Fermat's Last Theorem

Modular Forms and Galois Representations

Leonardo Colò

March 7^{th}, 2017

Group Representations

Definition. A linear representation ρ of a group G on a K-vector space V is a set-theoretic action on V which preserves the linear structure, that is,

$$\rho(g)(v_1 + v_2) = \rho(g)v_1 + \rho(g)v_2 \qquad \forall\ v_1, v_2 \in V$$
$$\rho(g)(k \cdot v) = k \cdot \rho(g)v \qquad \forall\ k \in K,\ v \in V$$

up to automorphisms of V. Unless otherwise mentioned, representation will mean finite-dimensional representation. We will call dimension of ρ (sometimes degree or rank of ρ) the dimension of V as K-vector space.

Definition. A representation ρ of a group G is a group homomorphism

$$\rho : G \longrightarrow GL_n(K)$$

up to conjugation. We call n the dimension of ρ.

Lemma 1.1. *The two definitions above are equivalent.*

Proof. Suppose we are given a homomorphism

$$\rho : G \longrightarrow GL_n(K)$$

then define an action of G on K^n as follows:

$$g * v = \rho(g)v$$

It is easy to check that this action preserves the linear structure of K^n. It can also be shown that if ρ and ρ' are equivalent (i.e., $\rho' = \rho \circ \mathrm{c}$ with c a conjugation) then ρ and ρ' give rise to the same action on K^n up to isomorphisms of K^n.
Viceversa, given an action of G on $V = K^n$ we define a map

$$\rho : G \longrightarrow GL_n(K)$$
$$g \longrightarrow (g * \underline{e}_1, \dots, g * \underline{e}_n)$$

where $\{\underline{e}_1, \dots, \underline{e}_n\}$ is a basis for V. □

Definition. If G is a topological group, a continuous representation ρ of a group G is a continuous homomorphism

$$\rho : G \longrightarrow GL_n(K)$$

where the topology on $GL_n(K)$ is given by the fact that $GL_n(K) \subseteq M_{n\times n}(K)$ is open.
Equivalently, a continuous representation ρ of a group G is a continuous action of G on a K vector space, i.e., a continuous map

$$\rho : G \times V \longrightarrow V$$

which preserves the linear structure.

Galois Representations

We will let $\mathbb{Q}$ denote the field of rational numbers and $\overline{\mathbb{Q}}$ denote the field of algebraic numbers, the algebraic closure of $\mathbb{Q}$. We will also let $\mathcal{G}_{\mathbb{Q}}$ denote the group of automorphisms of $\overline{\mathbb{Q}}$, that is $\mathcal{G}al(\overline{\mathbb{Q}}/\mathbb{Q})$, the absolute Galois group of $\mathbb{Q}$.
An important technical point is that $\mathcal{G}_{\mathbb{Q}}$ is naturally a topological group, a basis of open neighbourhoods of the identity being given by the subgroups $\mathcal{G}al(\overline{\mathbb{Q}}/K)$ as K runs over subextensions of $\overline{\mathbb{Q}}/\mathbb{Q}$ which are finite over $\mathbb{Q}$. In fact, $\mathcal{G}_{\mathbb{Q}}$ is a profinite group, being identified with the inverse limit of discrete groups

$$\mathcal{G}al(\overline{\mathbb{Q}}/\mathbb{Q}) = \lim_{\leftarrow} \mathcal{G}al(K/\mathbb{Q})$$

where K runs over finite normal subextensions of $\overline{\mathbb{Q}}/\mathbb{Q}$.
For each prime number p we may define an absolute value $|\ |_p$ on $\mathbb{Q}$ by setting

$$|\alpha|_p = p^{-r}$$

if $\alpha = p^r a/b$ with a and b integers coprime to p. If we complete $\mathbb{Q}$ with respect to this absolute value we obtain the field $\mathbb{Q}_p$ of p-adic numbers, a totally disconnected, locally compact topological field. We will write $\mathcal{G}_{\mathbb{Q}_p}$ for its absolute Galois group $\mathcal{G}al(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. The absolute value $|\ |_p$ has a unique extension to an absolute value on $\overline{\mathbb{Q}}_p$ and $\mathcal{G}_{\mathbb{Q}_p}$ is identified with the group of automorphisms of $\overline{\mathbb{Q}}_p$ which preserve $|\ |_p$, or, equivalently, the group of continuous automorphisms of $\overline{\mathbb{Q}}_p$. For each embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ we obtain a closed embedding $\mathcal{G}_{\mathbb{Q}_p} \hookrightarrow \mathcal{G}_{\mathbb{Q}}$.
$\overline{\mathbb{Q}}_p/\mathbb{Q}_p$ is an infinite extension and $\overline{\mathbb{Q}}_p$ is not complete. We will denote its completion by $\mathbb{C}_p$. The Galois group $\mathcal{G}_{\mathbb{Q}_p}$ acts on $\mathbb{C}_p$ and is in fact the group of continuous automorphisms of $\mathbb{C}_p$.
The elements of $\mathbb{Q}_p$ (respectively $\overline{\mathbb{Q}}_p$, $\mathbb{C}_p$) with absolute value less than or equal to 1 form a closed subring $\mathbb{Z}_p$ (respectively $\mathcal{O}_{\overline{\mathbb{Q}}_p}$, $\mathcal{O}_{\mathbb{C}_p}$). These rings are local with maximal ideals $p\mathbb{Z}_p$ (respectively $\mathfrak{m}_{\overline{\mathbb{Q}}_p}$, $\mathfrak{m}_{\mathbb{C}_p}$) consisting of the elements with absolute value strictly less than 1. The field

$$\frac{\overline{\mathbb{Q}}_p}{\mathfrak{m}_{\overline{\mathbb{Q}}_p}} = \frac{\mathbb{C}_p}{\mathfrak{m}_{\mathbb{C}_p}}$$

is an algebraic closure of the finite field with p elements

$$\mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$$

and we will denote it by $\overline{\mathbb{F}}_p$. Thus we obtain a continuous map

$$\mathcal{G}_{\mathbb{Q}_p} \longrightarrow \mathcal{G}_{\mathbb{F}_p}$$

which is surjective. Its kernel is called the inertia subgroup of $\mathcal{G}_{\mathbb{Q}_p}$ and is denoted $I_{\mathbb{Q}_p}$. We want to focus here on attempts to describe $\mathcal{G}_{\mathbb{Q}}$ via its representations. Perhaps the most obvious to consider are those representations

$$\mathcal{G}_{\mathbb{Q}} \longrightarrow GL_n(\mathbb{C})$$

with open kernel; these are called Artin representations and they are already very interesting. However one obtains a richer theory considering representations

$$\mathcal{G}_{\mathbb{Q}} \longrightarrow GL_n(\overline{\mathbb{Q}}_l)$$

which are continuous with respect to the l-adic topology on $GL_n(\overline{\mathbb{Q}}_l)$. We refer to these as l-adic representations.

Examples of Representations

Continuous Character

Suppose we have a group G. A one-dimensional continuous representation of G is given by a continuous homomorphism

$$\rho : G \longrightarrow GL_1(K) = K^{\times}$$

or, equivalently, by a continuous action of G on K which preserve the linear structure.
If $K/\mathbb{Q}$ is a finite galois extension and $L/\mathbb{Q}$ is a subextension, then the representation of $\mathcal{G}al(K/\mathbb{Q})$ factors:

$$\begin{array}{ccc} \mathcal{G}al(K/\mathbb{Q}) & \xrightarrow{\rho} & K^{\times} \\ \downarrow \pi & \nearrow & \\ \mathcal{G}al(L/\mathbb{Q}) & Ind_{\mathcal{G}_{K/\mathbb{Q}}}^{\mathcal{G}_{L/\mathbb{Q}}}\rho & \end{array}$$

Cyclotomic Character

Suppose we have a prime $p > 0$ and consider a compatible family of primitive p^n-th roots of unity

$$(\zeta_p, \zeta_{p^2}, \zeta_{p^3}, \dots, \zeta_{p^n}, \dots)$$

where the compatibility is given by the fact that

$$(\zeta_{p^n})^{p^n} = 1 \quad \text{and} \quad (\zeta_{p^n})^p = \zeta_{p^{n-1}}$$

Consider a group G with an action on the set of primitive p^i-th roots of unity such that

$$g * \zeta_{p^n} = \zeta_{p^n}^{a_n} \qquad \text{where } a_n \in \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right)^{\times} \qquad \text{and } a_n \equiv a_{n-1} \mod p^{n-1}$$

then we have a compatible system

$$(a_n)_n \in \varprojlim \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right)^{\times} = \mathbb{Z}_p^{\times}$$

and we can define a continuous homomorphism

$$\begin{aligned} \rho : G \longrightarrow & \mathbb{Z}_p^{\times} \subseteq \mathbb{Q}_p^{\times} \\ g \longrightarrow & (a_n)_n \end{aligned}$$

It can be shown that ρ is a continuous representation.

Representations Associated to an Elliptic Curve

Suppose we have an elliptic curve $E_{/\mathbb{Q}}$ and consider a prime $p > 0$. We define $E[p^n]$ the p^n-torsion group. We have $E[p^n] \subseteq \overline{\mathbb{Q}}$.

$$E[p^n] = \{P \in E(\overline{\mathbb{Q}}) \mid [p^n] \cdot P = 0\}.$$

We have a compatible system where the maps are given by $[p]$, the multiplication by p.

$$E[p] \xleftarrow{[p]} E[p^2] \xleftarrow{[p]} E[p^3] \xleftarrow{[p]} \dots$$

Suppose we have a point $P \equiv (x, y) \in E(\overline{\mathbb{Q}})$ and a group $\mathcal{G} = \mathcal{G}al(\overline{\mathbb{Q}}/\mathbb{Q})$. Then $\mathcal{G}$ acts on $E(\overline{\mathbb{Q}})$ in the following way:

$$g * P = (g(x), g(y)) \in E(\overline{\mathbb{Q}})$$

Furthermore, if $P \in E[p^n]$ then $g * P \in E[p^n]$.

Definition. We define the p-adic Tate module attached to E:

$$T_pE = \varprojlim_n (E[p^n], [p])$$

Clearly there is an action of $\mathcal{G}$ on this Tate module: $\mathcal{G} \circlearrowleft T_pE$

Observation. The key point in this construction is that we have a group law over an elliptic curve.

Proposition 3.1. *We have a group isomorphism*

$$E[n] \simeq \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^2$$

Then we have the following system

$$\begin{array}{ccccccc}
E[p] & \xleftarrow{[p]} & E[p^2] & \xleftarrow{[p]} & E[p^3] & \longleftarrow & \dots \\
\wr\| & & \wr\| & & \wr\| & & \\
\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^2 & \xleftarrow[\pi]{} & \left(\frac{\mathbb{Z}}{p^2\mathbb{Z}}\right)^2 & \xleftarrow[\pi]{} & \left(\frac{\mathbb{Z}}{p^3\mathbb{Z}}\right)^2 & \longleftarrow & \dots
\end{array}$$

where the maps π are the canonical projections. Then we conclude that

$$T_pE = \varprojlim_n (E[p^n], [p]) = \varprojlim \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right)^2 = \mathbb{Z}_p^2$$

It might be convenient to work with

$$V_pE = T_pE \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq \mathbb{Z}_p^2 \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq \mathbb{Q}_p^2$$

and we have an action of $\mathcal{G}$ on V_pE.

Representations Associated to an Abelian Variety

Example. Consider $\mathbb{G}_m$, the multiplicative group. We have

$$\mathbb{G}_m(\overline{\mathbb{Q}}) = \overline{\mathbb{Q}}^\times$$

Then we define

$$\mathbb{G}_m[p^n] = \{x \in \overline{\mathbb{Q}}_p^\times \mid x^{p^n} = 1\}$$

and we follow the construction we have already done for the p-torsion group of an elliptic curve. What we obtain is that $T_p\mathbb{G}_m(\overline{\mathbb{Q}})$ is a free $\mathbb{Z}_p$- module of rank one: this is a general construction for the cyclotomic character.

References. See "Theory of p-adic Galois Representations" by J.M. Fontaine and Yi Ouyang.
See "The Arithmetic of Elliptic Curves" by J.H. Silverman, Section III.7.3.

In general, given an abelian variety A of dimension $g \geq 1$ we can use the same argument and construct the p-adic Tate module attached to A. It can be proved that

$$A[p^n] \simeq \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right)^{2g}$$

$$\begin{array}{ccccccc}
A[p] & \xleftarrow{[p]} & A[p^2] & \xleftarrow{[p]} & A[p^3] & \longleftarrow & \dots \\
\wr\| & & \wr\| & & \wr\| & & \\
\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^{2g} & \xleftarrow[\pi]{} & \left(\frac{\mathbb{Z}}{p^2\mathbb{Z}}\right)^{2g} & \xleftarrow[\pi]{} & \left(\frac{\mathbb{Z}}{p^3\mathbb{Z}}\right)^{2g} & \longleftarrow & \dots
\end{array}$$

from which we conclude:

$$T_pA = \varprojlim_n (A[p^n], [p]) = \varprojlim \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right)^{2g} = \mathbb{Z}_p^{2g}$$

Galois Representations Associated to a Modular Form

Consider a modular curve X. We have a Riemann surface $X_{|\mathbb{C}}$ and we associate to it a complex abelian variety.
$X_{|\mathbb{C}}$ is a smooth curve of genus g. We have $H_1(X,\mathbb{Z})$, the abelianization of the fundamental group, which is a free abelian group of rank $2g$, i.e., $H_1(X,\mathbb{Z}) \simeq \mathbb{Z}^{2g}$. Furthermore we consider $H^0(X,\Omega^1_X)$, the group of holomorphic 1-forms over X, which is a $\mathbb{C}$-vector space of dimension g.
We construct the Abel-Jacobi map

$$\begin{aligned} H_1(X,\mathbb{Z}) &\xrightarrow{\quad\varphi\quad} H^0(X,\Omega^1_X)^V \\ [\gamma] &\longrightarrow \varphi([\gamma]) \quad \text{where } \varphi([\gamma])(\omega) = \int_\gamma \omega \end{aligned}$$

If γ is a path on X ($\gamma : [0,1] \longrightarrow X$) and ω is a differential on X then

$$\int_\gamma \omega = \int_0^1 \gamma^*(\omega)$$

It turns out that φ is injective and it is a group homomorphism.

$$H_1(X,\mathbb{Z}) \hookrightarrow H^0(X,\Omega^1_X)^V$$

and the image is a lattice of dimension $2g$:

$$\mathbb{Z}^{2g} \subseteq \mathbb{C}^g$$

Definition. We can construct an abelian variety

$$A = \frac{H^0(X,\Omega^1_X)^V}{H_1(X,\mathbb{Z})}$$

of dimension g. Observe that $A \simeq \mathbb{C}^g/\Lambda$ where Λ is the lattice $\mathbb{Z}^{2g}$.

Theorem 4.1 (Abel - Jacobi)**.** *We have an isomorphism of algebraic varieties:*

$$A_{/\mathbb{Q}} \simeq \frac{\{D \in Div(X) \mid \deg D = 0\}}{\{D \in Div(X) \mid D \textit{ is principal}\}} = \frac{Div^0(X)}{P(X)} = Pic^0(X)$$

Furthermore, whether a point $O \in X$ is fixed, we have the following map

$$\begin{aligned} u_O : X &\longrightarrow Pic^0(X) = \frac{Div^0(X)}{P(X)} \\ Q &\longrightarrow [(Q) - (O)] \end{aligned}$$

When $g = 1$ this map is an isomorphism. In general it is still true that:

Proposition 4.2. *If the genus $g \geq 1$, the map u_O is an embedding*

Definition. We indicate A as the Jacobian of X:

$$A = Jac(X)_{/\mathbb{Q}}$$

References. See "Abel-Jacobi theorem" by Seddik Gmira.

Hecke Algebra and Shimura Construction

Definition. Suppose $\Gamma = \Gamma_1(N)$ and consider $d \in (\mathbb{Z}/\mathbb{N}\mathbb{Z})^\times$ (N is the level of Γ). We define the Diamond operator $\langle d\rangle$ to be the map such that

$$\langle d\rangle f(E, \xi, \omega) = f(E, d\xi, \omega)$$

Definition. If p is a prime not dividing N, the level of Γ, then define the Hecke operator T_p acting on the space $S_2(\Gamma)$ by the formula

$$T_p(f) = \frac{1}{p}\sum_{i=0}^{p-1} f(\frac{\tau+i}{p}) + p\langle p\rangle f(p\tau)$$

Definition. If p is a prime dividing N, the level of Γ, then define the Hecke operator U_p acting on the space $S_2(\Gamma)$ by the formula

$$U_p(f) = \frac{1}{p}\sum_{i=0}^{p-1} f(\frac{\tau+i}{p}) = \sum_{p|n} a_n q^{\frac{n}{p}}$$

Consider $\mathbb{T}$ the Hecke Algebra, i.e., the subring of $\mathrm{End}_{\mathbb{C}}(S_2(\Gamma))$ generated over $\mathbb{C}$ by all the Hecke operators T_p for $p \nmid N$, U_q for $q \mid N$, and $\langle d\rangle$ acting on $S_2(\Gamma)$.

$$\mathbb{T} \subseteq S_2(\Gamma)^V = H^0(X, \Omega'_X)$$

We have an action of $\mathbb{T}$ on $Jac(X)_{/\mathbb{Q}}$ via duality that fixes $\Lambda = H_1(X, \mathbb{Z})$; for $T \in \mathbb{T}$ we call this action

$$\varphi_T : Jac(X) \longrightarrow Jac(X)$$

Suppose we have $f \in S_2(\Gamma)$ an eigenform for $\mathbb{T}$. Then $T(f) = a_T f$ where $a_T \in \overline{\mathbb{Q}}$. We call K_f the field generated over $\mathbb{Q}$ by all the eigenvalues associated to f: $K_f = \mathbb{Q}(\{a_T\}_T)$ It is possible to prove that $K_f/\mathbb{Q}$ is a finite extension.
We have a ring morphism

$$\begin{aligned} \Psi_f : \mathbb{T} &\longrightarrow K_f \\ T &\longrightarrow a_T \end{aligned}$$

We have $\mathbb{T} \circlearrowleft Jac(X)$. Define

$$I_f = \ker \Psi_f$$

and set

$$A_f = \frac{Jac(X)}{I_f \cdot Jac(X)}$$

It turns out that A_f is an abelian variety and we call it the variety associated to f. It is easy to observe that I_f annihilates A_f and therefore $\mathbb{T}/I_f \subseteq End(A_f)$.

Lemma 4.3.

$$\dim A_f = [K_f : \mathbb{Q}]$$

In particular, if $K_f = \mathbb{Q}$, then A_f is an elliptic curve.

Suppose now we have a prime l. To the abelian variety A_f we can associate the l-adic Tate module $T_l A_f$.
$T_l A_f$ is a $\mathbb{Z}_l$ free module of rank $2[K_f : \mathbb{Q}]$ and we can construct

$$V_l A_f = T_l A_f \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$$

V_lA_f is a free module over $K_f \otimes_{\mathbb{Q}_l} \mathbb{Q}_l$ of rank 2 with a linear action of $\mathcal{G}_{\mathbb{Q}}$ (Galois Representation). Consider the splitting beahviour of l in $\mathcal{O}_{K_f}$:

$$l\mathcal{O}_{K_f} = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_t^{e_t}$$

then

$$K_f \otimes_{\mathbb{Q}_l} \mathbb{Q}_l = \prod_{i=1}^{t} (K_f)_{\mathfrak{P}_i}$$

where $(K_f)_{\mathfrak{P}}$ is the completion of K_f with respect to $\mathfrak{P}$. Then we can write

$$V_lA_f = \bigoplus_{i=1}^{t} V_{l,i}$$

where $V_{l,i}$ is a $(K_f)_{\mathfrak{P}_i}$-vector space of dimension 2. For each i we have

$$\rho_i : \mathcal{G}_{\mathbb{Q}} \longrightarrow GL_2(K_{f_{\mathfrak{P}_i}})$$

a representation of dimension 2.

References. See "A First Course in Modular Forms" - F. Diamond and J. Shurman

From Modular Forms to Galois Representations

Notation. We define $\mathbb{T}_{\mathbb{Z}}$ to be the ring generated over $\mathbb{Z}$ by the Hecke operators T_n and $< d >$ acting on the space $S_2(\Gamma, \mathbb{Z})$.
More generally, if A is any ring, we define $\mathbb{T}_A$ to be the A-algebra $\mathbb{T}_{\mathbb{Z}} \otimes A$. This Hecke ring acts on the space $S_2(\Gamma, A)$ in a natural way.
Finally, we will write J_Γ for the jacobian variety of X_Γ.

In this section we suppose that $f = \sum_n a_n(f)q^n$ is a newform of weight 2 and level N_f.

Definition. We define the old subspace of $S_2(\Gamma)$ to be the space spanned by those functions which are of the form $g(az)$, where g is in $S_2(\Gamma_1(M))$ for some $M < N_f$ and aM dividing N_f. We define the new subspace of $S_2(\Gamma)$ to be the orthogonal complement of the old subspace with respect to the Petersson scalar product. A normalized eigenform in the new subspace is called a newform of level N_f.

Recall. The spaces $S_2(\Gamma)$ are equipped with a natural Hermitian inner product given by the Petersson scalar product:

$$< f, g >= \frac{i}{8\pi} \int_{X_\Gamma} \omega_f \wedge \overline{\omega}_g = \int_{\mathcal{H}/\Gamma} f(\tau)\overline{g}(\tau) dx dy$$

Let K_f denote the number field in $\mathbb{C}$ generated by the Fourier coefficients $a_n(f)$. Let ψ_f denote the character of f, i.e., the homomorphism $(\mathbb{Z}/N_f\mathbb{Z})^\times \longrightarrow K_f^\times$ defined by mapping d to the eigenvalue of $< d >$ on f.

Recall. The construction of Shimura that we have seen before associates to f (or rather, to the orbit $[f]$ of f under $\mathcal{G}_{\mathbb{Q}}$) an abelian variety A_f of dimension $[K_f : \mathbb{Q}]$.
Let $f = \sum_n a_n q^n$ be an eigenform on Γ with (not necessarily rational) Fourier coefficients, corresponding to a surjective algebra homomorphism $\lambda_f : \mathbb{T}_{\mathbb{Q}} \longrightarrow K_f$. Let $I_f \subseteq \mathbb{T}_{\mathbb{Z}}$ be the ideal $\ker(\lambda_f) \cap \mathbb{T}_{\mathbb{Z}}$. The image $I_f(J_\Gamma)$ is a (connected) subabelian variety of J_Γ which is stable under $\mathbb{T}_{\mathbb{Z}}$ and is defined over $\mathbb{Q}$.

Definition. The abelian variety A_f associated to f is the quotient

$$A_f = J_\Gamma / I_f(J_\Gamma)$$

A_f is defined over $\mathbb{Q}$ and depends only on $[f]$, and its endomorphism ring contains $\mathbb{T}_{\mathbb{Z}}/I_f$ which is isomorphic to an order in K_f.

This abelian variety is a certain quotient of $J_1(N_f)$, and the action of the Hecke algebra on $J_1(N_f)$ provides an embedding

$$K_f \hookrightarrow End_{\mathbb{Q}}(A_f) \otimes \mathbb{Q}.$$

We saw also that for each prime l the Tate module $\mathcal{T}_l(A_f) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ becomes a free module of rank two over $K_f \otimes \mathbb{Q}_l$. The action of the Galois group $\mathcal{G}_{\mathbb{Q}}$ on the Tate module commutes with that of K_f, so that a choice of basis for the Tate module provides a representation

$$\mathcal{G}_{\mathbb{Q}} \longrightarrow GL_2(K_f \otimes \mathbb{Q}_l)$$

As $K_f \otimes \mathbb{Q}_l$ can be identified with the product of the completions of K_f at its primes over l, we obtain from f certain 2-dimensional l-adic representations of $\mathcal{G}_{\mathbb{Q}}$.

l-adic Representations

In this discussion, we fix a prime l and a finite extension K of $\mathbb{Q}_l$. We let $\mathcal{O}$ denote the ring of integers of K, λ the maximal ideal and k the residue field. We shall consider l-adic representations with coefficients in finite extensions of our fixed field K. We regard K as a subfield of $\overline{\mathbb{Q}}_l$ and fix embeddings $\overline{\mathbb{Q}} \longrightarrow \overline{\mathbb{Q}}_l$ and $\overline{\mathbb{Q}} \longrightarrow \mathbb{C}$. If K' is a finite extension of K with ring of integers $\mathcal{O}'$, then we say that an l-adic representation $\mathcal{G}_l \longrightarrow GL_2(K')$ is good (respectively, ordinary, semistable) if it is conjugate over K' to a representation $\mathcal{G}_l \longrightarrow GL_2(\mathcal{O}')$ which is good (respectively, ordinary, semistable).

Definition. Let G be any topological group; by a finite $\mathcal{O}[G]$-module we shall mean a discrete $\mathcal{O}$-module of finite cardinality with a continuous action of G. By a profinite $\mathcal{O}[G]$-module we shall mean an inverse limit of finite $\mathcal{O}[G]$-modules.
If M is a profinite $\mathcal{O}[\mathcal{G}_l]$-module then we will call M

- good, if for every discrete quotient M' of M there is a finite flat group scheme $\mathcal{F}/\mathbb{Z}_l$ such that $M' \simeq \mathcal{F}(\overline{\mathbb{Q}}_l)$ as $\mathbb{Z}_l[\mathcal{G}_l]$-modules;
- ordinary, if there is an exact sequence

$$(0) \longrightarrow M^{(-1)} \longrightarrow M \longrightarrow M^{(0)} \longrightarrow (0)$$

  of profinite $\mathcal{O}[\mathcal{G}_l]$-modules such that I_l acts trivially on $M^{(0)}$ and by ϵ on $M^{(-1)}$ (equivalently, if and only if for all $\sigma, \tau \in I_l$ we have $(\sigma - \epsilon(\sigma))(\tau 1) = 0$ on M);
- semistable, if M is either good or ordinary.

Suppose that R is a complete Nöetherian local $\mathcal{O}$-algebra with residue field k. We will call a continuous representation $\rho : \mathcal{G}_l \to GL_2(R)$ good, ordinary or semistable, if

$$\det \rho_{|I_l} = \epsilon \qquad \text{(cyclotomic character)}$$

and if the underlying profinite $\mathcal{O}[\mathcal{G}_l]$-module, M_ρ is good, ordinary or semistable.

Definition. A representation ρ of $\mathcal{G}_{\mathbb{Q}}$ is said to be unramified at p if ρ is trivial on the inertia group I_p.

Observation. If ρ is unramified at p then $\rho(Frob_p)$ is well defined.

Let K'_f denote the K-algebra in $\overline{\mathbb{Q}}_l$ generated by the Fourier coefficients of f. Thus K'_f is a finite extension of K, and it contains the completion of K_f at the prime over l determined by our choice of embeddings. We let $\mathcal{O}'_f$ denote the ring of integers of K'_f and write k'_f for its residue field. We define

$$\rho_f : \mathcal{G}_{\mathbb{Q}} \longrightarrow GL_2(K'_f)$$

as the pushforward of $\mathcal{G}_{\mathbb{Q}} \longrightarrow GL_2(K_f \otimes \mathbb{Q}_l)$ by the natural map $K_f \otimes \mathbb{Q}_l \longrightarrow K'_f$. We assume the basis is chosen so that ρ_f factors through $GL_2(\mathcal{O}'_f)$. We also let ψ'_f denote the finite order l-adic character

$$\mathcal{G}_{\mathbb{Q}} \twoheadrightarrow \mathcal{G}al(\mathbb{Q}(\zeta_{N_f})/\mathbb{Q}) \longrightarrow (K'_f)^\times$$

obtained from ψ_f.

The following theorem lists several fundamental properties of the l-adic representations ρ_f obtained from Shimura's construction. In the statement we fix f as above and write simply N, a_n, ρ, ψ, ψ' and K' for N_f, $a_n(f)$, ρ_f, ψ_f, ψ'_f and K'_f respectively.

Theorem 5.1. *The l-adic representation*

$$\rho : \mathcal{G}_{\mathbb{Q}} \longrightarrow GL_2(K')$$

has the following properties.

(a) *If $p \nmid N_f$ then ρ is unramified at p and $\rho(Frob_p)$ has characteristic polynomial*

$$X^2 - a_p X + p\psi(p)$$

(b) $\det(\rho)$ *is the product of ψ' with the l-adic cyclotomic character ϵ, and $\rho(c)$ is conjugate to*

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

(c) *ρ is absolutely irreducible.*

(d) *The conductor $N(\rho)$ is the prime-to-l-part of N.*

(e) *Suppose that $p \neq l$ and $p \mid\mid N$. Let χ denote the unramified character $\mathcal{G}_p \longrightarrow (K')^{\times}$ satisfying $\chi(Frob_p) = a_p$. If p does not divide the conductor of ψ, then $\rho \mid_{\mathcal{G}_p}$ is of the form*

$$\begin{pmatrix} \chi\epsilon & * \\ 0 & \chi \end{pmatrix}$$

If p divides the conductor of ψ, then $\rho \mid_{\mathcal{G}_p}$ is of the form

$$\chi^{-1}\epsilon\psi' \mid_{\mathcal{G}_p} \oplus \chi$$

(f) *If $l \nmid 2N$, then $\rho \mid_{\mathcal{G}_l}$ is good. Moreover, $\rho \mid_{\mathcal{G}_l}$ is ordinary if and only if a_l is a unit in the ring of integers of K', in which case $\rho_{I_l}(Frob_l)$ is the unit root of the polynomial $X^2 - a_l X + l\psi(l)$.*

(g) *If l is odd and $l \mid\mid N$, but the conductor of ψ is not divisible by l, then $\rho \mid_{\mathcal{G}_l}$ is ordinary and $\rho_{I_l}(Frob_l) = a_l$.*

Proof. Recall that $J_1(N)$ has good reduction at those prime p that do not divide N. Then the action of $\mathcal{G}_p$ on $V_l A_f$ is unramified.

(a) The key ingredient is the Eichler-Shimura congruence relation (Theorem 1.29 on the notes):

Theorem 5.2. *If $p \nmid N$ then the endomorphism T_p of $J_{\Gamma/\mathbb{F}_p}$ satisfies*

$$T_p = F + \langle p \rangle F'$$

where F is the Frobenius endomorphism and F' is the dual endomorphism (Verschiebung) on $J_{\Gamma/\mathbb{F}_p}$.

Recall that $J_1(N)$ has good reduction at those prime p not dividing N; so the action of $\mathcal{G}_p$ on $T_l A_f \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ is unramified and it is in fact described by the action of $\text{Frob}_p \in \mathcal{G}_{\mathbb{F}_p}$ on the Tate module of its reduction. But this is given by the Frobenius endomorphism F whose characteristic polynomial has been already computed (Corollary 1.41 on the notes):

Lemma 5.3. *For p not dividing Nl, the characteristic polynomial of F on the $\mathbb{T}_{\mathbb{Q}_l}$-module ν is*

$$X^2 - T_p X + \langle p \rangle p = 0$$

(The proof of the Lemma consists in multiplying the Shimura congruence relation by F and observing that $FF' = p$).

References. See "Introduction to the Arithmetic of Automorphic Functions" and "On the Factors of the Jacobian Variety of a Modular Function Field" by Goro Shimura.

(b) The first statement follows from (a) applying the Chebotarev density Theorem. The second assertion is a consequence of the fact that $\psi(-1) = 1$.

(c) It was proved by Ribet by contraddiction to the following theorem assuming the reducibility of the representation (Theorem 1.24 on the notes):

Theorem 5.4. *Let $f \in S_2(\Gamma_1(N))$. The coefficients $a_n \in \mathbb{C}$ satisfy the inequality*

$$|a_n| \leq c(f)\sigma_0(n)\sqrt{n}$$

where $c(f)$ is a constant depending only on f, and $\sigma_0(n)$ denotes the number of positive divisors on n.

In "On l-adic Representation Attached to Modular Forms II", Ribet showed that, assuming the reducibility of the representation, we can conclude that Theorem 5.4 is false for infinitely many primes p; indeed, we get an equality $a_p = 1 + p^{k-1}$ for $k = 2$ (weight of f).

(d)-(e) They follow from a deep result of Carayol based on the work of Langlands, Deligne and others characterizing $\rho_{|\mathcal{G}_p}$ in terms of $\psi_{|\mathcal{G}_p}$.

(f) The first assertion follows from the fact that A_f has good reduction at l if $l \nmid N$. The second statement follows from the Eichler-Shimura congruence relation (Theorem 5.2).

(g) It follows from the work of Deligne - Rapoport.

□

mod l Representations

Let K be an extension of $\mathbb{Q}_l$ and let $\mathcal{O}_K$ denotes its ring of integers. Suppose $\mathfrak{m}$ the maximal ideal of $\mathcal{O}_K$ and call k the residue field.
If $\rho : \mathcal{G}_{\mathbb{Q}} \to GL_d(K)$ is an l-adic representation (i.e., a continuous representation $\mathcal{G}_{\mathbb{Q}} \to GL_d(K)$ where K is a finite extension of $\mathbb{Q}_l$ and ρ is unramified at all but finitely many primes) then the image of ρ is compact, and hence ρ can be conjugated to a homomorphism $\mathcal{G}_{\mathbb{Q}} \to GL_d(\mathcal{O}_K)$. Reducing modulo the maximal ideal $\mathfrak{m}$ gives a residual representation

$$\overline{\rho} : \mathcal{G}_{\mathbb{Q}} \longrightarrow GL_d(k)$$

This representation may depend on the particular $GL_d(K)$-conjugate of ρ chosen, but its semisimplification

$$\overline{\rho}^{ss}$$

(i.e., the unique semi-simple representation with the same Jordan-Hölder factors) is uniquely determined by ρ.
In our situation we have K_f which is a finite extension of $\mathbb{Q}_l$ and an l-adic representation $\rho_f : \mathcal{G}_{\mathbb{Q}} \longrightarrow GL_2(K_f)$. Now define

$$\overline{\rho}_f : \mathcal{G}_{\mathbb{Q}} \longrightarrow GL_2(k_f)$$

the semi-simplification of the reduction of ρ_f. Assertions analogous to those in Theorem 5.1 hold for $\overline{\rho} = \overline{\rho}_f$, except that

- The representation need not be absolutely irreducible (as in **(c)**). However if l is odd, one checks using **(b)** that $\overline{\rho}$ is irreducible if and only if it is absolutely irreducible.
- In **(d)**, one only has divisibility of the prime-to-l part of N_f by $N(\overline{\rho})$.

Proposition 5.5. *Suppose that p is a prime such that $p \mid N_f$, $p \not\equiv 1$ mod l and $\overline{\rho}_f$ is unramified at p. Then $tr(\overline{\rho}_f(Frob_p))^2 = (p+1)^2$ in k_f.*

Artin Representations

The theory of Hecke operators and newforms extends to modular forms on $\Gamma_1(N)$ of arbitrary weight. The construction of l-adic representations associated to newforms was generalized to weight greater than 1 by Deligne using etale cohomology. There are also Galois representations associated to newforms of weight 1 by Deligne and Serre, but an essential difference is that these are Artin representations.

Theorem 5.6 (Deligne - Serre)**.** *Let $N \in \mathbb{N}$ and consider χ an odd Dirichlet character. Let $0 \neq g = \sum_n a_n(g)q^n \in M_1(N,\chi)$ be a normalised eigenform for the Hecke operators. Then there exists a 2-dimensional complex Galois representation*

$$\rho : \mathcal{G}_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{C})$$

that is unramified at all primes p that do not divide N and such that

$$Tr(Frob_p) = a_p \qquad and \qquad \det(Frob_p) = \chi(p)$$

for all primes $p \nmid N$. Such a representation is irreducible if and only if g is a cusp form.

Sketch of proof. If f is as in the hypothesis, then f is uniquely associated to two Dirichlet characters ϕ, ψ that (raised to modulo N) have product χ. Hence the map $\rho : \mathcal{G}_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{C})$ defined by

$$\sigma \longrightarrow \begin{pmatrix} \phi(\sigma) & 0 \\ 0 & \psi(\sigma) \end{pmatrix}$$

is a reducible representation with the desired properties.
If $g = \sum_{n=1}^{+\infty} a_n q^n$ is a cusp form, then the Theorem follows considering $L \subseteq \mathbb{C}$, the algebraic number field containing a_p and $\chi(p)$ for all p, and the reduction modulo some place λ_l of L (where l is a prime that splits completely). □

Theorem 5.7. *If $g = \sum_n a_n(g)q^n$ is a newform of weight one, level N_g and character ψ_g, then there is an irreducible Artin representation*

$$\rho_g : \mathcal{G}_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{C})$$

of conductor N_g with the following property: if $p \nmid N_g$, then the characteristic polynomial of $\rho_g(Frob_p)$ is

$$X^2 - a_p(g)X + \psi_g(p)$$

Sketch of proof. We can observe the following things:

- $\det(\rho_g)$ is the character of $\mathcal{G}_{\mathbb{Q}}$ corresponding to ψ and $\rho_g(c)$ is conjugated to the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- A basis can be chosen so that the representation ρ_g takes values in $GL_2(K_g)$ (where K_g is the number field generated by the $a_n(g)$). Moreover suppose that K is a finite extension of $\mathbb{Q}_l$ in $\overline{\mathbb{Q}}_l$ and we have fixed embeddings of $\overline{\mathbb{Q}}$ in $\mathbb{C}$ and $\overline{\mathbb{Q}}_l$). If K_g is contained in K, then we can view ρ_g as giving rise to an l-adic representation $\mathcal{G}_{\mathbb{Q}} \to GL_2(K)$ and hence a mod l representation $\mathcal{G}_{\mathbb{Q}} \to GL_2(k)$.
- A key idea in the construction of ρ_g is to first construct the mod l representations using those already associated to newforms of higher weight. More precisely, suppose that $K_g \longrightarrow K$ as in the previous point. One can show that for some newform f of weight 2 and level N_f dividing Nl we have

$$a_p(g) \equiv a_p(f) \qquad \psi_g(p) \equiv p\psi_f(p)$$

  for all $p \nmid Nl$, the congruence being modulo the maximal ideal of the ring of integers of K'_f. Thus $\overline{\rho}_f$ is the semi-simplification of the desired mod l representation (with scalars extended to k_f).

□

From Galois Representations to Modular Forms

In the previous sections we have seen how to constuct a Galois representation starting from a modular form.We now want to understand if it is possible to do the inverse road.
It is conjectured that certain types of two-dimensional representations of $\mathcal{G}_{\mathbb{Q}}$ always arise from the constructions described in the previous section. We now state some of the conjectures and the results known prior to Wiles's work.

Artin Representations

Conjecture 6.1 (Artin's Conjecture). *Let $\rho : \mathcal{G}_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{C})$ be a continuous irreducible representation with $\det(\rho(c)) = -1$. Then ρ is equivalent to ρ_g for some newform g of weight one.*

Observation. Conjecture 6.1 is equivalent to the statement that the Artin L-functions attached to ρ and to all its twists by one-dimensional characters are entire. (The Artin conjecture predicts that the Artin L-function $L(s, \rho)$ is entire, for an arbitrary irreducible, non-trivial Artin representation $\rho : \mathcal{G}_{\mathbb{Q}} \longrightarrow GL_d(\mathbb{C})$).

A large part of conjecture 6.1 was proved by Langlands.

Theorem 6.2 (Weil-Langlands). *Given $\rho : \mathcal{G}_{\mathbb{Q}} \to GL_2(\mathbb{C})$ satisfying*

(a) *ρ is irreducible;*

(b) $\det \rho$ *is odd;*

(c) *for all continuous characters $\chi : \mathcal{G}_{\mathbb{Q}} \to \mathbb{C}^{\times}$, the L-function $L(\rho \otimes \chi, s) = \sum_{n=1}^{+\infty} \chi(n) a_n n^{-s}$ has an analytic continuation to the entire complex plane*

with Artin conductor N, let

$$L(\rho, s) = \sum_{n=1}^{+\infty} a_n n^{-s}$$

be its Artin L-function. Then $f = \sum_{n=1}^{+\infty} a_n q^n$ is a normalized newform lying in $S_1(N, \chi)$.

Sketch of proof. The proof consists in realizing a bijection between the set of (isomorphism classes of) complex Galois representations of conductor N satisfying (a),(b) and (c) above and the set of normalized newforms on $S_1(N, \chi)$. □

The results were extended by Tunnell.

Theorem 6.3. *Let $\rho : \mathcal{G}_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{C})$ be a continuous irreducible representation such that $\rho(\mathcal{G}_{\mathbb{Q}})$ is solvable and $\det(\rho(c)) = -1$. Then ρ is equivalent to ρ_g for some newform g of weight one.*

Remark. The solvability hypothesis excludes only the case where the projective image of ρ is isomorphic to A_5 the alternating group of order 5.

Remark. If the projective image of ρ is dihedral, then ρ is induced from a character of a quadratic extension of $\mathbb{Q}$. In this case the result can already be deduced from the work of Hecke.

Remark. A recent work of Khare and Wintenberger on Serre's modularity conjecture has shown that the Artin conjecture about L-functions for odd, 2-dimensional representations is true. The case of n dimensional representations

$$\rho : \mathcal{G}_{\mathbb{Q}} \to GL_n(\mathbb{C})$$

with n even is still open.

mod l Representations

Definition. We say that a representation $\overline{\rho} : \mathcal{G}_{\mathbb{Q}} \longrightarrow GL_2(k)$ is modular (of level N) if, for some newform f of weight 2 (and level N), $\overline{\rho}$ is equivalent over k_f to $\overline{\rho}_f$.

Proposition 6.4. *If $f \in S_2(M, \chi)$ is a newform of some level M dividing N, then its Fourier coefficients lie in a finite extension K of $\mathbb{Q}$. Moreover, if $\sigma \in \mathcal{G}al(\overline{\mathbb{Q}}/\mathbb{Q})$ is any Galois automorphism, then the Fourier series f^{σ} obtained by applying σ to the Fourier coefficients is a newform in $S_2(M, \chi\sigma)$.*

By Proposition 6.4 the notion is independent of the choices of embeddings $K \hookrightarrow \overline{\mathbb{Q}}_l$, $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_l$ and $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Moreover, if K' is a finite extension of K with residue field k', then $\overline{\rho}$ is modular if and only if $\overline{\rho} \otimes_k k'$ is modular.

Theorem 6.5. *Let $\overline{\rho} : \mathcal{G}_{\mathbb{Q}} \to GL_2(k)$ be a continuous absolutely irreducible representation with* $\det(\overline{\rho}(c)) = -1$. *Suppose that one of the following holds:*

(a) $k = \mathbb{F}_3$;

(b) *the projective image of $\overline{\rho}$ is dihedral.*

Then $\overline{\rho}$ is modular.

Sketch of proof. We will study the two cases separately.

(a) Let's consider the surjection

$$GL_2(\mathbb{Z}[\sqrt{-2}]) \longrightarrow GL_2(\mathbb{F}_3)$$

defined by reduction mod $(1 + \sqrt{-2})$. One checks that there is a section

$$s : GL_2(\mathbb{F}_3) \longrightarrow GL_2(\mathbb{Z}[\sqrt{-2}])$$

and applies theorem 6.3 to $s \circ \overline{\rho}$. The resulting representation arises from a weight one newform, and hence its reduction $\overline{\rho}$ is equivalent to $\overline{\rho}_f$ for some f.

(b) $\overline{\rho}$ is equivalent to a representation of the form $\mathrm{Ind}_{\mathcal{G}_F}^{\mathcal{G}_{\mathbb{Q}}} \overline{\xi}$ where F is a quadratic extension of $\mathbb{Q}$ and $\overline{\xi}$ is a character $\mathcal{G}_F \longrightarrow k^{\times}$. (We have here enlarged K if necessary.) Let n be the order of $\overline{\xi}$; choose an embedding

$$\mathbb{Q}(e^{\frac{2\pi i}{n}}) \hookrightarrow K$$

and lift $\overline{\xi}$ to a character $\xi : \mathcal{G}_F \longrightarrow \mathbb{Z}[e^{2\pi i/n}]^{\times}$. We may always choose ξ so that the Artin representation $\rho = \mathrm{Ind}_{\mathcal{G}_F}^{\mathcal{G}_{\mathbb{Q}}} \xi$ is odd, i.e., $\det(\rho(c)) = -1$. (In the case $l = 2$ and F real quadratic, we may have to multiply ξ by a suitable quadratic character of $\mathcal{G}_F$). We then apply 6.3 to ρ and deduce as in case **(a)** that $\overline{\rho}$ is modular.

□

In general we have the following

Conjecture 6.6 (Serre's Conjecture)**.** *Let $\overline{\rho} : \mathcal{G}_{\mathbb{Q}} \to GL_2(k)$ be a continuous absolutely irreducible representation with* $\det(\overline{\rho}(c)) = -1$. *Then $\overline{\rho}$ is modular.*

Serre also proposed a refinement of the conjecture which predicts that $\overline{\rho}$ is associated to a newform of specified weight, level and character. This refinement, known as "Serres refined conjecture", excludes weight 1 modular forms although a further reformulation was made by Edixhoven to include them. Through work of Mazur, Ribet, Carayol, Gross and others, this refinement is now known to be equivalent to Conjecture 6.6 if l is odd, and also when $l = 2$ in many cases. (One also needs to impose a mild restriction in the case $l = 3$).
Today this conjecture is known to be true thanks to a work of Chandrashekhar Khare (that already in 2005 proved some cases of it) and Jean-Pierre Wintenberger.

Here we give a variant which applies to newforms of weight two. Before doing so, we assume l is odd and define an integer $\delta(\overline{\rho})$ as follows:

- $\delta(\overline{\rho}) = 0$ if $\overline{\rho}_{|\mathcal{G}_l}$ is good;
- $\delta(\overline{\rho}) = 1$ if $\overline{\rho}_{|\mathcal{G}_l}$ is not good and $\overline{\rho}_{|I_l} \otimes_k \overline{k}$ is of the form

$$\begin{pmatrix} \epsilon^a & * \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} \epsilon & * \\ 0 & \epsilon^a \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \psi^a & 0 \\ 0 & \psi^a \end{pmatrix}$$

  for some positive integer $a < l$. (Recall that ϵ is the cyclotomic character and ψ is the character of I_l).
- $\delta(\overline{\rho}) = 2$ otherwise.

Theorem 6.7. *Suppose that l is odd and $\overline{\rho}$ is absolutely irreducible and modular. If $l = 3$, then suppose also that $\overline{\rho}_{|\mathcal{G}_{\mathbb{Q}(\sqrt{-3})}}$ is absolutely irreducible. Then there exists a newform f of weight two such that*

- *$\overline{\rho}$ is equivalent over k_f to $\overline{\rho}_f$;*
- *$N_f = N(\overline{\rho})l^{\delta(\overline{\rho})}$;*
- *the order of ψ_f is not divisible by l.*

Proof. The existence of such an f follows from the work of Diamond "The refined Conjecture of Serre", but with N_f dividing $N(\overline{\rho})l^{\delta(\overline{\rho})}$. It can be shown that N_f is divisible by $N(\overline{\rho})$. The divisibility of N_f by $\delta(\overline{\rho})$ follows from some results in the works of Gross and Edixhoven. □

l-adic Representations

Let $\rho : \mathcal{G}_{\mathbb{Q}} \to GL_2(K)$ be an l-adic representation.

Definition. We say that ρ is modular if, for some weight 2 newform f, ρ is equivalent over K'_f to ρ_f.

The notion is independent of the choices of embeddings and well-behaved under extension of scalars. The following is a special case of a conjecture of Fontaine and Mazur.

Conjecture 6.8 (Fontaine-Mazur)**.** *If $\rho : \mathcal{G}_{\mathbb{Q}} \to GL_2(K)$ is an absolutely irreducible l-adic representation and $\rho_{|\mathcal{G}_{\mathbb{Q}_l}}$ is semistable, then ρ is modular.*

(Recall that for us l-adic representations are defined to be unramified at all but finitely many primes. Recall also that if $\rho_{|\mathcal{G}_l}$ is semistable, then by definition $\det \rho_{|I_l}$ is the cyclotomic character ϵ).

Remark. Relatively little was known about this conjecture before Wiles' work. Wiles proves that under suitable hypotheses, the modularity of $\overline{\rho}$ implies that of ρ.

Remark. In the work of Fontaine and Mazur there is a stroger conjecture than the one here; in particular, the semistability hypothesis could be replaced with a suitable notion of potential semistability. On the other hand, one expects that if $\rho_{|\mathcal{G}_l}$ is semistable, then it is equivalent to ρ_f (over K'_f) for some f on $\Gamma_1(N(\rho)) \cap \Gamma_0(l)$ (and on $\Gamma_1(N(\rho))$ if $\rho_{|\mathcal{G}_l}$ is good).

Conjecture 6.9 (Shimura-Taniyama)**.** *All elliptic curves defined over $\mathbb{Q}$ are modular.*

The Shimura-Taniyama conjecture can be viewed in the framework of the problem of associating modular forms to Galois representations. Let E be an elliptic curve defined over $\mathbb{Q}$. For each prime l, we let $\rho_{E,l}$ denote the l-adic representation $\mathcal{G}_{\mathbb{Q}} \to GL_2(\mathbb{Q}_l)$ defined by the action of $\mathcal{G}_{\mathbb{Q}}$ on the Tate module of E.

Proposition 6.10. *The following are equivalent:*

(a) *E is modular.*

(b) *$\rho_{E,l}$ is modular for all primes l.*

(c) *$\rho_{E,l}$ is modular for some prime l.*

Proof. We have already seen that if E is modular, then E is isogenous to A_f for some weight two newform f with $K_f = \mathbb{Q}$. It follows that for each prime l, $\rho_{E,l}$ is equivalent to the l-adic representation ρ_f . Hence **(a)$\Longrightarrow$(b)$\Longrightarrow$(c)**.
To show **(c)$\Longrightarrow$(b)**, suppose that for some l and some f, the representations $\rho_{E,l}$ and ρ_f are equivalent. First observe that for all but finitely primes p, we have

$$tr(\rho_f(Frob_p)) = tr(\rho_{E,l}(Frob_p))$$

We deduce that for all but finitely many primes p

$$a_p(f) = p + 1 - \#\overline{E}_p(\mathbb{F}_p) \in \mathbb{Z}$$

We find that for each prime l, $\rho_{E,l}$ is equivalent to ρ_f and is therefore modular.
We finally show that **(b)$\Longrightarrow$(a)**. The equality above holds for all primes p not dividing N_f, which by theorem 5.1, part **(d)**, is the conductor of E. Since $\det(\rho_f) = \det(\rho_{E,l}) = \epsilon$, we see by Theorem 5.1 Part **(b)** that ψ_f is trivial. We conclude that a_p is in $\{0, \pm 1\}$ for primes p dividing N_f.
Thus $K_f = \mathbb{Q}$ and A_f is an elliptic curve. Faltings' isogeny Theorem now tells us that E and A_f are isogenous and we conclude that E is modular. □

Remark. Note that the equivalence **(b)$\Longleftrightarrow$(c)** does not require Faltings' isogeny Theorem.

Remark. Tate conjectured that the L-function determined the elliptic curve E up to isogeny over k. More precisely, that the map of $\mathbb{Z}_l$-modules:

$$\mathrm{Hom}_k(E, E') \otimes \mathbb{Z}_l \to \mathrm{Hom}_{\mathcal{G}_k}(T_l E, T_l E')$$

is an isomorphism, for any two elliptic curves E and E' over k. This was proved (for abelian varieties) by Faltings and it is know known as Falting's Isogeny Theorem.

Remark. In the paper "On the Modularity of Elliptic Curves over $\mathbb{Q}$" we can find the following chain of equivalences:

(1) The L-function $L(E, s)$ of E equals the L-function $L(f, s)$ for some eigenform f.

(2) The L-function $L(E, s)$ of E equals the L-function $L(f, s)$ for some eigenform f of weight 2 and level $N(E)$.

(3) $\rho_{E,l}$ is modular for some prime l.

(4) $\rho_{E,l}$ is modular for all primes l.

(5) There is a non-constant holomorphic map $X_1(N)(\mathbb{C}) \to E(\mathbb{C})$ for some positive integer N.

(6) There is a non-constant morphism $X_1(N(E)) \to E$ which is defined over $\mathbb{Q}$.

(7) E is modular.

The implications **(2)$\Longrightarrow$(1)**, **(4)$\Longrightarrow$(3)**, and **(6)$\Longrightarrow$(5)** are tautological. The implication **(1)$\Longrightarrow$(4)** follows from the characterisation of $L(E, s)$ in terms of $\rho_{E,l}$. The implication **(3)$\Longrightarrow$(2)** follows from a Theorem of Carayol and a Theorem of Faltings. The implication **(2)$\Longrightarrow$(6)** follows from a construction of Shimura and a Theorem of Faltings. The implication **(5)$\Longrightarrow$(3)** seems to have been first noticed by Mazur.

Proposition 6.11. *If the Fontaine-Mazur conjecture (Conjecture 6.8) holds for some prime l, then the Shimura-Taniyama conjecture holds. If Serre's conjecture (Conjecture 6.6) holds for infinitely many l, then the Shimura-Taniyama conjecture (Conjecture 6.9) holds.*

Proof. The first assertion is immediate from Proposition 6.10 and the irreducibility of $\rho_{E,l}$. The second follows from the work of Serre. (We have implicitly chosen the field K to be $\mathbb{Q}_l$ in the statements of Conjectures 6.8 and 6.6, but it may be replaced by a finite extension). □

Remark. Note that to prove a given elliptic curve E is modular, it suffices to prove that Conjecture 6.8 holds for a single l at which E has semistable reduction. Wiles' approach is to show that certain cases of Conjecture 6.6 imply cases of Conjecture 6.8 and hence cases of the Shimura-Taniyama conjecture.

Now the Shimura-Taniyama conjecture is known to be true with the name of "Modularity Theorem".