MODULARITY PROBLEMS OF $\mathbb{Q}$–MOTIVES AND BASE-CHANGE

HARUZO HIDA

Contents

1. Lecture 1

1.1. **Introduction.** As everyone knows, Wiles (and Taylor) proved that, under some mild conditions, if a p–adic Galois representation is congruent modulo p to that of an elliptic cusp form, then the representation itself is associated to a cusp form. It has been reported that the Shimura-Taniyama conjecture has been settled in this way, that is, every $\mathbb{Q}$–rational elliptic curve appears as a $\mathbb{Q}$–rational factor of the jacobian variety of the modular curve $\Gamma_0(N)\backslash\mathfrak{H}$. Taniyama posed another (but related) problem after stating his now famous problem which was one of the origins of the conjecture:

Decompose modular jacobians into simple factors up to isogeny.

As often the case in his problems, the question is not very specific. My interpretation is that he wanted to find a good explicit condition for an abelian variety to appear in a modular jacobian as a simple factor (either over $\mathbb{Q}$ or over $\overline{\mathbb{Q}}$). [1]

The cusp form associated to an elliptic curve over $\mathbb{Q}$ is invariant under $\Gamma_0(N)$, often called "*Haupt*" type. For an elliptic cusp form $f : \mathfrak{H} \to \mathbb{C}$ on the upper half complex plane $\mathfrak{H}$, if each integral matrix $\left(\begin{smallmatrix} a & b \\ cN & d \end{smallmatrix}\right)$ with $ad - Nbc = 1$ acts on f as

$$f\left(\frac{az+b}{cNz+d}\right) = \chi(d)f(z)(cNz+d)^k.$$

When χ is non-trivial, Hecke called such a f "of weight k" and with "*Neben*" type χ (modulo N). I would like to study simple factors rather emphasizing cusp forms with *non-trivial* Neben type.

It is often the case, when the 'Neben' type is a quadratic character, that the compatible system of Galois representations associated to a Hecke eigenform has a special member $\rho_{\mathfrak{q}}$ for a prime $\mathfrak{q}$ such that $\overline{\rho} = (\rho_{\mathfrak{q}} \mod \mathfrak{q})$ has dihedral image, even if $\rho_{\mathfrak{q}}$ is not an induced representation. Explicit characterization of primes with this property would be an interesting question, because a 2-dim induced Galois representation is always modular. In this first lecture, I would like to give a simple constructive method, which actually gives all residually dihedral non-dihedral representations, and its application to some modularity problems.

Let Σ be a finite set of primes including the fixed odd prime p and $\mathbb{Q}^\Sigma$ be the maximal extension unramified outside Σ and ∞. Let $\mathrm{G} = \mathrm{Gal}(\mathbb{Q}^\Sigma/\mathbb{Q})$. We pick an absolutely irreducible *odd* representation $\overline{\rho} : \mathrm{G} \to GL_2(\mathbb{F})$ for a finite field $\mathbb{F}$ of characteristic p. All Galois representations are supposed to be *continuous*, and all valuation rings will be finite flat over $\mathbb{Z}_p$. Always the fixed prime p is supposed to be odd.

We consider the following conditions:

(Ordinarity) $\overline{\rho}|_{D_p} \cong \left(\begin{smallmatrix} \overline{\varepsilon} & * \\ 0 & \overline{\delta} \end{smallmatrix}\right)$ with $\overline{\delta}$ unramified and $\overline{\delta} \neq \overline{\varepsilon}$ on the decomposition group D_p at p;
(Flatness) $\overline{\rho}$ restricted to the decomposition group at p is isomorphic to a Galois module associated to a locally free group scheme over $\mathbb{Z}_p$ of rank $|\mathbb{F}|^2$;
(Irreducibility) $\overline{\rho}$ restricted to $\mathrm{Gal}(\mathbb{Q}^\Sigma/\mathbb{Q}(\mu_p))$ remains absolutely irreducible;
(Modularity) $\overline{\rho}$ is associated to an elliptic cusp form.

Theorem 1.1 (Wiles-Taylor-Diamond)**.** *Suppose modularity and irreducibility and either ordinarity or flatness of $\overline{\rho}$. Let $\rho : \mathrm{G}_\Sigma \to GL_2(\mathcal{O})$ be a Galois representation for a DVR $\mathcal{O}$ such that*

1. $\rho \equiv \overline{\rho} \mod \mathfrak{m}_{\mathcal{O}}$;
2. $\det\rho = \nu_p^{k-1}$ *up to finite order characters for $k \geq 2$, where ν_p is the p–adic cyclotomic character;*
3. $\rho|_{D_p} \cong \left(\begin{smallmatrix} \varepsilon & * \\ 0 & \delta \end{smallmatrix}\right)$ *for an unramified character $\delta \equiv \overline{\delta} \mod \mathfrak{m}_{\mathcal{O}}$ when $\overline{\rho}$ is ordinary;*
4. *When $\overline{\rho}$ is flat, $k = 2$ and $\det\rho|_{I_p} = \nu_p|_{I_p}$ and ρ is associated to a p–divisible group over $\mathbb{Z}_p$ in the sense of Tate.*

Then there exist a positive integer N and a Hecke eigenform $f \in S_k(\Gamma_1(N))$ such that $\rho \cong \rho_f$.

[1] An exact English translation of the two problems can be found in Shimura's notes: "Yutaka Taniyama and his time" in Bull. London Math. Soc. 21 (1989).

This theorem was proven in the now famous paper of Wiles (Ann. of Math. 141 (1995)) as Theorem 0.2, assuming a ring theoretic property of the Hecke algebra, which was in turn proven by Taylor-Wiles in the paper following the above. A condition of ramification outside p imposed in the work of Wiles was later removed by Diamond. The flatness condition is now eased by Breuil-Conrad-Diamond-Taylor to potential flatness.

1.2. **Residually induced representation.** I always write A for a DVR. Let F be a quadratic extension of $\mathbb{Q}$, and fix a finite set S of rational primes including p. We look into a little smaller $G = \mathrm{Gal}(F^S/\mathbb{Q})$ and $H = \mathrm{Gal}(F^S/F)$. First I explain how to create a Galois representation $\rho_G : G \to GL_2(B)$ (for a canonical $B \supset A$) residually dihedral from a Galois representation $\rho = \rho_H : H \to GL_2(A)$.

We write Δ for G/H and fix an element $\delta \in G$ which generate Δ. Put $V = A^2$, and let H act on V via ρ_H. We may assume $V = A[H]v$ for $\exists v \in V$ (replacing V by $A[H]v$ if necessary). We assume that ρ_H to satisfy the following two conditions:

(I1) ρ_H is absolutely irreducible over the quotient field of A (and $V = A[H]v$);
(I2) We have an A–linear endomorphism $T : V \to V$ such that $T(hx) = \delta h \delta^{-1} T(x)$ and $\det T \neq 0$, where $\Delta = \langle \delta \rangle$.

The existence of T assures us the existence of an extension ρ_G of ρ_H. Here is how to create an universal extension ρ_G. Consider the induced module: $W = A[G] \otimes_{A[H]} V$, which is free of rank 4 over A. Define an A–linear endomorphism $\widetilde{T} : W \to W$ by $\widetilde{T}(\delta^i \otimes v) = \delta^{i-1} \otimes T(v)$ for $i \in \mathbb{Z}/2\mathbb{Z}$. By

$$\widetilde{T}(h\delta^i \otimes v) = \delta^{i-1} \otimes T(\delta^{-i} h \delta^i v) = \delta^{i-1} \otimes \delta^{1-i} h \delta^{i-1} T(v) = h\delta^{i-1} \otimes T(v) = h\widetilde{T}(\delta^i \otimes v),$$

$\widetilde{T}$ commutes with $A[H]$ and obviously commutes with δ and hence commutes with $A[G]$. Thus $B = \mathrm{End}_{A[G]}(W)$ is bigger than A.

Dividing T by a suitable element in A, we may assume that $\overline{T} = (T \mod \mathfrak{m}_A)$ for the maximal ideal $\mathfrak{m}_A$ of A does not vanish. By definition, $\rho_H(\delta^{-2})T^2$ commutes with ρ_H and hence is a scalar t by Schur's lemma. The scalar t is uniquely determined in $O = (A - \{0\})/(A^\times)^2$, and we call the class $Ob(\rho_H) \in O$ the obstruction class of ρ_H. It is easy to see:

Proposition 1.2. *We have*

(1) $B = A[\sqrt{t}] = A[X]/(X^2 - t)$;
(2) W *is free of rank* 2 *over* B;
(3) *If* $Ob(\rho_H) \in \mathfrak{m}_A$, *then* B *is a local ring; so, write* $\rho_G : G \to GL_2(B)$ *for the representation realized on* W;
(4) *If* $Ob(\rho_H) \in \mathfrak{m}_A$ *and* $\overline{\rho} = (\rho_G \mod \mathfrak{m}_B)$ *is absolutely irreducible, then there exists a character* $\xi : H \to (B/\mathfrak{m}_B)^\times$ *such that* $\overline{\rho} \cong \mathrm{Ind}_H^G \xi$.

All assertions can be easily proven. For example, (4) follows from the fact that $\overline{T} \not\equiv 0 \mod \mathfrak{m}_A$ but $\det \overline{T} = 0$. Thus we have an exact sequence of H–modules: $0 \to \mathrm{Ker}(\overline{T}) \to V/\mathfrak{m}_A V \to \mathrm{Im}(T) \to 0$; so, $\overline{\rho}_H$ is reducible with semi-simplification isomorphic to $\xi \oplus \xi^\delta$ ($\xi^\delta(h) = \xi(\delta h \delta)$). □

The ring B has an involution $\sigma : \circlearrowright B$ such that $\rho_G \otimes \chi \cong \sigma \circ \rho_G$ and $\sigma(\sqrt{t}) = -\sqrt{t}$ ($\chi : G/H \cong \{\pm 1\}$).

There is a converse of the above proposition: Start with a Galois representation $\varphi : G \to GL_2(\mathcal{O})$ for a DVR $\mathcal{O}$ with irreducible $\overline{\varphi} = (\varphi \mod \mathfrak{m}_\mathcal{O}) \cong \mathrm{Ind}_H^G \xi$. We assume that $\varphi_H = \varphi|_H$ is absolutely irreducible. Since, for $\chi : G/H \cong \{\pm 1\}$,

$$\phi \cong \mathrm{Ind}_H^G \eta \ \exists \eta \iff \phi \otimes \chi \cong \phi,$$

we can divide our consideration into two cases:

(a) There exists an involution σ of $\mathcal{O}$ such that $\sigma \circ \varphi \cong \varphi \otimes \chi$;
(b) No such involution.

We may assume that $\mathcal{O}$ is generated by $\mathrm{Tr}(\varphi)$ because $\varphi(\delta)$ has eigenvalues ± 1 and φ has Schur index 1. In Case (b), we regard $\Phi = \varphi \oplus (\varphi \otimes \chi)$ as representations into $GL_2(B')$ for the subring $B' \subset \mathcal{O} \oplus \mathcal{O}$ generated over $\mathcal{O}$ by $\mathrm{Tr}(\Phi(g))$ for all $g \in G$. Then we define $\sigma \in \mathrm{Aut}(B')$ by $\sigma(x, y) = (y, x)$. In Case (a), we write B' for $\mathcal{O}$ and Φ for φ. We have

Proposition 1.3. *Let $A_0 = H^0(\langle\sigma\rangle, B')$. Then there exist a DVR A unramified over A_0 and $\rho_H : H \to GL_2(A)$ such that*

(1) $\mathrm{Tr}\rho_H = \mathrm{Tr}\varphi_H$;
(2) *We have an isomorphism $\iota : B \hookrightarrow A \otimes_{A_0} B'$ such that $\iota \circ \rho_G \cong \varphi$ or Φ according as we are in Case (a) or (b),*

where ρ_G is the representation constructed in the previous proposition.

Since this is slightly technical, I will not prove this here. A proof is given in my new book [H00b] Chapter V, and a summary on this result can be downloaded from my web site: www.math.ucla.edu/~hida as a preprint: "Modular Galois Representations of Neben type".

1.3. **Modularity Problems.** We start with an irreducible Galois representation $\rho_H : H \to GL_2(A)$ satisfying the following three conditions in addition to (I1-2):

(I3) We have $Ob(\rho_H) \in \mathfrak{m}_A$;
(I4) $\overline{\rho}_G = \rho_G \mod \mathfrak{m}_B$ is absolutely irreducible;
(I5) $\det \rho_G(c) = -1$ for complex conjugation c.

Combining the two proposition with the theorem of Wiles-Taylor-Diamond, we get

Theorem 1.4. *Suppose the five conditions* (I1-5) *and that the representation ρ_G is either p–ordinary with $\det \rho_G = \nu_p^{k-1}$ up to finite order characters for $k \geq 2$ or flat with $\det \rho|_{I_p} = \nu_p|_{I_p}$. Then for any extension $\varphi : G \to GL_2(\mathcal{O})$ of ρ_H for a DVR $\mathcal{O}$ over A, if $\overline{\varphi} = (\varphi \mod \mathfrak{m}_{\mathcal{O}})$ is absolutely irreducible on $\mathrm{Gal}(F^S/\mathbb{Q}(\mu_p))$, then there exist an integer $N > 0$ and a Hecke eigenform $f : S_k(\Gamma_1(N))$ such that $\varphi \cong \rho_f$.*

1.4. **Elliptic $\mathbb{Q}$–Curves.** An elliptic curve E defined over a number field is called $\mathbb{Q}$–*curve* if for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we have an isogeny $\mu_\sigma : E \to E^\sigma$. By a result of Elkies, all elliptic $\mathbb{Q}$-curves have a model over a $(2, 2, \ldots, 2)$–extension of $\mathbb{Q}$.

Corollary 1.5. *Let E be an elliptic curve defined over F with an isogeny $\theta : E \to E^\delta$. Suppose that $\mathrm{End}(E_{/\overline{\mathbb{Q}}}) = \mathbb{Z}$ and that there exists a prime $5 \leq p \nmid D$ with the following two properties:*

(1) *E has semi-stable reduction at p;*
(2) *$p|\deg(\theta)$ and the p–primary part of $\mathrm{Ker}(\theta)$ is cyclic.*

Then there exists a positive integer N such that E shows up as a factor over an abelian extension of F of the jacobian of the modular curve $X_1(N)$.

Proof. We need to check the five conditions: (I1-5) and the assumptions of Theorem 1.4 for $V(\varphi) = T_p(E)$. I indicate how to create the linear operator T in (I2).

Assume that p divides $\deg(\theta)$ and that $p \geq 5$. We may identify $E^\delta[p^\infty]$ with $E[p^\infty]$ by $x \mapsto \delta x$. We get a natural identification of $V(\varphi^\delta)$ and $V(\varphi)$. Writing this identification as $i : V(\varphi) \cong V(\varphi^\delta)$, then $i(h(x)) = \delta h \delta^{-1} i(x)$. The isogeny θ induces $T = i \circ \theta : V(\varphi) \to V(\varphi)$ such that $T(hx) = \varepsilon(h)\delta h \delta^{-1} T(x)$ for a character $\varepsilon : H \to \{\pm 1\}$. The character ε is trivial if and only if θ is defined over F. We can show that $\varepsilon = \eta^{\delta-1}$ for another character η of H. Then $\eta \otimes \varphi$ satisfies (I2). Thus E is a factor of the jacobian over the splitting field of η. □

Here is how to find examples of Elliptic $\mathbb{Q}$–curves: p–isogenies $\{\theta : E \to E'\}$ between elliptic curves are classified by the modular curve $X_0(p)$. For each point $y \in X_0(p)(\overline{\mathbb{Q}})$ represented by θ, $\mathbb{Q}(y)$ is characterized as the field of moduli of θ defined over $\overline{\mathbb{Q}}$: $\mathbb{Q}(y)$ is the fixed field of

$$G(\theta) = \left\{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \middle| \theta^\sigma \cong \theta \text{ over } \overline{\mathbb{Q}}\right\},$$

Take a point y with $\mathbb{Q}(y) = F$. As is well known, we can choose a model of E defined over F. For this model, we are in the situation of the corollary. Thus the main point is to find $y \in X_0(p)$ quadratic over $\mathbb{Q}$. The functorial correspondence $\theta \mapsto {}^t\theta$ induces an involution τ of $X_0(p)$. We make a quotient curve $X^*(p) = X_0(p)/\langle\tau\rangle$. If $x \in X^*(p)(\mathbb{Q})$ and $y \in X_0(p)$ is over x, $\mathbb{Q}(y)$ is either $\mathbb{Q}$ or a quadratic extension F.

Here is a list of primes $p \geq 5$ for which $X^*(p) \cong \mathbf{P}^1_{/\mathbb{Q}}$:

$$p = 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71.$$

By a work of Mazur if $p \geq 11$ in the above list, there are no non-CM rational points of $X_0(p)$ (actually there is at most one non-cuspidal $\mathbb{Q}$–rational point in these cases). Thus all points on $X_0(p)$ over infinitely many (non-CM) $\mathbb{Q}$–rational points of $X^*(p)$ yield examples of type (1) or (2).

Even if the genus of $X_0(p)$ is 0, by Hilbert's irreducibility theorem, for infinitely many $x \in X^*(\mathbb{Q})$, we find $\mathbb{Q}(y)$ quadratic over $\mathbb{Q}$ (for $y \in X_0(p)$ over x) as explicitly done by Shimura in his Annals paper in 1972 for $p = 5$.

2. Lecture 2

In this second lecture, we describe a theory of Ribet on abelian $\mathbb{Q}$–varieties with real multiplication (see [H] Section 8 for a generalization to $\mathbb{Q}$–motives). In the third lecture, we generalize the technique we employed in the first lecture to the present case and give a sufficient condition for the modularity of such abelian varieties.

2.1. **Abelian F–varieties with real multiplication.** We consider abelian varieties X defined over a number field F. We write $\mathrm{End}(X_{/F})$ for the F–endomorphism algebra of X, and put

$$\mathrm{End}^{\mathbb{Q}}(X_{/F}) = \mathrm{End}(X_{/F}) \otimes_{\mathbb{Z}} \mathbb{Q},$$

which is a finite dimensional semi-simple algebra over $\mathbb{Q}$. For a subalgebra $E \subset \mathrm{End}^{\mathbb{Q}}(X_{/F})$, we write $\mathrm{End}^{\mathbb{Q}}_E(X_{/F})$ for the E–linear endomorphism subalgebra of $\mathrm{End}^{\mathbb{Q}}(X_{/F})$. We call X has *real multiplication* (an AVRM) if the following two conditions are satisfied:

(rm1) $E \subset \mathrm{End}^{\mathbb{Q}}(X_{/\overline{\mathbb{Q}}})$ for a totally real field E with $[E:\mathbb{Q}] = \dim X$;

(rm2) $$E = \mathrm{End}^{\mathbb{Q}}_E(X_{/\overline{\mathbb{Q}}}).$$

An AVRM $X_{/\overline{\mathbb{Q}}}$ is called an *F–AVRM* if we have an E–linear isogeny $\mu_\sigma : \sigma(X) \to X$ for all $\sigma \in G_F = \mathrm{Gal}(\overline{\mathbb{Q}}/F)$. Here E acts naturally on $\sigma(X)$ through conjugation by σ. An F–AVRM $X_{/\overline{\mathbb{Q}}}$ has a *model* $X_{/K}$ for an extension K/F if the following three conditions are satisfied:

- X is defined over K;
- $X_{/K} \times_K \overline{\mathbb{Q}}$ is isogenous to $X_{/\overline{\mathbb{Q}}}$;
- $E \subset \mathrm{End}^{\mathbb{Q}}(X_{/K}) \subset \mathrm{End}^{\mathbb{Q}}(X_{/\overline{\mathbb{Q}}})$.

Since $X_{/\overline{\mathbb{Q}}}$ is defined over a finitely generated subfield of $\overline{\mathbb{Q}}$, it has a model over a finite Galois extension L over F. We may assume that μ_σ for $\sigma \in \mathrm{Gal}(L/F)$ is defined over L. We define a 2–cocycle $c(\sigma,\tau)$ on G_F by $c(\sigma,\tau) = \mu_\sigma{}^\sigma\mu_\tau\mu_{\sigma\tau}^{-1}$ which has values in $E^\times$. The cocycle factors through $G_F/G_L = \mathrm{Gal}(L/F)$, and therefore locally constant (that is, continuous under the discrete topology on $E^\times$). We consider the cohomology class $Ob_{\overline{\mathbb{Q}}}(X) = [c]$ in the continuous cohomology group $H^2(G_F, E^\times)$ under the discrete topology on $E^\times$.

Lemma 2.1. *If $Ob_{\overline{\mathbb{Q}}}(X) = 0$ in $H^2(G_K, E^\times)$ for an extension K/F, X has a model defined over K.*

Proof. Let $L/K/F$ be an intermediate field. For a given projective variety $Y_{/L}$, Y has a model if and only if the Galois group $\mathrm{Gal}(L/K)$ acts on $Y_{/K}$ through automorphisms of the scheme $Y_{/K}$ compatible with its action on $\mathrm{Spec}(L)$, which is in turn equivalent to have an isomorphism $f_\sigma : \sigma(Y) \cong Y$ for each $\sigma \in \mathrm{Gal}(L/K)$ satisfying a cocycle relation $f_\sigma \circ {}^\sigma f_\tau = f_{\sigma\tau}$. We consider $Y_{/L} = \bigoplus_{\sigma\in\mathrm{Gal}(L/K)} \sigma(X)$. We define $\varepsilon_\sigma : \sigma(Y) \cong Y$ by $\varepsilon_\sigma(x_\tau) = (x_{\sigma\tau})$. By computation, we check the cocycle relation $\varepsilon_\sigma \circ {}^\sigma\varepsilon_\tau = \varepsilon_{\sigma\tau}$. We find a model $Y_{/K} = \mathrm{Res}_{L/K}X$. This model is characterized by the Frobenius reciprocity law:

$$\mathrm{Hom}(Z_{/K}, \mathrm{Res}_{L/K}X) \cong \mathrm{Hom}(Z_{/L}, X_{/L}).$$

From this, we have

$$\mathrm{End}^{\mathbb{Q}}_E(Y_{/K}, Y_{/K}) \cong \mathrm{End}_E(\oplus_\sigma \sigma(X), X_{/L}) \cong \bigoplus_\sigma E\mu_\sigma.$$

As an endomorphism of $Y_{/L}$, we have $\mu_\sigma(\oplus_\tau x_{\tau\sigma}) = \oplus_\tau{}^\tau\mu_\sigma(x_{\tau\sigma})$, where $x_\tau \in \tau(X)$. From this, we conclude $\mu_\sigma\mu_\tau = c(\sigma,\tau)\mu_{\sigma\tau}$ for the obstruction cocycle c. If $c = 1$, then $\sigma \mapsto \mu_\sigma$ induces $E[\mathrm{Gal}(L/K)] \cong \mathrm{End}_E(Y_{/K})$. In particular, we have the idempotent $e = [L:K]^{-1}\sum_\sigma \sigma$. For sufficiently large integer N, Ne induces an endomorphism of $Y_{/K}$ and $Ne(Y)$ gives a model of X over K, since $Ne(Y)$ is isogenous to X over L.

If $Ob_{\overline{\mathbb{Q}}}(X) = 0$ in $H^2(G_K, E^\times)$, enlarging L if necessary, we find a cochain $\alpha : \mathrm{Gal}(L/K) \to E^\times$ such that $c(\sigma,\tau) = \alpha(\sigma)\alpha(\tau)\alpha(\sigma\tau)^{-1}$. Replacing μ_σ by $\alpha(\sigma)^{-1}\mu_\sigma$, the obstruction cocycle becomes trivial, and hence we find a model of X over K. □

Proposition 2.2 (K. Ribet)**.** *Each F–AVRM has a model over a composite of (finitely many) quadratic extensions of F.*

An extension L/F is a composite of quadratic extensions of F if and only if $\mathrm{Gal}(L/F)$ is killed by 2, that is, a $(2,2,\dots,2)$–elementary group; so, we call such an extension a $(2,2,\dots,2)$–extension in the rest of the lectures.

Proof. The rational Betti cohomology group $H^1(X,\mathbb{Q})$ is two dimensional over E. Take an E–linear polarization $\lambda : X \to {}^tX$ for the dual abelian variety ${}^tX$. This induces the E–linear map of $H^1(X,\mathbb{Q})$ to $H_1(X,\mathbb{Q})$ and hence induces by the Poincaré duality $\wedge^2_E H^1(X,\mathbb{Q}) \cong E$. Conjugating the polarization, we have the identity $\wedge^2_E H^1(\sigma(X),\mathbb{Q}) \cong E$. In this way, any homomorphism $\alpha : X \to \sigma(X)$ induces multiplication by $\deg(\alpha) : \wedge^2 H^1(X,\mathbb{Q}) \to \wedge^2 H^1(\sigma(X),\mathbb{Q})$, which is multiplicative in composition. By definition, $\deg(e) = e^2$ for $e \in E$, and we have

$$c(\sigma,\tau)^2 = \deg(c(\sigma,\tau)) = \frac{\deg(\mu_\sigma)\deg(\mu_\tau)}{\deg(\mu_{\sigma\tau})}.$$

Thus $Ob_{\overline{\mathbb{Q}}}(X)$ is killed by 2.

Look at the split exact sequence of the trivial G_F–modules:

$$1 \to \mu_2 \to E^\times \to P \to 1.$$

We have

$$H^2(G_F, E^\times) \cong H^2(G_F,\mu_2) \times H^2(G_F,P).$$

By a theorem of Mercuriev, cohomology classes of order 2 in the Brauer group $Br(F) \cong H^2(G_F,\mu_2)$ get trivialized over a quadratic extension (they are generated by the classes of quarternion algebras). Thus we need to show that cohomology classes killed by 2 in $H^2(G_F,P)$ get trivialized over a $(2,2,\dots,2)$–extension.

Since P is a $\mathbb{Z}$–free module, we have a short exact sequence:

$$0 \to \mathrm{Hom}(G_F,P)\otimes\mathbb{Z}/2\mathbb{Z} \to \mathrm{Hom}(G_F,P/2P) \to H^2(G_F,P)[2] \to 0,$$

where $[2]$ indicates the kernel of the multiplication by 2. Since P is discrete and torsion-free, $\mathrm{Hom}(G_F,P) = 0$ and hence,

$$\mathrm{Hom}(G_F,P/2P) \cong H^2(G_F,P)[2],$$

which shows the desired result. □

Corollary 2.3. *For an F–AVRM $(X,\mu_\sigma)_{/\overline{\mathbb{Q}}}$, we can find a $(2,2,\dots,2)$–extension L/F over which X has a model with all μ_σ rational over L.*

Proof. Take a model of X over a $(2,2,\dots,2)$–extension K/F. Since $H^0(X,\Omega_{X/K})$ is free of rank 1 over $K\otimes_{\mathbb{Q}} E$, we take a generator ω. For any $\delta \in G_F$, we have $e_\delta \in (\overline{\mathbb{Q}}\otimes E)^\times$ such that $\mu_\delta^*\omega = e_\delta\delta(\omega)$. We have for $\sigma \in G_K$,

$$({}^\sigma\mu_\delta)^*\omega = {}^{\sigma\otimes 1}e_\delta\delta(\omega).$$

Thus

$${}^{\sigma\otimes 1}e_\delta\delta(\omega) = ({}^\sigma\mu_\delta)^*\omega = e_\delta(\mu_\delta^{-1}\circ {}^\sigma\mu_\delta)^*\delta(\omega)$$

and

$$e_\delta^{-1}({}^{\sigma\otimes 1}e_\delta) = \mu_\delta^{-1}\circ {}^\sigma\mu_\delta =: \zeta_\sigma \in \mathrm{End}_E(M_{/K}) = E.$$

Since $\sigma \mapsto e_\delta^{-1}(\sigma\otimes 1)(e_\delta)$ is a character of G_K with values in $E^\times$, we see that ζ_σ is a root of unity in E, that is $\{\pm 1\}$. The map: $\sigma \mapsto {}^{\sigma-1}e_\delta \in \{\pm 1\}$ gives an isomorphism α of $\mathrm{Gal}(K_\delta/K)$ into $\{\pm 1\}$ for at most a quadratic extension K_δ/K, which is the minimal field of definition of μ_δ. We have ${}^\sigma\mu_\delta = \alpha(\sigma)\mu_\delta$ and ${}^\sigma e_\delta = \alpha(\sigma)e_\delta$.

Suppose that $[K_\delta : K] = 2$ (otherwise there is nothing to prove). Since

$$(\mu_\delta\circ {}^\delta\mu_\delta)^*\omega = e_\delta{}^\delta e_\delta\omega,$$

we see that $a = e_\delta{}^\delta e_\delta \in E$ for any extension of δ to G_F. From this, we have

$${}^{\delta^2}e_\delta = \delta(ae_\delta^{-1}) = e_\delta,$$

and $\delta^2 = 1$ for all $\delta \in \mathrm{Gal}(K_\delta/K)$ inducing δ on K. Thus again $\mathrm{Gal}(K_\delta/K)$ is a $(2,\dots,2)$–group. □

A similar argument shows, if an F–AVRM is defined over K

all elements in $\mathrm{End}(X_{/\overline{\mathbb{Q}}})$ *is defined over a* $(2,2,\dots,2)$*–extension of* K.

2.2. **Endomorphism algebra of an F–AVRM.** In the rest of the lecture, the couple (X,μ_σ) is an F–AVRM defined over a $(2,2,\dots,2)$–extension L/F. We suppose that the pair $(X,\mu_\sigma)_{/L}$ cannot be defined over a subfield of L. By changing X in its isogeny class, we assume that $O_E \subset \mathrm{End}(X_{/\overline{\mathbb{Q}}})$ for the integer ring O_E of E.

Let $c:\Delta\times\Delta\to A$ be a 2–cocycle for $\Delta=\mathrm{Gal}(L/F)$. We call the class $[c]\in H^2(\Delta,A)$ commutative if $c(\sigma,\tau)=c(\tau,\sigma)$ for all $\sigma,\tau\in\Delta$. Since Δ is an abelian group, any 2–coboundary with values in a module with trivial action is commutative. Thus commutativity is a well defined notion of cohomology class.

The map $c\mapsto b(\sigma,\tau)=c(\sigma,\tau)-c(\tau,\sigma)$ induces a surjective homomorphism:

$$\theta: H^2(\Delta,A)\to \mathrm{Hom}(\wedge^2\Delta,A),$$

and its kernel is made up of commutative classes (see Brown's book GTM 87 page 127). Let c be the obstruction cocycle of $X_{/L}$. As we have already seen,

$$\mathrm{End}_E(\mathrm{Res}_{L/F}X)=\bigoplus_{\delta\in\Delta} E\mu_\delta$$

and $\mu_\sigma\mu_\tau=c(\sigma,\tau)\mu_{\sigma\tau}$. Thus $Ob_L(X)=[c]\in H^2(\Delta,E^\times)$ is commutative if and only if $\mathrm{End}_E(\mathrm{Res}_{L/F}X)$ is commutative.

For the obstruction cocycle $c:\Delta\times\Delta\to E^\times$, by the above fact, its projection to torsion-free $P=E^\times/\{\pm1\}$ is commutative. The non-commutative part concentrate on the Brauer part $c_\pm$, which is the projection to μ_2.

Lemma 2.4. *Suppose that* $Ob_L(X)\in H^2(\Delta,E^\times)$ *is non-commutative. Then there exist a finite extension* E'/E*, a splitting* $\Delta=\Delta'\times\Delta''$ *and an abelian variety* $Y_{/L'}$ *for* $L'=L^{\Delta'}$ *such that*

- *Over a finite abelian extension of* L, $Y\cong X\otimes_{O_E}O_{E'}$*; so,* $E'=\mathrm{End}_{E'}(Y_{/\overline{\mathbb{Q}}})$*;*
- $\mathrm{End}_{E'}(Y_{/L'})=E'$ *and* $\mu_\sigma\otimes 1:\sigma(Y)\to Y$ *is rational over* L' *for all* $\sigma\in\Delta''$*;*
- $Ob_{L'}(Y)$ *is commutative.*

We do not prove this technical lemma (see [H] Lemma 11). When X is an elliptic curve defined over a quadratic extension $L'/\mathbb{Q}$ with an isogeny $\sigma(X)\xrightarrow{\mu}X$ for the non-trivial automorphism σ of L', $Ob(X)$ is non-commutative if μ is not defined over L'. As we have done in the previous lecture, twisting by a character η of $G_{L'}$, we can make $Ob(X\otimes\eta)$ commutative. The proof of the above lemma is a generalization of this argument. By the above lemma, we may assume that $Ob_L(X)$ commutative without losing much generality. In the rest of my talk, I assume that

$$Ob_L(X) \text{ is commutative.}$$

Proposition 2.5. *Choose a base* $\{\delta_1,\dots,\delta_r\}$ *of* Δ*, and write* $c_i=c(\delta_i,\delta_i)\in E$*. Then we have*

$$\mathrm{End}_E^{\mathbb{Q}}((\mathrm{Res}_{L/F}X)_{/F})\cong E[X_1,\dots,X_r]/(X_1^2-c_1,\dots,X_r^2-c_r)$$

via $\mu_{\delta_i}\mapsto\sqrt{c_i}$.

Proof. Write the algebra at right-hand-side as D. Since $\mu_\sigma\mu_\sigma=c(\sigma,\sigma)\mu_{\sigma^2}$, from $\sigma^2=1$, we conclude $\mu_\sigma^2=c(\sigma,\sigma)$. By the commutativity of $Ob_L(X)$, we have an E–algebra homomorphism from D taking X_i to μ_{δ_i} in $\mathrm{End}_E^{\mathbb{Q}}((\mathrm{Res}_{L/F}X)_{/F})$. Comparing the dimension over E, we conclude the isomorphism. □

In the third lecture, we will prove that for each odd prime $\mathfrak{q}$ dividing c_i as above, the action on $X[\mathfrak{q}]$ on G_L is reducible, giving rise to a character $\xi:G_L\to\mathbb{F}_{N(\mathfrak{q})}^\times$. Often, for example, either if X has good reduction at q (residual characteristic of q) or L is real, the G_F acts on $(\mathrm{Res}_{L/F}X)[\mathfrak{p}]$ through an irreducible induced representation; so, we have the modularity of $\mathrm{Res}_{L/F}X$ if F is totally real under some assumption on X (or ξ).

3. Lecture 3

In this third lecture, we interpret the determination of the endomorphism algebra of an F–AVRM in terms of the Galois representations of the F–AVRM. Then we shall give a sufficient condition for modularity when $F = \mathbb{Q}$. At the end of this lecture, we see that all factors of modular jacobians are made of $\mathbb{Q}$–AVRM's.

3.1. **Extension of Galois representations.** For each $\delta \in \Delta = \mathrm{Gal}(L/F)$, we fix an extension of δ to $\overline{\mathbb{Q}}$, still written as $\delta \in G_F$. Let A be a discrete valuation ring finite flat over $\mathbb{Z}_p$. Let $V = A^2$ be a continuous $A[H]$–module for $H = \mathrm{Gal}(\overline{\mathbb{Q}}/L)$ whose ramification is restricted to a finite set. Writing ρ_H for the Galois representation on V, we suppose

(I0) $V = V(\rho_H)$ is cyclic over $A[H]$;
(I1) ρ_H is absolutely irreducible over the quotient field of A;
(I2) We have an A–linear endomorphism $T_\delta : V \to V$ such that

$$T_\delta(hx) = \delta h \delta^{-1} T_\delta(x) \quad \text{and} \quad \det T_\delta \neq 0.$$

We then define $T_{h\delta} = hT_\delta$ for $h \in H$. It is easy to check the property (I2) for $T_{h\delta}$ and $h\delta$ in place of T_δ and δ. Dividing T_δ by an element of A, we may assume that $\overline{T}_\delta = (T_\delta \mod \mathfrak{m}_A) \neq 0$ for the maximal ideal $\mathfrak{m}_A$ of A.

We consider $W = A[G] \otimes_{A[H]} V$ for $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, which is again cyclic. We see from (I2),

$$\left(\rho_H(\delta^{-2}) T_\delta^2\right)(hx) = h\left(\rho_H(\delta^{-2}) T_\delta^2\right)(x).$$

The operator $\widetilde{T}_\sigma : W \to W$ given by $\widetilde{T}_\sigma(\delta \otimes v) = \delta\sigma^{-1} \otimes T_\sigma(v)$ is firstly well-defined and secondly commutes with the action of H. To see well-definedness, we have, for $h \in H$

$$(h\sigma)^{-1} \otimes T_{h\sigma}(v) = \sigma^{-1} \otimes h^{-1} T_{h\sigma} = \sigma^{-1} \otimes T_\sigma,$$

because $hT_\sigma = T_{h\sigma}$. In particular, $\widetilde{T}_\sigma$ only depends on the restriction of σ to L. The commutativity of T_σ with the multiplication by $g \in G$ from the left is obvious, because we have multiplied δ by σ from the right. The commutativity of T_σ and T_τ is more subtle. Since $T_\sigma T_\tau$ has the same effect as $T_{\sigma\tau}$, by Schur's lemma, we get $c(\sigma, \tau) \in A$ such that $T_\sigma T_\tau = c(\sigma, \tau) T_{\sigma\tau}$. If this obstruction cocycle is commutative, the commutativity between $\widetilde{T}_\delta$ with $\delta \in G$ follows from the following computation:

$$\widetilde{T}_\tau \widetilde{T}_\sigma(\delta \otimes v) = \delta\sigma^{-1}\tau^{-1} \otimes T_\tau T_\sigma(v) = \delta(\tau\sigma)^{-1} \otimes T_\tau T_\sigma(v) = c(\tau, \sigma) \widetilde{T}_{\tau\sigma}(v).$$

We quote the following fact:

Lemma 3.1. *Suppose that $\rho_H \mod \mathfrak{m}_A = \xi \oplus \eta$. For a subgroup $\Delta' \subset \Delta$, ξ is invariant under Δ' and $T_\sigma \mod \mathfrak{m}_A$ ($\sigma \in \Delta'$) takes isomorphically the ξ–eigenspace to ξ–eigenspace, then ξ extends to a character of $H' = \mathrm{Gal}(\overline{\mathbb{Q}}/L^{\Delta'})$ into $\mathbb{F}^\times$ for $\mathbb{F} = A/\mathfrak{m}_A$.*

We would like to apply the above argument to the Galois representation arising from $\mathbb{Q}$–AVRM $(X, \mu_\delta)_{\delta \in \Delta}$ with a totally real field $E = \mathrm{End}_E(X_{/\overline{\mathbb{Q}}})$.

First we choose a prime ideal $\mathfrak{p}$ of E with odd residual characteristic p, put $A = O_{E,\mathfrak{p}}$. Take an A–lattice V stable in the $\mathfrak{p}$–adic Tate module $\varprojlim_n X[\mathfrak{p}^n]$ stable under G_L. Let S be the set of rational primes at which the Galois representation on V ramifies. We add p to S; thus $p \in S$.

Suppose (I0-1) for this choice of H. The condition (I1) is automatic if M is associated to H_1 of an abelian variety, by the solution of the Tate conjecture for abelian varieties by Faltings. If a similar conjecture holds for motives, (I1) follows from it. We can achieve (I0), replacing V by $A[H]v$ for $0 \neq v \in V$ under (I1).

For each $\delta \in \Delta$, we then define $T_\delta(v) = \mu_\delta(\delta(v))$. The pair (V, T_δ) satisfies (I0-2). Multiplying T_δ by scalar in $Frac(A) = E_\mathfrak{p}$, we may assume that $\overline{T}_\delta = T_\delta \mod \mathfrak{m}_A$ is non-zero. The obstruction cocycle $c(\sigma, \tau)$ given by $T_\sigma T_\tau = c(\sigma, \tau) T_\sigma \tau$ under this normalization is called the obstruction cocycle *normalized* at $\mathfrak{p}$. Let

$$W = A[G] \otimes_{A[H]} V = \bigoplus_{\delta \in \Delta} \delta \otimes V.$$

By (I0), $W = A[G]v$ for $v \in V$. Write $\rho_G(\sigma)$ for the action of $\sigma \in G$ on W as an A–linear operator. Choosing $\delta \in G$ inducing the original δ on L, we define $\widetilde{T}_\sigma(\delta \otimes v) = \delta\sigma^{-1} \otimes T_\sigma$.

Theorem 3.2. *Let the assumption and the notation be as above. Let $\delta_1, \dots, \delta_r$ be a minimal set of generators of $\Delta = \mathrm{Gal}(L/\mathbb{Q})$, and write $c_\delta \in A$ for $\widetilde{T}_\delta^2$ (that is, c_δ is the value of $c(\delta, \delta)$ for the obstruction cocycle normalized at $\mathfrak{p}$). In particular, we write c_j for c_{δ_j}. Then we have*

1. *$B = \mathrm{End}_{A[G]}(W) \cong A[X_1, \dots, X_r]/(X_1^2 - c_1, \dots, X_r^2 - c_r)$ via $\widetilde{T}_{\delta_j} \leftrightarrow X_j$.*
2. *W is free of rank 2 over B; so, we write $\rho_G : G \to GL_2(B)$ for the Galois representation on W.*
3. *If $c_\delta \in \mathfrak{m}_A$ for one $\delta \in \Delta$, $V/\mathfrak{m}_A V$ has a unique one dimensional subspace stable under H on which H acts by a character ξ. If $\xi \neq \xi^\delta$, then ξ extends to a character ξ' of a subgroup $H' \supset H$ of index two in G and for a unique maximal ideal $\mathfrak{m}$ of B, $W/\mathfrak{m}W$ is isomorphic to the absolutely irreducible representation $\mathrm{Ind}_{H'}^G \xi'$.*

Proof. The proof of (1) and (2) is similar (but more technical than) the case of $\mathrm{End}_E^{\mathbb{Q}}(\mathrm{Res}_{L/\mathbb{Q}})$; so, we omit it (see [H] Theorem 24). We only give a proof of (3). By the same argument in the first lecture, $c_\delta \in \mathfrak{m}_A$ implies that the semi-simplification $(V/\mathfrak{m}_A V)^{ss}$ of $V/\mathfrak{m}_A W$ is isomorphic to $\xi \oplus \xi^\delta$. Then we find a maximal ideal $\mathfrak{m} \subset B$ such that $(W/\mathfrak{m}W)^{ss} \cong \xi \oplus \xi^\delta$.

Since $\xi \neq \xi^\delta$, the stabilizer Δ' of ξ in Δ is of index 2 in Δ. If $\overline{T}_\sigma$ for $\sigma \in \Delta'$ is nilpotent, it takes ξ^δ–eigenspace to ξ–eigenspace (because it is upper triangular and nilpotent), which is impossible by $\xi^\sigma = \xi \neq \xi^\delta$. This implies that $\overline{T}_\sigma$ is invertible. Since $\overline{T}_\sigma$ for $\sigma \in \Delta'$ brings ξ–eigenspace to ξ–eigenspace, ξ extends to a character $\xi' : H' = \mathrm{Gal}(\overline{\mathbb{Q}}/L') \to \mathbb{F}^\times$ for $L' = L^{\Delta'}$. Since ${\xi'}^\delta \neq \xi'$, $W/\mathfrak{m}W \cong \mathrm{Ind}_{H'}^G \xi'$, which is absolutely irreducible. □

3.2. **Modularity of $\mathbb{Q}$–AVRM.** Let $(X, \mu_\sigma)_{/L}$ be a $\mathbb{Q}$–AVRM with commutative $Ob_L(X)$, where $L/\mathbb{Q}$ is a composite of finitely many quadratic extension. Ribet proved that Serre's conjecture on the modularity of 2-dim mod p Galois representations imply the modularity of $Y = \mathrm{Res}_{L/\mathbb{Q}}X$, that is, Y appears as factors of jacobian $J_1(N)$ for a suitable N. Here we try to deduce modularity, using the known modularity of induced representations. For an elliptic $\mathbb{Q}$–curve X, J. Ellenberg and C. Skinner proved modularity assuming semi-stability of reduction of X at 3 (and some ramification condition at 3 of L).

We first suppose that X is an elliptic $\mathbb{Q}$–curve.

Corollary 3.3. *Suppose that either $Ob_L(X)$ vanishes in $H^2(\Delta, \mathbb{Q}^\times/\mathbb{Z}^\times)$ or does not vanish in $H^2(\Delta, \mathbb{Q}^\times/\mathbb{Z}\left[\frac{1}{6}\right]^\times)$. Then if X is semi-stable over L, X is modular.*

If we can ease irreducibility assumption of Wiles-Taylor-Diamond theorem to irreducibility over $\mathbb{Q}$, we can change 6 to 2 in the above statement, and the semi-stability assumption can be removed if L is real. This seems likely by a work of Skinner-Wiles.

Proof. It is easy to see that if $Ob(X)$ vanishes in $\mathbb{Q}^\times/\mathbb{Z}^\times$, then we can find μ_σ, which are isomorphisms (because $\mu_\sigma \circ {}^\sigma\mu_\sigma = \pm\mu_1 = \pm 1$). Then it is well known that X has a model over $\mathbb{Q}$. By the solution of the Shimura-Taniyama conjecture (by Breuil-Conrad-Diamond- Taylor), X is modular.

We suppose that $Ob(X)$ is non-trivial in $H^2(\Delta, \mathbb{Q}^\times/\mathbb{Z}\left[\frac{1}{6}\right]^\times)$. Then there exists an odd prime $p \geq 5$ such that $5|c_\delta$ for an element $\delta \in \Delta$. Thus for the p–adic Tate module V, $(V/pV)^{ss} = \xi \oplus \xi^\delta$. By semi-stability, for a prime $\mathfrak{p}|p$, ξ is unramified at $\mathfrak{p}$ and ξ ramifies. Then it is easy to verify the irreducibility of $\mathrm{Ind}_{H'}^G \xi'$ over $\mathbb{Q}(\mu_p)$ if $p \geq 5$ (see [H] Proposition 10). Then Wiles-Taylor-Diamond theorem shows the result. □

By the above proof, if X has semi-stable reduction at p as in the proof, it is modular.

For a general $\mathbb{Q}$–AVRM, we have the following result:

Corollary 3.4. *Suppose that $Ob(X)$ does not vanish in $H^2(\Delta, E_\mathfrak{p}^\times/O_{E,\mathfrak{p}}^\times)$ for a prime $\mathfrak{p}$ of E with residual characteristic $p \geq 5$. Then if X has semi-stable or ordinary reduction at p over L, X is modular.*

Since the proof is similar to that of Corollary 3.3, we leave it to the audience.

3.3. **Factors of Modular Jacobians.** Let $f \in S_2(\Gamma_0(D),\chi)$ be a Hecke eigenform for a primitive quadratic character χ modulo D. Let Y be the abelian variety in $J_1(D)$ associated to f. Writing $F = \mathbb{Q}(f)$ for the field generated by Hecke eigenvalues for f, we have $F \subset \mathrm{End}^{\mathbb{Q}}(Y_{/\mathbb{Q}})$. Since $[F:\mathbb{Q}] = \dim Y$, $H^0(Y,\Omega_{Y/\mathbb{Q}})$ is one dimensional vector space over F. Since $\mathrm{End}^{\mathbb{Q}}_F(Y_{/\mathbb{Q}}) \subset \mathrm{End}_F(H^0(X,\Omega_{Y/\mathbb{Q}}))$, we see $\mathrm{End}^{\mathbb{Q}}_F(Y_{/\mathbb{Q}}) = F$. Since any $\theta \in \mathrm{End}^{\mathbb{Q}}(Y_{/\mathbb{Q}})$ commutes with Frobenius map ϕ on $Y \mod p$, it commutes with $T(p) = \phi + \chi(p)\phi^*$ by congruence relation. Thus $\theta \in \mathrm{End}^{\mathbb{Q}}_F(X_{/\mathbb{Q}}) = F$, and $\mathrm{End}^{\mathbb{Q}}(X_{/\mathbb{Q}}) = F$. We get

$$Y \text{ is a } \mathbb{Q}\text{–simple factor of } J_1(N). \tag{3.1}$$

Thus Taniyama's problem on $\mathbb{Q}$–simple factors (in our setting) is equivalent to:

Decompose the Hecke algebra of $S_2(\Gamma_0(D),\chi)$ over $\mathbb{Q}$ into simple factors,

where the Hecke algebra, denoted by $h_k(N,\chi;\mathbb{Q})$, is the subalgebra of the linear endomorphism algebra $\mathrm{End}_{\mathbb{C}}(S_k(\Gamma_0(N),\chi))$ generated over $\mathbb{Q}$ by Hecke operators $T(n)$.

For simplicity, we assume that D is square-free (so, it is odd). Let $L/\mathbb{Q}$ be the $(2,2,\dots,2)$–extension generated by $\sqrt{m^*}$ for $m^* = (-1)^{(m-1)/2}m$ for all factors m of D, and write $\Delta = \mathrm{Gal}(L/\mathbb{Q})$. Let $\mathcal{N}(\Gamma_0(D))$ be the normalizer of $\Gamma_0(D)$ in $GL_2^+(\mathbb{Q}) = \{\gamma \in GL_2(\mathbb{Q}) | \det\gamma > 0\}$. Then $\widehat{\Delta} = \mathrm{Hom}(\Delta,\{\pm 1\})$ is canonically isomorphic to $\mathcal{N}(\Gamma_0(D))/\Gamma_0(D)\mathbb{Q}^\times$ by

$$\mathcal{N}(\Gamma_0(D))/\Gamma_0(D) \ni \gamma \mapsto \left(\frac{\mathbb{Q}[\sqrt{\det(\gamma)^*}]}{}\right) \in \widehat{\Delta},$$

where γ is chosen so that $\det(\gamma)$ is a square-free integer (and $\det(\gamma)^*$ is defined like m^*). Thus $\widehat{\Delta}$ acts on $S_2(\Gamma_0(D),\chi)$ by $f \mapsto f|\gamma$, and for n prime to D, $\gamma \circ T(n) = \gamma(n)T(n)\circ\gamma$, thus as an endomorphism of the jacobian, we have $\gamma^\sigma = \gamma(\sigma)\gamma$. Let $Z = \sum_{\alpha\in\widehat{\Delta}} \alpha(Y) \subset J_1(D)$. The following fact is known:

Theorem 3.5. *Suppose that $\mathrm{End}^{\mathbb{Q}}_F(Y_{/\overline{\mathbb{Q}}}) = F$. Then the subfield E generated by $T(n)$ for n with $\gamma(n) = 1$ for all $\gamma \in \widehat{\Delta}$ is totally real, and there exists a $\mathbb{Q}$–AVRM (X,μ_σ) defined over L such that Z is isogenous over $\mathbb{Q}$ to $\mathrm{Res}_{L/\mathbb{Q}}X$. The $\mathbb{Q}$–AVRM X has everywhere good reduction over L.*

Proof. We give a sketch of a proof. This fact is basically due to Ribet and Shimura. We consider the action of $\chi \in \widehat{\Delta}$, which is the action of $\left(\begin{smallmatrix} 0 & -1 \\ D & 0\end{smallmatrix}\right)$ and is the complex conjugation c on F. The fixed subfield F_+ of F by c is totally real, and $Y = Y_+ + c(Y_+)$ for $Y_+ = (\chi-1)(Y)$, which is an $\mathbb{Q}$–AVRM defined over $\mathbb{Q}[\sqrt{D}]$. As we have already seen, all endomorphisms of Y_+ is defined over a $(2,2,\dots,2)$–extension of $\mathbb{Q}[\sqrt{D}]$. If Y has good reduction at a prime $\mathfrak{p}$ of L, $\mathrm{End}(Y) \subset \mathrm{End}(Y \mod \mathfrak{p})$ is defined over an extension unramified at $\mathfrak{p}$; so, it is defined over $(2,2,\dots,2)$–extension $L' \supset L$ of $\mathbb{Q}[\sqrt{D}]$ unramified everywhere over L, since Y has everywhere good reduction over L. Such a field coincides with L if D is odd by the theory of ambiguous classes. Thus $\mathrm{End}^{\mathbb{Q}}(Y_{/L})$ is a product of mutually isogenous simple factors: $Y \sim \prod_{\delta\in\Delta}\delta(X)$, where '$\sim$' indicates an isogeny. By congruence relation, every endomorphism of $X_{/L}$ commutes with E. Since $H^0(X,\Omega_{X/L})$ is free of rank 1 over $L\otimes_{\mathbb{Q}} E$, we conclude that $\mathrm{End}^{\mathbb{Q}}_E(X_{/L}) = \mathrm{End}^{\mathbb{Q}}(X_{/L}) = E$. Thus X is an absolutely simple $\mathbb{Q}$–AVRM. □

Let (X,μ_σ) be an absolutely simple $\mathbb{Q}$–AVRM defined over a composite of quadratic extensions $L/\mathbb{Q}$ unramified at 2. Suppose that $Ob_L(X)$ is commutative and that $X_{/L}$ has everywhere good reduction. For simplicity, we assume that $F = \mathrm{End}^{\mathbb{Q}}(\mathrm{Res}_{L/\mathbb{Q}}X)$ is a field. There is a unique maximally ramified quadratic extension $L'/\mathbb{Q}$ such that L/L' is unramified outside ∞, and $\mathrm{Res}_{L/L'}X = \mathrm{Res}_{O_L/O_{L'}}X$ has everywhere good reduction. The determinant character of $\mathfrak{l}$–adic representation is then $\varepsilon\nu_\ell$ for the cyclotomic character ν_ℓ and at most quadratic character ε. The criterion of Neron-Ogg-Shafarevich tells us that ε is unramified outside ramification prime of $L/\mathbb{Q}$ (for a prime $\mathfrak{l}$ of F). By a result of Ribet-Serre and Faltings, one expects that the Galois representation on $\mathfrak{l}$–torsion points $X[\mathfrak{l}]$ contains $SL_2(O_E/\mathfrak{l})$ for almost all primes $\mathfrak{l}$; so, ε is unramified over L' and is really ramified at primes of ramification of ε. Thus ε is a quadratic character of $L'/\mathbb{Q}$. It is known that ε is an even character, and L' is a real quadratic field.

Conjecture 3.6. *Let $L/\mathbb{Q}$ be a $(2,2,\ldots,2)$–extension unramified at 2. Suppose that $\mathbb{Q}$–AVRM $X_{/L}$ with commutative $Ob_L(X)$ has everywhere good reduction and that L is minimal among $(2,2,\ldots,2)$–extensions with such property. Then for the quadratic character χ ramified exactly at ramification primes of $L/\mathbb{Q}$, $\mathrm{Res}_{L/\mathbb{Q}}X$ is $\mathbb{Q}$–isogenous to a factor of $J_1(D)$ associated to a Hecke eigenform $f \in S_2(\Gamma_0(D),\chi)$ for the conductor D of χ.*

4. Lecture 4

4.1. **F–Modularity.** Let F be a totally real field and $\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to GL_2(\mathbb{F})$ for a field $\mathbb{F}$ of characteristic $p > 2$ be a representation unramified outside a finite set S of prime ideals prime to p in F. Write $D_{\mathfrak{q}} \subset \mathrm{Gal}(\overline{\mathbb{Q}}/F)$ for the decomposition group of a prime $\mathfrak{q}$ of F. We assume

(r0) $\overline{\rho}$ is absolutely irreducible over $F(\mu_p)$;
(r1) $\overline{\rho}|_{D_{\mathfrak{q}}} \cong \begin{pmatrix} \overline{\varepsilon}_{\mathfrak{q}} & * \\ 0 & \overline{\delta}_{\mathfrak{q}} \end{pmatrix}$ for all $\mathfrak{q} \in S \cup \{\mathfrak{p}|p\}$ with $\overline{\delta}_{\mathfrak{q}}$ unramified;
(r2) $\overline{\varepsilon}_{\mathfrak{q}} \neq \overline{\delta}_{\mathfrak{q}}$ on the inertia group $I_{\mathfrak{q}}$;
(r3) $\overline{\rho}$ is optimally modular, that is, there exists a Hilbert modular form of optimal level (that is, if $\overline{\rho}$ is flat at p, its level is the product C of conductors $C(\varepsilon_{\mathfrak{q}})$ for $\mathfrak{q} \in S$ and if $\overline{\rho}$ is not flat, its level is $C\prod_{\mathfrak{p}|p}\mathfrak{p}$).

Let $\mathcal{O}$ be a valuation ring finite flat over $\mathbb{Z}_p$. We take a p–ordinary deformation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to GL_2(\mathcal{O})$ unramified outside $S \cup \{\mathfrak{p}|p\}$; thus we suppose the F–version of Ordinarity at p. We further suppose that

(R1) $\rho|_{I_{\mathfrak{q}}} \cong \begin{pmatrix} \varepsilon_{\mathfrak{q}} & * \\ 0 & \delta_{\mathfrak{q}} \end{pmatrix}$ for the Teichmüller lifts $\delta_{\mathfrak{q}}$ and $\varepsilon_{\mathfrak{q}}$ of $\overline{\delta}_{\mathfrak{q}}$ and $\overline{\varepsilon}_{\mathfrak{p}}$ for all $\mathfrak{q} \in S$.

We have the following partial generalization of Wiles' result in the Hilbert modular case:

Theorem 4.1 (K. Fujiwara)**.** *Assume that $F/\mathbb{Q}$ is unramified at p if $\overline{\rho}$ is flat. If $\det\rho$ is equal to ν_p^{k-1} ($k \geq 2$) up to finite order character for the p–adic cyclotomic character ν_p, then ρ is optimally F–modular.*

Here ρ is called *F–modular*, if it is associated to a Hilbert modular form f of optimal level (that is, $L(s,f) = L(s,\rho)$). Actually Fujiwara's result is more general including the multiple weight case and the flat non-p-ordinary case.

Corollary 4.2. *Let $(X,\mu_\sigma)_{/L}$ be a F–AVRM with commutative $Ob_L(X)$, where L/F is a composite of finitely many quadratic extension. Suppose that L is unramified at p and X has everywhere good reduction. If the image of $Ob(X)$ in $H^2(\mathrm{Gal}(L/F), E_{\mathfrak{p}}^{\times}/O_{\mathfrak{p}}^{\times})$ is non-trivial for $\mathfrak{p}|p \geq 5$, then the L–function of $\mathrm{Res}_{L/F}X$ is associated to a Hilbert modular form for F.*

4.2. **Base-Change.** We start with an eigenform $f \in S_2(\Gamma_0(p),\psi)$ for an odd prime p. Define $\lambda(T(n)) \in \overline{\mathbb{Q}}$ by $f|T(n) = \lambda(T(n))f$, and write $\mathbb{Q}[\lambda]$ for the field generated by $\lambda(T(n))$ for all n. Pick a prime $\mathfrak{q}$ of $\mathbb{Q}[\lambda]$ and consider the $\mathfrak{q}$–adic Galois representation $\rho_{\lambda,\mathfrak{q}}$ of f acting on two dimensional $\mathfrak{q}$–adic vector space V. This Galois representation is unramified outside pq for the residual characteristic q of $\mathfrak{q}$ and has the characteristic polynomial $\det(1-\rho_{\lambda,\mathfrak{q}}(\mathrm{Frob}_\ell)|_{V^{I(\ell)}}X)$ independent of $\mathfrak{q}$ as long as $\ell \notin \mathfrak{q}$, where $I(\ell)$ is the inertia group of the prime ℓ.

The L–function $L(s,\lambda) = \sum_{n=1}^{n} \lambda(T(n))n^{-s}$ has Euler product expansion, which coincides with the Euler product of the system $\rho_\lambda = \{\rho_{\lambda,\mathfrak{q}}\}_{\mathfrak{q}}$ of Galois representations:

$$L(s,\rho_\lambda) = \prod_{\ell} \det(1-\rho_{\lambda,\mathfrak{q}}(Frob_\ell)|_{V^{I(\ell)}}\ell^{-s})^{-1},$$

where we always choose the prime $\mathfrak{q}$ outside ℓ to have well-defined Euler factor $\det(1-\rho_{\lambda,\mathfrak{q}}(Frob_\ell)|_{V^{I(\ell)}}\ell^{-s})^{-1}$. For a given number field $F \subset \overline{\mathbb{Q}}$, we can think of the Euler product

$$L(s,\rho_\lambda|_{\mathrm{Gal}(\overline{\mathbb{Q}}/F)}) = \prod_{\mathfrak{l}} \det\left(1-\rho_{\lambda,\mathfrak{q}}(\mathrm{Frob}_{\mathfrak{l}})|_{V^{I(\mathfrak{l})}}N(\mathfrak{l})^{-s}\right)^{-1}.$$

Here $\mathfrak{l}$ runs over all prime ideals of F. Multiplying out, we can expand the Euler product $L(s,\rho_\lambda|_{\mathrm{Gal}(\overline{\mathbb{Q}}/F)})$ into a Dirichlet series

$$L(s,\rho_\lambda|_{\mathrm{Gal}(\overline{\mathbb{Q}}/F)}) = L(s,\widehat{\lambda}) = \sum_{\mathfrak{n}} \widehat{\lambda}(T(\mathfrak{n}))N(\mathfrak{n})^{-s}.$$

Numbers $\widehat{\lambda}(\mathfrak{n})$ are well-defined for integral ideals $\mathfrak{n}$ of F. If there exists a cusp form $\widehat{f} : GL_2(F)\backslash GL_2(F_{\mathbb{A}}) \to \mathbb{C}$ such that $\widehat{f}|T(\mathfrak{n}) = \widehat{\lambda}(T(\mathfrak{n}))\widehat{f}$, the cusp form $\widehat{f}$ is called the base-change of f to F.

Since the Hecke eigenvalue $\widehat{\lambda}(T(\mathfrak{n}))$ is derived from $\lambda(T(n))$ in a purely arithmetic way, finding $\widehat{f}$ is a highly non-trivial question. This type of problem was first considered by Doi and Naganuma

in the late 60's and the existence of $\widehat{f}$ was proved in the late 70's by Langlands for prime cyclic extensions $F/\mathbb{Q}$ as long as the restriction of ρ_λ to $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ remains irreducible. In any case, the problem remains open for non-soluble or non-Galois extensions $F/\mathbb{Q}$.

4.3. **Speculation.** We study here the problem of base-change for a Hecke eigenform $f \in S_k(\Gamma_0(N), \psi)$ for $k \geq 2$. We call f *liftable* if there is a finite set of places S_f (including ∞) such that f has a base-change to F if $F/\mathbb{Q}$ is unramified at S_f.

The most significant assumption of Fujiwara's theorem is the optimal modularity of $\overline{\rho}$, and other conditions seem likely to be removed in coming years. We start our speculation by supposing that Fujiwara's result holds only assuming F–modularity of $\overline{\rho}$:

Starting with f, try to find a sequence of Hecke eigenforms $f_j \in S_{k_j}(\Gamma_0(N_j), \psi_j)$ for a suitable level N_j such that $f_j \equiv f_{j-1}^{\sigma_j} \mod \mathfrak{l}_j$ for $\sigma_j \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and for a prime $\mathfrak{l}_j$ of $\overline{\mathbb{Q}}$ dividing an odd prime ℓ_j. We write $f \sim f_j$ if such a sequence of congruence (and Galois conjugation) exists.

If we can find (optimally) liftable f_j, then applying Fujiwara's theorem to the prime ℓ_j in place of p and $\overline{\rho}$ associated to the base-change lift $\widehat{f_j}$ of f_j, f_{j-1} is (optimally) liftable, because the ℓ_j–adic Galois representation of f_j restricted to $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ is a deformation of $\overline{\rho}$. Applying the above argument for ℓ_{j-1} in place of p to f_{j-2} and the base-change $\widehat{f}_{j-1}$, f_{j-2} would be liftable to F, and so on, getting eventually the liftability of f by induction.

However at the present state of knowledge, to make the above argument work, we need to assume the following four conditions on $\chi = \chi_j$, $\ell = \ell_j$, $\mathfrak{l} = \mathfrak{l}_j$ and $\phi = f_j$ for all j:

(1) ϕ is $\mathfrak{l}$-ordinary;
(2) The Galois representation $\overline{\rho}_{\mathfrak{l},\phi}$ of ϕ modulo $\mathfrak{l}$ is absolutely irreducible as a representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mu_\ell)$);
(3) ℓ is odd and is unramified in $F/\mathbb{Q}$;
(4) χ has conductor equal to the level of ϕ and has order prime to ℓ.

The last assumption guarantees that the base-change if exists it has minimal level.

Proposition 4.3. *If we can remove the above four conditions on ℓ, then every modular form is liftable.*

Proof. By a theory of p–adic modular forms, for a given f, we can always find g such that $f \equiv g \mod \mathfrak{p}$. Thus we may assume that f is of weight 2. Take sufficiently large N so that $S_2(\Gamma_1(N))$ contains a liftable form h (for example, theta series). The following argument, proving the connectedness of the spectrum of the Hecke algebra over $\mathbb{Z}$ for $S_2(\Gamma_1(N))$, is due to B. Mazur: Let Σ be the system of eigenvalues of $T(n)$ (for n prime to N). If we can separate $\Sigma = \Sigma_1 \sqcup \Sigma_2$ so that (i) Σ_j is Galois stable and (ii) there is no congruences between eigenvalues in Σ_1 and Σ_2. Then we can split $J_1(N) = A \times B$ for abelian subvarieties A and B. Then the polarization divisor Θ has to be algebraically equivalent to $A \times D \cup D' \times B$ for divisors D and D'. It is well known the algebraic equivalence class of a theta divisor is made of irreducible degree 1 divisors; so, this is impossible. Thus we find a sequence f_j such that $f \sim f_1 \sim f_2 \sim \cdots \sim f_j \sim h$;so, f is liftable. □

Suppose that $f \in S_\kappa(\Gamma_0(N), \psi)$ is $\mathfrak{p}$–ordinary for a prime $\mathfrak{p}$ of $\overline{\mathbb{Q}}$, that is, for a prime $\mathfrak{p}$ of $\overline{\mathbb{Q}}$, a_p with $f|T(p) = a_p f$ is a $\mathfrak{p}$–adic unit. Then we can include f_κ in the $\mathfrak{p}$–adic family of modular forms $\{f_{k,\varepsilon}\}_{k\geq 2,\varepsilon}$ such that $f_k \equiv f_\kappa \mod \mathfrak{p}$ and $f_{k,\varepsilon} \in S_k(\Gamma_0(Np), \psi\varepsilon\omega_p^{\kappa-k})$ (see [H] Section 7.5 and Section 2). Here ε runs over all finite order characters of $1 + p\mathbb{Z}_p$ regarded as Dirichlet characters. Thus if f is liftable, then $f_{k,\varepsilon}$ is liftable. Pick any prime $\mathfrak{q}$ for which $f_{k,\varepsilon}$ is $\mathfrak{q}$–ordinary, we can include $f_{k,\varepsilon}$ in the $\mathfrak{q}$–adic family of Hecke eigenforms; so, $\{g_{\ell,\eta}\}$ is liftable for all $\ell \geq 2$ and all finite order character η of $1 + q\mathbb{Z}_q$.

Problem 1. *By repeating the above construction, what amount of modular forms can be proven to be liftable.*

The following conjecture might be some help to solve the above question.

Conjecture 4.4 (Ordinarity)**.** *Let f be a Hecke eigenform of weight ≥ 2 without complex multiplication. Then the Dirichlet density of primes q for which f is $\mathfrak{q}$–ordinary for some prime $\mathfrak{q}|q$ of $\overline{\mathbb{Q}}$ is equal to* 1.

This fact is proven by Serre for weight 2 Hecke eigenforms.

Let D be a discriminant of a real quadratic field. Now we prove that the space $S_k(\Gamma_0(D), \chi_D)$ for $\chi_D = \left(\frac{D}{\cdot}\right)$ has a liftable form. For complex conjugation c,

$$f^c|T(n) = \chi(n)\lambda(T(n))f^c \text{ if } f|T(n) = \lambda(T(n))f \text{ and } n \text{ is prime to } D.$$

Thus if $f \equiv f^c \mod \mathfrak{p}$, the mod $\mathfrak{p}$ representation $\overline{\rho}$ associated to f satisfies $\overline{\rho} \cong \overline{\rho} \otimes \chi$; thus, it is residually induced (and irreducible if $\mathfrak{p}$ is prime to p and $k > p$). I proved in Documenta Math. 3 (1998) the following

Proposition 4.5. *Embed $\mathbb{Q}[\sqrt{D}]$ in $\mathbb{R}$, and let u be a positive fundamental unit. For simplicity, suppose that $N(u) = -1$.*

1. *If $\mathfrak{q}$–adic representation is $\mathfrak{q}$–ordinary and residually dihedral non-dihedral and $\mathfrak{q}$ is odd, then $\mathfrak{q}|N(u^{k-1} - 1)$ and $\chi_D(q) = 1$;*
2. *If $q|N(u^{k-1} - 1)$ for an odd prime q with $k \geq 4$ or $q \geq 5$, then there exists a Hecke eigenform $f \in S_k(\Gamma_0(D), \chi_D)$ and a prime $\mathfrak{q}|q$ in $\overline{\mathbb{Q}}$ such that f is $\mathfrak{q}$–ordinary and $\mathfrak{q}$–adic Galois representation of f is residually dihedral non-dihedral.*

The set of odd prime factors of $N(u^{k-1} - 1)$ is non-empty if $k \geq 6$. There exist an odd prime factor of $N(u^{k-1} - 1)$ for all even k if $D \not\equiv 1 \mod 8$ and $D \neq 5$.

Speculation. *For each pair of Hecke eigenforms (f, g) in $S_k(\Gamma_0(D), \chi_D)$, we have $f \sim g$ by ordinary odd primes.*

This of course implies liftability of all elements in $S_k(\Gamma_0(D), \chi_D)$ if $k \geq 6$ (assuming the validity of Fujiwara's result only under F–modularity).

Related to this, there is a conjecture of Maeda:

Conjecture 4.6 (Y. Maeda)**.** *All Hecke eigenforms in $S_k(SL_2(\mathbb{Z}))$ are Galois conjugate each other.*

This conjecture is known to be true for $k \leq 1000$. Assuming this conjecture, one can prove the liftability of level 1 Hecke eigenforms for $k < 107128$.

Example 4.1. We study the liftability of $\Delta \in S_k(SL_2(\mathbb{Z}))$. Δ is p–ordinary for primes p with $p \geq 11$, $p \neq 2411$ and $p \leq 7,196,993$ (according to F. Q. Gouvêa). Use the prime $p = 13$, and take the 13–adic family of modular forms $\{\Delta_k\}_{k \geq 2}$ of Δ, we find $\Delta_6 \in S_6(\Gamma_0(13), \chi_{13})$. In this space, all forms are Galois conjugates (so Speculation holds). The prime $\mathfrak{q}$ for which Δ_6 is residually dihedral is $q = 131$. Thus if $F/\mathbb{Q}$ is unramified at 13 and 131, one can check from Fujiwara's theorem that Δ and Δ_k has base-change for F. For this, we used the fact that the image of mod p representation of Δ contains $SL_2(\mathbb{F}_p)$ if $p \notin \{3, 5, 7, 23, 691\}$ (due to Serre and Swinnerton-Dyer).

Similar argument shows that: all $f \in S_k(SL_2(\mathbb{Z}))$ is liftable for $k \leq 1000$. For more details, see my paper with Maeda in Pacific Journal in 1997.

Here is plain consequence of the validity of our speculations:

- Conjecture 4.4 and Speculation imply liftability of all level 1 Hecke eigenform;
- Conjectures 4.4 and 4.6 also imply the liftability of all Hecke eigenforms of level 1.

Since level 1 forms are dense in the space of p–adic modular forms of level p^∞, liftability without exceptional primes of level 1 forms would imply liftability of all p–power level forms (as p–adic modular forms).

‘

References

[H] H. Hida, Control Theorems and Applications, Lectures at Tata Institute of Fundamental Research, Mumbay, 1999 (posted at `http://www.math.tifr.res.in/~eghate/math.html`).

[H00a] H. Hida, *Modular Forms and Galois Cohomology*, Cambridge University Press, Cambridge, England 2000

[H00b] H. Hida, *Geometric Modular Forms and Elliptic Curves*, World Scientific Publishing Company, Singapore, 2000