REVIEW OF GALOIS DEFORMATIONS

SIMON RUBINSTEIN-SALZEDO

1. Deformations and framed deformations

We'll review the study of Galois deformations. Here's the setup. Let G be a profinite group, and let $\overline{\rho} : G \to \mathrm{GL}_n(k)$ be a representation of G over a finite field k of characteristic p. Let Λ be a complete DVR with residue field k, and let $\mathcal{C}_\Lambda$ denote the category whose objects are artinian local Λ-algebras with residue field k, and whose morphisms are local homomorphisms. Let $\widehat{\mathcal{C}}_\Lambda$ denote the category of complete noetherian local Λ-algebras with residue field k, which is the completion of $\mathcal{C}_\Lambda$ under limits. Frequently, Λ will be $W(k)$, the ring of Witt vectors over k.

We now define two deformation functors associated to $\overline{\rho}$. The first is the deformation functor $\mathrm{Def}(\overline{\rho}) : \widehat{\mathcal{C}}_\Lambda \to \underline{\mathrm{Sets}}$ given by

$$\mathrm{Def}(\overline{\rho})(A) = \{(\rho, M, \phi)\}/\cong,$$

where M is a free A-module of rank n, $\rho : G \to \mathrm{Aut}_A(M)$, and $\phi : \rho \otimes_A k \to \overline{\rho}$ is an isomorphism. The second is the framed deformation functor $\mathrm{Def}^\square(\overline{\rho}) : \widehat{\mathcal{C}}_\Lambda \to \underline{\mathrm{Sets}}$ given by

$$\mathrm{Def}^\square(\overline{\rho})(A) = \{(\rho, M, \phi, \mathcal{B}) \mid (\rho, M, \phi) \in \mathrm{Def}(\overline{\rho})(A)\}/\cong,$$

where $\mathcal{B}$ is a basis of M which is sent to the standard basis for k^n under ϕ.

We can compute both Def and $\mathrm{Def}^\square$ at the level of its artinian quotients: if $\mathfrak{m}$ is the maximal ideal of A, then

$$\mathrm{Def}(\overline{\rho})(A) = \varprojlim \mathrm{Def}(\overline{\rho})(A/\mathfrak{m}^i),$$
$$\mathrm{Def}^\square(\overline{\rho})(A) = \varprojlim \mathrm{Def}^\square(\overline{\rho})(A/\mathfrak{m}^i).$$

The functors Def and $\mathrm{Def}^\square$ are not always representable. However, we impose some restrictions to guarantee that at least $\mathrm{Def}^\square$ will be. We say that G satisfies the p-finiteness condition if for every open subgroup $H \subset G$ of finite index, there are only finitely many continuous homomorphisms $H \to \mathbb{Z}/p\mathbb{Z}$. From now on, we'll assume that G satisfies the p-finiteness condition. This is a reasonable assumption, since it holds in cases we're likely to care about. For example, if K is a global field not of characteristic p and S is a finite set of places, then $G_{K,S}$ satisfies the p-finiteness condition for all p. Also, if K is a local field of residue characteristic p, then G_K satisfies the ℓ-finiteness condition for all $\ell \neq p$.

Date: 30 March, 2010.

In this case, $\mathrm{Def}^{\square}(\overline{\rho})$ is representable; call its representing object $R^{\square}(\overline{\rho})$. If $\mathrm{Def}(\overline{\rho})$ is also representable, call its representing object $R(\overline{\rho})$. These are the framed deformation ring and the deformation ring, respectively. Concretely, when $\mathrm{Def}^{\square}(\overline{\rho})$ or $\mathrm{Def}(\overline{\rho})$ is representable, this means that there is some ring $R^{\square}(\overline{\rho})$ or $R(\overline{\rho})$ so that any deformation factors uniquely through the map

$$G \to \mathrm{GL}_n(R^{\square}(\overline{\rho})) \text{ or } G \to \mathrm{GL}_n(R(\overline{\rho})).$$

Schlessinger's criterion tells us when functors $\mathcal{C}_\Lambda \to \underline{\mathrm{Sets}}$ are (pro)-representable. When we apply it to the case of the deformation functor, we get the following:

Proposition 1. *If G satisfies the p-finiteness condition and $\mathrm{End}_G(\overline{\rho}) = k$ ($\overline{\rho}$ is absolutely irreducible, meaning that $\overline{\rho} \otimes_k k'$ is irreducible for all finite extensions k'/k), then $\mathrm{Def}(\overline{\rho})$ is representable.*

For another example of representability of deformation functors, we review ordinary defomrations. Let K be a p-adic field, and let $\psi : G_K \to \mathbb{Z}_p^\times$ be the p-adic cyclotomic character. An n-dimensional representation ρ of G is said to be (distinguished) ordinary if there exist integers $e_1 > e_2 > \cdots > e_{n-1} > e_n = 0$ so that

$$\rho\mid_{I_K} \sim \begin{pmatrix} \psi^{e_1} & * & \cdots & * \\ 0 & \psi^{e_2} & \cdot & * \\ 0 & 0 & \ddots & * \\ 0 & 0 & \cdots & \psi^{e_n} = 1 \end{pmatrix}.$$

For fixed $e_1, \ldots, e_n$ which are distinct modulo $p-1$, the ordinary deformation functor $\mathrm{Def}^{\mathrm{ord}}(\overline{\rho})$ is the subfunctor of $\mathrm{Def}(\overline{\rho})$ consisting of only the distinguished ordinary lifts of $\overline{\rho}$ for that choice of $e_1, \ldots, e_n$.

Proposition 2. *If a two-dimensional residual representation $\overline{\rho}$ is non-split, then $\mathrm{Def}^{\mathrm{ord}}(\overline{\rho})$ is representable. More generally, if $\overline{\rho}$ is n-dimensional, and every 2×2 diagonal minor is non-split, then $\mathrm{Def}^{\mathrm{ord}}(\overline{\rho})$ is representable.*

Let's recall some properties of deformation rings. An important property of deformation rings is that they commute with finite extension of residue fields. That is, suppose k'/k is a finite extension. Let $\overline{\rho}$ be an absolutely irreducible residual representation of k; we can extend scalars to k' to get an absolutely irreducible residual representation of k'. Then, if $W(k)$ denotes the ring of Witt vectors over k, we have

$$R^{\square}(\overline{\rho}) \otimes_{W(k)} W(k') \cong R^{\square}(\overline{\rho} \otimes_k k'),$$
$$R(\overline{\rho}) \otimes_{W(k)} W(k') \cong R(\overline{\rho} \otimes_k k').$$

Suppose $\overline{\rho}$ is an absolutely irreducible residual representation of dimension N, and let $\det : \mathrm{GL}_N(k) \to \mathrm{GL}_1(k)$ be the determinant map. Then there is a natural homomorphism

$$R(\det(\overline{\rho})) \to R(\overline{\rho}).$$

More generally, if $\delta : \mathrm{GL}_N \to \mathrm{GL}_M$ is a homomorphism of group schemes, we get a natural map of deformation rings

$$R(\delta(\overline{\rho})) \to R(\overline{\rho}).$$

Deformation rings also commute with tensor products of representations. Let $\overline{\pi}, \overline{\rho}$ be two absolutely irreducible residual representations whose tensor product is also absolutely irreducible. Then we get a natural map

$$R(\overline{\pi} \otimes \overline{\rho}) \to R(\overline{\pi}) \widehat{\otimes} R(\overline{\rho}).$$

If $\overline{\pi}$ is a one-dimensional representation, i.e. a character, we call this map **twisting** by $\overline{\pi}$.

Deformation rings are also functorial in the choice of profinite group. Let $\phi : G \to G'$ be a group homomorphism, and let $\overline{\rho}$ be a residual representation of G'. Then composition with ϕ gives a residual representation of G. This gives us a map

$$R_G(\overline{\rho}) \to R_{G'}(\overline{\rho}).$$

An important example of deformations comes from looking at the Zariski tangent space. Let $k[\varepsilon]$ denote the dual numbers. If $F : \widehat{\mathcal{C}}_\Lambda \to \underline{\mathrm{Sets}}$ is a functor, its tangent space is $F(k[\varepsilon]) =: t_F$.

Let $V \in t_{\mathrm{Def}(\overline{\rho})}$. Then $V/\varepsilon V \cong \overline{\rho}$, so we have a short exact sequence

$$0 \to \varepsilon V \to V \to \overline{\rho} \to 0.$$

As G-modules, $\varepsilon V \cong \overline{\rho}$, so

$$t_{\mathrm{Def}(\overline{\rho})} \cong \mathrm{Ext}^1_{k[G]}(\overline{\rho}, \overline{\rho}) = H^1(G, \mathrm{Ad}(\overline{\rho})) = (\mathfrak{m}/(\mathfrak{m}, p))^2$$

for $\overline{\rho}$ absolutely irreducible. Here, $\mathrm{Ad}(\overline{\rho})$ is defined as follows: it is the representation of G whose underlying vector space is $M_N(k)$, and whose G-action is given by $g.m = \overline{\rho}(g)^{-1} m \overline{\rho}(g)$.

Let G be G_K if K is a local field, or $G_{K,S}$ for some finite set of places S if K is a global field. Fix a residual representation $\overline{\rho} : G \to \mathrm{GL}_n(k)$. If a deformation functor F for $\overline{\rho}$ is represented by R, then we have

$$t_F = F(k[\varepsilon]) = \mathrm{Hom}_\Lambda(R, k[\varepsilon]) = \mathrm{Hom}_\Lambda(R/(\mathfrak{m}_R^2 + \mathfrak{m}_\Lambda), k[\varepsilon]).$$

Since we also have

$$\frac{R}{\mathfrak{m}_R^2 + \mathfrak{m}_\Lambda} = k \oplus \frac{\mathfrak{m}_R}{\mathfrak{m}_R^2 + \mathfrak{m}_\Lambda},$$

and the second summand has square zero, we have

$$t_F = \mathrm{Hom}_k\left(\frac{\mathfrak{m}_R}{\mathfrak{m}_R^2 + \mathfrak{m}_\Lambda}, k\right) = t_R^*,$$

where for $A \in \widehat{\mathcal{C}}_\Lambda$, we set

$$t_A = \frac{\mathfrak{m}_A}{\mathfrak{m}_A^2 + \mathfrak{m}_\Lambda},$$

and t_A^* is its dual.

2. Why study Galois deformations?

We're mostly interested in the case of $G = G_{K,S}$ for some finite set of places S of a number field K. There are several reasons that this is a good idea.

(1) We can specify a residual representation $\overline{\rho} : G_{K,S} \to \mathrm{GL}_N(k)$ using only a finite amount of data, and there are only finitely many such representations, for K, S, N, and k fixed. When $\overline{\rho}$ is absolutely irreducible, we saw that we have a universal deformation, so all the lifts of $\overline{\rho}$ can be packaged together into a single complete noetherian local ring with residue field k.
(2) We might sometimes be interested in studying those deformations of $\overline{\rho}$ that have particular properties. For example, we mentioned ordinary deformations earlier. Another possibility that's relevant to us would be to look at modular deformations: those representations coming from modular forms. These correspond to quotients of the universal deformation ring. Placing such conditions on the representations at least conjecturally amounts to imposing local conditions at the ramified primes. We'll discuss this a bit more later.

3. Galois cohomology

We now review some cohomology of local fields. Let K be a finite extension of $\mathbb{Q}_p$, with Galois group G_K. Let μ be the roots of unity of K^s. If M is a finite G_K-module, set $M' = \mathrm{Hom}(M, \mu)$. Then for $0 \le i \le 2$, the cup product

$$H^i(K, M) \otimes H^{2-i}(K, M') \to H^2(K, \mu) \cong \mathbb{Q}/\mathbb{Z}$$

is a perfect pairing.

We have a similar statement when M is an ℓ-adic representation of G_K. Let ℓ be a prime, possibly equal to p, and let F be a finite extension of $\mathbb{Q}_\ell$. Suppose T is a free $\mathfrak{o}_F$-module with a continuous $\mathfrak{o}_F$-linear G_K-action, and let $V = T \otimes_{\mathfrak{o}_F} F$ be the corresponding $\mathbb{Q}_\ell$-vector space. Then G_K acts on V as well. Let V^* be the dual representation given by $V^* = \mathrm{Hom}_{\mathfrak{o}_F}(V, F(1))$. Then we have the following duality induced by the cup product: for $0 \le i \le 2$,

$$H^i(K, V) \otimes H^{2-i}(K, V^*) \to H^2(K, F(1)) \cong F$$

is a perfect pairing.

If M is a finite G_K-module, then $H^i(K, M)$ is a finite group for $0 \le i \le 2$, and $H^i(K, M) = 0$ for $i \ge 3$. Let $h^i(K, M)$ be the size of $H^i(K, M)$. Then, we define the Euler-Poincaré characteristic of M to be

$$\chi(M) = \frac{h^0(K, M) h^2(K, M)}{h^1(K, M)}.$$

We recall a few key properties of the Euler-Poincaré characteristic.

- If $0 \to M'' \to M \to M' \to 0$ is a short exact sequence of finite G_K-modules, then $\chi(M'')\chi(M') = \chi(M)$.
- If $(p, \#M) = 1$, then $\chi(M) = 1$.
- More generally, if $x \in \mathfrak{o}_K$, let $\|x\|_K$ be the normalized absolute value of x, so that
$$\|x\|_K = \frac{1}{(\mathfrak{o}_K : x\mathfrak{o}_K)}.$$
If $\#M = n$, then
$$\chi(M) = \|n\|_K = p^{-[K:\mathbb{Q}_p]\operatorname{ord}_p(n)}.$$

Sometimes, we wish to talk about Euler-Poincaré characteristics when the G_K-module is a $\mathbb{Q}_p$-vector space or free $\mathbb{Z}_p$-module. In that case, it would not make sense to talk about the sizes of the cohomology groups, but only about their ranks or dimensions. We can make sense of this in the case of finite modules instead, by talking of their ranks as $\mathbb{F}_p$-vector spaces. Let's write $\tilde{h}^i(K, M)$ for the dimension of $H^i(K, M)$ over $\mathbb{F}_p$, and write
$$\tilde{\chi}(M) = \tilde{h}^0(K, M) - \tilde{h}^1(K, M) + \tilde{h}^2(K, M).$$
Then the above result is equivalent to
$$\tilde{\chi}(M) = -[K : \mathbb{Q}_p]\operatorname{ord}_p(n).$$
If M is instead a $\mathbb{Q}_p$-vector space or a free $\mathbb{Z}_p$-module, we'll let $\tilde{h}^i(K, M)$ be the dimension or rank of $H^i(K, M)$ as a $\mathbb{Q}_p$-vector space or $\mathbb{Z}_p$-module, and we'll define the Euler-Poincaré characteristic similarly.

Let V now be a $\mathbb{Q}_p$-vector space of dimension d. Find inside V a G_K-stable lattice T. Since $T = \varprojlim T/p^rT$ and cohomology commutes with inverse limits, we have
$$H^i(K, T) = \varprojlim H^i(K, T/p^rT) \cong \varprojlim H^i(K, M_r),$$
where M_r is a G_K-module of size p^{dr}. By the above,
$$\tilde{\chi}(M_r) = -dr[K : \mathbb{Q}_p].$$
Taking inverse limits gives us
$$\tilde{\chi}(T) = -d[K : \mathbb{Q}_p].$$
Tensoring doesn't change the dimensions of the cohomology groups, so we also have
$$\tilde{\chi}(V) = -d[K : \mathbb{Q}_p].$$

4. Examples of Deformation Rings

It can be helpful to have a rough idea of what deformation rings look like. When they exist, they tend to be quotients of power series rings over $\mathbb{Z}_p$. Let's look at some examples.

Let S be a finite set of places of $\mathbb{Q}$, and let $\overline{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_p)$ be a representation. Let E be the fixed field of $\ker(\overline{\rho})$, and let $H = \mathrm{Gal}(E/\mathbb{Q})$. Let

$$V = \mathrm{coker}\left(\mu_p(E) \to \bigoplus_{v \in S} \mu_p(E_v)\right).$$

A $k[H]$-module W is said to be **prime-to-adjoint** if there is some subgroup A of H of order prime to p so that W and the adjoint $k[H]$-module M are relatively prime as $k[A]$-modules (so they share no common ireducible subrepresentations as A-modules).

Let Z_S be the set of $x \in \mathbb{Q}^\times$ so that (x) is a p^{th} power, and so that $x \in E_v^{\times p}$ for each $v \in S$. Then $E^{\times p} \subset Z_S$. Let $B = Z_S/E^{\times p}$ be the quotient $\mathbb{F}_p[H]$-module.

We say $\overline{\rho}$ is **tame** if the size of the image of $\overline{\rho}$ is prime to p. We say $\overline{\rho}$ is **regular** if it is absolutely irreducible, odd, and V and B are prime-to-adjoint.

Example. If $\overline{\rho}$ is tame and regular, then $R(\overline{\rho}) \cong \mathbb{Z}_p[\![T_1, T_2, T_3]\!]$.

For a concrete example, let E be the splitting field of $X^3 - X - 1$ over $\mathbb{Q}$. Then E is unramified away from 23 and ∞. The Galois group $\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$. Since S_3 has a faithful representation in $\mathrm{GL}_2(\mathbb{F}_{23})$, we get an absolutely irreducible residual representation

$$\overline{\rho} : G_{\mathbb{Q},\{23,\infty\}} \to \mathrm{GL}_2(\mathbb{F}_{23}).$$

Its universal deformation ring is isomorphic to $\mathbb{Z}_{23}[\![T_1, T_2, T_3]\!]$.

If $\overline{\rho}$ is irregular, the situation is a bit more complicated.

Consider the residual representation

$$\overline{\rho} : G_{\mathbb{Q},\{3,7,\infty\}} \to \mathrm{GL}_2(\mathbb{F}_3)$$

coming from the elliptic curve $X_0(49)$. Then the universal deformation ring is isomorphic to $\mathbb{Z}_3[\![T_1, T_2, T_3, T_4]\!]/((1 + T_4)^3 - 1)$.

Example. Let D be an integer congruent to $-1 \pmod 3$ and also $\pm$ a power of 2, and let $E/\mathbb{Q}$ be the elliptic curve defined by $y^2 = x(x^2 - 4Dx + 2D^2)$. Then E has complex multiplication by $\mathbb{Q}(\sqrt{-2})$. Let $S = \{2, 3\}$, and let $\overline{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_3)$ be the representation associated to E. Then $R(\overline{\rho}) \cong \mathbb{Z}_3[\![T_1, T_2, T_3, T_4, T_5]\!]/I$, where I is an ideal that takes a while to define.

We can give bounds on the number of (profinite) generators and relations it takes to present a deformation ring. Samit showed the following in his lecture in the fall:

Theorem 3. *Let K be a p-adic field, and let $G = G_K$ (for example). Let $r = \dim Z^1(G, \mathrm{Ad}(\overline{\rho}))$ and $s = \dim H^2(G, \mathrm{Ad}(\overline{\rho}))$. Then $R^\square(\overline{\rho})$ exists, and can be presented as*

$$R^\square(\overline{\rho}) \cong \mathfrak{o}_K[\![T_1, \dots, T_r]\!]/(f_1, \dots, f_s).$$

In the unframed case, we have $\dim R(\overline{\rho}) \geq 2 - \tilde{\chi}(G, \mathrm{Ad}(\overline{\rho}))$.

We also have

$$\dim(R/pR) \geq \dim H^1(G, \mathrm{Ad}(\overline{\rho})) - \dim H^2(G, \mathrm{Ad}(\overline{\rho})),$$

where the left side is the Krull dimension.

5. Characteristic zero points of deformation rings

Let S be a finite set of places of $\mathbb{Q}$. Fix an absolutely irreducible residual representation $\overline{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_N(k)$, and let $\rho : G_{\mathbb{Q},S} \to \mathrm{GL}_N(R)$ be its universal deformation. We saw earlier that R looks something like $\mathbb{Z}_p[\![x]\!]$, but $R[1/p]$ is still far from being a local ring: in the case of $R = \mathbb{Z}_p[\![x]\!]$, $R[1/p] = \mathbb{Z}_p[\![x]\!][1/p] \subsetneq \mathbb{Q}_p[\![x]\!]$, since the power series on the left side need to have as denominators bounded powers of p. There are many $\mathbb{Q}_p$-algebra homomorphisms $\mathbb{Z}_p[\![x]\!][1/p] \twoheadrightarrow \mathfrak{o}_K[1/p]$ for various finite extensions $K/\mathbb{Q}_p$, where the first map sends x to a uniformizer of K. Thus, $R[1/p]$ has lots of maximal ideals, in this case. Something similar holds for general universal deformation rings. The maximal ideals of $R[1/p]$ correspond to deformations of $\overline{\rho}$ landing in finite extensions of $\mathbb{Q}_p$.

If W is a complete DVR, and R is a quotient of a power series ring in several variables over W, and ϖ is a uniformizer of W, then $R[1/\varpi]/\mathfrak{m}$ is finite over $W[1/\varpi]$ for any $\mathfrak{m} \in \mathrm{MaxSpec}(R[1/\varpi])$.

We'd like to understand what $R[1/p]$ looks like. Let $R = W[\![x_1, \dots, x_n]\!]/(f_1, \dots, f_m)$. Then, for any finite extension A of W,

$$\mathrm{Hom}(R, A) = \mathrm{Hom}(R[1/p], A[1/p] = \mathrm{Frac}(A)),$$

where the first Hom is in the category of local W-algebras, and the second is in the category of $\mathrm{Frac}(W)$-algebras.

Proposition 4. *If K'/K is a finite extension, then any K-algebra map $R[1/p] \to K'$ is given by sending the X_i's to various $x_i \in \mathfrak{m}_{K'} \subset \mathfrak{o}_{K'} \subset K'$. Hence the image of R lands in the valuation ring.*

Fix such a map $x : R[1/p] \twoheadrightarrow K'$. Let

$$\rho_x : G \xrightarrow{\rho} \mathrm{GL}_N(R) \to \mathrm{GL}_N(R[1/p]) \to \mathrm{GL}_N(K')$$

be the induced representation. We'd like to understand $\dim R[1/p]_{\mathfrak{m}_x} = \dim R[1/p]^{\wedge}_{\mathfrak{m}_x}$.

Theorem 5. *Let* $\rho_x^{\text{univ}} : G \to \text{GL}_N(R[1/p]^\wedge_{\mathfrak{m}_x})$ *be induced from* ρ *by the natural map* $R \to R[1/p]^\wedge_{\mathfrak{m}_x}$. *Then the diagram*

$$\begin{array}{ccc} G & \xrightarrow{\rho_x^{\text{univ}}} & \text{GL}_N(R[1/p]^\wedge_{\mathfrak{m}_x}) \\ & \searrow^{\rho_x} & \downarrow \\ & & \text{GL}_N(K') \end{array}$$

commutes, and ρ_x^{univ} *is universal for continuous deformations of* ρ_x.

This theorem is relevant for (at least) two reasons:

(1) We have $R[1/p] \cong K'[\![T_1, \ldots, T_n]\!]$ if and only if each $R[1/p]^\wedge_{\mathfrak{m}_x}$ is regular, if and only if the deformation functor is formally smooth, if and only if $H^2(G, \text{Ad}(\rho_x)) = 0$.
(2) We have $(\mathfrak{m}_x/\mathfrak{m}_x^2)^\vee \cong H^1_{\text{cts}}(G, \text{Ad}(\rho_x))$ by the continuity condition on the deformations in the theorem.

Let $\rho : G = G_{\mathbb{Q},S} \to \text{GL}_n(K)$ for some p-adic field K be a representation with absolutely irreducible reduction. Then $H^1(G, \text{Ad}(\overline{\rho}))$ is also equal to the tangent space of the deformation ring $R(\overline{\rho})$ at the reduction of the closed point of $R[1/p]$ corresponding to ρ. Hence, the completion of $R[1/p]$ at that point (with scalars extended to K, if necessary), is the deformation ring for ρ.

6. Wiles product formula

Recall the definition of unramified cohomology. Let K be a p-adic field. If M is a K-module, then the unramified cohomology is

$$H^i_{nr}(K, M) = H^i(\text{Gal}(K^{nr}/K), M^{I_K}).$$

If K is a global field, then for every place v of K, we have a map $G_{K_v} \hookrightarrow G_K$, and if M is a G_K-module, we have a restriction map $H^i(G_K, M) \to H^i(G_{K_v}, M)$ for each i. Let $\mathcal{L} = (L_v)$ be a collection of subgroups $L_v \subset H^1(G_{K_v}, M)$ so that $L_v = H^1_{nr}(G_{K_v}, M)$ for almost all v. Let

$$H^1_{\mathcal{L}}(G_K, M) = \{c \in H^1(G_K, M) \mid \text{res}_v(c) \in L_v \text{ for all } v\}.$$

Let $\mathcal{L}^D = (L_v^D)$, where L_v^D is the annihilator of L_v under the Tate local pairing. We call the L_v the local conditions.

Theorem 6 (Wiles Product Formula)**.** *Suppose* M *is a finite* G_K*-module,* $M' = \text{Hom}(M, \mu)$*, and* $\mathcal{L}$ *is a family of local conditions. Then*

$$\frac{\#H^1_{\mathcal{L}}(K, M)}{\#H^1_{\mathcal{L}^D}(K, M')} = \frac{\#H^0(K, M)}{\#H^0(K, M')} \prod_v \frac{\#L_v}{\#H^0(K_v, M)}.$$

We'll soon get to situations in which the denominator on the left-hand side of the Wiles Product Formula is 1. Thus, we'll have a formula for the size of the global H^1 in terms of sizes of H^0 as well as local terms. The local terms we'll be able to compute by studying various local deformation rings.

7. Example

Note: I don't really understand this example. I more or less copied Brian's email, but I'm including it for other people, who can probably understand it.

Let K be a p-adic field (p odd), and let $\omega : G_K \to k^\times$ be the mod-p cyclotomic character. Let $\rho : G_K \to \mathrm{GL}(V)$ be a residual representation, where V is a 2-dimensional k-vector space. Suppose the inertia group I_K acts nontrivially on V. Then let D be the subspace fixed by I_K. With respect to a suitable basis, then, we have

$$\rho = \begin{pmatrix} \theta_2 & * \\ 0 & \theta_1 \end{pmatrix},$$

where θ_1 and θ_2 are characters. We can write θ_1 and θ_2 uniquely in the form

$$\theta_1 = \omega^\alpha \varepsilon_1, \qquad \theta_2 = \omega^\beta \varepsilon_2,$$

where $\alpha, \beta \in \mathbb{Z}/(p-1)\mathbb{Z}$, and ε_1 and ε_2 are unramified characters $G_K \to k$. Hence the restriction of ρ to I_K is

$$\rho\,|_{I_K} = \begin{pmatrix} \omega^\beta & * \\ 0 & \omega^\alpha \end{pmatrix}.$$

We can normalize the exponents so that $0 \le \alpha \le p-2$ and $1 \le \beta \le p-1$.

Definition 7. If $\beta \neq \alpha + 1$, we say that ρ is **peu ramifié**. If $\beta = \alpha + 1$, we say that ρ is **très ramifié**.

Let $\mathcal{L}$ be a line in $H^1(K, \omega)$ not in the peu ramifié hyperplane. Let $\mathcal{H}$ be its orthogonal hyperplane in $H^1(K, k)$ with respect to the Tate pairing. Thus, $\mathcal{H}$ is a hyperplane not containing the unramified line. We wish to find a ramified character $\psi : G_K \to \Lambda^\times$ of finite order on I_K that lifts the trivial residual character and so that the image of $H^1(K, \varepsilon\psi) \to H^1(K, \omega)$ contains $\mathcal{L}$, where $\varepsilon : G_K \to \mathbb{Z}_p^\times$ is the p-adic cyclotomic character. Varying through nonzero points of $\mathcal{L}$ gives us a collection of non-isomorphic non-split extensions of a common reducible but indecomposable G_K-module, so gluing them together gives us a lifting result for 2-dimensional Galois representations.

ψ allows for a lift of $\mathcal{L}$ if and only if $\mathcal{L}$ is in the kernel of the connecting map to $H^2(K, \varepsilon\psi)$. Let F be the fraction field of Λ, and let ϖ be a uniformizer. This happens if and only if connecting map

$$H^0(K, (F/\Lambda)(\psi^{-1})) \to H^1(K, k)$$

attached to the sequence

$$0 \to k \to (F/\Lambda)(\psi^{-1}) \xrightarrow{\varpi} (F/\Lambda)(\psi) \to 0$$

has image contained in $\mathcal{H}$. So, let's figure out exactly what the connecting map does in order to see what it means on the ramified character ψ^{-1} of finite order on I_K that the image is contained in some hyperplane not containing the unramified line.

If $x = u\varpi^{-n}$ for $n > 0$ and $u \in \Lambda^*$, we have $x \in H^0(K, (F/\Lambda)(\psi^{-1}))$ if and only if $\psi^{-1} \equiv 1 \pmod{\varpi^n}$. Since ψ (and hence ψ^{-1}) is nontrivial, this only works for finitely many values of n, but including $n = 1$. The image of x under this connecting map is the k-torsor of points

$$(u\varpi^{-n})(\varpi^{-1} + \Lambda) \mod \Lambda,$$

and the corresponding character $G_K \to k = \varpi^{-1}\Lambda/\Lambda$ is

$$\phi_n : g \mapsto (\varpi^{-1} + \Lambda)((\psi^{-1}(g) - 1)\varpi^{-n}) \mod \Lambda = (\psi^{-1}(g) - 1)\varpi^{-n-1} \mod \Lambda.$$

Note that $(\psi^{-1}(g) - 1)\varpi^{-n} \in \Lambda$, and if n is not maximal with respect to this property, then $\phi_n = 0$. If we write

$$\psi^{-1} = 1 + \varpi^n \chi$$

and $\chi_0 = \chi \mod \varpi$, then χ_0 is a nontrivial character $G_K \to k$, and $1 + \varpi^n\chi$ restricted to I_K is valued in the p^{th} power roots of unity in $\Lambda^\times$. The condition on ψ^{-1} is that χ_0 is contained in $\mathcal{H} \subset H^1(K, k)$.

More concretely, this is equivalent to the following. Let $\mathcal{H}$ be a hyperplane in $H^1(K, k)$ not containing the unramified line. We seek a continuous character $\xi : G_K \to 1 + \mathfrak{m}_\Lambda$ with finite order on I_K and conductor $n > 0$ so that the nonzero additive character $(\xi - 1)\varpi^{-n} : G_K \to k$ lies in $\mathcal{H}$. This character *must* be ramified. We could have replaced ϖ^n with $u\varpi^n$ for any $u \in \Lambda^\times$.

In order to make the construction, we need to start with a Λ containing a primitive p^{th} root of unity ζ. Let $n = e/(p-1)$, where $e = e(\Lambda)$, so that $\zeta - 1 = \varpi^n$. Fix a nontrivial character $\xi : \mathfrak{o}_K^\times \to \mu_p$, and extend it to an order p character ϕ on G_K by class field theory, so that $\phi \equiv 1 \mod \mathfrak{m}_A^n$. The function

$$\chi = \frac{\phi - 1}{\zeta - 1} : G_K \to k$$

is an additive character that is not identically zero, and it is ramified: there is an element $\tau \in I_K$ taken to ζ^{-1}.

If $\chi \in \mathcal{H}$, we're done. If not, then $\mathcal{H}$ is a hyperplane not containing the unramified line, so any element not in $\mathcal{H}$ can be translated by a unique unramified k-valued character so that it does lie in $\mathcal{H}$. For a unit $u_0 \equiv 1 \mod \mathfrak{m}_A^{e/(p-1)}$, twisting by the unramified character taking Frob to u_0 has the effect of adding to χ the unramified character taking Frob to $(u_0 - 1)/(\zeta - 1)$. Varying u_0, this sweeps through all the unramified characters $G_K \to k$, so we can hit the one we need to land in $\mathcal{H}$.