1. Universal Deformation Ring (cont’d)

1.1. Witt Vectors (cont’d). We call $W(k)$ the ring of Witt vectors. Note that by construction $W(F_\ell) \simeq \mathbb{Z}_\ell$. Sometimes it is helpful to consider the vectors $W_n(k)$ of finite length $n$ i.e. the $\mathbb{Z}_\ell$-linear combinations of $(x_1, \ldots, x_n)$; by construction $W_n(F_\ell) \simeq \mathbb{Z}/\ell^n\mathbb{Z}$. In fact $W(k) = \varprojlim_n W_n(k)$.

The Witt vectors satisfy a canonical universal property. Let $K/\mathbb{Q}_\ell$ be a finite extension, $\mathcal{O}$ be the integral closure of $\mathbb{Z}_\ell$ in $K$, and $\lambda$ be the prime in $\mathcal{O}$ lying above $\ell$ in $\mathbb{Z}_\ell$. The residue field $k = \mathcal{O}/\lambda$ is a finite extension of $F_\ell$, so denote $e = [K : \mathbb{Q}_\ell]/[k : F_\ell]$ as the ramification index of $\ell$ in $\mathcal{O}$. There exists a injection $W(k) \hookrightarrow \mathcal{O}$ mapping $m \mapsto \lambda$, and $\mathcal{O}$ is a free $W(k)$-module of rank $e$. In particular, if we are given a residual representation $\overline{\rho} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_d(F_\ell)$ then any lift $\rho$ to characteristic 0 such that we have the composition

$$\overline{\rho} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho} GL_d(\mathcal{O}) \xrightarrow{\mod \lambda} GL_d(k)$$

implies $\mathcal{O}$ must be a $W(k)$-algebra. Of course, we still haven’t shown that such a lift exists!

1.2. Representability of the Deformation Functor. Fix a $d$-dimensional residual representation $\overline{\rho}$ as above. I claim that there exists a “versal deformation” $\rho^{\text{univ}} : G_Q \to GL_d(R(\overline{\rho}))$ of $\overline{\rho}$ in the sense that if $\rho : G_Q \to GL_2(\mathcal{O})$ is any deformation of $\overline{\rho}$ then there exists a $\mathcal{O}$-algebra homomorphism $\phi : R(\overline{\rho}) \to \mathcal{O}$ such that $\rho \simeq \phi \circ \rho^{\text{univ}}$. Moreover, if $\overline{\rho}$ is absolutely irreducible i.e. the group ring $F_\ell[G_Q(\overline{\rho})]$ is irreducible, then the word “versal” can be replaced by “universal” and the homomorphism $\phi$ is unique.

We sketch the proof given by Barry Mazur. Consider the functor

$$\mathcal{D}_{\overline{\rho}} : \left\{\begin{array}{l}
\text{Artinian } W(k)\text{-algebras } A \\
\text{having residue field } k \text{ along with a } W(k)\text{-homomorphism } A \to W(k) \\
\text{local } W(k)\text{-homomorphism } A \to W(k)
\end{array}\right\} \to \left\{\begin{array}{l}
\text{equivalence classes of deformations } \rho_A \\
\text{of } \overline{\rho}
\end{array}\right\}.$$ 

First let me explain what this means. Recall that an Artinian ring is one which satisfies the descending chain condition – whereas a Noetherian ring is one which satisfies the ascending chain condition. Canonical examples of Artinian $W(k)$-algebras are $A = \mathcal{O}/\lambda^n$ with maximal ideal $m_A = \lambda^{n-1}/\lambda^n$. Note that in this case the residue field is $A/m_A \simeq \mathcal{O}/\lambda \simeq k$. A local homomorphism $\phi : A \to W(k)$ is one such that $m_A = \phi^{-1}(m)$ and $\phi : A/m_A \to W(k)/m$ is an isomorphism. By a deformation $\rho_A : G_Q \to GL_2(A)$ we mean a continuous homomorphism such that $\overline{\rho} \simeq \rho_A \mod m_A$. Note that such a map must be surjective, since

$$[W(k) : \text{im}(\phi)] = \frac{\# (W(k)/m)}{\# (\text{im}(\phi)/\text{im}(m_A))} = \frac{\# (W(k)/m)}{\# (A/m_A)} = \frac{\# k}{\# k} = 1.$$
We say this functor is representable if there exists a complete, local Noetherian $W(k)$-algebra $R(\bar{\rho})$ depending only on the representation $\bar{\rho}$ such that

$$D_{\bar{\rho}}(A) \simeq \text{Hom}_{W(k)}(R(\bar{\rho}), A).$$

If this is the case, then the image $D_{\bar{\rho}}(R(\bar{\rho}))$ associated with the trivial homomorphism $R(\bar{\rho}) \rightarrow R(\bar{\rho})$ corresponds to a deformation $\rho^{\text{univ}}$ of $\bar{\rho}$. Moreover, the isomorphism above implies that any image $D_{\bar{\rho}}(A)$ may be associated with a unique surjective $W(k)$-algebra homomorphism $\phi_A : R(\rho) \rightarrow A$, so that $\rho_A \simeq \phi_A \circ \rho^{\text{univ}}$.

When $A = \mathcal{O}/\Lambda^n$ we have the inverse limit

$$\mathcal{O} = \text{proj lim}_{n \to \infty} \mathcal{O}/\Lambda^n \Rightarrow \rho \simeq \phi \circ \rho^{\text{univ}}$$

where $\phi : R_{\Sigma} \rightarrow \mathcal{O}$, so that the proposition follows. Hence it suffices to show that $D_{\bar{\rho}}$ is representable when $\bar{\rho}$ is absolutely irreducible. If $\bar{\rho}$ is not absolutely irreducible, the functor will have a pro-representable hull, in which case we say $R(\bar{\rho})$ is a versal deformation ring. One can prove all of this using Schlessinger’s Criteria.

1.3. Examples of Universal Deformation Rings. Let me give an example first constructed by Mazur. For integers $n$ consider the cubic polynomial $x^3 - nx + 1$ such that the discriminant $-\ell = 4n^3 - 27$ is prime. (When $n = 1$ we find $\ell = 23$.)

Then the Galois group of this polynomial is $S_3$, the symmetric group of three letters. Upon choosing an embedding $S_3 \rightarrow GL_2(\mathbb{F}_3)$, this gives a residual representation $\bar{\rho} : G_{\mathbb{Q}} \rightarrow S_3 \rightarrow GL_2(\mathbb{F}_3)$, and so the universal deformation ring is $R(\bar{\rho}) = \mathbb{Z}_\ell[T_1, T_2, T_3]$ as a polynomial ring in three variables.

In general, fix a finite set of places $S$ containing those where $\bar{\rho}$ is ramified, and denote $G_S = \text{Gal} (\mathbb{Q}_S/\mathbb{Q}) = \text{proj lim}_L \text{Gal} (L/\mathbb{Q})$ as the projective limit over those finite Galois extensions $L/\mathbb{Q}$ where the places $v \in S$ are unramified. (In the examples above $S = \{\ell, \infty\}$.) Mazur shows that if for the residual representation $\bar{\rho} : G_S \rightarrow GL_2(k)$ if $H^2(G_S, \text{ad} \bar{\rho}) = \{0\}$ – that is, the deformation problem is unobstructed – then $R(\bar{\rho}) = W(k)[T_1, T_2, \ldots, T_r]$ where $r = \dim_k H^1(G_S, \text{ad} \bar{\rho})$.

Moreover, Mazur shows that if $\bar{\rho}$ is odd i.e. $\det \rho : G_{\infty} \rightarrow \{\pm 1\}$ is nontrivial, then $r = 3$. We sketch the ideas. Say we have a deformation $\rho_A : G_S \rightarrow GL_d(A)$, and an Artinian $A$-algebra $B$ along with a surjective local homomorphism $\phi : B \rightarrow A$. We wish to construct a deformation $\rho_B$ as in the following diagram:

$$
\begin{align*}
G_S & \xrightarrow{\rho_B} GL_d(B) & \mod {m_B} & GL_d(k) \\
\downarrow \phi & & & \\
G_S & \xrightarrow{\rho_A} GL_d(A) & \mod {m_A} & GL_d(k)
\end{align*}
$$

For $\sigma \in G_S$ choose matrices $\alpha(\sigma) \in GL_d(B)$ such that $\alpha(\sigma) \equiv \bar{\rho}(\sigma) \mod m_B$. Then $\xi(\sigma_1, \sigma_2) = \alpha(\sigma_1) \circ \alpha(\sigma_2)^{-1} \in I \otimes \text{ad} \bar{\rho}$ where $I = \ker[B \rightarrow A]$. One easily checks that $\xi \in H^2(G_S, \text{ad} \bar{\rho}) \otimes I = \{0\}$ so that such a bona fide representation $\rho_B$ can be constructed. (Ravi Ramakrishna, a student of Mazur, has observed that one can always enlarge $\Sigma$ so that $H^2(G_S, \text{ad} \bar{\rho}) = \{0\}$.

Unfortunately this allows more ramification in the lifts $\rho$ of $\bar{\rho}$.)

2. Selmer Groups and Deformation Problems

Fix a continuous residual 2-dimensional representation $\bar{\rho} : G_{\mathbb{Q}} \rightarrow GL_2(k)$. Note that the continuity of this representation implies that we may assume $k$ is a finite
extension of $F_\ell$. Assume that there exists a continuous lift $\rho : G_{\mathbb{Q}} \to GL_2(O)$ to characteristic 0 i.e. the following composition holds:

$$
\overline{p} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho} GL_2(O) \xrightarrow{\text{mod } \lambda} GL_2(k).
$$

Note that if $K$ is the field of fractions of $O$ then the continuity of $\rho$ implies $K$ is a finite extension of $\mathbb{Q}_\ell$. We will state a precise definition of a deformation of $\overline{p}$, and then prove that such deformations exist – under suitable conditions.

Now say $\ell \neq 2$. We have seen in the previous lecture that equivalence classes of infinitesimal deformations $\overline{p}_v$ of $\overline{p}$ correspond to cohomology classes in $H^1(G_{\mathbb{Q}}, \text{ad}^0\overline{p})$. We will impose local conditions to gather even more information. Eventually, we will define subgroups $H^1_\Sigma(G_{\nu}, \text{ad}^0\overline{p}) \subseteq H^1(G_{\nu}, \text{ad}^0\overline{p})$ for each place $\nu$ of $\mathbb{Q}$ that will encode information about infinitesimal deformations.

### 2.1. Deformations of Type $\Sigma$.

Say that we are given a continuous $\ell$-adic representation

$$
\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\overline{\mathbb{Q}}_\ell).
$$

By the continuity of $\rho$, we know the image lies in $GL_2(K)$ for some finite extension $K/\mathbb{Q}_\ell$, and we can even conjugate $\rho$ so that $\rho : G_{\mathbb{Q}} \to GL_2(O)$ where $O$ is the ring of integers in $K$.

Fix a finite set of primes $\Sigma$; such a set may be the empty set. Let $O'$ be another complete, local Noetherian algebra with field of fractions $K'$, maximal ideal $\mathfrak{p}'$, and residue field $k' = O'/\mathfrak{p}'$. We say that a continuous representation $\rho' : G_{\mathbb{Q}} \to GL_2(O')$ is a deformation of $\overline{p}$ of type $\Sigma$ if

1. $\rho' \simeq \overline{p} \otimes_k k'$ (residually the same),
2. $\det \rho' = \det \rho$ (strict equivalence), and
3. $\rho'|_{\mathfrak{p}_{\nu}} \simeq \rho|_{\mathfrak{p}_{\nu}} \otimes_K K'$ for all $\nu \notin \Sigma$ (minimally ramified).

We strengthen (3) above by placing special conditions on the local representations at $\nu = \ell$. Any local residual representation $\overline{p} : G_\ell \to GL_2(k)$ has a group ring $\mathbb{F}_\ell[\rho(G_\ell)]$. If this ring is irreducible we say $\overline{p}|_{G_\ell}$ is absolutely irreducible, or that $\overline{p}$ is supersingular at $\ell$. Otherwise, we say $\overline{p}$ is ordinary at $\ell$. In the ordinary case, the restriction of $\overline{p}$ to $G_\ell$ is upper-triangular:

$$
\overline{p}|_{G_\ell} \simeq \begin{pmatrix} \chi_\ell & * \\ 0 & \chi_0 \end{pmatrix} \quad \text{where} \quad \chi_\ell \cdot \chi_0 = \det \overline{p}, \quad \chi_0|_{I_\ell} = 1.
$$

Hence, we force the deformation to be in that same form:

$$
\rho'|_{G_\ell} \simeq \begin{pmatrix} \chi_\ell & * \\ 0 & \chi_0 \end{pmatrix} \quad \text{where} \quad \chi_\ell = \det \rho \cdot \chi_0^{-1} \quad \text{and} \quad \chi_0|_{I_\ell} = 1 \quad \text{(ordinariness)}.
$$

We give a couple of examples. As one, if $\overline{p} = \overline{p}_{E,\ell}$ is associated to an elliptic curve which is ordinary at $\ell$ then $\chi_\ell = \epsilon_\ell$ mod $\ell$ is the mod $\ell$ cyclotomic character while $\chi_0 = 1$ is trivial. As another, if $\overline{p}$ is the mod $\ell$ reduction of a complex representation which is ordinary at $\ell$ then $\chi_\ell|_{I_\ell} = \chi_0|_{I_\ell} = 1$ when $\det \overline{p}$ is unramified at $\ell$. We say that $\overline{p}$ is wildly ramified if $*|_{I_\ell} \neq 1$.

As for the supersingular case, there is a fundamental character defined by

$$
\overline{\varphi}_\ell : I_\ell \xrightarrow{\sigma - \sigma(\mathfrak{N})/\mathfrak{N}} \mu_N \longrightarrow \mathbb{F}_\ell^\times \quad \text{where} \quad N = \ell^2 - 1
$$

$\overline{\varphi}_\ell^*$.
such that $\rho|_{I_\ell}$ has eigenvalues $\tilde{\phi}_\ell^n$ and $\tilde{\phi}_\ell^n \ell$ i.e.

$$(\rho|_{I_\ell})^{ss} \simeq \begin{pmatrix} \tilde{\phi}_\ell^n & 0 \\ 0 & \tilde{\phi}_\ell^n \ell \end{pmatrix}.$$ 

For example, if $\rho = \rho_{E,\ell}$ is associated to an elliptic curve which is supersingular at $\ell$ then $n \equiv 1 \mod N$ and $\det \rho|_{I_\ell} = \tilde{\phi}_\ell^{1+\ell} = \tau_{\ell}$ is the mod $\ell$ cyclotomic character. In fact, if $E$ is unramified at $\ell$ we say $\rho$ is finite flat at $\ell$. If $\rho$ is the mod $\ell$ reduction of a complex representation which is supersingular at $\ell$ then $n \equiv \ell - 1 \mod N$ and $\det \rho|_{I_\ell} = \tilde{\phi}_\ell^{n(1+\ell)} = 1$ when $\det \rho$ is unramified at $\ell$.

In the next lecture we will translate the condition of being an infinitesimal deformation of type $\Sigma$ into local conditions on cohomology classes.