Applications of Chebotarev density

$V.1$. *Definition of the deformation problem.* As in the previous sections, we let $\Gamma_{F^+} = Gal(\overline{\mathbb{Q}}/F^+)$, $\Gamma_F = Gal(\overline{\mathbb{Q}}/F)$. A decomposition group at the prime v is denoted Z_v, the inertia subgroup by I_v. The group $\mathcal{G}_n$, viewed as a $\mathbb{Z}$-group scheme, is as in the previous lectures. We fix a prime ℓ, *unramified* in F, and a representation $\overline{\rho} : \Gamma_{F^+} \to \tilde{G}(\overline{\mathbb{F}}_l)$, and let $r_{\overline{\rho}}$ denote the restriction of $\overline{\rho}$ to Γ_F. The representation $\overline{\rho}$ is assumed to satisfy the following conditions:

V.**1.1.0.** *There is a finite subfield $k \subset \overline{\mathbb{F}}_l$ such that $\overline{\rho}$ takes values in $\tilde{G}(k)$.*

V.**1.1.1.** *The composite $\Gamma_{F^+} \to \tilde{G}(\overline{\mathbb{F}}_l) \to \{1, c\}$ cuts out F/F^+.*

V.**1.1.2.** *$r_{\overline{\rho}}$ is unramified except at primes above ℓ and above a non-empty finite set of primes S_{min} of F^+. At primes above ℓ, $r_{\overline{\rho}}$ is crystalline. If $\mathfrak{p} \in S_{min}$ then $\mathfrak{p} = vv^c$ splits in F and $r_{\overline{\rho}}|_{Z_v}$ breaks up as a direct sum of irreducible representations $\mathfrak{r}_{i,v}$. Moreover, there is at least one $\mathfrak{p} \in S_{min}$ such that $r_{\overline{\rho}}|_{Z_v}$ is irreducible, with v as above.*

V.**1.1.3.** *Denote by c any lifting of c to a complex conjugation in Γ_{F^+}. In the adjoint representation $ad\, \overline{\rho}$ of Γ_{F^+} on $Lie(\tilde{G})$, the $+1$-eigenspace of c has dimension $\geq \frac{n(n-1)}{2}$.*

V.**1.1.4.** *The composite $\omega_{\overline{\rho}} = \nu \circ \overline{\rho} : \Gamma_{F^+} \to k^\times$, restricted to Γ_F, equals the $(1-n)$th power of the cyclotomic character, where $\nu : \tilde{G} \to GL(1)$ is the similitude character defined in §**I**.1.*

Here and in what follows the term "crystalline," applied to ℓ-torsion modules, is used to refer to Galois representations obtained by the Fontaine-Laffaille construction. The details of this theory were recalled in earlier notes.

We note the following consequence of (V.1.1.2):

V.**1.1.7.** *The intersection $F \cap \mathbb{Q}(\zeta_\ell) = \mathbb{Q}$.*

Let $\mathcal{O}$ denote the ring of integers in a totally ramified finite extension $\mathbb{K}$ of the fraction field of the Witt ring $W(k)$. Let $\mathcal{C}_\mathcal{O}$ denote the category of complete noetherian local $\mathcal{O}$-algebras with residue field k; morphisms in $\mathcal{C}_\mathcal{O}$ are assumed to be local (take maximal ideals to maximal ideals). If R is an object of $\mathcal{C}_\mathcal{O}$ we let m_R denote its maximal ideal. Since $\ell > 2$ by the banality hypothesis, the character $\omega_{\overline{\rho}}$ defined by V.1.1.4 has a unique lift $\omega_{\overline{\rho},R} : \Gamma_{F^+} \to R^\times$ for any object R of $\mathcal{C}_\mathcal{O}$.

V.**1.2.** *Let R be an object of $\mathcal{C}_\mathcal{O}$. A* **deformation** *of $\overline{\rho}$ to R is a homomorphism $\rho : \Gamma_{F^+} \to \tilde{G}(R)$ such that*

(V.1.2.1) $$\overline{\rho} \equiv \rho \pmod{m_R}.$$

$$(V.1.2.2) \qquad \nu \circ \rho(g) = \omega_{\overline{\rho},R}.$$

Here $\nu : \tilde{G}(R) \to R^\times$ *is the similitude character.*

We assume

V.1.3. $\overline{\rho}$ *has a deformation* ρ_0 *to* $\mathcal{O}$ *such that for each prime* λ *of* F *dividing* ℓ $r_{\rho_0}|_{\Gamma_\lambda}$ *is crystalline and the filtered module has* n *graded pieces, each free of rank one over* $\mathcal{O}$*, and of weights* $0, 1, \ldots, n-1$.

V.1.4. We will be considering deformations of $\overline{\rho}$ with conditions at certain auxiliary sets of primes. Let Q denote a finite set of height one primes $\mathfrak{q}$ of F^+ disjoint from $S_{min} \cup S_\ell$ [divisors of ℓ] which satisfy

V.1.4.1. $\mathfrak{q}$ *splits in* F *and the division algebras* D *and* $D^\#$ *are split above* $\mathfrak{q}$*;*

V.1.4.2. *The residue characteristic* q *of* $\mathfrak{q}$ *satisfies* $q \equiv 1 \pmod{\ell}$*;*

V.1.4.3. $\overline{\rho}(Frob_\mathfrak{q})$ *has a distinguished eigenvalue* $\alpha_\mathfrak{q}$ *of multiplicity one.*

As representations of $Z_\mathfrak{q}$, we write

$$(V.1.4.4) \qquad \overline{\rho} = \overline{\rho}_\alpha \oplus \overline{\rho}_\beta,$$

where $\overline{\rho}_\alpha$ is the $\alpha_\mathfrak{q}$-eigenspace of $\overline{\rho}(Frob_\mathfrak{q})$ and $\overline{\rho}_\beta$ is the direct sum of the remaining eigenspaces. Let $\Delta_\mathfrak{q}$ denote the maximal ℓ-power quotient of $(\mathbb{Z}/q\mathbb{Z})^\times$ and $\Delta_Q = \prod_{\mathfrak{q} \in Q} \Delta_\mathfrak{q}$.

By a deformation of $\overline{\rho}$ of type Q we shall mean a pair (R, ρ) as in Definition V.1.2 such that:

V.1.5.1. *For each prime* λ *of* F *dividing* ℓ*,* $r_\rho|_{Z_\lambda}$ *is crystalline and the filtered module has* n *graded pieces, each free of rank one over* R*, and of weights* $0, 1, \ldots, n-1$.

V.1.5.2. *If* $\mathfrak{q} \in Q$ *then* $r_\rho|_{Z_\mathfrak{q}} = \chi \oplus r'$ *where* $r' = r'_\mathfrak{q}$ *is unramified and* $\chi = \chi_\mathfrak{q} : Z_\mathfrak{q} \to R^\times$ *is a character whose reduction modulo* m_R *is unramified and takes* $Frob_\mathfrak{q}$ *to* $\alpha_\mathfrak{q}$.

V.1.5.3. *If* $v \notin Q \cup \{\ell\}$ *then* $\rho(I_v) \xrightarrow{\sim} \overline{\rho}(I_v)$.

Proposition V.1.6. *There exists a universal deformation* (R_Q, ρ_Q) *of* $\overline{\rho}$ *of type* Q.

Proof. We need to verify that the conditions in V.1.5 define a Ramakrishna subcategory.

$V.\mathbf{1.7}$ For $\mathfrak{q} \in Q$ we let $\chi_\mathfrak{q} : Z_\mathfrak{q} \to R_Q^\times$ be the character defined in $(V.1.5.2)$. Then $\chi_\mathfrak{q}$ necessarily factors through a natural map $\Delta_\mathfrak{q} \to R_Q^\times$. Thus R_Q is tautologically an $\mathcal{O}[\Delta_Q]$-module.

V.2. Bounding the Selmer group.

Henceforward, we assume $\ell > n$. We fix a finite set Q of primes of F^+ as in $V.1.4$. Let $ad\ r_{\overline{\rho}}$ denote the composition of $\overline{\rho}$ with the adjoint representation $ad : \tilde{G} \to Aut(\mathfrak{gl}(n))$, where $\mathfrak{gl}(n) \subset Lie(\tilde{G})$ is viewed as the kernel of the similitude map. For each place v of F^+ we fix a k-subspace $L_{Q,v} \subset H^1(Z_v, ad\ r_{\overline{\rho}})$. The $L_{Q,v}$ are chosen as follows:

$V.\mathbf{2.1.1.}$ *For v dividing ℓ, $L_{Q,v}$ is the Bloch-Kato group $H^1_f(Z_v, ad\ r_{\overline{\rho}})$.*

In [BlK], Bloch and Kato work with characteristic zero coefficients. The ℓ-torsion group $H^1_f(Z_v, ad\ r_{\overline{\rho}})$ will be defined in $V.4$, below.

$V.\mathbf{2.1.2.}$ *For $v = \mathfrak{q} \in Q$, write*

$$ad\ r_{\overline{\rho}} = ad\ \overline{\rho}_\alpha \oplus ad\ \overline{\rho}'_\alpha,$$

where

$$ad\ \overline{\rho}'_\alpha = ad\ \overline{\rho}_\beta \oplus Hom(\overline{\rho}_\alpha, \overline{\rho}_\beta) \oplus Hom(\overline{\rho}_\beta, \overline{\rho}_\alpha),$$

(notation $V.1.4.4$). We set

$$L_{Q,\mathfrak{q}} = H^1(Z_\mathfrak{q}, ad\ \overline{\rho}_\alpha) \oplus H^1(Z_\mathfrak{q}/I_\mathfrak{q}, ad\ \overline{\rho}'_\alpha).$$

$V.\mathbf{2.1.3.}$ *At all other finite primes v $L_{Q,v} = H^1(Z_v/I_v, ad\ r_{\overline{\rho}}^{I_v})$.*

$V.\mathbf{2.1.4.}$ *At archimedean primes we take $L_{Q,v} = 0$.*

There is a natural isomorphism (Poincaré duality)

$$ad\ r_{\overline{\rho}} \xrightarrow{\sim} ad\ r_{\overline{\rho}}^*,$$

hence natural non-degenerate pairings for each place v

$$(V.2.1.5) \qquad H^i(Z_v, ad\ r_{\overline{\rho}}) \times H^{2-i}(Z_v, ad\ r_{\overline{\rho}}(1)) \to \mathbb{Q}/\mathbb{Z}$$

(Tate's local duality), where (1) denotes Tate twist. For each v we let $L^\perp_{Q,v} \subset H^1(Z_v, ad\ r_{\overline{\rho}}(1))$ be the annihilator of $L_{Q,v}$ with respect to $(V.2.1.5)$, and define the Selmer group of $ad\ r_{\overline{\rho}}(1)$, relative to the data $L^\perp_{Q,v}$:

$$(V.2.1.6) \qquad H^1_{Q^*}(F^+, ad\ r_{\overline{\rho}}(1)) = \{h \in H^1(F^+, ad\ r_{\overline{\rho}}(1)) \mid \forall\ v\ r_v(h) \in L^\perp_{Q,v}\}$$

(So the index is Q rather than $\mathcal{S}$ or $\mathcal{D}$.) We write $\mathfrak{M}_Q$ for m_{R_Q}. The objective of this section is to prove the following theorem.

Theorem V.2.2. *The Selmer group $H^1_{Q^*}(F^+, ad\ r_{\overline{\rho}}(1))$ is finite and we have the inequality*

$$\dim_k \mathfrak{M}_Q/({\mathfrak{M}_Q}^2, \ell) \leq \#Q + \dim_k H^1_{Q^*}(F^+, ad\ r_{\overline{\rho}}(1)).$$

In particular, if $\dim H^1_{Q^*}(F^+, adr_{\overline{\rho}}) = 0$ then the $\mathcal{O}$-algebra R_Q can be topologically generated by $\#Q$ elements.

This theorem generalizes Lemma 5 of [TW]. Henceforward we write dim instead of $\dim_k$. We begin by translating the theorem into a statement purely in terms of Galois cohomology.

Proposition V.2.3. *Define the Selmer group of ad $r_{\overline{\rho}}$, relative to the data $L_{Q,v}$:*

$$H^1_Q(F^+, ad\ r_{\overline{\rho}}) = \{h \in H^1(F^+, ad\ r_{\overline{\rho}}) \mid \forall\ v\ r_v(h) \in L_{Q,v}\}.$$

Then

$$\dim \mathfrak{M}_Q/({\mathfrak{M}_Q}^2, \ell) = \dim H^1_Q(F^+, ad\ r_{\overline{\rho}}).$$

Proof. This is proved as in [DDT,Theorem 2.41]. Let $\mathcal{D}$ denote the category of $k[\Gamma_{F^+}]$-modules M finite over k with dimension divisible by n, satisfying the analogues of properties V.1.5.1-3:

V.2.3.1. *As a module over Z_v, v above ℓ, M is a Fontaine-Laffaille representation (cf. §V.4, below).*

V.2.3.2. *As a module over $Z_{\mathfrak{q}}$, $\mathfrak{q}$ in Q, M is a the sum of an unramified module B and a module A whose semisimplification is isotypic for the unramified character $\alpha_{\mathfrak{q}}$.*

V.2.3.3. *If $v \notin Q \cup \{\ell\}$ then the action of I_v on M is a direct sum of copies of irreducible direct summands of $\overline{\rho}(I_v)$.*

The category $\mathcal{D}$ is closed under products and taking subobjects and quotient objects. Obviously it contains $\overline{\rho}$. Thus Lemma 2.39 of [DDT] applies and yields

$$\dim \mathfrak{M}_Q/({\mathfrak{M}_Q}^2, \ell) = \dim H^1_{\mathcal{D}}(F^+, ad\ r_{\overline{\rho}}),$$

where $H^1_{\mathcal{D}}(F^+, ad\ r_{\overline{\rho}}) \subset H^1(F^+, ad\ r_{\overline{\rho}}) \simeq Ext^1_{\Gamma_{F^+}}(\overline{\rho}, \overline{\rho})$ is the subspace of classes whose corresponding extensions lie in $\mathcal{D}$.

Now we have to verify that conditions V.2.3.1-3 for extensions translate into the cohomological conditions V.2.1.1-3. Specifically, the equivalence of V.2.3.1 and V.2.1.1 is proved below in V.4.7. The equivalence of V.2.3.2 with V.2.1.2 is easy to verify. At finite places $v \notin Q \cup \ell \cup S_{min}$, and such that v is unramified in F,

$V.2.3.3$ says the action of I_v is trivial, which is obviously equivalent to $V.2.1.3$. Now suppose v in S_{min}. The compatibility of $V.2.3.3$ and $V.2.1.3$ is equivalent to the condition

$$H^1(Z_v/I_v, Hom_{I_v}(\overline{\rho},\overline{\rho})) \simeq Ker[H^1(Z_v, Hom(\overline{\rho},\overline{\rho})) \to H^1(I_v, Hom(\overline{\rho},\overline{\rho}))],$$

and this is just the inflation-restriction sequence. For v ramified in F, the argument is similar.

We thus need to prove the inequality

$$(V.2.4) \qquad \dim H^1_Q(F^+, ad\ r_{\overline{\rho}}) - \dim H^1_{Q^*}(F^+, ad\ r_{\overline{\rho}}(1)) \leq \#Q.$$

Following Wiles [W,Prop. 1.6], the left hand side of $(V.2.4)$ can be expressed as a sum of local terms. We write the formula as in [DDT, Theorem 2.19], where it is stated for a general number field:

Proposition V.2.5. *Let $h^0 = \dim H^0(F^+, ad\ r_{\overline{\rho}})$, $h^{0,*} = \dim H^0(F^+, ad\ r_{\overline{\rho}}(1))$. For any place v of F^+ let $h^0_v = \dim H^0(Z_v, ad\ r_{\overline{\rho}})$. Then we have the formula*

$$\dim H^1_Q(F^+, ad\ r_{\overline{\rho}}) - \dim H^1_{Q^*}(F^+, ad\ r_{\overline{\rho}}(1)) = h^0 - h^{0,*} + \sum_v (\dim L_{Q,v} - h^0_v).$$

Lemma V.2.6. *Under the hypotheses of Proposition $V.2.5$, the local terms are computed as follows:*

(a) For v real, $h^0_v \geq \frac{n(n-1)}{2}$, $\dim L_{Q,v} = 0$.
(b) For $v \in Q$, $\dim L_{Q,v} - h^0_v = 1$.
(c) For v above ℓ, $\dim L_{Q,v} - h^0_v = [k(v) : \mathbb{F}_\ell] \cdot \frac{n(n-1)}{2}$.
(d) For all other places v, $\dim L_{Q,v} - h^0_v = 0$.
Finally, the global terms are given by $h^0 = h^{0,*} = 0$.

Admit this lemma for the moment. Comparing Proposition $V.2.5$ with Lemma $V.2.6$, we find

$$\begin{aligned}(V.2.7) \quad & \dim H^1_Q(F^+, ad\ r_{\overline{\rho}}) - \dim H^1_{Q^*}(F^+, ad\ r_{\overline{\rho}}(1)) \\ & \leq \#Q - \sum_{v \text{ real}} \frac{n(n-1)}{2} + \sum_{v|\ell} [k(v) : \mathbb{F}_\ell] \cdot \frac{n(n-1)}{2} \\ & \leq \#Q - [F^+ : \mathbb{Q}]\frac{n(n-1)}{2} + [F^+ : \mathbb{Q}]\frac{n(n-1)}{2} \leq \#Q\end{aligned}$$

Theorem $V.2.2$ now follows by comparing $(V.2.7)$ with Proposition $V.2.3$.

$V.2.8$. We begin by calculating the global terms in Lemma $V.2.6$. The hypothesis that S_{min} is non-empty implies that $\overline{\rho}$ is already irreducible when restricted to a decomposition group of Γ_F above a prime in S_{min}. Thus $H^0(F, ad\ r_{\overline{\rho}})$ is one-dimensional and given by the trace of $r_{\overline{\rho}}$. But complex conjugation c acts as -1 on the center of the $GL(n)$-component of the L-group, so $H^0(F^+, ad\ r_{\overline{\rho}})$ is trivial. In the same way, and using $V.1.1.5$, we see that $h^{0,*} = 0$.

The local terms will be computed in the next two sections.

$V.3$. *Local calculations, char $v \neq \ell$.*

In this section we carry out the calculations summarized in Lemma $V.2.6$. For any place v and any finite $\mathbb{F}_\ell[Z_v]$-module M we set

$$h^i(M) = \dim H^i(\Gamma_v, M); \quad h^{i,unr}(M) = \dim H^i(Z_v/I_v, M^{I_v}),$$

$i = 0, 1, 2$.

$V.3.1$. If M is an unramified Z_v-module then of course $h^{0,unr}(M) = h^0(M)$. On the other hand, M is always assumed to be $Frob_v$-semi-simple when ℓ is not equal to the residue characteristic of v. Then M is the sum of characters of Z_v/I_v and

$$h^{1,unr}(M) = h^0(M) = \dim M^{Z_v}. \qquad (V.3.1)$$

It follows that, for v unramified, $v \notin Q$, we have

$$\dim L_{Q,v} - h^0_v = 0.$$

This verifies $V.2.6$ (d) at unramified places.

$V.3.2$. Now take $v \in Q$. We have

$$\dim L_{Q,v} - h^0_v = h^1(ad\ \overline{\rho}_\alpha) - h^0(ad\ \overline{\rho}_\alpha) + h^{1,unr}(ad\ \overline{\rho}_\alpha)' - h^0(ad\ \overline{\rho}_\alpha)'.$$

Since $ad(\overline{\rho}_\alpha)'$ is unramified the last two terms cancel, by $(V.3.1)$. On the other hand, the first two terms give

$$h^0(ad\ \overline{\rho}_\alpha(1))$$

by the local Euler characteristic formula and local duality (cf. [W,p. 473]). But $\overline{\rho}_\alpha$ is one-dimensional, so $ad(\overline{\rho}_\alpha)$ is the trivial Z_v module. Since $q \equiv 1 \pmod{\ell}$ the Tate twist is also trivial, and we find

$$\dim L_{Q,v} - h^0_v = 1,$$

which verifies $V.2.6$ (b).

$V.3.3$. For v real, we have $\dim L_{Q,v} = 0$, by hypothesis. On the other hand,

$$h^0_v = \dim [ad\ r_{\overline{\rho}}]^{c=1},$$

independently of v. Then (a) follows immediately from hypothesis $V.1.1.3$.
$V.3.4$. Now suppose v is ramified, but of residue characteristic $\neq \ell$. By hypothesis, either $v \in S_{min}$, or v ramifies in F/F^+ and $r_{\overline{\rho}}$ is unramified at the prime above v. We need to calculate

$$\dim L_{Q,v} - h_v^0 = h^{1,unr}(ad\ r_{\overline{\rho}}) - h^0(ad\ r_{\overline{\rho}}).$$

First, suppose $v \in S_{min}$, and $r_{\overline{\rho}} = \oplus_{i=1}^r (\mathfrak{r}_i)^{a_i}$, where the $\mathfrak{r}_i$ are irreducible and distinct. Returning to $V.1.1.2$, we find that

$$\dim[ad\ r_{\overline{\rho}}]^{Z_v} = \sum_i (a_i)^2.$$

Let $L_{ij} = H^1(Z_v/I_v, \mathfrak{r}_i \otimes \mathfrak{r}_j^*)$, where $*$ denotes dual. It suffices to show that $\dim L_{ij} = \delta_{ij}$. Suppose $\mathfrak{r}_i|_{I_v}$ breaks up as the sum of d irreducible representations τ_{ik}. Then

$$(V.3.5) \qquad (\mathfrak{r}_i \otimes \mathfrak{r}_i^*)^{I_v} = \oplus_{k=1}^d [ad\ \tau_k]^{I_v}$$

has dimension d. As a representation of the cyclic group Z_v/I_v, the right-hand side of $V.3.5$ is isomorphic to the sum $\oplus\chi$ of the distinct characters of Z_v/H, where $H \supset I_v$ is the stabilizer in Z_v of τ_1, say. Thus

$$\dim L_{ii} = \sum_\chi \dim H^1(Z_v/H, \chi) = 1,$$

since only the trivial character has non-trivial cohomology. The verification for L_{ij} with $i \neq j$ breaks up into two cases. If $\mathfrak{r}_j$ is not an unramified twist of r_i, then $(\mathfrak{r}_i \otimes \mathfrak{r}_j^*)^{I_v} = 0$. If $\mathfrak{r}_i = \mathfrak{r}_j \otimes \xi$, with ξ an unramified character, then we find

$$(\mathfrak{r}_i \otimes \mathfrak{r}_j^*)^{I_v} = \oplus_{k=1}^d \chi \cdot \xi$$

where χ runs through the characters of Z_v/H, as above. We conclude that $\dim L_{ij} = 0$ by observing that the non-isomorphy of $\mathfrak{r}_i$ and $\mathfrak{r}_j$ implies that ξ does not factor through Z_v/H.

Now suppose v ramifies in F/F^+. Let w denote the prime above v. In this case Z_v acts via the abelian group $Gal(F/F^+) \times Z_w/I_w$. Let M denote the subspace of $ad\ \overline{\rho}$ fixed by $Gal(F/F^+)$. Then $\dim L_{Q,v} - h_v^0 = h^{1,unr}(M) - h^0(M) = 0$ as in $V.3.1$. This completes the verification of (d).

To complete the proof of Lemma $V.2.6$, it remains to estimate the local terms at primes dividing ℓ. This is the subject of the next section.

V.5. Capturing ramification by tame classes.

In order to make Theorem $V.2.2$ effective, we need to find sets Q for which $\dim H^1_{Q^*}(F^+, ad\ \overline{\rho}) = 0$. We follow the strategy of [TW]. For this additional hypotheses are needed. Unfortunately, we have not found an optimal set of hypotheses. In the coordinates of (**I**.1.4) the map

$$(V.5.1) \qquad \tilde{G}^0 \to GL(n) \times GL(1);\ g \mapsto (g_1, a = \nu(g))$$

is an isomorphism. Let $r^i_{\overline{\rho}}$, $i = 1, 2$, denote the composition of $r_{\overline{\rho}}$ with projection on the i-th factor in (V.5.1.1). Thus $Ker(r^1_{\overline{\rho}})$ determines an extension F^1 of F with Galois group naturally a subgroup of $GL(n,k)$; $Ker(r^2(\overline{\rho}))$ determines the extension $F(\zeta_\ell^{n-1})$ of F, of degree $[\mathbb{Q}(\zeta_\ell^{n-1}) : \mathbb{Q}]$ (cf. (V.1.1.4) and (V.1.1.7)). We consider the following conditions.

Hypotheses V.5.2.

(a) $F^1 \cap F(\zeta_\ell) = F$.

(b) The group $Im(\overline{\rho})$ has no quotient of order ℓ.

(c) Let $V \subset ad\ \overline{\rho}$ be an irreducible subrepresentation. Then there is $s \in \Gamma_F$ such that $r_{\overline{\rho}}(s)$ has n distinct eigenvalues and such that $ad\ (\overline{\rho})(s)$ has eigenvalue 1 on V.

Theorem V.5.3. *Assume Hypotheses $V.5.2$. Then there is an integer r such that, for any $m \geq 1$ there is a set Q_m satisfying the hypotheses of $V.1.4$, and such that moreoever*

(a) $\#Q_m = r$;

(b) For all $\mathfrak{q} \in Q_m$ we have $q = N\mathfrak{q} \equiv 1 \pmod{\ell^m}$;

(c) $H^1_{Q_m^*}(F^+, ad\ \overline{\rho}(1)) = 0$.

(d) $r_{\overline{\rho}}(Frob_{\mathfrak{q}})$ has n distinct eigenvalues, and in particular a distinguished eigenvalue $\alpha_{\mathfrak{q}}$ of multiplicity one.

Proof. We begin by recalling that, for any Q as in V.1.4, and any $\mathfrak{q} \in Q$, the subspace $L^{\perp}_{Q,\mathfrak{q}} \subset H^1(Z_{\mathfrak{q}}, ad\ \overline{\rho}(1))$ is defined by

$$H^1(Z_{\mathfrak{q}}/I_{\mathfrak{q}}, ad\ \overline{\rho}'_\alpha(1))$$

in the notation of V.2.1.2. In other words, $L^{\perp}_{Q,\mathfrak{q}}$ consists of unramified classes with trivial $ad\ (\overline{\rho}_\alpha)(1)$-component. Thus

(V.5.3.1)

$$H^1_{Q^*}(F^+, ad\ r_{\overline{\rho}}(1)) = Ker[H^1_{\emptyset}(F^+, ad\ \overline{\rho}(1)) \to \oplus_{\mathfrak{q} \in Q_m} H^1(Z_{\mathfrak{q}}/I_{\mathfrak{q}}, ad\ \overline{\rho}_\alpha(1))].$$

For r we take the dimension of $H^1_\emptyset(F^+, ad^0\overline{\rho}(1))$. As in [TW,p. 567] we need to find sets Q_m satisfying conditions (a), (b), (d), and the hypotheses of V.1.4, and such that the natural map

$$(V.5.3.2) \qquad H^1_\emptyset(F^+, ad\overline{\rho}(1)) \to \oplus_{\mathfrak{q}\in Q_m} H^1(Z_\mathfrak{q}/I_\mathfrak{q}, ad(\overline{\rho}_\alpha)(1))$$

is injective, hence an isomorphism for dimension reasons. Condition (b) asserts that $\mathfrak{q}$ splits completely in $F(\zeta_{\ell^m})$.

Let $[\psi] \in H^1_\emptyset(F^+, ad\overline{\rho}(1))$ be a non-zero class. The objective is to find $\mathfrak{q}$ as above satisfying condition (b), (d), and V.1.4 and such that

$$(V.5.3.3) \qquad res_\mathfrak{q}[\psi] \in H^1(Z_\mathfrak{q}/I_\mathfrak{q}, ad\ \overline{\rho}_\alpha(1)) \text{ is nontrivial.}$$

By Chebotarev density it thus suffices to find $\sigma \in \Gamma_{F^+}$ such that

V**.5.3.4.** *(i) σ fixes $F^+(\zeta_{\ell^m})$;*
(ii) $\overline{\rho}(\sigma)$ has n distinct eigenvalues;
(iii) There is a distinguished eigenvalue α of $\overline{\rho}(\sigma)$ such that $\psi(\sigma) \notin ad\ \overline{\rho}'_\alpha(1)$

where $ad\ \overline{\rho}'_\alpha \subset ad\ \overline{\rho}$ is the codimension one subspace defined with respect to α by analogy with V.2.1.2.

Let $F^+_m = F^+(\zeta_{\ell^m})$, and let F_m denote the extension of F^+_m fixed by the kernel of $ad\ \overline{\rho}$. We claim ψ restricts to non-trivially to $H^1_{\emptyset^*}(F_m, ad\ \overline{\rho}(1))$. The kernel of the restriction map is $H^1(Gal(F_m/F^+), ad\ \overline{\rho}(1))$. It suffices to show

$$(V.5.3.5) \qquad H^1(Gal(F_m/F^+), ad\ \overline{\rho}(1)) = 0.$$

We argue as in [DDT], p. 84. The inflation-restriction sequence for $F_m \supset F_1 \supset F^+$ is an exact sequence

$$H^1(Gal(F_1/F^+), ad\ \overline{\rho}(1)^{\Gamma_{F_1}}) \hookrightarrow H^1(Gal(F_m/F^+), ad\ \overline{\rho}(1)) \to [H^1(Gal(F_m/F_1), ad\ \overline{\rho}(1))]^{\Gamma_{F^+}}.$$

Now Γ_{F_1} acts trivially on $ad\ \overline{\rho}(1)$. Hence

$$[H^1(Gal(F_m/F_1), ad\ \overline{\rho}(1))]^{\Gamma_{F^+}} \cong Hom(Gal(F_m/F_1), [ad\ \overline{\rho}(1))]^{\Gamma_{F^+}}).$$

Moreover, it follows from Condition V.5.2 (a) that $Gal(F_1/F^+)$ breaks up as the direct product $Gal(F_1/F_0) \times Gal(F_0/F^+)$. Thus

$$(V.5.3.6) \qquad [ad\ \overline{\rho}(1))]^{\Gamma_{F^+}} \subset [ad\ \overline{\rho}(1))]^{Gal(F_1/F_0)} = \{0\}.$$

Indeed, $Gal(F_1/F_0)$ acts on $ad\,\overline{\rho}(1))$ as a direct sum of copies of the natural action on the ℓth roots of unity. But $Gal(F_1/F_0)$ can be identified with the subgroup of $Aut(\mu_\ell)$ that acts trivially on $\mu_\ell^{\otimes(n-1)}$. The hypothesis $\ell > n$ implies that this subgroup is non-trivial.

Thus the above exact sequence simplifies to yield

$$(V.5.3.7) \qquad H^1(Gal(F_1/F^+), ad\,\overline{\rho}(1)) \xrightarrow{\sim} H^1(Gal(F_m/F^+), ad\,\overline{\rho}(1)).$$

On the other hand, applying the inflation restriction sequence for $F_1 \supset F_0 \supset F^+$ to the left-hand side of $(V.5.3.7)$, we find

$$H^1(Gal(F_0/F^+), ad\,\overline{\rho}(1)^{Gal(F_1/F_0)}) \hookrightarrow H^1(Gal(F_1/F^+), ad\,\overline{\rho}(1)) \to [H^1(Gal(F_1/F_0), ad\,\overline{\rho}(1))]^{Gal(F_0/F^+)}.$$

Here the right-hand side vanishes because $[F_1 : F_0]$ is prime to ℓ, while the left-hand side vanishes as in $(V.5.3.6)$. This completes the verification of $(V.5.3.5)$.

Now it follows from $V.5.2$ (a) and (b) that $\overline{\rho}$ remains absolutely irreducible upon restriction to $\Gamma_{F_m^+}$ for all m. Thus, to verify $(V.5.3.2)$, it suffices to find sets of height one primes of F_m^+ satisfying conditions (b), (d), $V.1.4$, and $(V.5.3.3)$, with F^+ replaced by F_m^+. Conditions $V.1.4.1$-2 are already satisfied, and $V.1.4.3$ concerns only a finite set of primes, which we can avoid. We have

$$H^1_\emptyset(F_m, ad\ r_{\overline{\rho}}(1)) \subset Hom(\Gamma_{F_m}, ad\ r_{\overline{\rho}}(1))$$

is the subset satisfying various ramification conditions. Thus let $\psi \in H^1_\emptyset(F_m^+, ad\,r_{\overline{\rho}}(1))$. Its restriction to F_m is a homomorphism from Γ_{F_m} to $ad\ r_{\overline{\rho}}$ whose image is a $Gal(F_m/F_m^+)$-submodule, say V_ψ. Moreover, $Gal(F_m/F_m^+) = Gal(F_0/F^+)$ by $V.5.2$ (a). Let $s \in Gal(F_m/F_m^+)$ satisfy the conditions of $V.5.2$ (c), and let σ_0 be a lifting of s to $\Gamma_{F_m^+}$. It already satisfies conditions (i) and (ii) of $V.5.3.4$, and so does $\sigma = \tau\sigma_0$ for any $\tau \in \Gamma_{F_m}$. It remains to show that we can choose α and τ so that σ satisfies condition (iii). Now the eigenvalues of $ad\ r_{\overline{\rho}}(s)$ are of the form $\alpha_i \cdot \alpha_j^{-1}$, where α_i, $i = 1, \ldots, n$ are the n distinct eigenvalues of $r_{\overline{\rho}}(s)$. Let v_{ij} be the corresponding eigenvectors. By hypothesis $V.5.2$ (c) the fixed subspace V_ψ^s is non-trivial and is spanned by r non-trivial linear combinations $v_k = \sum_i a_{ik} v_{ii}$, $1 \leq k \leq r$. Now $\psi(\sigma) = \psi(\tau) + \psi(\sigma_0)$. Write $\psi(\sigma_0) = \sum b_{ij} v_{ij}$, $\psi(\tau) = \sum c_k(\tau) v_k + v'$, where v' is a linear combination of the v_{ij} with $i \neq j$. Thus the coefficient of v_{ii} in $\psi(\sigma)$ is

$$b_i(\tau) = \sum c_k(\tau) a_{ik} + b_{ii}.$$

But we may vary the $c_k(\tau)$ freely, and it is clear that by doing so we can arrange that at least one $b_i(\tau)$ is non-zero. Taking $\alpha = \alpha_i$, we then see that σ satisfies condition (iii). This completes the proof.

V.6. Eliminating tame deformations

Let q be a rational prime, $q \neq \ell$, and let v be a prime of F^+ dividing q. The maximal ℓ-power quotient $I_{v,\ell}$ of the inertia group I_v is isomorphic to $\mathbb{Z}_\ell(1)$ as a module over Z_v/I_v, where the (1) denotes Tate twist. Let $P^\ell \subset I_v$ be the kernel of the canonical map to $I_{v,\ell}$; it is a profinite group with pro-order prime to ℓ. Thus, for any Z_v-module M, the canonical inflation map $H^1(Z_v/P^\ell, M) \to H^1(Z_v, M)$ is an isomorphism.

Now let $(\overline{\rho}, V)$ be an n-dimensional semi-simple unramified representation of Z_v with coefficients in a finite field k of characteristic ℓ, and let $M = ad\ \overline{\rho}$.

Lemma V.6.1. *Suppose $\overline{\rho}$ is trivial and $Nv \neq 1 \pmod{\ell}$. Then the inflation map*

$$H^1(Z_v/I_v, M) \to H^1(Z_v/P^\ell, M) \tag{V.6.2}$$

is an isomorphism.

Proof. We use the inflation-restriction sequence for the inclusion of $I_{v,\ell}$ in Z_v/P^ℓ:

$$\begin{aligned} 0 \to H^1(Z_v/I_v, M) \to H^1(Z_v/P^\ell, M) \to & \ Hom(I_{v,\ell}, M)^{Z_v/I_v} \\ & = Hom_{Z_v/I_v}(\mathbb{F}_\ell(1), M) \end{aligned} \tag{V.6.3}$$

By our hypothesis, Z_v/I_v acts non-trivially on $\mathbb{F}_\ell(1)$ but trivially on M. Thus the right-hand term in (V.6.3) vanishes.