Galois Deformation Theory

Ashwin Iyengar

Contents

1 Lecture 1

This course is an introduction to the theory of Galois representations and their deformation theory. The primary motivation for such a theory is to try to understand the p-adic variation of continuous representations of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

This topic, initially studied in Mazur's seminal article [Maz89], has garnered a lot of attention in the last 25 years, especially due to the proof of Fermat's Last Theorem by Wiles and Taylor–Wiles. Although I do not intend to cover modularity in much detail in this course, it is worth first giving a brief overview of how a Galois deformation ring is used in a modularity lifting theorem, so that I can pretend this course is about "number theory", when in reality it's about commutative algebra and representation theory. The original modularity lifting theorem was used to prove Fermat's Last Theorem, so let's start there.

1.1 Fermat

If $a^p + b^p + c^p = 0$ with $abc \neq 0$ is a counterexample, consider the elliptic curve (over $\mathbb{Q}$)

$$E : y^2 = x(x - a^p)(x + b^p).$$

One can show that this is a **semistable** elliptic curve, meaning that at the primes where E has bad reduction, it is of multiplicative type. This is another way of saying that when you take a minimal Weierstrass model and form the base change $E_{\mathbb{F}_p}$ and complete at the singularity you get $\mathrm{Spf}\, k[\![x, y]\!]/(xy)$.

A good replacement for E (which actually determines E up to isogeny, if you vary p) is the p-adic Tate module. Recall that E has a group structure, so we can define

$$T_p(E) = \varprojlim_n E(\overline{\mathbb{Q}})[p^n] \cong \mathbb{Z}_p^2.$$

which has a continuous linear action of $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Incidentally, $T_\ell(E) \cong H^1_{\text{ét}}(E_{\overline{\mathbb{Q}}}, \mathbb{Z}_p)^\vee$, and this is Galois equivariant. This gives a representation

$$\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$$

which satisfies a bunch of nice properties. The mod p reduction $\overline{\rho}_{E,p}$ does as well. We want to show that the fact that they satisfy a bunch of nice properties leads to some kind of contradiction. So how do we do that?

Well, we want to show that $\overline{\rho}_{E,p}$ satisfies some a *remarkable* property, which contradicts the nice property. I was lazy and didn't write down the nice properties, but we will next focus on the remarkable property, since it's the key to this argument.

1.2 Modularity

The remarkable property is called *modularity.* To explain this, we need to sidestep and talk about modular forms.

If $f = \sum_{n\geq 1} a_n q^n$ is a weight 2 normalized cuspidal new eigenform of level $\Gamma_0(N)$, the **Eichler–Shimura construction** associates to it an elliptic curve E_f appearing as a direct summand of $J_0(N)$, the Jacobian of $X_0(N)$, which is an algebraic curve whose complex points are $\Gamma_0(N)\backslash\mathcal{H}$.

A fact: $\rho_{f,p} := \rho_{E_f,p}$ is unramified at $\ell \nmid pN$, which means that $\rho_{f,p}(I_{\mathbb{Q}_\ell}) = 1$. Thus we can state that this elliptic curve satisfies the important **Eichler–Shimura relation**, which says that

$$\operatorname{tr}(\rho_{f,p}(\mathrm{Frob}_\ell)) = a_\ell \text{ and } \det(\rho_{f,p}(\mathrm{Frob}_\ell)) = \ell.$$

Saying that f is an eigenform in this context means that $T_\ell \cdot f = a_\ell f$, where T_ℓ is the usual Hecke operator in $\mathrm{End}(S_2(\Gamma_0(N)))$. Let $\mathbb{T}(N)$ denote the subring of $\mathrm{End}(S_2(\Gamma_0(N)))$ generated by T_ℓ for each $\ell \nmid Np$.

Definition 1.2.1. If A is a topological ring, a continuous representation

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(A)$$

is *modular* if there exists an integer $N > 0$ and a homomorphism $\pi : \mathbb{T}(N) \to A$ such that

- ρ is unramified outside of Np
- for every $\ell \nmid Np$,
$$\operatorname{tr}(\rho(\mathrm{Frob}_\ell)) = \pi(T_\ell) \text{ and } \det(\rho(\mathrm{Frob}_\ell)) = \ell.$$

We say an elliptic curve over $\mathbb{Q}$ is modular if $\rho_{E,p}$ is modular for some (equivalently any, as it turns out) prime p.

Fact 1.2.2. *An elliptic curve E over $\mathbb{Q}$ is modular if and only if there exists a weight 2 normalized cuspidal neweigen form f of level $\Gamma_0(N_E)$ as above satisfying*

$$\rho_{f,p} \cong \rho_{E,p}.$$

Here N_E is the conductor of E, defined by counting the primes of bad reduction for E with multiplicities depending on the reduction type.

Theorem 1.2.3 (Wiles, Taylor–Wiles)**.** *Every semistable elliptic curve over $\mathbb{Q}$ is modular.*

In fact, something stronger is true:

Theorem 1.2.4 (Breuil–Conrad–Diamond–Taylor)**.** *Every elliptic curve over $\mathbb{Q}$ is modular.*

So how do you prove such a theorem? First, assume that you know that $\overline{\rho}_{E,p}$ is modular for some prime p. This by itself is not enough; this only says that there exists some newform f such that $\rho_{E,p} \cong \rho_{f,p} \bmod p$. We need isomorphism on the nose.

This is where Wiles's work comes in. The rough idea is that there is a ring R parametrizing all "nice"[1] lifts of $\overline{\rho}_{E,p}$ (including $\rho_{E,p}$ itself), and there's a ring $\mathbb{T}$ parametrizing all nice *modular* lifts of $\rho_{E,p}$. The former is a Galois deformation ring, and the latter is a certain kind of Hecke algebra $\mathbb{T}$.

The way this works is roughly that if A is a certain kind of ring with a surjection onto $\mathbb{F}_p$, then

$$\{R \to A\} = \left\{\text{nice } \rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(A) \text{ lifting } \overline{\rho}_{E,p}\right\}.$$

In particular taking $A = R$ itself we get a universal nice lift $\rho_R : G_{\mathbb{Q}} \to \mathrm{GL}_2(R)$, which every other lift is specialized from. Also

$$\{R \to A\} = \left\{\text{nice modular } \rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(A) \text{ lifting } \overline{\rho}_{E,p}\right\}.$$

[1] What does nice mean? Remember that we said that $\rho_{E,p}$ is nice. The definition of nice applies to more general ρ.

In particular taking $A = \mathbb{T}$ itself we get a universal nice modular lift $\rho_{\mathbb{T}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T})$, which every other lift is specialized from.

But now notice that $\rho_{\mathbb{T}}$ therefore corresponds to some map $R \to \mathbb{T}$. The point is now to show that this map is an isomorphism! If you do this, this implies that $\rho_R \cong \rho_{\mathbb{T}}$, so every nice lift is actually modular, and you're done.

Constructing R is "easy", once you understand the basics of Galois deformation theory. Understanding its properties requires some work. Constructing $\mathbb{T}$ is a bit more subtle, but is not the hard part of the argument. For both, one of the subtleties is figuring out what "nice" should mean.

Finally, note that we didn't justify the fact that $\overline{\rho}_{E,p}$ is modular for some p. This follows from a deep theorem of Langlands–Tunnell, which proves this when $p = 3$ and $\overline{\rho}_{E,3}$ is irreducible. When it's reducible, you can perform some tricks involving the primes 3 and 5 to conclude the same thing.

1.3 Finishing Fermat

Recall we had $a^p + b^p + c^p = 0$ with p odd and $abc \neq 0$. We can also assume $a \equiv -1 \mod 4$ and $2 \mid b$. We then constructed an elliptic curve $E : y^2 = x(x - a^p)(x + b^p)$, and looked at $\rho_{E,p}$. One can compute the conductor is

$$N_E = \prod_{\ell \mid abc} \ell.$$

So the theorem says that E is modular, so there's a newform f of level N_E such that $\rho_{E,p} \cong \rho_{f,p}$.

We know that $\rho_{E,p}$ is unramified outside of pN_E. In fact, Frey and Serre show that $\rho_{E,p}$ is actually unramified outside of $2p$. Moreover, a level-lowering theorem of Ribet (called the ϵ-conjecture) says that in this situation there exists a weight 2 newform g of level $\Gamma_0(2)$ such that

$$\overline{\rho}_g \cong \overline{\rho}_{E,p}$$

But

$$\dim S_2(\Gamma_0(2)) = \mathrm{genus}(X_0(2)) = 0,$$

so we get a contradiction.

The rest of the course won't really involve modular forms and Hecke algebras. Instead, we'll focus on how to construct the ring R.