MATH 849 NOTES
FERMAT'S LAST THEOREM

LECTURES BY NIGEL BOSTON

Contents

Date: Spring 2018.

1. 2018-01-29: Inverse systems and limits; profinite completion

Last time, we outlined Wiles' strategy.

1.1. Dramatis Personae.

(1) Profinite groups (e.g. $G_{\mathbb{Q}}, G_{\mathbb{Q}_p}, \dots$) and complete local rings (e.g. $\mathcal{R}$ and $\mathbb{T}$)
(2) Galois representations and their properties
(3) Elliptic curves, modular forms, and their associated Galois representations
(4) Deformation theory
(5) Commutative algebra
(6) Galois cohomology
(7) L-functions of symmetric squares
(8) Null case (and reduction to it)
(9) 3-5 switch

1.2. Profinite groups and complete local rings.

Definition 1.1. A *directed set* I is a partially ordered set such that for all $i, j \in I$, there exists $k \in I$ such that $k \geq i$ and $k \geq j$.

Example 1.2 (Standard examples)**.** (1) Let G be any group. Index the normal subgroups of G by I, where $i \geq j \iff N_i \subseteq N_j$. Given i, j, we can take $N_k = N_i \cap N_j$.
(2) Let R be a commutative ring (with 1). Do the same with ideals of R of finite index.
(3) Replace "finite index" with any property closed under subquotients and direct products.
(4) Let K be a field. Index finite Galois extensions L_i of K by I. Set $i \geq j \iff L_i \subseteq L_j$. This is a directed set since we can take the compositum of any two finite Galois extensions.

Definition 1.3. An *inverse system* of groups is a collection $(G_i)_{i \in I}$ indexed by a directed set I, together with homomorphisms $\pi_{ij} \colon G_i \to G_j$ whenever $i \geq j$ such that $\pi_{ii} = \mathrm{id}_{G_i}$ and $\pi_{jk} \circ \pi_{ij} = \pi_{ik}$ whenever $i \geq j \geq k$.

Example 1.4. Let G be a group, and let I index the set of normal subgroups of G. Let $G_i = G/N_i$ for each $i \in I$. If $i \geq j$, then $N_i \subseteq N_j$ and we have a natural quotient map $G/N_i \to G/N_j$. Call this π_{ij}.

Note that this has the further property that, whenever $i \geq j$, we have a commutative diagram

$$\begin{tikzcd}
 & G \arrow[dl] \arrow[dr] & \\
G/N_i \arrow[rr, "\pi_{ij}"] & & G/N_j.
\end{tikzcd}$$

Example 1.5. Let K be a field, and let I index the set of finite Galois extension of G. Let $G_i = \mathrm{Gal}(L_i/K)$ for each $i \in I$. If $i \geq j$, then $L_i \supseteq L_j$, and π_{ij} is the restriction map $\mathrm{Gal}(L_i/K) \to \mathrm{Gal}(L_j/K)$.

Definition 1.6 (Category associated to inverse system)**.** Given an inverse system of groups $(G_i)_{i\in I}$, define a category whose objects $(H, (\phi_i)_{i\in I})$ consist of a group H and, for each $i \in I$, a homomorphism $\phi_i \colon H \to G_i$ such that, whenever $i \geq j$, the diagram

$$\begin{tikzcd}
& H \arrow[ld, "\phi_i"'] \arrow[rd, "\phi_j"] & \\
G_i \arrow[rr, "\pi_{ij}"] & & G_j
\end{tikzcd}$$

commutes. A morphism

$$(H, (\phi_i)_{i\in I}) \to (K, (\psi_i)_{i\in I})$$

in this new category is a group homomorphism $H \to K$ such that for all $i \in I$, the diagram

$$\begin{tikzcd}
H \arrow[rr] \arrow[rd, "\phi_i"'] & & K \arrow[ld, "\psi_i"] \\
& G_i &
\end{tikzcd}$$

commutes.

Definition 1.7. The *inverse limit* of the inverse system (G_i), denoted $\varprojlim_{i\in I} G_i$, is the *terminal object* of the above category, i.e., the unique object $(X, (\chi_i)_i)$ such that there is exactly one morphism to it from any object.

Theorem 1.8. *The above category always has a terminal object, i.e., the category of groups admits limits of all inverse systems.*

Proof. Given $(G_i)_{i\in I}$, let $C = \prod_{i\in I} G_i$, and let $\pi_i \colon C \to G_i$ be the i-th projection. Let

$$X = \{c \in C : \pi_{ij}(\pi_i(c)) = \pi_j(c)\ \forall i \geq j\},$$

and let $\chi_i = \pi_i|_X$. Note that X is a subgroup of C, so X is a group. Whenever $i \geq j$, the diagram

$$\begin{tikzcd}
& C \arrow[ld, "\chi_i"'] \arrow[rd, "\chi_j"] & \\
G_i \arrow[rr, "\pi_{ij}"] & & G_j
\end{tikzcd}$$

commutes by construction. So $(X, (\chi_i))$ is an object of the category. Next, say $(H, (\phi_i))$ is also an object, and consider a morphism

$$(H, (\phi_i)) \to (X, (\chi_i))$$

given by a homomorphism $\phi \colon H \to X$. Then $\phi(h)$ has to be $(\phi_i(h))_{i\in I}$, so this is the unique morphism $(H, (\phi_i)) \to (X, (\chi_i))$. Hence $(X, (\chi_i))$ is the terminal object. □

Example 1.9 (Profinite completion)**.** For each $i \geq 1$, let $G_i = \mathbb{Z}/i$. Say $i \geq j$ if $j \mid i$. If $i \geq j$, then there is a natural map $\mathbb{Z}/i \to \mathbb{Z}/j$. (This is standard example (1) with $G = \mathbb{Z}$.) Then

$$\varprojlim \mathbb{Z}/i = \{(a_1, a_2, \dots) : a_i \in \mathbb{Z}/i \text{ and } j \mid i \implies a_i = a_j \pmod{j}\}.$$

This is called $\hat{\mathbb{Z}}$, the *profinite completion* of $\mathbb{Z}$. More generally, given a group G,

$$\hat{G} = \varprojlim_{\substack{N_i \trianglelefteq G \\ \text{fin. index}}} G/N_i$$

is called the profinite completion of G.

Note that $\mathbb{Z} \hookrightarrow \hat{\mathbb{Z}}$, and $\hat{\mathbb{Z}}$ is uncountable. In general, there is a unique morphism $G \to \hat{G}$ compatible with the inverse system, but this is not always an injection. For example, $\hat{\mathbb{Q}} = 0$ because the additive group of $\mathbb{Q}$ is divisible.

Remark 1.10. Teaser: note that $\hat{G} \to \hat{\hat{G}}$ need not be an isomorphism.

2. 2018-01-31: Topology of inverse limits; complete local rings

2.1. Topology of inverse limits.

As before, let $(G_i)_{i \in I}$ be an inverse system with morphisms $\pi_{ij} \colon G_i \to G_j$ whenever $i \geq j$.

Suppose all G_i are finite. Give each G_i the discrete topology, $\prod_{i \in I} G_i$ the product topology, and $X = \varprojlim G_i \leq \prod_i G_i$ the subspace topology.

Each G_i is Hausdorff, compact, and totally disconnected, hence the product $\prod_i G_i$ is also Hausdorff, compact (by Tychonoff's theorem), and totally disconnected. Since X is a closed subspace of $\prod_i G_i$, it follows that X is also Hausdorff, compact, and totally disconnected.

So the profinite group $\varprojlim G_i$ is a compact, Hausdorff, and totally disconnected topological group.

Remark 2.1. If H is an open subgroup of a profinite group G, then the set of cosets of H is an open cover of G. By compactness, there are finitely many cosets, i.e., $[G : H] < \infty$.

The converse is false: subgroups of finite index are not always open. One can construct a counterexample in $\prod_{n \geq 1} \mathbb{Z}/2$ using ultrafilters.

Theorem 2.2 (Nikolov–Segal)**.** *If G is* topologically finitely generated *(i.e., G has a dense finitely generated subgroup), then every subgroup of finite index is open.*

Example 2.3. The image of $\mathbb{Z}$ is dense in $\hat{\mathbb{Z}}$, so $\hat{\mathbb{Z}}$ is topologically finitely generated (despite being uncountable, and hence not even countably generated as an abstract group).

2.2. Example: Galois groups of finite fields.

Consider finite Galois extensions of $\mathbb{F}_q$. For every positive integer n, there is exactly one extension of degree n, denoted $\mathbb{F}_{q^n}$. These form a directed set: $i \geq j \iff \mathbb{F}_{q^j} \subseteq \mathbb{F}_{q^i} \iff j \mid i$. Let $\bar{\mathbb{F}}_q = \bigcup_{n \geq 1} \mathbb{F}_{q^n}$, the algebraic closure of $\mathbb{F}_q$. We have restriction maps

$$\begin{tikzcd} & \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) \arrow[dl] \arrow[dr] & \\ \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q) \arrow[rr] & & \mathrm{Gal}(\mathbb{F}_{q^j}/\mathbb{F}_q). \end{tikzcd}$$

So we get a unique homomorphism

$$\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) \to \varprojlim_i \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q) \cong \varprojlim \mathbb{Z}/i \cong \hat{\mathbb{Z}}.$$

Claim 2.4. *This is an isomorphism and sends the Frobenius map ($x \mapsto x^q$) to $1 \in \hat{\mathbb{Z}}$.*

Theorem 2.5. *Let L/K be an algebraic Galois extension (so separable). Then*

$$\mathrm{Gal}(L/K) \cong \varprojlim_{\substack{L_i/K \mathit{fin.} \\ \mathit{Gal.\ subexts}}} \mathrm{Gal}(L_i/K).$$

Proof. As above, we have restriction maps

$$\begin{tikzcd}
& \mathrm{Gal}(L/K) \arrow[dl, "\phi_i"'] \arrow[dr, "\phi_j"] & \\
\mathrm{Gal}(L_i/K) \arrow[rr] & & \mathrm{Gal}(L_j/K)
\end{tikzcd}$$

whenever $L_i \supseteq L_j$. We get, as before, a unique homomorphism

$$\phi\colon \mathrm{Gal}(L/K) \to \varprojlim_i \mathrm{Gal}(L_i/K).$$

First we show injectivity. Let $g \in \mathrm{Gal}(L/K)$ such that $g \neq 1$. Then $g(x) \neq x$ for some $x \in L$. Since $L = \bigcup_i L_i$, there exists i such that $x \in L_i$. So $\phi_i(g) = g|_{L_i} \neq \mathrm{id}_{L_i}$, which means $\phi(g) = (\phi_i(g))_i \neq \mathrm{id}$.

Now we show surjectivity. Let $(g_i) \in \varprojlim \mathrm{Gal}(L_i/K)$ be arbitrary. For $x \in L$, we need to define $g(x)$. Pick i such that $x \in L_i$, and define $g(x) = g_i(x)$. This is well-defined because (G_i) is a directed set and $g_i|_{L_j} = g_j$ whenever $L_i \supseteq L_j$. One can check that $g \in \mathrm{Gal}(L/K)$, completing the proof. □

2.3. **Complete local rings.** Let R be a commutative ring (with 1). Let $I \subseteq R$ be an ideal. Using $\pi_{ij}\colon R/I^i \to R/I^j$ (defined when $i \geq j$), we have an inverse system of rings, and can define as above a topological ring

$$R_I = \varprojlim_i R/I^i.$$

This is called the *I-adic completion* of R.

Example 2.6. Let $R = \mathbb{Z}$ and $I = p\mathbb{Z}$, where p is a prime. Then

$$\mathbb{Z}_p = \varprojlim_i \mathbb{Z}/p^i = \{(a_1, a_2, \dots) : a_i \in \mathbb{Z}/p^i, a_i \equiv a_j \pmod{p^i} \text{ if } i \geq j\},$$

the ring of *p-adic integers*. Note that $\hat{\mathbb{Z}} = \prod_{p \text{ prime}} \mathbb{Z}_p$.

Remark 2.7. If I is maximal, as in the above example, then R_I is a local ring (i.e., R_I has a unique maximal ideal). For example, $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$, and $p\mathbb{Z}_p$ is the unique maximal ideal of $\mathbb{Z}_p$.

If k is a finite field, we'll be interested in the category $\mathscr{C}_k$ of complete Noetherian local rings R with residue field $R/\mathfrak{m}_R \cong k$.

By a theorem of Cohen, the objects of $\mathscr{C}_k$ are of the form $W(k)[[T_1, \dots, T_m]]\,/(\text{ideal})$, where $W(k)$ is the ring of infinite Witt vectors of k. (For example, $W(\mathbb{F}_p) = \mathbb{Z}_p$, and $W(k)$ is the initial object of $\mathscr{C}_k$.) Every ring in $\mathscr{C}_k$ is a $W(k)$-algebra.

Example 2.8 (Hida, 1983)**.** There are representations $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p[[T]])$ such that composing with

$$\begin{aligned} \mathbb{Z}_p[[T]] &\to \mathbb{Z}_p \\ T &\mapsto (1+p)^{k-1} - 1 \end{aligned}$$

yields representations $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$ associated with a weight k modular form. Note that $\mathbb{Z}_p[[T]]$ is in $\mathscr{C}_{\mathbb{F}_p}$, and has maximal ideal (p, T).

3. 2018-02-02: Topology of inverse limits; complete local rings

We intend to study certain continuous $\rho : G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ and R a complete local ring ($W(k)[[T_1, \cdots, T_m]]$/ideal for a finite field k). Last time, we saw that $G_{\mathbb{Q}}$ is a profinite group and saw its topology. Note that $\mathrm{GL}_2(R_I) \simeq \varprojlim \mathrm{GL}_2(R/I^n)$ is also profinite.

Remark 3.1. Let L/K be a Galois extension. Then not every subgroup of $\mathrm{Gal}(L/K)$ is necessarily $\mathrm{Gal}(L/M)$ for some intermediate field M.

Example 3.2. Consider the Frobenius map $\phi \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$, $\phi : x \mapsto x^q$. (In fact $G_{\mathbb{F}_q}$ is topologically generated by ϕ, i.e. ϕ generates a dense subgroup of $G_{\mathbb{F}_q}$.) Then the fixed field of ϕ is $\mathrm{Fix}(\phi) = \{x \in \bar{\mathbb{F}}_q \mid x^q = x\} = \mathbb{F}_q$. Every subgroup between $\langle\phi\rangle \subsetneq G_{\mathbb{F}_q}$ has fixed field $\mathbb{F}_q$.

One can show that $\mathrm{Fix}(H) = \mathrm{Fix}(\bar{H})$ for any subgroup $H \subseteq \mathrm{Gal}(L/K)$ and we have a Galois correspondence

$$\{\text{closed subgroups of } \mathrm{Gal}(L/K)\} \longleftrightarrow \{\text{intermediate fields between } K \text{ and } L\}.$$

Note that if $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(R)$ is continuous, then $\ker\rho = \rho^{-1}(\{1\})$ is a closed normal subgroup of $G_{\mathbb{Q}}$, so $\ker\rho = \mathrm{Gal}(\bar{\mathbb{Q}}/M)$ and $\mathrm{im}\,\rho \simeq \mathrm{Gal}(M/\mathbb{Q})$.

Remark 3.3. In a profinite group G, every open subgroup is closed. This is because G is the disjoint union of H and all the nontrivial cosets of H, where the union of nontrivial cosets of H is the union of finitely many open subgroups.

Example 3.4. Let L be the compositum of all quadratic extensions of $\mathbb{Q}$. Then $\mathrm{Gal}(L/\mathbb{Q}) \simeq \prod_I \mathbb{Z}/2$ for $I = \{\text{primes}\} \cup \{-1\}$.

Recall $\mathbb{Z}_p = \{(a_1, a_2, \cdots) \mid a_i \in \mathbb{Z}/p^i, a_i \equiv a_j (\mathrm{mod}\ p^j) \text{ if } i \geq j\}$. We have projections $\mathbb{Z}_p \to \mathbb{Z}/p^i$ with kernel $p^i\mathbb{Z}_p$ and

$$\mathbb{Z}_p \supset p\mathbb{Z}_p \supset p^2\mathbb{Z}_p \supset \cdots .$$

Definition 3.5. The p-adic valuation is defined to be $v_p : \mathbb{Z}_p \to \{0, 1, 2, \cdots\} \cup \{+\infty\}$ by $v_p(x) = n$ if $x \in p^n\mathbb{Z}_p - p^{n+1}\mathbb{Z}_p$ and $v_p(x) = +\infty$ if $x = 0$.

Exercise 3.6. x is a unit in $\mathbb{Z}_p$ if and only if $v_p(x) = 0$.

Corollary 3.7. *Every nonzero element x of $\mathbb{Z}_p$ can be written as $p^{v_p(x)} \cdot u$ for a unit u.*

Lemma 3.8. *v_p has the following properties.*

(1) $v_p(xy) = v_p(x) + v_p(y)$

(2) $v_p(x + y) \geq \min(v_p(x), v_p(y))$ and the equality holds if $v_p(x) \neq v_p(y)$.

Corollary 3.9. *$\mathbb{Z}_p$ is an integral domain.*

Definition 3.10. The p-adic metric on $\mathbb{Z}_p$ is given by

$$d_p(x, y) = \begin{cases} c^{v_p(x-y)} & \text{if } x \neq y \\ 0 & \text{if } x = y, \end{cases}$$

where $0 < c < 1$ (usually $c = \frac{1}{p}$).

By this definition, $p^n\mathbb{Z}_p = \{x \mid d_p(x,y) \leq c^n\}$. Let $\mathbb{Q}_p$ be the field of fractions of $\mathbb{Z}_p$. Note that v_p extends to a valuation on $\mathbb{Q}_p$, i.e. a homomorphism $\mathbb{Q}_p^\times \to \mathbb{Z}$. The following diagram yields a restriction map $G_{\mathbb{Q}_p} \hookrightarrow G_{\mathbb{Q}}$, which is a continuous homomorphism defined up to conjugacy.

$$\begin{tikzcd}
\bar{\mathbb{Q}} \arrow[r, hook] & \bar{\mathbb{Q}}_p \\
\mathbb{Q} \arrow[r, hook] \arrow[u, hook] & \mathbb{Q}_p \arrow[u, hook] \\
\mathbb{Z} \arrow[r, hook] \arrow[u, hook] & \mathbb{Z}_p \arrow[u, hook]
\end{tikzcd}$$

Given a continuous homomorphism $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(R)$, for each prime p, by composition we obtain $\rho_p : G_{\mathbb{Q}_p} \to \mathrm{GL}_2(R)$. The representations ρ_p for primes p are called the local data associated to ρ. (Presentations of $G_{\mathbb{Q}_p}$ are given by Jannsen and Winberg for very odd prime p.)

Next, we'll understand the structure of

$$G_{\mathbb{Q}_p} = \varprojlim_{\substack{K/\mathbb{Q}_p \text{ finite} \\ \text{Galois}}} \mathrm{Gal}(K/\mathbb{Q}_p).$$

Let K be a finite Galois extension of $\mathbb{Q}_p$.

Definition 3.11. A *discrete valuation* w on a field K is a surjective hom $w : K^\times \to \mathbb{Z}$ such that $w(x+y) \geq \min(w(x), w(y))$ for every $x, y \in K$ and $w(0) = +\infty$.

Let $A = \{x \in K \mid w(x) \geq 0\}$ and $\mathfrak{m} = \{x \in K \mid w(x) \geq 0\}$. Then one can check that A is a ring with a unique maximal ideal $\mathfrak{m}$ (so it's a local ring) K is the field of fractions of A. If $w(\pi) = 1$, then we call π a uniformizer. So $\mathfrak{m} = (\pi)$ and every element $x \in K$ can be uniquely written as $\pi^{w(x)}u$ where $u \in A - \mathfrak{m}$ is a unit. $A/\mathfrak{m}$ is a field, that we call the residue field of K.

Exercise 3.12. Understand v_p for $K = \mathbb{Q}_p$. ($A = \mathbb{Z}_p$, $\pi = p$ and $A/\mathfrak{m} = \mathbb{F}_p$).

Again, let K be a finite Galois extension of $\mathbb{Q}_p$ and set $n = [K : \mathbb{Q}_p]$. We have the norm map

$$\begin{array}{rcl} N : K^\times & \to & \mathbb{Q}_p^\times \\ x & \mapsto & \displaystyle\prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q}_p)} \sigma(x). \end{array}$$

Compose this with v_p, we get a homomorphism $K^\times \xrightarrow{N} \mathbb{Q}_p^\times \xrightarrow{v_p} \mathbb{Z}$. The image of this composition is nonzero (since the image of $x \in \mathbb{Q}_p$ is $v_p(x^n) = nv_p(x)$), so it has finite index in $\mathbb{Z}$, which implies it's $f\mathbb{Z}$ for some integer $f \neq 0$.

Define $w(x) = \frac{v_p(N(x))}{f}$. (Then one can check $w(x+y) \geq \min(w(x), w(y))$.) $e = \frac{n}{f}$ is the ramification index of $K/\mathbb{Q}_p$.

Claim 3.13. *w is the unique discrete valuation on K.*

The main idea to show this claim is that two norms on a finite dimensional complex vector space are equivalent. By this claim, we have $w(\sigma(x)) = w(x)$ for any $x \in K, \sigma \in \mathrm{Gal}(K/\mathbb{Q}_p)$.

Exercise 3.14. $|A/\mathfrak{m}| = p^f$.

4. 2018-02-05: Topology of inverse limits; complete local rings

Last time, we obtained continuous homomorphisms $G_{\mathbb{Q}_p} \to G_{\mathbb{Q}}$ for every prime p. So given $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(R)$, we obtain associated representations $\rho_p : G_{\mathbb{Q}_p} \to \mathrm{GL}_2(R)$. We therefore wish to understand $G_{\mathbb{Q}_p}$.

Let $K/\mathbb{Q}_p$ be a finite Galois extension with $G = \mathrm{Gal}(K/\mathbb{Q}_p)$. Last time, we introduced valuation $w : K^\times \to \mathbb{Z}$, and we let $A = \{x \in K \mid w(x) \geq 0\}$, $\mathfrak{m} = \{x \in K \mid w(x) > 0\}$, $k = A/\mathfrak{m}$.

4.1. **Ramification Groups.** Let $G_i = \{\sigma \in G \mid w(\sigma(x) - x) \geq i+1, \forall x \in A\}$ for $i = -1, 0, 1, \cdots$.

Claim 4.1. *$G_i \trianglelefteq G$.*

Proof. We first show G_i is a subgroup of G. It's clear that $1 \in G_i$. Let σ, τ be elements in G_i. Then

$$\begin{aligned} w(\sigma(\tau(x)) - x) &= w(\sigma(\tau(x) - x) + (\sigma(x) - x)) \\ &\geq \min(w(\sigma(\tau(x) - x)), w(\sigma(x) - x)) \\ &= \min(w(\tau(x) - x), w(\sigma(x) - x)) \geq i + 1. \end{aligned}$$

where the equality on the last line follows by $w \circ \sigma = w$. Thus, $\sigma \circ \tau \in G_i$ and hence G_i is a subgroup of G.

It suffices to show that G_i is normal in G. Let $\tau \in G_i$ and $\sigma \in G$.

$$w(\sigma\tau\sigma^{-1}(x) - x) = w(\sigma(\tau\sigma^{-1}(x) - \sigma^{-1}(x)) \geq i + 1.$$

So $G_i \trianglelefteq G$. □

So now we have a filtration of normal subgroups

$$G = G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \cdots, \text{ with } \cap_i G_i = \{1\}.$$

We call G_0 the inertia subgroup and G_1 the wild inertia subgroup.

Exercise 4.2. $G_i = \{\sigma \in G \mid w(\sigma(\pi) - \pi) \geq i + 1\}$ where π is a uniformizer (i.e. $w(\pi) = 1$).

Theorem 4.3. *(1) $G/G_0 \simeq \mathrm{Gal}(k/\mathbb{F}_p)$*
(2) $G_0/G_1 \hookrightarrow k^\times$; and $G_i/G_{i+1} \hookrightarrow k^+$ if $i \geq 1$.

Corollary 4.4. *G/G_0 is cyclic. G_0/G_1 is cyclic of order prime to p. For $i \geq 1$, G_i/G_{i+1} is elementary p-abelian (that is a direct product of $\mathbb{Z}/p$).*

Proof of Theorem 4.3. (1) Given $\sigma \in G$, σ acts on A and on $\mathfrak{m}$, so it acts on the residue field $A/\mathfrak{m} = k$. Consider the following group homomorphism

$$\begin{aligned} \phi : G &\to \mathrm{Gal}(k/\mathbb{F}_p) \\ \sigma &\mapsto (x + \mathfrak{m} \mapsto \sigma(x) + \mathfrak{m}) \end{aligned}$$

Note that $\ker\phi = \{\sigma \in G \mid \sigma(x) - x \in \mathfrak{m}\} = G_0$. So $G/G_0 \hookrightarrow \mathrm{Gal}(k/\mathbb{F}_p)$. As for sujectivity, let $k = \mathbb{F}_p(\bar{a})$ where $a \in A$ maps to $\bar{a}$. Let $p(x)$ be the monic polynomial $\prod_{\sigma\in G}(x - \sigma(a))$. Its image in k is $\bar{p}(x) = \prod_{\sigma\in G}(\overline{x - \sigma(a)}) \in k[x]$. For every $\tau \in \mathrm{Gal}(k/\mathbb{F}_p)$, $\tau(\bar{a})$ has to be a root of $\bar{p}(x)$, so $\tau(\bar{a}) = \overline{\sigma(a)}$ for some σ, hence we see $\sigma \mapsto \tau$ under ϕ.

(2)

$$\begin{aligned} \sigma \in G_i &\iff w(\sigma(\pi) - \pi) \geq i+1 \\ &\iff w(\frac{\sigma(\pi)}{\pi} - 1) \geq i \\ &\iff \frac{\sigma(\pi)}{\pi} \in 1 + (\pi)^i =: U_i \end{aligned} \tag{4.1}$$

(U_i's form a filtration of the units of A.) Consider the map

$$\begin{aligned} \theta_i : G_i &\to U_i/U_{i+1} \\ \sigma &\mapsto \frac{\sigma(\pi)}{\pi} \pmod{U_{i+1}}. \end{aligned}$$

θ_i is independent of the choice of π. Say $\pi' = \pi \cdot u$ for a unit u. Since $\sigma \in G_i$, $w(\sigma(u) - u) \geq i+1$ implies $w(\frac{\sigma(u)}{u} - 1) \geq i+1$, so $\frac{\sigma(u)}{u} \in U_{i+1}$ and $\frac{\sigma(\pi')}{\pi'} = \frac{\sigma(\pi)}{\pi} \cdot \frac{\sigma(u)}{u} \equiv \frac{\sigma(\pi)}{\pi}$ (mod U_{i+1}).

Also θ_i is a homomorphism, since

$$\frac{\sigma\tau(\pi)}{\pi} = \frac{\sigma(\pi)}{\pi} \cdot \frac{\tau(\pi)}{\pi} \cdot \frac{\sigma(u)}{u} \equiv \frac{\sigma(\pi)}{\pi} \cdot \frac{\tau(\pi)}{\pi} \pmod{U_{i+1}},$$

where $u = \frac{\tau(\pi)}{\pi}$ is a unit.

$$\sigma \in \ker \theta_i \iff \frac{\sigma(\pi)}{\pi} \in U_{i+1} \iff \sigma \in G_{i+1},$$

so $G_i/G_{i+1} \hookrightarrow U_i/U_{i+1}$. If $i = 0$, then $U_0/U_1 \simeq k^\times$ since the map $x \mapsto x$ (mod $\mathfrak{m}$) has kernel U_1. When $i \geq 1$, $U_i/U_{i+1} \simeq (\pi)^i/(\pi)^{i+1}$ since the homomorphism mapping $1 + x \in U_i$ to x (mod $(\pi)^{i+1}$) has kernel U_{i+1}. Note that $(\pi)^i/(\pi)^{i+1}$ is an $A/\mathfrak{m}$-module, and it is 1-dimensional as there is no ideal between $(\pi)^i$ and $(\pi)^{i+1}$, so $(\pi)^i/(\pi)^{i+1} \simeq k^+$. □

$$\begin{tikzcd}
G_{-1} \arrow[r, "="] & \mathrm{Gal}(K/\mathbb{Q}_p) \\
G_0 \arrow[u, hook, "\text{cyclic quotient}"] & \\
G_1 \arrow[u, hook, "\text{cyclic quotient of order prime to } p"] & \\
\{1\} \arrow[u, hook, "G_1 \text{ is a } p\text{-group}"] &
\end{tikzcd}$$

Corollary 4.5. *G is solvable. G_0 has a normal Sylow p-subgroup with cyclic quotient.*

4.2. **Application to Galois representations.** Say $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(k)$ is a continuous homomorphism, where k is a finite field with characteristic ℓ. Then we get $\rho_\ell : G_{\mathbb{Q}_\ell} \to \mathrm{GL}_n(k)$, and the image of ρ_ℓ is $\mathrm{Gal}(K/\mathbb{Q}_\ell)$ for some finite Galois extension $K/\mathbb{Q}_\ell$.

Theorem 4.6. *If ρ_ℓ is semisimple (i.e. a direct sum of irreducible representations), then $\rho_\ell(G_1) = \{1\}$, so ρ_ℓ factors through $G_{\mathbb{Q}_\ell}/G_1$.*

Proof. Let $V = k^n$. Assume ρ_ℓ is irreducible. Then $\rho_\ell(G_1)$ is the wild inertia subgroup of $\mathrm{Gal}(K/\mathbb{Q}_\ell)$. Consider $V' = \{v \in V \mid v^g = v, \forall g \in \rho_\ell(G_1)\}$. We want to show $V' = V$.

$\rho_\ell(G_1)$ is an ℓ-group, so every orbit in V has length a power of ℓ. So $|V'| \equiv |V| \equiv 0 \pmod{\ell}$ $\iff V' \neq \{0\}$. Since $\rho_\ell(G_1) \trianglelefteq \mathrm{Gal}(K/\mathbb{Q}_\ell)$, we see that V' is stable under $\mathrm{Gal}(K/\mathbb{Q}_\ell)$. Then it follows by the irreducibility of ρ_ℓ that $V' = V$ and $\rho_\ell(G_1) = \{1\}$. □

We have the following group extension

$$1 \to G_0/G_1 \to G/G_1 \to G/G_0 \to 1.$$

$G/G_0 = \mathrm{Gal}(k/\mathbb{F}_p)$ acts on $G_0/G_1 \hookrightarrow k^\times$ by the natural action of $\mathrm{Gal}(k/\mathbb{F}_p)$ on k. So we obtain $G/G_1 \simeq \langle x, y \mid xyx^{-1} = x^p, \cdots \rangle$. (Fact: Iwasawa showed that $xyx^{-1} = x^p$ is the only relation.)

5. 2018-02-07: Ramification groups on the absolute galois group

We turn to defining the ramification groups G_0 and G_1 for the group $G_{\mathbb{Q}_p}$. With many fields in the picture, we will introduce the following notation for this section. Given a finite Galois extension $K/\mathbb{Q}_p$, let $w_K : K^* \to \mathbb{Z}$ be the normalized valuation on K, let A_K be the integers of K, and let $G_i^{(K)}$ be the i^{th} ramification group in $\mathrm{Gal}(K/\mathbb{Q}_p)$.

Let M, L be finite extensions of $\mathbb{Q}_p$ such that $\mathbb{Q}_p \subseteq M \subseteq L$. We have the restriction map

$$\mathrm{Gal}(L/\mathbb{Q}_p) \xrightarrow{\text{res}} \mathrm{Gal}(M/\mathbb{Q}_p)$$

For arbitrary i, $G_i^{(L)}$ need not map to $G_i^{(M)}$ under this restriction map. The numbering system used for these ramification groups does not respect the action of taking quotients. One fix for this is to introduce the upper numbering of the ramification groups. However, for $i = 0, 1$, the restriction map does send

Theorem 5.1. *For $i = 0, 1$, $\mathrm{res}(G_i^{(L)}) = G_i^{(M)}$.*

Proof. For $i = 0$, the main point is that w_L is a positive integer multiple of w_M. If $\sigma \in Gm_0^{(L)}$, then $w_L(\sigma(x) - x) > 0$ for all $x \in A_L$. For $y \in A_M \subseteq A_L$, this implies that $w_M(\sigma(y) - y) > 0$.

We refer the reader to [Con] to show that the restriction map is surjective onto $G_0^{(M)}$.

To see that $G_1^{(M)}$ is the image of $G_1^{(L)}$, use the fact that under a surjective map, a Sylow p subgroup is taken to a Sylow p subgroup. □

We have just shown that the systems $(G_0^{(K)})$ and $(G_1^{(K)})$ as K ranges through the finite Galois extensions of $\mathbb{Q}_p$ with restriction maps form a compatible system as in the definition of inverse limit. From this, we will define the inertia group I_p and the group G_1 on the whole of $G_{\mathbb{Q}_p}$ as follows, where in each case the projective limit runs over finite Galois extensions of $\mathbb{Q}_p$.

$$I_p := \varprojlim_{K/\mathbb{Q}_p} G_0^{(K)} \qquad G_1 := \varprojlim_{K/\mathbb{Q}_p} G_1^{(K)}$$

Theorem 5.2. *(a)*

$$G_{\mathbb{Q}_p}/I_p \cong G_{\mathbb{F}_p} \cong \hat{\mathbb{Z}}$$

(b)

$$I_p/G_1 \cong \varprojlim_{k/\mathbb{F}_p \text{ finite}} k^\times \cong \prod_{q \neq p} \mathbb{Z}_q$$

(c) G_1 is a pro p-group.

(d) $G_{\mathbb{Q}_p}$ is topologically generated by x, y where the image of x in $G_{\mathbb{Q}_p}/I_p$ is the distinguished generator Frob_p (see note following this Theorem), y generates I_p/G_1 and $x^{-1}yx = y^p$.

Note 5.3. Under the isomorphisms in part (a) of this Theorem, we will define Frob_p as the coset in $G_{\mathbb{Q}_p}/I_p$ whose image in $G_{\mathbb{F}_p}$ is the Frobenius map $x \mapsto x^p$ or equivalently whose image in $\hat{\mathbb{Z}}$ is 1.

The maps for the inverse system in part (b) of this Theorem are the norm maps.

Sketch. For each finite Galois extension $K/\mathbb{Q}_p$ with residue field k, we have a map

$$\phi_K : G_{\mathbb{Q}_p}/I_p \twoheadrightarrow \operatorname{Gal}(K/\mathbb{Q}_p)/G_0^{(K)} \cong \operatorname{Gal}(k/\mathbb{F}_p)$$

Claim 5.4. *For each extension $k/\mathbb{F}_p$, there exists a unique $\phi : G_{\mathbb{Q}_p}/I_p \to \operatorname{Gal}(k/\mathbb{F}_p)$*

Proof of Claim. For existence, suppose $|k| = q$. Let ζ denote a primitive $(q-1)^{\text{st}}$ root of unity and define $L := \mathbb{Q}_p(\zeta)$. Then $k_L = \mathbb{F}_p(\zeta) = k$.

The point of the uniqueness is that different local fields can have the same residue field. Suppose L, M are local fields with $k_L = k_M = k$. Look at the compositum LM and consider the map ϕ_{LM} making the following diagram commute.

$$\begin{tikzcd}
G_{\mathbb{Q}_p}/I_p \arrow[r, "\phi_{LM}"] \arrow[dr] & \operatorname{Gal}(k_{LM}/\mathbb{F}_p) \arrow[d, two heads] \\
 & \operatorname{Gal}(k/\mathbb{F}_p)
\end{tikzcd}$$

As $\operatorname{Gal}(k_{LM}/\mathbb{F}_p)$ is cyclic, the quotient map to $\operatorname{Gal}(k/\mathbb{F}_p)$ is uniquely determined and so we get the unique map from $G_{\mathbb{Q}_p}/I_p \to \operatorname{Gal}(k/\mathbb{F}_p)$. □

In the new category for inverse limits, the group $G_{\mathbb{Q}_p}/I_p$ together with the above maps is an object, hence there is a unique map $G_{\mathbb{Q}_p}/I_p \to \varprojlim_k \operatorname{Gal}(k/\mathbb{F}_p)$ which is an isomorphism.

For part (b) of the theorem, suppose $M \subseteq L$ are both finite Galois extensions of $\mathbb{Q}_p$. Then, the restriction map $G_0^{(L)} \to G_0^{(M)}$ makes the following diagram commute.

$$\begin{tikzcd}
G_0^{(L)}/G_1^{(L)} \arrow[r, hook] \arrow[d] & k_L^\times \arrow[d, "\mathrm{Nm}"] \\
G_0^{(M)}/G_1^{(M)} \arrow[r, hook] & k_M^\times
\end{tikzcd}$$

Claim 5.5. *Given a finite extension $k/\mathbb{F}_p$, there exists a finite Galois extension $L/\mathbb{Q}_p$ such that $k_L \cong k$ and $G_0^{(L)}/G_1^{(L)} \cong k^\times$.*

Proof. Suppose $|k| = q$ and let ζ be a primitive $(q-1)^{\text{st}}$ root of unity. Let $L = \mathbb{Q}_p(\zeta, p^{\frac{1}{q-1}})$. □

From the above, we get the isomorphism $I_p/G_1 \to \varprojlim k^\times$.

Claim 5.6.

$$\varprojlim k^\times \cong \prod_{q \neq p} \mathbb{Z}_q$$

Proof. Consider another inverse system. For $(n,p)=1$, define μ_n by

$$\mu_n = \{x \in \overline{\mathbb{F}_p} : x^n = 1\}$$

where, if $m \mid n$, there is a map

$$\begin{aligned} \mu_n &\to \mu_m \\ x &\mapsto x^{\frac{n}{m}} \end{aligned}$$

Exercise 5.7. Show that $\varprojlim k^\times \cong \varprojlim \mu_n$. (Hint: Use the fact that for a given n with $(n,p)=1$, we have that $n \mid p^f - 1$ for some integer f).

Then, as each $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$, the claim follows. □

Part (c) of the theorem follows from Corollary 4.4.

For part (d), for any finite Galois $L/\mathbb{Q}_p$, the map $G_0^{(L)}/G_1^{(L)} \hookrightarrow k_L^\times$ is $\mathrm{Gal}(L/\mathbb{Q}_p)$ equivariant. Therefore, the map $I_p/G_1 \to \varprojlim k^\times$ is $G_{\mathbb{Q}_p}$ equivariant. □

Turning back to the big picture, we will encounter continuous representations $\rho : G_\mathbb{Q} \to \mathrm{GL}_2(R)$. Restricting this map to $G_{\mathbb{Q}_p} \subseteq G_\mathbb{Q}$ gives us a representation $\rho_p : G_{\mathbb{Q}_p} \to \mathrm{GL}_2(R)$ (only defined up to conjugacy, since $G_{\mathbb{Q}_p}$ is defined as a subgroup of $G_\mathbb{Q}$ up to conjugacy). To say that ρ satisfies a certain property at p will mean that ρ_p satisfies that property.

Definition 5.8. A representation $\rho_p : G_{\mathbb{Q}_p} \to \mathrm{GL}_2(R)$ is unramified if $\rho_p(I_p) = \{1\}$.

Note that if ρ is unramified at p, then $\rho(\mathrm{Frob}_p)$ is a well defined conjugacy class, $\rho(\mathrm{Frob}_p)$ determines ρ_p and the trace and determinant of $\rho(\mathrm{Frob}_p)$ are well defined and are important!

6. 2018-02-09: Galois representations from elliptic curves; group schemes

We will study naturally occurring Galois representations. These will have the property that they are unramified except for a finite set of primes.

Let $E : y^2 = f(x)$ be an elliptic curve over $\mathbb{Q}$. That is to say, $f(x) \in \mathbb{Q}[x]$ is cubic and has distinct roots in $\overline{\mathbb{Q}}$.

Definition 6.1. For a number field K, define the set of K points of E as

$$E(K) := \{(x,y) \in K^2 : y^2 = f(x)\} \cup \{\infty\}$$

The point at infinity is the point $[0:1:0] \in \mathbb{P}_K^2$ that we obtain from homogenizing the equation from E. Here, we review facts from the theory of elliptic curves.

- **Fact 1**: $E(K)$ is an abelian group with ∞ acting as the identity.

  The group law is defined so that $P+Q+R=\infty$ whenever $P,Q,R \in E(K)$ are collinear. This group law has the property that the coordinates of $P+Q$ can be explicitly given in terms of the coordinates of P, the coordinates of Q, and the coefficients of f.

  There are a few different ways to prove Fact 1.
  - The equations defining the group law can be plugged into a computer algebra system. There are a few different cases based on whether or not P and Q are equal, or the line between them intersects the curve in affine space or at infinity.
  - Using the theory of doubly periodic functions, it can be shown that $E(\mathbb{C})$ is isomorphic to $\mathbb{C}/\Lambda$ for $\Lambda \subseteq \mathbb{C}$ a lattice.

  - It can be shown that E is in bijection with $\mathrm{Pic}^0(E)$, the group of degree 0 line bundles on E, which forms a group under tensor product.
- **Fact 2**: As topological spaces, $E(\mathbb{C}) \cong S^1 \times S^1$.

  Definition 6.2. For an integer n, define the n-torsion points of E as
  $$E[n] = \{P \in E(\mathbb{C}) : nP = \infty\} \leq E(\mathbb{C})$$
  Fact 2 implies that $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ as groups.

  Example 6.3. Suppose $f(x)$ factors as $f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ with $\alpha_i \in \overline{\mathbb{Q}}$. Then,
  $$E[2] = \{\infty, (\alpha_1, 0), (\alpha_2, 0), (\alpha_3, 0)\}$$
  Since $G_{\mathbb{Q}}$ acts on $\{\alpha_1, \alpha_2, \alpha_3\}$, we have an action of $G_{\mathbb{Q}}$ on $E[2]$ or equivalently a map $G_{\mathbb{Q}} \to \mathrm{Aut}(E[2]) \cong S_3$. The image of this representation is $\mathrm{Gal}(K/\mathbb{Q})$ where K is a splitting field of f.

- **Fact 3**: $E[n] \subseteq E(\overline{\mathbb{Q}})$ and $G_{\mathbb{Q}}$ acts on $E[n]$.
  This gives us Galois representations $\rho_{E,n} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.
  For ℓ a prime, and n an integer, the following diagram commutes
  $$\begin{tikzcd} & G_{\mathbb{Q}} \arrow[dl] \arrow[dr] & \\ \mathrm{GL}_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z}) \arrow[rr] & & \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}). \end{tikzcd}$$
  And therefore, we get the ℓ-adic representation
  $$\rho_{E,\ell^\infty} : G_{\mathbb{Q}} \to \varprojlim_n \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z}_\ell)$$
  .
  For most elliptic curves E, ρ_{E,ℓ^∞} is surjective for every ℓ.
- **Fact 4**: There exists $N \in \mathbb{N}$ such that ρ_{E,ℓ^∞} is unramified at p for every $p \nmid N\ell$.
  For such p, we have that
  $$\mathrm{tr}(\rho_{E,\ell^\infty}(\mathrm{Frob}_p)) = p + 1 - \#\widetilde{E}(\mathbb{F}_p)$$
  $$\det(\rho_{E,\ell^\infty}(\mathrm{Frob}_p)) = p.$$
  We note that both quantities do not depend on ℓ.

To study an elliptic curve over $\mathbb{Q}$, we saw that we also needed to consider the set of K points for a number field K. An elliptic curve gives us a way to associate an abelian group for every number field K. We generalize this idea with the notion of a group scheme.

Let R be a commutative ring with 1.

Definition 6.4. An R-algebra is a commutative ring A together with a map $\pi_A : R \to A$. A map between R-algebras A and B is a map of rings $f : A \to B$ such that the following commutes
$$\begin{tikzcd} A \arrow[rr, "f"] & & B \\ & R \arrow[ul, "\pi_A"] \arrow[ur, "\pi_B"'] & \end{tikzcd}$$

Definition 6.5. A functor $G : \{R\text{-algebras}\} \to \{\text{Groups}\}$ is representable if there exists an R-algebra $\mathcal{R}$ such that $G(-) \cong \mathrm{Hom}_{R-\mathrm{alg}}(\mathcal{R}, -)$.

Definition 6.6. An affine group scheme G over R is a representable functor $G : \{R\text{-algebras}\} \to \{\text{Groups}\}$.

Example 6.7. The additive group is the functor $\mathbb{G}_a$ defined by $\mathbb{G}_a(A) = A$, the additive group of A.

This functor is representable by the R-algebra $R[T]$, since $\mathrm{Hom}_{R-\mathrm{alg}}(R[T], A) \cong A$. We note that this is only an isomorphism of sets. We leave it to the reader to determine a group structure on $\mathrm{Hom}_{R-\mathrm{alg}}(R[T], A)$ giving the additive group of A. The reader should use the map

$$\begin{aligned} R[T] &\to R[T] \otimes_R R[T] \\ T &\mapsto T \otimes 1 + 1 \otimes T \end{aligned}$$

Example 6.8. The functor $\mathbb{G}_m$ defined by $\mathbb{G}_m(A) = A^\times$, the group of units of A. This functor is represented by the ring $R[X, Y]/(XY - 1)$, because an R-algebra homomorphism $R[X, Y]/(XY - 1)$ to A is determined by the image of X and Y, call them a and b respectively. Since $ab = 1$, we have that a and b are units and moreover a determines b.

Example 6.9. SL_n is an affine group scheme, represented by the ring $R[X_{11}, \ldots, X_{nn}]/(\det(X_{ij}) - 1)$.

Example 6.10. GL_n is an affine group scheme, represented by the ring $R[X_{11}, \ldots, X_{nn}, Y]/(\det(X_{ij})Y - 1)$.

Example 6.11. For an R-algebra A, let $\mu_n(A) = \{x \in A : x^n = 1\}$. Then, μ_n is an affine group scheme, represented by the ring $R[T]/(T^n - 1)$.

Furthermore, since $\mu_n(A) \leq \mathbb{G}_m(A)$ for any R-algebra A, we say that μ_n is a subgroup scheme of $\mathbb{G}_m$.

7. 2018-02-12: Galois representations associated to elliptic curves; group schemes

Last time, we introduced Galos representations associated to elliptic curves E over $\mathbb{Q}$. Moreover, we introduced affine group schemes over a commutative ring R with 1 as representable functors from R-Algebras to Groups.

We will now study how group schemes produce Galois representations.

Example 7.1. Suppose R is a field K and $\ell \neq charK$ is prime. Then G_K acts continuously on $\mu_{\ell^n}(\overline{K})$. As a group, $\mu_{\ell^n}(\overline{K}) \cong \mathbb{Z}/\ell^n$. So we get the representation:

$$\chi_{\ell^n} : G_K \to (\mathbb{Z}/\ell^n)^\times = GL_1(\mathbb{Z}/\ell^n)$$

Explicitly, $\sigma(\zeta) = \zeta^{\chi_{\ell^n}(\sigma)}$, where $\sigma \in G_K$ and $\zeta \in \mu_{\ell^n}(\overline{K})$. We call χ_{ℓ^n} a cyclotomic character.

Moreover, for every n, we have the following commutative diagram:

$$\begin{tikzcd} & \mathbb{G} \arrow[dl, "\chi_{\ell n+1}"'] \arrow[dr, "\chi_{\ell^n}"] & \\ GL_1(\mathbb{Z}/\ell^{n+1}) \arrow[rr, "\text{reduction mod } \ell^n"'] & & GL_1(\mathbb{Z}/\ell^n) \end{tikzcd}$$

so the universal property of inverse limits yields (unique)

$$\chi_{\ell^\infty} : G_K \to \varprojlim_n GL_1(\mathbb{Z}/\ell^n) = GL_1(\mathbb{Z}_\ell) = \mathbb{Z}_\ell^\times.$$

Since $\mathbb{Z}_\ell$ is the initial object of $\mathscr{C}_{\mathbb{F}_\ell}$, for any ring A in $\mathscr{C}_{\mathbb{F}_\ell}$, we have a unique $\mathbb{Z}_\ell$-algebra homomorphism $\mathbb{Z}_\ell \to A$. Therefore, composition with χ_{ℓ^∞} gives a cyclotomic character $\chi : \mathbb{G} \to GL_1(\mathbb{Z}_\ell) \to GL_1(A)$.

Example 7.2. Let $K = \mathbb{Q}$ and ℓ any prime. We have $\chi_{\ell^\infty} : \mathbb{G}_\mathbb{Q} \to GL_1(\mathbb{Z}_\ell)$.

Claim 7.3. *χ_{ℓ^∞} is unramified at every prime $p \neq \ell$.*

For $p \neq \ell$, $\chi_{\ell^\infty}(Frob_p) = p$, since $Frob_p(\zeta) = \zeta^p$. Note this implies that $\det \rho_{E,\ell^\infty} = \chi_{\ell^\infty}$, since they agree on $Frob_p$ for $p \nmid N\ell$ and the $Frob_p$ are dense by Chebotarev.

Likewise: $\det \rho_{E,n} = \chi_n$ when $\chi_n : G_\mathbb{Q} \to \mathrm{Aut}(\mu(\overline{\mathbb{Q}}))$.

Definition 7.4. Call an R-algebra finite if it is finitely generated as an R-module.

For example, $R[T]$ is not finite; it is finitely generated as R-algebra, not as an R-module.

Suppose R is a field K. Call a finite K-algebra A étale if $A \otimes_K \overline{K} \cong \overline{K} \times \cdots \times \overline{K}$ (p.o.f, product of fields).

Call an affine group scheme blah if its representing ring is blah. For example, $\mathbb{G}_a$ is not a finite group scheme over R since its representing ring $R[T]$ is not finite.

Example 7.5. $R[T]/(T^n - 1)$ is a finite R-algebra since we can consider it as an R-mod generated by $1, T, \cdots, T^{n-1}$. So μ_n is a finite group scheme over R.

Let R be a field K. Is μ_ℓ étale?

Let $A = (K[T]/(T^\ell - 1)) \otimes_K \overline{K} = \overline{K}[T]/(T^\ell - 1)$. If $\ell = \mathrm{char} K$, then $A \cong \overline{K}/(T-1)^\ell$ is not a p.o.f since A has nilpotents, so here μ_ℓ is not étale.

If $\ell \neq char K$, then $A \cong \prod_{i=0}^{\ell-1} \overline{K}[T]/(T - \zeta^i)$ where ζ is primitive ℓth root of 1. Then $A \cong \overline{K} \times \cdots \times \overline{K}$, so we have μ_ℓ is étale. In general, μ_n is étale over K if and only if $\mathrm{char}\, K \nmid n$.

Theorem 7.6. *The category of étale group schemes over K is equivalent to the category of finite groups with continuous G_K-action.*

Proof. (Sketch) Let G be an étale group scheme over K. Let $\mathfrak{R}$ be the representing ring, an étale K-algebra. Consider $G(\overline{K}) = \mathrm{Hom}_{K\text{-alg}}(\mathfrak{R}, \overline{K})$. This is a finite group since G is finite of order $\dim_K \mathfrak{R}$. Let $\sigma \in G_K, \phi \in G(\overline{K})$. Then composing $\mathfrak{R} \xrightarrow{\phi} \overline{K} \xrightarrow{\sigma} \overline{K}$ yields $\sigma \circ \phi \in G(\overline{K})$. This defines an action of G_K on $G(\overline{K})$.

Moreover, this gives a *continuous* action of G_K on $G(\overline{K})$ since the K-algebra $\mathfrak{R}$ is generated by finitely many elements, all lying in a fixed finite Galois extension of K.

Conversely say H is a finite group on which G_K acts continuously. First, assume G_K acts transitively. By continuity, the action of G_K factors through some $\mathrm{Gal}(L/K)$ for L/K a finite extension. Pick $h \in H$ and let S be the subgroup of G_K fixing h and $\mathfrak{R}$ the fixed field in $\overline{K}$ of S.

Define

$$\begin{aligned} H &\to \mathrm{Hom}_{K\text{-alg}}(\mathfrak{R}, \overline{K}) \\ h &\mapsto \theta \end{aligned}$$

for some embedding $\theta\colon \mathfrak{R} \to \overline{K}$. Note that all such choices of θ are all conjugate under G_K. This extends to a map $\sigma h \mapsto \sigma\theta$ and so by transitivity of the Galois action, the map extends uniquely to H.

For an intransitive G_K action, we take as the representing ring $\mathfrak{R}$ the product of the rings $\mathfrak{R}_{\mathcal{O}}$ obtained from each orbit $\mathcal{O}$ of the action via the above process. We leave it to the reader to fill in the details. □

Big picture: Say we are given $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}/\ell^n)$, then $\rho_\ell : G_{\mathbb{Q}_\ell} \to GL_2(\mathbb{Z}/\ell^n)$ typically won't be unramified. What do we mean for ρ_ℓ to be “nice"? By the last theorem, ρ_ℓ corresponds to some étale group scheme G over $\mathbb{Q}_\ell$. Call ρ good at ℓ if there exists a flat $\mathbb{Z}_\ell$-algebra $\mathfrak{R}$ such that G is represented by $\mathfrak{R} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$.

8. 2018-02-14: Galois representations associated to elliptic curves; group schemes

Last time, we showed the equivalence of categories between étale group schemes over K and finite groups with continuous $\mathbb{G}_K$-action.

Definition 8.1. Call an R-module A flat if tensoring with A is exact, i.e., if $0 \to L \to M \to N \to 0$ is a short exact sequence of R-modules, then $0 \to L \otimes_R A \to M \otimes_R A \to N \otimes_R A \to 0$ is a short exact sequence of A-modules. Since $- \otimes_R A$ is always right exact, we only need to show whether it preserves injection.

An affine group scheme over R is flat if its representing ring is a flat R-module.

Example 8.2. Free modules are flat, so every module over a field is flat. In fact, if R is a principal ideal domain, then an R-module is flat if and only if it is torsion free, which occurs if and only if it is free. In particular, a $\mathbb{Z}_\ell$-module is flat if and only if it is torsion free.

We have an example of non-flat module.

Example 8.3. We have an inclusion:

$$\mathbb{Z}_\ell \hookrightarrow \mathbb{Q}_\ell$$

But

$$\mathbb{Z}/\ell^n = \mathbb{Z}_\ell \otimes \mathbb{Z}/\ell^n \not\hookrightarrow \mathbb{Q}_\ell \otimes \mathbb{Z}/\ell^n = 0$$

So $\mathbb{Z}/\ell^n$ is not a flat $\mathbb{Z}_\ell$-algebra.

Example 8.4. μ_ℓ over $\mathbb{Z}_\ell$ is represented by $\mathbb{Z}_\ell[T]/(T^\ell - 1)$. It is free over $\mathbb{Z}_\ell$ so is flat. So μ_ℓ is a finite flat affine group scheme over $\mathbb{Z}_\ell$.

Definition 8.5. Let G' be an étale group scheme over $\mathbb{Q}_\ell$ represented by $\mathfrak{R}$'. Call G' good if there exists a finite flat group scheme over $\mathbb{Z}_\ell$ represented by $\mathfrak{R}$ such that $\mathfrak{R} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell = \mathfrak{R}'$, i.e. G' is the base change of G from $\mathbb{Z}_\ell$ to $\mathbb{Q}_\ell$.

Example 8.6. μ_ℓ is good étale group scheme over $\mathbb{Q}_\ell$.

Remark 8.7. Let $\operatorname{Spec}(R) = \{\text{prime ideals of } R\}$ with the Zariski topology, i.e., closed sets $V(I) = \{\mathfrak{p} \in \operatorname{Spec}(R),\ \mathfrak{p} \supset I\}$, where I ranges over ideals of R.

Example 8.8. $\operatorname{Spec}(\mathbb{Z}_\ell) = \{\ell\mathbb{Z}_\ell, 0\}$. Closed sets are $\emptyset, \{\ell\mathbb{Z}_\ell\}, V(0) = Spec(\mathbb{Z}_\ell)$.

Ring homomorphisms $R \xrightarrow{f} S$ yield continuous maps $\operatorname{Spec}(S) \to \operatorname{Spec}(R)$ sending $\mathfrak{p}$ to $f^{-1}(\mathfrak{p})$.

Suppose we have a $\mathbb{Z}_\ell$-algebra A. Then $\operatorname{Spec}(A)$ is divided into two fibers: The fiber over $\mathbb{F}_\ell$, $\operatorname{Spec}(A \otimes_{\mathbb{Z}_\ell} \mathbb{F}_\ell)$, called the special/closed fiber and the fiber over $\mathbb{Q}_\ell$, $\operatorname{Spec}(A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)$, called the generic fiber.

A *good* group scheme over $\mathbb{Q}_\ell$ is the generic fiber of a finite flat group scheme over $\mathbb{Z}_\ell$.

Definition 8.9. Given continuous homomorphism $\rho\colon G_{\mathbb{Q}} \to GL_2(R)$, where R is a finitely generated ring in $\mathscr{C}_k$. We call ρ good at ℓ if the étale group scheme associated to ρ_ℓ is good.

Now we go back briefly to elliptic curves over $\mathbb{Q}$.

For each $\mathbb{Q}$-algebra A, we can define $E(A)$. We want to know whether it is an affine group scheme.

Example 8.10. Try $\mathfrak{R} = \mathbb{Q}[x,y]/(y^2 - f(x))$. Then we have the following 1-1 correspondence:

$$\operatorname{Hom}_{\mathbb{Q}\text{-alg}}(\mathfrak{R}, A) \longleftrightarrow \{\text{affine points of } E(A)\}$$

In fact, E is a group scheme, but is not affine. On the other hand, the n-torsion $E[n]$ is affine.

Theorem 8.11. *If E has good reduction at ℓ ($f(x)$ has distinct roots mod ℓ), then $E[n]$ comes from a finite flat group scheme over $\mathbb{Z}_\ell$, which implies that $\rho_{E,n}$ is good at ℓ.*

Sketch of Proof. Let $\mathscr{E}$ be the minimal Weierstrass model for E over $\mathbb{Q}_\ell$, where minimal means that coefficients are in $\mathbb{Z}_\ell$ and of as small valuation as possible. We can check using elementary methods that $\mathscr{E}$ is a group scheme over $\mathbb{Z}_\ell$ extending E. It remains to check that $\mathscr{E}[n]$ is affine, finite, and flat over $\mathbb{Z}_\ell$. By the classical theory of elliptic curves, the n-torsion of $\mathscr{E}$ over $\overline{\mathbb{Q}}_\ell$ and $\overline{\mathbb{F}}_\ell$, and hence both the closed and generic fibers, are finite group schemes of the same rank n^2. Suppose $\mathscr{E}[n]$ is affine, say $\operatorname{Spec}(A)$. We can show that A is integral over $\mathbb{Z}_\ell$, so is finite over $\mathbb{Z}_\ell$. By classification of modules over a PID, we know $A \cong \mathbb{Z}_\ell^n \oplus T$. Moreover, by our remarks on the ranks of the generic and closed fibers of $\mathscr{E}[n]$, the dimensions of $A \otimes_{\mathbb{Z}_\ell} \mathbb{F}_\ell$ and $A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ are the same. Consequently, $T = 0$, so A is free as a $\mathbb{Z}_\ell$-module, and so is flat.

To prove $\mathscr{E}[n]$ is affine, we note first that it is certainly a closed subscheme of $\mathbb{P}^2_{\mathbb{Z}_\ell}$. Hence, it suffices to show we can find an open affine space in $\mathbb{P}^2_{\mathbb{Z}_\ell}$ containing it. To this end, choose $\overline{f} \in \mathbb{F}_\ell[X,Y,Z]$ such that $V(\overline{f}) \subset \mathbb{P}^2_{\mathbb{F}_\ell}$ does not meet the closed fiber of $\mathscr{E}[n]$. Lift $\overline{f}$ to a homogeneous polynomial $f \in \mathbb{Z}_\ell[X,Y,Z]$. We claim that $V(f) \subset \mathbb{P}^2_{\mathbb{Z}_\ell}$ does not meet the closed fiber of $\mathscr{E}[n]$ and so $\mathscr{E}[n]$ is contained in the open affine $\operatorname{Spec}(\mathbb{Z}_p[X,Y,Z]_{(f)}) = \mathbb{P}^2_{\mathbb{Z}_\ell} \setminus V(f)$. If instead $V(f)$ and $\mathscr{E}[n]$ have nonempty intersection, then their intersection contains a closed point x and by properness of projective space over $\mathbb{Z}_\ell$, x is defined over the closed point $\operatorname{Spec}(\mathbb{F}_\ell) \subset \operatorname{Spec}(\mathbb{Z}_\ell)$. But this contradicts the choice of $\overline{f}$ avoiding the closed fiber of $\mathscr{E}[n]$. We conclude $\mathscr{E}[n]$ is affine. □

For more detailed proofs, you may refer to [Con97] or watch Prof. Andrew Snowden's lectures online[Sno13].

9. 2018-02-16: Galois Representations Associated to Modular Forms

Last time, we showed how to use the associated étale group scheme to define when a continuous representation $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{Z}/\ell^m)$ is good at ℓ. We now define modular forms and explore sources of continuous Galois representations associated to modular forms. We refer the reader to [DI95a] for a more comprehensive introduction to modular forms.

Fix integers $k \geq 0$, $N > 0$ and a homomorphism $\epsilon\colon (\mathbb{Z}/N)^\times \to \mathbb{C}^\times$. We will call k, N, ϵ the weight, level, and Nebentypus, respectively. Let

$$\mathcal{H} = \{z \in \mathbb{C} \mid \Im(z) > 0\}$$

denote the upper half plane in $\mathbb{C}$ and let

$$\mathcal{H} = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$$

denote the compactification of $\mathcal{H}$, with $\mathbb{Q}$ thought of as a subset of $\mathbb{R} \subset \mathbb{C}$ and ∞ thought of as lying at $i\infty$ on the imaginary axis. We have an action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$ and $\mathcal{H}^*$ acting by

$$\sigma \cdot z = \frac{az+b}{cz+d} \quad \text{for } \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

with the usual exceptions for ∞; that is, for σ as above, $\sigma z = \infty$ if $cz + d = 0$ (for $z = -d/c$ rational) and $\sigma\infty = a/c$. More uniformly, one can realize the action of σ on projective coordinates $\sigma[z, w] = [az + bw : cz + dw]$.

For a function f on $\mathcal{H}$ or $\mathcal{H}^*$ and $\sigma \in \mathrm{SL}_2(\mathbb{Z})$, let $f|_{[\sigma]_k}$ be the function defined by

$$f|_{[\sigma]_k}(z) = (cz+d)^{-k} f(\sigma z)$$

Finally, define subgroups $\Gamma_1(N) < \Gamma_0(N) < \mathrm{SL}_2(\mathbb{Z})$ by

$$\Gamma_0(N) = \left\{ \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \mod N \right\}$$

$$\Gamma_1(N) = \left\{ \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \;\middle|\; d \equiv 1 \mod N \right\}$$

Definition 9.1. A *modular function* f of weight k, level N, and Nedentypus ϵ on $\mathcal{H}^*$ is a function f which satisfies the following three properties:

(1) f is meromorphic on $\mathcal{H}$;
(2) $f|_{[\sigma]_k} = \epsilon(d) f$ for all $\sigma \in \Gamma_0(N)$.
(3) f is meromorphic at all cusps. (See Remark 9.2 below for meaning of this condition.)

Furthermore, if f is holomorphic on $\mathcal{H}$ and at the cusps, then f is called a *modular form*, and if f is holomorphic on $\mathcal{H}$ and vanishes at the cusps, then f is a *cusp form*.

Remark 9.2. Let f satisfy conditions (1) and (2) in Definition 9.1; we explain here what it means for f to satisfy condition (3). By condition (2) applied to the matrix $\sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $f(z) = f(z+1)$ for all $z \in \mathcal{H}$. Hence, f has a Fourier expansion in $q = e^{2\pi i z}$. Write $f = \sum_{n=-\infty}^{\infty} a_n q^n$ for this expansion. Then f is meromorphic at infinity if there exists N_0 such that $a_n = 0$ for all $n < N_0$; f is holomorphic at infinity if $a_n = 0$ for $n < 0$; and f vanishes at infinity if $a_n = 0$ for $n \leq 0$.

We say that f is meromorphic, resp. holomorphic, resp. vanishes at ∞ if $f|_{[\sigma]_k}$ is meromorphic, resp. holomorphic, resp. vanishes at infinity for all $\sigma \in \mathrm{SL}_2(\mathbb{Z})$.

Remark 9.3. We define the *cusps* of the quotient space $X_0(N) := \mathcal{H}^*/\Gamma_0(N)$ to be the orbits $\mathbb{Q} \cup \{\infty\}$ under the $\Gamma_0(N)$ action. Remark 9.2 gives conditions on f for each cusp of $X_0(N)$. For $N = 1$, $\Gamma_0(N) = \mathrm{SL}_2(\mathbb{Z})$ acts transitively on $\mathbb{Q} \cup \{\infty\}$, so there is a single cusp. In general, there are finitely many cusps and hence finitely many conditions on f.

Let $S(k, \epsilon)$ denote the set of all cusp forms of type (k, N, ϵ). It is an easy exercise to see that $S(k, \epsilon)$ is a complex vector space; we will see that it is finite dimensional and give a formula for its dimension.

Example 9.4. Consider the case of level $N = 1$ and trivial Nebentypus. Then, $\Gamma_0(N) = \Gamma_1(N) = \mathrm{SL}_2(\mathbb{Z})$. In particular, $f|_{[\sigma]_k} = f$ for all $\sigma \in \mathrm{SL}_2(\mathbb{Z})$, and one must only check conditions at infinity for f since there is only a single cusp. In this case, the following is a cusp form for $(N, k, \epsilon) = (1, 12, 1)$.

$$\Delta = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n$$

where $\tau(n)$ is the Ramanujan τ-function.

Serre conjectured in 1968 and Deligne proved in 1969 that this cusp form was intricately linked to Galois representations in the following sense: For all $n \geq 1$, there exists a continuous homomorphism $\rho_{\Delta,n} \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/n)$ unramified at every prime $p \nmid n$ at which

$$\mathrm{trace}\Big(\rho_{\Delta,n}(\mathrm{Frob}_p)\Big) = \tau(p) \quad \text{and} \quad \det\Big(\rho_{\Delta,n}(\mathrm{Frob}_p)\Big) = p^{11} = p^{k-1}$$

In particular, the latter fact implies also that $\det \rho_{\Delta,n} = \chi_n^{11}$ is the cyclotomic character. Note that this has many applications in understanding $\tau(n)$. For example, if $n = 691$, then one can show $\rho_{\Delta,n}$ has image contained in

$$\mathrm{image}(\rho_{\Delta,n}) \subset \left\{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \;\middle|\; b \in \mathbb{Z}/n, \;\; d \in (\mathbb{Z}/n)^{\times} \right\} \subset \mathrm{GL}_2(\mathbb{Z}/n)$$

where, for such a matrix M, $\mathrm{tr}(M) = 1 + \det(M)$. Hence, applying this to the element $\rho_{\Delta,n}(\mathrm{Frob}_p)$, $p \neq 691$, gives the well-known congruence

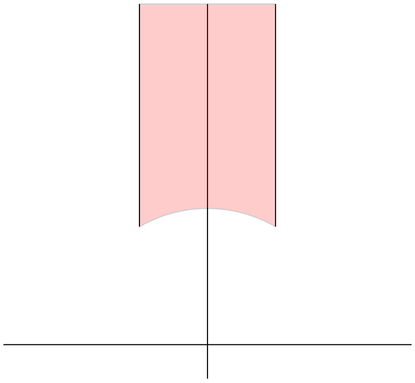
$$\tau(p) = 1 + p^{11} \mod n$$

Swinnerton-Dyer used these representations to prove all know congruences for τ plus some new statements.

As in the example, we will seek to connect Galois representations to some special cusp forms whose trace and determinants at Frobenius elements can be expressed in terms of the arithmetic of the cusp form. To do so, we must establish a source for such representations; namely, the n-torsion of Jacobians of modular curves.

Define the modular curve $X_0(N) = \mathcal{H}/\Gamma_0(N)$ and let $J_0(N) := \mathrm{Pic}^0\Big(X_0(N)\Big)$ be its Jacobian. Note that $\mathrm{Pic}^0(X_0(N))$, the set of isomorphism classes of codimension one divisors modulo principal divisors, is naturally a group scheme over $\mathbb{Q}$ (or over $\mathbb{Z}[\frac{1}{n}]$).

Example 9.5. If $N = 1$, then $X_0(1) = \mathcal{H}/\mathrm{SL}_2(\mathbb{Z})$ has fundamental domain the shaded region below with the appropriate identification on the boundary and with the point at infinity though of as $i\infty$.



In particular, $X_0(1)$ is topologically a sphere. In fact, $X_0(N)$ remains topologically a sphere for $N < 11$, but the space $X_0(N)$ grows more complicated for higher N. For example, $X_0(11)$ has the structure of an elliptic curve.

9.1. **Preview of future directions.** We now state some results and facts on modular curves and their Jacobians, leaving their proofs and exposition for later. Namely, if $g = \dim S_2(N,1)$, then $X_0(N)$ is a compact Riemann surface of genus g and its Jacobian $J := J_0(N)$ is then a g-dimensional abelian variety when considered over $\mathbb{C}$. Let $J(\mathbb{C}) := J_0(N)(\mathbb{C})$ denote the $\mathbb{C}$-points of $J_0(N)$, and let $J(\mathbb{C})[n]$ denote the n-torsion of $J(\mathbb{C})$. The following facts will be our motivation:

Fact 9.6. As abelian groups, $J(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda$ for Λ a lattice in $\mathbb{C}$, i.e. Λ is a discrete subgroup of $\mathbb{C}^g$ such that $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{C}$.

Fact 9.7. $J(\mathbb{C})[n] \simeq (\mathbb{Z}/n)^{2g}$

Fact 9.8. $J(\mathbb{C})[n] \subset J(\overline{\mathbb{Q}})$, i.e. the n-torsion of $J(\mathbb{C})$ has algebraic coordinates. In particular, $G_{\mathbb{Q}}$ acts on $J(\mathbb{C})[n]$, yielding a representation

$$\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_{2g}(\mathbb{Z}/n)$$

Fact 9.9. The representation obtained by Fact 9.8 breaks into a sum of 2 dimensional representations. Moreover, if $f_1, \ldots, f_g$ are a basis of $S_2(N,1)$ consisting of cuspidal eigenforms and $f_i = \sum_n a_{n,i} q^i$, then $J(\mathbb{C})[n] \simeq V_1 \oplus \cdots \oplus V_g$ for representations

$$\rho_{f_i,n}\colon G_{\mathbb{Q}} \to \mathrm{Aut}(V_i) = \mathrm{GL}_2(\mathbb{Z}/n)$$

unramified outside primes dividing n and N, with

$$\mathrm{trace}\Big(\rho_{f_i,n}(\mathrm{Frob}_p)\Big) = a_{p,i} \quad \text{and} \quad \det\Big(\rho_{f_i,n}(\mathrm{Frob}_p)\Big) = p.$$

10. 2018-02-19: Riemann Surfaces and Functions on Modular Curves

We now study the structure of the modular curves $X_0(N)$, beginning with Riemann surfaces.

10.1. Definition and Examples of Riemann Surfaces.

Definition 10.1. A *surface* is a Hausdorff, connected topological space with an open cover $\{U_\alpha \mid \alpha \in A\}$ and homeomorphisms $\phi_\alpha\colon U_\alpha \to V_\alpha$ for $V_\alpha \subseteq \mathbb{C}$ open. We call a pair (U_α, ϕ_α) a *chart* and the set of charts an *atlas*.

If (U_α, ϕ_α) and (U_β, ϕ_β) are two charts with $U_\alpha \cap U_\beta \neq \emptyset$, then we call the map

$$t_{\alpha,\beta} = \phi_\beta \phi_\alpha^{-1} \colon \phi_\alpha(U_\alpha \cap U_\beta) \to \phi_\beta(U_\alpha \cap U_\beta)$$

a "transition map" for α, β.

Definition 10.2. We call a surface S a Riemann surface if, whenever transition maps $t_{\alpha,\beta}$ are defined, they are analytic.

Example 10.3. (1) The complex plane, $\mathbb{C}$, is a Riemann surface with the single chart $U = \mathbb{C}$, $\phi \colon U \to \mathbb{C}$ the identity map.

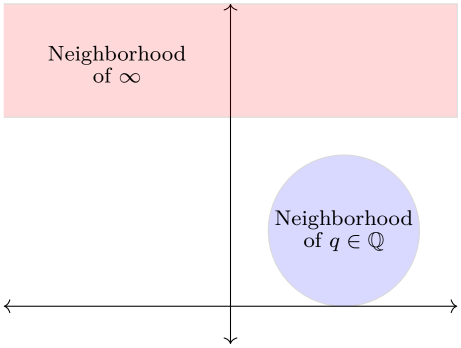
(2) The *Riemann sphere* $\mathbb{C}_\infty := \mathbb{C} \cup \{\infty\} = \mathbb{P}^1(\mathbb{C})$ is a Riemann surface with the following two charts:

$$U_1 = \mathbb{C} = \mathbb{C}_\infty - \{\infty\} \xrightarrow{\phi_\alpha = \mathrm{id}_{\mathbb{C}}} \mathbb{C} \qquad\qquad U_2 = \mathbb{C}_\infty - \{0\} \xrightarrow{\phi_\beta} \mathbb{C}$$

$$z \longmapsto z \qquad\qquad z \mapsto \begin{cases} 1/z & \text{if } z \in \mathbb{C}^\times \\ 0 & \text{if } z = \infty \end{cases}$$

(3) Let $\Lambda \subset \mathbb{C}$ be a lattice in $\mathbb{C}$. The complex torus $\mathbb{C}/\Lambda$ has the structure of a (compact) Riemann surface with cover (U_α, ϕ_α) defined locally so each U_α has no monodromy. This example shows that the $\mathbb{C}$-points of an elliptic curve give it the structure of a Riemann surface.

(4) $\mathcal{H}$ is clearly a Riemann surface whose basic open sets are the open discs, with charts the identity maps. Moreover, $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$ has the structure of a Riemann surface with basic open sets the standard open sets in $\mathcal{H}$ together with neighborhoods of ∞ of the form $\{z \in \mathcal{H} \mid \Im(z) > r\} \cup \{\infty\}$ for some $r > 0$ and neighborhoods of $q \in \mathbb{Q}$ of the form $\{z \in \mathcal{H} \mid |q + ir - z| < r\} \cup \{q\}$, that is, open discs tangent to the real line at $q \in \mathbb{Q}$ together with the point q. See the diagram below for a visual picture of the basic open sets in $\mathcal{H}^*$.



Note that in example (4) above, the Riemann structure on $\mathcal{H}^*$ descends to a Riemann structure on the quotient $X_0(N) = \mathcal{H}^*/\Gamma_0(N)$. Moreover, the latter space is a compact Riemann surface since it has a finite atlas. In fact, compact Riemann surfaces are well understood by the following theorem:

Theorem 10.4 (Uniformization Theorem)**.** *Every Riemann surface is the quotient by a proper holomorphic action of a discrete group on its universal cover and the universal cover is holomorphically isomorphic (i.e. conformally equivalent) to the Riemann sphere $\mathbb{C}_\infty$, the complex plane $\mathbb{C}$, or the open unit disc Δ.*

By the theorem, any compact surface S is the quotient $U/\pi_1(S)$ for U the universal cover of S and $\pi_1(S)$ the fundamental group of S. For instance, example (3) above is obtained from the action of the fundamental group $\Lambda \simeq \mathbb{Z} \times \mathbb{Z}$ on the covering space $\mathbb{C}$.

10.2. **Intermission on Modular Forms.** To each lattice $\Lambda \subseteq \mathbb{C}$ and each $k \geq 2$, define the *Eisenstein series of* Λ to be

$$G_{2k}(\Lambda) := \sum_{\substack{\lambda \in \Lambda \\ \lambda \neq 0}} \frac{1}{\lambda^{2k}}$$

By standard analysis, this sum converges absolutely for $k \geq 2$. If $\lambda_\tau = \langle 1, \tau \rangle$ for $\tau \in \mathcal{H}$, then we set $G_{2k}(\tau) := G_{2k}(\Lambda_\tau)$.

Theorem 10.5. *$G_{2k}(\tau)$ is a modular form of weight $2k$, level 1, and trivial Nebentypus.*

Proof. Firstly, it is a simple exercise using uniform convergence to show that $G_{2k}(\tau)$ is holomorphic on $\mathcal{H}$. The modularity condition follows from the computation:

$$\begin{aligned} G_{2k}|_{[\sigma]_{2k}}(z) &= (cz+d)^{2k} G_{2k}\left(\frac{az+b}{cz+d}\right) = (cz+d)^{2k} \sum_{(\alpha,\beta)\neq(0,0)} \frac{1}{\left[\alpha\left(\frac{az+b}{cz+d}\right)+\beta\right]^{2k}} \\ &= \sum_{(\alpha,\beta)\neq(0,0)} \frac{1}{[(\alpha a+\beta c)z + (\alpha b + \beta d)]^{2k}} = \sum_{(\gamma,\delta)\neq(0,0)} \frac{1}{(\gamma z+\delta)^{2k}} = G_{2k}(z) \end{aligned}$$

where the latter equality follows by reindexing the summation. Finally, since $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$ acts transitively on the cusps, it suffices to show G_{2k} has Fourier expansion having nonnegative coefficients. It follows from the direct computation that

$$G_{2k}(\tau) = 2\zeta(2k)\left(1 - \frac{4k}{B_{2k}} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n\right)$$

where B_k is the kth Bernoulli number, $\sigma_r(n) := \sum_{d|n} d^r$, and $q = e^{2\pi i \tau}$. Hence, G_{2k} is holomorphic at infinity and so is a modular form. □

By Theorem 10.5, the functions $g_2 = 60G_4$ and $g_6 = 140G_6$ are modular of level 1 and weights 4 and 6, respectively. In particular, g_2^3 and g_3^2 are both modular of weight 12, level 1, and so can be combined to give a cusp form $g_2^3 - 27g_3^2 \in S(12,1)$. In fact, $\dim_{\mathbb{C}} S(12,1) = 1$ and $\Delta \in S(12,1)$, so we have the relation

$$g_2^3 - 27g_3^2 = (2\pi)^{12}\Delta = (2\pi)^{12} q \prod_{n=1}^{\infty}(1-q^n)^{24}.$$

Sacrificing holomorphicity, we may then construct the ratio

$$j = \frac{1728 g_2^3}{g_2^3 - 27g_3^2}.$$

Then, j is a modular function of weight 0 and level 1, and so gives a map

$$j \colon \mathcal{H}^*/\Gamma_0(1) = X_0(1) \to \mathbb{C}_\infty.$$

10.3. **Morphisms of Riemann Surfaces.** We will now establish a dictionary between maps of Riemann surfaces and their associated function fields and preview some future directions. We begin with the basic definition.

Definition 10.6. Let R, S be Riemann surfaces with atlases $(U_\alpha, \phi_\alpha), (V_\beta, \psi_\beta)$, respectively. A continuous map $f\colon R \to S$ is called *analytic* if for all α, β the maps $\psi_\beta \phi_\alpha^{-1}$ are analytic as complex functions wherever they are defined.

Definition 10.7. Given a Riemann surface R, we call the set of all analytic functions from R to the Riemann sphere $\mathbb{C}_\infty$ the *field of meromorphic functions on R*, which we denote by

$$K(R) := \{f\colon R \to \mathbb{C}_\infty \mid f \text{ is analytic}\}.$$

These definitions give us a dictionary through which we can analyze maps of Riemann surfaces. For instance, we will show that $K(X_0(1)) = \mathbb{C}(j)$ and $K(X_0(N)) = \mathbb{C}(j, j_N)$ for the functions j as above and $j_N(z) := j(Nz)$, so that the following diagrams correspond to one another:

$$\begin{tikzcd}
\Gamma_0(N) \arrow[d, hook] & X_0(N) \arrow[d] & K(X_0(N)) \\
\Gamma_0(1) & X_0(1) & K(X_0(1)) \arrow[u, hook]
\end{tikzcd}$$

Furthermore, we will prove an integrality condition for j_N over $\mathbb{C}(j)$ which will allow us to build a $\mathbb{Q}(j, j_N)$ model for $X_0(N)$ over $\mathbb{Q}$.

11. 2018-02-21: Functions on Modular Curves II

11.1. **Functions on $X_0(1)$.** As discussed earlier, in this section we aim at describing the functions on $X_0(1)$ and $X_0(N)$. To do so, we first state some properties of the modular j-function.

Fact 11.1. The q-expansion of the j-function is: $\frac{1}{q} + 744 + 196884q + \cdots$.

Exercise 11.2. (1) The j-function is one-to-one on the upper half plane $\mathcal{H} \cup P^1(\mathbb{Q})$.
(2) j has a simple pole at ∞.

Both these follow from the aforementioned fact about the q-expansion.

Lemma 11.3. *$K(X_0(1)) = \mathbb{C}(j)$, where j denotes the usual modular j-function.*

Proof. Since j is modular function of level 1 and weight 0, we already know that $\mathbb{C}(j) \subset K(X_0(1))$. Conversely, let f be some modular function of level 1, with poles $\tau_1, \tau_2 \cdots \tau_n$. Then:

$$g(\tau) := f(\tau) \prod_{i=1}^{n} (j(\tau) - j(\tau_i)$$

has no poles on the upper half plane $\mathcal{H}$. Thus it can only have a pole at ∞. If g has a pole of order m at ∞, then by part 2 of the exercise, there is a constant c such that $g - cj^m$ has a pole of order $m-1$ at ∞. Continuing iteratively, we obtain that there is a polynomial $P(j)$ such that $g - P(j)$ has no poles and is therefore constant. Thus, $g \in \mathbb{C}(j)$ and so $f \in \mathbb{C}(j)$. □

Remark 11.4. Note that in the above proof, if $g = \sum_{n=n_0}^{\infty} c_n q^n$, then $P(j)$ must have coefficients in the $\mathbb{Z}$ module generated by all the c_n's. This will be important when we prove the properties of modular polynomials in the next section.

11.2. **Aside: A Crash course in Elliptic curves over $\mathbb{C}$.** Before we proceed, we state a few results about elliptic curves over $\mathbb{C}$ and their classification as complex tori. This helps us understand better the relation between Elliptic curves and modular forms and establish a direct connection between the j-function and the j-invariant of the Elliptic curve. More details on this section can be found in [Sil09]

Let Λ be a lattice in $\mathbb{C}$. Recall the definitions of g_2 and g_3 associated to Λ from the last section. Define

$$E_\Lambda : y^2 = 4x^3 - g_2 x - g_3$$

Claim 11.5. *E_Λ is an elliptic curve if and only if $g_2^3 - 27g_3^2 \neq 0$.*

The proof of this claim is a discriminant argument that follows from one of the facts stated later.

We now establish a bijection between the complex points of E_Λ and the 1-dimensional complex torus $\mathbb{C}/\Lambda$. Define:

$$\begin{aligned} \Phi : \mathbb{C}/\Lambda &\to E_\Lambda(\mathbb{C}) \\ z &\mapsto (\mathfrak{P}_\Lambda(z), \mathfrak{P}'_\Lambda(z)) \end{aligned}$$

where $\mathfrak{P}_\Lambda(z)$ is the Weierstrass $\mathfrak{P}$ function defined as:

$$\mathfrak{P}_\Lambda(z) = \frac{1}{z^2} + \sum_{w \in \Lambda} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right)$$

Exercise 11.6. Show that Φ is well defined (this follows from the fact that the Weierstrass $\mathfrak{P}$ function and its derivative are doubly periodic with respect to Λ, which is a straightforward calculation).

Of course, we must verify that the image of Φ is indeed contained in $E_\Lambda(\mathbb{C})$. To do this, define:

$$f(z) = \mathfrak{P}'_\Lambda(z)^2 - (4\mathfrak{P}_\Lambda(z)^3 - g_2\mathfrak{P}_\Lambda(z) - g_3)$$

Lemma 11.7. *$f(z)$, as defined above, is identically 0.*

Proof. We break this proof up into steps as follows:
Step I: Expanding the $\mathfrak{P}$ function, we have: $\mathfrak{P}_\Lambda(z) = \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 \cdots$. Further, expanding $f(z)$, we notice that the coefficients of z^{-6}, z^{-4} and z^{-2} all vanish, leaving us with a holomorphic function.
Step II: f is also doubly periodic with respect to Λ, being built up from the Weierstrass $\mathfrak{P}$ function and its derivative.
Step III: f must be bounded on the (compact) fundamental domain of Λ and by Step II, on the entire complex plane. Thus, by Louiville's theorem, f must be constant on $\mathbb{C}$. Further, a calculation that the constant term is $f(z)$ is also 0, i.e. $f(0) = 0$, which completes the proof. □

Therefore, we have shown: Image$(\Phi) \subset E_\Lambda(\mathbb{C})$.

Exercise 11.8. (1) Show that Φ is an isomorphism. (This gives us a group structure on $E_\Lambda(\mathbb{C})$.)

(2) Show that the group structure obtained by this isomorphism is the same as the one obtained in the traditional way (by requiring that for 3 collinear points P, Q and R, $P \oplus Q \oplus R = 0$)

Fact 11.9. Let ω_1, ω_2 be a basis for Λ and $\omega_3 = \omega_1 + \omega_2$. Then $\mathfrak{P}'_\Lambda(\omega_i/2) = 0$. Further, the $\mathfrak{P}_\Lambda(\omega_i)$ are all distinct if and only if $g_2^3 - 27g_3^2 \neq 0$.

Proposition 11.10. *The set of 1-dimensional complex tori is in bijection with the set of elliptic curves over* $\mathbb{C}$.

Proof. We have already constructed an elliptic curve E_Λ corresponding to each lattice Λ. Conversely: Let E be an elliptic curve defined by $y^2 = 4x^3 - Ax - B$. Since the j function is surjective, we can find a τ such that $j(\tau) = \frac{1728A^3}{A^3 - 27B^2}$. By a uniformization theorem, there exists a lattice Λ, unique up to homothety, such that $g_2(\Lambda) = A$ and $g_3(\Lambda) = B$. In fact, one can take: $\Lambda = c(\mathbb{Z} + \mathbb{Z}\tau)$, $c \in \mathbb{C}$. By construction, $E = E_\Lambda$. □

11.3. **Back to Functions on $X_0(N)$.** After an aside on elliptic curves, we turn back to showing that $K(X_0(N)) = \mathbb{C}(j, j_N)$. We first set up some notation to aid us in this endeavor. Recall the definition of the modular subgroup

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 \mod N \right\}$$

- $\mu(N) := [SL_2(\mathbb{Z}) : \Gamma_0(N)]$. Note that this is finite, since $\mathrm{Ker}(SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})) = \Gamma(N) \subset \Gamma_0(N)$.
- $\Delta_N = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_2(\mathbb{Z}) \mid ad = N, d > 0, 0 \leq b < d, \gcd(a, b, d) = 1 \right\}$. It is a straightforward calculation to show that there are $\mu(N)$ such matrices. We label them $\alpha_1, \alpha_2 \cdots \alpha_{\mu(N)}$.
- $\alpha := \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \in \Delta_N$
- Thus: $j_N(z) = j(Nz)$ defined earlier, is just $j \circ \alpha$

Exercise 11.11. $\mu(N) = N \prod_{p|N} \left(1 + \dfrac{1}{p}\right)$. You may want to use/prove the fact that $SL_2(\mathbb{Z}/n\mathbb{Z})$ has size: $N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)$

Definition 11.12. We define the *modular polynomial of level N* to be $\Phi_N(x) := \prod_{i=1}^{\mu(N)} (x - j \circ \alpha_i)$

Next time: we will show that $K(X_0(N)) = \mathbb{C}(j, j_N)$. Further, Φ_N has coefficients in $\mathbb{C}(j)$, i.e. its coefficients are modular functions of level 1.

12. 2018-02-23: Functions on Modular curves, and Jacobians

In this section, we complete our quest of describing the function field of $X_0(N)$ and introduce the classical, complex analytic notion of the Jacobian of a curve.

12.1. **Function field of $X_0(N)$ continued.** We continue to prove the result we claimed earlier.

Lemma 12.1. *$\Phi_N(x)$ has coefficients in $\mathbb{Z}[j]$ and is irreducible over $\mathbb{C}(j)$ (and is thus the irreducible polynomial of j_N over $\mathbb{C}(j)$). Thus, $K(X_0(N)) = \mathbb{C}(j, j_N)$.*

Remark 12.2. The above lemma enables us to define $X_0(N)$ as a curve over $\mathbb{Q}$ and in fact, over $\mathbb{Z}[1/N]$ for $N > 3$. (The importance of $Z[1/N]$ lies in the moduli space interpretation of $X_0(N)$ as parameterizing elliptic curves of a certain conductor. For $N \leq 3$, there are issues with the representability of the functor.

Proof. j is a modular function of level 1 and hence of level N. Further, for $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, $\alpha\sigma\alpha^{-1} = \begin{pmatrix} a & Nb \\ c/N & d \end{pmatrix} \in SL_2(\mathbb{Z})$

$$j_N(\sigma z) = j \circ \alpha \circ \sigma(z) = j(\alpha\sigma\alpha^{-1})(\alpha(z)) = j(\alpha(z)) = j_N(z)$$

This shows that $\mathbb{C}(j, j_N) \subset K(X_0(N))$.

The converse is more involved. First note that all the $j \circ \alpha_i$'s are distinct. For $\alpha_i = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$:

$$j \circ \alpha_i(z) = j\left(\frac{az+b}{d}\right) = \frac{1}{q_d^a \zeta_d^b} + P(q_d^a \zeta_d^b)$$

where P is some holomorphic function, $q_d = e^{2\pi i z/d}$ and ζ_d is the primitive d-th root of unity,$e^{2\pi i/d}$. Now suppose $j \circ \alpha_i = j \circ \alpha_k$. Thus $j \circ \alpha_i(z) = j \circ \alpha_k(z) \forall\ z \in \mathcal{H}$. Now, let $\mathrm{Im}(z) \to \infty$, i.e. $q_d \to 0$. This forces $q_d^a \zeta_d^b = q_d'^{a'} \zeta_d'^{b'}$ and therefore $\frac{a}{d} = \frac{a'}{d'}$. But $ad = N = a'd'$ and $dd' > 0$. Thus, $a = a'$, etc. and $\alpha_i = \alpha_k$.

Now, if $\gamma \in SL_2(\mathbb{Z})$, $\exists$ some k and some $\beta \in SL_2(\mathbb{Z})$ such that $\alpha_i\gamma = \beta\alpha_k$. This gives us a permutation action of $SL_2(/Z)$ on the roots of Φ_N as follows: $j \circ \alpha_i \circ \gamma = j \circ \beta\alpha_k = j \circ \alpha_k$ (since j has level 1 and so $j \circ \beta = j$). Thus the coefficients of Φ_N are $SL_2(\mathbb{Z})$ invariant. Further, since all the $j \circ \alpha_i's$ are meromorphic (at infinity), so are the coefficients. Thus they must lie in $\mathbb{C}(j)$

Exercise 12.3. Show that the $SL_2(\mathbb{Z})$ action described above is transitive.

Thus we have shown that Φ_N is irreducible over $\mathbb{C}[j]$. Added to the fact that the degree of Φ_N is $\mu(N)$, this gives us that $K(X_0(N)) \subset \mathbb{C}(j, j_N)$. We now proceed to show that the coefficients lie in $\mathbb{Z}[j]$.

Fact 12.4. The coefficients lie in $\mathbb{Z}[\zeta_N][j]$

For a proof of this fact, you may refer to the section on Modular equations in [Lan87].

Further, the action of of $\mathrm{Gal}(\mathbb{Q}[\zeta_N]/\mathbb{Q})$ permutes the $j \circ \alpha_i$. To obtain the action of the map $\zeta_N \mapsto \zeta_N^r$, one can modify $\alpha_i = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ to $\alpha_{i'} = \begin{pmatrix} a & b' \\ 0 & d \end{pmatrix}$ where $b' \equiv rb \mod d$

This tells us that the coefficients must lie in $\mathbb{Z}[j]$.

□

12.2. **Jacobian of $X_0(N)$.** We now proceed to describe the Jacobian of the curve $X_0(N)$ (or for any Riemann surface in general). We start with the space of holomorphic differentials on $X_0(N)$, which will be denoted $W(= H^0(X_0(N), \Omega^1))$.

Let $f \in S_2(N, 1)$. Then $f(z)dz$ is a differential on $X_0(N)$ since for $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$:

$$f(\sigma z)d(\sigma z) = (cz+d)^2 f(z) \frac{1}{(cz+d)^2} dz = f(z)dz$$

Since $dz = \frac{dq}{2\pi i q}$ and f is a *cusp* form, $f(z)dz$ is holomorphic on all of $X_0(N)$. One can also go in the opposite direction.

This establishes a bijection between W and $S_2(N, 1)$. Let $g = \dim_{\mathbb{C}}(W)$, which is the genus of $X_0(N)$. Let $c_1, c_2 \cdots c_{2g}$ be the generating cycles of $H_1(X_0(N), \mathbb{Z})$. Consider the map:

$$\phi : H_1(X_0(N), \mathbb{Z}) \to \mathrm{Hom}(W, \mathbb{C})$$
$$C \mapsto \{\omega \mapsto \int_C \omega\}$$

The image of ϕ is a lattice, called the *period lattice*, which we will call Λ.

Definition 12.5. For a Riemann surface X, the *Jacobian* of X, $Jac(X)$ is defined as $\mathrm{Hom}(W, \mathbb{C})/\Lambda$ ($\cong \mathbb{C}^g/\Lambda$)

Further, if X is defined over a field k, then so if $Jac(X)$.

Definition 12.6. Let $\omega_1, \omega_2 \cdots \omega_g$ be a basis for W. The *Abel map* is defined as follows:

$$X \to Jac(X)$$
$$x \mapsto \{\int_{x_0}^{x} \omega_j\}_{j=1}^{g}$$

Exercise 12.7. Show that the Abel map is well defined. Further, show that this is a bijection for $g = 1$ and an embedding for $g \geq 2$.

Let $Div(X)$ denote the group of divisors on X. The Abel map can be extended linearly to $Div(X)$ and we can consider the induced map:

$$A : Div^0(X) \to Jac(X)$$

Fact 12.8. Define the subgroup of principal divisors ($Prin(X)$) to be those of the form $div(f)$, where f is a rational function on the Riemann surface X. Then:

$$A : Div^0(X)/Prin(X) \cong Jac(X)$$

This is called the Abel Jacobi theorem and can be found in any standard treatise on abelian varieties.

In the next lecture, we will talk about Hecke operators and their actions on modular forms, which in turn will help us build 2-dimensional Galois representations associated to modular curves.

13. 2018-02-26: Hecke Operators and Hecke Algebra

As discussed earlier, the Abel map yields a bijection between the following sets.

$$Pic^0(X) = Div^0(X)/Prin(X) \cong Jac(X)$$

Since $X_0(N)$ is defined over $\mathbb{Q}$, it holds that $J = Pic^0(X_0(N))$ is also defined over $\mathbb{Q}$. Hence we have the following isomorphism, where Λ is a lattice in $\mathbb{C}^g$ and g is the genus of $X_0(N)$, i.e. the dimension of the space $S_2(N, 1)$.

$$J(\mathbb{C}) \cong \mathbb{C}^g/\Lambda$$

The equation also implies the following isomorphism.

$$J[n] = \{P \in J(\mathbb{C}) \mid nP = 0\} \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$$

Such isomorphism yields a continuous Galois action since the coefficients of $P \in J[n]$ are algebraic over $\mathbb{Q}$.

$$G_{\mathbb{Q}} \to GL_{2g}(\mathbb{Z}/n\mathbb{Z})$$

The above map gives a $2g$-dimensional Galois representation of $J[n]$. We may ask whether it is possible to decompose the $2g$-dimensional Galois representation into g copies of 2-dimensional representations. To do so, we first construct Hecke Operators, which will help us construct the desired copies of 2-dimensional representations.

13.1. **Hecke Operators.**

Remark 13.1. Recall that the Eisenstein series has the following property, where Λ is a lattice in $\mathbb{C}$.

$$G_{2k}(\lambda\Lambda) = \lambda^{-2k}G_{2k}(\Lambda)$$

The above transformation yielded modular forms of weight $2k$ and level 1.

On the other hand, suppose Λ is a lattice in $\mathbb{C}$ generated by $1, \tau \in \mathcal{H}$, where $\mathcal{H}$ is the upper half plane in $\mathbb{C}$. By setting $G_{2k}(\tau) = G_{2k}(\Lambda)$, we achieve the following transformation, where a, b, c, d are integers such that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$.

$$G_{2k}\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^{2k}G_{2k}(\tau)$$

This can be understood as a variant of the aforementioned transformation:

$$G_{2k}(\lambda\Lambda) = \lambda^{-2k}G_{2k}(\Lambda)$$

Analogously, given a modular function f of weight k and level 1, we can construct an induced map where Λ is a lattice in $\mathbb{C}$ with basis $\{w_1, w_2\}$ such that $Im\left(\frac{w_1}{w_2}\right) > 0$.

$$\tilde{f}(\Lambda) = w_1^{-k} f\left(\frac{w_1}{w_2}\right)$$

Exercise 13.2. Show that $\tilde{f}$ depends only on Λ and not on the choice of basis of Λ.

Exercise 13.3. Show that $\tilde{f}$ satisfies the following equation.

$$\tilde{f}(\lambda\Lambda) = \lambda^{-k}\tilde{f}(\Lambda)$$

Using $\tilde{f}$, we can also construct the following expression, which can be considered as an operator which takes the average of values of $\tilde{f}$ over sub-lattices of index $m \in \mathbb{N}$.

$$(T_k(m)\tilde{f})(\Lambda) = m^{k-1} \sum_{[\Lambda:\Lambda']=m} \tilde{f}(\Lambda')$$

Exercise 13.4. Show that $T_k(m)\tilde{f}$ also satisfies the following equation.

$$(T_k(m)\tilde{f})(\lambda\Lambda) = \lambda^{-k}(T_k(m(\tilde{f})(\Lambda)$$

The equation implies that there exists a corresponding modular function.

Definition 13.5. If f is a cusp form of weight k, level N, and trivial nebentypus ϵ, define the Hecke Operator $T_k(m)$ for each $m \in \mathbb{N}$ as follows.

$$T_k(m)f := m^{\frac{k}{2}-1} \sum_j f|_{[\alpha_j]_k}$$

If $N = 1$, then α_j runs through the set Δ_m defined as follows:

$$\Delta_m = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_2(\mathbb{Z}) \mid ad = N, d > 0, 0 \leq b < d, \gcd(a,b,d) = 1 \right\}$$

For general N, α_j runs through the sets Δ_m such that $(a, N) = 1$ for each corresponding matrix entry a of α_j.

Exercise 13.6. Show that $T_k(m)$ acts on $S_k(N, \epsilon)$, in particular $T_k(m)f \in S_k(N, \epsilon)$. (Note that these facts do not arise as naturally as the previous exercises on $\tilde{f}$ and $T_k(m)\tilde{f}$.)

Suppose f, a cusp form of weight k, level N, and nebentypus ϵ, has the following q-expansion at ∞, where $q = e^{2\pi i z}$.

$$f(z) = \sum_{n=1}^{\infty} a_n q^n$$

One can then show that $T_k(m)f$ has the corresponding q-expansion at ∞:

$$(T_k(m)f)(z) = \sum n = 1^{\infty} b_n q^n$$

where each coefficients b_n are given as:

$$b_n = \sum_{d|(m,n)} \epsilon(d) d^{k-1} a_{\frac{mn}{d^2}}$$

In particular, if $(d, N) \neq 1$, we set $\epsilon(d) = 0$.

Remark 13.7. The q-expansion of $T_k(m)f$ implies that $T_k(m)$ acts linearly on $S_n(N, \epsilon)$.

We note several properties of the operator $T_k(m)$. The proof of these facts are explained in [Kna92].

$$T_k(m)T_k(n) = T_k(mn) \textit{ if } (m,n) = 1$$
$$T_k(p^r)T_k(p) = T_k(p^{r+1}) + p^{k-1}T_k(p^{r-1}) \textit{ for } r \geq 1 \textit{ and } p \textit{ prime.}$$

The first property can be derived by considering the intersections of sublattices of index m and n. In fact, all $T_k(m)$ commute with each other with varying values of m. The second statement hence implies that all $T_k(m)$'s are determined by $T_k(p)$ for prime p.

Definition 13.8. A cusp form f is a cuspidal eigenform if $T_k(m)f = \lambda_m f$ for all $m \in \mathbb{N}$, where $\lambda_m \in \mathbb{C}$

Using cuspidal eigenforms, we will construct the associated 2-dimensional Galois representations.

Example 13.9. Consider the following cusp form, which is an element of $S_{12}(1,1)$.

$$\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24}$$

Note that $S_{12}(1,1)$ is a 1-dimensional $\mathbb{C}$-vector space. Hence, Δ is a cuspidal eigenform.

Observe that the q-expansion of $T_k(m)f$ implies that the coefficient of q is given as follows.

$$\begin{aligned} b_1 &= \sum_{d|(m,1)} \epsilon(d)d^{k-1}a_{\frac{m}{d^2}} \\ &= \sum_{d|1} \epsilon(d)d^{k-1}a_{\frac{m}{d^2}} \\ &= \epsilon(1)1^{k-1}a_{\frac{m}{1^2}} \\ &= a_m \end{aligned}$$

Note that a_m corresponds to the coefficient of q^m of the q-expansion of f. Hence this shows that $T_k(m)f = \lambda_m f$ with $a_m = \lambda_m a_1$. In fact we can normalize the cuspidal eigenform, i.e. setting $a_1 = 1$, to derive $\lambda_m = a_m$.

Note 13.10. From now on, we will assume all cuspidal eigenforms are normalized, i.e. the coefficient of q in the q-expansion of a cusp form f is equal to 1. This will allow us to derive various results using Hecke Operators without worrying about possible deviations arising from possibly non-algebraic coefficients of q-expansion of f.

Now we define the Hecke Algebra $\mathcal{T}$.

Definition 13.11. The Hecke Algebra $\mathcal{T}$ is the commutative ring generated by Hecke Operators.

Note that the collection of Hecke Operators can be thought as a subset of $End(S_k(N,\epsilon))$, as Hecke Operators acts linearly on $S_k(N,\epsilon)$.

We first state one of the important facts about Hecke Operators.

Corollary 13.12. *Suppose $f = \sum_{n=1}^{\infty} a_n q^n$ is a cuspidal eigenform. Then the map $T_k(m) \mapsto a_m$ extends to a ring homomorphism $\theta : \mathcal{T} \to \mathbb{C}$.*

Note that the construction of θ depends on our choice of the cuspidal eigenform f. The corollary implies that $\mathcal{T}$ can be considered as a universal modular form of a certain weight.

Remark 13.13. The corollary implies that there exists an injective map

$$S_k(N,\epsilon) \hookrightarrow \mathbb{C}\llbracket q \rrbracket$$

which sends a cusp form f to its q-expansion at ∞.

Remark 13.14. Given $\theta : \mathcal{T} \to \mathbb{C}$, we can in fact reconstruct the corresponding cuspidal eigenform. Consider the aforementioned injective map.

$$\begin{tikzcd} S_k(N,\epsilon) \arrow[r, hook] & \mathbb{C}\llbracket q \rrbracket \\ & \mathbb{Z}\llbracket q \rrbracket \arrow[u, hook, "\supseteq"] \end{tikzcd}$$

Define $S_k(N,\epsilon;\mathbb{Z})$ be the inverse image of $\mathbb{Z}[\![q]\!]$ under injection. We also define $S_k(N,\epsilon;A)$ as follows for any commutative ring A with 1.

$$S_k(N,\epsilon;A) := S_k(N,\epsilon;\mathbb{Z}) \otimes_{\mathbb{Z}} A$$

In fact, the following statement holds. The proof of the theorem can be found in [Kat72].

Theorem 13.15 (q-expansion principle)**.**

$$S_k(N,\epsilon;\mathbb{C}) = S_k(N,\epsilon;\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{C} = S_k(N,\epsilon) \tag{13.1}$$

The theorem implies that $S_k(N,\epsilon)$ has basis contained in $S_k(N,\epsilon;\mathbb{Z})$, i.e. one can choose the set of basis of $S_k(N,\epsilon)$ from $\mathbb{Z}[\![p]\!]$. The theorem comes from the fact that $X_0(N)$ is defined over $\mathbb{Z}$.

Recall the explicit formulae of q-expansion of $T_k(m)$ at ∞. By definition, $\mathcal{T}$ acts on $S_k(N,\epsilon;\mathbb{Z})$. Hence, $\mathcal{T}$ embeds in $End(S_k(N,\epsilon;\mathbb{Z}))$.

Note that $End(S_k(N,\epsilon;\mathbb{Z}))$ can be considered as a subset of the matrix ring $M_{g\times g}(\mathbb{Z})$ where g is the dimension of the $\mathbb{C}$-vector space $S_k(N,\epsilon)$. These observations imply a crucial fact about the Hecke Algebra $\mathcal{T}$.

Theorem 13.16. *$\mathcal{T}$ is a finite free $\mathbb{Z}$-algebra.*

Remark 13.17. Note that the existence of θ implies that $Im\theta$ is a finite free $\mathbb{Z}$-algebra in $\mathbb{C}$, i.e. an algebraic number ring of a finite extension of $mathbbQ$. The above theorem hence implies that if f is a normalized cuspidal eigenform, then there exists an algebraic number ring containing all coefficients of f and the image of θ, i.e. $Im(\theta) \subseteq \mathcal{O}_f$ for some algebraic number ring $\mathcal{O}_f$.

Using Hecke Algebra, we will decompose $2g$-dimensional Galois representations into g copies of 2-dimensional representations.

14. 2018-02-28: Hecke Operators and Hecke Algebra II

We start with an example of a Hecke Algebra whose correlated space $S_2(N,\epsilon)$ is not monodimensional.

Example 14.1 (Nasrecki)**.** Let $N = 40$, and consider the set $S_2(40,\epsilon)$, the space of all cusp forms of weight 2, level 40, and trivial nebentypus ϵ. We show that $S_2(40,\epsilon)$ is a 3-dimensional $\mathbb{C}$-vector space, i.e. $X_0(40)$ has genus 3. Note that $S_2(40,\epsilon)$ has the following basis in $S_2(40,\epsilon;\mathbb{Z})$.

$$\begin{aligned} f_1 &= q + q^5 + O(q^6) \\ f_2 &= q^2 + O(q^6) \\ f_3 &= q^3 + q^5 + O(q^6) \end{aligned}$$

Consider the following elements in $End(S_2(40,\epsilon;\mathbb{Z}))$. Note that these elements are not cuspidal eigenforms. If so, then these matrices should be diagonal matrices.

$$T_2(2) = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & -2 \\ 0 & 0 & 0 \end{pmatrix}$$

$$T_2(3) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -2 & 0 \\ 1 & 0 & -2 \end{pmatrix}$$

By the aforementioned properties of Hecke Operators, the following equations hold, where Id is the identity matrix.

$$\begin{aligned} T_2(1) &= Id \\ (T_2(2))^2 &= 0 \\ T_2(3)(T_2(3)+2Id) &= 0 \\ T_2(2)T_2(3) &= -2T_2(2) \\ T_2(4) &= (T_2(2))^2 - 2T_2(1) = -2Id \\ T_2(5) &= T_2(1) + T_2(3) = Id + T_2(3) \\ T_2(6) &= T(2)T(3) = -2T_2(2) \\ &\cdots \end{aligned}$$

It holds that $\mathcal{T}$ is a finitely generated $\mathbb{Z}$-algebra with generators $\{T_2, T_3\}$. In fact, the following equation holds.

$$\mathcal{T} = \mathbb{Z}[T_2(2), T_2(3)] \cong \mathbb{Z}[x,y]/(x^2, y(y+2), xy+2x)$$

Remark 14.2. One may ask whether it is possible to reconstruct a cuspidal form f from the Hecke Algebra $\mathcal{T}$. Let ϵ be a trivial nebentypus. Consider the following construction of $\phi : S_k(N, \epsilon; \mathbb{Z}) \to Hom(\mathcal{T}, \mathbb{Z})$.

$$\phi(f) = (t \mapsto a_1(tf))$$

Here, a_1 is the coefficient of q of the q-expansion of tf. Alternatively, we can also consider the following pairing.

$$\begin{aligned} S_k(N, \epsilon; \mathbb{Z}) \times \mathcal{T} &\to \mathbb{Z} \\ (f, t) &\mapsto a_1(tf) \end{aligned}$$

In fact, ϕ is injective, and $\mathcal{T}$ is free of rank less than the rank of $S_k(N, \epsilon; \mathbb{Z})$. Therefore, ϕ is a bijection.

Recall that the q-expansion Theorem gives the following isomorphism.

$$S_k(N, \epsilon; \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{C} = S_k(N, \epsilon; \mathbb{C}) \cong S_k(N, \epsilon)$$

Therefore, every element in $S_k(N, \epsilon; \mathbb{Z})$ originate from $Hom(\mathcal{T}, \mathbb{Z})$.

Note 14.3. Notice that Hecke Operators also act on $Div^0(X_0(N))$, and hence on $Pic^0(X_0(N)) = J_0(N)$ by linearly extending the following action.

$$T_2(m)[z] = \sum [\alpha_i z]$$

Here, $[z]$ denotes the orbit of $z \in \mathcal{H}^*$ under $\Gamma_0(N)$, and α_i runs through the elements of Δ_N.

Note 14.4. Recall that the image of the homomorphism $\theta : \mathcal{T} \to \mathbb{C}$ associated to a normalized cuspidal eigenform f of weight k, level N, and nebentypus ϵ is contained in some algebraic number ring $\mathcal{O}_f$. Let $f = \sum_{n=1}^{\infty} a_n q^n$ be the q-expansion of f. From now on we will notate $\mathcal{O}_f$ as the smallest number ring containing the following ring.

$$\mathcal{O}_f \supseteq \mathbb{Z}[a_1, a_2, \cdots, a_n, \cdots, Im(\epsilon)]$$

Using Hecke Operators and Hecke Algebra, we can hence decompose the $2g$-dimensional Galois representation into 2-dimensional Galois representations. The following theorem can be understood, in fact, as a special case of Étale cohomology.

Theorem 14.5 (Eichler-Shimura, Deligne, Deligne-Serre)**.** *Let $f = \sum_{n=1}^{\infty} a_n q^n$ be a cuspidal eigenform of weight k, level N, and nebentypus ϵ. Then for each prime ideal λ of $\mathcal{O}_f$ above a rational prime l (i.e. $l = \lambda \cap \mathbb{Z}$), there exists a unique semisimple continuous homomorphism*

$$\rho : G_{\mathbb{Q}} \to GL_2(K_\lambda)$$

which are unramified at primes $p \nmid lN$. Here, K_λ is the fraction field of the λ-adic completion of $\mathcal{O}_f$. Furthermore, the following equation holds for ρ.

$$tr_\rho(Frob_p) = a_p$$
$$det_\rho(Frob_p) = \epsilon(p)p^{k-1}$$

Remark 14.6. Eichler and Shimura proved the case for $k = 2$. Deligne proved the case for $k > 2$ by using Kuga-Sato varieties. Later, Deligne and Serre proved the case for $k = 1$ by using certain congruence to higher weight modular forms. We will focus on proving the case when $k = 2$ and ϵ is trivial.

Sketch of Proof of Theorem 14.5. The uniqueness of the homomorphism ρ follows from Chebotarev Density Theorem, i.e. the image of $Frob_{\mathfrak{p}}$ for each unramified prime $\mathfrak{p}$ is a dense subset of the image of $G_{\mathbb{Q}}$.

For fixed N, consider the set $J_0(N)[l^n]$. We showed that $J_0(N)[l^n] \cong (\mathbb{Z}/l^n)^{2g}$ where $g = dim_{\mathbb{C}}(S_2(N, \epsilon))$. Define the Tate module as follows.

$$T_l(J_0(N)) = \varprojlim_n J_0(N)[l^n]$$

Hence we have the following isomorphism.

$$T_l(J_0(N)) = (\mathbb{Z}_l)^{2g}$$

The idea of the proof is as follows. We will observe the actions of both the Galois group $G_{\mathbb{Q}}$ and the Hecke Algebra $\mathcal{T}$ by possibly extending the scalars of $T_l(J_0(N))$. A composition of group actions will hence result in the desired 2-dimensional Galois representation.

Note that $G_{\mathbb{Q}}$ acts on $T_l(J_0(N))$, as $J_0(N)[l^n] \subset J_0(N)[\overline{\mathbb{Q}}]$. Hence, we can derive the following Galois representation.

$$G_{\mathbb{Q}} \to GL_{2g}(\mathbb{Z}_l)$$

Let W be defined as follows.

$$W = T_l(J_0(N)) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \cong \mathbb{Q}_l^{wg}$$

Hence, we can derive the following relation.

$$G_{\mathbb{Q}} \to GL_{2g}(\mathbb{Z}_l) \subset GL_{2g}(\mathbb{Q}_l)$$

Therefore, $G_{\mathbb{Q}}$ acts on W.

But also note that $\mathcal{T} \otimes_{\mathbb{Z}} \mathbb{Q}_l$ also acts on W. To understand the $\mathcal{T} \otimes_{\mathbb{Z}} \mathbb{Q}_l$-action, we refer to the following crucial Lemma.

Lemma 14.7. *W is free of rank 2 over $\mathcal{T} \otimes_{\mathbb{Z}} \mathbb{Q}_l$.*

The lemma hence explains why we are able to derive 2-dimensional representations. The idea behind proving the lemma is as follows. There exists a Hodge Decomposition of the the first cohomology group of $X_0(N)$ with coefficients in $\mathbb{C}$. A rigorous description of Hodge Decomposition is in [PS89].

$$H^1(X_0(N); \mathbb{C}) = S_2(N, \epsilon) \oplus \overline{S_2}(N, \epsilon)$$

Here, $S_2(N, \epsilon)$ is bijective to the set of homolomorphic differentials on $X_0(N)$ and $\overline{S_2}(N, \epsilon)$ is bijective to the set of anti-holomorphic differentials on $X_0(N)$. Note that $S_2(N, \epsilon; \mathbb{Q}_l)$ is free of rank 1 over $\mathcal{T} \oplus_{\mathbb{Z}} \mathbb{Q}_l$. This follows from the previous remark that $S_k(N, \epsilon; \mathbb{Z})$ is bijective to $Hom(\mathcal{T}, \mathbb{Z})$, i.e. tensoring with $\mathbb{Q}_l$ gives the desired structure of $S_2(N, \epsilon; \mathbb{Q}_l)$. Analogously, $\overline{S_2}(N, \epsilon; \mathbb{Q}_l)$ is free of rank 1 over $\mathcal{T} \oplus_{\mathbb{Z}} \mathbb{Q}_l$. Hence, $H^1(X_0(N); \mathbb{C})$ is free of rank 2 over $\mathcal{T} \oplus_{\mathbb{Z}} \mathbb{Q}_l$.

Note that the stated decomposition of $H^1(X_0(N); \mathbb{C})$ also holds analogously for the first cohomology group $H^1(X_0(N); \mathbb{Q}_l)$, which is in fact the dual of W, i.e. $W = H_1(X_0(N); \mathbb{Q}_l)$. Hence, we have shown that W is free of rank 2 over $\mathcal{T} \oplus_{\mathbb{Z}} \mathbb{Q}_l$, thus proving the Lemma.

Since $G_{\mathbb{Q}}$ acts on W, the Lemma hence yields a 2-dimensional Galois representation.

$$\overline{\rho} : G_{\mathbb{Q}} \to GL_2(\mathcal{T} \oplus_{\mathbb{Z}} \mathbb{Q}_l)$$

Note that the representation above is unramified at primes $p \nmid lN$. This follows from the observation that $X_0(N)$ has good reduction at primes not dividing N.

To understand the formulae of $tr_{\overline{\rho}}(Frob_p)$ and $det_{\overline{\rho}}(Frob_p)$, we refer to Eichler-Shimura relation.

Remark 14.8 (Eichler-Shimura Relation)**.** A heuristic statement of the Eichler-Shimura Relation is that the cusp form inducing the Hecke Operator $T(p)$ can be decomposed as follows.

$$\begin{aligned} T(p) &= Frob_p + V_p \\ p &= Frob_p V_p \end{aligned}$$

Here, V_p denotes the transpose (or the dual) of the Frobenius element, also called as Verschiebung. A rigorous formulation of the relation is described in [Kna92] and [Shi71].

Using Eichler-Shimura Relation, we hence obtain the formulae for the trace and the determinant:

$$\begin{aligned} tr_{\overline{\rho}}(Frob_p) &= T(p) \in \mathcal{T} \otimes_{\mathbb{Z}} \mathbb{Q}_l \\ det_{\overline{\rho}}(Frob_p) &= \epsilon(p) p^{k-1} \end{aligned}$$

Note that we haven't used any condition on f at all to construct the Galois representation $\overline{\rho}$. Now we fix f. We then have the following ring homomorphism, where a_m is the coefficient of q^m-term in the q-expansion of f.

$$\begin{aligned} \theta : \mathcal{T} &\to \mathcal{O}_f \\ T(m) &\mapsto a_m \end{aligned}$$

This hence induces the following ring homomorphism.

$$\theta \otimes_{\mathbb{Z}} \mathbb{Q}_l : \mathcal{T} \otimes_{\mathbb{Z}} \mathbb{Q}_l \to \mathcal{O}_f \otimes_{\mathbb{Z}} \mathbb{Q}_l \cong \prod_{\lambda | l} K_\lambda$$

Consider the following projection, denoted as π_λ.

$$\pi_\lambda : \prod_{\lambda | l} K_\lambda \to K_\lambda$$

Hence, the composition $\pi_\lambda \circ \theta \otimes_{\mathbb{Z}} \mathbb{Q}_l$ induces the following map.

$$\pi_\lambda \widetilde{\circ\, \theta \otimes_{\mathbb{Z}}} \mathbb{Q}_l : GL_2(\mathcal{T} \otimes_{\mathbb{Z}} \mathbb{Q}_l) \to GL_2(K_\lambda)$$

Therefore, there exists the following 2-dimensional Galois representation.

$$\rho:\ G_{\mathbb{Q}} \xrightarrow{\bar{\rho}} GL_2(\mathcal{T}\otimes_{\mathbb{Z}}\mathbb{Q}_l) \xrightarrow{\widetilde{\pi_\lambda\circ\theta\otimes_{\mathbb{Z}}\mathbb{Q}_l}} GL_2(K_\lambda)$$

The desired formulae of the trace and the determinant also follows from the above composition of maps.

$$\begin{aligned} tr_\rho(Frob_p) &= (\pi_\lambda\circ\theta\otimes_{\mathbb{Z}}\mathbb{Q}_l)(T(p)) = a_p \\ det_\rho(Frob_p) &= (\pi_\lambda\circ\theta\otimes_{\mathbb{Z}}\mathbb{Q}_l)(\epsilon(p)p^{k-1}) = \epsilon(p)p^{k-1} \end{aligned}$$

□

In next lecture, we will be discussing Serre's Conjecture and return to understanding Frey's elliptic curves.

15. 2018-03-02: Invariants of Galois Representations and Semistable Representations I

Exercise 15.1. Show that any compact subgroup of $\mathrm{GL}_2(K_\lambda)$ lies inside some conjugate of $\mathrm{GL}_2(\mathcal{O}_\lambda)$ where $\mathcal{O}_\lambda$ is the valuation ring of K_λ.

In this lecture, we are going to introduce the notion of the semistable Galois representations and discuss Serre's modularity conjecture.

Problem 15.2. *Let F be a finite field of char $l>2$ and $\bar{\rho}: G_{\mathbb{Q}}\to\mathrm{GL}_2(F)$ a continuous homomorphism. Does $\bar{\rho}$ come from some cuspidal eigenform?*

Thinking of the previous lecture and the exercise above, we have the following diagram

$$\begin{tikzcd} & \mathrm{GL}_2(\mathcal{O}_\lambda)\ , \arrow[d, two heads] \\ G_{\mathbb{Q}} \arrow[ru] \arrow[r] & \mathrm{GL}_2(k_\lambda) \end{tikzcd}$$

here k_λ is the residue field of $\mathcal{O}_\lambda$. Regarding the problem, F may be viewed as k_λ and the question could be translated as whether we could find such lift which comes from some cuspidal eigenform.

Note the fact $\det\bar{\rho} = \epsilon\circ\chi^{k-1}$, here χ is the cyclotomic character. The complex conjugation denoted by c sends ζ to $\bar{\zeta}$ and if ζ is a root of 1, $\bar{\zeta}=\zeta^{-1}$. So $\chi(c)=-1$ which tells $\det\bar{\rho}(c)=-1$. We introduce

Definition 15.3. A representation $\bar{\rho}$ is called odd if $\det\bar{\rho}(c)=-1$ and even if $\det\bar{\rho}(c)=+1$.

According to the note above, $\bar{\rho}$ had better be odd if it is going to come from a cuspidal eigenform.

Definition 15.4. Given $\bar{\rho}: G_{\mathbb{Q}}\to\mathrm{GL}_2(F)$ as above, we could get $\bar{\rho}_l: G_{\mathbb{Q}_l}\to\mathrm{GL}_2(F)$. A $G_{\mathbb{Q}_l}$-action on F^2 defines an étale group scheme over $\mathbb{Q}_l$. We call ρ good at l if this group scheme comes via base change from a finite flat group scheme over $\mathbb{Z}_l$ and $\det\bar{\rho}_l|_{I_l}=\chi|_{I_l}$, here I_l is the inertial subgroup of $G_{\mathbb{Q}_l}$. We call $\bar{\rho}$ ordinary at l if $\bar{\rho}_l|_{I_l}$ is conjugate to $\begin{pmatrix}\chi|_{I_l} & * \\ 0 & 1\end{pmatrix}$. $\bar{\rho}$ is called semistable at l if it is either good or ordinary at l.

For the prime number $p \neq l$, we look at the local representation $\bar{\rho}_p : G_{\mathbb{Q}_p} \to \mathrm{GL}_2(F)$. $\bar{\rho}$ is called good at p if $\bar{\rho}$ is unramified at p. $\bar{\rho}$ is called semistable at p if $\bar{\rho}(I_p)$ is unipotent, i.e., all its eigenvalues are 1, which tells that it is conjugate to $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

We call $\bar{\rho}$ semistable if $\bar{\rho}$ is semistable at all primes.

Remark 15.5. The meaning of 'base change' in the definition is that there exists a $\mathbb{Z}_l$-algebra R such that $R \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ represents the given étale group scheme.

Given $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(F)$, here F is a finite field with the characteristic $l > 2$. Assume $\bar{\rho}$ is odd, we want to define positive integers $N(\bar{\rho})$, $k(\bar{\rho})$ and a group homomorphism $\epsilon(\bar{\rho}) : (\mathbb{Z}/N(\bar{\rho}))^\times \to \mathbb{C}^\times$. We make a further assumption that $\bar{\rho}$ is absolutely irreducible, i.e., $\bar{F}^2$ acted on by $G_{\mathbb{Q}}$ has no nontrivial invariant subspace.

In [Ser87], Serre made the following two conjectures.

Conjecture 15.6 (weak Serre conjecture)**.** *There exists a cuspidal eigenfrom whose associated Galois representation is $\bar{\rho}$.*

Conjecture 15.7 (strong Serre conjecture)**.** *There exists a cuspidal eigenform f of level $N(\bar{\rho})$, weight $k(\bar{\rho})$ and Nebentypus $\epsilon(\bar{\rho})$ whose associated Galois representations is $\bar{\rho}$.*

Remark 15.8. The strong Serre conjecture would imply Fermat's last theorem. Assume there exists a counterexample to the Fermat's last theorem, a triple of integers (a, b, c) such that $a^l + b^l + c^l = 0$. The Frey elliptic curve E, $y^2 = x(x - a^l)(x + b^l)$ produces the Galois representation $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[l]) \cong \mathrm{GL}_2(\mathbb{F}_l)$. According to the rule how $N(\bar{\rho}), k(\bar{\rho}), \epsilon(\bar{\rho})$ are determined, we get $N(\bar{\rho}) = 2, k(\bar{\rho}) = 2$ and $\epsilon(\bar{\rho})$ is trivial. But the important fact is that there does not exist a nonzero cuspidal eigenform of weight 2, level 2 and trivial Nebentypus.

In 1986-87, Ribet and others showed that the weak Serre conjecture implies the strong Serre conjecture. (To the reader who wants to learn more about Serre's conjecture or curious about the meaning of the implication, we recommend [RS01].) Serre's conjecture is now a theorem and was proved by Chandrashekhar Khare and Jean-Pierre Wintenberger in 2008. Some partial results were independently obtained by Luis Dieulefait.

Next, we give the prescription for $N(\bar{\rho}), k(\bar{\rho}), \epsilon(\bar{\rho})$. $N(\bar{\rho})$ comes form the local behavior at $p \neq l$ while $k(\bar{\rho})$ and $\epsilon(\bar{\rho})$ come from the local behavior at l.

Consider the prime $p \neq l$ and $\bar{\rho}_p : G_{\mathbb{Q}_p} \to \mathrm{GL}_2(F)$. Let $\mathcal{G}_i$ be the image of the i-th ramification subgroup, here we use the lower numbering. Note that

Fact 15.9. $\mathcal{G}_0 = G_0$ and $\mathcal{G}_1 = G_1$.

Let V_i be the subspace of V fixed by $\mathcal{G}_i$. We set

$$n(p, \bar{\rho}) = \sum_{i=0}^{\infty} \frac{\dim(V/V_i)}{|\mathcal{G}_0/\mathcal{G}_i|}.$$

In [Ser79], it is shown that

Theorem 15.10. *$n(p, \bar{\rho})$ is a non-negative integer.*

Furthermore, one can easily show the following two facts.

Fact 15.11. $n(p, \bar{\rho}) = 0$ if and only if $V = V_0$. The latter is equivalent to $\mathcal{G}_0 (= I_p)$ acting trivially on V. Furthermore, it is true if and only if $\bar{\rho}$ is unramified at p.

Fact 15.12. $n(p, \bar{\rho}) = \dim V$ if and only if $V = V_1$. The latter is equivalent to $\mathcal{G}_1$ acting trivially on V. Furthermore, $n(p, \bar{\rho}) = \dim V$ if and only if $\bar{\rho}$ is tamely ramified at p.

Now, we define the Artin conductor of $\bar{\rho}$, which is

Definition 15.13 (Artin conductor)**.**

$$N(\bar{\rho}) = \prod_{p \neq l} p^{n(p,\bar{\rho})}.$$

According to the fact above, $N(\bar{\rho})$ is well-defined since $\bar{\rho}$ is unramified at all but finitely many primes.

16. 2018-03-09: Invariants of Galois Representations and Semistable Representations II

In the previous lecture we have defined the Artin conductor $N(\bar{\rho})$. Now we turn to define $k(\bar{\rho})$ and $\epsilon(\bar{\rho})$ which come from $\bar{\rho}|_{G_{\mathbb{Q}_l}}$.

Since the map $\det \bar{\rho} : G_{\mathbb{Q}} \to F^\times$ has abelian image, it factors through $\mathrm{Gal}(K/\mathbb{Q})$ for some abelian extension K over $\mathbb{Q}$. By Kronecker-Weber theorem, there exists an integer m for which $K \subseteq \mathbb{Q}(\zeta_m)$ where ζ_m is a primitive root of unity. One can show that

Fact 16.1. The smallest m here is $lN(\bar{\rho})$.

We have the map $\det \bar{\rho} : G_{\mathbb{Q}} \to F^\times$ which induces a map from $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ to $F^\times$. It is known that $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/m)^\times \cong (\mathbb{Z}/l)^\times \times (\mathbb{Z}/N(\bar{\rho}))^\times$. Let us consider the restriction on the second factor $(\mathbb{Z}/N(\bar{\rho}))^\times$. Then we get a homomorphism $(\mathbb{Z}/(N(\bar{\rho}))) \to F^\times \hookrightarrow \bar{F}^\times$. Denote the ring of algebraic integers by A. Consider the diagram

$$\begin{tikzcd}
& A^\times \arrow[d] \\
(\mathbb{Z}/N(\bar{\rho}))^\times \arrow[r] \arrow[ur, dashed] & \bar{F}^\times
\end{tikzcd}$$

$\epsilon(\bar{\rho})$ is defined to be the lift composed with the map $A^\times \hookrightarrow \mathbb{C}^\times$.

We would like to have $\det \bar{\rho} = \epsilon(\bar{\rho})\chi^{k(\bar{\rho})-1}$. This determines the value of $k(\bar{\rho}) \mod l-1$. One can show that

Fact 16.2. $\chi : G_{\mathbb{Q}} \to F^\times$ has image landing in $\mathbb{F}_l^\times$.

In section 5, it was shown that $\bar{\rho}|_{G_{\mathbb{Q}_l}}$ is tamely ramified. This tells us that $\bar{\rho}|_{I_l}$ has cyclic image of order prime to l in $\mathrm{GL}_2(\bar{F})$ and so is diagonalizable over $\bar{F}$. Let $\phi, \phi' : I_l \to \bar{F}^\times$ be the two characters this produces. Serre gives a prescription for $k(\bar{\rho})$ in terms of ϕ, ϕ' which is quite complicated but just depends on what ϕ, ϕ' are in terms of fundamental characters. Here, we provide the following example.

Example 16.3. If $\bar{\rho}|_{I_l} \sim \begin{pmatrix} \chi^a & 0 \\ 0 & \chi^b \end{pmatrix}$, here $0 < a < b < l-1$, then $k(\bar{\rho}) = 1 + a + b + (l-1)a$.

Theorem 16.4. *$\bar{\rho}$ is semistable if and only if $N(\bar{\rho})$ is square-free, $\epsilon(\bar{\rho})$ is trivial and $k(\bar{\rho})$ is 2 or $l+1$.*

Sketch of the proof. $\bar{\rho}$ is semistable implies $\det \bar{\rho}|_{I_l} = \chi|_{I_l}$ while $\det \bar{\rho}|_{I_l} = \epsilon(\bar{\rho})\chi^{k(\bar{\rho})-1}$. So it is equivalent to $\epsilon(\bar{\rho})$ is trivial and $k(\bar{\rho}) - 1 \equiv 1 \mod l-1$. The exact form of $k(\bar{\rho})$ requires Serre's prescription.

As for $N(\bar{\rho}) = \prod_{p \neq l} p^{n(p,\bar{\rho})}$ being square-free, $n(p, \bar{\rho}) = 1$ if and only if V_0 $(= V^{\mathcal{G}_0})$ has dimension 1 and V_1 $(= V^{\mathcal{G}_1})$ is V, which is equivalent to $\bar{\rho}$ is ordinary at p. □

Suppose R is a complete Noetherian local ring with residue field F which is finite of characteristic $l > 2$. It is natural to ask the following question.

Problem 16.5. *If we have a Galois representation $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(F)$, does there exist a lift $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(R)$?*

$$\begin{tikzcd}
 & GL_2(R) \arrow[d] \\
G_{\mathbb{Q}} \arrow[ur, dashed, "\rho"] \arrow[r, "\bar{\rho}"] & \mathrm{GL}_2(F)
\end{tikzcd}$$

The notions of 'good' and 'semistable' could be extended to more general representations. R is a $\mathbb{Z}_l$-algebra and we can view the cyclotomic character as a map to R via $\chi : G_{\mathbb{Q}} \to \mathbb{Z}_l^{\times} \to R^{\times}$.

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(R)$ be a continuous homomorphism, giving a $G_{\mathbb{Q}}$-action on $V = R^2$. We have

Definition 16.6. If $|R| < \infty$, then we call ρ good at l if the associated étale group scheme over $\mathbb{Q}_l$ extends to a finite flat group scheme over $\mathbb{Z}_l$ and $\det \rho|_{I_l} = \chi|_{I_l}$. For general R, we call ρ good at l, if for every closed ideal I of finite index in R, the representation $G_{\mathbb{Q}} \to \mathrm{GL}_2(R/I)$ is good at l.

We call ρ ordinary at l if there is a short exact sequence $0 \to V^{-1} \to V \to V^0 \to 0$ of free R-modules stable under $G_{\mathbb{Q}_l}$, such that I_l acts trivially on V_0 and χ on V_1 such that

$$\rho|_{I_l} \sim \begin{pmatrix} \chi|_{I_l} & * \\ 0 & 1 \end{pmatrix}.$$

We call ρ semistable at l if ρ is good or ordinary at l and $\det \rho|_{I_l} = \chi|_{I_l}$.

In [FM95], Fontaine and Mazur have made an extremely influential conjecture. The following is a special case of the major conjecture.

Conjecture 16.7 (Fontaine-Mazur conjecture)**.** *If $\mathcal{O}$ is the valuation ring of a finite extension of $\mathbb{Q}_l$ and $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O})$ is a continuous absolutely irreducible homomorphism which is unramified at all but finitely many primes and semistable at l, then there exists a cuspidal eigenform f whose associated Galois representation is ρ.*

Remark 16.8. In our big picture of Fermat's last theorem, assuming there exists a counterexample, it gives us a Frey elliptic curve E. In the following lectures, we will show it is a semistable elliptic curve. The associated Galois representation $\bar{\rho}_E$ will be semistable.

Consider the lifts of $\bar{\rho}_E$ coming from elliptic curves and from modular forms. They are all semistable Galois representations lifting $\bar{\rho}_E$. Our goal is to show the lifts from elliptic curves are included in the lifts from modular forms. Fontaine-Mazur conjecture predicts that under certain conditions every semistable representations is modular. Wiles' work or the proof of Fermat's last theorem amounts to establishing some special and nontrivial cases of the conjecture.

17. 2018-03-12: Semistable Elliptic Curves

17.1. **Semistable Elliptic Curves.**

The plan is to define semistable elliptic curves, show that the Frey curve associated to a supposed counterexample to FLT is semistable, and finally to show that semistable elliptic curves give rise to semistable Galois representations. This will allow us to live entirely in the world of semistable representations.

Definition 17.1. A *Weierstrass Model* for an elliptic curve $E/\mathbb{Q}$ is an equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{17.1}$$

We will call a Weierstrass model *minimal* at a prime p if $v_p(\Delta)$ is minimal amongst all models with coefficients in $\mathbb{Z}_p$.

Remark 17.2. We can complete the square on the left hand side and complete the cube on the right hand side of (17.1) to obtain a new Weierstrass equation

$$y^2 = x^3 - 27c_4x - 54c_6, \tag{17.2}$$

where

$$\begin{array}{ll} b_2 = a_1^2 + 4ac, & c_4 = b_2^2 - 24b_4, \\ b_4 = 2a_4 + a_1a_3, & c_6 = -b_2^3 + 36b_2b_4 - 216b_6. \\ b_6 = a_3^2 + 4a_6\ , & \end{array}$$

This new curve has discriminant

$$\Delta = \frac{c_4^3 - c_6^2}{1728}.$$

This model will be of use to us in the future.

Definition 17.3. We say that E has *good reduction* at a prime p if there exists a Weierstrass equation for E with coefficients in $\mathbb{Z}_p$ such that reducing the coefficients mod p gives an elliptic curve over $\mathbb{F}_p$. For such a Weierstrass equation, this is equivalent to $\Delta \notin p\mathbb{Z}_p$.

Example 17.4. Here is an example showing that good reduction is more subtle than it may appear. Consider the elliptic curve $E : y^2 = x^3 - 64$. It certainly looks like this curve has bad reduction at 2, but the change of variables $x = 4X, y = 8Y$ defines an isomorphism of E with the curve $Y^2 = X^3 - 1$. Thus E has good reduction at 2, since we found an isomorphic curve whose reduction mod 2 is nonsingular.

Example 17.5 (Frey Curve)**.** Let A, B, C be nonzero, relatively prime integers such that $A + B + C = 0$. The example we are most interested in is $A = a^l$, $B = b^l$, $C = c^l$ where $l \geq 5$ is prime (i.e. a counterexample to FLT). Consider the elliptic curve $E : y^2 = x(x - A)(x - B)$. One can work out that the discriminant is $\Delta = 16(ABC)^2$, so E has good reduction at all primes $p \nmid ABC$ (note that one of A, B, C must be even, so I'm not pulling any tricks by not writing 2 explicitly). But could it be that one of these seemingly bad primes secretly has good reduction, like in Example 17.4?

In the case that A, B, C are a counterexample to FLT, we can assume, by relabeling the variables as needed, that $A \equiv -1 \bmod 4$ and $B \equiv 0 \bmod 32$ (here we are using that $l \geq 5$). Make the change of variables $x \mapsto 4x, y \mapsto 8y + 4x$ to obtain the Weierstrass equation

$$y^2 + xy = x^3 + \frac{B - A - 1}{4}x^2 - \frac{AB}{16}x.$$

For this equation, the discriminant turns out to be $2^{-8}(ABC)^2$. How do we know that this model is minimal? If we compute the value of c_4 associated to this Weierstrass model as in (17.2), we find that

$$c_4 = A^2 + AB + B^2.$$

Since $(A, B, C) = 1$, we see that $v_p(C_4) = 0$ for all $p \mid ABC$. Now use the following exercise.

Exercise 17.6 ([Sil09], Exercise 7.1)**.** Let E be an elliptic curve given by a Weierstrass model. Show that this model is minimal at p if and only if $v_p(\Delta) < 12$ or $v_p(c_4) < 4$.

The upshot is that the Frey curve has bad reduction at all primes dividing ABC. We would like a way of classifying the severity of the singularities modulo these primes.

Definition 17.7. If p is a prime of bad reduction for an elliptic curve E, then the reduction of E mod p has a unique singular point, which is either a node or a cusp. If the singularity is a node (resp. cusp), then we say that E has *multiplicative reduction* (resp. *additive reduction*) at p.

We will say that E has *semistable reduction* at p if it has good or multiplicative reduction at p. We say E is *semistable* if E has semistable reduction at every prime.

Example 17.8. The Frey curve is semistable. Intuitively, this can be explained as follows: given a Weierstrass equation $y^2 = f(x)$, a nodal singularity occurs when the $f(x)$ has a double root, while a cuspidal singularity occurs when $f(x)$ has a triple root. The roots of the Frey curve are $0, a^l, b^l$. But since we are assuming that $(a, b, c) = 1$, we cannot have all three roots be equivalent mod p, and so we expect to have at worst multiplicative reduction at all primes. To see this more rigorously, use the following proposition.

Proposition 17.9. *Let E be an elliptic curve over $\mathbb{Q}$ with Weierstrass model*

$$y^2 = x^3 - 27c_4x - 54c_6.$$

Then E has multiplicative reduction at p if and only if $v_p(\Delta) > 0$ and $v_p(c_4) = 0$.

Proof. See Proposition VII.5.1 of [Sil09]. □

We want to know that semistable elliptic curves give us semistable Galois representations. For primes of good reduction, this is accomplished by the following theorem.

Theorem 17.10 (Néron-Ogg-Shafarevich)**.** *Let E an elliptic curve over $\mathbb{Q}$ and $p \nmid m$ a prime. Then E has good reduction at p if and only if the $G_{\mathbb{Q}}$-action on $E[m]$ is unramified at p.*

Proof. ($\Rightarrow$): Let $K/\mathbb{Q}_p$ be a finite extension such that $E[m] \subset E(K)$. Let F be the residue field of K. One can check that the kernel of the reduction map $\phi : E(K) \to E(F)$ contains no points of order prime to p, and so the restriction $E[m] \to E(F)$ is injective. Let $P \in E[m]$, $\tilde{P} = \phi(P)$. If $\sigma \in I_p$, then

$$\phi(\sigma P - \sigma) = \sigma\tilde{P} - \tilde{P} = 0$$

because I_p acts trivially on $E(F)$. Thus $\sigma P - P \in \ker \phi$, and so by injectivity $\sigma P = P$. Therefore I_p acts trivially on $E[m]$.
($\Leftarrow$): Since we will not need this direction, we will not prove it. The interested reader can find a proof in Theorem VII.7.1 of [Sil09]. □

What about the primes of multiplicative reduction? This will be taken care of by the theory of Tate curves.

18. 2018-03-14: Tate Curves

Last time, we introduced the notion of semistability for elliptic curves. We wanted to know that semistable elliptic curves give rise to semistable Galois representations.

Theorem 18.1. *If E is a semistable elliptic curve over $\mathbb{Q}$, then $\rho_{E,l^\infty} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_l)$ is semistable for all primes l.*

Proof. First note that the Weil pairing implies that $\bigwedge^2 T_l(E) \simeq \mu_{l^\infty}$ as $G_{\mathbb{Q}}$-modules. Thus $\det \rho_{E,l^\infty} = \chi$, the cyclotomic character. It remains to check that ρ_{E,l^∞} is either good or ordinary at all primes. There are four cases to consider:

Case 1: E has good reduction at $p \neq l$
We handled this case in Theorem 17.10.

Case 2: E has good reduction at l.
We showed this implies $E[l^n]$ comes from a finite flat group scheme over $\mathbb{Z}_l$, and so by definition ρ_{E,l^∞} is good at l.

Case 3: E has bad (hence multiplicative) reduction at $p \neq l$

Case 4: E has bad reduction at l

To handle the final two cases, we will need to develop the theory of Tate curves.

18.1. Tate Curves.

There is an isomorphism

$$\begin{aligned} \mathbb{C}/\mathbb{Z} &\xrightarrow{\sim} \mathbb{C}^\times \\ z &\mapsto e^{2\pi i z} \end{aligned}$$

relating the additive structure on $\mathbb{C}$ to the multiplicative structure. Something similar can be done for elliptic curves over $\mathbb{C}$. Let Λ be a lattice in $\mathbb{C}$ with basis $1, \tau$ where $\tau \in \mathcal{H}$. Let $q = e^{2\pi i \tau}$. We know that there is an isomorphism $E_\Lambda(\mathbb{C}) \to \mathbb{C}/\Lambda$ where E_Λ is the elliptic curve defined by

$$y^2 = 4x^3 - 60G_4(\Lambda)x - 140G_6(\Lambda). \tag{18.1}$$

Furthermore, there is an isomorphism

$$\begin{aligned} \mathbb{C}/\mathbb{Z} &\xrightarrow{\sim} \mathbb{C}^\times \\ z &\mapsto e^{2\pi i z} \end{aligned} \tag{18.2}$$

Tate's observation was that while we don't have a good notion of lattices in $\overline{\mathbb{Q}}_p$, we can define an analogue of (18.2). Towards this end, make the change of variables

$$\begin{aligned} x &= (2\pi i)^2 \left(X + \frac{1}{12} \right), \\ y &= (2\pi i)^3 (2Y + X) \end{aligned}$$

in (18.1) to obtain the new curve

$$E_q : Y^2 + XY = X^3 + a_4 X + a_6;$$

the a_i are defined by

$$\begin{aligned} a_4 &= \frac{-15G_4(\Lambda)}{(2\pi i)^4} + \frac{1}{48} = -5 \sum_{n=1}^{\infty} \frac{n^3 q^n}{1 - q^n}, \\ a_6 &= \frac{-35G_6(\Lambda)}{(2\pi i)^6} - \frac{5G_4(\Lambda)}{4(2\pi i)^4} + \frac{1}{1728} = -q - 23q^2 - \cdots . \end{aligned}$$

The discriminant of E_q is given by $\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24}$, and the j-invariant is the usual

$$j = \frac{1}{q} + 744 + 196884q + \cdots . \tag{18.3}$$

Exercise 18.2. Show that $a_4, a_6 \in \mathbb{Z}[[q]]$. Thus we may consider E_q as a curve defined over any field.

Theorem 18.3. *Let $K/\mathbb{Q}_p$ be a finite extension. Let $q \in K^\times$ with $|q| < 1$. Then a_4, a_6 converge in K. If we define*

$$E_q : y^2 + xy = x^3 + a_4x + a_6,$$

then E_q is an elliptic curve over K and for any algebraic extension L/K, there is an isomorphism of G_K-modules

$$E_q(L) \simeq L^\times/q^{\mathbb{Z}}$$

Remark 18.4. Since $|q| < 1$, the reduction of E_q is given by $y^2 + xy = x^3$, which has split multiplicative reduction. Conversely, if E has multiplicative reduction at p, then its j-invariant $j = c_4^3/\Delta$ satisfies $v_p(j) < 0$. We can then solve for j in (18.3) to obtain

$$q = j^{-1} + 744j^{-2} + 750420j^{-3} + \cdots .$$

Because $v_p(j) < 0$, this series converges and $v_p(q) = -v_p(j) > 0$, hence $|q| < 1$.

This shows that given an elliptic curve E with multiplicative reduction at p, we get a Tate curve E_q with $j(E_q) = j(E)$. By standard properties of j-invariants, we see that E and E_q are isomorphic over a quadratic extension of K. We can in fact say more.

Theorem 18.5. *Let E be an elliptic curve over $\mathbb{Q}$ with multiplicative reduction at p. Let $\delta : G_{\mathbb{Q}_p} \to \{\pm 1\}$ be the trivial character if E has split multiplicative reduction at p, and let δ be the unique unramified quadratic character otherwise. Then there exists $q \in \mathbb{Q}_p^\times$ such that there is an isomorphism*

$$\phi : E(\overline{\mathbb{Q}}_p) \to (\overline{\mathbb{Q}}_p^\times/q^{\mathbb{Z}})(\delta)$$

of $G_{\mathbb{Q}_p}$-modules, where $\sigma \in G_{\mathbb{Q}_p}$ acts on the right hand side by $\sigma(x) = \sigma(x^{\delta(\sigma)})$. Thus

$$\rho_{E,l^\infty}|_{G_{\mathbb{Q}_p}} \sim \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix} \otimes \delta$$

Sketch of proof. The first statement is essentially Theorem 18.3. We need to prove the statement about ρ_{E,l^∞}. Given an elliptic curve E, construct the Tate curve E_q as explained. We have

$$E_q[l^n] \hookrightarrow E_q(\overline{\mathbb{Q}}_p) \xrightarrow{\sim} \overline{\mathbb{Q}}_p^\times/q^{\mathbb{Z}}.$$

It is much easier to describe the l^n torsion on the right hand side. In particular, $x \in \overline{\mathbb{Q}}_p^\times/q^{\mathbb{Z}}$ is such that x^{l^n} is trivial if and only if $x^{l^n} = q^m$ for some $m \in \mathbb{Z}$, which is if and only if $x = \zeta_{l^n}^a(q^{1/l^n})^b$ for some $0 \le a, b < l^n$. Consider the map

$$\begin{aligned} E[l^n] &\to \langle q\rangle/\langle q^{l^n}\rangle \\ x &\mapsto x^{l^n}. \end{aligned}$$

This is a homomorphism with kernel $\mu_{l^n}(\overline{\mathbb{Q}}_p)$. In other words, we have a short exact sequence of $G_{\mathbb{Q}_p}$-modules

$$0 \longrightarrow \mu_{l^n}(\overline{\mathbb{Q}}_p) \longrightarrow E[l^n] \longrightarrow \mathbb{Z}/l^n \longrightarrow 0,$$

where $G_{\mathbb{Q}_p}$ acts by the cyclotomic character on the left and trivially on the right, because $q \in \mathbb{Q}_p$. Now twist by δ. □

This finishes the remaining cases in the proof of Theorem 18.1.

Theorem 18.6. *Suppose that $E/\mathbb{Q}$ has multiplicative reduction at $p > 2$. Then $\rho_{E,l} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_l)$ is good at p if and only if $l \mid v_p(\Delta_{\min})$.*

Proof. Consider the l-division field of E_q, namely $K = \mathbb{Q}_p(\zeta_l, q^{1/l})$. In the case that $p \neq l$, note that

$$\begin{aligned} l \mid v_p(\Delta_{\min}) &\iff l \mid v_p(q) \\ &\iff K/\mathbb{Q}_p \text{ is unramified at } p \\ &\iff \rho_{E,l} \text{ is unramified at } p. \end{aligned}$$

The case $p = l$ is much more complicated; we refer the reader to section 8 of [Edi92]. □

For the Frey curve $E : y^2 = x(x-a^l)(x-b^l)$ where l is a prime at least 5 and $a^l + b^l + c^l = 0$, we saw that $\Delta_{\min} = 2^{-8}(abc)^{2l}$. If $p \neq 2$, then $l \mid v_p(\Delta_{\min})$; therefore $\rho_{E,l}$ is good at all primes $p > 2$. Being good at l gives that $k(\rho_{E,l}) = 2$, and being good at $p \neq l$ and semistable at 2 implies $N(\rho_{E,l}) = 2$. Since $\det \rho_{E,l} = \chi$, with no twist, $\epsilon(\rho_{E,l})$ is trivial. Therefore Serre's strong conjecture says that $\rho_{E,l}$ is associated to a cuspidal eigenform of weight 2, level 2, and trivial Nebentypus. But one can easily show that there are no nonzero such forms!

The upshot is that the strong Serre conjecture implies Fermat's last theorem. We will see that Ribet showed, at least in our circumstances, that the weak Serre conjecture implies the strong conjecture. Consequently, to prove Fermat's last theorem it will be enough to prove a special case of the Taniyama-Shimura conjecture.

19. 2018-03-16: Deformation theory I

19.1. **Ribet's Theorem.** Last time we have shown that a semistable elliptic curve E, e.g. Frey curve, will give rise to a semistable Galois representation $\rho_{E,l}$. If $\rho_{E,l}$ is absolutely irreducible, then we could apply strong form of Serre's conjecture to relate $\rho_{E,l}$ to a certain cuspidal eigenform. By studying the good primes of $\rho_{E,l}$, we could determine such a cuspidal eigenform $\rho_{E,l}$ associated to must have weight 2, level 2 and trivial Nebentypus, which does not exist.

Firstly, we want to show that our $\rho_{E,l}$ satisfies the condition of Serre's conjecture.

Question 19.1. Is $\rho_{E,l}$ absolutely irreducible?

By definition, absolutely irreducible means that $\rho_{E,l}$ is irreducible over the algebraic closure of $\mathbb{F}_l$. The answer is yes. Suppose it is reducible, then $E[l]$ would have a 1-dimensional subspace or quotient space on which $G_{\mathbb{Q}}$ acts trivially. This corresponds to a rational non-cuspidal point on the modular curve $X_0(l)$ on which $G_{\mathbb{Q}}$ acts trivially, which means that $X_0(l)$ has a rational point over $\mathbb{Q}$, which contradicts Mazur's theorem for large l.

Theorem 19.2 (Mazur)**.** *If $E/\mathbb{Q}$ has a rational subgroup of order l, then $l \leq 19$, or $l = 37, 43, 67, 163$.*

Serre has the following conjecture in this direction, which is still open.

Conjecture 19.3 (Serre's uniformity conjecture)**.** *If $E/\mathbb{Q}$ has no complex multiplication, and $l > 37$, then $\rho_{E,l} : G_{\mathbb{Q}} \to Aut(E[l])$ is surjective (which implies irreducible).*

Secondly, Ribet's following theorem on level lowering prove that weak form of Serre's conjecture implies strong form of Serre's conjecture.

Theorem 19.4 (Ribet, 1987)**.** *Suppose $\rho : G_{\mathbb{Q}} \to GL_2(F)$ is odd, continuous, absolutely irreducible, over a finite field F of character $l > 2$. Suppose ρ is associated to some cuspidal eigenform of level N, weight 2. If $p|N$ and ρ is good at p, then ρ is associated to some cuspidal eigenform of level $\frac{N}{p}$, weight 2 and trivial ϵ.*

Therefore FLT follows from Taniyama-Shimura conjecture.

19.2. **Deformation Theory.** In this section, we are going to give a start to introduce deformation theory. It is a key tool used in the proof of Taniyama-Shinura. Taniyama-Shimura conjecture says that any semistable Galois representation that comes from a semistable elliptic curve is modular. Given $\bar{\rho}$ a semistable Galois representation, Wile's proof basically shows that the space of semistable deformation associated to modular forms is the same as the space of semistable deformations of $\bar{\rho}$, and proves that any semistable deformation of $\bar{\rho}$ is associated to a modular form.

Fix a profinite group G, a finite field F and a continuous homomorphism $\bar{\rho} : G \to GL_n(F)$. Denote $\mathscr{C}_F$ to be the category of complete Noetherian local ring with residue field F. The morphism in this category are those $\phi : R \to S$ which map $\phi(m_R)$ to m_S and induce an identity $R/m_R \simeq S/m_S \simeq F$.

Definition 19.5. Given R a ring in $\mathscr{C}_F$, a *lift of $\bar{\rho}$ to R* is a continuous homomorphism $\rho : G_{\mathbb{Q}} \to GL_n(R)$ which induces $\bar{\rho}$ by mod m_R.

Definition 19.6. Two lifts ρ_1 and ρ_2 are called *strictly equivalent* if $\exists M \in Ker(GL_n(R) \to GL_n(F))$ such that $\rho_1 = M^{-1}\rho_2 M$.

Definition 19.7. A *deformation* of $\bar{\rho}$ to R is a strict equivalent class of lift of $\bar{\rho}$ to R.

Now fix a group representation $\bar{\rho} : G \to GL_n(F)$, we define the following function from $\mathscr{C}_F$ to sets

$$E(R) = \{\text{deformations of } \bar{\rho} \text{ to } R\}.$$

It has functorial property that a morphism $R \to S$ will yield $E(R) \to E(S)$.

20. 2018-03-19: Deformation theory II

20.1. **Mazur's theorem.** We want to understand the following question:

Question 20.1. Is the functor E representable?

If E is representable, then we can parametrize the deformations by a certain $\mathcal{R}$, therefore we could compare two spaces of deformations by comparing their $\mathcal{R}$. For certain type of groups G, Mazur gives a positive answer to this question.

Definition 20.2. We say that G *satisfies* (†) if the maximal elementary-l-abelian quotient of every open subgroup if finite.

Exercise 20.3. Both $G_{\mathbb{Q}_p}$ and $G_{\mathbb{Q},S}$ satisfy (†).

Indeed, these could be shown by local and global class field theory respectively. Notice that by Neron-Ogg-Shafarevich, all Galois representations associated to elliptic curves factor through $G_{\mathbb{Q},S}$ for some finite set of primes S.

Theorem 20.4 (Mazur)**.** *Suppose $\bar{\rho}$ is absolutely irreducible and that G satisfies* (†)*, then the associated functor E is representable, i.e., $\exists\mathcal{R}(\bar{\rho})$ in $\mathscr{C}_F$ and a continuous homomorphism $\xi : G \to GL_n(\mathcal{R}(\bar{\rho}))$, a universal deformation, such that for every lift ρ of $\bar{\rho}$ to R in $\mathscr{C}_F$, $\exists$ a unique morphism $\pi : \mathcal{R}(\bar{\rho}) \to R$ such that ρ is strictly equivalent to $\pi \circ \xi$.*

Exercise 20.5. Say $\bar{\rho} : G_{\mathbb{Q},S} \to GL_2(\mathbb{F}_l)$ is odd, absolutely irreducible and $l \in S$, then $\mathcal{R}(\bar{\rho})$ is $\mathbb{Z}_l[[T_1, T_2, T_3]]$.

20.2. **Schlessinger's criterion.** The proof of Mazur's theorem follows from Schlessinger's work on criterion for representability. We will first describe Schlessinger's work here.

Let $\mathscr{C}_F^0$ denote the subcategory of $\mathscr{C}_F$ of Artinian rings.

Definition 20.6. Call a morphism $R \to S$ *small* if it is surjective and the kernel is a principal ideal where product with m_R is 0.

Example 20.7. The ring of dual numbers for F is the ring $F[\epsilon] = F[T]/(T^2)$. The morphism $\pi : F[\epsilon] \to F$ which maps $\pi(a + b\epsilon) = a$ is small.

Definition 20.8. Suppose E is a functor from $\mathscr{C}_F$ to sets and $|E(F)| = 1$. Let $R_1 \to R_0$ and $R_2 \to R_0$ be morphisms in $\mathscr{C}_F^0$. Consider the natural map $(*)$

$$E(R_1 \times_{R_0} R_2) \to E(R_1) \times_{E(R_0)} E(R_2).$$

The existence of this map comes from the universal property of the fiber product, which is $E(R_1) \times_{E(R_0)} E(R_2)$ here. *Schlessinger's criterion* are as follows:

(1) H1. If the morphism $R_2 \to R_0$ is small, then $(*)$ is a surjection.
(2) H2. If $R_0 = F$, $R_2 = F[\epsilon]$, and $R_2 \to R_0$ is π defined before, then $(*)$ is bijective. (Therefore H2 guarantees that $t_E = E(F[\epsilon])$ has an F-vector space structure. We call t_E the tangent space.)
(3) H3. t_E is finite dimensional F vector space.
(4) H4. If $R_1 = R_2$ and $R_i \to R_0$ for $i = 1, 2$ are the same small morphism, then $(*)$ is bijective.

Theorem 20.9 (Schlessinger)**.** *H1, H2, H3, H4 holds if and only if E is representable.*

Proof of Mazur's theorem. By Schlessinger's criterion, it suffices to show $E(R)$ satisfies H1, H2, H3 and H4.

Let $E_i = \{$continuous homomorphisms $: G \to GL_n(R_i)$ lifting $\bar{\rho}\}$ and $K_i = \Gamma_n(R_i) := Ker(GL_n(R_i) \to GL_n(F))$. Then by definition of $E(R)$, we have $E(R_i) = E_i/K_i$. Denote R_3 to be $R_1 \times_{R_0} R_2$.

To show H1, we take $\rho_1 \in E_1$, $\rho_2 \in E_2$ that are mapped to the same element of E_0/K_0, i.e., $\bar{\rho_1} = M\bar{\rho_2}M^{-1}$ for some $M \in K_0$. Since $R_2 \to R_0$ is surjective, then $K_2 \to K_0$ is surjective. Let N be a preimage of $M \in K_0$. Then $(\rho_1, N\rho_2 N^{-1})$ is a preimage of (ρ_1, ρ_2).

To show H4, it suffices to show $(*)$ is injective. One can show that if the map between centralizers $C_{K_2}(\rho_2(G)) \to C_{K_0}(\rho_0(G))$ is surjective, then $(*)$ is injective. If $\bar{\rho}$ is absolutely irreducible, then both centralizers consist of scalar matrix, therefore the map is surjective. So H4 holds, and H2 follows in the same way.

Finally, we show H3. First, the kernel $\Gamma_n(F[\epsilon])$ is elementary-l-abelian. Indeed, the kernel consists of elements in the form

$$\begin{bmatrix} 1+a_{11}\epsilon & a_{12}\epsilon & \cdots & \cdots & a_{1n}\epsilon \\ a_{21}\epsilon & 1+a_{22}\epsilon & \cdots & \cdots & a_{2n}\epsilon \\ \vdots & \ddots & \cdots & \cdots & \vdots \\ \vdots & \vdots & \ddots & \cdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1}\epsilon & \cdots & \cdots & \cdots & 1+a_{nn}\epsilon \end{bmatrix}$$

where $a_{ij} \in F$. So $\Gamma_n(F[\epsilon]) \simeq (F)^{n^2}$. Therefore we can find a subgroup H where the maximal elementary-l-abelian quotient of $Ker(\bar{\rho})$ is $Ker(\bar{\rho})/H$. Then any lift $\rho : G \to GL_n(F[\epsilon])$ must factor through G/H. By (†), the quotient $Ker(\bar{\rho})/H$ is finite, so G/H is finite. Therefore $E(F[\epsilon])$ counts all homomorphisms from a finite group G/H to the finite group $GL_n(F[\epsilon])$, thus finite. □

20.3. **Ramakrishna's refinement.** We're interested in representations satisfying further conditions, e.g. let $\bar{\rho} : G_{\mathbb{Q},S} \to GL_2(\mathbb{F}_l)$ be semistable and absolutely irreducible. Then let

$$E_{ss}(R) = \{\text{semistable deformations of } \bar{\rho} \text{ to } R\}.$$

Question 20.10. Is $E_{ss}(R)$ representable?

Let X be a property of $W(F)[G]$-modules of finite cardinality such that X is closed under isomorphism, direct sum, submodules and quotient modules. Fix $\bar{\rho} : G \to GL_n(F)$ such that F^n considered as a $W(F)[G]$-module satisfies X. For R in $\mathscr{C}_F^0$, let

$$E_X(R) = \{\text{deformations satisfying } X\} \subset E(R).$$

Theorem 20.11 (Ramakrishna). *E_X is a functor on $\mathscr{C}_F^0$. Moreover, if E satisfies H1, H2, H3, H4, then so does E_X.*

It implies that we can extend E_X to $\mathscr{C}_F$ by viewing R in $\mathscr{C}_F$ as an inverse limit.

21. 2018-03-21: Deformation theory III

We define $E_X(R)$ to be the set of deformations of $\bar{\rho}$ to R s.t $\forall$ ideal I of finite index, the induced representations to R/I satisfies X, which is a subset of E(R).

Theorem 21.1. *$E_X$is a representable functor $\mathscr{C}_F^0 \dashrightarrow$Sets , being represented in $\mathscr{C}_F$ (note not in $\mathscr{C}_F^0$)*

Proof. Let R,S be objects in $\mathscr{C}_F^0$, $\phi : R \to S$ a morphism. To show that E_X is a functor, we need to show that if a lift $\rho : G \to GL_n(R)$ has X then so does the composition $G \to GL_n(S)$. Let $B = R^n, D = S^n$ (with given G-actions).ϕ induces a map $B \to D$, making D a finitely generated B-module, thus it's a quotient of B^m. Next note that H1 holds for E_X implies H2 and H4 since the restriction of an injective map is still injective. As for H3, $E_X(F[\epsilon]) \subset E(F[\epsilon])$, so it's also finite dimensional.
To show H1 holds, let $R_3 = R_1 \times_{R_0} R_2$, let $\rho_1 \times_{\rho_0} \rho_2 \in E_X(R_1) \times_{E_X(R_0)} E_X(R_2)$. Since H1 holds for E, it implies that there exists $\rho \in E(R_3)$ mapping to this, we have to show that ρ has X. Note $R_3 \hookrightarrow R_1 \times R_2$ implies $R_3^n \hookrightarrow R_1^n \times R_2^n$, thus R_3 is a submodule of the direct product of $W(F)[G]$-modules, both of which have X, so R_3^n also has X. □

Theorem 21.2. *suppose E and E_X satisfy the hypothesis of the previous theorem, let $\mathcal{R}$ and $\mathcal{R}_X$ be their universal deformation rings respectively, then there's a natural surjection $\mathcal{R} \twoheadrightarrow \mathcal{R}_X$*

Proof. Let $\xi : G \to GL_n(\mathcal{R})$ and let $\xi_X : G \to GL_n(\mathcal{R}_X)$ be the universal deformations. ξ_X is a lift of $\bar{\rho}$, so $\exists!$ morphism $\phi : \mathcal{R} \to \mathcal{R}_X$ (up to strict equivalence) s.t. $\phi \circ \xi = \xi_X$. Let the image of ϕ be S. Then we have a representation $\rho : G \to GL_n(S)(\rho := \phi \circ \xi)$ which has X. Thus there exists a unique morphism $\mathcal{R}_X \to S$ producing this, now consider $\mathcal{R}_X \to S \hookrightarrow \mathcal{R}_X$ and universality, the composition has to be the identity map, which implies that $S \simeq \mathcal{R}_X$ □

Fix $\bar{\rho} : G_{\mathbb{Q}} \to Gl_2(F)$, (F finite field with characteristic > 2) which is absolutely irreducible and semistable (note this induces $\det \bar{\rho} =$ cyclotomics, so $\bar{\rho}$ is odd) Next we need an auxiliary finite set Σ of primes. Let R be in $\mathscr{C}_F^0$, if ρ is a lift of $\bar{\rho}$ to R, say ρ is of type Σ if
(1) $\det \rho =$ cyclotomic character
(2) ρ is semistable at l.
(3) if $l \in \Sigma$ and $\bar{\rho}$ is good at l then ρ is good at at l; If $p \notin \Sigma \cup \{l\}$ and $\bar{\rho}$ is unramified at p, then ρ is unramified at p; if $p \notin \Sigma \cup \{l\}$ and $\bar{\rho}$ is ramified (so ordinary) then ρ is ordinary at p.

Remark 21.3. At primes $\notin \Sigma$, the behavior of ρ is constrained to be no worse than the behavior of $\bar{\rho}$. While within Σ, any behavior of ρ is okay so long as it's semistable at l.

Example 21.4. Frey curve $E : y^2 = x(x-A)(x-B)$ where $A = a^l$, $B = b^l$, $C = c^l$ satisfies $A + B + C = 0$, then $\bar{\rho} = \rho_{E,p} : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_p)$ is unramified outside 2,l (Recall that $l | v_p(\Delta_{min})$ while a lift $\rho = \rho_{E,l^\infty} : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}_l)$ is ramified at those primes dividing abc

Remark 21.5. (1) If E is a semistable elliptic curve over $\mathbb{Q}$ and $\rho_{E,l}$ is absolutely irreducible then $\rho = \rho_{E,l^\infty}$ is a lift of type Σ if Σ constrains all primes of bad reductions for E
(2) If ρ is of type $\Sigma \subseteq \Sigma'$ then ρ is also of type Σ'
(3) If ρ is of type Σ, then ρ is unramified outside $\{p | lN(\bar{\rho})\} \cup \Sigma$
(4) A lift ρ of $\bar{\rho}$ unramified outside Σ with $\det \bar{\rho} =$ cyclotomic character, semistable at l is of type $\Sigma \cup \{l\}$

Theorem 21.6. *(Ramakrishna) The functor $E_\Sigma : \mathscr{C}_F \dashrightarrow$Sets that $R \mapsto \{$deformations of $\bar{\rho}$ to R of type $\Sigma\}$ is representable*

We'll prove later that another functor $\mathscr{C}_F \dashrightarrow$Sets defined by $R \mapsto \{$deformations of $\bar{\rho}$ to R of type Σ, associated to a modular form$\}$ is also representable, if we denote their universal representing rings by R_Σ and $\mathbb{T}_\Sigma$ respectively, then we'll show that the natural surjection $R_\Sigma \twoheadrightarrow \mathbb{T}_\Sigma$ is an isomorphism.

22. 2018-03-23: Deformation theory IV

Last time we introduced the theorem of Ramakrishna and it yields a unique universal deformation of type Σ, say $\rho_\Sigma : G_{\mathbb{Q}} \to GL_2(R_\Sigma)$
Note that lifts of $\bar{\rho}$ of type Σ are unramified outside $S = \{p | lN(\bar{\rho})\} \cup \Sigma$, so factor through $G_{\mathbb{Q},S}$, which satisfies (†)
We'll show that there exists a unique universal "modular" deformation of type Σ, say

$G_{\mathbb{Q}} \to GL_2(\Pi_\Sigma)$

$$\begin{tikzcd}
\mathcal{R}_{\Sigma\cup\{p\}} \arrow[r, two heads, "\Pi_{\Sigma\cup\{p\}}"] \arrow[d, two heads] & \mathbb{T}_{\Sigma\cup\{p\}} \arrow[d, two heads] \\
\mathcal{R}_{\Sigma} \arrow[r, two heads, "\Pi_{\Sigma}"] \arrow[d, two heads] & \mathbb{T}_{\Sigma} \arrow[d, two heads] \\
\mathcal{R}_{\emptyset} \arrow[r, two heads, "\Pi_{\emptyset}"] & \mathbb{T}_{\emptyset}
\end{tikzcd}$$

It's natural that the above diagram is commutative and eventually we'll show that
(1) $\Pi_\emptyset$ is an isomorphism
(2) Π_Σ is an isomorphism and so is $\Pi_{\Sigma\cup\{p\}}$
Then this would tell us every lift of type Σ is modular!

22.1. **Proof of Ramakrishna theorem.** We'll proceed by dealing with each condition for type Σ. First consider the group scheme condition (good at l, extends to a finite flat group scheme over $\mathbb{Z}_l$)
Consider $\rho : G_{\mathbb{Q}} \to GL_2(R)$ (R in $\mathscr{C}_F^0$), then get R^n as a finite set with $G_{\mathbb{Q}_l}$-action, which corresponds to an étale group scheme over $\mathbb{Q}_l$ say represented by $\mathcal{R}$. Say that ρ has property X if this group scheme extends to a finite flat group scheme over $\mathbb{Z}_l$ (i.e. $\exists$ finite flat $\mathbb{Z}_l$-algebra R' such that $R' \otimes_{\mathbb{Z}_l} \mathbb{Q}_l = \mathcal{R}$). Now we have to consider the following question.

Question 22.1. Is X preserved under submodule, quotient and direct sum?

Definition 22.2. Let G be an affine group scheme over $\mathbb{Z}_l$, say represented by A, let G_{gen} be its generic fiber over $\mathbb{Q}_l$, i.e. represented by $A \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$. Let H_{gen} be a closed subgroup scheme of G_{gen}, say represented by $(A \otimes_{\mathbb{Z}_l} \mathbb{Q}_l)/J$ (note that J has to be a Hopf ideal). Let I be $\phi^{-1}(J)$ where $\phi : A \to A \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$, then the group scheme represented by A/I is a sub group scheme of G called the schemetic closure of H_{gen}.

Lemma 22.3. *A/I is torsion-free*

Proof. ϕ induces an injection $A/I \hookrightarrow (A \otimes_{\mathbb{Z}_l} \mathbb{Q}_l)/J$ which is torsion-free as $(A \otimes_{\mathbb{Z}_l} \mathbb{Q}_l)/J$ is a $\mathbb{Q}_l$-algebra, therefore A/I must also be torsion-free □

The lemma shows if G_{gen} extends to a finite flat group scheme over $\mathbb{Z}_l$, then so does H_{gen}
As for quotient, in general the functor sending A to $G(A)/H(A)$ is not representable. However we have the following:
(Raymond) If G,H are both finite and flat, then G/H is representable and finite flat as well.
As for direct sum, let G,H be represented by R and S. Let $F(A) = G(A) \times H(A)$, we can check that it's represented by $R \otimes_{\mathbb{Z}_l} S$ and since R and S are finite and flat over$\mathbb{Z}_l$, so is $R \otimes_{\mathbb{Z}_l} S$
Let G be a profinite group and I be a closed subgroup of G.

Definition 22.4. Let G be a profinite group and I be a closed subgroup of G. Call a representation $\rho : G \to GL_2(R)$ I-ordinary if the fixed points of R^2 under I form a free direct summand of rank 1.

Theorem 22.5. *If $\bar{\rho}$ is I-ordinary and absolutely irreducible and G satisfies (†), then $\exists$ universal I-ordinary deformation of $\bar{\rho}$*

Proof. Let $E_I(R) = \{I\text{-ordinary deformations of } \bar{\rho} \text{ to } R\} \subseteq E(R)$, then H2,H3,H4 follows from them holding for E, we need to show H1. Let $R_3 = R_1 \times_{R_0} R_2$, consider $E_I(R_3) = E_I(R_1 \times_{R_0} R_2) \to E_I(R_1) \times_{E_I(R_0)} E_I(R_2)$, let $\rho_1 \times_{\rho_0} \rho_2$ be an element in the right, since H1 holds for E, we know that $\exists \rho \in E(R_3) \to \rho_1 \times_{\rho_0} \rho_2$, we need to show this ρ is actually I-ordinary, which is left an exercise for the reader. □

Third, we need to show that $\det \rho$ agrees with cyclotomic character.

Proof. Suppose we have a universal deformation $\xi : G_{\mathbb{Q}} \to GL_2(\mathcal{R})$ satisfying everything except for this. For $p \in S = \{p | lN(\bar{\rho})\} \cup \Sigma$, ξ is unramified at p, so $\xi(Frob_p)$ is well-defined up to conjugacy. Let $\det \xi(Frob_p) = r_p \in \mathcal{R}$ and I be the ideal of $\mathcal{R}$ generated by $r_p - p$ $(p \notin S)$. Consider $\bar{\xi} : G_{\mathbb{Q}} \to GL_2(\mathcal{R}/I)$ be ξ composed with $\mathcal{R} \to \mathcal{R}/I$. For $p \notin S$, $\det \bar{\xi}(Frob_p) = r_p(modI) = p(modI) = \chi(Frob_p)$ where χ is the cyclotomic character.
Now by Chebotarev density theorem, we know that $\det \bar{\xi} = \chi$ as the p's not in S have density 1. One can check that $\bar{\xi}$ is the universal deformation of type Σ □

Remark 22.6. $\mathcal{R}/I$ is nontrivial for the I that we constructed above as we have the following commutative diagram

$$\begin{tikzcd} \mathcal{R} \arrow[r, two heads] \arrow[dr, two heads] & \mathcal{R}/I \arrow[d, two heads] \\ & F \end{tikzcd}$$

so $I \subseteq Ker(\mathcal{R} \twoheadrightarrow F)$ which is a nontrivial ideal

22.2. **tangent space of functors.** Let $t_{E_\Sigma} = E_\Sigma(F[\epsilon]) \subseteq t_E = E(F[\epsilon])$ (recall this is a finite dimensional F-vector space). dim t_{E_Σ} is an important invariant of $\mathcal{R}_\Sigma$. We'll show $\mathcal{R} \mapsto \mathbb{T}_\Sigma$ is an isomorphism if and only if $inv_1(\mathcal{R}_\Sigma) \leq inv_2(\mathbb{T}_\Sigma)$ where we would take inv_1 as dim t_{E_Σ}. If E is represented by $\mathcal{R}$, $t_E(F[\epsilon]) = \hom(R, F[\epsilon])$. Every such morphism sends $m_{\mathcal{R}} \to \{b\epsilon | b \in F\}$ and the kernal contains $m_{\mathcal{R}}^2 + l\mathcal{R}$ (char$F$=l). We can show that $t_E = E(F[\epsilon]) \simeq m_{\mathcal{R}}/(m_{\mathcal{R}}^2 + l\mathcal{R})$

23. 2018-04-02: Deformation theory V

Our aim for now to to describe $\mathrm{inv}_1(\mathcal{R})$ in more detail. Today we will work towards setting up a construction that will allow us to compute it. We will start in a very general setting.

Fix $\bar{\rho} : G \to \mathrm{GL}_n(F)$

We will consider lifts of $\bar{\rho}$ to $F[\epsilon]$, i.e. maps that make the following commute

$$\begin{tikzcd} G \arrow[r] \arrow[dr, "\bar{\rho}"] & \mathrm{GL}_n(F[\epsilon]) \arrow[d, "\epsilon \mapsto 0"] \\ & \mathrm{GL}_n(F) \end{tikzcd}$$

One such lift is given by the the inclusion $F \hookrightarrow F[\epsilon]$, we will denote this lift simply by $\bar{\rho}$.

Now let $\sigma : G \to \mathrm{GL}_n(F[\epsilon])$ be any lift. Since it is a lift we can write it as

$$\sigma(g) = (1 + \epsilon a(g))\bar{\rho}(g)$$

for some $a : G \to \mathrm{M}_n(F)$.

We can use the fact that σ is a group homomorphism to obtain a condition on a:

$$a(gh) = a(g) + \bar{\rho}(g)^{-1}a(h)\bar{\rho}(g)$$

So a is not quite a group homomorphism, in fact we will see it is what is called a 1-cocycle.

Definition 23.1. Let M be a G module. (With continuous action if G is profinite)

A 1-cocycle is a map $f : G \to M$ such that

$$f(gh) = f(g) + gf(h) \quad \forall g, h \in G$$

A 1-coboundary is a map $f : G \to M$ such that f is of the form

$$f(g) = gx - x \quad \text{for some fixed } x \in M$$

1-coboundaries form a subgroup of 1-cocycles. We then set

$$H^1(G, M) = \{\text{1-cocycles}\}/\{\text{1-coboundaries}\}$$

Example 23.2. If G acts trivially on M then

$$H^1(G, M) = \mathrm{Hom}_{grp}(G, M)$$

Returning to our previous case we have $\mathrm{GL}_n(f) \circlearrowleft M_n(F)$ by conjugation so the map $\bar{\rho}$ makes $M_n(F)$ into a G-module, which we will call $\mathrm{Ad}(\bar{\rho})$.

In this set-up we immediately see that the $a(g)$ defined earlier is a 1-cocycle for $M = \mathrm{Ad}(\bar{\rho})$. In fact one can check that strictly equivalent lifts of $\bar{\rho}$ correspond to 1-cocycles which differ by 1-coboundaries and so we get a map

$$\{\text{deformations of } \bar{\rho} \text{ to } F[\epsilon]\} \to H^1(G, \mathrm{Ad}(\bar{\rho}))$$

Conversely given a 1-cocycle $a : G \to \mathrm{Ad}(\bar{\rho})$ we obtain a lift of $\bar{\rho}$ defined as $\sigma(g) = (1 + a(g))\bar{\rho}(g)$. So in fact the above map is a bijection.

Next recall that we care about counting deformations that have property X, under the above bijection these will correspond to some subspace $H^1_X(G, \mathrm{Ad}(\bar{\rho}) \subseteq H^1(G, \mathrm{Ad}(\bar{\rho}))$.

In particular we care about lifts of type Σ and so we need to determine what the subspace $H^1_\Sigma(G, \mathrm{Ad}(\bar{\rho}))$ looks like. Recall that there are two parts that go into a lift being of type sigma, namely that the determinant of the lift is cyclotomic and (roughly) that the behavior of the lift is "no worse" than the behavior of $\bar{\rho}$ at primes outside Σ. We will deal with each of these separately.

First the condition that the lift σ has determinant the cyclotomic character. If $\sigma(g) = (1 + a(g))\bar{\rho}(g)$, then since we know that $\det \bar{\rho}$ is cyclotomic we have that

$$\det \sigma \text{ is cyclotomic} \iff \det(1 + \epsilon a(g)) = 1$$

We can do easily compute $\det(1 + \epsilon a(g))$:

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

So $\det(1 + \epsilon a(g) = 1 + \epsilon(a_{11} + a_{22}) = 1$ occurs exactly when $a_{11} + a_{22} = 0$ i.e. when $\mathrm{tr}(a(g)) = 0 \forall g$

Since conjugation fixes trace we have that $\mathrm{Ad}^0(\bar{\rho}) = \{m \in \mathrm{Ad}(\bar{\rho}) : \mathrm{tr}(m) = 0\}$ is a G submodule of $\mathrm{Ad}(\bar{\rho})$ and so we can simply work with $\mathrm{Ad}^0(\bar{\rho})$ in order to insure our first condition holds.

In order to deal with the remaining conditions we recall a fact from Galois cohomology: If $H \leq G$ then we have a restriction map

$$\mathrm{res} : H^1(G, M) \to H^1(H, M)$$

In our case we will care about the case $G_{\mathbb{Q}_p} \hookrightarrow G_{\mathbb{Q}}$, and we will denote the corresponding restriction map by res_p. We will see that these maps are enough to capture the remaining properties required to be of type Σ.

Example 23.3. Suppose a lift σ corresponds to an element of the kernel from $H^1(G_{\mathbb{Q}}, \mathrm{Ad}^0(\bar{\rho})) \to H^1(I_p, \mathrm{Ad}^0(\bar{\rho}))$.

Then $\sigma(g) = \bar{\rho}(g)\ \forall g \in I_p$ so we have

$$\sigma \text{ unramified at } p \iff \bar{\rho} \text{ unramified at } p$$

This motivates the following

$$H^1_{ur}(G_{\mathbb{Q}_p}, \mathrm{Ad}(\bar{\rho})) := \ker(H^1(G_{\mathbb{Q}_p}, \mathrm{Ad}^0(\bar{\rho})) \to H^1(I_p, \mathrm{Ad}^0(\bar{\rho})))$$

Definition 23.4. Let $M = \mathrm{Ad}^0(\bar{\rho})$. By local conditions we mean a collection $\mathcal{L} = \{L_p\}$ where for each prime p we are specifying a subgroup $L_p \leq H^1(G_{\mathbb{Q}_p}, M)$ such that for all but finitely many p, $L_p = H^1_{ur}(G_{\mathbb{Q}_p}, M)$.

Then we define a Selmer group

$$H^1_{\mathcal{L}}(G_{\mathbb{Q}}, M) = \{c \in H^1(G_{\mathbb{Q}}, M) : \mathrm{res}_p(c) \in L_p \forall \text{ primes } p\}$$

Finally we will use this to state the following important theorem.

Theorem 23.5. *Let $M = Ad^0(\bar{\rho})$ and define $\mathcal{L}$ by $L_\infty = 0$ and for finite primes*

$$\begin{aligned} L_P = \quad & H^1_{ur}(G_{\mathbb{Q}_p}, M) && \text{if } p \notin \Sigma \cup \{l\} \\ & H^1(G_{\mathbb{Q}_p}, M) && \text{if } p \in \Sigma, p \neq l \\ & H^1_f(G_{\mathbb{Q}_p}, M) && \text{if } p = l \notin \Sigma \\ & H^1_{ss}(G_{\mathbb{Q}_p}, M) && \text{if } p = l \in \Sigma \end{aligned}$$

Then

$$H^1_\Sigma(G_{\mathbb{Q}}, Ad^0(\bar{\rho})) = H^1_{\mathcal{L}}(G_{\mathbb{Q}}, M)$$

We will define H^1_f and H^1_{ss} next time. One final remark for today:

Remark 23.6. Regarding the condition at ∞ we have $G_{\mathbb{Q}_\infty} \hookrightarrow G_{\mathbb{Q}}$ is generated by complex conjugation so is order 2. Moreover one can show that if G is order 2 and M is finite of odd order then $H^1(G, M) = 0$. So in fact our condition at ∞ is not restrictive at all.

24. 2018-04-04: Deformation theory VI

We will begin today by describing the two subspaces H^1_f and H^1_{ss} apearing in the statement of our Theorem from the end of the last day. We start with a definition.

Definition 24.1. Given $\bar{\rho} : G \to \mathrm{GL}_n(F)$, Let $V = F^n$ be a G module via $\bar{\rho}$.

Consider extension E of V by V, i.e short exact sequences of $F[G]$ modules

$$\begin{tikzcd} 0 \arrow[r] & V \arrow[r, "\alpha"] & E \arrow[r, "\beta"] & V \arrow[r] & 0 \end{tikzcd}$$

We will call two such extensions equivalent if there is a commutative diagram of the form

$$\begin{tikzcd} 0 \arrow[r] & V \arrow[r, "\alpha"] \arrow[d, equal] & E \arrow[r, "\beta"] \arrow[d] & V \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & V \arrow[r, "\alpha'"] & E' \arrow[r, "\beta'"] & V \arrow[r] & 0 \end{tikzcd}$$

Then $\mathrm{Ext}^1_{F[G]}(V, V)$ is the set of these equivalence classes.

Theorem 24.2. *There exists a bijection:*

$$H^1(G, Ad(\bar{\rho})) \leftrightarrow Ext^1_{F[G]}(V, V)$$

Proof. We will sketch how to construct this bijection, at least in one direction. Pick some F linear map $\phi : V \to E$ such that $\beta(\phi(m)) = m \ \forall m \in V$.

Then given $g \in G$, we define $T_g : V \to V$ by

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

If we consider T_g as an $n \times n$ matrix then we can check

$$T_{gh} = T_g + gT_h$$

where the action of G is conjugation. Hence the map $g \to T_g$ is a 1-cocycle.

□

Recall that an $F[G]$ module V of finite cardinality is good if $\exists$ finite flat group scheme H over $\mathbb{Z}_l$ such that

$$V \simeq H(\bar{\mathbb{Q}_l}) \quad \text{as } F[G_{\mathbb{Q}_l}] \text{ modules}$$

Next recall that V is called ordinary if there is an exact sequence

$$0 \longrightarrow V^{-1} \longrightarrow V \longrightarrow V^0 \longrightarrow 0$$

of $F[G_{\mathbb{Q}_l}]$ modules such that I_l acts trivially on V_0 and via the cyclotomic character on V^{-1}.

We then call V semistable if V is either good or ordinary.

Definition 24.3. Identify $H^1(G_{\mathbb{Q}_l}, \mathrm{Ad}(\bar{\rho}))$ with $\mathrm{Ext}^1_{F[G]}(V, V)$.

We then let $H^1_{ss}(G_{\mathbb{Q}_l}, \mathrm{Ad}(\bar{\rho}))$ be the subspace of $H^1(G_{\mathbb{Q}_l}, \mathrm{Ad}(\bar{\rho}))$ which corresponds to extensions of V by V that are semistable.

Then if $\bar{\rho}$ is not good at l then we set

$$H^1_f(G_{\mathbb{Q}_l}, \mathrm{Ad}(\bar{\rho})) = H^1_{ss}(G_{\mathbb{Q}_l}, \mathrm{Ad}(\bar{\rho}))$$

If $\bar{\rho}$ is good at l then we take $H^1_f(G_{\mathbb{Q}_l}, \mathrm{Ad}(\bar{\rho}))$ to be the subspace corresponding to good extensions.

Finally

$$H^1_{ss}(G_{\mathbb{Q}_l}, \mathrm{Ad}^0(\bar{\rho})) = H^1_{ss}(G_{\mathbb{Q}_l}, \mathrm{Ad}(\bar{\rho})) \cap H^1(G_{\mathbb{Q}_l}, \mathrm{Ad}^0(\bar{\rho}))$$

$$H^1_f(G_{\mathbb{Q}_l}, \mathrm{Ad}^0(\bar{\rho})) = H^1_f(G_{\mathbb{Q}_l}, \mathrm{Ad}(\bar{\rho})) \cap H^1(G_{\mathbb{Q}_l}, \mathrm{Ad}^0(\bar{\rho}))$$

Now we have finally defined all the terms appearing in our Theorem from the last lecture. Our next goal will be to understand the size of $H^1_{\mathcal{L}}(G_{\mathbb{Q}}, M)$.

In order to do this we will take a step back into Galois cohomology. Let M be a G module, $H \trianglelefteq G$. Then

$$M^H = \{m \in M : hm = m \forall h \in H\}$$

is a G/H module. We then have an exact sequence, the so called Inflation-Restriction exact sequence

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

Corollary 24.4.

$$H^1_{ur}(G_{\mathbb{Q}_p}, M) = H^1(G_{\mathbb{Q}_p}/I_p, M^{I_p})$$

This will be useful since $G_{\mathbb{Q}_p}/I_p$ is infinite procyclic and the group cohomology of infinite procyclic groups is relatively straightforward.

Exercise 24.5. If $G \simeq \hat{Z}$, say generated by g and M is finite then

$$H^1(G, M) \simeq M/(g-1)M$$

Theorem 24.6. *For finite M:*

$$|H^1_{ur}(G_{\mathbb{Q}_p}, M)| = |H^0(G_{\mathbb{Q}_p}, M)| < \infty$$

Proof. Consider the following exact sequence

$$0 \longrightarrow M^{G_{\mathbb{Q}_p}} \longrightarrow M^{I_p} \xrightarrow{\text{Frob}_{p-1}} M^{I_p} \longrightarrow M^{I_p}/(\text{Frob}_p - 1)M^{I_p} \longrightarrow 0$$

The alternating product of the cardinalities in an exact sequence is equal to 1 so we have

$$|M^{G_{\mathbb{Q}_p}}||M^{I_p}|^{-1}|M^{I_p}||M^{I_p}/(\text{Frob}_p - 1)M^{I_p}|^{-1} = 1$$

So

$$|M^{G_{\mathbb{Q}_p}}| = |M^{I_p}/(\text{Frob}_p - 1)M^{I_p}|$$

Then by the previous exercise

$$M^{I_p}/(\text{Frob}_p - 1)M^{I_p} \simeq H^1(G_{\mathbb{Q}_p}/I_p, M^{I_p}) \simeq H^1_{ur}(G_{\mathbb{Q}_p}, M)$$

and so we are done. □

Finally for today we will state an important theorem of Wiles:

Theorem 24.7. *Let $\mathcal{L}$ be a collection of subgroups $L_p \leq H^1(G_{\mathbb{Q}_p}, M)$.*

Set $\mathcal{L}^*$ be the collection of subgroups of $L_p^* \leq H^1(G_{\mathbb{Q}_p}, M^*)$ defined as follows: Let $M^* = \mathrm{Hom}(M, \mu_n(\bar{\mathbb{Q}}_p))$ where $n = |M|$, we then have a pairing

$$H^1(G_{\mathbb{Q}_p}, M) \times H^1(G_{\mathbb{Q}_p}, M^*) \to H^2(G_{\mathbb{Q}_p}, \mu_p(\bar{\mathbb{Q}}_p))$$

L_p^* is then defined to be the annihilator of L_p under this pairing.

With this setup we then have:

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

Remark 24.8. For all but finitely many primes $L_p = H^1_{ur}(G_{\mathbb{Q}_p}, M)$ and so for all but finitely many primes we have

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

by our previous theorem, hence the infinite product in the above theorem is indeed well defined.

Remark 24.9. We will try to avoid dealing with H^2 as much as possible however it does appear in the statement above so for the sake of completeness we recall that we can describe $H^2(G, M)$ as {2-cocycles}/{2-coboundaries} where

$$\{\text{2-coycles}\} = \{f : G \times G \to M | gf(h,k) - f(gh,k) + f(g,hk) - f(g,h) = 0 \forall g,h,k \in G\}$$

$$\{\text{2-coboundaries}\} = \{f : G \times G \to M | f(g,h) = g\phi(h) - \phi(gh) + \phi(g) \text{ for some fixed } \phi : G \to M\}$$

25. 2018-04-06: Deformation theory VII

25.1. **Sketch of proof of Wiles' Theorem.** Let S be a finite set of primes containing ∞, primes dividing n, primes at which M is ramified, and all primes where $L_p \neq H^1_{ur}$.
There is an exact sequence:

$$0 \to H_{\mathscr{L}}(G_{\mathbb{Q}}, M) \to H^1(G_{\mathbb{Q},S}, M) \to \bigoplus_{p \in S} H^1(G_{\mathbb{Q}_p}, M)/L_p$$

Dual sequence for M^*:

$$\bigoplus_{p \in S} L_p \to H^1(G_{\mathbb{Q},S}, M^*)^\vee \to H_{\mathscr{L}^*}(G_{\mathbb{Q}}, M^*)^\vee \to 0$$

Consider the Poitou-Tate 9-term exact sequence:

$$\begin{tikzcd}
0 \arrow[r] & H^0(G_{\mathbb{Q},S}, M) \arrow[r] & (\bigoplus_{p \in S} H^0(G_{\mathbb{Q}_p}, M))/(1+c)M \arrow[r] & H^2(G_{mQ,s}, M^*)^\vee \arrow[d] \\
 & & & H^1_{\mathscr{L}}(G_{\mathbb{Q}}, M^*) \arrow[d] \\
0 & H^1_{\mathscr{L}^*}(G_{\mathbb{Q}}, M^*)^\vee \arrow[l] & H^1(G_{\mathbb{Q},S}, M^*)^\vee \arrow[l] & \bigoplus_{p \in S} L_p \arrow[l]
\end{tikzcd}$$

Here c is the complex conjugation and $(1+c)M \leq H^0(G_{\mathbb{Q}_\infty}, M)$.
We have

$$\frac{|H^1_{\mathscr{L}}(G_{\mathbb{Q}}, M)|}{|H^1_{\mathscr{L}^*}(G_{\mathbb{Q}}, M^*)|} = \frac{|H^0(G_{\mathbb{Q},s}, M)||H^2(G_{\mathbb{Q},S}, M^*)||(1+c)M| \prod_{p \in S} |L_p|}{|H^1(G_{\mathbb{Q},s}, M^*)| \prod_{p \in S} |H^0(G_{\mathbb{Q}_p}, M)|}$$

Plug in the Global Euler characteristic formula:

$$\frac{|H^1(G_{\mathbb{Q},S}, M^*)|}{|H^0(G_{\mathbb{Q},S}, M^*)||H^2(G_{\mathbb{Q},S}, M^*)|} = \frac{|M^*|}{|H^0(G_{\mathbb{Q}_\infty}, M^*)|} = |(1+c)M|$$

Recall the main strategy:

$$\begin{tikzcd}
\mathcal{R}_{\Sigma'} \arrow[r, two heads, "\phi_{\Sigma'}"] \arrow[d, two heads] & \mathbb{T}_{\Sigma'} \arrow[d, two heads] \\
\mathcal{R}_{\Sigma} \arrow[r, two heads, "\phi_{\Sigma}"] & \mathbb{T}_{\Sigma}
\end{tikzcd}$$

ϕ_Σ is an isomorphism $\Leftrightarrow \mathrm{inv}_1(\mathcal{R}_\Sigma) \leq \mathrm{inv}_2(\mathbb{T}_\Sigma)$

Here $\Sigma' = \Sigma \cup \{q\}$.
We can use Wiles' formula to show that

$$\mathrm{inv}_1(\mathcal{R}_\Sigma) \leq \text{something} \Rightarrow \mathrm{inv}_1(\mathcal{R}_{\Sigma'}) \leq \text{(something)factor}$$

Then ϕ_Σ is an isomorphism $\Rightarrow$ $\phi_{\Sigma'}$ is an isomorphism. This reduces to the minimal case $\phi_\varnothing$ is an isomorphism (here $\varnothing$ is the empty set).

Question 25.1. What happens to both sides of Wiles' formula if Σ is replaced by $\Sigma' = \Sigma \cup \{q\}$?

Think about the simplest case $q \neq l$, say Σ, Σ' given by local conditions $\mathscr{L}, \mathscr{L}'$, and let $\mathscr{L} = \{L_p\}, \mathscr{L}' = \{L'_p\}$. If $p \neq q$, $L'_p = L_p$, $L_q = H^1_{ur}(G_{\mathbb{Q}_p}, M)$, $L'_q = H^1(G_{\mathbb{Q}_p}, M)$.

RHS: The only change is the $p \neq q$ term.
Before $(\mathscr{L})$: 1.
After $(\mathscr{L}')$: $\frac{|H^1(G_{\mathbb{Q}_p}, M)|}{|H^1(G_{\mathbb{Q}_q}, M)|}$.
The local Euler characteristic formula says

$$\frac{|H^1(G_{\mathbb{Q}_q}, M)|}{|H^0(G_{\mathbb{Q}_q}, M)||H^2(G_{\mathbb{Q}_q}, M)|} = 1,$$

so the new factor at q is $|H^2(G_{\mathbb{Q}_q}, M)|$.
But the local Tate duality imples $|H^2(G_{\mathbb{Q}_q}, M)| = |H^0(G_{\mathbb{Q}_q}, M^*)|$, so the RHS is multiplied by $|H^0(G_{\mathbb{Q}_q}, M^*)|$ in going from $\mathscr{L}$ to $\mathscr{L}'$.

LHS: $|H^1_{\mathscr{L}'^*}(G_{\mathbb{Q}}, M^*)| \leq |H^1_{\mathscr{L}^*}(G_{\mathbb{Q}}, M)|$ since conditions of $\mathscr{L}'^*$ (in particular, $L'_{q^*} = 0$) are more restrictive than those of $\mathscr{L}^*$. Now

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

Remark 25.2. We can do likewise for the case $q = l$.

25.2. **Criteria for ring isomorphism.** Given $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(F)$ absolutely semistable, and given a finite set of primes Σ, there is a universal deformation of $\bar{\rho}$ of type Σ

$$G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{R}_\Sigma).$$

We'll get a universal deformation of ρ of type Σ

$$G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T}_\Sigma)$$

so long as $\bar{\rho}$ is associated to some cupidal eigenform f.
Associated to f is a Galois representation $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathscr{O})$ where $\mathscr{O}$ is the valuation ring of some finite extension of $\mathbb{Q}_l$ (here $\mathscr{O}$ is in $\mathscr{C}_F$ and has characteristic 0).
By universality, we have

$$\begin{tikzcd}
\mathcal{R}_\Sigma \arrow[rr, two heads] \arrow[dr, "\pi_1"'] & & \mathbb{T}_\Sigma \arrow[dl, "\pi_2"] \\
& \mathscr{O} &
\end{tikzcd}$$

Let $\mathscr{C}^*_{\mathscr{O}}$ be the category with objects (A, π_A), where A is in $\mathscr{C}_F$ and is an $\mathscr{O}$-module, $\pi_A : A \to \mathscr{O}$ such that everything commutes; morphisms are morphisms $A \to B$ in $\mathscr{C}_F$ such that everything commutes.
Then $(\mathcal{R}_\Sigma, \pi_1), (\mathbb{T}_\Sigma, \pi_2)$ are in $\mathscr{C}^*_{\mathscr{O}}$.

26. 2018-04-09: Deformation theory VIII

Definition 26.1. Associated to an object (A, π_A) of $\mathscr{C}^*_{\mathscr{O}}$, attach two invariants.

(1) Cotangent space $\Phi_A = \ker \pi_A / (\ker \pi_A)^2$ (a finitely generated $\mathscr{O}$-module).
(2) Congruence ideal $\eta_A = \pi_A(\mathrm{Ann_A}(\ker \pi_A))$ (an ideal in $\mathscr{O}$).

Call a ring A in $\mathscr{C}_{\mathscr{O}}$ a complete intersection ring if A is free of finite rank as an $\mathscr{O}$-module and can be presented as $[\![T_1, \cdots, T_r]\!]/(f_1, \cdots, f_r)$.

Example 26.2. Let f be a cupidal eigenform associated to the elliptic curve 57B. This has level 57, weight 2, trivial Nebentypus.
Look at the associated mod 3 representation

$$\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/3)$$

which ramifies at $3, 19$.

Claim 26.3. *$\bar{\rho}$ is surjective.*

Proof. The image of Frob_2 has trace $a_2(f) = 1$ and determinant 2. In $\mathrm{GL}_2(\mathbb{Z}/3)$, all such elements have order 8.
Next, look at the local representation at 19. Note that 57 is square-free, so F has multiple reduction at 19.
Use Tate curves to see that 3 divides order of the image, then 24 divides order of the image, hence the image has order 24 or 48.
Note that the image is not $\mathrm{SL}_2(\mathbb{Z}/3)$, so it must be the whole of $GL_2(\mathbb{Z}/3)$. □

Now that $\bar{\rho}$ is surjective, it is absolutely irreducible. Also, 57B is semistable (since 57 is square-free), so is $\bar{\rho}$.
We'll see that $A = \mathcal{R}_\Phi = \mathbb{T}_\Phi \sim \mathbb{Z}_3[\![T]\!]/(T(T-3))$ is a complete intersection ring.
Computation gives $\Phi_A = \mathbb{Z}/3$ and $\eta_A = (3)$ (ideal of $\mathbb{Z}/3$), which satisfies what is expected: $|\Phi_A| = |\mathbb{Z}_3/\eta_A|$.

Theorem 26.4. *(Wiles, improve by Lenstra)Let $\phi : R \to T$ be a surjective morphism in $\mathscr{C}_{\mathscr{O}}$. Assume that T is free of finite rank as an $\mathscr{O}$-module, and that $\eta_T \neq (0)$ (so $|\mathscr{O}/\eta_T| < \infty$). The following are equivalent:*
(1) $|\Phi_R| \leq |\mathscr{O}/\eta_T|$.
(2) $|\Phi_R| = |\mathscr{O}/\eta_T|$.
(3) ϕ is an isomorphism of complete intersection rings.

Let $\Sigma' = \Sigma \cup \{q\}$ (cf. the main strategy in subsection 25.1), there is a commutative diagram

$$\begin{tikzcd}
\mathcal{R}_{\Sigma'} \arrow[r, two heads, "\phi_{\Sigma'}"] \arrow[d, two heads] & \mathbb{T}_{\Sigma'} \arrow[d, two heads] \\
\mathcal{R}_{\Sigma} \arrow[r, two heads, "\phi_{\Sigma}"] & \mathbb{T}_{\Sigma}
\end{tikzcd}$$

we want to show ϕ_Σ is an isomorphism if and only if $\phi_{\Sigma'}$ is an isomorphism (so reduces to $\Sigma = \varnothing$).
Note that if $\exists L_q \leq \mathscr{O}$ such that $|\Phi_{R'}|/|\Phi_R| \leq |\mathscr{O}/L_q|$, and if ϕ_Σ is an isomorphism, then

$$|\Phi_{R'}| \leq |\mathscr{O}/L_q||\Phi_R| = |\mathscr{O}/L_q||\mathscr{O}/\eta_T| \leq |\mathscr{O}/\eta_{T'}|,$$

so by Wiles-Lenstra, $\Phi_{\Sigma'}$ is an isomorphism, and vice versa.

In order to prove the Wiles-Lenstra Theorem, we introduce the following lemma:

Lemma 26.5. *Suppose A, B are in $\mathscr{C}^*_{\mathscr{O}}$ and that there's a surjection $\phi : A \to B$, then*

1. *ϕ induces a surjection $\tilde{\phi} : \Phi_A \to \Phi_B$ and so $|\Phi_A| \geq |\Phi_B|$, and $\eta_A \subseteq \eta_B$.*
2. *$|\Phi_A| \geq |\mathscr{O}_/\eta_A|$.*
3. *Suppose B is a complete intersection ring, if $\tilde{\phi}$ is an isomorphism and Φ_A is finite, then ϕ is an isomorphism (we say "$\tilde{\phi}$ detects complete intersection rings").*

(4) *Suppose A is a complete intersection ring, if $\eta_A = \eta_B \neq (0)$ and A, B are free of finite rank as $\mathscr{O}$-modules, then ϕ is an isomorphism (we say "η detects ismorphisms from complete intersection rings").*
(5) *Suppose A is free of finite rank as an $\mathscr{O}$-module, then $\exists$ complete intersection ring $\tilde{A}$ with $\tilde{A} \to A$ such that the induced $\Phi_{\tilde{A}} \to \Phi_A$ is an isomorphism.*

26.1. **Proof of this lemma $\Rightarrow$ Wiles-Lenstra Theorem.** We focus on the key part of the theorem: (1) $\Rightarrow$ (3).

Proof. We have

$$|\mathscr{O}/\eta_T| \geq |\Phi_R| \geq text(by(1))|\Phi_T| \geq \text{(by (2))}\ |\mathscr{O}/\eta_T|,$$

so

$$|\mathscr{O}/\eta_T| = |\Phi_T| = \text{(by (5))}\ |\Phi_{\tilde{T}}| \geq \text{(by (2))}\ |\mathscr{O}/\eta_{\tilde{T}}|.$$

By (1), $\eta_{\tilde{T}} \subseteq \eta_T$, so $\eta_{\tilde{T}} = \eta_T$, hence by (4) $\tilde{T} \to T$ is an isomorphism, so T is a complete intersection ring.
Now $|\Phi_R| = |\Phi_T|$, by (3) $\phi : R \to T$ is an isomorphism. □

27. 2018-04-11: Wiles-Lenstra Theorem and the lemma

Last time, we introduced Wiles-Lenstra theorem and the lemma. We also showed how Wiles-Lenstra theorem deduced from the lemma. Today we will prove part (1) and (2) of the lemma.

First, we introduce some preparatory knowledge.

Lemma 27.1. *A local ring, M finitely generated A-module. If I is an ideal of A, s.t., $IM = M$, then $M = 0$. This is called Nakayama's Lemma.*

Proof. Let $m_1, \cdots, m_n$ be minimal generating set for M. Then

$$\begin{aligned} m_n \in M = IM &\Rightarrow m_n = r_1 m_1 + \cdots + r_n m_n \\ &\Rightarrow (1 - r_n) m_n = r_1 m_1 + \cdots + r_{n-1} m_{n-1} \\ &\Rightarrow m_n \in \text{submodule generated by } m_1, \cdots, m_{n-1} \end{aligned}$$

which contradicts minimality. □

Corollary 27.2. *Suppose $\psi : M \to N$ is a homomorphism of finitely generated A-modules, and I an ideal s.t., $M/IM \to N/IN$ is surjective, then ψ is surjective.*

Proof. Apply Nakayama's lemma to cokernel.

$$M/IM \cong M \otimes_A A/I$$

Both $\mathscr{O}$ and F are of the form A/I, so if after tensoring with $\mathscr{O}$ or F, ψ becomes surjective, then it was surjective in the first place. □

Then we introduce fitting ideals.

Definition 27.3. Let R be in $\mathscr{C}_{\mathscr{O}}$ and M be a finitely generated R-mod, so $\exists$ an exact sequence

$$0 \to M' \to R^n \to M \to 0$$

We called this presentation of M. The fitting ideal $Fitt_R(M)$ is the ideal of R generated by $det(v_1, \cdots, v_n)$ as the $v_i \in R^n$ run through M'.

Exercise 27.4. (i) The fitting ideal is independent of choice of presentation. [Hint: Consider two different representations, $R^n \to M \to 0$ and $R^m \to M \to 0$, then we have a new presentation $R^{n+m} \to M \to 0$. Show that the $Fitt_R$ of the new presentation is the same as the $Fitt_R$ of former ones.]

(ii) Suppose $R = \mathscr{O}$, without loss of generality,

$$M = \mathscr{O} \oplus (\mathscr{O}/\lambda^{n_1}) \oplus \cdots \oplus (\mathscr{O}/\lambda^{n_k})$$

where λ is the uniformizer of $\mathscr{O}$. Show that

$$Fitt_{\mathscr{O}}(M) = \begin{cases} (0) & r > 0 \\ \lambda^{n_1 + \cdots + n_k} & r = 0 \end{cases}$$

In particular,

$$|M| = |\mathscr{O}/Fitt_{\mathscr{O}}(M)|$$

Now, we prove part (1) and (2) of the lemma.

Proof. (1) Have ϕ:

$$\begin{tikzcd} A \arrow[rr, two heads] \arrow[dr, two heads, "\pi_A"'] & & B \arrow[dl, two heads, "\pi_B"] \\ & \mathscr{O} & \end{tikzcd}$$

it induces

$$ker\pi_A \twoheadrightarrow ker\pi_B$$

which implies

$$ker\pi_A \twoheadrightarrow ker\pi_B/(ker\pi_B)^2 = \Phi_B$$

Since the image of $(ker\pi_A)^2$ is 0. Have

$$ker\pi_A \to ker\pi_A/(ker\pi_A)^2 = \Phi_A \to \Phi_B$$

As for $\eta_A \subset \eta_B$, point here is that $\exists$ a map

$$Ann_A(ker\pi_A) \to Ann_B(ker\pi_B)$$

(2) First note that $Fitt_R(M) \subset Ann_R(M)$, where $R \in \mathscr{C}_{\mathscr{O}}$, M is a finitely generated R-module. Take a presentation

$$0 \to M' \to R^n \to M \to 0$$

Let $x_1, \cdots, x_n \in M$ be the images of the standard generators of R^n (note that $x_1, \cdots, x_n$ generate M). Let $v_1, \cdots, v_n \in M'$ and $(c_{ij}) = (v_1, \cdots, v_n)$, $d = det(c_{ij})$. We just need to show $d \in Ann_R(M)$. Write $dI_n = (d_{ij})(c_{ij})$ where $d(ij)$ gives the adjoint matrix. We have

$$\sum_j c_{ij} x_j = 0$$

which implies that $dx_j = 0$ for $j = 1, \cdots, n$. But $x_1, \cdots, x_n$ generate M, so $d \in Ann_R(M)$. Second, note that

$$\pi_A(Fitt_R(M)) = Fitt_{\mathscr{O}}(M \otimes_A \mathscr{O})$$

since π_A is an $\mathscr{O}$-module, then

$$M \otimes_A \mathscr{O} = M/(ker\pi_A)M$$

is defined by the same relation as those defining M as an A-module. In particular,

$$ker\pi_A \otimes_A \mathscr{O} = \Phi_A$$

so

$$\begin{aligned} Fitt_{\mathscr{O}}(\Phi_A) &= \pi_A(Fitt_A(ker\pi_A)) \\ &\subset \pi_A(Ann_A(ker\pi_A)) = \eta_A \end{aligned}$$

so

$$|\Phi_A| = |\mathscr{O}/Fitt_{\mathscr{O}}(\Phi_A)| \geq |\mathscr{O}/\eta_A|$$

Note that in Wiles-Lenstra theorem, $(a) \Leftrightarrow (b)$ follows since if $R \twoheadrightarrow T$, then always $|\Phi_R| \geq |\Phi_T| \geq |\mathscr{O}/\eta_T|$.

□

28. 2018-04-13: Wiles-Lenstra Theorem and the lemma II

Recall the lemma we want to prove.

Lemma 28.1. *Suppose A and B are in $\mathscr{C}^*_{\mathcal{O}}$ and that there is a surjection $\phi : A \twoheadrightarrow B$.*

(1) ϕ induces a surjection $\tilde{\phi} : \Phi_A \to \Phi_B$ and so $|\Phi_A| \geq |\Phi_B|$, and $\eta_A \subset \eta_B$.
(2) $|\Phi_A| \geq |\mathcal{O}/\eta_A|$
(3) Suppose B is a complete intersection ring. If $\tilde{\phi}$ is an isomorphism, and Φ_A is finite, then ϕ is an isomorphism.
(4) Suppose A is a complete intersection ring. If $\eta_A = \eta_B \neq (0)$, and A, B are free finite rank $\mathcal{O}$-modules, then ϕ is an isomorphism.
(5) Suppose A is free and of finite rank as an $\mathcal{O}$-module. Then there exists a complete intersection ring $\tilde{A}$ mapping onto A such that the induced map $\Phi_{\tilde{A}} \to \Phi_A$ is an isomorphism.

Proof. Recall $\Phi_A = Ker(\pi_A)/Ker^2(\pi_A)$ and $\eta_A = \pi_A(Ann_A(Ker\pi_A))$.

(1) Consider $U = \mathcal{O}[[T_1, \cdots, T_r]]$ as in $\mathscr{C}^*_{\mathcal{O}}$ via $\pi_U : T_i \to 0$. Since B is a complete intersection ring, there exists the following morphism

$$\begin{tikzcd} \nu_B : U \arrow[rr, "h"] \arrow[dr, "\pi_U"'] & & B \arrow[dl, "\pi_B"] \\ & \mathcal{O} & \end{tikzcd}$$

with $Ker(\nu_B) = (f_1, \cdots, f_r)$. Let $b_i = \nu_B(T_i)$, then $b_i \in Ker(\pi_B)$. Recall from proof of statement (1) that the surjection from $A \to B$ induces a surjection $Ker(\pi_A) \to Ker(\pi_B)$ and the surjection $\tilde{\phi} : \Phi_A \to \Phi_B$:

$$\begin{tikzcd} Ker(\pi_A) \arrow[r, "\phi"] \arrow[d] & Ker(\pi_B) \arrow[d] \\ \Phi_A \arrow[r, "\tilde{\phi}"] & \Phi_B \end{tikzcd}$$

Therefore we can take $a_i \in Ker(\pi_A)$ such that $\phi(a_i) = b_i$. Since $\tilde{\phi}$ is an isomorphism and images of b_i generate Φ_B, we know the images of a_i generate Φ_A. Now define $\nu_A : U \to A$ by $T_i \to a_i$, this gives a surjection $\tilde{\nu_A} : \Phi_U \to \Phi_A$. By NAK, we have that

$\nu_A : Ker(\pi_U) \to Ker(\pi_A)$ is surjective since after tensoring with $\mathcal{O} = A/Ker(\pi_A)$, the map $\tilde{\nu_A}$ is surjective, and it is equivalent to that ν_A is surjective.

So far, we have shown that

$$\begin{tikzcd} U \arrow[r, "\nu_A"] \arrow[dr, "\nu_B"'] & A \arrow[d, "\phi"] \\ & B \end{tikzcd}$$

in the above diagram, $Ker(\nu_A) \subset Ker(\nu_B)$. It suffices to show the equality. We know that $\Phi_U \simeq \mathcal{O}^r$. Given Φ_A is finite, $Ker(\tilde{\nu_A})$ has finite index in $\mathcal{O}^r$, therefore it has r generators, say $\bar{g}_1, \cdots, \bar{g}_r$. Lift these to $g_1, \cdots, g_r$ to $Ker(\nu_A)$. Since $Ker(\nu_A) \subset Ker(\nu_B)$,

$$(g_1, \cdots, g_r) = (f_1, \cdots, f_r)M$$

where $M \in M_r(U)$. Let $\bar{M}$ be the matrix $M \pmod{(T_1, \cdots, T_r)}$, then

$$(\bar{g}_1, \cdots, \bar{g}_r) = (\bar{f}_1, \cdots, \bar{f}_r)\bar{M}$$

These two sets of generators generate the same submodule of Φ_U, therefore $M \in \mathcal{O}^*$. So $Ker(\nu_A) = Ker(\nu_B)$, and $\nu_A \cdot \nu_B^{-1} : B \to A$ is well-fined, and produces an inverse to ϕ. So ϕ is an isomorphism.

(2) Firstly, we show that $Ker(\pi_A) \cap Ann_A(Ker(\pi_A)) = 0$. Let $x \in \eta_A$ and $x \neq 0$. Say $x = \pi_A(x')$ and $x' \in Ann_A(Ker(\pi_A))$. Let $a \in Ker(\pi_A) \cap Ann_A(Ker(\pi_A))$. Note that $\pi_A(x - x') = 0$, we have

$$0 = a(x - x') = ax - ax' = ax(x \neq 0).$$

Therefore a is a $\mathcal{O}$-torsion. But A is a free $\mathcal{O}$-module, so $a = 0$.

Let's consider the restriction of π_A to $Ann_A(Ker(\pi_A)) \to \eta_A$. The above implies that the map is injective. Therefore it is an isomorphism. Similarly we could show the same thing for B. Therefore we get an isomorphism $Ann_A(Ker(\pi_A)) \to Ann_B(Ker(\pi_B))$.

Now consider the exact sequence

$$0 \to Ker\phi \bigoplus Ann_A(Ker(\pi_A)) \to A,$$

where the cokernel is

$$A/Ker\phi \bigoplus Ann_A(Ker(\pi_A)) \simeq B/Ann_B(Ker(\pi_B))$$

which is embedded into $End_{\mathcal{O}}(Ker(\pi_B))$. So the cokernel is torsion free over $\mathcal{O}$. This gives us a splitting. Let $A^\wedge = Hom_{\mathcal{O}}(A, \mathcal{O})$ and get a dual exact sequence

$$A^\wedge \to (Ker\phi)^\wedge \bigoplus (Ann_A(Ker(\pi_A)))^\wedge \to 0.$$

The key point is that if A is a complete intersection ring, then $A \simeq A^\wedge$ (i.e., A is Gorenstein). Therefore

$$A \to (Ker\phi)^\wedge \bigoplus (Ann_A(Ker(\pi_A)))^\wedge \to 0.$$

Tensor with F, we can check the dimension that $dim_F(A \bigotimes_A F) = 1$, and $(Ann_A(Ker(\pi_A)))^\wedge \bigotimes_A F \neq 0$ since $\eta_A \neq (0)$. So $(Ker\phi)^\wedge \bigotimes_A F = 0$. Finally applying NAK (so $Ker(\phi)^\wedge = 0$) and dualize, we get $Ker(\phi) = 0$. So ϕ is an isomorphism.

(3) Firstly, let's write A as a quotient of $U = \mathcal{O}[[T_1, \cdots, T_r]]$ (so we have a surjection $U \to A$) where the T_i map to elements of $Ker(\pi_A)$. The ideal is to choose $\bar{f}_1, \cdots, \bar{f}_r$, generate the kernel of the induced map $\Phi_U \to \Phi_A$ and lift these to U and set $\tilde{A} = U/(f_1, \cdots, f_r)$. Then it is good so long as $\tilde{A}$ is finitely generated as an $\mathcal{O}$-module.

Let $a_1, \cdots, a_r$ be $\mathcal{O}$-module generator of $Ker(\pi_A)$. Let $V = \mathcal{O}[T_1, \cdots, T_r]$. Define $\phi : V \to A$ by $T_j \to a_j$. Then ϕ is surjective since it is surjective on $Ker(\pi_A)$. Now pick $f_1, \cdots, f_r \in Ker(\phi)$ and let m be the maximal degree. Since $a_i^2 \in Ker(\pi_A)$, we have $a_i^2 = h_i(a_1, \cdots, a_n)$ where h_i is linear. Now replace f_i by $f_i + T_i^m \cdot (h_i - T_i^2)$. Then $V/(f_1, \cdots, f_r)$ is finitely generated as an $\mathcal{O}$-module. Finally complete at the maximal ideal $(\lambda, T_1, \cdots, T_r)$ to get $\tilde{A} = U/(f_1, \cdots, f_r)$ finitely generated $\mathcal{O}$-module. Note that $\tilde{A} \to A$ induces an isomorphism on cotangent space, since the leading term of f_i are the ones generate the kernel of $\Phi_U \to \Phi_A$.

□

29. 2018-04-16: Reduction to the minimal case on R side

Have $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(F)$ an absolutely irreducible semistable representation associated to the cuspidal eigenform f (with level $N(\bar{\rho})$). It gives us $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O})$. Let λ be a uniformizer of $\mathcal{O}$.

Consider lifts σ of ρ_f of type Σ to $\mathcal{O}[\epsilon]/(\lambda^n\epsilon, \epsilon^2)$. Every deformation yields a homomorphism in $\mathrm{Hom}_{\mathcal{O}}(R, \mathcal{O}[\epsilon]/(\lambda^n\epsilon, \epsilon^2))$. Indeed, we have the following diagram

$$\begin{tikzcd}
\ker \pi_R \arrow[r] \arrow[d] & (\mathcal{O}/\lambda^n)\epsilon \arrow[d] \\
R \arrow[r] \arrow[d, "\pi_R"'] & \mathcal{O}[\epsilon]/(\lambda^n\epsilon, \epsilon^2) \arrow[d, "\epsilon\to 0"] \\
\mathcal{O} \arrow[r, "id"] & \mathcal{O}
\end{tikzcd}$$

Furthermore, the map in the top row factors through $\ker \pi_R/(\ker \pi_R)^2 = \Phi_R$ so gives a homomorphism in $\mathrm{Hom}_{\mathcal{O}}(\Phi_R, \mathcal{O}/\lambda^n)$

One such lift σ is $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}) \hookrightarrow \mathrm{GL}_2(\mathcal{O}[\epsilon]/(\lambda^n\epsilon, \epsilon^2))$. As we did before, write $\sigma(g) = \rho_f(g)(1 + a(g)\epsilon)$ and get a 1-cocycle $G_{\mathbb{Q}} \to M_2(\mathcal{O}/\lambda^n)$ where strictly equivalent lifts are corresponding to 1-cocycles differing by a 1-coboundary.

We have the bijections between

$$\text{Deformations of } \rho_f \text{ to } \mathcal{O}[\epsilon]/(\lambda^n\epsilon, \epsilon^2) \longleftrightarrow H^1_\Sigma(G_{\mathbb{Q}}, \mathrm{Ad}^0(\rho_f) \otimes \mathcal{O}/\lambda^n)$$

and

$$\mathrm{Hom}_{\mathcal{O}}(\Phi_R, \lambda^{-n}\mathcal{O}/\mathcal{O}) \longleftrightarrow H^1_\Sigma(G_{\mathbb{Q}}, \mathrm{Ad}^0(\rho_f) \otimes \lambda^{-n}\mathcal{O}/\mathcal{O}).$$

Let E be the fraction field of $\mathcal{O}$. Take the union over n (direct limit).

Theorem 29.1. *There is a natural bijection between*

$$\mathrm{Hom}_{\mathcal{O}}(\Phi_R, E/\mathcal{O}) \longleftrightarrow H^1_\Sigma(G_{\mathbb{Q}}, \mathrm{Ad}^0(\rho_f) \otimes E/\mathcal{O})$$

Remark 29.2. If $|\Phi_R|$ is finite, every homomorphism in $\mathrm{Hom}_{\mathcal{O}}(\Phi_R, E/\mathcal{O})$ lands in some $\mathrm{Hom}_{\mathcal{O}}(\Phi_R, \lambda^{-n}\mathcal{O}/\mathcal{O})$.

Corollary 29.3.
$$|\Phi_R| = |H^1_\Sigma(G_\mathbb{Q}, \mathrm{Ad}^0(\rho_f) \otimes E/\mathcal{O})|.$$

From now on in this section, we denote $\mathrm{Ad}^0(\rho_f) \otimes E/\mathcal{O}$ by M and $\mathrm{Hom}(M, \mu_n(\bar{\mathbb{Q}}_l)))$ by M^*.

Recall the strategy of the reduction to the minimal case. Say $\Sigma' = \Sigma \cup \{q\}, q \notin \Sigma$. Let $R = R_\Sigma, R' = R_{\Sigma'}, T = T_\Sigma, T' = T_{\Sigma'}$. We have the following commutative diagram

$$\begin{tikzcd}
R' \arrow[r, two heads, "\phi'"] \arrow[d, two heads] & T' \arrow[d, two heads] \\
R \arrow[r, two heads, "\phi"] & T
\end{tikzcd}$$

We saw that Wiles-Lenstra criterion leads to

Theorem 29.4. *Suppose there exists $c_q \in \mathcal{O}$ satisfying*
$$\frac{|\Phi_{R'}|}{|\Phi_R|} \leq |\mathcal{O}/c_q|, \quad \eta_{T'} \subseteq c_q\eta_T$$
then ϕ is an isomorphism implies that ϕ' is an isomorphism.

With this theorem, the big question is what c_q works. We will specify c_q by classifications. The choice here is made so that $\frac{|\Phi_{R'}|}{|\Phi_R|} \leq |\mathcal{O}/c_q|$. However, later we will show the same choice will indeed satisfy the other half $\eta_{T'} \subseteq c_q\eta_T$.

(1) $q \neq l$

  (a) $\bar{\rho}$ is unramified at q.
  ρ_f is unramified at q so Σ lifts have ρ unramified at q ($q \notin \Sigma$), Σ' lifts could have any ρ at q. As an example of calculation with Wiles' formula for the order of a generator of the Selmer group, we have shown
  $$\frac{|\Phi_{R'}|}{|\Phi_R|} = \frac{|H^1_{\Sigma'}(G_\mathbb{Q}, M)|}{|H^1_\Sigma(G_\mathbb{Q}, M)|} \leq |H^0(G_{\mathbb{Q}_q}, M^*)|,$$
  here $H^0(G_{\mathbb{Q}_q}, M^*) = (M^*)^{G_{\mathbb{Q}_q}} = (M^*)^{\mathrm{Frob}_q}$.
  $\mathrm{Ad}^0(\rho_f) : G_\mathbb{Q} \to \mathrm{GL}_3(\mathcal{O})$, where $\mathrm{Ad}^0(\rho_f) \simeq \mathrm{Sym}^2(\rho_f) \otimes \det{}^{-1}$.
  Suppose $\rho_f(\mathrm{Frob}_q)$ has eigenvalues α_q, β_q. Its characteristic polynomial is $T^2 - a_qT + q$, $\alpha_q + \beta_q = a_q$ and $\alpha_q\beta_q = q$. Then $\mathrm{Sym}^2(\rho_f)(\mathrm{Frob}_q)$ has eigenvalues $\alpha_q^2, \alpha_q\beta_q, \beta_q^2$. The eigenvalues of $id - \mathrm{Sym}^2(\rho_f)(\mathrm{Frob}_q)$ are $1-\alpha_q^2, 1-\alpha_q\beta_q, 1-\beta_q^2$. Let $c_q = (1-\alpha_q^2)(1-\alpha_q\beta_q)(1-\beta_q^2)$, then $|H^0(G_{\mathbb{Q}_q}, M^*)| = |\mathcal{O}/c_q|$. Simplify the expression of c_q, then get
  $$\begin{aligned} c_q &= (1-q)(1-(\alpha_q^2+\beta_q^2)+(\alpha_q\beta_q)^2) \\ &= (1-q)(1-(a_q^2-2q)+q^2) \\ &= (q-1)(a_q^2-(q+1)^2) \end{aligned}$$

  Remark 29.5. $c_q \neq 0$ follows from the Petersson-Ramanujan inequality $|a_q| \leq 2\sqrt{q}$.

  (b) $\bar{\rho}$ is ramified at q.
  We set $c_q = q^2 - 1$. (Left as an exercise.)

(2) $q = l$.

The factor in Wiles-Lenstra goes up by $\frac{|H^1_{ss}|}{|H^1_f|}$.

If $\bar{\rho}$ is not good at l, then H^1_f was defined to be H^1_{ss} and take $c_q = 1$.

If $\bar{\rho}$ is not ordinary at l, then its lifts are not ordinary. So a lift of $\bar{\rho}$ is semistable at l if and only if it is good at l.

If $\bar{\rho}$ is both good and ordinary at l, $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O})$ is both good and ordinary at l. We have

$$\rho_f|_{G_{\mathbb{Q}_l}} \sim \begin{pmatrix} \psi_1\chi & * \\ 0 & \psi_2 \end{pmatrix},$$

where ψ_1, ψ_2 are unramified characters. $\psi_1, \psi_2 : G_{\mathbb{Q}_l} \to G_{\mathbb{Q}_l}/I_l \to \mathcal{O}^\times$.

Applying Fontaine-Lafaille theory, we have

$$|H^1_f(G_{\mathbb{Q}_l}, M)| = |H^0(G_{\mathbb{Q}_l}, M)||\mathcal{O}/\lambda^n|$$

and

$$|H^1_{ss}(G_{\mathbb{Q}_l}, M)| = |H^0(G_{\mathbb{Q}_l}, M)||\mathcal{O}/\lambda^n||\mathcal{O}/(\lambda^n, c_l)|$$

where

$$c_l = \frac{\psi_1(\mathrm{Frob}_l)}{\psi_2(\mathrm{Frob}_l)} - 1.$$

The polynomial $T^2 - a_l T + l = 0$ has roots α_l, β_l. For the ordinary case, one of α_l, β_l is a unit, say $\alpha_l = \psi_2(\mathrm{Frob}_l)$. $\psi_1 = \psi_2^{-1}$ since $\det = \chi$. So set $c_l = \alpha_l^{-2} - 1$. Up to units, we can also take $c_l = \alpha_l^2 - 1$ or $c_l = \alpha_l^2 - (l+1)^2$.

30. 2018-04-18: The Universal Modular Deformation

In this lecture, our goal will be to understand the T-side of our deformation-theoretic results; namely, we seek to show there is a universal modular deformation $(\mathbb{T}_\Sigma, \pi)$ parametrizing modular deformations of type Σ.

Fix an absolutely irreducible, semistable, continuous homomorphism $\bar{\rho}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(F)$ for F a finite field of characteristic $\ell > 0$. Assume that $\bar{\rho}$ corresponds to a cuspidal eigenform f of weight 2, level $N(\bar{\rho})$, and trivial Nebentypus; that is, for all but finitely many primes p, $\operatorname{tr}\bar{\rho}(\mathrm{Frob}_p) = a_p(f)$. Let

$$K = \begin{cases} \mathbb{Q}(\sqrt{\ell}) & \text{if } \ell \equiv 1 \mod 4 \\ \mathbb{Q}(\sqrt{-\ell}) & \text{if } \ell \equiv 3 \mod 4 \end{cases}$$

be the unique quadratic field ramified only at ℓ. We also assume that $\bar{\rho}|_{G_K}$ is absolutely irreducible. This latter assumption follows for $\ell \geq 5$; we shall say more on it later. Fix a finite set of primes Σ. Our goal will be to obtain a lift of $\bar{\rho}$ of type Σ that parametrizes all lifts of type Σ associated to cuspidal eigenforms.

Recall that $S_2(N)$ denotes the $\mathbb{C}$-vector space of cusp forms of level N, weight 2, and trivial Nebentypus and $\mathcal{T} = \mathcal{T}(N)$ denotes the Hecke algebra. Let $\mathcal{T}'$ be the subring of $\mathcal{T}$ generated by the Hecke operators T_n for $(n, \ell N) = 1$.

Theorem 30.1. *Let $\mathfrak{m}$ be the maximal ideal of $\mathcal{T}'$ and suppose that* $\mathrm{char}(\mathcal{T}'/\mathfrak{m}) = \ell$. *Then:*

(1) There exists a continuous semistable homomorphism $\tilde{\rho}_{\mathfrak{m}}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{T}'/\mathfrak{m})$ unramified outside ℓN such that

$$\operatorname{tr}\tilde{\rho}_{\mathfrak{m}}(\mathrm{Frob}_p) = T_p \quad \textit{and} \quad \det\tilde{\rho}_{\mathfrak{m}}(\mathrm{Frob}_p) = p$$

for all $p \nmid \ell N$.

(2) *Suppose that the representation $\tilde{\rho}_{\mathfrak{m}}$ as above is absolutely irreducible. Let $\mathcal{T}'_{\mathfrak{m}}$ denote the $\mathfrak{m}$-adic completion of $\mathcal{T}'$. Then there exists a continuous homomorphism $\rho_{\mathfrak{m}}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{T}'_{\mathfrak{m}})$ such that*

$$\operatorname{tr}\tilde{\rho}_{\mathfrak{m}}(\mathrm{Frob}_p) = T_p \quad \textit{and} \quad \det\tilde{\rho}_{\mathfrak{m}}(\mathrm{Frob}_p) = p$$

(now with equality as elements of $\mathcal{T}'_{\mathfrak{m}}$) for all $p \nmid \ell N$.

Proof. Earlier, we obtained a free $(\mathcal{T} \otimes_{\mathbb{Z}} \mathbb{Q}_\ell)$-module $W = T_\ell(J_0(N)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ of rank 2 on which $G_{\mathbb{Q}}$ acts.

The inclusion $\mathcal{T}' \hookrightarrow \mathcal{T}$ induces an inclusion $\mathcal{T}'_{\mathfrak{m}} \hookrightarrow \mathcal{T} \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$, so we may view $\mathcal{T}'_{\mathfrak{m}} \subset \mathcal{T} \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$. By our earlier results, the trace and determinant forumlas above hold in $\mathcal{T} \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$, with traces of Frob_p landing in $\mathcal{T}'_{\mathfrak{m}}$ for all but finitely p. (See the proof of theorem 14.5.) By Chebytarev, this implies that all traces must land in $\mathcal{T}'_{\mathfrak{m}}$.

Note that in general, to conclude that a representation factors through a subring of the target, it is not enough to know that the traces land in that subring, see Remark 30.2 below. However, a result of Carayole implies that there exists a representation into $\mathrm{GL}_2(\mathcal{T}'_{\mathfrak{m}})$ with the same traces as the representation on W into $\mathrm{GL}_2(\mathcal{T} \otimes_{\mathbb{Z}} \mathbb{Q}_\ell)$. [Car94] □

Remark 30.2. Carayole's result does *not* imply that it is enough for the traces of a representation to lie in a subring for the representation to factor through that subring. Consider for example the usual 2-dimensional representations

$$\rho_1\colon Q_8 \to \mathrm{GL}_2(\mathbb{C}) \quad \text{and} \quad \rho_2\colon D_4 \to \mathrm{GL}_2(\mathbb{C})$$

Both ρ_i have $\mathbb{Z}$-valued characters, but only ρ_2 factors through $\mathrm{GL}_2(\mathbb{R})$. The issue at play here is the *Schur index*, which is 1 for ρ_2 and 2 for ρ_1. See [Rei+61] for further details.

Let $\overline{N} = \overline{N}(\bar{\rho})$ be the product of primes at which $\bar{\rho}$ fails to be good or unramified. Since $\bar{\rho}$ is semistable, its level $N(\bar{\rho})$ is squarefree and

$$\overline{N} = \begin{cases} N(\bar{\rho}) & \text{if } \bar{\rho} \text{ is good at } \ell \\ \ell N(\bar{\rho}) & \text{otherwise.} \end{cases}$$

Theorem 30.3. *There exists a unique ring homomorphism $a\colon \mathcal{T}'(\overline{N}) \to F$ such that $a(T_p) = \operatorname{tr}\bar{\rho}(\mathrm{Frob}_p)$ for all $p \nmid \ell\overline{N}$, and if $\mathfrak{m} = \ker(a)$, then $\bar{\rho}$ is ismorphic to the composition*

$$G_{\mathbb{Q}} \xrightarrow{\tilde{\rho}_{\mathfrak{m}}} \mathrm{GL}_2\left(\mathcal{T}'(\overline{N})/\mathfrak{m}\right) \xrightarrow{a} \mathrm{GL}_2(F)$$

Proof. The above is a restatement of the theorem of Ribet and others that the weak Serre conjecture implies the strong Serre conjecture. [Rib90] Namely, if $\bar{\rho}$ is modular, then [Rib90] implies that it is associated to a cuspidal eigenform of weight 2, level $\overline{N}$, and trivial Nebentypus. Then, let a be the associated eigencharacter, i.e. the unique homomorphism such that $T(f) = a(T)f$ for all $T \in \mathcal{T}'(\overline{N})$. Then, a satisfies the conditions of the theorem. □

Next, we introduce the set Σ. Let $N_\Sigma = \prod_p p^{n_p}$ where

$$n_p = \begin{cases} \text{exponent of } p \text{ in } \overline{N} & \text{if } p \notin \Sigma \\ 2 & \text{if } p \in \Sigma, p \neq \ell \\ 1 & \text{if } p \in \Sigma, p = \ell. \end{cases}$$

For example, $N_\emptyset = \overline{N}$ and for any Σ, $\overline{N}$ divides N_Σ. This divisibility implies that there exists a cannonical ring map $r\colon \mathcal{T}'(N_\Sigma) \to \mathcal{T}'(\overline{N})$. Let $\mathfrak{m}_\Sigma = r^{-1}(\mathfrak{m})$ be the corresponding maximal ideal of $\mathcal{T}'(N_\Sigma)$.

Theorem 30.4. *Let ρ be a lift of $\bar{\rho}$ to a ring $A \in \mathscr{C}_F$. Then the following are equivalent:*

(a) ρ is unramified outside primes dividing ℓN_Σ and there exists a ring homomorphism $\alpha\colon \mathcal{T}'(N_\Sigma) \to A$ such that $\operatorname{tr}\rho(\mathrm{Frob}_p) = \alpha(T_p)$ for all $p \nmid \ell N_\Sigma$.

(b) There exists a ring homomorphism $\hat{\alpha}\colon \mathcal{T}'(N_\Sigma)_{\mathfrak{m}_\Sigma} \to A$ such that ρ is isomorphic to the composition

$$G_{\mathbb{Q}} \xrightarrow{\rho_{\mathfrak{m}_\Sigma}} \mathrm{GL}_2\left(\mathcal{T}'(N_\Sigma)_{\mathfrak{m}_\Sigma}\right) \xrightarrow{\hat{\alpha}} \mathrm{GL}_2(A).$$

Moreover, (a) determines $\hat{\alpha}$ uniquely, $\hat{\alpha}$ extends α continuously, and ρ is a lift of $\bar{\rho}$ of type Σ.

Proof. In this section, we show the equivalence of conditions (a) and (b), leaving the final statement for next time.

First, we show (b) implies (a). Given such a map $\hat{\alpha}$, let α be the composition of $\hat{\alpha}$ with the completing map:

$$\mathcal{T}'(N_\Sigma) \to \mathcal{T}'(N_\Sigma)_{\mathfrak{m}_\Sigma} \xrightarrow{\hat{\alpha}} A.$$

Then, by the trace formula for $\rho_{\mathfrak{m}_\Sigma}$, we have $\alpha(\mathrm{Frob}_p) = \alpha(T_p)$ for all $p \nmid \ell N_\Sigma$.

Now, we show (a) implies (b). Since $T_p \mapsto \operatorname{tr}\bar{\rho}(\mathrm{Frob}_p)$ under α for $p \notin \Sigma$ and $p \nmid \ell N_\Sigma$, the following diagram commutes

$$\begin{tikzcd}
\mathcal{T}'(N_\Sigma) \arrow[r, "\alpha"] \arrow[d] & A \arrow[d] \\
\mathcal{T}'(\overline{N}) \arrow[r, "\alpha"] & F
\end{tikzcd}$$

It therefore follows that $\alpha(\mathfrak{m}_\Sigma)$ is contained in the maximal ideal for A, and so α factors through a map $\hat{\alpha}\colon \mathcal{T}'(N_\Sigma)_{\mathfrak{m}_\Sigma}$. □

31. 2018-04-20: The Universal Modular Deformation II

In this lecture, we continue our study of the universal modular deformation. The moral of the theorems and results in the first part of this section, as with the last lecture too, is that all maps factor throught the nicest possible Hecke alebra.

31.1. **Understanding the Universal Modular Deformation.**

Recall theorem 30.4 from the last lecture. We had proved the equivalence of parts (a) and (b), whose essence is captured in the existence of the following diagram:

$$\begin{tikzcd}
\mathcal{T}'(N_\Sigma) \arrow[rr, "\alpha"'] \arrow[dr] & & A \\
& \mathcal{T}'(N_\Sigma)_{\mathfrak{m}_\Sigma} \arrow[ur, "\hat{\alpha}"'] \arrow[u, phantom, "\circlearrowleft"] &
\end{tikzcd}$$

where the arrow on the left is the usual completing map. Note that it remains to show the rest of the theorem that states: (a) determines $\hat{\alpha}$ uniquely, $\hat{\alpha}$ extends α continuously, and ρ is a lift of $\bar{\rho}$ of type Σ.

Proof. The first claim that (a) determines $\hat{\alpha}$ uniquely is clear from the construction of $\hat{\alpha}$. So is the second claim. Showing that ρ is of type Σ however, takes a little more work.

Let us begin by recalling the definition of $N_\Sigma = \prod_p p^{n_p}$, where:

$$n_p = \begin{cases} \text{exponent of } p \text{ in } \bar{N} & p \notin \Sigma \\ 2 & p \in \Sigma,\, p \neq \ell \\ 1 & p = \ell \end{cases}$$

By part (b) of the theorem, ρ decomposes as:

$$G_{\mathbb{Q}} \xrightarrow{\rho_{\mathfrak{m}_\Sigma}} \mathrm{GL}_2\left(\mathcal{T}'(N_\Sigma)_{\mathfrak{m}_\Sigma}\right) \xrightarrow{\hat{\alpha}} \mathrm{GL}_2(A).$$

Further, the first arrow depends on the Galois action on $J_0(N_\Sigma)$, going back to the construction of $G_{\mathbb{Q}} \to \mathrm{GL}_2\left(\mathcal{T}'(N_\Sigma)g\right)$ and evoking the result of Carayole. Now, $J_0(N_\Sigma)$ has good reduction all primes $p \nmid N_\Sigma$. Therefore by Néron-Ogg-Shafarevich ([Sil09], or any book on arithmetic geometry), ρ is unramified at all primes $p \nmid \ell N_\Sigma$, as required.

If $p^2 \nmid N_\Sigma$, then $J_0(N_\Sigma)$ has semistable reduction at p. In particular, $J_0(N_\Sigma)$ has semistable reduction at ℓ, therefore ρ is semistable at ℓ.(This is a non-trivial fact. To prove this, one must develop a theory analogous to that of Tate curves in the elliptic curve case. Fortunately, Grothendieck has us covered [Gro72])

For the rest of the primes (outside Σ, but still dividing N_Σ), we have defined n_p in by picking the exponent of p in $\bar{N}$, so that ρ can only be as constrained as $\bar{\rho}$. This concluded the proof. □

Definition 31.1. We call a lift ρ of $\bar{\rho}$ satisfying the equivalent conditions of the previous theorem, a *Modular lift of* $\bar{\rho}$ *of type* Σ.

We now proceed to construct a universal such lift!

Let F_0 be the subfield of F, generated by $\operatorname{tr}\bar{\rho}(g)$, $g \in G_{\mathbb{Q}}$. By the Chebotarev Density Theorem, this is the same as the subfield generated by $\operatorname{tr}\bar{\rho}(\mathrm{Frob}_p)$. Thus, since the Hecke operators T_p, $p \nmid \bar{N}$ generate $\mathcal{T}'(\bar{N})$, and these are the traces of the images of Frob_p, we have:

$$\mathcal{T}'(\bar{N})/\mathfrak{m} \cong F_0$$

Further, from the definition of $\mathfrak{m}_\Sigma = r^{-1}\mathfrak{m}$, we have:

$$\mathcal{T}'(N_\Sigma)/\mathfrak{m}_\Sigma \cong \mathcal{T}'(\bar{N})/\mathfrak{m}$$

Set: $\mathcal{T}_\Sigma = \mathcal{T}'(N_\Sigma)_{\mathfrak{m}_\Sigma} \otimes_{W(F_0)} W(F)$. Composing the usual map $\mathcal{T}'(N_\Sigma)_{\mathfrak{m}_\Sigma} \to \mathcal{T}_\Sigma$, with $\rho_{\mathfrak{m}_\Sigma}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{T}'(N_\Sigma)_{\mathfrak{m}_\Sigma})$, gives a map:

$$\rho_\Sigma^{mod}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{T}_\Sigma)$$

Theorem 31.2. *Given a modular lift ρ of $\bar{\rho}$ of type Σ to a ring A in $\mathscr{C}_F$, there exists a unique $\phi\colon \mathcal{T}_\Sigma \to A$, such that the composition:*

$$G_{\mathbb{Q}} \xrightarrow{\rho_\Sigma^{mod}} \mathrm{GL}_2(\mathcal{T}_\Sigma) \xrightarrow{\phi} \mathrm{GL}_2(A)$$

is strictly equivalent to ρ.

This theorem is a statement of the universality of $\mathcal{T}_\Sigma$ (along with ρ_Σ^{mod}) among modular lift of type Σ.

Remark 31.3.

(1) If $\Sigma \subset \Sigma'$, then any modular lift of type Σ, is also one of type Σ'. As a result, theorem 31.2 implies that there is a map:

$$\mathcal{T}_{\Sigma'} \to \mathcal{T}_\Sigma$$

Exercise 31.4. Show that this map must be surjective, since $\mathcal{T}_\Sigma$ is generated by that traces of Frobenius in the image of ρ_Σ^{mod}.

(2) By the universality of $\mathcal{R}_\Sigma$ among *all* lifts of $\bar\rho$ of type Σ, there is a unique map:

$$\phi\colon \mathcal{R}_\Sigma \to \mathcal{T}_\Sigma$$

Further, ρ_Σ^{mod} decomposes as:

$$G_\mathbb{Q} \xrightarrow{\rho_\Sigma^{univ}} \mathrm{GL}_2(\mathcal{R}_\Sigma) \xrightarrow{\phi} \mathrm{GL}_2(\mathcal{T}_\Sigma)$$

By a similar argument as above, $\phi\colon \mathcal{R}_\Sigma \twoheadrightarrow \mathcal{T}_\Sigma$.
We set $\mathbb{T}_\Sigma = \mathcal{T}_\Sigma \otimes_{W(F)} \mathcal{O}$. Tensoring to $\mathcal{O}$, gives us a surjection:

$$\phi_\Sigma\colon \mathcal{R}_\Sigma \twoheadrightarrow \mathbb{T}_\Sigma$$

Note that our goal is to apply the Wiles-Lenstra criteria to the map $\phi_\Sigma\colon \mathcal{R}_\Sigma \twoheadrightarrow \mathbb{T}_\Sigma$. Therefore it still remains to show that $\mathbb{T}_\Sigma$ is free of finte rank as an $\mathcal{O}$-module.

Recall that as corollary to Theorem 13.15 (the q-expansion principle), we obtained that $\mathcal{T}(N) \subset End(S_2(N,\epsilon,\mathbb{Z}))$. Therefore $\mathcal{T}'(N_\Sigma) \subset End(S_2(N_\Sigma, triv, \mathbb{Z}))$. This tells us that $\mathcal{T}_\Sigma$ is a reduced $\mathbb{Z}$ module that is free of finite rank. From this, it is straightforward to deduce that $\mathcal{T}_\Sigma$ is a reduced $W(F)$ module, free of finite rank and hence, $\mathbb{T}_\Sigma$ is a reduced $\mathcal{O}$, free of finite rank.

While it might seem strange, as number theorists, to emphasize the reduced-ness of certain rings, this will later prove handy: it implies that $\eta_{\mathbb{T}_\Sigma} \neq 0$

31.2. **Explicit Construction and Examples.** In this subsection, we try to illustrate how one might go about constructing the $\mathbb{T}_\Sigma$ that we have discussed so far.

The idea is as follows: Givern $\bar\rho$, consider the set of newforms f, such that

$$\rho_f\colon G_\mathbb{Q} \to \mathrm{GL}_2(\mathcal{O}_f)$$

is a (by definition modular) lift of $\bar\rho$ of type Σ. We have not discussed newforms in this course. Newforms at a particular level are those which "don't come from" a lower level. An introductory description can be found in any standard book on modular forms. Further, it is important to note that by the work of Ribet [Rib90], the aforementioned set (which, for convenience, I will denote by M) is non empty: there exists a modular lift of type $\emptyset$, and of type Σ, for any finite set Σ.

Consider the product $\displaystyle\prod_{f\in M} \mathcal{O}_f$. For any $p \notin \Sigma$ and not dividing $\ell N(\bar\rho)$, $\bar\rho$ is unramified at p. For such p, consider $(a_p(f))_f \in \prod_{f\in M} \mathcal{O}_f$. Since $a_p(f) = \operatorname{tr}\bar\rho(\mathrm{Frob}_p)$ for these primes, it follows that $\mathcal{T}_\Sigma$ is the $W(F)$ algebra generated by these elements.

Example 31.5. Consider the newform associated to the elliptic curve with Cremona Label 57B:

$$f_1(\tau) = q + q^2 + q^3 - q^4 - 2q^5 + q^6 - 3q^8 + q^9 - 2q^{10} - q^{12} + O(q^{13})$$

and the newform associated to the curve 57C:

$$f_2(\tau) = q - 2q^2 + q^3 + 2q^4 + q^5 - 2q^6 + 3q^7 + q^9 - 2q^{10} - 3q^{11} + 2q^{12} + O(q^{13})$$

It turns out that f_1 and f_2 are indeed congruent modulo 3. Therefore, $\bar{\rho}_{f_1} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_3)$ and $\bar{\rho}_{f_1} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_3)$ are strictly equivalent. (It turns out that their mod 9 representations are different - in particular, the q-expansions are not congruent modulo 9 - and so their lifts, unfortunately, cannot be strictly equivalent). Further, these are the only two newforms of level 57 and weight 2, that are congruent modulo 3. Even though the dimension of the space of newforms of this level and weight has dimension 3, the third turns out to be incongruent modulo three to the others.

Let us now construct $\mathbb{T}_\emptyset$. By our construction, we must look at tuples: $(a_p(f_1), a_p(f_2))$, for $p \neq 3$. By the congruence observed above, we have:

$$\mathbb{T}_\emptyset = \{(x, y) \in \mathbb{Z}_3^2 \mid x \equiv y \mod 3\} \cong \mathbb{Z}[[T]]/T(T-3)$$

In particular, $\mathbb{T}_\emptyset = 3\mathbb{Z}_3$.

Remark 31.6. If we had congruences module 3^n for some n, we would obtain $\mathbb{T}_\emptyset \cong \mathbb{Z}[[T]]/T(T-3^n)$ and $\eta_{\mathbb{T}_\Sigma} = 3^n\mathbb{Z}_3$. This is why η is often called the *congruence ideal.*

For next time:
Recall that we calculated the values of c_q's that we must use in Theorem 29.4. We must now show that they indeed satisfy the hypothesis for Theorem 29.4, namely that $\eta_{T'} \subset c_q\eta_T$, with $T = \mathbb{T}_\Sigma$

32. 2018-04-23: The Universal Modular Deformation III

In this lecture, we return to the main strategy for proving Fermat's Last Theorem by using our constructions of universal modular deformations. Recall the following commutative diagram.

$$\begin{tikzcd}
R' \arrow[r, two heads, "\phi'"] \arrow[d, two heads] & T' \arrow[d, two heads] \\
R \arrow[r, two heads, "\phi"] & T
\end{tikzcd}$$

Here, we assume $R = \mathcal{R}_\Sigma$, $R' = \mathcal{R}_{\Sigma'}$, $T = \mathbb{T}_\Sigma$, and $T' = \mathbb{T}_{\Sigma'}$ where $\Sigma' = \Sigma \cup \{q\}$ and $q \notin \Sigma$. As mentioned in previous lectures, Wiles-Lenstra Theorem (or Theorem 26.4) implies the following theorem (or Theorem 29.4).

Theorem 32.1. *Suppose there exists $c_q \in \mathcal{O}$ such that:*

(1) $\frac{\Phi_{R'}}{\Phi_R} \leq |\mathcal{O}/c_q|$

(2) $\eta_{T'} \subset c_q\eta_T$

Then ϕ' is an isomorphism if ϕ is an isomorphism.

From last lecture (or in Theorem 29.4), we have constructed a suitable c_q which satisfies the first condition of the above theorem. In this lecture, we show that c_q satisfies the second condition of the above theorem as well.

Theorem 32.2. *With the construction of c_q in Theorem 29.4, $\eta_{T'} \subset c_q\eta_T$.*

We refer to [DDT97] for a rigorous proof of the above theorem. Here we present the idea of the proof of the above theorem.

Proof. Let $\rho_\Sigma^{mod} : G_{\mathbb{Q}} \to GL_2(\mathbb{T}_\Sigma)$ be the universal modular deformation of type Σ. Let M_Σ be the corresponding $G_{\mathbb{Q}}$-module, which is a free $\mathbb{T}_\Sigma$-module of rank 2. One can think of M_Σ as the localization of the Tate module $T_l(J_0(N)) \otimes_{\mathbb{Z}_l} \mathcal{O}$. Since Tate modules have the Weil pairing, M_Σ also has non-degenerate alternating the Weil Pairing.

$$\langle -, - \rangle_\Sigma : M_\Sigma \times M_\Sigma \to \mathcal{O}$$

Here, we say the Weil paring is non-degenerate if $M_\Sigma \cong Hom_{\mathcal{O}}(M_\Sigma, \mathcal{O})$.

Let $p_\Sigma = Ker(\mathbb{T}_\Sigma \to \mathcal{O})$ and $L_\Sigma = M_\Sigma[p_\Sigma]$, i.e. the set of elements annhilated by p_Σ. Here, we may need to make a choice of map $\mathbb{T}_\Sigma \to \mathcal{O}$. Note that L_Σ is a $\mathbb{T}_\Sigma/p_\Sigma = \mathcal{O}$-module, which is free of rank 2.

We first state the following claim. We will skip the proof of the claim.

Claim 32.3. *If {x,y} is a basis for L_Σ as a free $\mathcal{O}$-module, then $\eta_T = (\langle x, y\rangle_\Sigma)$*

The claim shows that in order to compare η_T and η_T', it suffices to compare the corresponding modules M_Σ and $M_{\Sigma'}$. We will compare both modules based on the cases we used for constructing c_q.

Suppose $q \neq l$ and $\overline{\rho}$ is unramified at q. Our construction of c_q was $c_q = (q-1)(a_q^2 - (q+1)^2$, where a_q is the q-th coefficient of associated modular form to ρ. Then $N_{\Sigma'} = N_\Sigma q^2$. (Recall the definition of N_Σ from Theorem 30.3). Let $X = X_0(N_\Sigma)$, $X' = X_0(N_{\Sigma'})$, $J = J_0(N_\Sigma)$, and $J' = J_0(N_{\Sigma'})$.

Consider the degeneracy maps $\delta_i : X' \to X$ defined on the upper half plane, where $\delta_i(\tau) = q^i\tau$ for $i = 0, 1, 2$. These maps induce a map from J' to J, by the functoriality of Albanese variety. We can also induce a map from J' to J in other cases as follows.

(1) if $q \neq l$ and $\overline{\rho}$ is ramified at q, then define the degeneracy maps $\delta_i : X' \to X$ analogously for $i = 0, 1$.
(2) if $q = l$ and $\overline{\rho}$ is good and ordinary at q, then define the degeneracy maps $\delta_i : X' \to X$ analogously for $i = 0, 1$.
(3) if $q = l$ and $\overline{\rho}$ is not both good and ordinary at q, then define the degeneracy maps $\delta_i : X' \to X$ analogously for $i = 0$.

The degeneracy maps δ_i induces the following map.

$$T_l(J') \otimes_{\mathbb{Z}_l} \mathcal{O} \to T_l(J) \otimes_{\mathbb{Z}_l} \mathcal{O} \to M_\Sigma$$

Using the degeneracy maps, we can consider the following maps on $T_l(J') \otimes_{\mathbb{Z}_l} \mathcal{O} \to M_\Sigma$ for each cases of construction of c_q.

(1) if $q \neq l$ and $\overline{\rho}$ is unramified at q, then consider the induced map of $\delta_0 - q^{-1}T_q\delta_1 + q^{-1}\delta_2$.
(2) if $q \neq l$ and $\overline{\rho}$ is ramified at q, then consider the induced map of $delta_0 - q^{-1}T_q\delta_1$.
(3) if $q = l$ and $\overline{\rho}$ is good and ordinary at q, then consider the induced map of $\delta_0 - \alpha_l^{-1}\delta_1$. Here, α_l is the unit roof of $x^2 - T_lx + l = 0$.
(4) if $q = l$ and $\overline{\rho}$ is not both good and ordinary at q, then consider the induced map of δ_0

Hence, we get a map $\beta : M_{\Sigma'} \to M_\Sigma$ from the following commutative diagram.

$$\begin{tikzcd}
 & M_{\Sigma'} \arrow[dr, "\beta"] & \\
T_l(J') \otimes_{\mathbb{Z}_l} \mathcal{O} \arrow[ur] \arrow[r] & T_l(J) \otimes_{\mathbb{Z}_l} \mathcal{O} \arrow[r] & M_\Sigma
\end{tikzcd}$$

Let $\beta' : M_\Sigma \to M_{\Sigma'}$ be the adjoint of β, i.e. $\langle x, \beta y\rangle_\Sigma = \langle \beta' x, y\rangle_{\Sigma'}$.

Wiles computed $\beta\beta' : M_\Sigma \to M_\Sigma$ as an endomorphism of J^3, and computed its effects on cotangent space $S_2(N)^3$, i.e. what the 3×3 matrix does on cusp forms. We will only state the results of $\beta\beta'$ for the first case:

$$\beta\beta' = -q^{-2}(q-1)(T_q^2 - (q+1)^2)$$

Observe that the above computation is c_q up to a unit. One can derive an analogous result for all other cases: that $\beta\beta'$ is c_q up to a unit. For the second and third cases, we need to deal with the action of 2×2 matrix on $S_2(N)^2$, while for the fourth case, we need to deal with the action of the identity matrix on $S_2(N)$.

We state another claim, which allows us to express the basis of $M_{\Sigma'}$ in terms of the basis of M_Σ.

Claim 32.4. *If $\{x, y\}$ is a basis for M_Σ, then $\{\beta'(x), \beta'(y)\}$ is a basis for $M_{\Sigma'}$.*

The proof of the above claim is highly nontrivial. In fact, the claim is a consequence of Ihara's Lemma.

Lemma 32.5 (Ihara's Lemma)**.** *The Kernel of the sum of two p-degeneracy maps from $J_0(N) \times J_0(N)$ to $J_0(N_p)$ is Eisenstein whenever the prime p does not divide N.*

Assuming the claim, then the following holds, which proves the Theorem.

$$\begin{aligned}
\eta_{\mathbb{T}_{\Sigma'}} &= (\langle \beta'(x), \beta'(y)\rangle_{\Sigma'}) \\
&= (\langle x, \beta\beta'(y)\rangle_\Sigma) \quad \textit{(β' is an adjoint of β)} \\
&= c_q(\langle x, y\rangle_\Sigma) \quad \textit{($\beta\beta' = c_q$ up to a unit)} \\
&= c_q \eta_{\mathbb{T}_\Sigma}
\end{aligned}$$

□

Note in order to show Claim 32.4, we need to show that β' has torsion-free cokernel, i.e. β is surjective. This requires using cohomology theory of modular curves and abelian varieties. These are standard techniques in arithmetic geometry, which was not much of a problem for Wiles. What was problematic, however, was that the cohomology theory did not necessarily give insights on handling the minimal case of the aforementioned main strategy of the proof of Fermat's Last Theorem.

The idea was that for certain special Σ, commutative algebra may reveal more properties of R_Σ and T_Σ. Fix $\overline{\rho} : G_{\mathbb{Q}} \to GL_2(F)$ where F is a finite field of odd characteristic l. We assume $\overline{\rho}$ is absolutely irreducible, semistable, and associated to cuspidal eigenform.

Definition 32.6. A prime number q is special if the following criteria hold.

(1) $q \equiv 1 \; mod \; l$
(2) $\overline{\rho}$ is unramified at q.
(3) $\overline{\rho}(Frob_q)$ has distinct eigenvalues in F.

Lemma 32.7. *Let ρ be a lift of $\overline{\rho}$ to some ring A in $\mathcal{C}_F$. Let $\rho : G_{\mathbb{Q}} \to GL_2(A)$ and $M = A^2$. Then there exists a basis of M on which $\rho(M_{\mathbb{Q}_q})$ acts diagonally. In fact, the following equation holds, where $\chi_1, \chi_2 : I_q \to A^\times$ are characters of order a power of l dividing $q-1$.*

$$\rho|_{I_q} = \begin{pmatrix} \chi_1 & 0 \\ 0 & \chi_2 \end{pmatrix}$$

Proof. By Hensel's Lemma, there exists a basis with respect to which a lift of $\overline{\rho}(Frob_q)$ is diagonal, say $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$. Let $x \in I_q$ and $\overline{\rho}$ be unramified at q. Then $\rho(x)$ is an element of $Ker(GL_2(A) \to GL_2(F)) = \Gamma_2(A)$, which is a pro-$l$ group. Recall that the wild inertia subgroup G_1 of I_q is pro-q group. Since $q \neq l$, it holds that $\rho(G_1) = \{1\}$. Therefore, $\rho|_{G_{\mathbb{Q}_q}}$ factors through the following group:

$$G_{\mathbb{Q}_q}/G_1 = \langle x, Frob_q \mid Frob_q x Frob_q^{-1} = x^q \rangle$$

So, the following equation holds.

$$\rho(Frob_q)\rho(x)\rho(Frob_q)^{-1} = \rho(x)^q$$

The above equation can be expressed as the following matrix equation.

$$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \begin{pmatrix} 1 + a_{11} & a_{12} \\ a_{21} & 1 + a_{22} \end{pmatrix} \begin{pmatrix} \frac{1}{\lambda_1} & 0 \\ 0 & \frac{1}{\lambda_2} \end{pmatrix} = \begin{pmatrix} 1 + a_{11} & a_{12} \\ a_{21} & 1 + a_{22} \end{pmatrix}^q$$

Hence, $\rho(x)$ is diagonal, which proves the lemma. □

Next time, we will show that if certain properties hold for infinitely many Σ, then they also hold for the minimal case.

33. 2018-04-25: The Universal Modular Deformation IV

Let's first finish the proof of Lemma 32.7.

Proof of Lemma 32.7 (cont.) Last time, we got an equation

$$\begin{aligned} \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \begin{pmatrix} 1 + a_{11} & a_{12} \\ a_{21} & 1 + a_{22} \end{pmatrix} \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda_2^{-1} \end{pmatrix} &= \begin{pmatrix} 1 + a_{11} & a_{12} \\ a_{21} & 1 + a_{22} \end{pmatrix}^q \\ &\equiv \begin{pmatrix} 1 + qa_{11} & qa_{12} \\ qa_{21} & 1 + qa_{22} \end{pmatrix} (\operatorname{mod} mI), \end{aligned}$$

where $I =$ ideal of A generated by a_{ij} for $i \neq j$. and $m = \ker(A \to F)$. So we have the following equations

$$\lambda_1 \lambda_2^{-1} a_{12} \equiv q a_{12} (\operatorname{mod} mI), \quad \lambda_2 \lambda_1^{-1} a_{21} \equiv q a_{21} (\operatorname{mod} mI).$$

By the assumption that q is special, we see that $\lambda_1 \lambda_2^{-1} \not\equiv 1 (\operatorname{mod} \ell)$ but $q \equiv 1 (\operatorname{mod} \ell)$, which together with the equations above imply that $a_{12}, a_{21} \in mI$, whence $I = mI$. Then by Nakayama's lemma, $I = (0)$ and so $a_{12} = a_{21} = 0$.Thus $\rho(\alpha)$ is diagonal and $\rho|_{G_{\mathbb{Q}_q}}$ has diagonal image.

Moreover, it follows from the equations above that $\rho(x) = \rho(x)^q$. So $\chi_1|_{I_q}, \chi_2|_{I_q}$ has finite order that divides $q-1$ and is a power of ℓ. □

Now, let Δ_q be the biggest quotient of $(\mathbb{Z}/q)^\times$ of order a power of ℓ. Then there is a surjective homomorphism

$$I_q \twoheadrightarrow \Delta_q \quad \text{(via cyclotomic character)}.$$

So Lemma 32.7 shows that each $\chi_i|_{I_q}$ factors through Δ_q. Next, we shall consider finite set of primes Q consisting entirely of special primes. Let $\Delta_Q = \prod_{q\in Q}\Delta_q$. Choosing one of χ_1 and χ_2 yields a homomorphism $\Delta_Q \to A^\times$. In particular, taking A to be the universal type Q deformation ring of $\bar{\rho}$, i.e. $\mathcal{R}_Q$, we have homomorphism $\Delta_Q \to \mathcal{R}_Q^\times$. Composing with $\mathcal{R}_Q \to \mathbb{T}_Q$, we get $\Delta_Q \to \mathbb{T}_Q^\times$. This makes $\mathcal{R}_Q$ and $\mathbb{T}_Q$ into $\mathcal{O}[\Delta_Q]$-modules.

Theorem 33.1. *A lift of $\bar{\rho}$ of type Q to A in $\mathscr{C}_\mathcal{O}$ is unramified at all $q \in Q$ if and only if the kernel of the representing map $\mathcal{R}_Q \to A$ contains $I_Q\mathcal{R}_Q$, where I_Q is the augmentation ideal of $\mathcal{O}[\Delta_Q]$, i.e.*

$$\begin{array}{rcl}\ker(\mathcal{O}[\Delta_Q] & \to & \mathcal{O}) \\ \sum \lambda_i\delta_i & \mapsto & \sum \lambda_i.\end{array}$$

Thus, the natural map $\mathcal{R}_Q \twoheadrightarrow \mathcal{R}_\emptyset$ induces an isomorphism $\mathcal{R}_Q/I_Q\mathcal{R}_Q \xrightarrow{\sim} \mathcal{R}_\emptyset$.

Proof. First, note that $\chi_2|_{I_q} = \chi_1^{-1}|_{I_q}$ for any q, since $\det\rho$ lies in $\Gamma_1(A)$ and $\mathbb{Z}_\ell^\times$ and has finite order, so it's trivial. Thus, one of these two characters, say χ_q, determines the other. A lift is unramified at q if and only if χ_q is trivial.

I_Q is generated by $\delta - 1$ for $\delta \in \Delta_Q$, so by $\delta - 1$ for $\delta \in \Delta_q, q \in Q$. So we just need to show that $\chi_q = 1$ if and only if $(\delta - 1)x$ for $x \in \mathcal{R}_Q$ maps to 0 in A. Indeed, the image of $(\delta-1)x$ is $\chi_q(\delta)x - x$, which is zero if and only if $\chi_q(\delta) = 1$. □

We say $|Q| = r$. Define a ring homomorphism

$$\begin{array}{rcl}\mathcal{O}[[S_1, \cdots, S_r]] & \to & \mathcal{O}[\Delta_Q] \\ 1 + S_i & \mapsto & \text{generator of } \Delta_{q_i}.\end{array}$$

This induces an isomorphism

$$\mathcal{O}[[S_1,\cdots,S_r]]/\left((1+S_1)^{|\Delta_{q_1}|}-1,\cdots,(1+S_r)^{|\Delta_{q_r}|}-1\right) \to \mathcal{O}[\Delta_Q],$$

under which I_Q corresponds to $\langle S_1, \cdots, S_r\rangle$. Via this map, we consider $\mathcal{R}_Q$ and $\mathbb{T}_Q$ as $\mathcal{O}[[S_1,\cdots,S_r]]$-algebras.

Theorem 33.2. *If Q consisting of r special primes, and also satisfies*

$$H^1_{\emptyset^*}(G_\mathbb{Q}, \mathrm{Ad}^0(\bar{\rho})^*) \xrightarrow{\prod res_q} \oplus_{q\in Q} H^1(G_{\mathbb{Q}_q}, \mathrm{Ad}^0(\bar{\rho})^*)$$

is an isomorphism. Then $\mathcal{R}_Q$ is generated by r elements (i.e. is a quotient of $\mathcal{O}[[T_1,\cdots,T_r]]$.

Proof. Note that $\mathcal{R}_Q$ is a quotient of $\mathcal{O}[[T_1,\cdots,T_d]]$ where

$$d = \dim H^1_Q(G_\mathbb{Q}, \mathrm{Ad}^0(\bar{\rho})).$$

So we want to show $d \le r$.

Look at the right-hand side, by applying Wile's formula, we have

$$\begin{aligned}\frac{|L_q|}{|H^0(G_{\mathbb{Q}_q}, \mathrm{Ad}^0(\bar\rho))|} &= \frac{|H^1(G_{\mathbb{Q}_q}, \mathrm{Ad}^0(\bar\rho))|}{|H^0(G_{\mathbb{Q}_q}, \mathrm{Ad}^0(\bar\rho))|} \\ &= |H^2(G_{\mathbb{Q}_q}, \mathrm{Ad}^0(\bar\rho))| \quad \text{(by Euler's local characteristic formula)} \\ &= |H^0(G_{\mathbb{Q}_q}, \mathrm{Ad}^0(\bar\rho)^*)| \quad \text{(by local Tate duality)} \\ \text{(``}\bar\rho \text{ unramified at } q\text{''} \implies) &= |(\mathrm{Ad}^0(\bar\rho)^*)^{\bar\rho(\mathrm{Frob}_q)}| = |F|.\end{aligned}$$

We get such a term for each $q \in Q$, so overall, we have

$$\dim_F H^1_Q(G_{\mathbb{Q}}, \mathrm{Ad}^0(\bar\rho)) = \dim_F H^1_{Q^*}(G_{\mathbb{Q}}, \mathrm{Ad}^0(\rho)^*) + r.$$

Since $\mathcal{R}_Q$ is generated by the same number of elements as $\mathcal{R}_\emptyset$. The argument above for $r = 0$ says $\mathcal{R}_\emptyset$ is generated by $\dim_F H^1_{\emptyset^*}(G_{\mathbb{Q}}, \mathrm{Ad}^0(\bar\rho)^*)$. Finally, to show this is r, we invoke hypothesis and use $\dim_F H^1(G_{\mathbb{Q}_q}, \mathrm{Ad}^0(\bar\rho)^*) = 1$. □

34. 2018-04-27: A Commutative Algebra Theorem

We are trying to prove that the natural surjection $\mathcal{R}_\emptyset \twoheadrightarrow \mathbb{T}_\emptyset$ is an isomorphism. We saw in the last lecture that for any finite set Q of special primes, there is an isomorphism $\mathcal{R}_Q/I_Q\mathcal{R}_Q \xrightarrow{\sim} \mathcal{R}_\emptyset$. The analagous statement for the $\mathbb{T}_Q$ is also true, i.e. there is an isomorphism $\mathbb{T}_Q/I_Q\mathbb{T}_Q \xrightarrow{\sim} \mathbb{T}_\emptyset$. This is due to Mazur, using the cohomology of modular curves, c.f. Chapter 4 of [DDT97]. Moreover, $\mathbb{T}_Q$ is a free, finite rank $\mathcal{O}[\Delta_Q]$-module. It turns out that this is exactly enough information to prove that $\mathcal{R}_\emptyset \to \mathbb{T}_\emptyset$ is an isomorphism thanks to a commutative algebra theorem of Taylor and Wiles.

Theorem 34.1 ([TW95]). *Let $\phi : R \twoheadrightarrow T$ be a surjective ring homomorphism in $\mathscr{C}_{\mathcal{O}}$, and assume that T is a free $\mathcal{O}$-module of finite rank. Suppose that there exists some $r \geq 1$ such that for every $n \geq 1$, there are rings R'_n and T'_n in $\mathscr{C}_{\mathcal{O}}$ and a commutative diagram*

$$\begin{tikzcd} \mathcal{O}[[S_1, \ldots, S_r]] \arrow[d] & \\ R'_n \arrow[r, two heads] \arrow[d, two heads] & T'_n \arrow[d, two heads] \\ R \arrow[r, two heads] & T \end{tikzcd}$$

satisfying the following:

(a) $(S_1, \ldots, S_r)R'_n = \ker(R'_n \to R)$;
(b) $(S_1, \ldots, S_r)T'_n = \ker(T'_n \to T)$;
(c) $I_n := \ker(\mathcal{O}[[S_1, \ldots, S_r]] \to T'_n) \subset \Big((1+S_1)^{\ell^n} - 1, \ldots, (1+S_r)^{\ell^n} - 1\Big)$, and T'_n is free of finite rank as an $\mathcal{O}[[S_1, \ldots, S_r]]/I_n$-module;
(d) R'_n is topologically generated as an $\mathcal{O}$-algebra by r elements.

Then $\phi : R \to T$ is an isomorphism, and R, T are complete intersection rings.

Idea of proof. One should think of (b) and (c) as saying that the T'_n are large and nicely controlled by the S_i, and think of (d) as saying that the R'_n are uniformly small. The idea is to pass to a kind of limit as $n \to \infty$

$$\begin{tikzcd}
& \mathcal{O}\llbracket S_1, \dots, S_r \rrbracket \arrow[d] & \\
\mathcal{O}\llbracket X_1, \dots, X_r \rrbracket \arrow[r, two heads] & R_\infty \arrow[r, two heads] \arrow[d, two heads] & T_\infty \arrow[d, two heads] \\
& R \arrow[r, two heads] & T
\end{tikzcd}$$

and show that $R_\infty \simeq T_\infty \simeq \mathcal{O}\llbracket X_1, \dots, X_r \rrbracket$ and $R \simeq T \simeq \mathcal{O}\llbracket X_1, \dots, X_r \rrbracket / (S_1, \dots, S_r)$. □

We will want to use this theorem with $R'_n = \mathcal{R}_Q$, $T'_n = \mathbb{T}_Q$, $R = \mathcal{R}_\emptyset$, and $T = \mathbb{T}_\emptyset$. To do this, we will need an ample supply of special primes. This is accomplished by the following theorem.

Theorem 34.2. *Let $K = \mathbb{Q}(\sqrt{\ell^*})$, where $\ell^* = (-1)^{(\ell-1)/2}\ell$. Assume that $\bar{\rho}|_{G_K}$ is absolutely irreducible. Then there exists a nonzero integer r such that for all $n \geq 1$, we can find a finite set of primes Q_n satisfying:*
(a) if $q \in Q_n$, then $q \equiv 1 \bmod \ell^n$;
(b) if $q \in Q_n$, then $\bar{\rho}$ is unramified at q and $\bar{\rho}(\mathrm{Frob}_q)$ has distinct eigenvalues;
(c) $|Q_n| = r$;
(d) $\mathcal{R}_{Q_n}$ can be topologically generated by r elements as an $\mathcal{O}$-algebra.

Proof. We need to take $r = \dim_F H^1_{\emptyset^*}(G_\mathbb{Q}, \mathrm{Ad}^0(\bar{\rho})^*)$ so that Theorem 33.2 applies. For each integer n and $\psi \in H^1_{\emptyset^*}(G_\mathbb{Q}, \mathrm{Ad}^0(\bar{\rho})^*)$, we want a prime q (depending on ψ) such that
(a) $q \equiv 1 \bmod \ell^n$;
(b) q is special;
(c) $\mathrm{res}_q(\psi) \neq 0$.
We can do this with Chebotarev. The conditions on q translate to finding $\sigma \in G_\mathbb{Q}$ satisfying
(a) $\sigma \in G_{\mathbb{Q}(\zeta_{\ell^n})} = \ker(G_\mathbb{Q} \to \mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^n})/\mathbb{Q}))$;
(b) $\mathrm{Ad}^0(\bar{\rho})(\sigma)$ has an eigenvalue not equal to 1;
(c) $\psi(\sigma) \notin (\sigma - 1)\,\mathrm{Ad}^0(\bar{\rho})^*$
where $\mathrm{Ad}^0 : \mathrm{GL}_2(F) \to \mathrm{Aut}(M_2^0(F)) \simeq \mathrm{GL}_3(F)$ is the conjugation action.

Exercise 34.3. If $\bar{\rho}$ has eigenvalues λ, μ, then $\mathrm{Ad}^0(\bar{\rho})$ has eigenvalues $1, \lambda/\mu, \mu/\lambda$. Conclude that the conditions listed are indeed equivalent.

Let L be the fixed field of $\mathrm{Ad}^0(\bar{\rho})|_{G_{\mathbb{Q}(\zeta_{\ell^n})}}$. Since scalar matrices act trivially by conjugation, Ad^0 factors as

$$\begin{tikzcd}
\mathrm{GL}_2(F) \arrow[rr, "\mathrm{Ad}^0"] \arrow[dr] & & \mathrm{GL}_3(F) \\
& \mathrm{PGL}_2(F) \arrow[ur, hook] &
\end{tikzcd}$$

Thus the image of $G_{\mathbb{Q}(\zeta_{\ell^n})}$ under $\mathrm{Ad}^0(\bar{\rho})$ can be considered as a finite subgroup of $\mathrm{PGL}_2(F) \subset \mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$. However, all finite subgroups of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$ are explicitly known. Up to conjugacy, all finite subgroups of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$ are groups of upper triangular matrices, $\mathrm{PGL}_2(\mathbb{F}_{\ell^n})$,

$\mathrm{PSL}_2(\mathbb{F}_{\ell^n})$, dihedral groups, A_4, S_4, or A_5. In each of these cases, one can check that

$$H^1(\mathrm{Gal}(L/\mathbb{Q}), \mathrm{Ad}^0(\overline{\rho})^*) = 0$$

either by calculation with a theorem of Cline-Parshall-Scott or by using that $\mathrm{Gal}(L/\mathbb{Q})$ has order prime to ℓ. □

35. 2018-04-30: The Beginning of The End

We begin by continuing the proof of Theorem 34.2 from last time.

Proof of Theorem 34.2 Continued. Consider the following diagram.

$$\begin{tikzcd}
G_{\mathbb{Q}} \arrow[r, "\overline{\rho}"] & \mathrm{GL}_2(F) \arrow[r] \arrow[dr] & \mathrm{Aut}(\mathrm{M}_2^0(F)) \arrow[r, "\cong"] & \mathrm{GL}_3(F) \\
G_{\mathbb{Q}(\zeta_{\ell^n})} \arrow[u, hook] \arrow[ur] & & \mathrm{PGL}_2(F) \arrow[ur, hook] &
\end{tikzcd}$$

Denote by $\widetilde{H}$ the image of the map $G_{\mathbb{Q}(\zeta_{\ell^n})} \to \mathrm{GL}_2(F)$, where $\widetilde{H} = \mathrm{Gal}(M/G_{\mathbb{Q}(\zeta_{\ell^n})})$. Denote by H the image of the map $\mathrm{PGL}_2(F) \hookrightarrow \mathrm{GL}_3(F)$, where $H = \mathrm{Gal}(L/G_{\mathbb{Q}(\zeta_{\ell^n})})$. Then, M is the fixed field of $\overline{\rho}|_{G_{\mathbb{Q}(\zeta_{\ell^n})}}$ and L is the fixed field of $\mathrm{Ad}^0(\overline{\rho})|_{G_{\mathbb{Q}(\zeta_{\ell^n})}}$.

Lemma 35.1.

$$H^1(\mathrm{Gal}(L/\mathbb{Q}), \mathrm{Ad}^0(\overline{\rho})^*) = 0$$

Before proving the lemma, we will indicate how we can use this Lemma to produce a suitable σ. We have the following inflation-restriction exact sequence,

$$0 \to H^1(\mathrm{Gal}(L/\mathbb{Q}), \mathrm{Ad}^0(\overline{\rho})^*) \xrightarrow{\mathrm{inf}} H^1(G_{\mathbb{Q}}, \mathrm{Ad}^0(\overline{\rho})^*) \xrightarrow{\mathrm{res}} H^1(G_L, \mathrm{Ad}^0(\overline{\rho})^*)^{\mathrm{Gal}(L/\mathbb{Q})}$$

The lemma implies that the restriction map is injective. Therefore, $\psi|_{G_L} \neq 0$ and $\psi|_{G_L} \in \mathrm{Hom}(G_L, \mathrm{Ad}^0(\overline{\rho}))$. Now, $\psi(G_L)$ is a $G_{\mathbb{Q}}$ submodule of $\mathrm{Ad}^0(\overline{\rho})^*$ and so the following exercise implies that $\psi(G_L) = \mathrm{Ad}^0(\overline{\rho})^*$.

Exercise 35.2. Using the absolute irreducibility of $\overline{\rho}|_{G_K}$, show that $\mathrm{Ad}^0(\overline{\rho})^*$ is irreducible.

Next, we claim that it is possible to find $\sigma_0 \in G_{\mathbb{Q}(\zeta_{\ell^n})}$ such that $\overline{\rho}(\sigma_0)$ has distinct eigenvalues. If this were not the case, then up to conjugation, $\overline{\rho}(G_{\mathbb{Q}(\zeta_{\ell^n})})$ would be contained in the upper triangular matrices, which would contradict the absolute irreducibility of $\overline{\rho}(G_K)$ (we leave the rest of the details to the interested reader).

Recall that if the eigenvalues of σ_0 are α, β, then the eigenvalues of $\mathrm{Ad}^0(\overline{\rho})(\sigma_0)$ are $1, \frac{\alpha}{\beta}, \frac{\beta}{\alpha}$. Since σ_0 fixes ζ_ℓ, these are also the eigenvalues of $\mathrm{Ad}^0(\overline{\rho})^*(\sigma_0)$. Therefore, $(\sigma_0 - 1)\,\mathrm{Ad}^0(\overline{\rho})^* \neq \mathrm{Ad}^0(\overline{\rho})^*$ and thus

$$\psi(G_L) \not\subseteq (\sigma_0 - 1)\,\mathrm{Ad}^0(\overline{\rho})^* \tag{😸}$$

For $\tau \in G_L$ consider $\sigma = \tau\sigma_0 \in G_{\mathbb{Q}(\zeta_{\ell^n})}$. As τ acts trivially on $\mathrm{Ad}^0(\overline{\rho})$ and $\mathrm{Ad}^0(\overline{\rho})^*$, we have that $\overline{\rho}(\tau)$ is a scalar and hence $\overline{\rho}(\sigma)$ also has distinct eigenvalues. So for this choice of σ, (a) and (b) both still hold. Moreover, by the cocycle condition, we have that

$$\psi(\sigma) = \tau\psi(\sigma_0) + \psi(\tau) = \psi(\sigma_0) + \psi(\tau).$$

We want $\psi(\sigma) \notin (\sigma - 1)\,\mathrm{Ad}^0(\overline{\rho})^*$. If $\psi(\sigma_0) \notin (\sigma_0 - 1)\,\mathrm{Ad}^0(\overline{\rho})^*$, then we're done. If not, then by (😸), we can find a τ such that adjusting $\psi(\sigma_0)$ by $\psi(\tau)$ gives $\psi(\tau\sigma_0) \notin (\sigma_0 - 1)\,\mathrm{Ad}^0(\overline{\rho})^*$. □

Now, we sketch a proof of Lemma 35.1.

Proof of Lemma 35.1. This lemma is a case by case calculation of cohomology, using the following theorem of Dickson.

Theorem 35.3 (Dickson)**.** *[Dic01] Any finite subgroup of* $\mathrm{PGL}_2(\overline{F})$ *is one of the following:*

- *A subgroup of a Borel subgroup,*
- *Conjugate to* $\mathrm{PGL}_2(k)$ *or* $\mathrm{PSL}_2(k)$ *for* k *a finite field,*
- *Dihedral of the form* D_{2n} *with* $(n, \ell) = 1$*,*
- A_4*,* S_4*, or* A_5*.*

Consider the following diagram of fields $\mathbb{Q} \subseteq L' \subseteq M'$, where $\mathrm{Gal}(M'/\mathbb{Q}) = \mathrm{im}(\overline{\rho}) \leq \mathrm{GL}_2(F)$, $\mathrm{Gal}(M'/L') = Z$, the subgroup of scalar matrices in $\mathrm{Gal}(M'/\mathbb{Q})$ and thus $\mathrm{Gal}(L'/\mathbb{Q}) = \mathrm{im}(\mathrm{Ad}^0(\overline{\rho})) \leq \mathrm{PGL}_2(F)$.

First, suppose $Z = \{\pm 1\}$ and $\ell > 3$. Since $\det|_Z = 1$, we have that Z fixes $\mathbb{Q}(\zeta_\ell)$. Thus, $\Delta = \mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q})$ is a quotient of $\mathrm{Gal}(L/\mathbb{Q}) \leq \mathrm{PGL}_2(F)$. Using Dickson's classification, we have that $\mathrm{Gal}(L/\mathbb{Q})$ is contained in a Borel subgroup or has order prime to ℓ (the other cases don't have cyclic quotients of order $\ell - 1$). The absolute irreducibility of $\overline{\rho}$ shows that $\mathrm{Gal}(L/\mathbb{Q})$ is not contained in a Borel.

Thus, $\mathrm{Gal}(L/\mathbb{Q})$ has order prime to ℓ, and $H = \mathrm{Gal}(L/\mathbb{Q}(\zeta_{\ell^n}))$ also has order prime to ℓ. Therefore,

$$H^1(\mathrm{Gal}(L/\mathbb{Q}), \mathrm{Ad}^0(\overline{\rho})^*) = H^1(\mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^n})/\mathbb{Q}), (\mathrm{Ad}^0(\overline{\rho})^*)^H)$$

The latter cohomology is 0 unless $\mathrm{Ad}^0(\overline{\rho})$ is reducible, but this reducibility contradicts the absolute irreducibility of $\rho|_{G_K}$. The reader can find the further cases in [De 97]. □

Now, we can finally get to the proofs we have all been waiting for.

Theorem 35.4 (Wiles)**.** *If* a, b, c, n *are integers, with* $n \geq 3$*, such that* $a^n + b^n + c^n = 0$*, then* $abc = 0$*.*

Theorem 35.5 (Wiles)**.** *Every semistable elliptic curve over* $\mathbb{Q}$ *is modular.*

Proof of Theorem 35.4. Suppose we have a counterexample, let E be the associated Frey curve, and let $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_3)$ be the 3 division representation, which is either reducible or irreducible.

Lemma 35.6. *If* $\overline{\rho}$ *is irreducible, then* $\overline{\rho}|_{G_{\mathbb{Q}(\sqrt{-3})}}$ *is absolutely irreducible.*

Proof. Let H be the image of $\overline{\rho}$ in $\mathrm{PGL}_2(\mathbb{F}_3) \cong S_4$. If the lemma is false, then $H \neq S_4$ (since the only subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ mapping onto $\mathrm{PGL}_2(\mathbb{F}_3)$ must be all of $\mathrm{GL}_2(\mathbb{F}_3)$). Then, we must have that $\mathrm{im}(\overline{\rho}|_{G_{\mathbb{Q}(\sqrt{3})}}) = \mathrm{SL}_2(\mathbb{F}_3)$, which is absolutely irreducible.

We can go through the rest of the subgroups of S_4. Since $\det(\overline{\rho})$ is surjective, we have $H \neq \mathrm{PSL}_2(\mathbb{F}_3) \cong A_4$. Since $\mathrm{im}(\overline{\rho})$ is not contained in a Borel subgroup, H cannot be a subgroup of S_3.

The only remaining possibilities are for H to be a dihedral group or index 2 in a dihedral group. Now, E is semistable at every prime $p \neq 3$. So $\overline{\rho}(I_p)$ has order 1 or 3, but since $\mathrm{im}(\overline{\rho})$ has 2 power order, we have that $\overline{\rho}$ is unramified at every $p \neq 3$.

Then, H^{ab}, the abelianization of H is an abelian 2 group of order 4, and is the Galois group of an extension of $\mathbb{Q}$ ramified only at 3. Such an extension must be contained in $\mathbb{Q}(\zeta_{3^r})$ for some r, but the group $(\mathbb{Z}/3^r\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^{r-1}\mathbb{Z}$ does not have such a quotient. □

We can apply all of our machinery, which we leave to a future lecture. □

36. 2018-05-02: The End of The End

Putting it all together- The final trick

Theorem 36.1. *Fermat's Last Theorem holds, i.e. if a, b, c, n are integers such that $a^n + b^n + c^n = 0$ and $n \geq 3$, then $abc = 0$.*

Theorem 36.2. *Every semistable elliptic curve over $\mathbb{Q}$ is modular.*

Say there is a counter example to FLT, let E be the corresponding Frey curve (For the second theorem, take E to be any semistable elliptic curve). Let $\bar{\rho} : G_{\mathbb{Q}} \longrightarrow Gl_2(\mathbb{F}_3)$ be the associated 3-division representation.
Case 1 $\bar{\rho}$ is irreducible. We will introduce the following lemma.

Lemma 36.3. *In this case $\bar{\rho}|G_{\mathbb{Q}(\sqrt{-3})}$ is absolutely irreducible.*

Proof. Let H be the image of $\bar{\rho}$ in $PGL_2(\mathbb{F}_3) \cong S_4$, then one has the following possibilities. If $H = S_4$, then one can show that $\bar{\rho}$ is also surjective, so $\bar{\rho}(G_{\mathbb{Q}(\sqrt{-3})}) = SL_2(\mathbb{F}_3)$ which is absolutely irreducible; If $H = A_4$, then it implies $Im\bar{\rho} = SL_2(\mathbb{F}_3)$, contradicting that $det\bar{\rho} = \xi$ is surjective. If $H \subset S_3$, then one can show $\bar{\rho}$ has to be reducible, which is a contradiction. So it leaves the cases $H = D_8$ or a subgroup of index 2 in D_8, then $\bar{\rho}$ being semi-stable at $p \neq 3$ implies that $|\bar{\rho}(I_p)| = 1$ or 3 (Recall that $\bar{\rho}(I_p)$ is of the form $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$). $3 \nmid 8$ implies that $\bar{\rho}$ is unramified at p. Then H^{ab} is the Galois group of a degree 4 abelian extension L of $\mathbb{Q}$ ramified only at 3 (and ∞). Then by Kronecker-Weber theorem, $L \subset \mathbb{Q}(\xi_{3^k})$ but then $4 \nmid |Gal(L/\mathbb{Q})|$ □

So now hypotheses of the general case are satisfied, namely $\bar{\rho}$ is absolutely irreducible (even when restricted to $G_{\mathbb{Q}(\sqrt{-3})}$), $\bar{\rho}$ is semistable and $\bar{\rho}$ is modular. Note that the modularity follows from Langlands-Tunnell's theorem by using the embedding $\bar{\rho} : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{F}_3) \hookrightarrow GL_2(\mathbb{Z}[\sqrt{-2}]) \hookrightarrow GL_2(\mathbb{C})$ has solvable image.
Let $\Sigma = \Big\{primes|abc\Big\}$. Action of $T_3(E)$, namely $\rho_{3^\infty} : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{Z}_3)$ is a lift of $\bar{\rho}$ of type Σ. We know that $\mathcal{R}_\Sigma \longrightarrow \mathbb{T}_\Sigma$ is an isomorphism, so the map $\mathcal{R}_\Sigma \longrightarrow \mathbb{Z}_3$ yielding ρ_{3^∞} factors through $\mathbb{T}_\Sigma$, so ρ_{3^∞} is modular, i.e. there exists a cuspidal eigenform f such that $tr_{\rho_{3^\infty}}(Fr_p) = a_p(f)$ for all but finitely many primes p.
Next consider $\rho_{n^\infty} : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{Z}_n)$ where n is the FLT exponent (as we know, it can always chosen to be a prime), $tr_{\rho_{n^\infty}}(Fr_p) = tr_{\rho_{3^\infty}}(Fr_p) = a_p(f)$ for all but finitely many primes p, namely ρ_{n^∞} is modular, so ρ_n is modular as well.
However, we saw that ρ_n is good/unramified at all primes $\neq 2$ and semi-stable at 2. This implies $N(\rho_n) = 2$, by Ribet, ρ_n is associated to a cuspidal eigenform of level 2, weight 2, trivial Nebentypus. But there are no such non-zero eigenforms!
Case 2 $\bar{\rho}$ is reducible. We will apply the following 3-5 switch trick.

Theorem 36.4. *Suppose E is an elliptic curve such that $\rho_3 : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{F}_3)$ is reducible. Then the associated $\rho_5 : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{F}_5)$ is irreducible.*

Proof. Say both are reducible, then $E(\bar{\mathbb{Q}})$ has a $G_{\mathbb{Q}}$-stable subgroup of order 15. By the correspondence:

$$Y_0(N)(K) \leftrightarrow \left\{ \begin{matrix} \text{isomorphism clasees of elliptic curves/K} \\ \text{with a subgroup of order N defined over K} \end{matrix} \right\}$$

where $Y_0(N)(K)$ is the compactification of $X_0(N)$, so E corresponds to a point on $Y_0(15)(\mathbb{Q})$. One can check that $X_0(15)$ is an elliptic curve (15A in the table), known to have 8 rational points. 4 of these are cusps (so $\notin Y_0(15)(\mathbb{Q})$), other 4 corresponds to elliptic curves of conductor 50 which is not square free, so they are not semi-stable, but E is known to be semi-stable. □

So now ρ_5 is absolutely irreducible (even when restricted to $G_{\mathbb{Q}(\sqrt{-3})}$), and semistable, it remains to show that it is modular. Unfortunately, we do not have Langlands-Tunnell's theorem this time as $GL_2(\mathbb{F}_5)$ is not solvable. Thanks to Weils, we have the following trick to overcome this barricade.

Theorem 36.5. *("3-5 switch")*
Say we have the same assumptions on E as before. There exists a semistable elliptic curve A defined over $\mathbb{Q}$ such that $A[5] \simeq E[5]$ as $G_{\mathbb{Q}}$-modules, and $A[3]$ irreducible as $G_{\mathbb{Q}}$-module.

Proof. Consider the collection of all elliptic curves A over $\mathbb{Q}$ such that $A[5] \simeq E[5]$ as $G_{\mathbb{Q}}$ and the diagram of Weil pairings commutes.

$$\begin{tikzcd}
A[5] \times A[5] \arrow[r] \arrow[dr] & E[5] \times E[5] \arrow[d] \\
 & \mu_5
\end{tikzcd}$$

This is in 1-1 correspondence with points on a curve Y', which is twist of $Y(5) = \mathfrak{H}/\Gamma$, where $\Gamma = \left\{M \in SL_2(\mathbb{Z}) | M \cong I \pmod 5\right\}$.
One can show this compactification has genus 0, so if Y' has genus 0, Y' has a point X_0 corresponding to E, so it must be $\mathbb{P}^1$, .
So there are lots of A's satisfying the above constrain on $A[5] \times A[5]$ as a $G_{\mathbb{Q}}$-module. What about $A[3]$ being irreducible as a $G_{\mathbb{Q}}$-module?
Consider $Y'(5,3)$, curve classifying A such that $A[5] \simeq E[5]$ as $G_{\mathbb{Q}}$ modules and A has a subgroup of order 3. One can show its compactification must have genus ≥ 1, so by Faltings (Mordell Conjecture) [**Falt**] has only finitely many points over $\mathbb{Q}$. This shows that there lose only finitely many such A's, which implies there are infinitely many A satisfying $A[5] \simeq E[5]$ as $G_{\mathbb{Q}_p}$-modules and $A[3]$ being irreducible.
One can pick A semistable by picking points 5-adically close to X_0 □

So now A is modular by earlier argument. In particular we know that its associated ρ_5 is modular, but this is the same ρ_5 of E. Therefore ρ_5 is absolutely irreducible, semi-stable and modular, we can apply the same argument as at the end of Case 1! Q.E.D

Thankfully this time I have enough room to write my demonstrationem mirabilem

References

[Bos95] Nigel Boston. “A Taylor-Made Plug for Wiles’ Proof”. *The College Mathematics Journal* 26.2 (1995), pp. 100–105.

[Car94] Henri Carayol. “Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet”. *Contemporary Mathematics* 165 (1994), pp. 213–213.

[Con97] Brian Conrad. “Finite Flat Group Schemes”. *Modular Forms and Fermat’s Last Theorem.* Ed. by Cornell, Silverman, and Stevens. Springer-Verlag New York, 1997, pp. 121–154.

[Con] Brian Conrad. *Surjectivity for Inertia Groups.* URL: `http://math.stanford.edu/~conrad/676Page/handouts/inertiasurj.pdf`.

[DDT97] Henri Darmon, Fred Diamond, and Richard Taylor. “Fermat’s last theorem”. Int. Press, Cambridge, MA, 1997, pp. 2–140.

[De 97] Ehud De Shalit. “Hecke Rings and Universal Deformation Rings”. *Modular Forms and Fermat’s Last Theorem.* Ed. by Cornell, Silverman, and Stevens. Springer-Verlag New York, 1997, pp. 421–445.

[DI95a] Fred Diamond and John Im. “Modular forms and modular curves”. *Seminar on Fermat’s Last Theorem, Providence, RI.* 1995, pp. 39–133.

[DI95b] Fred Diamond and John Im. “Modular forms and modular curves”. *Seminar on Fermat’s Last Theorem (Toronto, ON, 1993–1994).* Vol. 17. CMS Conf. Proc. Amer. Math. Soc., Providence, RI, 1995, pp. 39–133.

[Dic01] L.E. Dickson. “Linear Groups with an Exposition of the Galois Field Theory”. *Teubner* (1901).

[Edi92] Bas Edixhoven. “The weight in Serre’s conjecture on modular forms”. *Invent. Math.* 109 (1992), pp. 563–594.

[FM95] Jean-Marc Fontaine and Barry Mazur. “Geometric Galois representations”. *Elliptic curves, modular forms, & Fermat’s last theorem (Hong Kong, 1993).* Ser. Number Theory, I. Int. Press, Cambridge, MA, 1995, pp. 41–78.

[Gro72] ALexandre Grothendieck. “Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I)”. *Groupes de Monodromie en Géométrie Algébrique I.* Springer-Verlag New York, 1972.

[Kat72] Nicholas M. Katz. *P-adic Properties of Modular Schemes and Modular Forms.* 1972. URL: `https://web.math.princeton.edu/~nmk/old/padicpropMFMS.pdf`.

[Kna92] Anthony W. Knapp. *Elliptic Curves.* Princeton University Press, 1992.

[Lan87] Serge Lang. *Elliptic Functions.* Springer-Verlag New York, 1987.

[PS89] Alexey N. Parshin and Igor R. Shafarevich. *Algebraic Geometry III: Complex Algebraic Varieties, Algebraic Curves, and Their Jacobians.* Springer, 1989.

[Rei+61] Irving Reiner et al. “The Schur index in the theory of group representations.” *The Michigan Mathematical Journal* 8.1 (1961), pp. 39–47.

[Rib90] K. A. Ribet. “On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms”. *Invent. Math.* 100.2 (1990), pp. 431–476.

[Rib95] Kenneth A. Ribet. “Galois representations and modular forms”. *Bull. Amer. Math. Soc. (N.S.)* 32.4 (1995), pp. 375–402.

[RS01] Kenneth Ribet and William Stein. *Arithmetic algebraic geometry.* 2001, pp. 143–232.

[Ser72] Jean-Pierre Serre. “Propriétés galoisiennes des points d’ordre fini des courbes elliptiques”. *Invent. Math.* 15.4 (1972), pp. 259–331.

[Ser79] Jean-Pierre Serre. *Local Fields*. Springer-Verlag New York, 1979.

[Ser87] Jean-Pierre Serre. "Sur les représentations modulaires de degré 2 de Gal($\overline{\mathbf{Q}}/\mathbf{Q}$)". *Duke Math. J.* 54.1 (1987), pp. 179–230.

[Shi71] Goro Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton University Press, 1971.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag New York, 2009.

[Sno13] Andrew Snowden. *Course on Mazur's theorem*. 2013. URL: `http://www-personal.umich.edu/~asnowden/teaching/2013/679/`.

[TW95] Richard Taylor and Andrew Wiles. "Ring-theoretic properties of certain Hecke algebras". *Ann. of Math. (2)* 141.3 (1995), pp. 553–572.

[Wil95] Andrew Wiles. "Modular elliptic curves and Fermat's last theorem". *Ann. of Math. (2)* 141.3 (1995), pp. 443–551.

Index