

Galois representations, Modularity and Applications to Arithmetic

March 7, 2007

Introduction

One of the main goals of modern number theory is to understand the structure of the absolute Galois group $G_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

But one of the most common approaches to studying the structure of a group is by way of its representations.

And so the theory of Galois representations arises from the need to understand the structure of the group $G_{\mathbb{Q}}$.

Introduction

One of the main goals of modern number theory is to understand the structure of the absolute Galois group $G_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

But one of the most common approaches to studying the structure of a group is by way of its representations.

And so the theory of Galois representations arises from the need to understand the structure of the group $G_{\mathbb{Q}}$.

Introduction

One of the main goals of modern number theory is to understand the structure of the absolute Galois group $G_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

But one of the most common approaches to studying the structure of a group is by way of its representations.

And so the theory of Galois representations arises from the need to understand the structure of the group $G_{\mathbb{Q}}$.

Introduction

The Langlands philosophy, which appears in various disguises, is that one can relate (nice) representations of $G_{\mathbb{Q}}$ which are algebraic in a nature to automorphic representations which, on the other hand, are analytic objects.

In this talk, we introduce some of the various conjectures that are related to this circle of ideas.

Introduction

The Langlands philosophy, which appears in various disguises, is that one can relate (nice) representations of $G_{\mathbb{Q}}$ which are algebraic in nature to automorphic representations which, on the other hand, are analytic objects.

In this talk, we introduce some of the various conjectures that are related to this circle of ideas.

Let F be a perfect field, choose an algebraic closure \bar{F} of F and let $G_F = \text{Gal}(\bar{F}/F)$ be the absolute Galois group of F .

The group G_F is equipped with the usual profinite topology:

$$G_F = \varprojlim \text{Gal}(E/F),$$

where the limit is taken over all finite Galois extension E of F .

In the rest of this talk, we will assume all Galois groups equipped with this topology.

Galois Theory

Let $p \geq 2$ be a prime, and let \mathbb{Q}_p be the p -adic completion of \mathbb{Q} at p . We choose algebraic closures $\overline{\mathbb{Q}}$ and $\overline{\mathbb{Q}_p}$ of \mathbb{Q} and \mathbb{Q}_p , respectively, such that the following diagram commutes.

$$\begin{array}{ccc} \mathbb{Q} & \hookrightarrow & \overline{\mathbb{Q}} \\ \downarrow & & \downarrow \\ \mathbb{Q}_p & \hookrightarrow & \overline{\mathbb{Q}_p} \end{array}$$

This induces an inclusion of Galois groups

$$G_{\mathbb{Q}_p} = \text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \hookrightarrow \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = G_{\mathbb{Q}}.$$

We call $G_{\mathbb{Q}_p}$ the **decomposition group of \mathbb{Q} at p** .

Galois Theory

There is a reduction map $\varrho : G_{\mathbb{Q}_p} \rightarrow G_{\mathbb{F}_p}$, and the groups $G_{\mathbb{Q}_p}$ and $G_{\mathbb{F}_p}$ fit into the exact sequence

$$1 \longrightarrow I_p \longrightarrow G_{\mathbb{Q}_p} \xrightarrow{\varrho} G_{\mathbb{F}_p} \longrightarrow 1.$$

The kernel I_p is called the **inertia group** at p .

A **Frobenius** element Frob_p is an element in $G_{\mathbb{Q}_p}$ whose image under ϱ is the automorphism $x \mapsto x^p$. It is well-defined up to conjugation.

Galois Theory

The following two theorems explain that the group structures of the abelianization of the groups $G_{\mathbb{Q}_p}$ and $G_{\mathbb{Q}}$ are well understood.

Theorem (Local Kronecker-Weber)

There is an isomorphism

$$G_{\mathbb{Q}_p}^{ab} \cong \mathbb{Z}_p^\times \times \prod_{\ell} \mathbb{Z}_\ell.$$

Theorem (Kronecker-Weber)

There is an isomorphism

$$G_{\mathbb{Q}}^{ab} \cong \prod_{\ell} \mathbb{Z}_\ell^\times.$$

Galois Theory

The following two theorems explain that the group structures of the abelianization of the groups $G_{\mathbb{Q}_p}$ and $G_{\mathbb{Q}}$ are well understood.

Theorem (Local Kronecker-Weber)

There is an isomorphism

$$G_{\mathbb{Q}_p}^{ab} \cong \mathbb{Z}_p^\times \times \prod_{\ell} \mathbb{Z}_\ell.$$

Theorem (Kronecker-Weber)

There is an isomorphism

$$G_{\mathbb{Q}}^{ab} \cong \prod_{\ell} \mathbb{Z}_\ell^\times.$$

Galois representations: Definition

Definition

A d -dimensional **Galois representation** is a homomorphism

$$\rho : G_{\mathbb{Q}} \rightarrow GL_d(K),$$

where K is a field.

Definition

We say that a representation ρ is **unramified** at p if it is trivial on the inertia group I_p . We say that it is **ramified** otherwise.

Galois representations: Definition

In Arithmetic, one is often interested in 3 classes of Galois representations:

- **Artin representations: continuous** representations $\rho : G_{\mathbb{Q}} \rightarrow GL_d(\mathbb{C})$.

The only totally disconnected compact subgroups of $GL_d(\mathbb{C})$ are finite.

Hence, Artin representations have **finite** images.

Hence, they are unramified at all but finitely many primes.

Galois representations: Definition

- **mod ℓ representations: continuous**
representations $\rho : G_{\mathbb{Q}} \rightarrow GL_d(k)$, where k is a finite field of characteristic ℓ .

They always have finite images.

Hence, like Artin representations, they are unramified at all but finitely many primes.

Galois representations: Definition

- **l -adic representations: continuous** representations $\rho : G_{\mathbb{Q}} \rightarrow GL_d(K)$, where K is a finite extension of \mathbb{Q}_l .

They can be ramified at infinitely many primes.

But we will only be interested in the ones that are unramified almost everywhere.

Let ρ be a Galois representation of one of the three types we just described. The **conductor** of ρ is a quantity that measures the level of ramification of ρ . It is a natural number we will denote by $N(\rho)$.

Galois representations: Definition

- **l -adic representations:** **continuous** representations $\rho : G_{\mathbb{Q}} \rightarrow GL_d(K)$, where K is a finite extension of \mathbb{Q}_l .

They can be ramified at infinitely many primes.

But we will only be interested in the ones that are unramified almost everywhere.

Let ρ be a Galois representation of one of the three types we just described. The **conductor** of ρ is a quantity that measures the level of ramification of ρ . It is a natural number we will denote by $N(\rho)$.

Artin representations: Example

The implication of the Kronecker-Weber theorem is that one-dimensional Galois representations are well understood. We will restrict ourselves to 2-dimensional representations in the rest of this talk.

Example

Let K be the splitting field of the polynomial $h = x^5 + 2x^4 + 6x^3 + 8x^2 + 10x + 8$. The Galois group $\text{Gal}(K/\mathbb{Q})$ is isomorphic to A_5 . So there is a homomorphism $G_{\mathbb{Q}} \rightarrow A_5 \subset \text{PGL}_2(\mathbb{C})$. Let $\rho : G_{\mathbb{Q}} \rightarrow \text{GL}_2(\mathbb{C})$ be any lift of this homomorphism. Then ρ is an Artin representation.

The L-series attached to an Artin representation

The **L-series** $L(\rho, s)$ attached to ρ is defined as follows:

- Let p be an unramified prime, and $x^2 - a_p x + \psi_p$ be the characteristic polynomial of $\rho(\text{Frob}_p)$. The local factor at p is given by

$$L_p(\rho, s) := (1 - a_p p^{-s} + \psi_p p^{-2s})^{-1}.$$

- For a ramified prime p , the local factor $L_p(\rho, s)$ can still be defined but this requires additional care.
- The **Artin L-series** is given by

$$L(\rho, s) := \prod_p L_p(\rho, s).$$

This is a meromorphic function.

The L-series attached to an Artin representation

The **L-series** $L(\rho, s)$ attached to ρ is defined as follows:

- Let p be an unramified prime, and $x^2 - a_p x + \psi_p$ be the characteristic polynomial of $\rho(\text{Frob}_p)$. The local factor at p is given by

$$L_p(\rho, s) := (1 - a_p p^{-s} + \psi_p p^{-2s})^{-1}.$$

- For a ramified prime p , the local factor $L_p(\rho, s)$ can still be defined but this requires additional care.
- The **Artin L-series** is given by

$$L(\rho, s) := \prod_p L_p(\rho, s).$$

This is a meromorphic function.

The L-series attached to an Artin representation

The **L-series** $L(\rho, s)$ attached to ρ is defined as follows:

- Let p be an unramified prime, and $x^2 - a_p x + \psi_p$ be the characteristic polynomial of $\rho(\text{Frob}_p)$. The local factor at p is given by

$$L_p(\rho, s) := (1 - a_p p^{-s} + \psi_p p^{-2s})^{-1}.$$

- For a ramified prime p , the local factor $L_p(\rho, s)$ can still be defined but this requires additional care.
- The **Artin L-series** is given by

$$L(\rho, s) := \prod_p L_p(\rho, s).$$

This is a meromorphic function.

The L-series attached to an Artin representation

The following conjecture was made by Artin himself.

Conjecture (Artin)

The L-series $L(\rho, s)$ is an entire function.

Many cases of the conjecture are known thanks to the following theorem.

Theorem (Langlands-Tunnells)

*Let $\rho : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{C})$ be an Artin representation whose image is **solvable**. Then $L(\rho, s)$ is an entire function.*

This theorem is proved by establishing the much stronger assertion that ρ is automorphic or modular. We will come back to this later.

The L-series attached to an Artin representation

The following conjecture was made by Artin himself.

Conjecture (Artin)

The L-series $L(\rho, s)$ is an entire function.

Many cases of the conjecture are known thanks to the following theorem.

Theorem (Langlands-Tunnells)

*Let $\rho : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{C})$ be an Artin representation whose image is **solvable**. Then $L(\rho, s)$ is an entire function.*

This theorem is proved by establishing the much stronger assertion that ρ is automorphic or modular. We will come back to this later.

The L-series attached to an Artin representation

The following conjecture was made by Artin himself.

Conjecture (Artin)

The L-series $L(\rho, s)$ is an entire function.

Many cases of the conjecture are known thanks to the following theorem.

Theorem (Langlands-Tunnells)

*Let $\rho : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{C})$ be an Artin representation whose image is **solvable**. Then $L(\rho, s)$ is an entire function.*

This theorem is proved by establishing the much stronger assertion that ρ is automorphic or modular. We will come back to this later.

mod ℓ and ℓ -adic Galois representations

One of the main sources for mod ℓ and ℓ -adic Galois representations is algebraic geometry.

Let E/\mathbb{Q} be an elliptic curve, and choose a prime ℓ of good reduction.

For any integer $n \geq 2$, the subgroup of n -torsion points $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ come equipped with a Galois action. This gives rise to a Galois representation of $(\mathbb{Z}/n\mathbb{Z})$ -module

$$\rho_{E,n} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(E[n]).$$

mod ℓ and ℓ -adic Galois representations

One of the main sources for mod ℓ and ℓ -adic Galois representations is algebraic geometry.

Let E/\mathbb{Q} be an elliptic curve, and choose a prime ℓ of good reduction.

For any integer $n \geq 2$, the subgroup of n -torsion points $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ come equipped with a Galois action. This gives rise to a Galois representation of $(\mathbb{Z}/n\mathbb{Z})$ -module

$$\rho_{E,n} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(E[n]).$$

mod ℓ and ℓ -adic Galois representations

One of the main sources for mod ℓ and ℓ -adic Galois representations is algebraic geometry.

Let E/\mathbb{Q} be an elliptic curve, and choose a prime ℓ of good reduction.

For any integer $n \geq 2$, the subgroup of n -torsion points $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ come equipped with a Galois action. This gives rise to a Galois representation of $(\mathbb{Z}/n\mathbb{Z})$ -module

$$\rho_{E,n} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(E[n]).$$

mod ℓ and ℓ -adic Galois representations

By choosing an \mathbb{F}_ℓ -basis of $E[\ell] \cong (\mathbb{Z}/\ell)^2$, we get the mod ℓ representation

$$\bar{\rho}_{E,\ell} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell).$$

It can also be shown that the maps $E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n]$ determine an inverse system with a compatible Galois action. By taking inverse limit and then extending scalar to \mathbb{Q}_ℓ , we get

$$\rho_{E,\ell} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Q}_\ell).$$

Theorem

Let E/\mathbb{Q} be an elliptic curve, and ℓ a prime of good reduction. The representations $\rho_{E,\ell}$ and $\bar{\rho}_{E,\ell}$ satisfy the following conditions:

- 1 $\det(\rho_{E,\ell}(c)) = -1$, where c is the complex conjugation.
- 2 $\rho_{E,\ell}$ and $\bar{\rho}_{E,\ell}$ are irreducible for almost every prime ℓ .
- 3 $\rho_{E,\ell}$ and $\bar{\rho}_{E,\ell}$ are unramified almost everywhere. And for each unramified at p , we have

$$\mathrm{tr}\rho(\mathrm{Frob}_p) = p + 1 - \#E(\mathbb{F}_p), \text{ and } \det \rho(\mathrm{Frob}_p) = p.$$

mod ℓ and ℓ -adic Galois representations

More generally, let A/\mathbb{Q} be a g -dimensional abelian variety whose endomorphism ring is an order \mathcal{O} in a number field F of degree g . Let λ be a prime in F , with residue field \mathbb{F}_{ℓ^s} , and define

$$A[\lambda] := \{x \in A(\overline{\mathbb{Q}}) : \alpha x = 0 \text{ for all } \alpha \in \lambda\}.$$

Again by choosing an \mathbb{F}_{ℓ^s} -basis for $A[\lambda]$, we get a mod ℓ Galois representation

$$\bar{\rho}_{A,\lambda} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_{\ell^s}).$$

The Galois action on the Tate module $T_{\ell}(A)$ also gives rise to λ -adic representations

$$\rho_{A,\lambda} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(F_{\lambda}).$$

Finally, if X/\mathbb{Q} is a smooth projective variety, one can obtain ℓ -adic Galois representations of higher dimension by taking the Galois action on the étale cohomology $H_{\text{ét}}^i(X, \overline{\mathbb{Q}}_\ell)$.

In the next talk, we will examine another source of Galois representations. In the Langlands philosophy, there should exist a natural correspondence between those two sources. We will examine the various conjectures related to this philosophy.

Finally, if X/\mathbb{Q} is a smooth projective variety, one can obtain ℓ -adic Galois representations of higher dimension by taking the Galois action on the étale cohomology $H_{\text{ét}}^i(X, \overline{\mathbb{Q}}_\ell)$.

In the next talk, we will examine another source of Galois representations. In the Langlands philosophy, there should exist a natural correspondence between those two sources. We will examine the various conjectures related to this philosophy.

Modular forms and Hecke operators

- We fix an integer $N \geq 1$, and let

$$\Gamma_0(N) = \left\{ \gamma \in \mathbf{SL}_2(\mathbb{Z}) : \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, N|c \right\}.$$

- The Poincaré upper-half plane is defined by

$$\mathcal{H} = \{z \in \mathbb{C} \text{ such that } \text{Im}(z) > 0\}.$$

Then $\Gamma_0(N)$ acts on \mathcal{H} by the Möbius transformations:

$$\gamma \cdot z := \frac{az + b}{cz + d}, \quad z \in \mathcal{H}, \quad \gamma \in \Gamma_0(N).$$

Modular forms and Hecke operators

Definition

A **modular form of level N and weight 2** is a holomorphic function $f : \mathcal{H} \rightarrow \mathbb{C}$ such that

$$f(\gamma z) = (cz + d)^2 f(z), \quad \text{for all } z \in \mathcal{H}, \gamma \in \Gamma_0(N).$$

Let f be a modular form of level N and weight 2. It must be invariant under the action of the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ which belongs to $\Gamma_0(N)$. And so,

$$f(z + 1) = f(z), \quad \text{for all } z \in \mathcal{H}.$$

Modular forms and Hecke operators

From elementary harmonic analysis, we get that f admits the following expansion:

$$f(z) = \sum_{n > -\infty} a_n q^n, \quad q = e^{2\pi iz}, \quad \text{and } a_n \in \mathbb{C}.$$

- We call this expression the **q -expansion** of f .
- We say that f is a **cusp form** if $a_n = 0$ for all $n \leq 0$.
- We denote the space of all cusp forms by $S_2(N)$.
- The connection of cusp forms to arithmetic lies very much in the behaviour of their q -expansion.

Important Fact:

Theorem (Shimura)

*The space $S_2(N)$ is **finite** dimensional.*

Modular forms and Hecke operators

Let f be a cusp form of weight 2 and p a prime, and define T_p by

$$T_p f(z) := \frac{1}{p} \sum_{i=0}^{p-1} f\left(\frac{z+i}{p}\right) + f(pz) \quad \text{if } p \nmid N,$$

and

$$T_p f(z) := \frac{1}{p} \sum_{i=0}^{p-1} f\left(\frac{z+i}{p}\right) \quad \text{if } p \mid N.$$

One can show that T_p is a linear operator on $S_2(N)$. We call T_p the **Hecke operator at p** .

Modular forms and Hecke operators

We extend this definition to all integers $n \geq 1$ by

- $T_{mn} = T_m T_n$ for all $(m, n) = 1$.
- $T_{p^{k+1}} = T_p T_{p^k} + p T_{p^{k-1}}$ for all $(p, N) = 1$.
- $T_{p^k} = T_p^k$ for all $(p, N) > 1$.

Then we have the following result of Shimura.

Theorem (Shimura)

The operators T_n , $n \geq 1$, commute and admit a common basis of eigenvectors. Furthermore, if f is a common eigenvector, with q -expansion $f = \sum_{n \geq 1} a_n q^n$, then

$$T_n f = a_n f, \text{ for all } n \geq 1.$$

Modular forms and Hecke operators

We say that a common eigenvector $f = \sum_{n \geq 1} a_n q^n$ is **normalized** if $a_1 = 1$.

The following theorem gives the main reason why normalized eigenvectors play such a crucial role in modern arithmetic.

Theorem (Shimura)

*Let f be a normalized eigenvector. The eigenvalues of f are **algebraic integers**, and the field $F := \mathbb{Q}(a_n, n \geq 1)$ obtained by adjoining all the coefficients to \mathbb{Q} is a number field. Furthermore, the a_n satisfy the following relations:*

- $a_{nm} = a_n a_m$ for all $(n, m) = 1$.
- $a_{p^{k+1}} = a_{p^k} a_p + p a_{p^{k-1}}$ for all $(p, N) = 1$.
- $a_{p^k} = a_p^k$ for all $(p, N) > 1$.

L -series attached to a cusp form

The L -series attached to a modular cusp form $f = \sum_{n \geq 1} a_n q^n$ is given by

$$L(f, s) := \sum_{n \geq 1} \frac{a_n}{n^s}.$$

- It can be shown that $L(f, s)$ satisfies the following Euler product relation

$$L(f, s) = \prod_{p \nmid N} (1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p \mid N} (1 - a_p p^{-s})^{-1}.$$

- The L -series $L(f, s)$ admits an analytic continuation to the whole complex plane.

Computational aspects of modular forms

Let $Y_0(N) = \Gamma_0(N) \backslash \mathcal{H}$.

By adding a finite number of points, one can make $Y_0(N)$ into a compact Riemann surface $X_0(N)$.

In this setting, if $f = \sum_{n \geq 1} a_n q^n$ is a cusp form then $\omega_f = 2\pi i f(z) dz$ is a holomorphic differential form on $X_0(N)$, and we have the following theorem.

Theorem

The map $f \mapsto \omega_f := 2\pi i f(z) dz$ is an isomorphism of complex spaces between $S_2(N)$ and the space $\Omega_{X_0(N)}^1$ of holomorphic differential forms on $X_0(N)$.

Computational aspects of modular forms

By combining this theorem with the Poincaré duality, one gets an isomorphism of Hecke modules

$$S_2(N) \oplus \overline{S_2(N)} \cong H_1(X_0(N), \mathbb{C}).$$

The following beautiful theorem explains how cuspidal modular forms are amenable to computation.

Theorem

- a) *The integral homology $H_1(X_0(N), \mathbb{Z})$ admits a **finite presentation** by **modular symbols**.*
- b) $H_1(X_0(N), \mathbb{C}) = H_1(X_0(N), \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{C}$.

The proof of this theorem can be made into an efficient algorithm for the computation of cusp forms. (See John Cremona and William Stein homepages for more on this.)

Computational aspects of modular forms

```
> M:=ModularSymbols(Gamma0(2));
```

```
> M;
```

Full modular symbols space for $\Gamma_0(2)$ of weight 2 and dimension 1 over Rational Field

```
> S:=CuspidalSubspace(M);
```

```
> S;
```

Modular symbols space for $\Gamma_0(2)$ of weight 2 and dimension 0 over Rational Field

This is a crucial result in the proof of Fermat's Last Theorem.

Computational aspects of modular forms

```
> M:=ModularSymbols(Gamma0(11));
```

```
> M;
```

Full modular symbols space for Gamma_0(11) of weight 2 and dimension 3 over Rational Field

```
> S:=CuspidalSubspace(M);
```

```
> qEigenform(S, 20);
```

```
q - 2*q^2 - q^3 + 2*q^4 + q^5 + 2*q^6 - 2*q^7  
- 2*q^9 - 2*q^10 + q^11 - 2*q^12 + 4*q^13  
+ 4*q^14 - q^15 - 4*q^16 - 2*q^17 + 4*q^18 + O(q^19)
```

```
> SystemOfEigenvalues(S, 20);
```

```
[ -2, -1, 1, -2, 1, 4, -2, 0 ]
```

We will see later that this corresponds to the unique elliptic curve of conductor 11 given by

$$y^2 + y = x^3 - x^2 - 10x - 20.$$

Galois representations attached to modular forms

The following theorem which is one of the most important results in the theory of modular forms relies very deeply on the arithmetic theory of the modular curve $X_0(N)$.

Theorem

Let $f = \sum_{n \geq 1} a_n q^n$ be a normalized eigenvector of weight 2 and level N , and let K_f be the number field generated by its coefficients. Let $\ell \geq 2$ be a prime such that $\ell \nmid N$, and choose a prime $\lambda \in K_f$ above ℓ . Then, there exists a λ -adic Galois representation

$$\rho_{f, \lambda} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{GL}_2(K_{f, \lambda})$$

such that, for all $p \nmid N$,

$$\text{tr} \rho(\text{Frob}_p) = a_p, \text{ and } \det \rho(\text{Frob}_p) = p.$$

Galois representations attached to modular forms

We can reduce the representation modulo λ to get a mod λ representation

$$\bar{\rho}_{f,\lambda} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{GL}_2(\bar{\mathbb{F}}_\ell).$$

Definition

Let ρ be an ℓ -adic representation (of dimension 2). We say that ρ is **modular** if there exists a normalized eigenvector f such that $\rho \cong \rho_{f,\ell}$.

The modularity of Artin and mod ℓ representations are defined in a similar way.

Galois representations: modularity conjectures

There are several conjectures that predict that a Galois representation that is **well-behaved** should be modularity. To name few of those conjectures, we have:

- Fontaine-Mazur conjecture: ℓ -adic representations.
- Serre's conjecture: mod ℓ representations. Recently, there have been some substantial progress toward this conjecture (Khare).
- Artin's conjecture: Artin's representation. (Known for 2-dimensional representations except for the ones with projective image A_5).

Modularity of elliptic curves

The following theorem was proven by Wiles and several other people.

Theorem (Wiles 95, BCDT 99)

Let E/\mathbb{Q} be an elliptic curve of conductor $N > 1$. Then there exists a modular form f of weight 2 and level N such that the following equivalent conditions hold:

- a)** $\rho_{E,\ell} \cong \rho_{f,\ell}$ for some prime $\ell \nmid N$.
- b)** $\rho_{E,\ell} \cong \rho_{f,\ell}$ for all prime $\ell \nmid N$.
- c)** $L(E, s) = L(f, s)$.

We say that the elliptic curve E is **modular**.

Applications to analytic continuation

Applications to Arithmetic