WHAT IS . . .

a Galois Representation?

Mark Kisin

Let $\overline{\mathbb{Q}}$ be the field of algebraic numbers. The Galois group $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is the group of automorphisms of the field $\overline{\mathbb{Q}}$. A *Galois representation* is simply a representation of this group, or indeed of any Galois group.

Since $G_{\mathbb{Q}}$ is a profinite group—the projective limit of the finite groups $\mathrm{Gal}(K/\mathbb{Q})$ where K is a finite Galois extension of $\mathbb{Q}$—any continuous representation of $G_{\mathbb{Q}}$ on a complex vector space V acts through a finite quotient. We get a richer theory if we consider the action of $G_{\mathbb{Q}}$ on vector spaces over the p-adic numbers $\mathbb{Q}_p$.

In this case a continuous representation may have infinite image. Moreover, very interesting examples of p-adic Galois representations arise from geometry. An algebraic variety X over $\mathbb{Q}$ is an object defined by finitely many algebraic equations with rational coefficients. Grothendieck's *p-adic étale cohomology* attaches to such an X a collection of finite dimensional $\mathbb{Q}_p$-vector spaces with a continuous action of $G_{\mathbb{Q}}$. We will denote these by $H^i(X, \mathbb{Q}_p)$, where i is a non-negative integer.

The vector spaces $H^i(X, \mathbb{Q}_p)$ have a simple description in terms of the complex solutions of the equations defining X. These form a topological space $X(\mathbb{C})$, and the $H^i(X, \mathbb{Q}_p)$ are obtained from the singular cohomology groups $H^i(X(\mathbb{C}), \mathbb{Z})$ by tensoring by $\mathbb{Q}_p$. Unfortunately, one cannot see the action of $G_{\mathbb{Q}}$ with this definition!

At this point it is natural to ask the following question:

> *Which p-adic representations of $G_{\mathbb{Q}}$ occur as an $H^i(X, \mathbb{Q}_p)$ for some X?*

Mark Kisin is professor of mathematics at the University of Chicago. His email address is kisin@math.uchicago.edu.

There is a remarkable conjecture due to Fontaine and Mazur which predicts the answer. To explain this we need to say something about the anatomy of $G_{\mathbb{Q}}$. If ℓ is a prime, let $\overline{\mathbb{Q}}_\ell$ be an algebraic closure of $\mathbb{Q}_\ell$ and fix an embedding $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_\ell$. The elements of $G_{\mathbb{Q}}$ which admit a continuous extension to $\overline{\mathbb{Q}}_\ell$ form a subgroup $D_\ell \subset G_{\mathbb{Q}}$, which is isomorphic to $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$ and depends on the chosen embedding $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_\ell$ only up to conjugation by elements of $G_{\mathbb{Q}}$. There is a short exact sequence

$$0 \to I_\ell \to D_\ell \to \mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell) \to 0$$

where $\overline{\mathbb{F}}_\ell$ is an algebraic closure of the finite field $\mathbb{F}_\ell$ of ℓ elements. The quotient $\mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$ is pro-free and topologically generated by the Frobenius automorphism $\mathrm{Frob}_\ell : x \mapsto x^\ell$ of $\overline{\mathbb{F}}_\ell$. A representation of $G_{\mathbb{Q}}$ is said to be *unramified* at ℓ if I_ℓ acts trivially.

There is an analogy between this picture and the fundamental group of a punctured Riemann surface. The analogues of the groups I_ℓ are the subgroups generated by a loop around a puncture. The latter subgroups are of course isomorphic to $\mathbb{Z}$, but the groups I_ℓ are much more complicated than this. Moreover in the topological picture the analogue of the quotient $\mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$ is trivial.

The conjecture of Fontaine-Mazur says that a continuous representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}(V)$ on a finite dimensional $\mathbb{Q}_p$-vector space V is a subquotient of some $H^i(X, \mathbb{Q}_p)$—we will say that ρ *comes from geometry*—if and only if it satisfies the following two conditions

(1) ρ is unramified at all but finitely many primes
(2) $\rho|_{D_p}$ is *potentially semi-stable*

(More precisely one should consider not just $H^i(X, \mathbb{Q}_p)$ but all its twists by a power of the cyclotomic character.)

The first condition is very natural because if X has good reduction at a prime ℓ then $H^i(X, \mathbb{Q}_\ell)$ will be unramified at ℓ. The second condition is more subtle. Although we have not explained what it means, it depends only on the restriction of ρ to D_p. This is rather remarkable, because if ρ comes from geometry, then results of Deligne and de Jong imply that for a prime ℓ at which ρ is unramified, the eigenvalues of $\rho(\mathrm{Frob}_\ell)$ are *Weil numbers*. This means that they are algebraic and their complex absolute values all have the form $\ell^{w/2}$, where w belongs to a finite collection of integers depending only on X. A priori these eigenvalues are just p-adic numbers, and have no reason to be algebraic. A ρ which comes from geometry is also conjectured to be part of a compatible system of ℓ-adic representations, as well as have an associated complex L-function. It seems incredible that a condition at only one prime p could imply all this, and yet there is mounting evidence for the truth of the conjecture! A representation ρ satisfying (1) and (2) is said to be *geometric*.

That a ρ which comes from geometry satisfies (2) is a consequence of the work of many people, beginning with a paper of Fontaine-Messing. In fact, this is a local result—any variety $X/\mathbb{Q}_p$ gives rise to representations of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ which are potentially semi-stable. However the local version of the converse is completely false—a potentially semi-stable representation of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ need not come from geometry.

Most of the work on the Fontaine-Mazur conjecture has exploited a connection between Galois representations and *automorphic forms*. The most classical example is that of modular forms. If k, N are non-negative integers, a *modular form* of weight k on $\Gamma_1(N)$ is a holomorphic function f on the complex upper half plane, which satisfies $f(\gamma(z)) = (cz + d)^k f(z)$ for elements $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{Z})$, whose reduction modulo N has the form $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$. In particular, $f(z + 1) = f(z)$ so that f has a Fourier expansion $f = \sum_{n\in\mathbb{Z}} a_n q^n$, where $q = e^{2\pi i z}$. Modular forms are also required to satisfy certain growth conditions, which imply that $a_n = 0$ for $n < 0$.

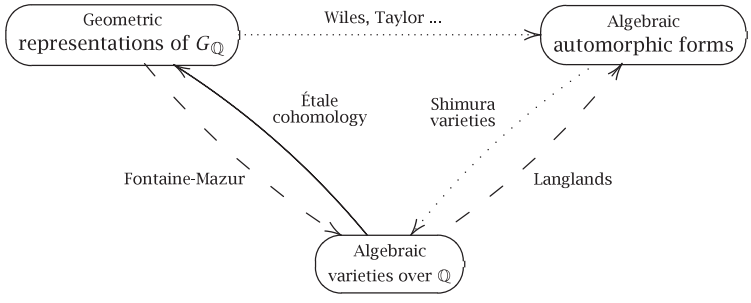
The space of modular forms on $\Gamma_1(N)$ of weight k is finite dimensional, and comes equipped with a collection of commuting operators T_n, $n \geq 1$. If $f = \sum_{n=0}^{\infty} a_n q^n$ is a simultaneous eigenvector for these operators, then $a_1 \neq 0$, and T_n has eigenvalue $\lambda_n = \frac{a_n}{a_1}$.

A theorem of Shimura, Deligne, and Deligne-Serre asserts that for such an f, the field $\mathbb{Q}(\lambda_n)_{n\geq 1}$ is a number field E_f, and that if λ is a finite prime of E_f then there is a continuous representation

$$\rho_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(E_{f,\lambda})$$

which is unramified at primes ℓ not dividing λN. Moreover at such primes the trace of the representation is given by the Fourier coefficients: $\mathrm{tr}(\rho_{f,\lambda}(\mathrm{Frob}_\ell)) = a_\ell$. The *Cebotarev density theorem* asserts that the elements Frob_ℓ are dense in the group $G_{\mathbb{Q}}$, so the existence of the representation $\rho_{f,\lambda}$ implies that the a_ℓ satisfy a plethora of λ-adic congruences, and even do so simultaneously for all possible λ. This is quite remarkable, given their definition as Fourier coefficients.

Starting with the spectacular work of Wiles and Taylor-Wiles on the modularity of elliptic curves and Fermat's Last Theorem, there has been significant progress, due to many people, toward establishing the Fontaine-Mazur conjecture for 2-dimensional representations. The basic idea is to show that a geometric representation ρ is equivalent to one of the representations $\rho_{f,\lambda}$, the latter coming from geometry by construction. This relationship between modular forms and geometric objects is an instance of a philosophy of Langlands that algebraic geometry over $\mathbb{Q}$ should be related to certain (so called algebraic) automorphic forms. Together with the Fontaine-Mazur conjecture it suggests that three, apparently completely different, kinds of objects should be intimately related. The situation can be summarized in the following diagram.



Here the dashed arrows indicate a conjecture, while the dotted ones indicate partial progress. Sadly there is only one completely solid arrow! Getting from one bubble to another is usually a highly nontrivial exercise, however success often carries enormous rewards. For example, Deligne was able to pass from modular forms to algebraic geometry and thereby prove the Ramanujan conjecture (and construct the $\rho_{f,\lambda}$ by moving up the solid arrow). Wiles (and his students) was able to pass from Galois representations to modular forms, and thereby prove (via the solid arrow) that elliptic curves were modular, and that their L-functions were therefore entire, as well as proving Fermat's Last Theorem!

Despite some partial results, the basic mechanism linking these three worlds is still largely a mystery. Attempts to understand it are sure to be a rich source of mathematics for decades to come.