|}{|H_{ur}^1(G_{\mathbb{Q}_\ell}, M/W)|} = \frac{|\text{Im}(\theta)|}{|H^0(G_{\mathbb{Q}_\ell}, M/W)|}.$$

Putting this together,

$$\begin{aligned} |L_\ell| &= \frac{|H^1(G_{\mathbb{Q}_\ell}, M)|}{|\text{Im}(\text{res} \circ \theta)|} \leq \frac{|H^1(G_{\mathbb{Q}_\ell}, M)||H^0(G_{\mathbb{Q}_\ell}, M/W)|}{|\text{Im}(\theta)|} \\ &= \frac{|H^0(G_{\mathbb{Q}_\ell}, M)||H^1(G_{\mathbb{Q}_\ell}, W)|}{|H^0(G_{\mathbb{Q}_\ell}, W)|}. \end{aligned}$$

Thus, we get

$$\frac{|L_\ell|}{|H^0(G_{\mathbb{Q}_\ell}, M)|} \leq \frac{|H^1(G_{\mathbb{Q}_\ell}, W)|}{|H^0(G_{\mathbb{Q}_\ell}, W)|} = |H^2(G_{\mathbb{Q}_\ell}, W)||F| = |H^0(G_{\mathbb{Q}_\ell}, W^*)||F|$$

by using, respectively, Euler characteristic formula, noting $v_\ell(|W|) = 1$, and local Tate duality.

To compute $|H^0(G_{\mathbb{Q}_\ell}, W^*)|$, let $c_\ell = (\psi_1(Fr_\ell)/\psi_2(Fr_\ell)) - 1$, which will turn out to be very important in chapter 9, for example see theorem 9.10. Let $\phi \in W^*$ be fixed by $G_{\mathbb{Q}_\ell}$, i.e. $\phi(gr) = g\phi(r)$ for all $g \in G_{\mathbb{Q}_\ell}, r \in W \cong F$. If $\alpha = \psi_1(Fr_\ell)/\psi_2(Fr_\ell)$, then by (*), $\phi(\alpha r) = \phi(r)$ ($\chi(Fr_\ell)$ cancels), i.e. $\phi(c_\ell r) = 0$, and so ϕ factors through $F/(c_\ell F)$. (This looks a little strange but later on we use the same calculation with $\bar{\rho}$ replaced by $\rho : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{Z}/\ell^n)$ and so F is replaced by $R = \mathbb{Z}/\ell^n$ and $F/(c_\ell F)$ by $R/(c_\ell R)$.) In any case, $|H^0(G_{\mathbb{Q}_\ell}, W^*)| = |F/(c_\ell F)|$. In conclusion, we get:

Theorem 19. *Using the notation above, if $\ell \notin \Sigma$, then we have*

$$\frac{|H_{\mathcal{L}}^1(G_{\mathbb{Q}}, Ad^0(\bar{\rho}))|}{|H_{\mathcal{L}^*}^1(G_{\mathbb{Q}}, Ad^0(\bar{\rho})^*)|} = \prod_{\substack{p \in \Sigma \\ p \neq \ell}} |H^0(G_{\mathbb{Q}_p}, Ad^0(\bar{\rho})^*)|;$$

if $\ell \in \Sigma$, then we have

$$\frac{|H_{\mathcal{L}}^1(G_{\mathbb{Q}}, Ad^0(\bar{\rho}))|}{|H_{\mathcal{L}^*}^1(G_{\mathbb{Q}}, Ad^0(\bar{\rho})^*)|} \leq |F/(c_\ell F)| \prod_{\substack{p \in \Sigma \\ p \neq \ell}} |H^0(G_{\mathbb{Q}_p}, Ad^0(\bar{\rho})^*)|.$$

Exercises

1. Check the 1-cocycles and 1-coboundaries do indeed form abelian groups, the first containing the second.
2. Show that if G acts trivially on M , then $H^1(G, M) = Hom(G, M)$.
3. Let $A \in Ad^0(\bar{\rho})$ be fixed under conjugation by the matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Then $A = \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}$ for some $a \in F$.
4. Fill in the details of Theorem 8.4.
5. The purpose of this exercise to show that Selmer group $H_{\mathcal{L}}^1(G_{\mathbb{Q}}, M)$ is finite for $M = Ad^0(\bar{\rho})$.
 - i. Let S be a finite set of primes containing all the “bad” ones, i.e. ∞, ℓ , the primes p such that I_p acts nontrivially on M , and such that $L_p \neq H_{ur}^1$. Let $H = \ker(G_{\mathbb{Q}, S} \rightarrow Aut(M))$. Show that $H^1(H, M) = Hom(H, M)$.
 - ii. Use the Hermite-Minkowski theorem to show that $H^1(H, M)$ is finite.
 - iii. Use the inflation-restriction sequence to show that $H^1(G_{\mathbb{Q}, S}, M)$ is finite. Conclude that $H_{\mathcal{L}}^1(G_{\mathbb{Q}}, M)$ is finite.

6. Show that $\frac{|\text{Ad}^0(\bar{\rho})^*|}{|H^0(G_{\mathbb{Q}_\infty}, \text{Ad}^0(\bar{\rho})^*)|} = |(1+c)\text{Ad}^0(\bar{\rho})|$.