What is the Langlands program all about?

Laurent Lafforgue*

November 13, 2013

Hua Loo-Keng Distinguished Lecture
Academy of Mathematics and Systems Science, Chinese Academy of Sciences

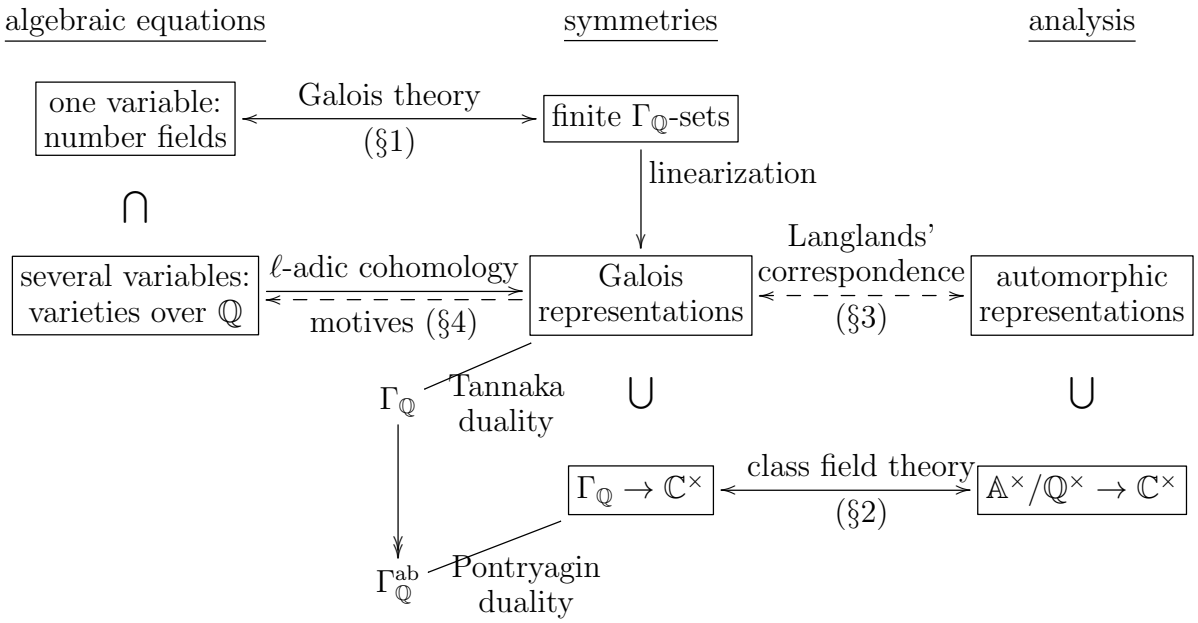
This talk is mainly intended for people who don't know the Langlands program at all, for people who are not working in algebraic geometry or automorphic theory. I want to give an idea for what the Langlands program is about. But I think that even for people who are working in the subject, it is always good to keep in mind the general picture.

The Langlands program has to do with number theory. Number theory consists primarily in the study of the ring of integers $\mathbb{Z}$ and the field of rational numbers $\mathbb{Q}$. At first sight these are very simple objects. However, a basic feature of number theory, and especially of the Langlands program, is that most questions are extremely elementary, but if the questions are not very easy, they are extremely difficult, and in order to try to solve them, we need extremely sophisticated theories.

In this talk, I shall present the basic objects of three such sophisticated theories: algebraic equations, symmetries, and analysis. They are all built from $\mathbb{Z}$ or $\mathbb{Q}$, but in three truly different directions. The general idea of the Langlands program, and of a closely-related program which can be called the motivic program, is that these three different theories in some sense tell the same story. The statements relating these theories are extremely difficult, because the objects in these theories are a priori completely different and unrelated. It is really a miracle of mathematics that there exists a relationship between such different objects.

*These informal notes were taken by Weizhe Zheng. The note taker is responsible for any inaccuracies.

The contents of the talk are summarized in the following table.



1 Algebraic equations

The theory of algebraic equations is the most elementary among the three, and it is the theory we are basically interested in.

1.1 Algebraic equations in one variable

An algebraic equation in one variable has the form

$$P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 = 0.$$

In history, people have been interested in this type of equations for a very long time. Here "algebraic" means that in the writing of the equation, we only need addition and multiplication. We need to choose the coefficients $a_{n-1}, \ldots, a_0$, and the simplest coefficients are rational coefficients. These can be considered the most elementary equations in mathematics.

The degree of the equation, n, is a basic ingredient. Equations of degree 1

$$X + a_0 = 0$$

can be solve immediately: $X = -a_0$. Equations of degree 2

$$X^2 + a_1X + a_0 = 0$$

can be solved by introducing an extra symbol $\sqrt{\bullet}$ for square roots: $X = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_0}}{2}$. In other words, if we can solve equations of the form $X^2 = a_0$, then we can solve equations of degree 2 in general. Equations of degree 3

$$X^3 + a_2X^2 + a_1X + a_0 = 0$$

are more difficult to solve. It is known however that they can be solved with the help of the symbols $\sqrt{\bullet}$ and $\sqrt[3]{\bullet}$ for square roots and cube roots. In other words, if we can solve equations of the form $X^2 = a_0$ and equations of the form $X^3 = a_0$, then we can solve equations of degree 3 in general. Similarly, equations of degree 4

$$X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 = 0$$

can be solved by introducing roots $\sqrt{\bullet}$, $\sqrt[3]{\bullet}$, $\sqrt[4]{\bullet}$ of degrees 2, 3, 4. This has been known since the 16th century.

Is it possible to solve equations of higher degrees just by introducing n-th roots? This question remained unsolved for several centuries. In the 19th century, it was discovered independently by Abel and Galois that equations of degrees at least 5 cannot be solved in this way.

We can rephrase the problem as follows. As the degree becomes higher and higher, equations become more and more difficult to solve. So one may ask the following question: In order to solve a general algebraic equation $P(X) = 0$ of degree n, is it useful or not to solve some equations of lower degrees? One may ask an even more general question: Given two algebraic equations $P(X) = 0$ and $Q(X) = 0$ of degrees n and n', is there a relationship between the two equations?

In order to give a precise meaning to these questions, let us consider an algebraic equation $P(X) = 0$ of degree n with coefficients in $\mathbb{Q}$, or more generally with coefficients in a subfield K of the field of complex numbers $\mathbb{C}$. Here "subfield" means a subset closed under addition, multiplication, minus, and inverse. Consider an element $\alpha \in \mathbb{C}$, which is a solution of the equation: $P(\alpha) = 0$. We consider numbers related to α, namely numbers obtained from α and elements of K by addition and multiplication. The set of such numbers

$$K(\alpha) = \{b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 \mid b_i \in K\},$$

is clearly closed under addition, multiplication, and minus, and one can check that it is also closed under inverse. This set is a subfield of $\mathbb{C}$ containing K and we have $\dim_K(K(\alpha)) \leq n$. Moreover, if the polynomial $P(X)$ is irreducible, then $\dim_K(K(\alpha))$ is precisely n. In this case, the isomorphism class of the field $K(\alpha)$ does not depend on α and we denote it by K_P.

Given two such equations $P(X) = 0$ and $Q(X) = 0$, a *relation* between them is a morphism from K_P to K_Q over K, that is, a map $k\colon K_P \to K_Q$ that preserves addition and multiplication, and fixes scalars in K. In other words,

$$k(a + b) = k(a) + k(b), \qquad k(ab) = k(a)k(b)$$

for $a, b \in K_P$, and $k|_K = \mathrm{id}_K$.

This precise definition of relations between algebraic equations allows us to organize algebraic equations into a *category*, which is a collection of objects and relations (called "morphisms" in technical terms) between objects. We can now phrase the main theorem of Galois theory as follows.

Theorem (Galois)**.** *There exist a group Γ_K, called the* Galois group of K*, and an equivalence of categories*

$$\{\text{irreducible algebraic equations with coefficients in } K\} \xrightarrow{\sim} \{\text{finite sets endowed with transitive actions of } \Gamma_K\}.$$

Relations between finite sets endowed with group actions are defined to be maps between the sets that are compatible with the group actions. The Galois group Γ_K is a profinite group and we endow it with the profinite topology.

The theorem can be stated more explicitly. We let $\overline{K}$ denote the set of all solutions of algebraic equations with coefficients in K. This is a subfield of $\mathbb{C}$ containing K, called the algebraic closure of K. The Galois group is the automorphism group of $\overline{K}$ over K: $\Gamma_K = \mathrm{Aut}_K(\overline{K})$. The equivalence of categories in the theorem carries an equation $P(X) = 0$ to the set $\mathrm{Hom}_K(K_P, \overline{K})$ of morphisms from K_P to $\overline{K}$ over K. The set is naturally endowed with an action of $\mathrm{Aut}_K(\overline{K})$. It is part of the theorem that this set is finite.

The theorem can in fact be stated and proved for any base field K.

The theorem provides a dictionary between algebraic equations of one variable and symmetries under the Galois group. Such a dictionary is rather surprising as it reduces the knowledge of all algebraic equations with coefficients in K and their mutual relations to the knowledge of one single group, the Galois group Γ_K. We are thus led to the following question.

Question. What is the Galois group of $\mathbb{Q}$ (or K)?

This is a fundamental question in mathematics. In fact, the Langlands program is an attempt to partially answer this question.

1.2 Algebraic equations in several variables

An algebraic equation in d variables has the form

$$P(X_1, \ldots, X_d) = 0.$$

Such an equation defines a geometric object. For example the equation

$$X^2 + Y^2 = 1$$

defines a circle. More generally, algebraic equations in two variables define curves. The study of geometric objects defined by algebraic equations is algebraic geometry. To study algebraic equations in several variables thus means to move from algebra to algebraic geometry. We will come back to algebraic geometry in Section 4.

2 Abelianization of the Galois group

The abelianization of $\Gamma_{\mathbb{Q}}$ is the maximal abelian quotient and is defined by $\Gamma_{\mathbb{Q}}^{\mathrm{ab}} = \Gamma_{\mathbb{Q}}/[\Gamma_{\mathbb{Q}}, \Gamma_{\mathbb{Q}}]$, where $[\Gamma_{\mathbb{Q}}, \Gamma_{\mathbb{Q}}]$ is the commutator subgroup of $\Gamma_{\mathbb{Q}}$ generated by elements of the form $\sigma\sigma'\sigma^{-1}\sigma'^{-1}$, $\sigma, \sigma' \in \Gamma_{\mathbb{Q}}$. One hundred fifty years of number theory have been devoted to the computation of $\Gamma_{\mathbb{Q}}^{\mathrm{ab}}$, culminating in the class field isomorphism.

2.1 Class field isomorphism

We have seen that the Galois group $\Gamma_{\mathbb{Q}}$ controls algebraic extensions of $\mathbb{Q}$. The computation of $\Gamma_{\mathbb{Q}}^{\mathrm{ab}}$ depends on another kind of extensions, on which we can do

analysis. We know that the field of real numbers $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to the usual norm $|\cdot|$:

$$\mathbb{Q} \hookrightarrow \mathbb{R}.$$

There are norms on $\mathbb{Q}$ other than the usual norm. For every prime number p, we define the p-adic norm $|\cdot|_p$ as follows. Every rational number $r \neq 0$ can be written as $r = \pm p^v p_1^{v_1} \cdots p_k^{a_k}$ and we define $|r|_p = p^{-v}$. Thus, the more divisible by p is r, the smaller is its p-adic norm $|r|_p$. One can check that this is indeed a norm: $|rs|_p = |r|_p|s|_p$ and $|r+s|_p \leq |r|_p + |s|_p$. In fact we have a stronger inequality: $|r+s|_p \leq \max\{|r|_p, |s|_p\}$. The completion of $\mathbb{Q}$ with respect to the p-adic norm is called the field of the p-adic numbers $\mathbb{Q}_p$:

$$\mathbb{Q} \hookrightarrow \mathbb{Q}_p.$$

Completion is a topological process, and the field obtained are quite different from algebraic extensions. In fact, $\mathbb{R}$ and the $\mathbb{Q}_p$'s are uncountable. One can show that $\mathbb{R}$ and the $\mathbb{Q}_p$'s are the only completions of $\mathbb{Q}$.

Consider the embedding

$$\mathbb{Q} \hookrightarrow \mathbb{R} \times (\prod_p \mathbb{Q}_p).$$

Note that for any rational number $r \neq 0$, we have $|r|_p = 1$ for all but finitely many p. Consider the subset

$$\mathbb{A} = \{(x_p)_p \mid |x_p|_p \leq 1 \text{ for all but finitely many } p\} \subseteq \mathbb{R} \times (\prod_p \mathbb{Q}_p).$$

This subset is a ring, called the *adèle ring of* $\mathbb{Q}$. It is an important object in number theory. The adèle ring is endowed with a locally compact topology, making it a topological ring. The embedding

$$\mathbb{Q} \hookrightarrow \mathbb{A}$$

is similar to the embedding $\mathbb{Z} \hookrightarrow \mathbb{R}$ in that the image subgroup is discrete and the quotient group is compact. Taking invertible elements, we get an embedding of topological groups

$$\mathbb{Q}^\times \hookrightarrow \mathbb{A}^\times$$

of discrete image. The quotient $\mathbb{A}^\times/\mathbb{Q}^\times$ is a locally compact group, called the *idèle class group.*

Theorem (Class field isomorphism)**.** *We have an isomorphism of topological groups*

$$\Gamma_{\mathbb{Q}}^{\mathrm{ab}} \simeq (\mathbb{A}^\times/\mathbb{Q}^\times)\widehat{\ }.$$

Here $(\mathbb{A}^\times/\mathbb{Q}^\times)\widehat{\ }$ *denotes the profinite completion of* $\mathbb{A}^\times/\mathbb{Q}^\times$*, projective limit of the finite quotients of* $\mathbb{A}^\times/\mathbb{Q}^\times$ *by open subgroups.*

2.2 Characters

The Pontryagin duality says that knowing a profinite abelian group I is equivalent to knowing the group of continuous characters $I \to \mathbb{C}^\times$, necessarily with finite images. Thus the class field isomorphism amounts to an equivalence between continuous characters of $\Gamma_{\mathbb{Q}}^{\mathrm{ab}}$ and continuous characters of $(\mathbb{A}^\times/\mathbb{Q}^\times)\widehat{\ }$:

$$\{\Gamma_{\mathbb{Q}}^{\mathrm{ab}} \to \mathbb{C}^\times\} \longleftrightarrow \{(\mathbb{A}^\times/\mathbb{Q}^\times)\widehat{\ } \to \mathbb{C}^\times\}.$$

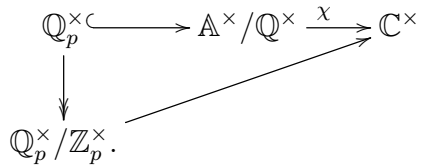
Characters $\Gamma_{\mathbb{Q}} \to \mathbb{C}^\times$ factorizes uniquely through $\Gamma_{\mathbb{Q}}^{\mathrm{ab}}$. Continuous characters of $\mathbb{A}^\times$ with finite images factorizes uniquely through $\mathbb{A}^\times/\mathbb{Q}^\times$. Thus we get an equivalence between continuous characters with finite images

$$\{\Gamma_{\mathbb{Q}} \to \mathbb{C}^\times\} \longleftrightarrow \{\mathbb{A}^\times/\mathbb{Q}^\times \to \mathbb{C}^\times\}.$$

Let $\chi\colon \mathbb{A}^\times/\mathbb{Q}^\times \to \mathbb{C}^\times$ be a continuous character with finite image. Consider the composition of χ with the projection $\mathbb{A}^\times \to \mathbb{A}^\times/\mathbb{Q}^\times$:

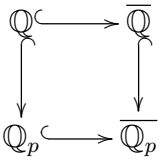
$$\mathbb{A}^\times \to \mathbb{A}^\times/\mathbb{Q}^\times \xrightarrow{\chi} \mathbb{C}^\times.$$

We have $\mathbb{A}^\times \subseteq \mathbb{R}^\times \times \prod_p \mathbb{Q}_p^\times$, and the composite character is a product $\chi_\infty \prod_p \chi_p$ of local characters $\chi_\infty\colon \mathbb{R}^\times \to \mathbb{C}^\times$, $\chi_p\colon \mathbb{Q}_p^\times \to \mathbb{C}^\times$. For all but finitely many p, χ_p is trivial on $\mathbb{Z}_p^\times = \{\alpha \in \mathbb{Q}_p^\times \mid |\alpha|_p = 1\}$, so that χ_p factorizes through $\mathbb{Q}_p^\times/\mathbb{Z}_p^\times$:

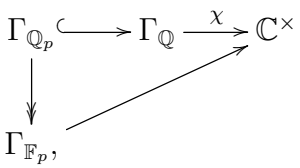


Note that $\mathbb{Q}_p^\times/\mathbb{Z}_p^\times \simeq \mathbb{Z}$, with a generator given by the image σ_p of p. Thus, for all but finitely many p, χ_p is determined by the image of σ_p in $\mathbb{C}^\times$. One can show that χ is in fact determined by this family of numbers in $\mathbb{C}^\times$.

The situation is similar on the Galois side. Let $\chi\colon \Gamma_{\mathbb{Q}} \to \mathbb{C}^\times$ be a character. The diagram of embeddings



induces an embedding $\Gamma_{\mathbb{Q}_p} \hookrightarrow \Gamma_{\mathbb{Q}}$. For all but finitely many p, the restriction of χ to $\Gamma_{\mathbb{Q}_p}$ factorizes through $\Gamma_{\mathbb{F}_p}$:



where $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. We have $\Gamma_{\mathbb{F}_p} \simeq \widehat{\mathbb{Z}}$, and the Frobenius substitution, which we also denote by σ_p, is a topological generator. Thus for all but finitely many p, the

restriction of χ to $\Gamma_{\mathbb{Q}_p}$ is determined by the image of σ_p in $\mathbb{C}^\times$. Moreover, χ is determined by this family of numbers in $\mathbb{C}^\times$.

In fact, the equivalence between characters of $\Gamma_{\mathbb{Q}}$ and characters on $\mathbb{A}^\times/\mathbb{Q}^\times$ is defined by requiring that the associated families of numbers are the same. We can rephrase this fact as follows. We are interested in $\Gamma_{\mathbb{Q}}^{\mathrm{ab}}$ and we consider continuous characters of $\Gamma_{\mathbb{Q}}$. We have seen that to such a character we can associate a family of numbers in $\mathbb{C}^\times$. One can ask the converse question: given a family of numbers in $\mathbb{C}^\times$, when does it come from a character of $\Gamma_{\mathbb{Q}}$?

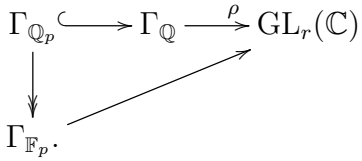
Theorem (Class field isomorphism, rephrased)**.** *A family of numbers in $\mathbb{C}^\times$ indexed by all but finitely many primes p comes from a continuous character of $\Gamma_{\mathbb{Q}}$ if and only if it comes from a continuous character with finite image of $\mathbb{A}^\times/\mathbb{Q}^\times$.*

The condition that the family of numbers comes from a character of $\mathbb{A}^\times/\mathbb{Q}^\times$ means more explicitly that the family of characters χ_p on $\mathbb{Q}_p^\times$ determined by the family of numbers can be completed to a family indexed by all prime numbers and ∞ so that their product $\chi_\infty \prod_p \chi_p$, which is a character of $\mathbb{A}^\times$, is trivial on the discrete subgroup $\mathbb{Q}^\times$.

3 Langlands' correspondence

How to get information about the whole Galois group $\Gamma_{\mathbb{Q}}$? We need to replace Pontryagin duality by Tannaka duality, which says that knowing a profinite group G is equivalent to knowing the (tensor) category of its continuous representations, namely finite-dimensional vector spaces V over $\mathbb{C}$ endowed with an action of G. If $\dim_{\mathbb{C}}(V) = r$, choosing a basis of V, the action can be written as a homomorphism $G \to \mathrm{GL}_r(\mathbb{C})$, necessarily with finite image.

Let $\rho\colon \Gamma_{\mathbb{Q}} \to \mathrm{GL}_r(\mathbb{C})$ be a continuous representation. As in the case of characters, for all but finitely many p, the restriction of ρ to $\Gamma_{\mathbb{Q}_p}$ factorizes through $\Gamma_{\mathbb{F}_p}$:



For such p, the conjugacy class of the image of σ_p is well-defined, and we can consider its eigenvalues, which form an unordered r-tuple of nonzero complex numbers. We thus get a family of r-tuples of numbers. This family of numerical invariants characterizes the representation if the representation is irreducible.

We can now ask the converse question: Given a family of r-tuples of nonzero complex numbers, when does it come from an irreducible Galois representation? Of course, an answer to this question would provide very deep information about the Galois group $\Gamma_{\mathbb{Q}}$ itself.

Langlands proposed a conjectural answer as follows. The embedding

$$\mathrm{GL}_r(\mathbb{Q}) \hookrightarrow \mathrm{GL}_r(\mathbb{A})$$

has discrete image. Since the group GL_r is not commutative, the quotient $\mathrm{GL}_r(\mathbb{Q})\backslash\mathrm{GL}_r(\mathbb{A})$ is not a group, but only a topological space endowed with a continuous action of the group $\mathrm{GL}_r(\mathbb{A})$ on the right. The invariant measure on $\mathrm{GL}_r(\mathbb{A})$ induces a measure on the quotient and we consider the Hilbert space $L^2(\mathrm{GL}_r(\mathbb{Q})\backslash\mathrm{GL}_r(\mathbb{A}))$ of square-integrable complex-valued functions on the quotient. This space is a representation of $\mathrm{GL}_r(\mathbb{A})$ and is a sum of irreducible representations π of $\mathrm{GL}_r(\mathbb{A})$. The π's that appear in this decomposition are called *automorphic representations of* $\mathrm{GL}_r(\mathbb{A})$.

Let π be an automorphic representation of $\mathrm{GL}_r(\mathbb{A})$. We have $\mathrm{GL}_r(\mathbb{A}) \subseteq \mathrm{GL}_r(\mathbb{R}) \times \prod_p \mathrm{GL}_r(\mathbb{Q}_p)$, and

$$\pi = \pi_\infty \otimes \bigotimes_p \pi_p,$$

where π_∞ is an irreducible representation of $\mathrm{GL}_r(\mathbb{R})$ and π_p is an irreducible representation of $\mathrm{GL}_r(\mathbb{Q}_p)$. For all but finitely many p, π_p is "unramified" and thus is naturally parameterized by an unordered r-tuple of nonzero complex numbers.

Conjecture (Langlands' correspondence)**.** *A family of unordered r-tuples of nonzero complex numbers indexed by all but finitely many primes p comes from an irreducible r-dimensional Galois representation of $\Gamma_{\mathbb{Q}}$ only if it comes from an automorphic representation of* $\mathrm{GL}_r(\mathbb{A})$.

Note that the number r is present on both sides of the story, but play very different roles. On the Galois side, r is the dimension of the representation. On the automorphic side, the group is GL_r, but the representations are often huge, infinite-dimensional.

Some progress toward this conjecture has been made, but we are still very far from proving it. This conjecture is very deep, as it relates two completely different kinds of objects. The Galois group stems from consideration of algebraic equations, while automorphic representations belong to functional analysis.

Another remark is that in both Galois theory and Langlands' correspondence, the Galois group intervenes via actions: actions on finite sets in Galois theory and linear actions in Langlands' correspondence. The two types of actions are directly related by linearization, which produces a linear Galois representation from every finite set endowed with a Galois action.

The Langlands' correspondence stated above is only between representations considered as objects, but it says nothing about the structures of the categories of representations. So what about tensor products of representations. What about relations between representations? At the present moment we don't even have any conjectural partial answer to these questions.

4 Algebraic geometry and motives

We have seen that an algebraic equation in several variables defines a geometric object. More generally, the geometric object defined by a system of such equations is called an algebraic variety. We are very far from having an analogue of Galois theory for varieties over $\mathbb{Q}$.

Grothendieck's theory of ℓ-adic cohomology allows us to go one way. Let ℓ be a prime number. Given an algebraic variety V over $\mathbb{Q}$, its i-th ℓ-adic cohomology group $H^i(V \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}, \mathbb{Q}_\ell)$ is a finite-dimensional $\mathbb{Q}_\ell$-vector space, endowed with a continuous action of the Galois group $\Gamma_{\mathbb{Q}}$. The images of such representations are not finite in general. The Langlands program predicts that such representations should also correspond to automorphism representations.

How to come back from cohomology to algebraic geometry? This is the subject of the conjectural theory of motives. There are many conjectures related to motives, such as the Tate conjecture and the Hodge conjecture. Of course one cannot expect to completely recover a variety from its cohomology. The goal of the theory of motives is to understand exactly what information is preserved when going from geometry to cohomology.